Indice

CAPÍTULO 1

Lógica y demostraciones

Contents

1.1. Lógica proposicional

(Ref.: Sec. 1.1, p. 1, Rosen)

1.1.1. Proposición

Definición. Una *proposición* es una oración que es, o bien verdadera, o bien es falsa, pero no ambas cosas a la vez. *Notación*: para las proposiciones emplearemos letras y, por convenio, empezaremos con p, q, r, s, ..., también usaremos P, Q, R, S, ..., y cuando no alcanza también con α, β, γ, ...

1.1.2. Valor de verdad

Definición. El Valor de Verdad (VV) de una proposición dada, o bien es verdadero si la proposición es verdadera, o bien es falsa en caso contrario. *Notación*: en el primer caso simbolizaremos con T y con F en el segundo caso.

Observación. Denotaremos "verdadero" con T, como en estas notas, aunque también se suele usar V, como en el texto de referencia [4]. Un motivo de la primera elección es para aminorar confusiones con el símbolo $\vee$.

Observación. También se suele simbolizar falso y verdadero con 0 y 1, respectivamente, lo cual es una notación controversial porque 0 ni 1 son valores lógicos, no obstante, se encuentra muy difundida, *e.g.* en técnicas digitales, en la Sec. 2.7 del texto de referencia [4], etc.

1.1.3. Proposición compuesta

Definición. Una *proposición compuesta* es un proposición obtenida por la combinación de una o más proposiciones dadas mediante el uso de *operadores (o conectivos) lógicos*.

1.1.4. Tabla de verdad

Definición. La Tabla de Verdad (TV) muestra en forma sistemática los valores de verdad de una proposición compuesta en función de los *todas las combinaciones posibles* de los valores de verdad de las proposiciones que la componen.

1.1.5. Operadores o conectivos lógicos

Comentario. Consideraremos 6 operadores (o conectivos) lógicos:

1) Negación (**not**)
2) Conjunción (**and**)
3) Disyunción (inclusiva) (**or**)
4) Disyunción exclusiva (**xor**)
5) Implicación (*material implication*)
6) Doble implicación o bicondicional (**eqv**)

en donde, en negrita, se destacan los conectivos lógicos de uso tan frecuente que han sido incorporados en pseudolenguajes, técnicas digitales, y en lenguajes de programación.

En el libro de texto de referencia [4] se emplean casi indistintamente las frases "operador lógico" y "conectivo lógico" excepto para la negación, en donde prefiere la primera (porque sólo hay una proposición p).

Comentario. Ocasionalmente intercalaremos programas demos en algunos temas. Los mismos serán escritos en el lenguaje Python [3] y, para su seguimiento, será suficiente un conocimiento rudimentario del mismo. Con respecto a Python:

1) Es gratis, con más precisión, posee una licencia de código abierto denominada *Python Software Foundation License*, y que es compatible con la Licencia Pública General de GNU (GPL) a partir de la versión 2.1.1;
2) Está disponible para las principales plataformas (Linux, MS-Windows, Mac OS y otras), y las nuevas versiones son lanzadas simultáneamente;
3) Tiene diversos entornos integrados para el desarrollo, de cuales mencionamos el idle;
4) La distribución oficial incluye una amplia variedad de extensiones (denominadas módulos);
5) No obstante, las versiones 3.x son incompatibles hacia atrás ex-profeso con las versiones 2.x. Todos los demos en el curso emplean las versiones Python 3.x.

1.1.6. Negación

Definición. Sea p una proposición. El enunciado "no se cumple p" es otra proposición llamada la negación de p. *Notación*: la negación de p se denota con $\neg p$ y se lee "no p". La TV de la negación es la dada en la Tabla 1.1.

p	$\neg p$
F	T
T	F

Tabla 1.1: Negación (**not**).

1.1.7. Conjunción

Definición. Sean p y q proposiciones. La proposición compuesta "p y q" es la proposición que es verdadera cuando tanto p como q son verdaderas y es falsa en los demás casos. *Notación*: la conjunción de p y q se denota con $p \wedge q$ y se lee "p y q". La TV de la conjunción es la dada en la Tabla 1.2.

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

Tabla 1.2: Conjunción (**and**).

1.1.8. Disyunción (o disyunción inclusiva)

Definición. Sean p y q proposiciones. La proposición "p ó q" es la proposición que es falsa cuando tanto p como q son falsas y es verdadera en los demás casos. La TV de la disyunción inclusiva es la Tabla 1.3. *Notación*: la disyunción de p y q se denota con $p \vee q$ y se lee "p ó q".

Observación. En ciencias jurídicas, para evitar ambiguedades, se suele emplear "p y/o q", lo cual justifica el calificativo "disyunción inclusiva", esto es, $p \vee q$ es verdadera cuando, o bien p es verdadera y q es falsa, o bien p es falsa y q es verdadera, o bien ambas p y q son verdaderas.

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

Tabla 1.3: Disyunción (o disyunción inclusiva, **or**).

1.1.9. Disyunción exclusiva

Definición. Sean p y q proposiciones. La proposición "o bien p o bien q" es aquella que es verdadera cuando exactamente solo una de las proposiciones es verdadera, y es falsa en los demás casos. *Notación*: la disyunción exclusiva de p y q la denotaremos con $p \oplus q$ y se puede leer como "o bien p, o bien q". La TV de la disyunción exclusiva es la dada en la Tabla 5.10.

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Tabla 1.4: Disyunción exclusiva (**xor**).

Observación.

- En el texto de referencia [4] se emplea la notación $p \oplus q$, y es la que adoptada aquí;
- Mientras que en el texto de consulta [2] se emplea la notación $p \veebar q$.

Observación. Las TV de la disyunción exclusiva $p \oplus q$ y de $(p \wedge \neg q) \vee (\neg p \wedge q)$ son las mismas, como se muestra en la Tabla 5.11.

Tarea. Mostrar que las TV de la disyunción exclusiva $p \oplus q$ y de $\neg(p \wedge q) \wedge (p \vee q)$ son las mismas.

Observación. Una implementación de la disyunción exclusiva $p \oplus q$, teniendo en cuenta la Observ. 5.9.1, es la mostrada en la función `logical_xor(p,q)`. Tener presente que

p	q	$p \oplus q$	$(p \wedge \neg q) \vee (\neg p \wedge q)$
F	F	F	F
F	T	T	T
T	F	T	T
T	T	F	F

Tabla 1.5: Las TV de la disyunción exclusiva $p \oplus q$ y de $(p \wedge \neg q) \vee (\neg p \wedge q)$ son las mismas.

las líneas 6-12 fueron agregadas para definir un demo autocontenido pero en los subsecuentes ejemplos las omitiremos. Por otra parte, en Python se acostumbra a: (i) no poner un espacio entre el nombre de las funciones y el paréntesis de comienzo de la lista de argumentos; (ii) dejar una línea en blanco antes de que empiece una función nueva.

Observación. Líneas de código auxiliares, tales como 6-12 en la siguiente función, **deben omitirse en las evaluaciones**.

```
1  # In idle3 open this file and hit F5 ("run module").
2  def logical_xor(p,q):
3      z = (p and not q) or (not p and q)
4      return z
5
6  # Test
7  if __name__ == '__main__':
8      test_data = [ [False , False],  [False , True ],
9                    [True  , False],  [True  , True ]]
10     for (p, q) in test_data:
11         print (p, q, logical_xor(p,q))
12 # end
```

1.1.10. Tabla de verdad con más de dos proposiciones

- Con dos proposiciones p y q se observa que las TV tienen 4 filas, *e.g.* las correspondientes a los conectivos lógicos (excepto la negación);
- En general, la TV de una proposición obtenida por la combinación de n proposiciones, tendrá 2^n filas. Este resultado se demuestra en conteo (y suele preguntarse en el parcial 2, globalizador y finales!);
- Si bien no es importante el orden dado a las filas en una TV, sin embargo, puede ser conveniente adquirir un criterio sistemático, para no omitir alguna fila combinatoria y/o no repetir alguna (un error algo frecuente en evaluaciones).

Ejemplo.

- Si una proposición compuesta está formada por 2, 3, 4, y 5 proposiciones, entonces hay 4, 8, 16, y 32 filas en su TV, respectivamente, lo cual no parece tan extenso de hacer;
- Pero con 200, 300, 400, y 500 proposiciones habrán, aproximadamente, 1×10^6, 2×10^{90}, 2×10^{120}, y 3×10^{150} filas en su TV, respectivamente, lo cual es muy caro, aún computacionalmente. Adelantamos que leyes de crecimiento como 2^n, donde n es el tamaño del problema, son muy "malas noticias" en computación.

1.2. Equivalencias proposicionales

(Ref.: Sec. 1.2, p. 19, Rosen)

1.2.1. Implicación

Definición. Sean p y q proposiciones. La implicación "si p entonces q" es la proposición que es falsa únicamente cuando p es verdadera y q es falsa, y es verdadera en los demás casos. *Notación*: la implicación "si p entonces q", se denota con $p \to q$. *Nomenclatura*: en la implicación $p \to q$, la p es el *antecedente* (o *premisa* o *hipótesis*), y la q es el *consecuente* (o *conclusión* o *tesis*). La TV de la implicación es la dada en la Tabla 1.6.

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

Tabla 1.6: Implicación.

Observación.

- La definición de la implicación $p \to q$ es más general que en el lenguaje corriente, *i.e.* a diferencia del sentido común, no hay una relación "causa-efecto" entre la premisa p y la conclusión q, lo cual es sorprendente para el neófito (verlo en la Guía de Trabajos Prácticos (GTP));
- Una forma útil de entender el VV de la implicación es pensarla como un contrato legal. *Tarea*: leer el ejemplo alusivo en el libro de texto [4];

Observación. Hay muchas maneras de expresar la implicación $p \to q$ (todas se preguntan en las evaluaciones!). Mencionamos 12:

1) **Si** p**, entonces** q.
2) **Si** p**,** q.
3) p **es suficiente para** q.
4) q **si** p.
5) q **cuando** p.
6) **Una condición necesaria para** p **es** q.
7) p **implica** q.
8) p **sólo si** q.
9) **Una condición suficiente para** q **es** p.
10) q **siempre que** p.
11) q **es necesaria para** p.
12) q **se deduce de** p.

Observación. En los cursos de lógica se analiza con más cuidado el siguiente detalle en el enunciado de la implicación "si p entonces q":

- *Normalmente la palabra* **si** *introduce al antecedente*. O sea, lo que viene a continuación de la palabra **si** *es la premisa* p;
- La excepción es cuando aparece la frase **sólo si**, en donde se invierten los terminos. O sea, *lo que sigue después del* **solo si** *es la conclusión* q.

Ejemplo. [por Eli Haye]. Sea p: ser santafesino, y q: ser argentino. Se tiene:

1) Si (es santafesino), entonces (es argentino).
2) Si (es santafesino), (es argentino).
3) (Ser santafesino) es suficiente para (ser argentino).
4) (Es argentino) si (es santafesino).
5) (Es argentino) cuando (es santafesino).
6) Una condición necesaria para (ser santafesino) es (ser argentino).
7) (Ser santafesino) implica (ser argentino).
8) (Es santafesino) sólo si (es argentino).
9) Una condición suficiente para (ser argentino) es (ser santafesino).
10) (Es argentino) siempre que (sea santafesino).
11) (Ser argentino) es necesario para (ser santafesino).
12) (Ser argentino) se deduce de (ser santafesino).

Observación. Una implementación de la implicación $p \to q$ es la mostrada en la función `implicacion(p,q)`.

```
def implicacion(p,q): # donde "p" y "q" son valores booleanos
    if (p == False):
        r = True
    else:
        r = q
    return r
```

1.2.2. Recíproca, contrapositiva (o contra-recíproca) e inversa

Definición. A partir de la implicación $p \to q$ se definen:

- La proposición $q \to p$ es la *recíproca* de $p \to q$;
- La proposición $\neg q \to \neg p$ es la *contrapositiva* (o *contra-recíproca*) de $p \to q$;
- La proposición $\neg p \to \neg q$ es la *inversa* de $p \to q$.

Observación. Las TV de la implicación $p \to q$ y de su *contrapositiva* $\neg q \to \neg p$ son las mismas, ver la Tabla 1.7.

Tarea. Mostrar que las TV de la recíproca $q \to p$ y de la inversa $\neg p \to \neg q$ de la implicación $p \to q$ son las mismas.

1.2.3. Doble implicación (o bicondicional)

Definición. Sean p y q proposiciones. La doble implicación (o bicondicional) de p y q es la proposición compuesta que es verdadera cuando p y q tienen los mismos valores de verdad y es falsa en los demás casos. *Notación*: la doble implicación de p y q se denota con $p \leftrightarrow q$. La TV de la doble implicación es la dada en la Tabla 1.8.

p	q	$p \to q$	$\neg q \to \neg p$
F	F	T	T
F	T	T	T
T	F	F	F
T	T	T	T

Tabla 1.7: Las TV de la implicación $p \to q$ y de su *contrapositiva* $\neg q \to \neg p$ son las mismas.

p	q	$p \leftrightarrow q$
F	F	T
F	T	F
T	F	F
T	T	T

Tabla 1.8: Doble implicación (o bicondicional, **eqv**).

Observación. Hay varias maneras de expresar la doble implicación $p \leftrightarrow q$ (y se preguntan en las evaluaciones!). Mencionamos 4:

1) p **si y sólo si** q.
2) p **es necesario y suficiente para** q.
3) **Si** p **entonces** q **y recíprocamente**.
4) p **ssi** p.

Observación. La TV de la doble implicación (o bicondicional) $p \leftrightarrow q$ y de $(p \to q) \wedge (q \to p)$ son las mismas, ver la Tabla 1.9. Esto es útil en las demostraciones.

p	q	$p \leftrightarrow q$	$(p \to q) \wedge (q \to p)$
F	F	T	T
F	T	F	F
T	F	F	F
T	T	T	T

Tabla 1.9: Las TV de la doble implicación (o bicondicional) $p \leftrightarrow q$ y de $(p \to q) \wedge (q \to p)$ son las mismas.

Observación. Las TV del bicondicional $p \leftrightarrow q$ y de $(p \wedge q) \vee (\neg p \wedge \neg q)$ son las mismas, como se muestra en la Tabla 1.10.

Observación. Las TV del bicondicional $p \leftrightarrow q$ y de $\neg(p \oplus q)$ son las mismas, como se puede concluir al comparar las Tablas 5.10 y 1.8.

Observación. La Observ. 1.2.3 permite programar el bicondicional $p \leftrightarrow q$ con la función `bicondicional_version1(p,q)`.

```
def bicondicional_version1(p, q): # donde "p" y "q" son valores booleanos
    r = (p and q) or (not p and not q)
    return r
```

Observación. La Observ. 1.2.3 permite programar el bicondicional $p \leftrightarrow q$ con la función `bicondicional_version2(p,q)`, con menos operaciones booleanas: una binaria y una unaria.

```
def bicondicional_version2(p,q):# donde "p" y "q" son valores booleanos
    r = not logical_xor(p,q)
    return r
```

p	q	$p \leftrightarrow q$	$(p \wedge q) \vee (\neg p \wedge \neg q)$
F	F	T	T
F	T	F	F
T	F	F	F
T	T	T	T

Tabla 1.10: Las TV de la doble implicación (o bicondicional) $p \leftrightarrow q$ y de $(p \wedge q) \vee (\neg p \wedge \neg q)$ son las mismas.

prioridad de precedencia	operador lógico	nombre
1	$\neg$	negación
2	$\wedge$	conjunción (*and*)
3	$\vee$	disyunción (*or*)
4	$\rightarrow$	implicación
5	$\leftrightarrow$	doble implicación

Tabla 1.11: Reglas de precedencia de los operadores lógicos.

1.2.4. Reglas de precedencia de los operadores lógicos

- La proposición compuesta $(p \vee q) \wedge (\neg r)$ es la conjunción de $p \vee q$ y de $\neg r$;
- Para reducir el número de paréntesis se conviene que la negación se aplica antes que los demás operadores, *e.g.* la proposición $(\neg p) \wedge q$, se reduce a $\neg p \wedge q$, pero $(\neg p) \wedge q$ no es lo mismo que $\neg(p \wedge q)$;
- En general se acostumbra, si no hay ambiguedades, utilizar las Reglas de precedencia (RP) dadas en la Tabla 1.11. Empero, si hay dudas, entonces emplear los paréntesis;
- Ejemplo: la notación $p \vee q \rightarrow r$ quiere significar $(p \vee q) \rightarrow r$. De ningún modo equivale, por ejemplo, a $p \vee (q \rightarrow r)$, un *fatal error* en un examen;
- Las RP se usan libremente tanto en los libros como en la GTP y en las evaluaciones.

1.2.5. Tautología, contradicción y contingencia

Definición. Una proposición compuesta que siempre es verdadera, no importando los VV de sus proposiciones componentes, se denomina *tautología*.

Definición. Una proposición compuesta que siempre es falsa, no importando los VV de sus proposiciones componenentes, se denomina *contradicción*.

Definición. Una proposición compuesta que no es una tautología ni una contradicción se denomina *contingencia*.

Ejemplo. En la Tabla 1.12 se muestra un ejemplo de una tautología y de una contradicción.

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
F	T	T	F
T	F	T	F

Tabla 1.12: Un ejemplo de una tautología (la columna $p \vee \neg p$ siempre es T), y de una contradicción (la columna $p \wedge \neg p$ siempre es F).

Equivalencia Lógica (EL)	Ley	
$p \vee F \equiv p$ $p \wedge T \equiv p$	identidad	1
$p \vee T \equiv T$ $p \wedge F \equiv F$	dominación	2
$p \vee p \equiv p$ $p \wedge p \equiv p$	idempotencia	3
$\neg(\neg p) \equiv p$	doble negación	4
$p \vee q \equiv q \vee p$ $p \wedge p \equiv q \wedge p$	conmutativas	5

Tabla 1.13: Tabla de EL de uso **muy** frecuente (continúa en la Tabla 1.14).

EL	Ley	
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	asociativas	6
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	distributivas	7
$\neg(p \vee q) \equiv \neg p \wedge \neg q$ $\neg(p \wedge q) \equiv \neg p \vee \neg q$	De Morgan	8
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	absorción	9
$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	negación	10

Tabla 1.14: Tabla de EL de uso **muy** frecuente (continuación de la Tabla 1.13).

1.2.6. Equivalencia lógica

Definición. Se dice que las proposiciones p y q son lógicamente equivalentes (LE), o que p y q definen una equivalencia lógica, siempre que $p \leftrightarrow q$ es una tautología. *Notación*: cuando p y q son LE se denota con $p \equiv q$.

Observación. El símbolo $\equiv$ no es un operador (o conectivo) lógico, puesto que $p \equiv q$ no es una proposición compuesta, sino que quiere indicar que $p \leftrightarrow q$ es una tautología.

Ejemplo. En las Tablas 1.13-1.14 se listan las equivalencias lógicas de uso **muy** frecuente en las evaluaciones.

Ejemplo. En las Tablas 1.15-1.16 se incluye listados de EL relacionadas con condicionales y bicondicionales, respectivamente.

Tarea. Verificar cada una de las leyes listadas en las Tablas 1.13-1.16, *e.g.* como se hace en el siguiente ejemplo.

$p \to q \equiv \neg q \to \neg p$	(c1)
$p \to q \equiv \neg p \vee q$	(c2)
$\neg(p \to q) \equiv p \wedge \neg q$	(c3)
$p \vee q \equiv \neg p \to q$	(c4)
$p \wedge q \equiv \neg(p \to \neg q)$	(c5)
$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$	(c6)
$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r)$	(c7)
$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$	(c8)
$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r)$	(c9)

Tabla 1.15: Algunas EL relacionadas con condicionales.

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$	(b1)
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$	(b2)
$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$	(b3)
$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$	(b4)

Tabla 1.16: Otras EL relacionadas con bicondicionales.

p	q	$\overbrace{\neg(p \vee q)}^{P}$	$\overbrace{\neg p \wedge \neg q}^{Q}$	$P \leftrightarrow Q$
F	F	T	T	T
F	T	F	F	T
T	F	F	F	T
T	T	F	F	T

Tabla 1.17: Demostración mediante TV de las leyes de De Morgan para proposiciones en el caso $\neg(p \vee q)$.

Ejemplo. Leyes de De Morgan para dos proposiciones. En las Tablas 1.17-1.18 se demuestra, por medio de una TV que:

- $\neg(p \vee q) \equiv \neg p \wedge \neg q$, que puede enunciarse como: "no (p o q) es equivalente a (*no* p) y (no q)";
- $\neg(p \wedge q) \equiv \neg p \vee \neg q$, que puede enunciarse como: "no (p y q) es equivalente a (*no* p) o (no q)".

Ejemplo. *Consigna*: justificar, con y sin el uso de TV, si $((p \to q) \wedge (q \wedge r)) \to (p \to r)$, es una tautología, contradicción o contingencia. Solución:

- Con TV: para el hogar!
- Sin TV: considerar los pasos detallados en la Ec (1.1);
- *Comentario*: la técnica es eliminar las implicaciones, luego las negaciones, luego asociar o distribuir para obtener alguna ley conocida (*e.g.* identidad, dominación, absorción, negación, etc. Hay muchos caminos... el mejor es el de intentar, e intentar, e intentar, ...

p	q	$\overbrace{\neg(p \wedge q)}^{P}$	$\overbrace{\neg p \vee \neg q}^{Q}$	$P \leftrightarrow Q$
F	F	T	T	T
F	T	T	T	T
T	F	T	T	T
T	T	F	F	T

Tabla 1.18: Demostración mediante TV de las leyes de De Morgan para proposiciones en el caso $\neg(p \wedge q)$.

$$
\begin{aligned}
A \wedge (B \vee C) &= [(p \to q) \wedge (q \to r)] \to (p \to r) && \text{uso Tabla 1.15-c1}\\
&\equiv \neg[(p \to q) \wedge (q \to r)] \vee (p \to r) && \text{uso ley de De Morgan}\\
&\equiv [\neg(p \to q) \vee \neg(q \to r)] \vee (p \to r) && \text{elimino corchetes}\\
&\equiv \neg(p \to q) \vee \neg(q \to r) \vee (p \to r) && \text{uso Tabla 1.15-c1}\\
&\equiv \neg(\neg p \vee q) \vee \neg(\neg q \vee r) \vee (\neg p \vee r) && \text{De Morgan y saco último ()}\\
&\equiv (p \wedge \neg q) \vee (q \wedge \neg r) \vee (\neg p) \vee r && \text{asocio convenientemente}\\
&\equiv [(p \wedge \neg q) \vee \neg p] \vee [(q \wedge \neg r) \vee r] && \text{uso ley distributiva}\\
&\equiv [(p \vee \neg p) \wedge (\neg q \vee \neg p)] \vee [(q \vee r) \wedge (\neg r \vee r)] && \text{uso ley de la negación}\\
&\equiv [T \wedge (\neg q \vee \neg p)] \vee [(q \vee r) \wedge T] && \text{uso ley de identidad}\\
&\equiv (\neg q \vee \neg p) \vee (q \vee r) && \text{puedo quitar paréntesis}\\
&\equiv \neg q \vee \neg p \vee q \vee r && \text{asocio convenientemente}\\
&\equiv (\neg q \vee q) \vee (\neg q \vee r) && \text{uso ley de la negación}\\
&\equiv T \vee (\neg q \vee r) && \text{uso ley de la dominación}\\
&\equiv T && \text{es una tautología.}
\end{aligned}
\tag{1.1}
$$

1.3. Predicados y cuantificadores

(Ref.: Sec. 1.3, p. 26, Rosen)

1.3.1. Función proposicional

Definición.

- Sea $P(x)$ un enunciado que incluye a la variable $x \in D$. Se denomina Función Proposicional (FP), o predicado, al enunciado P si, para cada valor $x \in D$, se tiene que $P(x)$ es una proposición;
- Se denomina Dominio de Discurso (DD) al conjunto D del enunciado P.
- Caso con más de una variable: un enunciado de la forma $P(x_1, x_2, ..., x_n)$ es el VV de la FP P en la n-tupla $(x_1, x_2, ..., x_n)$;

Observación. Algunos conjuntos de uso frecuente:

- Enteros: $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ (notar que el 0 no-tiene signo);
- Enteros positivos: $\mathbb{Z}^+ = \{1, 2, 3, ...\}$;
- Enteros negativos: $\mathbb{Z}^- = \{..., -3, -2, -1\}$;
- Enteros **no-negativos**: $\mathbb{Z}_0^+ = \{0, 1, 2, 3, ...\}$;
- Números reales $\mathbb{R}$.

Observación. En general, el VV de una FP $P(x)$ puede ser, o bien T, o bien F, según sea el DD, como se muestra en el siguiente ejemplo.

Ejemplo. Sea el enunciado $P(x) :\ x + 1 > 2x$, con $x \in \mathbb{Z}$. Entonces

1) si el DD es el intervalo $-\infty < x < 1$, entonces $P(x)$ es T;
2) si el DD es el intervalo $1 \leq x < \infty$, entonces $P(x)$ es F.

1.3.2. Cuantificador existencial

Definición. La *cuantificación existencial* de la función proposicional P con DD D, es la proposición: $P(x)$ es verdadera para **al menos un** valor x en el DD. *Notación*. Se denota con $\exists x, P(x)$, donde $\exists$ es el **cuantificador existencial**. *Nomenclatura*. La notación $\exists x, P(x)$ se puede leer indistintamente como sigue:

- Hay **UN** x tal que $P(x)$;
- Hay **AL MENOS UN** x tal que $P(x)$;
- Para **ALGUN** x, $P(x)$;
- **EXISTE** x tal que $P(x)$.

Observación.

- Cuando todos los elementos del DD se pueden enumerar, o sea cuando x_1, x_2, ... x_n, se tiene que
$$\exists x \; P(x) \equiv P(x_1) \vee P(x_2) \vee ... \vee P(x_n) \tag{1.2}$$
puesto que la disyunción es verdadera ssi **al menos uno** de $P(x_1)$, $P(x_2)$, ..., o $P(x_n)$ es verdadero;
- Notación: el lado derecho de la Ec. (1.2) lo abreviaremos con
$$\textbf{any}\ (P(x)) = \bigvee_{i=1}^{n} P(x_i) = P(x_1) \vee P(x_2) \vee ... \vee P(x_n) \tag{1.3}$$
- La evaluación dada por la Ec. (1.2) la ejemplificaremos en un programa demo en la Sec. 1.3.5, y es tan frecuente en la práctica que en algunos lenguajes de programación, e.g. Python o Fortran, se dispone de la función intrínseca **any**.

1.3.3. Cuantificador universal

Definición. La *cuantificación universal* de la función proposicional P con DD D, es la proposición: $P(x)$ es verdadera para **todos** los valores x en el DD. *Notación*. Se denota con $\forall x, P(x)$, donde $\forall$ es el **cuantificador universal**. *Nomenclatura*. La notación $\forall x, P(x)$ se puede leer indistintamente como sigue:

- Para **TODO** x se cumple $P(x)$;
- Para **CUALQUIER** x se cumple $P(x)$;
- Para **CADA** x se cumple $P(x)$.

Observación.

- Cuando todos los elementos del DD se pueden enumerar, o sea cuando x_1, x_2, ..., x_n, se tiene que

$$\forall x, P(x) \equiv P(x_1) \wedge P(x_2) \wedge ... \wedge P(x_n) \tag{1.4}$$

  puesto que la conjunción es verdadera ssi $P(x_1)$, $P(x_2)$, ..., $P(x_n)$ son **todas** verdaderas;
- Notación: el lado derecho de la Ec. (1.4) lo abreviaremos con

$$\textbf{all}\ (P(x)) = \bigwedge_{i=1}^{n} P(x_i) = P(x_1) \wedge P(x_2) \wedge ... \wedge P(x_n) \tag{1.5}$$

- La evaluación dada por la Ec. (1.4) la ejemplificaremos en un programa demo en la Sec. 1.3.5, y es tan frecuente en la práctica que en algunos lenguajes de programación, e.g. Python o Fortran, se dispone de la función intrínseca **all**.

Observación. En la Tabla 1.19 se resume cuándo una sentencia cuantificada es T o F.

Observación. Enfatizamos la importancia que tiene el DD en los ejercicios: para una misma sentencia cuantificada, el resultado puede ser verdadero o falso dependiendo de cómo se haya definido el DD, como se muestra en el siguiente ejemplo.

Ejemplo. Evaluar el VV de $\forall x\ (x^2 \geq x)$ cuando: (i) $x \in \mathbb{R}$ (tema 1); y (ii) $x \in \mathbb{Z}$ (tema 2). Solución: sea $x^2 \geq x$. Restando x miembro a miembro, se tiene que $x^2 - x \geq x - x$, y sacando factor común x en el lazo izquierdo de esta última desigualdad queda $x(x-1) \geq 0$, cuyas soluciones son $x \leq 0$ o $x \geq 1$. En cuanto al intervalo $0 < x < 1$ se puede observar:

i) Cuando la variable x puede tomar valores *reales*, habrán (infinitos) valores de x en dicho intervalo pero, en ese caso, la última desigualdad es inválida (verificarlo!). Por eso, se concluye que $\forall x\ (x^2 \geq x)$ es F *cuando* $x \in \mathbb{R}$;
ii) Cuando la variable x sólo puede tomar valores *enteros*, no existen valores de x en dicho intervalo tales que hagan F la última desigualdad. Por tanto, en este caso se concluye que $\forall x\ (x^2 \geq x)$ es T *cuando* $x \in \mathbb{Z}$.

Observación. Hay que tener cuidado cuando se usan los cuantificadores $\forall x$ o $\exists x$. Por ejemplo, sean:

$$\begin{aligned} P(n) &: n \text{ es par} \\ Q(n) &: n \text{ es impar.} \end{aligned} \tag{1.6}$$

donde el DD es conjunto de los enteros $\mathbb{Z}$. Entonces:

- $\forall n\ (P(n) \vee Q(n))$, se puede enunciar como "para todo entero n, se tiene que n es par o n es impar", lo cual es T;
- Pero $(\forall n\ P(n)) \vee (\forall n\ Q(n))$, se puede enunciar como "todos los enteros n son pares, o todos los enteros n son impares", lo que es F;
- Se concluye que, en general,

$$\forall n\ (P(n) \vee Q(n)) \not\equiv (\forall n\ P(n)) \vee (\forall n\ Q(n)) \tag{1.7}$$

sentencia cuantificada	cuándo es T	cuándo es F
$\exists x, P(x)$	$P(x)$ es T para **AL MENOS UN** x	$P(x)$ es F para **TODO** x
$\forall x, P(x)$	$P(x)$ es T para **TODO** x	**Al menos un** x tal que $P(x)$ es F

Tabla 1.19: Casos cuando una sentencia cuantificada es T o F.

1.3.4. Negación de proposiciones cuantificadas o leyes de De Morgan generalizadas para la lógica

Teorema. Sea P una FP en un DD dado. Entonces

$$\begin{aligned} \neg(\exists x, P(x)) &\equiv \forall x \neg P(x) \\ \neg(\forall x, P(x)) &\equiv \exists x \neg P(x) \end{aligned} \tag{1.8}$$

Demostración de la primera parte (la segunda queda como tarea para el hogar):

- Suponga que $\neg(\exists x, P(x))$ es T. Eso significa que $\exists x, P(x)$ es F. Por la definición del cuantificador existencial, la proposición $\exists x, P(x)$ es F cuando $P(x)$ es F para **todo** $x \in D$. Pero si $P(x)$ es F para **todo** $x \in D$, eso significa que $\neg P(x)$ es T para **todo** $x \in D$. Por la definición del cuantificador universal, cuando $\neg P(x)$ es T para **todo** $x \in D$, la proposición $\forall x, \neg P(x)$ es T. Entonces, cuando $\neg(\exists x, P(x))$ es T, la proposición $\forall x, \neg P(x)$ también es T;
- Suponga que $\neg(\exists x, P(x))$ es F. Eso significa que $\exists x, P(x)$ es T. Por la definición del cuantificador existencial, la proposición $\exists x, P(x)$ es T cuando $P(x)$ es T para **algún** $x \in D$. Pero si $P(x)$ es T para **algún** $x \in D$, eso significa que $\neg P(x)$ es F para **todo** $x \in D$. Por la definición del cuantificador universal, cuando $\neg P(x)$ es F para **todo** $x \in D$, la proposición $\forall x, \neg P(x)$ es F. Entonces, cuando $\neg(\exists x, P(x))$ es F, la proposición $\forall x, \neg P(x)$ también es F.

1.3.5. Algoritmos para cuantificadores

Ejemplo. Algunos lenguajes de programación preven instrucciones para los cuantificadores $\exists x$ y $\forall x$ en el caso en que todos los elementos del DD se pueden enumerar (o sea x_1, x_2, ... x_n).

Consigna: dados una función proposicional P y un dominio de discurso X, escriba funciones en lenguaje Python que simulen el comportamiento de los cuantificadores existenciales y universales.

Solución: se pueden pensar implementaciones básicas (mínimas), intermedias (para entusiastas), y avanzadas (para muy entusiastas), como se hacen a continuación, en donde las funciones `any(L)` y `all(L)` son nativas de este lenguaje. La función `any(L)` devuelve verdadero si al menos un elemento de L es verdadero, y falso en caso contrario. En cambio, la función `all(L)` devuelve verdadero solo cuando todos los elementos de L son verdaderos, y falso en caso contrario.

```
# Cuantificadores existenciales y universales.
# Caso A: implementaciones basicas (minimas).
def ExisteX(P,X):
    for x in X:
        if P(x):
```

```
                return True
    return False

def ParaTodoX(P,X):
    for x in X:
        if not P(x):
            return False
    return True

# Caso B: implementaciones intermedias (para entusiastas).
def ExisteX(P,X):
    if any (P(x) for x in X):
        return True
    return False
def ParaTodoX(P,X):
    if all (P(x) for x in X):
        return True
    return False

# Caso C: implementaciones avanzadas (para muy entusiastas).
def ExisteX(P,X):
    return any(P(x) for x in X)
def ParaTodoX (P, X):
    return all(P(x) for x in X)
```

1.4. Cuantificadores doblemente anidados

(Ref.: Sec. 1.4, p. 40, Rosen)
Veremos únicamente el caso de cuantificadores doblemente anidados, a través de un ejemplo y los ejercicios en la GTP.

Ejemplo.
Exprese en palabras y determine el VV de las siguientes proposiciones cuantificadas, en donde $x, y \in \mathbb{R}$:

- Sea $\exists x \exists y\ (x + y = 17)$. En palabras: para algún x, existe un y tal que $x + y = 17$. Valor de Verdad: en este caso es posible hallar, al menos, un par x, y tal que $x + y = 17$ (*e.g.* sea el par $x = 7$ e $y = 10$). Como ambos cuantificadores son existenciales, un ejemplo es suficiente para concluir que el VV de esta proposición es T;
- Sea $\forall x \exists y\ (x + y = 17)$. En palabras: para todo x, existe un y tal que $x + y = 17$. Valor de Verdad: en este caso también es posible hallar, para cada x, un y tal que satisfaga la propiedad, y que está dado por $y = 17 - x$. Esto es, cada x tiene asegurado un y (único en cada caso) y, por eso, el VV de esta proposición es T;
- Sea $\exists x \forall y\ (x + y = 17)$. En palabras: para algún x, y para todo y, debe ser $x + y = 17$. Valor de Verdad: debería existir un x tan particular que sumándole cualquier y diera siempre 17. Pero eso no es posible, por lo que el VV de esta proposición es F;
- Sea $\forall x \forall y\ (x + y = 17)$. En palabras: para todo x, y para todo y, debe ser $x + y = 17$. Valor de Verdad: para cualquier x debería ser posible sumarle cualquier y y siempre dar 17. Otra vez, eso no es posible, por lo que el VV de esta proposición es F.

Observación.
Sin demostrarlo se tiene en general que

$$\begin{array}{ll} \exists x \exists y\ P(x,y) \equiv \exists y \exists x\ P(x,y) & \text{conmutan} \\ \forall x \forall y\ P(x,y) \equiv \forall y \forall x\ P(x,y) & \text{conmutan} \\ \forall x \exists y\ P(x,y) \not\equiv \exists y \forall x\ P(x,y) & \text{no conmutan} \end{array} \tag{1.9}$$

1.4.1. Negación en proposiciones con cuantificadores doblemente anidados

Para negar proposiciones con cuantificadores doblemente anidados, se emplea sucesivamente las reglas de negación para proposiciones con único cuantificador.

Ejemplo. Negar la proposición $\exists x \forall y\ (x + y = 17)$, donde $x, y \in \mathbb{R}$. *Solución*:

$$\begin{array}{l} \neg(\exists x \forall y\ (x+y=17)) \\ \equiv \forall x\ \neg(\forall y\ (x+y=17)) \\ \equiv \forall x\ \exists y\ \neg(x+y=17) \\ \equiv \forall x\ \exists y\ (x+y \neq 17) \end{array} \tag{1.10}$$

Observación. Cuando todos los elementos del DD se pueden enumerar, o sea x_1, x_2, ... x_n, puede ser útil pensar a los cuantificadores anidados como recorridos anidados. Por ejemplo, para determinar si $\forall x \forall y\ P(x, y)$ es T o F, recorremos todos los valores x e y de la siguiente manera. Para cada x revisamos con un recorrido anidado todos los valores de y. Si encontramos que $P(x, y)$ es T en todos los casos, la conclusión inevitable es que $\forall x \forall y\ P(x, y)$ es T. Si por el contrario, cuando encontramos el primer par de valores x e y tal que $P(x, y)$ es F, podrían haber más de un par, es suficiente para concluir que $\forall x \forall y\ P(x, y)$ es F.

1.4.2. Algoritmos para cuantificadores doblemente anidados

Como en el caso de cuantificadores simples, se pueden pensar implementaciones básicas, intermedias o avanzadas. En las implementaciones básicas tenemos

```
def ParaTodoX_ParaTodoY(P,X,Y):
    for x in X:                # lazo para cada ”x”
        for y in Y:            # lazo para cada ”y”
            if not P(x,y):     # si P (x,y) fuera True, entonces:
                return False   #   aborta lazos ”x,y”, y retorna False
    return True                # fuera de ambos lazos

def ParaTodoX_ExisteY(P,X,Y):
    for x in X:                # lazo para cada ”x”
        b = False              # inicia auxiliar (somos pesimistas)
        for y in Y:            # lazo para cada ”y”
            if P(x,y):         # si P (x,y) fuera True, entonces:
                b = True       #   encontro un P(x,y) que verifica
                break          #   y aborta lazo ”y”
        if not b:              # si nunca encontro un P(x,y) entonces:
            return False       #   aborta lazo ”x” y retorna False
    return True                # fuera de ambos lazos

def ExisteX_ParaTodoY(P,X,Y):
```

```
    for x in X:                # lazo para cada ”x”
        b = True               # inicia auxiliar (somos optimistas)
        for y in Y:            # lazo para cada ”y”
            if not P(x,y):     # si P (x,y) fuera True, entonces:
                b = False      #   encontro un P(x,y) que falla
                break          #   lo registra en ”b” y aborta lazo ”y”
        if b:                  # si encontro un P(x,y) entonces:
            return True        #   aborta lazo ”x” y retorna True
    return False               # fuera de ambos lazos

def ExisteX_ExisteY(P,X,Y):
    for x in X:                # lazo para cada ”x”
        for y in Y:            # lazo para cada ”y”
            if P(x,y):         # si P (x,y) fuera True, entonces:
                return True    #   aborta lazos ”x,y”, y retorna True
    return False               # fuera de ambos lazos
```

Mientras que para implementaciones intermedias (para los entusiastas)

```
def ParaTodoX_ParaTodoY(P,X,Y):
    for x in X:
        if not all (P(x,y) for y in Y):
            return False
    return True

def ParaTodoX_ExisteY(P,X,Y):
    for x in X:
        if not any (P(x,y) for y in Y):
            return False
    return True

def ExisteX_ParaTodoY(P,X,Y):
    for y in Y:
        if any (P(x, y) for x in X):
            return True
    return False

def ExisteX_ExisteY(P,X,Y):
    for x in X:
        if any (P(x,y) for y in Y):
            return True
    return False
```

Finalmente, como implementaciones “más avanzadas” (para los muy entusiastas)

```
def ParaTodoX_ParaTodoY(P,X,Y):
    return all(P(x, y) for x in X for y in Y)

def ParaTodoX_ExisteY(P,X,Y):
    for x in X:
        if not any(P(x,y) for y in Y):
            return False
    return True

def ExisteX_ParaTodoY(P,X,Y):
    for x in X:
        if all(P(x,y) for y in Y):
            return True
    return False

```

```
def ExisteX_ExisteY(P,X,Y):
    return any(P(x, y) for x in X for y in Y)
```

De nuevo, las instrucciones `any` y `all` son nativas de este lenguaje.

1.5. Métodos en demostraciones

(Ref.: Sec. 1.5, p. 52, Rosen)

1.5.1. Alguna terminología

Definición.

- **Axioma** o **postulado**: es una suposición no demostrable y que se supone verdadera. *Comentario*: en Física suele emplearse "principio";
- **Definición**: es una oración declarativa que describe con precisión el significado y alcance de un término (palabra, frase u otro conjunto de símbolos);
- **Demostración**: es una serie de proposiciones conexas que definen un razonamiento. Para construir una demostración hacen falta métodos para obtener nuevas proposiciones a partir de las ya dadas, en donde estas últimas pueden incluir axiomas o lemas;

- **Reglas de inferencia**: son proposiciones compuestas tautológicas. *Comentario*: sirven para obtener conclusiones válidas a partir de la veracidad de otras afirmaciones. La Tabla 1.20 lista las más usuales;
- **Teorema**: es un enunciado escrito como una implicación que se demuestra como verdadero usando una demostración. *Comentario*: se reserva para un resultado de mayor alcance o más importante;
- **Lema**: es un teorema auxiliar (de menor alcance) que se usa para demostrar otro teorema más destacado (de mayor alcance);
- **Corolario**: es una consecuencia de un teorema ya demostrado;
- **Falacia**: es una forma de razonamiento incorrecta;
- **Paradoja**: es una inconsistencia lógica. Intuitivamente, un razonamiento es inconsistente cuando contiene una ambigüedad;
- **Conjetura**: es una proposición cuyo VV es desconocido. A veces se logra probar que es T o F.

Ejemplo. Un ejemplo de una *conjetura* en computación está relacionada con el algoritmo de Collatz: elegir un entero positivo n arbitrario distinto de 1. Si n es par entonces dividirlo por 2, sino multiplicarlo por 3 y sumarle 1. Si el resultado es 1, entonces finalizar, sino repetir el proceso. La conjetura presume que n *siempre* llegará al valor 1. Una implementación de la conjetura de Collatz es la mostrada en la función `collatz(n)`.

```
def collatz (n): # conjetura de Collatz
   while (n != 1):
       if (n %2 == 0):
           n = n / 2
       else:
```

```
        n = (3 * n) + 1
    return
```

Definición. Razonamientos (o argumentos) válidos:

- Un *razonamiento* (o argumento) es una implicación formada por n proposiciones de la forma:
$$(p_1 \wedge p_2 \wedge ... \wedge p_n) \to q \tag{1.11}$$
- Las implicaciones usadas en los razonamientos suelen escribirse en forma expandida (cuando hay lugar) de la siguiente manera:
  premisa p_1: ...
  premisa p_2: ...
  ... ...
  premisa p_n: ...
  ___
  conclusión c: / $\therefore$ ...
  en donde cada premisa p de la implicación se escribe en columna, una debajo de la otra, y la conclusión c debajo de una raya horizontal, donde el símbolo $\therefore$ se lee "por lo tanto" o "luego";
- Otra notación más compacta (usada en parciales, recuperatorios y exámenes) es escribirlo en una línea de texto: p_1 **y** p_2 **y**, ..., **y** p_n, / $\therefore$ q;
- Se dice que *un razonamiento (o argumento) es válido si siempre que* **TODAS** *las premisas son* T, *la conclusión también lo es*;
- En consecuencia, demostrar que la conclusión q se deduce lógicamente de las premisas p_1, p_2, ..., p_n, es lo mismo que demostrar que la implicación $(p_1 \wedge p_2 \wedge ... \wedge p_n) \to q$ **siempre** es T;
- En un razonamiento (o argumento) válido, cuando **todas** las premisas son T, se llega (siempre) a que la *conclusión* que también es T;
- *Receta* (con TV): para determinar si un razonamiento (o argumento) es válido, se construye su TV y se mira **únicamente** las filas en donde **todas** las premisas p_1, p_2, ..., p_n son T, y se chequea que **siempre** se tiene una conclusión q también es T.

Tarea. Dadas las proposiciones p y q:

1) Demostrar que $(p \wedge (p \to q)) \to q$ es una tautología;
2) Analizar el razonamiento: p y $p \to q$, / $\therefore$ q.
3) Analizar el razonamiento:
   premisa p_1: p
   premisa p_2: $p \to q$
   ___
   conclusión c: $\therefore$ q

Ejemplo. Dadas las proposiciones r, s, t, u, analizar el razonamiento:

premisa p_1: $r \to s$
premisa p_2: $\neg s \vee t$
premisa p_3: $\neg t \vee u$
premisa p_4: $\neg u$
___
conclusión c: $\therefore$ $\neg r$

Solución:

Razonamiento	Tautología	Nombre
p $\therefore p \vee q$	$p \to (p \vee q)$	adición
$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	simplificación
p q $\therefore p \wedge q$	$(p) \wedge (q) \to (p \wedge q)$	combinación
p $p \to q$ $\therefore q$	$(p \wedge (p \to q)) \to q$	*modus pones*
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	*modus tollens*
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	silogismo hipotético
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge (\neg p) \to q$	silogismo hipotético
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	resolución

Tabla 1.20: Reglas de inferencia más usuales.

1) La única opción en p_4 para que sea T, es que u sea F;
2) Comoo u es F, la única opción en p_3 para que sea T, es que t sea F;
3) Como t es F, la única opción en p_2 para sea T, es que s sea F;
4) Como s es F, la única opción en p_1 para que sea T, es que r sea F, entonces $\neg r$ es T;
5) Como $\neg r$ es T, la conclusión c es T, por lo que el razonamiento es válido.

1.5.2. Métodos en demostraciones

Definición.

- Muchos teoremas son implicaciones de la forma $p \to q$;
- Notar que una implicación $p \to q$ es T excepto cuando p es T y q es F;
- Cuando se demuestra que $p \to q$ es T, hay que probar que q es T cuando p lo es, o sea, no se demuestra que q sea T (en forma aislada);
- Existen diversas formas para realizar una demostración.

Definición.

- **Demostración directa** (DeD): la implicación $p \to q$ se puede probar comprobando que si p es T entonces q también lo es. *Receta*: se asume que p es T y, usando definiciones y teoremas dados, se comprueba que q también debe ser T;
- **Demostración indirecta** (DeI): como la implicación $p \to q$ es LE a su contrapositiva (o contra-recíproca) $\neg q \to \neg p$, la implicación $p \to q$ se puede probar demostrando que su contrapositiva (o contra-recíproca) es T; *Receta*: se asume que $\neg q$ es T y, usando definiciones y teoremas dados, se comprueba que $\neg p$ también debe ser T;

- **Demostración vacua** [en $p \to q$ cuando p es F]: suponga que la premisa es F, en ese caso la implicación es T porque tiene las formas $F \to T$ o $F \to F$, las cuales son ambas T;
- **Demostración trivial**: [en $p \to q$ cuando q es T]: suponga que la conclusión es T, en ese caso la implicación es T porque tiene las formas $F \to T$ o $T \to T$, las cuales son ambas T;
- **Demostración por contradicción** (o **por Reducción al Absurdo**) (DrA): suponga que se puede hallar una contradicción q (o sea una proposición compuesta q que siempre es F) tal que $\neg p \to q$ fuera T. Para que el caso particular $\neg p \to F$ resulte T, la única chance es que p también debe ser T. De ese modo se tiene $\neg T \to F \equiv F \to F \equiv T$.
- **Demostración por resolución**: para probar una implicación de la forma $(p_1 \vee p_2 ... \vee p_n) \to q$ se puede optar en emplear la EL dada por $(p_1 \vee p_2 ... \vee p_n) \to q \equiv (p_1 \to q) \wedge (p_2 \to q) \wedge ...(p_n \to q)$.

Ejemplo. Sea $\neg p \to (r \wedge \neg r)$. Tenemos que la proposición compuesta $(r \wedge \neg r)$ es una contradicción (siempre es F sin importar los VV de r). Si la implicación dada fuera T, entonces p tiene que ser T;

Observación. Una Demostración Indirecta (DeI) puede re-escribirse como una Demostración por Reducción al Absurdo (DrA). En una DeI de que $p \to q$ es T, utilizamos una DeD aplicada a la contrapositiva $\neg q \to \neg p$, *i.e.* asumimos que $\neg q$ es T y, usando definiciones y teoremas dados, se comprueba que $\neg p$ también lo es. Para re-escribir una DeI de $p \to q$ como una DrA, suponemos que tanto la premisa p como la conclusión negada $\neg q$ son T. Luego usamos la DeD en $\neg q \to \neg p$ para concluir que $\neg p$ también debe ser T, lo que da lugar a la contradiccón $p \wedge \neg p$, completando una DeD.

Observación. Las TV de la implicación $p \to q$ y de $(p \wedge \neg q) \to (r \wedge \neg r)$ son las mismas, como se muestra en la Tabla 1.21.

Observación. Para probar la implicación $p \to q$:

- En una DeD no suponemos que la conclusión q fuera F, sino que asumimos a la premisa p como T, y comprobamos si la conclusión q también resulta T;
- En una DeI suponemos que la premisa p es F, y comprobamos si la contrapositiva $\neg q \to \neg p$ fuera T;
- En una DrA suponemos que la premisa p es T y que la conclusión q es F, y tratamos de llegar a alguna contradicción $r \wedge \neg r$.

Definición. Un entero n es par si existe un entero k tal que $n = 2k$. Un entero n es impar si existe un entero k tal que $n = 2k + 1$. Observación: un entero n, o bien es par, o bien es impar.

Ejemplo. Demostrar: si (n^2 es entero par), entonces (n es entero par). Solución. Sean p : n^2 es entero par, y q : n es entero par. La contrapositiva es: si n es entero impar, entonces n^2 es entero impar. DeI: si n es un entero impar, entonces usamos la definición de entero impar para escribir $n = 2k + 1$, donde k es un entero. Elevando al cuadrado lado a lado

p	q	r	$\alpha \equiv p \to q$	$p \wedge \neg q$	$r \wedge \neg r$	$\beta \equiv (p \wedge \neg q) \to (r \wedge \neg r)$
F	F	F	F	F	F	T
T	F	F	F	T	F	F
F	T	F	T	F	F	T
T	T	F	T	F	F	T
F	F	T	F	F	F	T
T	F	T	F	T	F	F
F	T	T	T	F	F	T
T	T	T	T	F	F	T

Tabla 1.21: Las TV de la implicación $p \to q$ y de $(p \wedge \neg q) \to (r \wedge \neg r)$ son las mismas.

$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2\tilde{k} + 1$, donde $\tilde{k} = 2k^2 + 2k$ es otro entero. Se tiene que $n^2 = 2\tilde{k} + 1$, lo que indica que n^2 es entero impar.

Ejemplo. Demostrar: si $(x + y) \geq 2$, entonces $x \geq 1 \vee y \geq 1$, con $x, y \in \mathbb{R}$.

Solución. Sean $p : (x + y) \geq 2$, $q : x \geq 1 \vee y \geq 1$, donde

- DeI: su contrapositiva es si $x < 1 \wedge y < 1$, entonces $(x + y) < 2$, con $x, y \in \mathbb{R}$. En este caso asumimos $x < 1$ e $y < 1$, luego sumamos cada desigualdad para obtener $x + y < 2$, con lo cual $\neg p$ es T;
- DrA: asumimos que la premisa p y conclusión negada $\neg q$ son ambas T. Pero si $\neg q$ es T, ya vimos en el caso anterior que $\neg p$ también es T. Así llegamos a la contradicción $p \wedge \neg p$. La única chance es concluir que q es T.

Ejemplo. (demostración por casos) Probar que $|xy| = |x||y|$, con $x, y \in \mathbb{R}$, donde $|x| = x$ cuando $x \geq 0$, pero $|x| = -x$ cuando $x < 0$.

Solución. Dados los signos de x, y en los 4 cuadrantes, podemos escribir la implicación compuesta $(p_1 \vee p_2 \vee p_3 \vee p_4) \to q \equiv (p_1 \to q) \wedge (p_2 \to q) \wedge (p_3 \to q) \wedge (p_4 \to q)$, donde

a) p_1: $x \geq 0 \wedge y > 0$ (primer cuadrante). Aquí, si $x \geq 0$ e $y > 0$, entonces $xy \geq 0$, por lo que $|xy| = xy = |x||y|$;
b) p_2: $x < 0 \wedge y \geq 0$ (segundo cuadrante). Ahora, si $x < 0$ e $y \geq 0$, entonces $xy \leq 0$, por lo que $|xy| = -xy = (-x)y = |x||y|$;
c) p_3: $x < 0 \wedge y < 0$ (tercer cuadrante). Pero si $x < 0$ e $y < 0$, entonces $xy > 0$, por lo que $|xy| = xy = (-x)(-y) = |x||y|$;
d) p_4: $x \geq 0 \wedge y < 0$ (cuarto cuadrante). Finalmente, si $x \geq 0$ e $y < 0$, entonces $xy \leq 0$, por lo que $|xy| = -xy = x(-y) = |x||y|$.

Definición. Un número real x es racional si existen dos enteros p y q, con $q \neq 0$, tales que $x = p/q$. Un número real que no es racional es irracional.

Ejemplo. Demostrar usando una DrA que $\sqrt{2}$ no es un número racional. Solución. Sea p : $\sqrt{2}$ es irracional. En una DrA suponemos que $\neg p$ es T. Si $\sqrt{2}$ fuera racional, entonces existen dos enteros positivos a y b tales que $\sqrt{2} = a/b$, con $b \neq 0$, donde a y b no tienen factores comunes (i.e. no existe un entero h que divida a ambos sino simplificaríamos). A continuación hacemos

$$\begin{aligned} \sqrt{2} &= \frac{a}{b} \quad \text{con } b \neq 0 \\ 2 &= \frac{a^2}{b^2} \\ 2b^2 &= a^2 \end{aligned} \tag{1.12}$$

La forma de la Ec. (1.12) indica que a^2 es un entero par. Si a^2 es entero par, entonces a también es un entero par, i.e. $a = 2k$, con k entero. En ese caso

$$\begin{aligned} 2b^2 &= a^2 = (2k)^2 = 2(2k^2) = 2\tilde{k} \\ \tilde{k} &= 2k^2 \quad \text{es otro entero} \end{aligned} \tag{1.13}$$

Vemos que $\neg p$ equivale, por una parte, aseverar que $\sqrt{2} = a/b$, donde a y b no tiene factores comunes pero, por otra parte, que 2 divide divide a a y b. Esto es una contradicción.

Tarea. Demostrar que la implicación $((p \to q) \wedge q) \to p$ **no es** una tautología. *Comentario*: esta implicación conduce a la (muy) conocida falacia de "afirmar la conclusión".

Ejemplo. Analizar el razonamiento:

premisa p_1:	$r \to s$
premisa p_2:	$\neg s \vee t$
premisa p_3:	$\neg t \vee u$
premisa p_4:	$\neg u$
conclusión c:	$\therefore \quad \neg r$

Solución:

1) La única opción en p_4 para que p_4 resulte T, es que u sea F;
2) La única opción en p_3, como u es F, para que p_3 resulte T, es que t sea F;
3) La única opción en p_2, como t es F, para que p_2 resulte T, es que s sea F;
4) La única opción en p_1, como s es F, para que p_1 resulte T, es que la r sea F, entonces $\neg r$ es T, por lo que conclusión es T. Finalmente, se concluye que el razonamiento es válido.

Ejemplo. Demostrar que las únicas terminaciones de n^4 cuando $n = 10k + h$, donde k es un entero y $h = 0, 1, ..., 8, 9$, son 0,1,5,6. Usar una demostración por casos. Solución: si

$n > 0$ o $n < 0$, entonces $n^4 > 0$, por lo que basta el caso $n > 0$ y analizar por casos:

$$\begin{aligned}
(10k+0)^4 &= 10^4k^4 + 0^4 && \text{donde } 0^4 = 0\\
(10k+1)^4 &= 10^4k^4 + a_1k^3 + a_2k^2 + a_3k + 1^4 && \text{donde } 1^4 = 1\\
(10k+2)^4 &= 10^4k^4 + b_1k^3 + b_2k^2 + b_3k + 2^4 && \text{donde } 2^4 = 16\\
(10k+3)^4 &= 10^4k^4 + c_1k^3 + c_2k^2 + c_3k + 3^4 && \text{donde } 3^4 = 81\\
(10k+4)^4 &= 10^4k^4 + d_1k^3 + d_2k^2 + d_3k + 4^4 && \text{donde } 4^4 = 256\\
(10k+5)^4 &= 10^4k^4 + e_1k^3 + e_2k^2 + e_3k + 5^4 && \text{donde } 5^4 = 625\\
(10k+6)^4 &= 10^4k^4 + f_1k^3 + f_2k^2 + f_3k + 6^4 && \text{donde } 6^4 = 1296\\
(10k+7)^4 &= 10^4k^4 + g_1k^3 + g_2k^2 + g_3k + 7^4 && \text{donde } 7^4 = 2401\\
(10k+8)^4 &= 10^4k^4 + h_1k^3 + h_2k^2 + h_3k + 8^4 && \text{donde } 8^4 = 4096\\
(10k+9)^4 &= 10^4k^4 + i_1k^3 + i_2k^2 + i_3k + 9^4 && \text{donde } 9^4 = 6561
\end{aligned} \tag{1.14}$$

Tarea. Demostrar que las únicas terminaciones de n^2 cuando $n = 10k + h$, donde k es un entero y $h = 0, 1, ..., 8, 9$, son 0,1,4,5,6,9.

Ejemplo. Dado un entero n cualquiera, demostrar que

(a) n es par;
(b) $n + 1$ es impar;
(c) $3n + 1$ es impar;
(d) $3n$ es par.

son equivalentes. Solución:

(a) Si (n es par), entonces ($n + 1$ es impar). Empleando una DeD: si n es par, entonces, usando la definición de entero par, se tiene que $n = 2k$ donde k es entero. A continuación, sumamos 1, lado a lado, dando $n + 1 = 2k + 1$, lo cual, por definición de entero impar, es un entero impar.

(b) Si ($n+1$ es impar), entonces ($3n+1$ es impar). Empleando una DeD: si $n+1$ es impar, entonces, usando la definición de entero impar, se tiene que $n + 1 = 2k + 1$ donde k es entero. A continuación, multiplicamos por 3, lado a lado,

$$\begin{aligned}
3(n+1) &= 3(2k+1)\\
3n+3 &= 3\cdot 2k + 3\\
3n+1+2 &= 3\cdot 2k + 1 + 2\\
3n+1 &= 2\cdot 3k + 1\\
3n+1 &= 2\tilde{k} + 1
\end{aligned} \tag{1.15}$$

donde $\tilde{k} = 3k$ es otro entero. Por lo cual, por definición de entero impar, $3n + 1$ es un entero impar.

(c) Si ($3n$ es par), entonces (n es par). La contrapositiva es: si (n es impar), entonces ($3n$ es impar). Usando la definición de entero impar, se tiene que $n = 2k + 1$ donde k es entero. A continuación, multiplicamos por 3, lado a lado, dando $3n = 3(2k + 1) =$

$6k + 3 = 2 \cdot 3k + 2 + 1 = 2(3k + 1) + 1 = 2\tilde{k} + 1$, donde $\tilde{k} = 3k + 1$ es otro entero. Por lo cual, por definición de entero impar, $3n$ es un entero impar.

(d) Finalmente, si ($n^2 + 1$ es par), entonces (n^2 es impar). Empleando una DeD: si $n^2 + 1$ es par, entonces, usando la definición de entero par, se tiene que $n^2 + 1 = 2k$ donde k es entero. A continuación,

$$\begin{aligned} n^2 + 1 &= 2k \\ n^2 &= 2k - 1 \\ n^2 &= 2(\tilde{k} + 1) - 1 \\ n^2 &= 2\tilde{k} + 1 \end{aligned} \tag{1.16}$$

donde $\tilde{k} = k - 1$ es otro entero. Por lo cual, por definición de entero impar, $n^2 + 1$ es un entero impar.

CAPÍTULO 2

Principios de inducción

Contents

2.1. Algunas conjeturas

Conjetura. De la Tabla 2.1 se puede conjeturar que la suma de los n primeros enteros impares es igual a n^2. Pero una tabla de valores, por mas extensa que sea, no es una prueba que permita inferir que se cumple para todos los enteros n posibles. Hace falta alguna técnica que demuestre o refute este tipo de conjetura.

Conjetura. Sea $f(n) = n^2 - 3n - 80$ con $n \in \mathbb{Z}^+$. Si calculamos $f(n)$ para los primeros 11 valores de n resulta $f(n) < 0$, por lo que se podría conjeturar que $f(n) < 0$ para todo $n \in \mathbb{Z}^+$. Pero para $n = 12$ se obtiene $f(12) = 8$, por lo que esta conjetura es F.

Conjetura. Sea $f(n) = n^2 + n + 41$ con $n \in \mathbb{Z}^+$. Si calculamos $f(n)$ para los primeros 39 valores de n resulta $f(n)$ es un entero primo, i.e. solo divisible por 1 y por si mismo, por lo que se podría conjeturar que $f(n)$ es un entero primo para todo $n \in \mathbb{Z}^+$. Pero, cuando $n = 40$, se obtiene $f(40) = 1681$, el cual no es un entero primo porque se puede expresar como $1681 = 41^2$. Por lo anterior, esta conjetura también es F.

número de sumandos n	sumatoria de los n primeros enteros impares	resultado	conjetura
1	1	1	1^2
2	$1 + 3$	4	2^2
3	$1 + 3 + 5$	9	3^2
4	$1 + 3 + 5 + 7$	16	4^2
5	$1 + 3 + 5 + 7 + 9$	25	5^2

Tabla 2.1: Suma de los primeros n enteros impares.

2.2. Principio de inducción

Intro. El Principio de Inducción Matemática (PIM) (Sec. 3.3, p. 222, Rosen; Sec. 1.7, p. 53, Johnsonbaugh) lo usaremos para demostrar proposiciones cuantificadas de la forma $\forall n\ P(n)$, donde $P(n)$ es una FP en el entero n, mientras que el DD es el conjunto de los enteros a partir de un entero n_0 dado, i.e. el conjunto $\{n_0, n_0 + 1, n_0 + 2, ...\}$.

Enunciado. Sea la proposición cuantificada de la forma $\forall n\ P(n)$, donde $P(n)$ es una FP en el entero n, mientras que el DD es el conjunto de los enteros a partir de un n_0 dado. El PIM sostiene que si se cumplen tanto el PB como el PI, en donde:

- Paso Base (PB) (cuando $n = n_0$): se demuestra que $P(n_0)$ es T;
- Paso de Inducción (PI): se demuestra que la implicación $P(n) \to P(n + 1)$ es T para algún entero $n \geq n_0$, arbitrario pero fijo;

entonces $P(n)$ vale para todos los enteros $n \geq n_0$. El PIM puede simbolizarse con la regla de inferencia compuesta dada por la Ec. (2.1).

$$\begin{aligned} &[P(n_0) \wedge H(n)] \to \left[\forall n :\ P(n) \quad \text{con } n \in \mathbb{Z}^+_{n_0}\right] \quad \text{, en donde} \\ &H(n) \equiv (P(n) \to P(n + 1)) \quad \text{para algún } n \geq n_0 \text{ arbitrario pero fijo.} \end{aligned} \tag{2.1}$$

Observación.

i) En los ejercicios frecuentemente es $n_0 = 0$, $n_0 = 1$ u, ocasionalmente, $n_0 > 1$;
ii) La frase $n > n_0$ arbitrario pero fijo en la implicación de la Ec. (2.1) es fundamental, e.g. si por error uno indicara ahí para "todo" n ahí, entonces se estaría aseverando algo que todavía no se ha demostrado, i.e. hay que probar $P(n + 1)$ a través de la verdad de la implicación $P(n) \to P(n + 1)$ cuando se asume que $P(n)$ es T;
iii) El antecedente de la implicación en $H(n)$, que se asume T cuando se demuestra el PI, frecuentemente es denominado como la Hipótesis Inductiva (HI).

Ejemplo. [PIM con una igualdad en donde $n_0 = 1$]: suma de Gauss. Demostrar usando el PIM que

$$\underbrace{1 + 2 + 3 + ... + n}_{I_n} = \underbrace{\frac{n(n + 1)}{2}}_{D_n} \tag{2.2}$$

para todos los enteros n positivos. Solución:

- PB ($n = 1$): en el lado izquierdo $I_1 = 1$, mientras que en el lado derecho $D_1 = 1{\cdot}2/2 = 1$. Como se cumple la igualdad $I_1 = D_1$, se verifica el PB.
- PI: asumimos que la HI dada por la Ec. (2.2) es T para algún entero $n \geq 1$ arbitrario

pero fijo, y planteamos:

$$\begin{aligned} I_{n+1} &= \{1 + 2 + 3 + ... + n\} + (n + 1) && \text{; introducimos la HI en } \{...\} \\ &= \frac{n(n+1)}{2} + (n + 1) && \text{; sumamos fracciones} \\ &= \frac{n(n+1) + 2(n+1)}{2} && \text{; sacamos factor común } (n+1) \\ &= \frac{(n+1)(n+2)}{2} \equiv D_{n+1} \end{aligned} \tag{2.3}$$

por lo que $I_{n+1} = D_{n+1}$, y se cumple el PI.

Ejemplo. [PIM con una igualdad en donde $n_0 = 1$]: suma de los primeros n enteros impares. Demostrar usando el PIM que

$$\underbrace{1 + 3 + 5 + ... + (2n - 1)}_{I_n} = \underbrace{n^2}_{D_n} \tag{2.4}$$

para todos los enteros n positivos. Solución:

- PB ($n = 1$): en el lado izquierdo $I_1 = 1$, mientras que en el lado derecho $D_1 = 1^2 = 1$, y se cumple la igualdad $I_1 = D_1$.
- PI: asumimos que la HI dada por la Ec. (2.4) es T para algún entero $n \geq 1$ arbitrario pero fijo, y planteamos:

$$\begin{aligned} I_{n+1} &= \{1 + 3 + 5 + ... + (2n - 1)\} + 2((n + 1) - 1) && \text{; introducimos la HI en } \{...\} \\ &= n^2 + 2(n + 1) && \text{; prop. distributiva} \\ &= n^2 + 2n + 2 && \text{; cuadrado del binomio} \\ &= (n + 1)^2 \equiv D_{n+1} \end{aligned} \tag{2.5}$$

por lo que $I_{n+1} = D_{n+1}$, y se cumple el PI.

Ejemplo. [PIM con una desigualdad en donde $n_0 = 1$]. Demostrar usando el PIM que

$$\underbrace{n}_{I_n} < \underbrace{2^n}_{D_n} \tag{2.6}$$

para todos los enteros n positivos. Solución:

- PB ($n = 1$): en el lado izquierdo $I_1 = 1$, mientras que en el lado derecho $D_1 = 2^1 = 2$, y se cumple la desigualdad $I_1 < D_1$.
- PI: asumimos que la HI dada por la Ec. (2.6) es T para algún entero $n \geq 1$ arbitrario pero fijo, y planteamos:

$$\begin{aligned} I_{n+1} &= \{n\} + 1 && \text{; introd. HI en } \{...\} \\ &< 2^n + 1 && \text{; reemplazo } 1 < 2^n \text{ para } n > 0 \\ &< 2^n + 2^n && \text{; usamos } A + A = 2A \\ &= 2 \cdot 2^n = 2^{n+1} \equiv D_{n+1} && \text{; pot. de igual base} \end{aligned} \tag{2.7}$$

por lo que $I_{n+1} < D_{n+1}$, y se cumple el PI.

Ejemplo. [PIM con una desigualdad en donde $n_0 = 4$]. Demostrar usando el PIM que

$$\underbrace{2^n}_{I_n} < \underbrace{n!}_{D_n} \tag{2.8}$$

para todos los enteros $n \geq 4$. Solución:

- PB ($n = 4$): en el lado izquierdo $I_4 = 2^4 = 16$, mientras que en el lado derecho $D_4 = 4! = 24$, y se cumple la desigualdad $I_4 < D_4$.
- PI: asumimos que la HI dada por la Ec. (2.8) es T para algún entero $n \geq 4$ arbitrario pero fijo, y planteamos:

$$\begin{aligned} I_{n+1} &= 2^{n+1} && \text{; potencia de igual base} \\ &= \{2^n\} \cdot 2 && \text{; introd. HI en \{...\} y permutamos} \\ &< 2 \cdot \{n!\} && \text{; usamos } 2 < n+1 \text{ para } n \geq 4 \\ &< (n+1) \cdot (n!) && \text{; usamos def. de factorial} \\ &= (n+1)! \equiv D_{n+1} && \text{; pot. de igual base} \end{aligned} \tag{2.9}$$

  por lo que $I_{n+1} < D_{n+1}$, y se cumple el PI.

Ejemplo. [PIM cuando no es una igualdad ni una desigualdad, en donde $n_0 = 1$]: Demostrar usando el PIM que $(n^3 - n)$ es divisible por 3, para todos los enteros positivos n. Solución:

- Previo: por ejemplo, como $8 \div 4 = 2$, y $8 \mod 4 = 0$, decimos que 8 es divisible por 4. En general decir que un entero B es divisible por otro entero positivo A, significa que $B \mod A = 0$. En particular, como $0 \div 3 = 0$ y $0 \mod 3 = 0$, decimos en general que **cero es divisible por cualquier entero positivo**.
- PB ($n = 1$): tenemos $P(1) = 1^3 - 1 = 0$. Como 0 es divisible por 3, se concluye que el PB es Verdadero (por *True*) (T).
- PI: asumimos que la HI dada por:

$$P(n) : \underbrace{(n^3 - n)}_{I_n} \text{ es divisible por 3} \tag{2.10}$$

  es T para algún entero $n \geq 1$ arbitrario pero fijo, y planteamos:

$$\begin{aligned} I_{n+1} &= (n+1)^3 - (n+1) && \text{; desarrollamos } (...)^3 \\ &= (n^3 + 3n^2 + 3n + 1) - (n+1) && \text{; reagrupamos monomios} \\ &= \underbrace{\{(n^3 - n)\}}_{\text{por HI es divisible por 3}} + \underbrace{3(n^2 + n)}_{\text{3 veces un entero}} \end{aligned} \tag{2.11}$$

  por lo que $P(n+1)$ también es divisible por 3, y se cumple el PI.

Observación. Los ejemplos de uso del PIM en ejercicios relacionados con *conjuntos* rehacerlos después de haber visto dicho tema.

Teorema. Si un conjunto finito A tiene n elementos, entonces $|\mathcal{P}(A)| = 2^n$, para todo entero $n \geq 0$. Demostración: (i) por PIM (en el parcial 1); y (ii) por conteo (después, en el parcial 2).

- PB si $n = 0$, entonces no hay elementos, y se reduce al conjunto vacío. El único subconjunto del conjunto vacío es el conjunto vacío. Así que en el lado izquierdo $I_0 = 1$, mientras que en el lado derecho $D_0 = 2^0 = 1$, y se cumple la igualdad $I_1 = D_1$.
- PI: cuando $n \geq 0$:

  i) Sea A_{n+1} el conjunto con $n + 1$ elementos, y sea A_n el conjunto obtenido de A_{n+1} al eliminar un elemento cualquiera x, por lo que A_n tiene n elementos;
  ii) Notar que cada subconjunto de $\mathcal{P}(A_{n+1})$ que contiene a un elemento genérico x, se lo puede coordinar de un modo único con un subconjunto que no lo contiene. Por eso, exactamente la mitad de los subconjuntos de $\mathcal{P}(A_{n+1})$ contienen al elemento x, y la otra mitad no;
  iii) Como A_n tiene n elementos, podemos utilizar la HI para concluir que $|\mathcal{P}(A_n)| = 2^n$;
  iv) Pero los subconjuntos de $\mathcal{P}(A_n)$ son los de $\mathcal{P}(A_{n+1})$ que no contienen al elemento x y su número es la mitad, recordar la coordinación entre $\mathcal{P}(A_n)$ y $\mathcal{P}(A_{n+1})$, o sea $|\mathcal{P}(A_n)| = |\mathcal{P}(A_{n+1})|/2$. Por lo tanto $|\mathcal{P}(A_{n+1})| = 2|\mathcal{P}(A_n)| = 2 \cdot 2^n = 2^{n+1}$, que es lo predicho por la HI para $n + 1$.

Ejemplo. [PIM en leyes generalizadas de De Morgan para conjuntos, en donde $n_0 = 2$]. Demostrar usando el PIM que

$$\underbrace{\overline{\bigcap_{k=1}^{n} A_k}}_{I_n} = \underbrace{\bigcup_{k=1}^{n} \overline{A_k}}_{D_n} \tag{2.12}$$

para todos los enteros $n \geq 2$, donde $A_1, A_2, ..., A_n$ son subconjuntos de un cierto conjunto universal U. Solución:

- PB ($n = 2$): la Ec. (2.12) cuando $n = 2$ se reduce a:

  $$\overline{A_1 \cap A_2} = \overline{A_1} \cup \overline{A_2} \tag{2.13}$$

  que es una de las leyes de De Morgan para 2 conjuntos, por lo que se concluye que el PB es T.
- PI: asumimos que la HI dada por la Ec. (2.12) es T para algún entero $n \geq 2$ arbitrario

pero fijo, y planteamos:

$$
\begin{aligned}
I_{n+1} &= \overline{\bigcap_{k=1}^{n+1} A_k} && \text{; expandimos intersección generalizada} \\
&= \overline{\bigcap_{k=1}^{n} A_k \cap A_{n+1}} && \text{; reemplazo } H_n = \textstyle\bigcap_{k=1}^{n} A_k \\
&= \overline{H_n \cap A_{n+1}} && \text{; introducimos ley de De Morgan para 2 conj.} \\
&= \left\{\overline{H_n}\right\} \cup \overline{A_{n+1}} && \text{; por HI es } \overline{H_n} = \overline{\textstyle\bigcap_{k=1}^{n} A_k} = \textstyle\bigcup_{k=1}^{n} \overline{A_k} \\
&= \left\{\bigcup_{k=1}^{n} \overline{A_k}\right\} \cup \overline{A_{n+1}} && \text{; usamos propiedad asociativa} \\
&= \bigcup_{k=1}^{n+1} \overline{A_k} \equiv D_{n+1}
\end{aligned}
\tag{2.14}
$$

por lo que $I_{n+1} = D_{n+1}$, y se cumple el PI.

Tarea. [PIM en leyes generalizadas de De Morgan para conjuntos, y con $n_0 = 2$]. Demostrar usando el PIM que

$$
\overline{\bigcup_{k=1}^{n} A_k} = \bigcap_{k=1}^{n} \overline{A_k}
\tag{2.15}
$$

para todos los enteros $n \geq 2$, donde $A_1, A_2, ..., A_n$ son subconjuntos de un cierto conjunto universal U.

Ejemplo. [PIM en conjuntos, en donde $n_0 = 2$]. Demostrar usando el PIM que

$$
\underbrace{X \cap \bigcup_{j=1}^{n} A_j}_{I_n} = \underbrace{\bigcup_{j=1}^{n} (X \cap A_j)}_{D_n}
\tag{2.16}
$$

para todos los enteros $n \geq 2$, donde X es un conjunto, mientras que $A_1, A_2, ..., A_n$ son subconjuntos de un cierto conjunto universal U. Solución:

- PB ($n = 2$): la Ec. (2.16) cuando $n = 2$ se reduce a:

$$
X \cap (A_1 \cup A_2) = (X \cap A_1) \cup (X \cap A_2)
\tag{2.17}
$$

  que es una de las leyes distributivas para 2 conjuntos, por lo que se concluye que el PB es T.
- PI: asumimos que la HI dada por la Ec. (2.15) es T para algún entero $n \geq 2$ arbitrario

pero fijo, y planteamos:

$$\begin{aligned}
I_{n+1} &= X \cap \bigcup_{j=1}^{n+1} A_j && \text{; expandimos unión generalizada} \\
&= X \cap \left[\bigcup_{j=1}^{n} A_j \cup A_{n+1} \right] && \text{; introducimos prop. ditributiva} \\
&= \left\{ X \cap \bigcup_{j=1}^{n} A_j \right\} \cup (X \cap A_{n+1}) && \text{; introducimos la HI en } \{...\} \\
&= \left\{ \bigcup_{j=1}^{n} (X \cap A_j) \right\} \cup (X \cap A_{n+1}) && \text{; reagrupo} \\
&= \bigcup_{j=1}^{n+1} \left(X \cap A_j \right) \equiv D_{n+1}
\end{aligned} \tag{2.18}$$

por lo que $I_{n+1} = D_{n+1}$, y se cumple el PI.

Tarea. [PIM en leyes generalizadas de De Morgan para conjuntos, y con $n_0 = 2$]. Demostrar usando el PIM que

$$\underbrace{X \cup \bigcap_{j=1}^{n} A_j}_{I_n} = \underbrace{\bigcap_{j=1}^{n} (X \cup A_j)}_{D_n} \tag{2.19}$$

para todos los enteros $n \geq 2$, donde X es un conjunto, mientras que A_1, A_2, ..., A_n son subconjuntos de un cierto conjunto universal U.

Ejemplo. [PIM con una igualdad algo "difícil", en donde $n_0 = 1$]. Demostrar usando el PIM que

$$\underbrace{\sum_{i=1}^{n} i^3}_{I_n} = \underbrace{\left\{ \sum_{i=1}^{n} i \right\}^2}_{D_n} \tag{2.20}$$

para todos los enteros n positivos. Solución:

- PB ($n = 1$): en el lado izquierdo $I_1 = 1^3 = 1$, mientras que en el lado derecho $D_1 = 1^2 = 1$, y se cumple la igualdad $I_1 = D_1$.
- PI: asumimos que la HI dada por la Ec. (2.20) es T para algún entero $n \geq 1$ arbitrario

pero fijo, y planteamos:

$$\begin{aligned}
I_{n+1} &= \sum_{i=1}^{n+1} i^3 \\
&= \sum_{i=1}^{n} i^3 + (n+1)^3 \\
&= \left\{ \sum_{i=1}^{n} i \right\}^2 + (n+1)^3 \\
&= (1 + 2 + ... + n)^2 + (n+1)(n+1)^2 \\
&= (1 + 2 + ... + n)^2 + (1+n)(n+1)^2 \\
&= (1 + 2 + ... + n)^2 + 1 \cdot (n+1)^2 + n \cdot (n+1)^2 \\
&= (1 + 2 + ... + n)^2 + (n+1)^2 + 2[(n(n+1)/2](n+1) \\
&= (1 + 2 + ... + n)^2 + (n+1)^2 + 2[1 + 2 + ... + n](n+1) \\
&= [(1 + 2 + ... + n) + (n+1)]^2 \\
&= [1 + 2 + ... + (n+1)]^2 \equiv D_{n+1}
\end{aligned} \tag{2.21}$$

por lo que $I_{n+1} = D_{n+1}$, y se cumple el PI.

2.3. Principio de inducción fuerte (o forma fuerte de inducción)

Observación.

i) El Principio de Inducción Fuerte (PIF) (Sec. 3.3, p. 232, Rosen; Sec. 1.8, p. 65, Johnsonbaugh) lo usaremos ocasionalmente para demostrar proposiciones cuantificadas de la forma $\forall n \; P(n)$, donde el DD es el conjunto de los enteros a partir de un entero n_0 dado, i.e. el conjunto $\{n_0, n_0 + 1, n_0 + 2, ...\}$.
ii) El texto de Johnsonbaugh denota a la afirmación que se va a probar por $P(n)$ en lugar de $P(n+1)$, convención que no seguiremos aquí.
iii) Omitir la propiedad del buen orden.

Enunciado. Sea la proposición cuantificada de la forma $\forall n \; P(n)$, donde $P(n)$ es una FP en el entero n, mientras que el DD es el conjunto de los enteros a partir de un n_0 dado. El PIF sostiene que si se cumplen tanto el PB como el PI fuerte, en donde:

- PB (cuando $n = n_0$): se demuestra que $P(n_0)$ es T;
- PI fuerte: se demuestra la implicación

$$\left[\bigwedge_{k=n_0}^{n} P(k) \right] \rightarrow P(n+1) \quad \text{es T para algún entero } n > n_0 \text{ arbitrario pero fijo;} \tag{2.22}$$

entonces $P(n)$ vale para todos los enteros $n \geq n_0$. El PIF puede simbolizarse con la regla de inferencia compuesta:

$$
\begin{aligned}
&[P(n_0) \wedge H(n)] \rightarrow \left[\forall n : \ P(n) \quad \text{con } n \in \mathbb{Z}^+_{n_0}\right] \quad \text{, en donde} \\
&H(n) \equiv \left[\bigwedge_{k=n_0}^{n} P(k)\right] \rightarrow P(n+1) \quad \text{para algún } n \geq n_0 \text{ arbitrario pero fijo.}
\end{aligned}
\tag{2.23}
$$

Ejemplo. [PIF cuando no es una igualdad ni una desigualdad, y con $n_0 = 12$]: Demostrar usando el PIF que toda TP de 12 o más centavos se puede cobrar usando estampillas de 4 o 5 centavos. Solución:

- PB: aunque basta demostrar el caso $n = 12$ pero después, para poder invocar el PIF, necesitaremos también chequear todos los casos hasta $n = 16$ (después se entenderá por qué). Tenemos:

  (a) Cuando $n = 12$ usamos 3 estamp. de 4 centavos y 0 de 5 cent.
  (b) Cuando $n = 13$ usamos 2 estamp. de 4 centavos y 1 de 5 cent.
  (c) Cuando $n = 14$ usamos 1 estamp. de 4 centavos y 2 de 5 cent.
  (d) Cuando $n = 15$ usamos 0 estamp. de 4 centavos y 3 de 5 cent.
  (e) Cuando $n = 16$ usamos 4 estamp. de 4 centavos y 0 de 5 cent.

  En particular, en el caso (a), cuando $n = 12$, se cumple el PB.
- Sea la FP

  $$P(n)\text{: una TP de } n \text{ centavos se cobra usando estampillas de 4 o 5 centavos} \tag{2.24}$$

  Ahora planteamos el PIF:

  $$[P(n-3) \wedge P(n-2) \wedge P(n-1) \wedge P(n)] \rightarrow P(n+1) \tag{2.25}$$

  para algún entero $n \geq 15$. En particular, si $n = 15$, la Ec. (2.25) se reduce a

  $$[P(12) \wedge P(13) \wedge P(14) \wedge P(15)] \rightarrow P(16) \tag{2.26}$$

  Dados los valores del inciso anterior, la Ec. (2.26) es T. Además la Ec. (2.26) muestra que según el valor del entero n podemos tener estampillas de 4 y 5 centavos, o solo de 4 centavos, o solo de 5 centavos. A continuación, para un entero $n \geq 15$, arbitrario pero fijo:

  i) Si habíamos usado, al menos, 1 estampilla de 4 centavos (en forma similar a los casos (a-c), entonces la reemplazamos por 1 de 5 centavos;

  ii) Pero si no habíamos usado estampillas de 4 centavos, o sea, que habían, al menos, 3 estampillas de 5 centavos (similar al caso (d) cuando $n = 15$). Luego, reemplazamos 3 estampillas de 5 centavos por 4 estampillas de 4 centavos.

  En cualquier caso, podemos pasar de una TP de n centavos a la TP de $n + 1$ centavos, por lo que se cumple el PI.

2.4. Definiciones recursivas e inducción estructural

Observación. Este tema hacerlo después de haber visto el tema de funciones (Sec.4.1), y el de principios de inducción (Sec.2.2).

Definición. Una función $f(n)$ cuyo dominio es el conjunto de los enteros $\mathbb{Z}^+_{n_0}$, donde n_0 es un cierto entero inicial, se puede definir en forma inductiva (o recursiva (Sec. 3.4, p. 239, Rosen)) utilizando dos etapas:

- PB ($n = n_0$): se especifica el valor de la función $f(n)$ en n_0;
- Paso Recursivo (PR): se define una regla para obtener el valor de la función $f(n)$ a partir de sus valores en los enteros anteriores a n.

Observación. Las funciones definidas en forma inductiva o recursiva frecuentemente, tienen dominio en los enteros no-negativos ($n_0 = 0$) o positivos ($n_0 = 1$).

Ejemplo. [Función factorial]. La función factorial $F(n) = n!$ con dominio en los enteros no-negativos se define como

$$F(n) = \begin{cases} nF(n-1) & \text{si } n \geq 1 \\ 1 & \text{si } n = 0 \end{cases} \tag{2.27}$$

Ejemplo. [Función potencia]. La función potencia a^n con dominio en los enteros no-negativos se define como

$$a^n = \begin{cases} aa^{(n-1)} & \text{si } n \geq 1 \\ 1 & \text{si } n = 0 \end{cases} \tag{2.28}$$

Ejemplo. [Números (o sucesión) de Fibonacci]. Los números (o sucesión) de Fibonacci f_n se define como

$$f_n = \begin{cases} f_{n-1} + f_{n-2} & \text{si } n \geq 3 \\ 1 & \text{si } n = 1 \text{ o } n = 2 \end{cases} \tag{2.29}$$

Por ejemplo, los primeros 8 valores de la sucesión de Fibonacci, definida por la Ec. (2.29), se listan en la Tabla 2.2.

Ejemplo. [Sucesión de Fibonacci y PIF, en donde $n_0 = 6$]. Demostrar usando el PIF que

$$\underbrace{f_n}_{I_n} > \underbrace{\left(\frac{3}{2}\right)^{n-1}}_{D_n} \tag{2.30}$$

para todos los enteros $n \geq 6$, donde f_n es la sucesión de Fibonacci definida por la Ec. (2.29). Solución:

- PB: aunque basta demostrar el caso $n = 6$ pero después, para poder invocar el PIF, necesitaremos también chequear los casos $n = 7$ y $n = 8$ (después se entenderá por qué). Entonces, los primeros 8 valores de la sucesión de Fibonacci y de la desigualdad definida por la Ec. (2.30), se listan en la Tabla 2.2. De esta última, vemos que
  (a) Cuando $n = 6$: se tiene $I_6 = 8$ y $D_6 \approx 7.5938$, por lo que $I_6 > D_6$;

n	1	2	3	4	5	6	7	8
f_n	1	1	2	3	5	8	13	21
$(3/2)^{n-1}$	1.0000	1.5000	2.2500	3.3750	5.0625	7.5938	11.3906	17.0859

Tabla 2.2: Los primeros 8 valores de la sucesión f_n de Fibonacci, y de la función $(3/2)^{n-1}$.

(b) Cuando $n = 7$: se tiene $I_7 = 13$ y $D_7 \approx 11.3906$, por lo que $I_7 > D_7$;
(c) Cuando $n = 8$: se tiene $I_8 = 21$ y $D_7 \approx 17.0859$, por lo que $I_8 > D_8$.

En particular, en el caso (a), cuando $n = 6$, se cumple el PB.

- Sea la FP

$$P(n)\text{: se cumple que } f_n > (3/2)^{n-1} \tag{2.31}$$

Ahora planteamos el PIF:

$$[P(n-1) \wedge P(n)] \to P(n+1) \tag{2.32}$$

para algún entero $n \geq 7$. En particular, si $n = 7$, la Ec. (2.32) se reduce a

$$[P(6) \wedge P(7)] \to P(8) \tag{2.33}$$

Dados los valores (a)-(c) del inciso anterior, la Ec. (2.33) es T. A continuación, para un entero $n \geq 7$, arbitrario pero fijo, planteamos:

$$\begin{aligned} f_{n-1} &> \left(\frac{3}{2}\right)^{n-2} \\ f_n &> \left(\frac{3}{2}\right)^{n-1} \end{aligned}$$

$$\begin{aligned} f_{n-1} + f_n &> \left(\frac{3}{2}\right)^{n-2} + \left(\frac{3}{2}\right)^{n-1} \\ f_{n+1} &> \left(\frac{3}{2}\right)^{n} \left[\left(\frac{3}{2}\right)^{-2} + \left(\frac{3}{2}\right)^{-1}\right] \\ f_{n+1} &> \left(\frac{3}{2}\right)^{n} \left[\frac{4}{9} + \frac{2}{3}\right] = \left(\frac{3}{2}\right)^{n} \cdot \frac{10}{9} > \left(\frac{3}{2}\right)^{n} \cdot 1 \equiv D_{n+1} \end{aligned}$$

donde $10/9 \approx 1.1111 > 1$, por lo que $I_{n+1} > D_{n+1}$, y se cumple el PI.

2.5. Ejemplos de ejercicios con inducción

Ejemplo. Demostrar usando el PIM que n rectas en el plano lo dividen en $(n^2 + n + 2)/2$ regiones, suponiendo que no hay rectas paralelas ni que tres rectas se corten.

Solución: es el teorema de Steiner. Sea n el número de cortes (rectas) y L_n el número de regiones definidos por los n cortes. Sería $L_n = 2^n$ si cada nueva recta pudiera dividir a cada región vieja en dos. Pero al agregar el tercer corte vemos que, a lo sumo, podemos dividir tres de las regiones viejas. La recta n incrementa el número de regiones en k siempre que

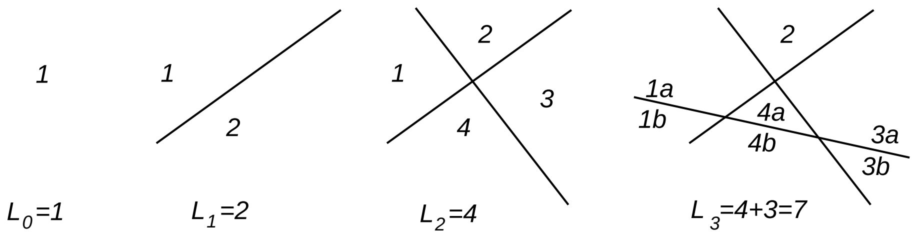

Figura 2.1: Rectas en el plano cuando no hay paralelas ni tres que se corten.

divida k regiones viejas, y eso ocurre si intersecta a las rectas previas en $k-1$ lugares. Como dos rectas se intersectan a lo más en un punto, entonces la nueva recta n intersecta las $n-1$ rectas previas a lo más en $n-1$ puntos, o sea $k \leq n$. Entonces, $L_n \leq L_{n-1} + n$, para $n > 0$. La igualdad la tendremos cuando exigimos que la recta n las intersecte (i.e. no sea paralela a las previas) y tendremos la RR

$$\begin{aligned} L_0 &= 1 \\ L_n &= L_{n-1} + n \qquad ; n > 0 \end{aligned} \tag{2.34}$$

Pero

$$\begin{aligned} L_n &= L_{n-1} + n \\ &= L_{n-2} + (n-1) + n \\ &= L_{n-3} + (n-2) + (n-1) + n = \ldots = \\ &= L_0 + \{1 + 2 + \ldots + (n-2) + (n-1) + n\} \\ &= L_0 + S_n \end{aligned} \tag{2.35}$$

Como $L_0 = 1$ y usando PIM se tiene que $S_n = n(n+1)/2$ (suma de Gauss), queda

$$L_n = 1 + \frac{n(n+1)}{2} = \frac{n^2 + n + 2}{2} \tag{2.36}$$

y que es la expresión pedida.

Ejemplo. Para $n \in \mathbb{N}$ sea

$$a_n = \sum_{k=1}^{n} ((k+1)^3 - k^3) \ . \tag{2.37}$$

1) Calcular a_1, a_2 y a_3.
2) Determinar una fórmula sencilla para a_n que no involucre sumatorias.
3) Demostrar usando PIM que la fórmula encontrada es correcta.

Solución:

1) $a_1 = 7$, $a_2 = 26$ y $a_3 = 63$.
2) De la sucesión 7, 26, 63, ... se concluye que $\{(2^3-1), (3^3-1), (4^3-1) \ldots\}$, y entonces

$$a_n = \sum_{k=1}^{n} ((k+1)^3 - k^3) = (n+1)^3 - 1 \qquad n \geq 1 \ . \tag{2.38}$$

3) PIM: eligiendo el lado izquierdo

$$\begin{aligned} a_{n+1} &= \sum_{i=1}^{n+1}[(k+1)^3 - k^3] \\ &= \sum_{i=1}^{n}[(k+1)^3 - k^3] + [(n+2)^3 - (n+1)^3] \\ &= [(n+1)^3 - 1] + (n+2)^3 - (n+1)^3 \\ &= (n+2)^3 - 1 \end{aligned} \tag{2.39}$$

Tarea. [Un ejercicio difícil]: dado un número igual de ceros y unos sobre un círculo, mostrar que es posible comenzar en algún número y recorrer el círculo hasta llegar a la posición inicial de modo que, en cualquier punto del ciclo, uno haya visto tanto ceros como unos.

Ejemplo. [requiere binomio de Newton (a ver más adelante)] Demostrar usando el PIM que $u_n = \left(3+\sqrt{5}\right)^n + \left(3-\sqrt{5}\right)^n$ es un número entero para todo entero $n = 0, 1, \ldots$. Solución:

$$\begin{aligned} u_{n+1} &= \left(3+\sqrt{5}\right)^{n+1} + \left(3-\sqrt{5}\right)^{n+1} && \text{separamos en cada sumando} \\ u_{n+1} &= \left(3+\sqrt{5}\right)^{n}\left(3+\sqrt{5}\right)^{1} \\ &\quad + \left(3-\sqrt{5}\right)^{n}\left(3-\sqrt{5}\right)^{1} && \text{re-agrupamos} \\ u_{n+1} &= 3\left(3+\sqrt{5}\right)^{n} + \sqrt{5}\left(3+\sqrt{5}\right)^{n} \\ &\quad + 3\left(3-\sqrt{5}\right)^{n} - \sqrt{5}\left(3-\sqrt{5}\right)^{n} && \text{acomodamos para la HI} \\ u_{n+1} &= 3\left[\left(3+\sqrt{5}\right)^{n} + \left(3-\sqrt{5}\right)^{n}\right] \\ &\quad + \sqrt{5}\left[\left(3+\sqrt{5}\right)^{n} - \left(3-\sqrt{5}\right)^{n}\right] && \text{el 1er sumando por HI es un entero} \end{aligned} \tag{2.40}$$

por lo que lo único que falta es demostrar que el segundo sumando es también un número entero. Para tal fin, usamos el binomio de Newton

$$\begin{aligned} A &= \left(3+\sqrt{5}\right)^n = \sum_{k=0}^{n} C(n,k)\, 3^{n-k} \left(\sqrt{5}\right)^k \\ B &= \left(3-\sqrt{5}\right)^n = \sum_{k=0}^{n} C(n,k)\, 3^{n-k} \left(-\sqrt{5}\right)^k \\ A - B &= \sum_{k=0}^{n} C(n,k)\, 3^{n-k} \left[\left(\sqrt{5}\right)^k - \left(-\sqrt{5}\right)^k\right] \\ A - B &= \sum_{k=0}^{n} C(n,k)\, 3^{n-k} \left(\sqrt{5}\right)^k \left[1 - (-1)^k\right] \end{aligned} \tag{2.41}$$

Multiplicando m. a m. la última línea de la Ec. 2.41 por $\sqrt{5}$, tenemos

$$\sqrt{5}(A - B) = \sum_{k=0}^{n} C(n,k)\, 3^{n-k} \left(\sqrt{5}\right)^{k+1} \left[1 - (-1)^k\right] \; ; \tag{2.42}$$

en donde

$$C = \left[1 - (-1)^k\right] = \begin{cases} 0 & \text{para } k = 2i \text{ (par) ;} \\ 2 & \text{para } k = 2i + 1 \text{ (impar).} \end{cases} \tag{2.43}$$

por lo que

1) Cuando k es impar, entonces $k + 1$ es par, por lo que la raíz cuadrada está elevada a un número par y, por tanto, es un número entero;
2) Cuando k es par, entonces C es nulo.

en conclusión, el segundo sumando $\sqrt{5}(A - B)$ también es un número entero.

Ejemplo. [difícil] Demostrar usando el PIM que

$$\underbrace{\cos(x) + \cos(2x) + ... + \cos(nx)}_{I_n} = \underbrace{\frac{\cos[(x/2)(n+1)]\sin(nx/2)}{\sin(x/2)}}_{D_n} \tag{2.44}$$

para todo entero $n > 0$ y siempre que $\sin(x/2) \neq 0$. Solución:

1) PB ($n = 1$):

$$\begin{aligned} I_1 &= \cos(x) \\ D_1 &= \frac{\cos[(x/2)(1+1)]\sin(x/2)}{\sin(x/2)} = \cos(x) \end{aligned} \tag{2.45}$$

por lo que $I_1 = D_1$, y se cumple el PB.

2) PIM: en lo que sigue introducimos $\alpha = (x/2)(n + 1)$ y $\beta = x/2$, por lo que $\alpha + \beta = (x/2)(n + 2)$, $\alpha - \beta = nx/2$ y $2\alpha = x(n + 1)$. Eligiendo el lado izquierdo en la Ec. (2.44)

$$\begin{aligned} I_{n+1} &= \{\cos(x) + \cos(2x) + ... + \cos(nx)\} + \cos[(n+1)x] && \text{; introd. la HI} \\ &= \left\{\frac{\cos[(x/2)(n+1)]\sin(nx/2)}{\sin(x/2)}\right\} + \cos[(n+1)x] && \text{; factor común} \\ &= \frac{\cos[(x/2)(n+1)]\sin(nx/2) + \sin(x/2)\cos[(n+1)x]}{\sin(x/2)} && \text{; introd. } \alpha \text{ y } \beta \\ &= \frac{\cos(\alpha)\sin(\alpha-\beta) + \sin(\beta)\cos(2\alpha)}{\sin(\beta)} \\ &= \frac{A_{n+1}}{\sin(\beta)} \; ; \end{aligned} \tag{2.46}$$

donde

$$A_{n+1} = \cos(\alpha)\sin(\alpha - \beta) + \sin(\beta)\cos(2\alpha) \,. \tag{2.47}$$

Analizando ahora A_{n+1} tenemos

$$\begin{aligned} A_{n+1} &= \cos(\alpha)\sin(\alpha-\beta)+\sin(\beta)\cos(2\alpha) \\ &= \cos(\alpha)[\sin(\alpha)\cos(\beta)-\sin(\beta)\cos(\alpha)]+\sin(\beta)\cos(2\alpha) \\ &= [\cos(\alpha)\sin(\alpha)\cos(\beta)-\cos(\alpha)\cos(\alpha)\sin(\beta)]+ \\ &+\cos(\alpha)\cos(\alpha)\sin(\beta)-\sin(\alpha)\sin(\alpha)\sin(\beta) \\ &= \cos(\alpha+\beta)\sin(\alpha)\ . \end{aligned} \tag{2.48}$$

por lo que

$$\begin{aligned} I_{n+1} &= \frac{\cos(\alpha+\beta)\sin(\alpha)}{\sin(\beta)} \\ &= \frac{\cos[(x/2)(n+2)]\sin[(x/2)(n+1)]}{\sin(x/2)} \\ &\equiv D_{n+1}\ . \end{aligned} \tag{2.49}$$

Ejemplo. [difícil] Demostrar usando el PIM que

$$\underbrace{\frac{1\cdot 3\cdot 5\cdot \ldots\cdot(2n-1)}{2\cdot 4\cdot 6\cdot \ldots\cdot(2n)}}_{I_n} \leq \underbrace{\frac{1}{\sqrt{n+1}}}_{D_n} \tag{2.50}$$

para todo entero $n>0$. Solución:

1) PB ($n=1$):

$$\begin{aligned} I_1 &= \frac{1}{2}\quad ; \\ D_1 &= \frac{1}{\sqrt{2}} \end{aligned} \tag{2.51}$$

por lo que se verifica que $I_1 \leq D_1$.

2) PIM: eligiendo el lado izquierdo en la Ec. (2.50)

$$\begin{aligned} I_{n+1} &= \left\{\frac{1\cdot 3\cdot 5\cdot \ldots\cdot(2n-1)}{2\cdot 4\cdot 6\cdot \ldots\cdot(2n)}\right\}\cdot\frac{2n+1}{2n+2} \\ &\leq \left\{\frac{1}{\sqrt{n+1}}\right\}\cdot\frac{2n+1}{2n+2} = \\ &= \frac{1}{\sqrt{(n+1)\left[\frac{2n+2}{2n+1}\right]^2}} = \\ &= \frac{1}{\sqrt{(n+1)\alpha}}\ ; \end{aligned} \tag{2.52}$$

donde

$$\alpha = \left[\frac{2n+2}{2n+1}\right]^2\ ; \tag{2.53}$$

pero

$$\begin{aligned}(n+1)\alpha &= (n+2-1)\alpha \\ &= (n+2)\alpha - \alpha \\ &= (n+2)\left[1 - \frac{1}{n+2}\right]\alpha \\ &= (n+2)\beta \; ;\end{aligned} \tag{2.54}$$

donde

$$\begin{aligned}\beta &= \left[1 - \frac{1}{n+2}\right]\alpha \\ &= \frac{n+2-1}{n+2}\alpha \\ &= \frac{n+1}{n+2}\alpha \\ &= \frac{n+1}{n+2}\left[\frac{2n+2}{2n+1}\right]^2 \\ &= \frac{(n+1)(4n^2+8n+4)}{(n+2)(4n^2+4n+1)} \\ &= \frac{(4n^3+8n^2+4n)+(4n^2+8n+4)}{(4n^3+4n^2+n)+(8n^2+8n+2)} \\ &= \frac{4n^3+12n^2+12n+4}{4n^3+12n^2+9n+2}\end{aligned} \tag{2.55}$$

De la Ec. (2.55) se concluye que $\beta > 1$ para $n > 1$, entonces $\sqrt{\beta} > 1$ también, o sea $1/\sqrt{\beta} < 1$. Voviendo a la Ec. (2.52),

$$\begin{aligned}I_{n+1} &\leq \frac{1}{\sqrt{(n+1)\alpha}} = \frac{1}{\sqrt{(n+2)\beta}} = \\ &= \frac{1}{\sqrt{(n+2)}}\frac{1}{\sqrt{\beta}} \leq \frac{1}{\sqrt{(n+2)}} \equiv D_{n+1} \; .\end{aligned} \tag{2.56}$$

Ejemplo. [PIM con una desigualdad en donde $n_0 = 4$]. Sea la matriz $\boldsymbol{A} = [\ a\ 0\ ;\ 0\ b\ ]$. Demotrar usando el PIM que $\boldsymbol{A}^n = [\ a^n\ 0\ ;\ 0\ b^n\ ]$, para todo entero positivo n. Solución: tarea para el hogar.

CAPÍTULO 3

Conjuntos

Contents

3.1. Conjuntos

(Ref.: Sec. 1.6, p. 71, Rosen)
Los conjuntos se emplean para agrupar "cosas" que, generalmente, tienen propiedades parecidas, *e.g.* el conjunto de los estudiantes de una clase, un conjunto de caramelos, etc.

Definición. *Conjunto*: es una colección de *elementos*, en donde se admite la presencia de elementos repetidos y no necesariamente estar ordenados. *Elemento*: es cualquier entidad cuya naturaleza interna no interesa y puede ser cualquiera, *e.g.* letras, enteros, cadenas de caracteres, colores, figuras, personas, puntos, rectas, planos, etc. Notación: los conjuntos se representarán con letras mayúsculas, A, B, etc, y los elementos con letras minúsculas, a, b, x, y, etc.

Definición. Se dice que cada elemento **pertenece** al conjunto, y que un conjunto **contiene** a sus elementos. **Notación**: se usa $x \in A$ para denotar que el elemento x *pertenece* al conjunto A, y $x \notin A$ en caso contrario.

Definición. *Conjunto universal* U: es un conjunto especial que contiene a todos los elementos posibles bajo consideración, y cambiará según el problema considerado.

Observación. Las definiciones de conjunto y de elementos vistas aquí lo son en un sentido intuitivo y da lugar a la teoría de conjuntos "informal", en la cual se apela a la intuición para determinar como se comportan los conjuntos.

Definición. Descripción de un conjunto. Hay tres maneras:

- Por **extensión** (o por enumeración): se enumeran todos los elementos del conjunto colocándolo entre un par de llaves. Notación: $\{x_1, x_2, ..., x_n\}$ cuando n es finito, sino $\{x_1, x_2, ..., x_n, ...\}$ cuando hay una cantidad infinita de elementos;
- Por **comprensión**: se caracteriza a los elementos por una propiedad que todos deben tener. Notación: $\{x \mid$ (propiedad que debe cumplir)$\}$.
- Mediante **diagramas de Venn**: es una representación gráfica en donde se representa al conjunto universal U con un gran rectángulo, los demás conjuntos con figuras cerradas cuasi-circulares, ubicadas dentro del universal, y los elementos, con puntos o marcas.

Ejemplo. Ejemplos de conjuntos por extensión:

- Tres caramelos de menta, cuatro de chocolate y tres de frutilla;
- El conjunto de las vocales: $\{a, e, i, o, u\}$;
- El conjunto de los enteros positivos impares menores a 10: $\{1, 3, 5, 7, 9\}$;
- Un conjunto arbitrario: $\{a, 2, \text{Alfredo}, \text{Grecia}, \alpha\}$.

Ejemplo. Ejemplos de conjuntos por comprensión:

- El conjunto de todos los caramelos: $\{x \mid x$ es un caramelo$\}$;
- $\{n \mid n$ es entero positivo impar menor a $10\}$;
- $\{x \mid x$ es un número real$\}$ que es lo mismo que decir $\{x \mid x \in \mathbb{R}\}$;

Ejemplo. Ejemplos de conjuntos universales U: el conjunto de todas las letras del alfabeto español (que es finito); el conjunto de todos los enteros (con un número infinito de elementos).

Definición. Igualdad de dos conjuntos: dos conjuntos son iguales ssi tienen los mismos elementos. **Notación**: cuando dos conjuntos A y B son iguales se denota con $A = B$.

Observación. No interesa el orden ni la presencia de elementos repetidos aunque, cuando se pueda y por comodidad, se acostumbra listar el conjunto con los elementos ordenados según algún orden, y sin repetidos.

Ejemplo.

- Los conjuntos $\{1, 3, 5\}$ y $\{5, 1, 3\}$ son iguales, pues contienen los mismos elementos;
- Los conjuntos $\{1, 3, 5\}$ y $\{1, 5, 5, 5, 1, 5, 1, 1, 3, 3\}$ son iguales, pues contienen los mismos elementos;
- Los conjuntos pueden tener a otros conjuntos como elementos, e.g. $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ y $\{x | x$ es un subconjunto de $\{a, b\}\}$. Notar que ambos conjuntos son iguales.

Definición. *Conjunto vacío*: es el conjunto sin elementos. **Notación**: el conjunto vacío se denota con $\emptyset$, también con $\{\ \}$ y, para evitar confusiones, evitaremos decir conjunto nulo.

Observación. El conjunto $\emptyset$ no es lo mismo que $\{\emptyset\}$, porque en el primero no hay elementos, mientras que en el segundo, es un conjunto que contiene al conjunto vacío, y por tanto hay un elemento.

Definición. *Subconjunto*: se dice que un conjunto A es subconjunto de otro conjunto B ssi, todo elemento de A pertenece a B. **Notación**: cuando A es un sunconjunto de B se denota con $A \subseteq B$. Empleando cuantificadores se tiene que $A \subseteq B$ ssi $\forall x\,(x \in A \rightarrow x \in B)$ es T.

Observación. En general $A \subseteq B$ no es lo mismo que $B \subseteq A$, como se observa en el siguiente ejemplo.

Ejemplo. Sean los conjuntos $A = \{1, 2, 3\}$, $B = \{1, 2, 3, 4, 5\}$:

- Como A y B no tienen los mismos elementos, se tiene $A \neq B$;
- Como cada elemento de A es un elemento de B, se tiene que $A \subseteq B$;
- Pero no todo elemento de B está en A, por eso $B \nsubseteq A$;

Teorema. Para cualquier conjunto A se tiene:

i) $\emptyset \subseteq A$. *Demostración*: empleando la definición de subconjuntos expresada a través cuantificadores que, en este caso, se re-escribe como $\forall x\,(x \in \emptyset \rightarrow x \in A)$ es T. Como el conjunto vacío no tiene elementos, se sigue que $x \in \emptyset$ es siempre F, con lo cual se tienen las formas $F \rightarrow F$ o $F \rightarrow T$, las cuales son ambas T. *Comentario*: este es un ejemplo de una demostración *vacua*;

ii) $A \subseteq A$. *Demostración*: empleando la defición de subconjuntos expresada a través cuantificadores que, en este caso, se re-escribe como $\forall x\,(x \in A \rightarrow x \in A)$ es T. Cuando $x \in A$ es T se tiene la forma $T \rightarrow T$ que es T, y cuando $x \notin A$, queda la forma $F \rightarrow F$ que también T. Luego, en cualquier caso, la implicación $\forall x\,(x \in A \rightarrow x \in A)$ es T.

Definición. *Subconjunto propio*: cuando se quiere enfatizar que un conjunto A es subconjunto de otro conjunto B pero $A \neq B$, se denota con $A \subset B$, y se dice que A es un *subconjunto propio* de B.

Observación. No confundir $\in$ (pertenencia) con $\subseteq$ (inclusión). Mientras que la relación de inclusión es transitiva, i.e. si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$. En cambio, la relación de pertenecia no lo es, i.e. si $\alpha \in B$ y $B \in C$, en general $\alpha \notin C$. Por ejemplo, si bien $a \in \{a, b\}$ y $\{a, b\} \in \{\{a, b\}, \{a, b, c\}\}$, pero $a \notin \{\{a, b\}, \{a, b, c\}\}$.

Observación.

- Para demostrar que dos conjuntos A y B tiene los mismos elementos, hay que probar que cada conjunto es subconjunto del otro, *i.e.* , hay que demostrar si $A \subseteq B \wedge B \subseteq A$, entonces $A = B$;

- La observación anterior equivale a: $(\forall x\,(x \in A \rightarrow x \in B)) \wedge (\forall x\,(x \in B \rightarrow x \in A))$, que equivale a $\forall x\,(x \in A \leftrightarrow x \in B)$.

Definición. *Número de elementos (o cardinal) de un conjunto*: cuando hay n elementos **distintos** en un conjunto A, donde n es un entero finito no negativo, se dice A es un conjunto finito, y que n es el cardinal de A. El cardinal de A se denota con $n = |A|$. Cuando A no es finito, entonces se dice que es un conjunto infinito.

Ejemplo.

- Como el conjunto vacío no tiene elementos, se tiene que $|\emptyset| = 0$;
- El conjunto de enteros, y el conjunto de los enteros positivos son infinitos;
- Los conjuntos $A = \{1, 3, 5\}$ y $B = \{1, 5, 5, 5, 1, 5, 1, 1, 3, 3\}$ tienen el mismo cardinal $n = |A| = |B| = 3$.

Definición. *Conjunto de partes de un conjunto (o conjunto potencia)*: dado un conjunto A, el conjunto de partes de un conjunto (o conjunto potencia), es el conjunto formado por todos los subconjuntos de A, y se denota con $\mathcal{P}(A)$.

Ejemplo.

- El conjunto de partes del conjunto $A = \{a, b, c\}$ es el conjunto de subconjuntos $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$;
- El conjunto de partes del conjunto vacío tiene exactamente 1 único elemento: el conjunto vacío, i.e. $\mathcal{P}(\emptyset) = \{\emptyset\}$;
- El conjunto de partes del conjunto $\{\emptyset\}$ tiene exactamente 2 elementos: el conjunto vacío y el mismo conjunto $\{\emptyset\}$, i.e. $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$;
- De lo anterior se concluye que $|\mathcal{P}(\emptyset)| = 1$, y $|\mathcal{P}(\{\emptyset\})| = 2$.

Observación. Coordinación entre los elementos de $\mathcal{P}(A_n)$ y $\mathcal{P}(A_{n+1})$. Por ejemplo, sea el conjunto finito $A = \{a, b, c\}$, entonces $\mathcal{P}(A)$ lo podemos separar en dos grupos, a saber: (i) los subconjuntos que contienen al elemento a, i.e. $\{\{a\}, \{a, b\}, \{a, c\}, \{a, b, c\}\}$, y (ii) y aquellos que no lo contienen, i.e. $\{\emptyset, \{b\}, \{c\}, \{b, c\}\}$. Observar que en el segundo grupo, al agregarles el elemento a, se obtienen los elementos del primer grupo, respectivamente. Además, el segundo grupo corresponde a los subconjuntos de $B = \{b, c\}$. Notar que cada subconjunto que contiene al elemento a, se lo puede coordinar de un modo único con un subconjunto que no lo contiene. Por eso, exactamente la mitad de los subconjuntos de $\mathcal{P}(A)$ contienen al elemento a, y la otra mitad no. Esta propiedad de coordinación entre los elementos de $\mathcal{P}(A_n)$ y $\mathcal{P}(A_{n+1})$ es general para cualquier número finito de elementos n, y será de utilidad después para demostrar una fórmula para el número de elementos de $\mathcal{P}(A)$ en función de n.

Definición. *Tupla*: la n-tupla ordenada $(a_1, a_2, ..., a_n)$ es la colección ordenada en la que a_1 es el primer elemento, a_2 es el segundo elemento, ..., a_n es el n-ésimo elemento. Dos tuplas $(a_1, a_2, ..., a_n)$ y $(b_1, b_2, ..., b_n)$ son iguales ssi $a_1 = b_1$, y $a_2 = b_2$, ..., y $a_n = b_n$.

Ejemplo.

- Las duplas (a, b) y (c, d) son iguales, ssi $a = c$ y $b = d$;

- Las duplas (a,b) y (b,a) no son iguales, a menos que $a=b$.

Definición. *Producto cartesiano* de dos conjuntos: el producto cartesiano de los conjuntos A y B se denota con $A\times B$, y es el conjunto formado por todos los pares ordenados (a,b), donde $a\in A$ y $b\in B$. En símbolos: $A\times B=\{(a,b)\mid a\in A\wedge b\in B\}$.

Ejemplo. Sea los conjuntos A y B_n, cada uno con $|A|=3$ y $|B_n|=n$ elementos, respectivamente, donde n es un entero $n\geq 1$. Demuestre usando el PIM que

$$\underbrace{|A\times B_n|}_{I_n}=\underbrace{3n}_{D_n} \tag{3.1}$$

para todos los enteros $n\geq 1$. Ayuda: tenga en cuenta las propiedades

$$\begin{aligned}|A\cup B|&=|A|+|B|+|A\cap B|\\ |(A\times B)\cup(A\times C)|&=|A\times B|+|A\times C|\quad \text{siempre que } B\cap C=\emptyset.\\ A\times(B\cup C)&=(A\times B)\cup(A\times C)\end{aligned} \tag{3.2}$$

para todos los conjuntos A, B y C.
Solución:

1) Previo: notar que la notación B_k denota un conjunto de k elementos con independencia del elemento concreto. Por eso, por ejemplo, los conjuntos $\{a\}$, $\{b\}$, $\{c\}$, y $\{d\}$ se simbolizan en este contexto como $\{B_1\}$ porque todos tienen un único elemento. En consecuencia,

$$\begin{aligned}B_1&=\{a\} &&=\emptyset\cup\{a\}=B_0\cup B_1\\ B_2&=\{a,b\} &&=\{a\}\cup\{b\}=B_1\cup B_1\\ B_3&=\{a,b,c\} &&=\{a,b\}\cup\{c\}=B_1\cup B_1\\ B_4&=\{a,b,c,d\} &&=\{a,b,c\}\cup\{d\}=B_1\cup B_1\end{aligned} \tag{3.3}$$

Además, como $|B_n|=n$ y $|B_{n+1}|=n+1$, debe ser $B_n\cap B_{n+1}=\emptyset$. Por otra parte, también se tiene que $B_n\cup B_1=B_{n+1}$.

2) PB ($n=1$): sea $A=\{a_1,a_2,a_3\}$, con 3 elementos (fijo), y sea $B_1=\{b_1\}$ con 1 elemento. Tenemos:

$$A\times B_1=\{a_1,a_2,a_3\}\times\{b_1\}\;=\{(a_1,b_1),(a_2,b_1),(a_3,b_1)\} \tag{3.4}$$

por lo que, por inspección, se comprueba que $|A\times B_1|=3$, por lo que se verifica el PB.

3) PI: asumimos que la HI dada por la Ec. (3.1) es T para **algún entero** $n\geq 2$ **arbitrario**

pero fijo, y planteamos:

$$
\begin{aligned}
I_{n+1} &= |A \times B_{n+1}| = && ;\text{ porque } B_{n+1} = B_n \cup B_1 \\
&= |A \times (B_n \cup B_1)| && ;\text{ intro. prop. aux. 3} \\
&= |(A \times B_n) \cup (A \times B_1)| && ;\text{ intro. prop. aux. 2 porque } B_n \cap B_{n+1} = \emptyset \\
&= |A \times B_n| + |A \times B_1| && ;\text{ introducimos la HI en el 1er sumando} \\
&= 3n + |A \times B_1| && ;\text{ pero } |A \times B_1| = 3 \\
&= 3n + 3 && ;\text{ sacamos factor común 3} \\
&= 3(n+1) \equiv D_{n+1}
\end{aligned}
\tag{3.5}
$$

por lo que $I_{n+1} = D_{n+1}$, y se cumple el PI.

Definición. *Relación entre dos conjuntos*: una relación de un conjunto A en otro conjunto B es un subconjunto R del producto cartesiano $A \times B$. En símbolos: $R \subseteq A \times B$.

Observación. Los productos cartesianos $A \times B$ y $B \times A$ no son iguales a menos que: $A = B$, o bien $A = \emptyset$, o bien $B = \emptyset$, o bien $A = B = \emptyset$.

Ejemplo. Justificar en cada caso si es T o F:

- $\emptyset \in \{\}$ (alternativas $\{\} \in \emptyset$, $\{\} \in \{\}$, $\emptyset \in \emptyset$): Sol.: como la pertenencia (símbolo $\in$) describe si un elemento pertenece (o no) a un conjunto, y como $\emptyset$ por definición no tiene elementos, se concluye que $\emptyset \in \{\}$ es F.
- $\emptyset \subseteq \{\emptyset\}$ (alternativas: $\{\} \subseteq \emptyset$, $\{\} \subseteq \{\}$, $\emptyset \subseteq \emptyset$): Sol.: como la inclusión (símbolo $\subseteq$) describe si un conjunto es (o no) un subconjunto de otro conjunto, y como $\emptyset$ es subconjunto de todo conjunto, se concluye que $\emptyset \subseteq \{\}$ es T.
- $\{\emptyset\} \subseteq \emptyset$ (alternativas: $\{\{\}\} \subseteq \emptyset$, $\{\{\}\} \subseteq \{\}$, $\{\emptyset\} \subseteq \{\}$): Sol.: como el elemento $\emptyset$ del conjunto $\{\emptyset\}$ no es un elemento del conjunto $\emptyset$, porque $\emptyset$ no tiene elementos, se concluye que $\{\emptyset\} \subseteq \emptyset$ es F;
- $\emptyset = \{\emptyset\}$: (alternativas: $\{\} = \{\emptyset\}$, $\{\} = \{\{\}\}$, $\emptyset = \{\{\}\}$): Sol.: si bien $\emptyset \subseteq \{\emptyset\}$ es T pero $\{\emptyset\} \subseteq \emptyset$ es F, por lo que $\emptyset = \{\emptyset\}$ es F;
- $A \subseteq A$: Sol.: como un conjunto A es un subconjunto de si mismo, $A \subseteq A$ es T (hay un teorema al respecto);
- $A \subset A$: Sol.: como un conjunto A no puede ser a la vez un subconjunto propio de si mismo, $A \subset A$ es F.

3.2. Operaciones con conjuntos

(Ref.: Sec. 1.7, p. 79, Rosen)

Definición. *Unión de dos conjuntos*: la unión de los conjuntos A y B es el conjunto que contiene los elementos que, o bien están en A, o bien están en B, o bien están en ambos. **Notación**: La unión de los conjuntos A y B se denota con $A \cup B$. **Simbología**: $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$.

Definición. *Intersección de dos conjuntos*: la intersección de los conjuntos A y B es el conjunto que contiene los elementos que están tanto en A como en B. **Notación**: La intersección de los conjuntos A y B se denota con $A \cap B$. **Simbología**: $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$.

Definición. *Diferencia de dos conjuntos*: la diferencia de los conjuntos A y B es el conjunto que contiene los elementos que están en A pero no en B. **Notación**: La diferencia de los conjuntos A y B se denota con $A - B$. **Simbología**: $A - B = \{x \mid (x \in A) \wedge (x \notin B)\}$. $B - A = \{x \mid (x \in B) \wedge (x \notin A)\}$. Notar que, en general, $A - B \neq B - A$.

Definición. *Diferencia simétrica de dos conjuntos*: la diferencia simétrica de los conjuntos A y B es el conjunto que contiene los elementos que están en A o bien que están en B, pero no en ambos. **Notación**: La diferencia simétrica de los conjuntos A y B se denota con $A \oplus B$. **Simbología**: $A \oplus B = \{x \mid ((x \in A) \wedge (x \notin B) \vee (x \in B) \wedge (x \notin A))\}$. Tarea: probar que $A \oplus B = B \oplus A$; **Igualdad 1**: $A \oplus B = (A - B) \cup (B - A)$; **Igualdad 2**: $A \oplus B = (A \cup B) - (A \cap B)$.

Definición. *Complemento de un conjunto*. Sea U el conjunto universal. El complemento del conjunto A es la diferencia $U - A$, o sea, es el conjunto que contiene los elementos que están en U pero no están en A. **Notación**: El complemento del conjunto A se denota con $\overline{A}$. **Simbología**: $\overline{A} = \{x \mid x \notin A\}$.

Tarea. Para los conjuntos A y B, trazar los diagramas de Venn de:

- La unión $A \cup B$;
- La intersección $A \cap B$;
- Las diferencias $A - B$ y $B - A$;
- Las diferencias simétricas $A \oplus B$ y $B \oplus A$;
- Los complementos $\overline{A}$ y $\overline{B}$.

Ejemplo. Sean los conjuntos $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6, 7\}$, y el universal $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$:

- Unión: $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$;
- Intersección: $A \cap B = \{3, 4\}$;
- Las diferencia $A - B = \{1, 2\}$ y $B - A = \{5, 6, 7\}$. Notar que, en general, $A - B \neq B - A$;
- Diferencias simétricas: $A \oplus B = (A - B) \cup (B - A) = \{1, 2, 5, 6, 7\}$, y $B \oplus A = (B - A) \cup (A - B) = \{1, 2, 5, 6, 7\}$. Notar que $A \oplus B = B \oplus A$.
- Diferencia simétrica (bis): $A \oplus B = (A \cup B) - (A \cap B) = \{1, 2, 5, 6, 7\}$, y $B \oplus A = (B \cup A) - (B \cap A) = \{1, 2, 5, 6, 7\}$;
- Complementos: $\overline{A} = U - A = \{5, 6, 7, 8, 9, 0\}$ y $\overline{B} = U - B = \{1, 2\}$;

Ejemplo. En las Tablas 3.1-3.2 se listan las identidades de conjuntos de uso **muy** frecuente en las evaluaciones.

Observación. *Identidades de conjuntos*: en el texto de referencia se emplean 3 métodos para probar que los conjuntos A y B son iguales, i.e. probar que $A = B$ equivale a demostrar:

a) Doble inclusión, i.e. si se logra probar que $A \subseteq B$ y $B \subseteq A$, entonces $A = B$;
b) A partir de las equivalencias lógicas asociadas en cada caso;
c) Utilizando Tablas de Pertenencia (TP) (sólo en el Rosen): se toma un elemento x y se considera cada combinación de conjuntos a la que puede pertenecer, verificando que los elementos de una misma combinación pertenecen a ambos conjuntos de la identidad a comprobar. Para indicar que un elemento x pertenece a un conjunto se indica con 1, y con 0 en caso contrario. Notar que las TP son practicamente muy similares a las TV.

Ejemplo. Probar que $A \cap (A \cup B) = A$. Solución: La igualdad $A \cap (A \cup B) = A$ significa que $A \cap (A \cup B) \subseteq A$ y que $A \subseteq A \cap (A \cup B)$. Introduciendo $p \equiv x \in A$, y $q \equiv x \in B$, se tiene:

a) i) Suponga que $A \subseteq A \cap (A \cup B)$. En ese caso, por definición de inclusión, se tiene

$$\begin{aligned}
&(x \in A) \to [x \in (A \cap (A \cup B))] \quad \text{por definición de inclusión}\\
&\equiv (x \in A) \to [(x \in A) \wedge x \in (A \cup B)] \quad \text{por definición de intersección}\\
&\equiv (x \in A) \to (x \in A) \wedge [(x \in A) \vee (x \in B)] \quad \text{por definición de unión}\\
&\equiv p \to [p \wedge (p \vee q)] \quad \text{cambio de notación}\\
&\equiv p \to p \quad \text{por ley de absorción}\\
&\equiv \mathrm{T} \quad \text{(es una tautología)}
\end{aligned} \tag{3.6}$$

y se concluye que $(x \in A) \to [x \in (A \cap (A \cup B))]$ es T (independiente de si $x \in A$ es T o es F).

ii) Ahora, suponga que $A \cap (A \cup B) \subseteq A$. En ese caso, por definición de inclusión, se tiene

$$\begin{aligned}
&x \in (A \cap (A \cup B)) \to (x \in A) \quad \text{por definición de inclusión}\\
&[x \in A \wedge x \in (A \cup B)] \to (x \in A) \quad \text{por definición de intersección}\\
&[x \in A \wedge (x \in A \vee x \in B)] \to (x \in A) \quad \text{por definición de unión}\\
&\equiv [p \wedge (p \vee q)] \to p \quad \text{cambio de notación}\\
&\equiv p \to p \quad \text{por ley de absorción}\\
&\equiv \mathrm{T} \quad \text{(es una tautología)}
\end{aligned} \tag{3.7}$$

y se concluye que $x \in (A \cap (A \cup B)) \to (x \in A)$ es T (independiente de si $x \in A$ es T o es F).

iii) Finalmente, como $L_I \subseteq L_D$ y $L_D \subseteq L_I$ son ambas T, entonces se concluye que $L_I = L_D$ es T.

A	B	$A \cup B$	$A \cap (A \cup B)$
0	0	0	0
1	0	1	1
0	1	1	0
1	1	1	1

b) Solución a partir de las equivalencias lógicas.

$$\begin{aligned} A \cap (A \cup B) &= \{x \mid x \in (A \cap (A \cup B))\} \\ &= \{x \mid (x \in A) \wedge x \in (A \cup B)\} \\ &= \{x \mid (x \in A) \wedge (x \in A \vee x \in B)\} \\ &= \{x \mid p \wedge (p \vee q)\} \\ &= \{x \mid (p \wedge p) \vee (p \wedge q)\} \\ &= \{x \mid p \vee (p \wedge q)\} \\ &= \{x \mid p\} \\ &= \{x \mid x \in A\} \\ &= A \end{aligned} \tag{3.8}$$

c) Solución a partir de las tablas de pertenencia ver Tabla 3.1.

Ejemplo. Probar que $A \times (B \cup C) = (A \times B) \cup (A \times C)$. Solución (únicamente por doble inclusión):

i) Sea $(a, b) \in A \times (B \cup C)$. Entonces, por definición de producto cartesiano, $a \in A \wedge b \in (B \cup C)$. Por definición de la unión $b \in (B \cup C) \equiv b \in B \vee b \in C$. Reemplazando, $a \in A \wedge (b \in B \vee b \in C)$, haciendo distributiva $(a \in A \wedge b \in B) \vee (a \in A \wedge b \in C)$, es decir, $(a, b) \in (A \times B \vee A \times C)$. por lo que $L_I \subseteq L_D$.

ii) Sea $(a, b) \in (A \times B) \cup (A \times C)$. Entonces, por definición de unión $(a, b) \in (A \times B) \vee (a, b) \in (A \times C)$. Por definición de producto cartesiano $(a \in A \wedge b \in B) \vee (a \in A \wedge b \in C)$. Sacando factor común queda $a \in A \wedge (b \in B \vee b \in C)$. Por definición de unión $a \in A \wedge (b \in (B \cup C))$. Por definición de producto cartesiano, $(a, b) \in A \times (B \cup C)$. por lo que $L_D \subseteq L_I$.

iii) Finalmente, como $L_I \subseteq L_D$ y $L_D \subseteq L_I$ son ambas T, entonces se concluye que $L_I = L_D$ es T.

Ejemplo. Determinar el VV de

1) $A - B = B - A$;

2) $\overline{(A \cap B)} \subseteq A$;

3) $(A \cap B) \cup (B - A) = B$;

para todos los conjuntos A y B. Solución: los tres ejemplos son falsos. Un contraejemplo común para cada caso es tomar $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$, y el conjunto universal $U = \{1, 2, 3, 4, 5, 6, 7\}$.

Identidad	Ley	
$A \cup \emptyset = A$ $A \cap U = A$	identidad	1
$A \cup U = U$ $A \cap \emptyset = \emptyset$	dominación	2
$A \cup A = A$ $A \cap A = A$	idempotencia	3
$\overline{\overline{A}} = A$	doble complemento	4
$A \cup B = B \cup A$ $A \cap B = B \cap A$	conmutativas	5

Tabla 3.1: Tabla de identidades entre conjuntos de uso **muy** frecuente (continúa en la Tabla 3.2).

Ejemplo. Probar que $A \cap B = A - \overline{B}$. Solución: primero haremos desde $n = 0$ hasta $n = 4$

$$\begin{aligned} A \cap B &= \{x \mid x \in A \wedge x \in B\} \\ &= \{x \mid x \in A \wedge x \notin \overline{B}\} \\ &= \{x \mid x \in (A - \overline{B})\} \\ A - \overline{B} &= \{x \mid x \in A \wedge x \notin \overline{B}\} \\ &= \{x \mid x \in A \wedge x \in B\} \\ &= \{x \mid x \in (A \cap B)\} \end{aligned} \tag{3.9}$$

Ejemplo. Probar que $A \cap (B - C) = (A \cap B) - (A \cap C)$. Solución: Introduciendo $p \equiv x \in A$, y $q \equiv x \in B$, $r \equiv x \in C$, se tiene:

i) Tomando el lado izquierdo:

$$\begin{aligned} A \cap (B - C) &= \{x \mid x \in A \cap (B - C)\} \\ &= \{x \mid x \in A \wedge x \in (B - C)\} \\ &= \{x \mid x \in A \wedge x \in B \wedge x \notin C\} \\ &= \{x \mid p \wedge q \wedge \neg r\} \end{aligned} \tag{3.10}$$

ii) Tomando el lado derecho:

$$\begin{aligned} (A \cap B) - (A \cap C) &= \{x \mid x \in (A \cap B) \wedge x \notin (A - C)\} \\ &= \{x \mid (x \in A \wedge x \in B) \wedge (x \notin A \vee x \notin C)\} \\ &= \{x \mid (p \wedge q) \wedge (\neg p \vee \neg r)\} \\ &= \{x \mid (p \wedge q \wedge \neg p) \vee (p \wedge q \wedge \neg r)\} \\ &= \{x \mid F \vee (p \wedge q \wedge \neg r)\} \\ &= \{x \mid p \wedge q \wedge \neg r\} \end{aligned} \tag{3.11}$$

iii) Los lados derechos de las Ecs. (3.10-3.11) son iguales, por lo que los lados izquierdos también lo son.

Definición. *Unión generalizada (de una colección de conjuntos)*: la unión de la colección finita de conjuntos A_1, A_2 ..., A_n, es el conjunto que contiene los elementos que pertenecen

Identidad	Ley	
$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$	asociativas	6
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	distributivas	7
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan	8
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	absorción	9
$p \cup \overline{A} = U$ $p \cap \overline{A} = \emptyset$	complemento	10

Tabla 3.2: Tabla de identidades entre conjuntos de uso **muy** frecuente (continuación de la Tabla 3.1).

al menos a uno de los conjuntos de la colección. **Notación**: usamos la notación $A_1 \cup A_2 \cup ... \cup A_n = \bigcup_{i=1}^{n} A_i$.

Definición. *Intersección generalizada (de una colección de conjuntos)*: la intersección de la colección finita de conjuntos A_1, A_2 ..., A_n, es el conjunto que contiene aquellos elementos que pertenecen a todos los conjuntos de la colección. **Notación**: usamos la notación $A_1 \cap A_2 \cap ... \cap A_n = \bigcap_{i=1}^{n} A_i$.

Ejemplo. Sea $A_i = \{i, i+1, ...\}$, con entero positivo i, con infinitos elementos. Entonces:

- $\bigcup_{i=1}^{n} A_i = \bigcup_{i=1}^{n}\{i, i+1, ...\} = \{1, 2, 3, ...\}$;
- $\bigcap_{i=1}^{n} A_i = \bigcap_{i=1}^{n}\{i, i+1, ...\} = \{n, n+1, n+2, ...\}$;

3.3. Principio de inclusión-exclusión (o de la criba)

(Ref.: Sec. 6.5, p. 420, Rosen)
El Principio de Inclusión-Exclusión (PIE) (o principio de la criba [1] es un recurso muy útil en problemas de conteo en donde intervienen conjuntos finitos [1]. En lo que sigue, seguiremos la presentación de Biggs [1]:

1) Si los conjuntos finitos A y B son disjuntos (o sea, $A \cap B = \emptyset$) se tiene que:

$$|A \cup B| = |A| + |B| \tag{3.12}$$

Ejemplo. *Sean los conjuntos $A = \{a, b, c\}$ y $C = \{d, e\}$. En este caso $A \cup C = \{a, b, c, d, e\}$ pero $A \cap C = \emptyset$. En este caso $|A| = 3$ y $|C| = 2$, verificándose que* $|A \cup C| = 3 + 2 = 5$.

2) Pero si los conjuntos finitos A y B no son disjuntos (o sea, $A \cap B \neq \emptyset$), al sumar $|A|$ y $|B|$, estamos contando dos veces los elementos que están en $A \cap B$.

Ejemplo. *Sean los conjuntos $A = \{a, b, c\}$ y $B = \{b, c, d, e\}$. Ahora tenemos que $A \cap B = \{b, c\}$ y $A \cup B = \{a, b, c, d, e\}$, por lo que $|A| = 3$ y $|B| = 4$, pero* $|A \cup B| = 5$.

Para corregirlo, notar que basta restar el número de elementos que fueron contados en forma doble, o sea, aquellos que están en $A \cap B$, es decir,

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{3.13}$$

Ejemplo. *En el caso del ejemplo anterior* $|A \cap B| = 2$*, y usando la Ec. (3.13) resulta que* $|A \cup B| = 3 + 4 - 2 = 5$*, como debe ser.*

3) En el caso de tres conjuntos finitos A, B y C, al sumar $|A|$, $|B|$ y $|C|$, los elementos de $A \cap B$, $B \cap C$, y $C \cap A$ los contamos dos veces (si es que no están en los tres conjuntos simultáneamente), mientras que los elementos de $A \cap B \cap C$ los hemos contado tres veces. Para corregirlo, restamos $|A \cap B|$, $|B \cap C|$, y $|C \cap A|$. Pero al hacerlo los elementos de $A \cap B \cap C$, que inicialmente fueron contados tres veces, ahora han sido quitados tres veces, por lo que a continuación hay que sumar $|A \cap B \cap C|$. Así se deduce la expresión

$$\begin{aligned} &|A \cup B \cup C| = \alpha_1 - \alpha_2 + \alpha_3 \\ &\alpha_1 = |A| + |B| + |C| \\ &\alpha_2 = |A \cap B| + |B \cap C| + |C \cap A| \\ &\alpha_3 = |A \cap B \cap C| \end{aligned} \tag{3.14}$$

En general, se tiene el siguiente resultado [1]:

Enunciado. *Para n conjuntos finitos* A_1*,* A_2*, ...,* A_n*:*

$$|A_1 \cup A_2 \cup ... \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - ... + (-1)^{n-1}\alpha_n \tag{3.15}$$

donde α_i *es la suma de los cardinales de todas las intersecciones de i conjuntos, con* $1 \leq i \leq n$*.*

Tarea. Usando los principios de conteo y el PIE, determinar el número de cadenas de 8 bits que empiezan con 101 y/o terminan con 01.

CAPÍTULO 4

Funciones

Contents

4.1. Función

(Sec. 1.8, p. 90, Rosen)

Definición. Sean dados los conjuntos A y B. *Función* (def. 1): una función f de A en B es una asignación de un UNICO elemento de B a CADA elemento de A. *Función* (def. 2): una función f de A en B es un subconjunto del producto cartesiano $A \times B$, tal que cumple con dos propiedades: (a) existencia: CADA elemento $a \in A$ tiene asignado un $b \in B$; (b) unicidad: CADA elemento $a \in A$ tiene asignado un UNICO $b \in B$; **Notación**: se denota $f(a) = b$, si b es el único elemento de B asignado por la función f a cada elemento de A. Además, si f es una función de A en B, entonces escribimos $f : A \to B$. **Comentario**: las *funciones* son un caso particular de las *relaciones* (ver más adelante).

Definición. *Dominio, codominio, imagen, preimagen, rango*: si f es una función de un conjunto A en otro B, decimos que A es el *dominio* de f, B es el *codominio* de f. Si $f(a) = b$, decimos que b es la *imagen* de a, y que a es la *preimagen* de b. El *rango* (o *imagen*) de la función f es el conjunto de todas las imágenes de los elementos del dominio A. Notar que, en general, rango$(f) \subseteq B$.

Observación. Especificación de una función $f : A \to B$. Entre otras, a través de:

1) Lista de pares ordenados (caso discreto);
2) Tabla de valores (caso discreto);
3) Fórmula matemática (caso discreto o continuo);

4) Diagrama de flechas (o digrafo), caso discreto;
5) Matrices (caso discreto);

Ejemplo. Subconjuntos f_1, f_2, f_3, y f_4 del producto cartesiano $A \times B$ de los conjuntos A y B, en donde $A = \{a, b, c\}$, $B = \{\alpha, \beta, \gamma, \delta\}$. En algunos son también funciones y otros no, ver Fig. 4.1:

1) $f_1 = \{(a, \beta), (b, \delta), (c, \alpha)\}$: en este caso se cumplen las condiciones de existencia y de unicidad, por lo que el subconjunto f_1 del producto cartesiano $A \times B$ es una función. Notar que el elemento γ del codominio B no tiene preimagen alguna (no importa);
2) $f_2 = \{(a, \beta), (b, \delta), (c, \beta)\}$: también se cumplen las condiciones de existencia y de unicidad. Luego, el subconjunto f_2 del producto cartesiano $A \times B$ es una función. Notar que el elemento β del codominio B tiene dos preimágenes (no importa);
3) $f_3 = \{(a, \delta), (b, \beta), (b, \gamma), (c, \alpha)\}$: notar que el elemento b del conjunto A tiene asignado dos elementos ((b, β) y (b, γ)). Luego, no se cumple la condición de unicidad, por lo que el subconjunto f_3 del producto cartesiano $A \times B$ no es una función;
4) $f_4 = \{(a, \delta), (c, \alpha)\}$: notar que el elemento b del conjunto A no tiene asignado elemento alguno en el codominio. Luego, no se cumple la condición de existencia para todos los elementos del dominio A, por lo que el subconjunto f_4 del producto cartesiano $A \times B$ no es una función.

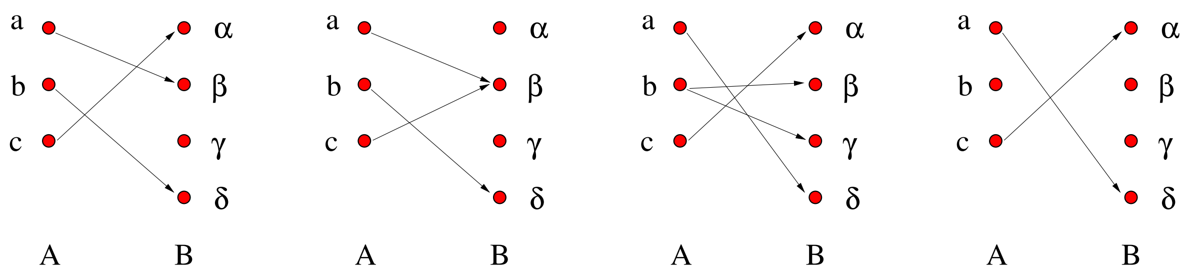

Figura 4.1: Diagramas de flechas de los subconjuntos f_1, f_2, f_3, y f_4, del producto cartesiano $A \times B$ de los conjuntos A y B. En algunos casos son funciones y en otros no.

Definición. Imagen de un subconjunto del dominio de una función (def. 4 del libro, pág. 91). Sean los conjuntos A y B, el subconjunto $C \subseteq A$, y la función f de A en B. La imagen de un subconjunto C del dominio A de la función f es el subconjunto de B formado por todas las imágenes de los elementos de C. **Notación**: $f(C) = \{f(x) \mid \forall x \in C\}$.

4.2. Función inyectiva, sobreyectiva, y biyectiva

Definición. Función inyectiva (def. 1): se dice que una función $f: A \to B$ es *inyectiva* (o *uno a uno*), si PARA CADA $b \in B$ existe A LO SUMO un $a \in A$, tal que $f(a) = b$ (o sea, podria no-existir). Función inyectiva (def. 2): se dice que una función $f: A \to B$ es *inyectiva* (o *uno a uno*), ssi $f(x) = f(y)$ implica que $x = y$, con $x, y \in A$. En otras palabras, cuando f es inyectiva: (i) si $f(x) = f(y)$, entonces $x = y$; y (ii) si $x = y$, entonces $f(x) = f(y)$, con $x, y \in A$.

Definición. Función sobreyectiva (def. 1): se dice que una función $f\colon A \to B$ es *sobreyectiva* (o *suryectiva*), si el rango de f es todo B. **Notación**: rango(f) $= B$ ssi f es sobreyectiva. O sea, cuando f es sobreyectiva: (i) si rango(f) $= B$, entonces f es sobreyectiva; y (ii) si f es sobreyectiva, entonces rango(f) $= B$. Función sobreyectiva (def. 2): se dice que una función $f\colon A \to B$ es *sobreyectiva* (o *suryectiva*), ssi para TODO elemento $y \in B$, existe un $x \in A$ tal que $f(x) = y$.

Definición. Función biyectiva (def.): una función $f\colon A \to B$ es *biyectiva* cuando es inyectiva y sobreyectiva simultáneamente.

Observación. Uso de la leyes de De Morgan generalizadas (o leyes De Morgan en proposiciones cuantificadas) en funciones no inyectivas ni sobreyectivas (Sec. 2.2, pp. 94-95, Johnsonbaugh).

1) Una función $f\colon X \to Y$ no es inyectiva cuando $\forall x_1 \forall x_2\, ((f_1 = f_2) \to (x_1 = x_2))$ es F, donde $f_1 = f(x_1)$, y $f_2 = f(x_2)$. Luego, su negación debe ser T y hacemos

$$\begin{aligned} &\neg(\forall x_1 \forall x_2\, ((f_1 = f_2) \to (x_1 = x_2))) \\ &\equiv \exists x_1 \neg(\forall x_2\, ((f_1 = f_2) \to (x_1 = x_2))) \\ &\equiv \exists x_1 \exists x_2\, \neg((f_1 = f_2) \to (x_1 = x_2)) \\ &\equiv \exists x_1 \exists x_2\, ((f_1 = f_2) \wedge (x_1 \neq x_2)) \end{aligned} \tag{4.1}$$

donde se usó la EL $\neg(p \to q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$. En palabras, la última línea de la Ec. (4.1) expresa que una función $f(x)$ no es inyectiva si existen x_1 y x_2 tales que $f(x_1) = f(x_2)$ pero $x_1 \neq x_2$.

2) Una función $f\colon X \to Y$ no es sobreyectiva cuando $\forall y \exists x\, (f(x) = y)$ es F, donde $x \in X$, e $y \in Y$. Luego, su negación debe ser T y hacemos

$$\begin{aligned} &\neg(\forall y \exists x\; f(x) = y) \\ &\equiv \exists y \neg(\exists x\; f(x) = y) \\ &\equiv \exists y \forall x\; \neg(f(x) = y) \\ &\equiv \exists y \forall x\; f(x) \neq y \end{aligned} \tag{4.2}$$

En palabras, la última línea de la la Ec. (4.2) expresa que una función $f(x)$ no es sobreyectiva si existe un $y \in Y$ tal que para todo $x \in X$ se comprueba que $f(x) \neq y$.

4.3. Función inversa, y composición de dos funciones

Definición. Función inversa (def.): sea $f\colon A \to B$ una función biyectiva del conjunto A en otro B. La función inversa de f es la función de $B \to A$ que asigna a cada elemento de $b \in B$ el único elemento $a \in A$ tal que $f(a) = b$, y se denota con $f^{-1} = \{(b,a) \mid (a,b) = f\}$. *Comentario*: en este contexto no confundir la notación f^{-1} con $1/f$.

Definición. Composición de dos funciones (o función de función): sean los conjuntos A, B y C, y las funciones $g\colon A \to B$ y $f\colon B \to C$. La composición de la función f con g se define con $f(g(a)$, para todo $a \in A$, siempre que Imagen$(g) \subseteq$ Dominio(f), y se denota con $(f \circ g)(a) = f(g(a))$. En símbolos:

$$g \colon A \to B \quad \text{y} \quad f \colon B \to C \quad : \quad f(g(a)) = f \circ g \quad \text{si Imagen}(g) \subseteq \text{Dominio}(f) \qquad (4.3)$$

Ejemplo. Sean $g \colon A \to A$ y $f \colon A \to C$, con $A = \{a, b, c\}$, y $C = \{1, 2, 3\}$, donde $g = \{(a, b), (b, c), (c, a)\}$ y $f = \{(a, 3), (b, 2), (c, 1)\}$. Como Imagen$(g) \subseteq$ Dominio(f), la composición $f \circ g$ es posible, y es: $f(g(a)) = f(b) = 2$, $f(g(b)) = f(c) = 1$, y$f(g(c)) = f(a) = 3$. Pero como Imagen$(f) \nsubseteq$ Dominio(g), no es posible hallar $g \circ f$.

4.4. Función piso y función techo

Definición. Función piso (o parte entera) (def.): asigna al número real x el MAYOR entero que es menor o igual que x, y se denota con $\lfloor x \rfloor$.

Definición. Función techo (o parte entera por exceso) (def.): asigna al número real x el MENOR entero que es mayor o igual que x, y se denota con $\lceil x \rceil$.

Observación. Prestar atención cuando x es positivo, cero o negativo. Se tiene:

- La función piso $\lfloor x \rfloor$ siempre asigna el entero más cercano a x “mirando hacia” $-\infty$, e.g. piso $(+2.345) = +2$ pero piso $(-2.345) = -3$;
- La función techo $\lceil x \rceil$ siempre asigna el entero más cercano a x “mirando hacia” $+\infty$, e.g. techo $(+6.789) = +7$ pero techo $(-6.789) = -6$.

Observación. Una implementación de la función piso $\lfloor x \rfloor$ para un número x ya sea positivo, cero o negativo, es la mostrada en la función `piso(x)`.

```
def piso(x):          # retorna la funcion piso de un numero x
    h = int (x)       # int (x) redondea hacia cero
    if   (h < x):     # x debe ser positivo
        z = h
    elif (h > x):     # x debe ser negativo
        z = h - 1
    else:             # x era un entero
        z = h
    return z
```

Observación. Una implementación de la función techo $\lceil x \rceil$ para un número x ya sea positivo, cero o negativo, es la mostrada en la función `techo(x)`.

```
def techo(x):         # retorna la funcion techo de un numero x
    h = int (x)       # int redondea hacia cero
    if   (h < x):     # x debe ser positivo
        z = h + 1
    elif (h > x):     # x debe ser negativo
        z = h
    else:             # x era un entero
        z = h
    return z
```

Ejemplo. Subconjuntos f_1, f_2, f_3, y f_4 del producto cartesiano $A \times B$ de los conjuntos A y B, en donde $A = \{a, b, c\}$, $B = \{\alpha, \beta, \gamma, \delta\}$. En algunos son también funciones y otros no, ver Fig. 4.1:

1) $f_1 = \{(a, \beta), (b, \delta), (c, \alpha)\}$: en este caso se cumplen las condiciones de existencia y de unicidad, por lo que el subconjunto f_1 del producto cartesiano $A \times B$ es una función. Notar que el elemento γ del codominio B no tiene preimagen alguna (no importa);
2) $f_2 = \{(a, \beta), (b, \delta), (c, \beta)\}$: también se cumplen las condiciones de existencia y de unicidad. Luego, el subconjunto f_2 del producto cartesiano $A \times B$ es una función. Notar que el elemento β del codominio B tiene dos preimágenes (no importa);
3) $f_3 = \{(a, \delta), (b, \beta), (b, \gamma), (c, \alpha)\}$: notar que el elemento b del conjunto A tiene asignado dos elementos ((b, β) y (b, γ)). Luego, no se cumple la condición de unicidad, por lo que el subconjunto f_3 del producto cartesiano $A \times B$ no es una función;
4) $f_4 = \{(a, \delta), (c, \alpha)\}$: notar que el elemento b del conjunto A no tiene asignado elemento alguno en el codominio. Luego, no se cumple la condición de existencia para todos los elementos del dominio A, por lo que el subconjunto f_4 del producto cartesiano $A \times B$ no es una función.

Ejemplo. Sean las funciones $g\colon A \to B$ y $f\colon B \to C$. Demuestre o dé un contraejemplo en cada caso:

1) Si f y $(f \circ g)$ son sobreyectivas, entonces g ¿es también sobreyectiva? Rpta: es F, contraejemplo: sea los conjuntos $A = \{a\}$, $B = \{2, 3\}$, y $C = \{\delta\}$, y las funciones $g = \{(a, 2)\}$, y $f = \{(2, \delta), (3, \delta)\}$. Se tiene que $(f \circ g) = \{(a, \delta)\}$, con lo cual se tiene que f y $(f \circ g)$ son sobreyectivas pero g no lo es.
2) Si f y g son inyectivas, entonces $(f \circ g)$ ¿es también inyectiva? Rpta. Sean los elementos a y b distintos en A. En ese caso:
   - Como $g\colon A \to B$ es inyectiva, hay unicidad de su preimagen, por lo que $g(a)$ y $g(b)$ son elementos distintos en B;
   - Como $f\colon B \to C$ es inyectiva, hay unicidad de su preimagen, por lo que $f(g(a))$ y $f(g(b))$ son elementos distintos en C;
   - Lo anterior vale para todo $a, b \in A$, con $a \neq b$. Se concluye que $(f \circ g)$ es inyectiva cuando f y g también lo son.
3) Si f y g son sobreyectivas, entonces $(f \circ g)$ ¿es también sobreyectiva? Rpta. Sea un elemento $c \in C$. En ese caso:
   - Como $f\colon B \to C$ es sobreyectiva, entonces para todo $c \in C$ se tiene que $c = f(b)$ para algún $b \in B$;
   - Como $g\colon A \to B$ es sobreyectiva, entonces para todo $b \in B$ se tiene que $b = g(a)$ para algún $a \in A$;
   - Eso significa que $c = f(b) = f(g(a))$. Esto vale para todo $c \in C$, por lo que se concluye que $(f \circ g)$ es sobreyectiva cuando f y g también lo son.

CAPÍTULO 5

Intro básico a Python 3

Contents

5.1. Computadoras, programas, y lenguajes de programacion

- Python es un Lenguaje de Programación (LP) de algoritmos que es de *alto nivel*, *multiparadigma*, *multiplataforma*, *fuertemente tipado*, e *interpretado*.

- *Multiplataforma*: diferentes tipos de computadoras y sistemas operativos (e.g. Windows, MAC, Linux).
- *Multiparadigma*: un LP que es multiparadigma permite al programador escribir un programa adoptando algún estilo particular de programación, e.g. en Python:
  - programación imperativa;
  - programación funcional;
  - programación orientada a objetos.
- Un *programa computacional* (o *programa* (a secas), o *código computacional*): es una secuencia finita de operaciones (instrucciones) que la compu realiza, una por una, para realizar una tarea especifica.
- Los programas **imperativos** indican expresamente a la compu **cómo debe realizar una tarea**, de la misma manera que el modo verbal imperativo en los lenguajes humanos le indica qué hacer al interlocutor.
- Observ. 1: en el curso introductorio de Python 3 (en la FIQ) el estilo de programación será exclusivamente el de programación imperativa.
- Observ. 2: hay un quiebre fuerte entre las versiones 2.x y 3.x de Python, y no son compatibles.

5.2. Lenguajes de Programación (LP)

- Los Lenguajes de Programación (LP) son herramientas de comunicación entre las personas y las compus.
- Permiten a una persona (programador) traducir un algoritmo dado en una secuencia de instrucciones de un modo tal que la compu las pueda ejecutar.
- Existe una cantidad gigantesca de LP distintos, con muchas formas de clasificarlos. Lo que sigue no-es exhaustivo.

5.2.1. LP de alto y bajo nivel

- La clasificación de LP de alto y de bajo nivel divide a los LP según la proximidad de las instrucciones que escribe el programador con las instrucciones que físicamente usa la compu.
- Las instrucciones que físicamente usa la compu son muy sencillas y definidas mediante valores numéricos, pero rápidamente se vuelve inmanejable para las personas.
- Para facilitar el trabajo de los programadores, los fabricantes definen lenguajes particulares para las instrucciones de sus microprocesadores en donde introducen identificadores mnemotécnicos, dando lugar así a los *Lenguajes de Ensamblador* (LE).
- Por ejemplo, muchos de los procesadores de Intel y AMD comparten el LE pero no en todos, y son incompatibles con los LE de los PowerPC (IBM), Apple, Playstation, Sun, Silicon Graphics, ni tampoco con el LE de una SONY Playstation.
- Lenguajes de *Bajo Nivel* (LBN): debido a la cercanía con las instrucciones más profundas de la microelectrónica, los LE son considerados como LBN.

- Lenguajes de *Alto Nivel* (LAN): los LAN abstraen al programador de los detalles de las instrucciones, mediante expresiones más cercanas al lenguaje natural o a las matemáticas discretas.

5.2.2. LP imperativos, funcionales, y orientados a objetos

- En los LP **imperativos** los programas se dividen tajantemente en **datos** y en **instrucciones**, siendo estas últimas las encargadas de manipular los datos de forma explícita. Es decir, se basan en la manipulación de variables a las que el programa les va asignado valores específicos posiblemente cambiantes durante la ejecución.
- En los LP **funcionales** se diluye un tanto la diferencia entre instrucciones y datos porque es posible asignar bloques de intrucciones a variables.
- En los LP **orientados a objetos** las instrucciones y los datos se unen en un único ente denominado un **objeto**. El tipo de un objeto queda definido por las operaciones que pueden realizarse sobre él y no por los datos que contiene.

5.2.3. LP interpretados y LP compilados

- El código de un programa suele escribirse en uno o varios ficheros de texto, y que si bien es entendido por un humano (o debiera serlo), no puede ser ejecutado directamente por la compu.
- Lenguajes Interpretados (LI): existe un componente de software llamado *intérprete* que lee las líneas de código y las ejecuta inmediatamente. Muchos intérpretes admiten dos modos de empleo: interactivo y de script.
- Intérprete Interactivo (II): el intérprete muestra al usuario un símbolo especial y espera a que el usuario introduzca las líneas a ejecutar na a una, ejecutándolas inmediatamente.
- Intérprete Script (IS): el usuario proporciona uno o más ficheros al intérprete quien ejecutará todas las líneas, una tras otra.
- Los LI son sencillos de usar y muy flexibles, pero no son eficientes, ya que se mezcla la tarea de interpretación y proceso del código con la ejecución.
- Para evitar bajos rendimientos, el código de un programa suele convertirse en código binario que el procesador pueda ejecutar directamente. Este proceso se denomina **compilación** y se emplea en lenguajes que requieran un gran rendimiento.

5.2.4. LP estructurados

Los LP estructurados son lenguajes de alto nivel que ofrecen una serie de construcciones de control de las instrucciones que hace un programa:

- **Bucles** (o lazos): en donde un bloque de código se ejecuta de forma repetida, o bien mientras que se cumpla una condición (ciclo *mientras* o `while`), o bien un número determinado de veces (ciclo *para* o `for`).
- **Bifurcaciones**(condicional *si-entonces-sino* `if ... elif ... else`): en donde un bloque de código se ejecutará dependiendo del VV de una proposición, a veces una proposición simple o, frecuentemente, una proposición compuesta, e.g. ver [4].

- **Funciones**: son bloques autónomos e independientes de código que realizan una serie de operaciónes concreta. Pueden recibir datos de otras partes del programa en forma de parámetros, y que pueden devolver uno o más valores al terminar de ejecutarse.

5.2.5. LP fuertemente y débilmente tipados

- Un LP *débilmente tipado* no define de forma explícita el tipo de las variables (cuáles las operaciones que le son válidas), sino que el tipo de variable se determina durante la ejecución, en función de los valores que se les asignan.
- Un LP *fuertemente tipado* se determina de forma explícita el tipo de las variables (cuales son las operaciones que son válidas). No se permiten violaciones de los tipos de datos, i.e. si el valor de una variable es de un tipo concreto, then no se puede usar como si fuera de otro tipo distinto, a menos que se haga una conversión adecuada.

5.3. Errores cuando se codifica con un LP

5.3.1. Errores de sintaxis

Los errores de sintaxis es cuando la codificación del programa no sigue las reglas de sintaxis definidas por la norma, e.g. la frase “La ratón comer queso un”, no sigue la sintaxis de la lengua castellana, y es incorrecta. Lo mismo ocurre en los LP, por lo que hay que recordar bien todas las reglas.

5.3.2. Errores lógicos

- Los errores lógicos son más intrincados de localizar. Un fallo en la lógica del programa está en alguna parte que hace que su funcionamiento no sea el que desea el programador.
- Este tipo de fallos son semejantes a la frase “El queso come un ratón” aunque es sintácticamente correcta, el sentido común nos dice que es imposible.
- Ningún compilador o intérprete es capaz de localizar los errores lógicos. El error lógico se hace presente durante la ejecución del programa.
- Los errores en tiempo de ejecución se detectan observando en dónde el programa no hace lo que el programador desea. Pueden dividirse en dos tipos:
    - **Errores lógicos con aviso**: puede suceder que el error sea de tal envergadura que haga saltar los mecanismos de protección del sistema operativo (en programas compilados) o que el intérprete (en programas interpretados) nos avise del error.
    - **Errores lógicos sin aviso**: son errores lógicos que pasan desapercibidos porque la única notoriedad que presentan es que el programa no hace lo que debería hacer.

  Tanto para la localización y eliminación los errores lógicos con aviso como sin aviso, se requiere de una herramienta adicional denominada *debugger*, que no veremos.

suma	$+$
resta	$-$
multiplicación	$*$
exponenciación	$**$
división	$/$
división entera	$//$
módulo (resto de la división $r = a \mod b$)	%

Tabla 5.1: Operadores aritméticos para números.

5.4. Python como calculadora de almacenero

5.4.1. Intro

- **Operadores aritméticos**: ver Tabla 5.1. Observ.: no confundir el operador % para resto con el porcentaje de la calculadoras.
- **Uso de espacios**: es posible usar (o no) espacios entre operadores. En general, se sugiere seguir un estilo uniforme (siempre de la misma forma).
- **División por cero exacto**: ya sea entero o con punto decimal, Python emitirá un mensaje de error.
- **Forma indeterminada** 0^0: si bien en matemáticas es una forma indeterminada, sin embargo, Python evalúa $0 * *0$ devolviendo **errroneamente** un 1.
- **Uso de paréntesis**: es posible introducir pares de paréntesis, siempre (para abrir y) para cerrar, Observa.: no se admiten corchetes, llaves, o barras porque tiene otro uso reservado.
- **Orden de precedencia**: cuando dos operadores comparten un operando (i.e. un número), el operador con mayor prioridad procede primero. Las prioridades de los operadores están dadas por las reglas de precedencia, y que son listadas en la Tabla 5.2. Ejemplo:

  1) $a + b * c$ es evaluado como $a + (b * c)$;
  2) $a * b + c$ es evaluado como $(a * b) + c$.

- **Asociatividad**: cuando dos operadores comparten un operando y los operadores tienen igual prioridad, la expresión es evaluada de acuerdo a las propiedades asociativas de ambos operadores. Ejemplo:

  1) Como el operador de exponenciación $**$ es asociativo **de derecha a izquierda**, la expresión $a * *b * *c$ es evaluado como $a * *(b * *c)$;
  2) Como el operador de división / es asociativo **de izquierda a derecha**, la expresión $a/b/c$ es evaluado como $(a/b)/c$.

- **Orden de evaluación**: las expresiones artiméticas se evaluan **de izquierda a derecha**, i.e. el operador a la izquierda es evaluado antes que el operador a la derecha. En caso de ambiguedades, se aplican reglas de asociatividad y de precedencia, ver Tabla 5.2.

1	exponenciación	$**$
2	multiplicación, división, división entera, y módulo	$*$, /, //, %
3	sumas, restas	$*$
4	exponenciación	$**$
5	división, división entera, módulo	/, //, %

Tabla 5.2: Reglas de precedencia en operaciones aritméticas.

5.4.2. Algunas funciones numéricas y tipos de números

- **Funciones aritméticas de uso básico**: algunas (pocas) funciones aritméticas de uso básico están disponibles directamente, e.g. ver Tabla 5.3.
- Python distingue las letras mayúsculas de las minúsculas, e.g. no es lo mismo `abs(...)`, que `ABS(...)`, o `Abs(...)`, entre otras de las 8 combinaciones posibles.
- Los **tipos de números** que veremos son:
  - `int` que viene de *integer* o entero;
  - `float` que viene de *float point number* o número de punto flotante, con lo cual se designa la codificación de los números decimales en la compu
- Las funciones `int(x)` y `round(x)` no son equivalentes: si bien `int(x)` y `round(x)` truncan la parte decimal del número decimal x, la función `int(x)` no altera la parte entera de x, mientras que `round(x)` tal vez si.
- **Números enteros**: en Python se puede trabajar con enteros de casi **cualquier tamaño**: su única limitaación es la capacidad de la memoria primaria, o RAM (por *Random-Access Memory*), i.e. a mayor RAM, mayor será el entero que se puede representar. Esto es así porque los números enteros en Python se manipulan internamente mediante software, lo cual lo hace relativamente lento. Ejemplo, evaluar $123 * *456$.
- **Números decimales**:
  - Los decimales se distinguen ya sea porque tienen un punto decimal, o también porque usan una variante de la notación científica, introduciendo la letra `e` en el número decimal. Ejemplo:
    - El decimal 123.45: observar que no se usa coma (como en las calculadoras;
    - El decimal 12.34×10^5 se escribe en Python como `12.34e5` o `12.34e+5`, e.g. notar que no explicitamos la base 10 ni usamos el operador de exponenciación $**$;
    - El decimal 12.34×10^{-5} se escribe en Python como `12.34-e5`;
    - Observación: **no-confundir** la letra `e` con el número $e = 2.71828...$
  - Pero el tamaño de los decimales en Python es **limitado** (como es lo usual en todos los lnguajes de programacón), e.g. el máximo decimnal que se puede representar es aproximadamente de 1.7977×10^{308}.

valor absoluto de x	`abs(x)`
redondeo de x a entero	`round(x)`
redondeo de x a entero con n decimales	`round(x,n)`
tipo de número	`type(x)`

Tabla 5.3: Algunas funciones aritméticas básicas.

5.5. Python como calculadora científica

5.5.1. Intro

- El Python cuando empieza tiene un conjunto relativamente pequeño de operaciones y funciones matemáticas predeterminadas.
- Para poder agregar nuevas posibilidades, de matemáticas y de otras yerbas, se dispone del mecanismo de *módulos* con nombres y posibilidades predefinidos. En particular, el módulo `math` permite acceder a otras funciones y constantes matemáticas.
- Existen diversas maneras de importar módulos pero en el curso será suficiente usar la forma básica `import math`, con lo cual se accede a todo lo disponible en dicho módulo.
- En la Tabla 5.6 se listan algunas funciones disponibles en el módulo `math`. Para usarlas hay que el nombre del módulo y un punto como separador, i.e. `math.`, e.g.
  - Con `math.pi` accedemos a un valor aproximado de π;
  - Con `math.exp(x)` accedemos a un valor aproximado de la función e^x. Notar el uso exclusivo de paréntesis;
  - La función logaritmo `math.log(x)` corresponde al logaritmo natural $\ln(x) = \log_e(x)$;
  - En computación también es útil el logaritmo en base 2 $\log_2(x)$ que se tipea como `math.log2(x)`;
  - Nota: no-usaremos `math.e` porque termina siendo **fatal** en parciales y finales, por lo que lo reemplazaremos con la forma equivalente `math.exp(1)`, puesto que $e = e^1$.
- **Funciones trigonométricas**:
  - Los argumentos de las funciones trigonométricas NO son en grados sino en radianes, por lo que hay que introducir factores de conversión de unidades antes de usarlas. Ejemplo: hallar el seno del ángulo $\alpha = 23°$:
    - En matemáticas: primero hay que convertirlo a radianes, y después calcular la función trigonométrica, o sea, $23° = 23° * (pi/180°) \approx 0.40143$ radianes, por lo que $sin(\alpha) = \sin(0.40143) \approx 0.39073$
    - En Python: se importa el módulo `math`, y se sigue el mismo orden en las cuentas, si bien no se indican las unidades en grados que quedan implícitas en radianes:

```
>>> import math
>>> alfa_rad = 23 * (math.pi/180.0)
>>> math.sin (alfa_rad)
```

año n	monto actual	interés sobre el monto actual	monto actualizado
1	1000	$1000 \times 10\,\% = 100$	1000+100=1100
2	1100	$1100 \times 10\,\% = 110$	1100+110=1210
3	1210	$1210 \times 10\,\% = 121$	1210+121=1331
4	1331	$1331 \times 10\,\% = 133.10$	1331+133.10=1464.10

Tabla 5.4: Ejemplo del cálculo con el interés compuesto.

año n	monto	actualizado a partir del monto anterior	actualizado a partir del monto inicial
1	1000	$1000(1+0.10) = 1100$	$1000(1+0.10)$
2	1100	$1100(1+0.10) = 1210$	$1000(1+0.10)(1+0.10) = 1000(1+0.10)^2$
3	1210	$1210(1+0.10) = 1331$	$1000(1+0.10)(1+0.10)(1+0.10) = 1000(1+0.10)^3$
4	1331	$1331(1+0.10) = 1464.10$	$1000(1+0.10)(1+0.10)(1+0.10)(1+0.10) = 1000(1+0.10)^4$

Tabla 5.5: Cálculo con el interés compuesto (cont.).

- Ovserv.: las funciones de Python de conversión `math.radians` y `math.degrees` **están prohibidas de usar en el curso (-5 puntos en parcial o examen)**.
- Atención con valores de argumentos en zonas problemáticas, e.g. si bien $\tan(pi/2) = \infty$, sin embargo,

```
>>> import math
>>> math.tan(math.pi/2)
1.633123935319537e+16
```

o sea, dá un resultado grande pero erróneo $1.633123935319537 \times 10^{16}$.

- Notar que `math.trunc(x)` es lo mismo que `int(x)`. Moraleja: a veces se puede hacer lo mismo en más d euna forma.
- **Función piso**: definida por $\lfloor x \rfloor = \max\{n \in \mathbb{Z}; n \leq x\}$. En Python se accede con `math.floor(x)`;
- **Función techo**: definida por $\lceil x \rceil = \min\{n \in \mathbb{Z}; n \geq x\}$. En Python se accede con `math.ceil(x)`;

Observación. La cantidad de cifras en base 10 de un entero n positivo puede encontrarse usando $\log_{10}(n)$, porque n tiene k cifras ssi $10^{k-1} \leq n < 10^k$, es decir, ssi $(k-1) \leq \log_{10}(n) < k$, o sea, ssi $k = 1 + \lfloor \log_{10}(n) \rfloor$, o alternativamente $k = \lceil \log_{10}(n+1) \rfloor$.

5.6. Python como calculadora financiera

5.7. Interés compuesto

- En el interés compuesto, calculamos el interés en el primer período y lo sumamos al total, luego calculamos el interés en el siguiente período y lo sumamos al total, y así hasta el final (i.e. es una RR), e.g. para un préstamo de ARS 1000 a 4 años al 10 % se tienen las cuentas detalladas en la Tabla 5.4 La cuenta básica es:
  - Calcular el interés (monto actual × tasa de interés);
  - Sumar el interés al monto actual para obtener el monto actualizado;

- Repetir la cuenta con el monto actualizado.

las cuales aplicadas en el primer año es

$$1000 + (1000 \times 10\,\%) = 1000 + (1000 \times 0.10) = 1000(1 + 0.10) \tag{5.1}$$

Así que sumar el 10 % de interés equivale a multiplicar por el factor $F = 1 + 0.10 = 1.10$, el cual será *constante* en cada uno de los 3 años siempre que la tasa t_c también lo sea. Luego, se puede re-escribir las cuentas como en la Tabla 5.5;

- Entonces, cuando la tasa t_c es *constante*, la fórmula del interés compuesto está dada por

$$P_n = P_0(1 + t_c)^n \tag{5.2}$$

donde P_0 es el monto inicial, P_n es el monto a pagar después de n períodos (años, meses, etc.), mientras que t_c es la tasa "tanto por uno" (la tasa porcentual t_p % dividido por 100 $t = t_p\,\%/100$);

- Pero cuando la tasa de interés t es *variable* la Ec. (5.3) se generaliza a:

$$P_n = P_0(1 + t_1)(1 + t_2)...(1 + t_n) \tag{5.3}$$

en donde ahora t_1, t_2, ... t_n son las tasas de interés en cada período y, en general, son todas distintas entre si;

- En contabilidad es frecuente recurrir a una tasa de *equivalente*, en donde la idea es obtener el mismo monto final P_n pero mediante una tasa de intereés *constante* t_e (ficticia):

$$P_n = P_0(1 + t_e)^n \tag{5.4}$$

Para hallar t_e igualamos las Ecs. (5.3) y (5.4), obteniendo

$$(1 + t_e)^n = (1 + t_1)(1 + t_2)...(1 + t_n) \tag{5.5}$$

sacando raíz n lado a lado

$$1 + t_e = \sqrt[n]{(1 + t_1)(1 + t_2)...(1 + t_n)} \tag{5.6}$$

en donde el lado derecho es la *Media Geométrica* (MG) de las tasas. Despejando, la tasa equivalente es

$$\begin{aligned} \alpha &= \mathrm{MG}\,(t_1, t_2, ..., t_n) \\ t_e &= \alpha - 1 \end{aligned} \tag{5.7}$$

5.8. Tasas de inflación

Existen diversas tasas de inflación, e.g. inflacón acumulada, inflación promedio anual, inflación mensual, etc. Para calcularlas hay que cambiar la palabra "interés" en la Sec. anterior por "inflación" y adaptar esas fórmulas.

Ejemplo. Ejercicio 3.11 (libro 2016, cuatrimestre 2):

a) Si la inflacion en el primer año fue del 22 %, y en el segundo año fue del 25 %: ¿Cuánto cuesta ahora un artículo que dos años atrás costaba ARS 100 ? Sol.

$$\begin{aligned} P_1 &= P_0(1+t_1) \\ P_2 &= P_1(1+t_2) \end{aligned} \tag{5.8}$$

donde $P_0 = 100$, $t_1 = 22/100$, $t_2 = 25/100$. Calculando con Python resulta

```
>>> 100*(1+0.22)
122.0
>>> 122*(1+0.25)
152.5
```

i.e. el artículo que 2 años atrás costaba 100, luego del 1er año y con inflación del 22 % costaba 122, y luego del 2do año y con inflación del 25 % cuesta 152.5.

b) Si la inflacion en el primer año fue del 22 %, y en el segundo año fue del 25 %: ¿Cuál es la inflación anual promedio de estos dos años? Aclaración: se busca un valor r tal que si la inflación anual hubiese sido constantemente r, en dos años habríamos obtenido la misma inflación acumulada que teniendo 22 % y 25 %. Sol.: utilizamos la Ec. (5.7)

$$\begin{aligned} \alpha &= \mathrm{MG}\,(t_1, t_2) = \sqrt{(1+t_1)(1+t_2)} \\ t_e &= \alpha - 1 \end{aligned} \tag{5.9}$$

donde $t_1 = 22/100$, $t_2 = 25/100$. Calculando con Python resulta

```
>>> ((1+0.22)*(1+0.25))**(1/2)           # Media Geometr. (MG) de los factores
1.2349089035228469
>>> round((1.2349089035228469-1)*100,2) # MG menos 1, por 100, redondeado a 2
23.49
>>> round(100*(1+0.2349)*(1+0.2349),2)  # verifica con el articulo de 100
152.5
```

c) El kilo de pan hoy cuesta 30 y (exactamente) dos años atrás costaba 15 ¿Qué estimación puede darse sobre el promedio de inflación en cada uno de estos dos años? Sol.: utilizamos la Ec. (5.3)

$$P_2 = P_0(1+t)^2 \quad \therefore \quad t = \sqrt{P_2/P_0} - 1 \tag{5.10}$$

donde $P_0 = 15$, $P_2 = 30$. Después, para verificar, re-calculamos los precios del pan en cada año

$$\begin{aligned} Q_1 &= P_0(1+t) \\ Q_2 &= Q_1(1+t) \end{aligned} \tag{5.11}$$

debiendo resultar $Q_2 \equiv P_2$. Calculando con Python resulta

```
>>> import math
>>> round(math.sqrt(30/15)-1,4) # tasa de inflacion promedio
0.4142
>>> round(15*(1+0.4142),2)      # costo del pan despues del 1er anio
21.21
>>> round(21.21*(1+0.4142),2)   # costo del pan despues del 2do anio
30.0
```

matemática:	Python:
π	`math.pi`
e	`math.exp(1)`
$\sqrt{x}$	`math.sqrt(x)`
e^x	`math.exp(x)`
$\ln(x)$	`math.log(x)`
$\log_{10}(x)$	`math.log10(x)`
$\sin(x)$	`math.sin(x)`
$\cos(x)$	`math.cos(x)`
$\tan(x)$	`math.tan(x)`

Tabla 5.6: Algunas funciones aritméticas en el módulo `math`.

d) En determinado año la inflación anual fue de 36 % ¿Cuál fue, en promedio, la inflación mensual de ese año? Sol.: buscamos una tasa t mensual equivalente a la anual t_a tal que

$$(1+t)^{12} = 1 + t_a \tag{5.12}$$

despejando t resulta

$$t = \sqrt[12]{1+t_a} - 1 \tag{5.13}$$

donde $t_a = 36/100$ (dato). Luego de calcular t mediante la Ec. (5.13), se debe verificar que

$$(1+t)^{12} - 1 = t_a \tag{5.14}$$

Calculando con Python resulta

```
>>> import math
>>> round(100*((1+0.36)**(1/12)-1),2) # inflacion media mensual porcentual
2.6
>>> round(((1+2.6/100)**12-1)*100)    # verificacion: debe dar 36%
36
```

e) Si la inflación mensual es de 3 % durante los 12 meses del año ¿Cuál será la inflación anual? Sol.: en la Ec. (5.6) despejamos

$$t_a = (1+t)^{12} - 1 \tag{5.15}$$

donde $t = 3/100$. Calculando con Python resulta

```
>>> round(100*((1+3/100)**12-1),2) # tasa de inflacion del 3% mensual
42.58                              # inflacion anual promedio
```

5.9. Tipos de datos básicos en Python

En el curso sólo se verán 4 tipos básicos:

- **Entero**: `int` (que es una abreviación de *integer*);
- **Decimal**: `float` (que es una abreviación de *float point number*);
- **Booleano**: `bool` (que es una abreviación de *boolean*);
- **Cadena**: `str` (que es una abreviación de *string*).

5.9.1. Datos de tipo booleano

- **Valores lógicos**: una expresión lógica equivale a una proposición por lo que, o bien es `True`, o bien es `False`;
- **Operadores lógicos**: en la Tabla 5.7 se muestran algunos operadores lógicos, en donde los dos primeros son de uso más frecuente;
- **Preguntas por igualdad o desigualdades**: en la Tabla 5.8 se resumen preguntas binarias por igualdad o desigualdad de dos valores A y B:
  - Para preguntar si el valor de A es igual al de B se emplea ==, es decir, se escribe `A == B`, lo cual es una pregunta frecuente con números o cadenas, y la respuesta es un valor lógico `True` o `False`;
  - Nota: en computación el significado de = es, en general, distinto al de = usado en matemática, dando lugar a confusiones a la novatada;
  - Para preguntar si el valor de A es distinto al de B se emplea $! =$, es decir, se escribe `A != B`, también es una pregunta frecuente con números o cadenas, y la respuesta es un valor lógico `True` o `False`.
- **Dos preguntas en una única expresión**: en Python es lícito codificar $a < b < c$ (en otros lenguajes no), y que es lógicamente equivalente a $(a < b) and (b < c)$;
- **Orden de evaluación en una expresión lógica**: las expresiones lógicas se evalúan de izquierda a derecha, por lo que en programación los operadores `and` o `or` no son conmutativos;
- **Precedencia de evaluación en una expresión lógica**: a diferencia d ela matemática, hay reglas de precedencia cuando dos operadores comparten un operando. Otra vez, el operador con mayor prioridad procede primero. Las reglas de precedencia son listadas en la Tabla 5.9;
- **Cortocircuitos en lógica**: una regla de facto en programación es la siguiente: cuando se va evaluando una expresión lógica, de izquierda a derecha, se evita continuar avanzando a menos que sea necesario para definir el VV de la misma. Ver el siguiente ejemplo, y hacer el Ejercicio 4.8;
- Observ.: las codificaciones que mezclan valores o expresiones numméricas con expresiones lógicas **están prohibidas de usar en el curso (-5 puntos en parcial o examen)**.

Ejemplo. La proposición compuesta $(p \vee q \vee r)$, donde p, q, y r son proposiciones dadas, es `True` si al menos una de las mismas lo es. En Python es `(p or q or r)`. La evaluación avanza de izquierda a derecha:

- Si p es `True` entonces deja de avanzar, porque el VV de la proposición compuesta es `True`, independiente de los VV de q y de r;
- Sino, continua evaluando q: si q es `True` entonces otra vez deja de avanzar, porque el VV de la proposición compuesta es `True`, independiente del VV de r;
- Sino, recién entonces evalua r.

Definición. Recordatorio. Sean p y q proposiciones. La proposición “o bien p o bien q” es aquella que es verdadera cuando exactamente solo una de las proposiciones es verdadera,

conjunción	$p \wedge q$	`p and q`
disyunción (inclusiva)	$p \vee q$	`p or q`
disyunción exclusiva	$p \oplus q \equiv p \wedge \neg q \vee \neg p \wedge q$	`(p and not q) or (not p and q)`

Tabla 5.7: Algunas operadores lógicos en Python.

por menor o igual	$a \leq b$	`a <= b`
por menor	$a < b$	`a < b`
si son iguales	$a = b$	`a == b`
si son distintos	$a \neq b$	`a != b`
por mayor	$a > b$	`a > b`
por mayor o igual	$a \geq b$	`a >= b`

Tabla 5.8: Preguntas binarias por igualdad o desigualdad en Python.

y es falsa en los demás casos. *Notación*: la disyunción exclusiva de p y q la denotaremos con $p \oplus q$ y se puede leer como "o bien p, o bien q", y su TV está dada en la Tabla 5.10.

Observación. Las TV de la disyunción exclusiva $p \oplus q$ y de $(p \wedge \neg q) \vee (\neg p \wedge q)$ son las mismas, como se muestra en la Tabla 5.11.

Tarea. Mostrar que las TV de la disyunción exclusiva $p \oplus q$ y de $\neg(p \wedge q) \wedge (p \vee q)$ son las mismas.

Observación. Una implementación de la disyunción exclusiva $p \oplus q$, teniendo en cuenta la Observ. 5.9.1, es listada en la función:

```python
# In idle3 open this file and hit F5 ("run module").
def logical_xor(p,q):
   z = (p and not q) or (not p and q)
   return z

# Test
if __name__ == '__main__':
   test_data = [ [False , False],  [False , True ],
                 [True  , False],  [True  , True ]]
   for (p, q) in test_data:
       print (p, q, logical_xor(p,q))
# end
```

Observación. Otra implementación de la disyunción exclusiva $p \oplus q$ es listada en la función:

```python
def logical_xor (p,q): # donde "p" y "q" son valores booleanos
   return (a^b)
```

5.9.2. Datos tipo cadena de caracteres

- Los caracteres son las letras, signos de puntuación, dígitos, y otros símbolos usados en la escritura.

1	negación	$\neg p$	`not`
2	conjunción	$p \wedge q$	`p and q`
3	disyunción	$p \vee q$	`p or q`

Tabla 5.9: Reglas de precedencia en operadore lógicos.

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Tabla 5.10: Disyunción exclusiva (**xor**).

p	q	$p \oplus q$	$(p \wedge \neg q) \vee (\neg p \wedge q)$
F	F	F	F
F	T	T	T
T	F	T	T
T	T	F	F

Tabla 5.11: Las TV de la disyunción exclusiva $p \oplus q$ y de $(p \wedge \neg q) \vee (\neg p \wedge q)$ son las mismas.

- Las cadenas de caracteres son sucesiones de estos caracteres que en Python van encerradas entre comillas, ya sean sencillas, e.g. como en `'Ana Luisa'`, o dobles, como en `''Ana Luisa''`.
- A diferencia de los tipos entero, decimal y lógico, las cadenas de caracteres son entes compuestos, constituidos por elementos más sencillos (los caracteres).
- En realidad, Python no tiene el tipo carácter: para representar un caracter se consideras una cadena de un elemento, e.g. la letra “a” se escribe como la cadena `'a'`.
- **Concatenación**: concatenar es poner una cadena a continuación de otra, para lo cual en Python se usa el mismo símbolo que para la suma de números, o sea, el símbolo `+`.
- **Cadena vacía**: la cadena vacía es la cadena `''`, o la equivalente , sin caracteres y tiene longitud 0. Es similar a la noción de conjunto vacío en el contexto de conjuntos o el cero en números.

5.10. Impresiones por pantalla

- El comando `print` imprime por pantalla expresiones de diversos tipos, con poco o mucho grado de detalle. La regla básica es: por omisión (mientras menos indicamos), se imprime lo más simple y claro posible.
- Observ.: que dos impresiones se vean iguales en la pantalla, no significa que correspondan a lo mismo, e.g. comparar `print (False)` y `print ('False')`:

```
>>> print (False)
False
>>> print ('False')
False
>>> type(False)
<class 'bool'>
>>> type('False')
<class 'str'>
```

- Cuando la cadena es muy larga y no cabe en un renglón, podemos usar la barra invertida \ para dividirla.
- Si bien podemos usar \ para indicar que el renglón continúa pero, si en realidad, se quiere imprimir \\, entonces tenemos que poner \\ dentro del argumento del `print`,

e.g. comparar `print('\')` con `print('\\')`.

- Aunque se puede agrandar la ventana de IDLE, es recomendable no-escribir renglones con más de 80 caracteres.

5.11. Variables y asignaciones

- Cuando escribimos valores como 123 o `'Kika'`, Python los guarda en la memoria de modo tal que podemos hacer uso posterior de esos valores. Para eso, debemos escribir un nombre apropiado a cada valor, llamado *identificador*, y luego una *asignación*, indicada mediante el símbolo =, que relaciona el *identificador* con el *valor*, e.g.

```
>>> aa = 123          # relaciona identific. con un valor de tipo entero
>>> bb = -5.67        # relaciona identific. con un valor de tipo decimal
>>> p = True          # relaciona identific. con un valor de tipo booleano
>>> texto = "mi mama" # relaciona identific. con un valor de tipo cadena
```

- A fin de conservar una nomenclatura parecida a la de otros lenguajes de programación, decimos que `aa`, `bb`, `p`, y `texto` son *variables*. Nota: en realidad el concepto es distinto en Python, ya que son una referencia a un lugar de la memoria, similar al enlace (*link*) en una página de internet.
- Reglas para los *identificadores* (los *nombres* de las *variables*) [no-veremos todas las reglas precisas, que son un tanto complicadas y están en el manual de referencia]:
  - Pueden tener cualquier longitud (cantidad de caracteres) pero no pueden usar todos los caracteres, como se indica a continuación;
  - No pueden tener espacios;
  - No pueden tener signos especiales de puntuación (como la coma, como en `a,b`, o el punto, como en `c.d`);
  - No pueden tener signos especiales como +, -, *, /, etc. para no-confundir con las operaciones;
  - No pueden empezar con un número, e.g. como en `2ab`, pero si es posible colocarlo entremedio, e.g. como en `a2b`, o al final, e.g. como en `ab2`;
  - Aunque se permite, los identificadores **no-deberán empezar ni terminar** con un *guión bajo*, e.g. `_zz` o `gravedad_`, dejando esta posibilidad para identificadores especiales que provienen de otra parte;
  - Pero si aceptaremos un guión bajo cuando esté entremedio de un identificador, e.g. como en `fibonacci_version2`;
  - Es conveniente no-usar tildes, i.e. á , é, í, ó, ú, ñ, ü, etc.;
  - Palabras reservadas del Python: algunas están prohibidas y otras es conveniente no-usarlas como identificadores, e.g.

```
>>> while=4                 # es una palabra reservada no-asignable
SyntaxError: invalid syntax
>>> for=4                   # es una palabra reservada no-asignable
SyntaxError: invalid syntax
>>> import math             # importamos el modulo math
>>> math=3                  # pero lo "pisamos" como un identificador
>>> math                    # el valor de math ahora es 3
3
>>> math.sqrt(4)            # no-se accede al contendio del modulo math
```

```
Traceback (most recent call last):
  File ”<pyshell#11>”, line 1, in <module>
    math.sqrt(4)
AttributeError: ’int’ object has no attribute ’sqrt’
>>> import math                  # volvemos a importar el modulo
>>> math.sqrt(25)                 # ahora si podemos calcular
5
```

- Los identificadores con mayúsculas y minúsculas son *diferentes*;
- Es conveniente evitar introducir identificadores que resulten muy parecidos, e.g. `sqr` (elevar al cuadrado) versus `sqrt` (raíz cuadrada) es algo que hay en Pascal (malo).

5.12. Variables globales y locales

- Cuando se define una función se crea un objeto de tipo `function` (función), con su propio contexto, y se construye una variable que tiene por identificador el nombre de la función;
- En el contexto de una función habrán objetos como instrucciones y variables, que son locales a la función;
- Los argumentos (si los hubiera) en la definición de una función se llaman *parámetros formales* (o *mudos*) y los que se usan en cada llamada son los *parámetros reales*;
- Cuando se llama a la función, se produce un mecanismo similar al de una asignación, asignando cada uno de los parámetros formales a sus correspondientes parámetros reales, en el mismo orden, e.g. si `f` está definida por `def f (a, b):` ..., entonces `a` y `b` son variables *locales* a la función, y cuando hacemos la llamada `f(x, y)` se hacen las asignaciones `a = x` y `b = y`, en ese orden, antes de continuar con las otras instrucciones en la `f`;
- Cuando dentro de la función aparece una variable, entonces:
  - Si la variable es un argumento *formal*, entonces es *local* a la función;
  - Si la variable siempre está en el lado *derecho* de una asignación, entonces es *global* y tendrá que ser asignada *antes* de llamar a la función;
  - Si la variable siempre está en el lado *izquierdo* de una asignación, la variable es *local* a la función y se desconoce afuera;
  - Si la variable esta declarada como variable global mediante la palabra reservada `global`, entonces será global.
- Cuando los identficadores de los parámetros mudos (formales) en la definición de la función coinciden con los nombres de otras variables fuera de la funcion, o cuando aparecen nuevas variables en la defnición de la función con los mismos nombres que otras defnidas fuera de ella, el seguimiento se complicada y puede confundir.

5.13. Estructuras de control

5.13.1. Una estructura `if-elif-else`

Cuando hay una única estructura `if-elif-else`, se hace la primera pregunta, si da *True* entonces se hace algo y se ignoran todas las subsiguientes preguntas, sino se hace la siguiente pregunta y si da *True*, entonces se hace algo y se ignoran todas las subsiguientess preguntas, y así hasta acabar, e.g.

```
# Receta basica:
# 1) En idle3 open this file.
# 2) Run Module (F5) of this file.
# 3) Eventualmente en la ventana interactiva ejecutar comandos.
def si_detecta_tramposillo (pibe,b1,b2,b3):
    """ Pibe invita salir a tres chicas """
    print ("--------------------------------------------------")
    if   (b1 and not b2 and not b3):     # solo Betina dice si
        print (pibe, "sale unicamente con Betina")
    elif (b2 and not b3 and not b1):     # solo Kika   dice si
        print (pibe, "sale unicamente con Kika")
    elif (b3 and not b1 and not b2):     # solo Julia  dice si
        print (pibe, "sale unicamente con Julia")
    elif (not b1 and not b2 and not b3): # nadie le dio bolilla
        print (pibe, "se queda a ver la repeticion de Bolivia-Argentina")
    else:
        print ("ATENCION:", pibe, "esta saliendo con MAS DE UNA PIBA!!")
    return
# test
if __name__ == '__main__':  # para evitar llamadas circulares
    si_detecta_tramposillo ("Pancho",True,False,False)
    si_detecta_tramposillo ("Pancho",False,True,False)
    si_detecta_tramposillo ("Pancho",False,False,True)
    si_detecta_tramposillo ("Pancho",True,True,False)
    si_detecta_tramposillo ("Pancho",False,True,True)
    si_detecta_tramposillo ("Pancho",True,True,True)
    si_detecta_tramposillo ("Pancho",False,False,False)
"""
>>> ================================ RESTART ================================
--------------------------------------------------
Pancho sale unicamente con Betina
--------------------------------------------------
Pancho sale unicamente con Kika
--------------------------------------------------
Pancho sale unicamente con Julia
--------------------------------------------------
ATENCION: Pancho esta saliendo con MAS DE UNA PIBA!!
--------------------------------------------------
ATENCION: Pancho esta saliendo con MAS DE UNA PIBA!!
--------------------------------------------------
ATENCION: Pancho esta saliendo con MAS DE UNA PIBA!!
--------------------------------------------------
Pancho se queda a ver la repeticion de Bolivia-Argentina
>>>
"""
#end
```

5.13.2. Varias estructuras `if-elif-else`

Cuando hay varias estructuras `if-elif-else`, una detrás de la otra, se repite el procediemiento anterior en **cada una** de las estructuras, e.g.

```
# Receta basica:
# 1) En idle3 open this file.
# 2) Run Module (F5) of this file.
# 3) Eventualmente en la ventana interactiva ejecutar comandos.
def no_detecta_tramposillo (pibe,b1,b2,b3):
    """ Pibe invita salir a tres chicas """
    print ("----------------------------------------------")
    if (b1==True): # Betina dice si
        print (pibe, "sale con Betina")
    if (b2==True): # Kika  dice si
        print (pibe, "sale con Kika")
    if (b3==True): # Julia dice si
        print (pibe, "sale con Julia")
    if not (b1 or b2 or b3):
        print (pibe, "se queda a ver la repeticion de Bolivia-Argentina")
    return
# test
if __name__ == '__main__':  # para evitar llamadas circulares
    no_detecta_tramposillo ("Fido",True,True,False)
    no_detecta_tramposillo ("Fido",False,True,True)
    no_detecta_tramposillo ("Fido",True,True,True)
    no_detecta_tramposillo ("Fido",True,False,False)
    no_detecta_tramposillo ("Fido",False,True,False)
    no_detecta_tramposillo ("Fido",False,False,True)
    no_detecta_tramposillo ("Fido",False,False,False)
"""
>>> ============================== RESTART ==============================
----------------------------------------------
Fido sale con Betina
Fido sale con Kika
----------------------------------------------
Fido sale con Kika
Fido sale con Julia
----------------------------------------------
Fido sale con Betina
Fido sale con Kika
Fido sale con Julia
----------------------------------------------
Fido sale con Betina
----------------------------------------------
Fido sale con Kika
----------------------------------------------
Fido sale con Julia
----------------------------------------------
Fido se queda a ver la repeticion de Bolivia-Argentina
"""
#end
```

CAPÍTULO 6

Números enteros

Contents

6.1. División de enteros

Definición. Divisor (def.): sean los enteros n, d, donde $d \neq 0$. Se dice que d divide a n si existe un entero q tal que $n = dq$, donde q es el cociente y d es el divisor. Cuando d divide a n, también se dice que d es un factor (o un divisor) de n, o que n es un múltiplo de d. **Notación**: cuando el entero $d \neq 0$ divide al entero n, se denota con $d|n$, y equivale a $\exists q\ (n = q \cdot d)$, para todo entero $d \neq 0$, donde $d, q \in \mathbb{Z}$.

Ejemplo. $3|12$ pues $12/3 = 4$, mientras que $4 \nmid 11$ pues $11/4 = 2.75$.

Lema. Sean los enteros positivos n, y d. Si $n|d$ y n, d, entonces $d \leq n$. *Demostración*: Si $n|d$ entonces, por definición de divisor, existe un entero q tal que $n = dq$. Como por hipótesis n, d son enteros positivos, entonces

$$\begin{aligned} q &\geq 1 && \text{multiplicando por } d \\ n = dq &\geq d && \text{es decir } d \leq n \end{aligned} \tag{6.1}$$

Definición. Cociente-residuo. Existen enteros únicos q (cociente) y r (residuo) que satisfacen $n = dq + r$, con $0 \leq r < d$, donde $r = 0$ sólo si $d|n$,

Teorema. Sean los enteros positivos a, b, y c cualesquiera. Se tiene:

$$\begin{aligned} &\text{Si } a|b, \text{ y } a|c, \text{ entonces } a|(b+c); \\ &\text{Si } a|b, \text{ entonces } a|(b\cdot c)\ ; \\ &\text{Si } a|b, \text{ y } b|c, \text{ entonces } a|c; \end{aligned} \tag{6.2}$$

Demostración:

i) Suponga que $a|b$ y que $a|c$. Entonces, por definición del divisor, se tiene:

$$\begin{aligned} b &= p \cdot a \\ c &= q \cdot a \\ b + c &= (p+q)a = ka \end{aligned} \tag{6.3}$$

ii) Suponga que $a|b$, entonces, por definición del divisor, se tiene que

$$\begin{aligned} b &= k \cdot a && \text{para algún entero } k \\ cb &= (c \cdot k)a && \\ cb &= \tilde{k}a && \text{donde } \tilde{k} = c \cdot a \text{ es otro entero} \end{aligned} \tag{6.4}$$

iii) Pendiente ...

Corolario. si a, b, c son enteros tales que $a|b$ y $a|c$, entonces se cumple $a|(mb + nc)$, para todos los enteros m, n. *Demostración*:

i) Si $a|b$, entonces $a|(b \cdot c)$ (de la parte 2 del teorema anterior), se tiene que $a|mb$ y $a|nc$, para todos los enteros m, n;
ii) Si $a|b$, y $a|c$, entonces $a|(b + c)$ (de la parte 1 del teorema anterior), se tiene que $a|(mb + nc)$.

Definición. Número primo (def.): un entero positivo p mayor a 1 es primo cuando sus únicos divisores positivos son 1 y p. **Número compuesto**: un entero mayor a 1 es compuesto cuando no es primo.

Observación. Si un entero positivo $n > 1$ es compuesto, entonces tiene divisor positivo d diferente de 1 y de sí mismo: (i) Como d es positivo y $d \neq 1$, debe ser $d \geq 2$; (ii) como d es un divisor de n y $d \neq n$, debe ser $d < n$. En definitiva para chequear si un entero positivo n es compuesto, hay que revisar si alguno de los enteros $2 \leq d < n$, es decir 2, 3, ..., $n - 1$ divide a n. Si no hay un entero en esa lista que divida a n, entonces n es primo. Pero, en realidad, la lista de enteros a revisar es más reducida, según el siguiente teorema.

Teorema. Un entero positivo n mayor a 1 es compuesto, *si y solo si* n tiene un divisor d tal que $2 \leq d \leq \sqrt{n}$.

i) Si (n es un entero compuesto), entonces (n tiene un divisor d tal que $2 \leq d \leq \sqrt{n}$). *Demostración*. Suponga que n es un entero compuesto, entonces, n tiene un divisor d' tal que $2 \leq d' < n$. Hay dos casos:

- Caso en que $d' \leq \sqrt{n}$. Si así fuera, n tiene un divisor d que satisface $2 \leq d \leq \sqrt{n}$ (e igual a d');
- Caso en que $d' > \sqrt{n}$. Si así fuera, como d' divide a n, debe existir un entero q tal que $n = qd'$, por lo cual q también es un divisor de n. Usaremos contradicción para concluir que $q \leq \sqrt{n}$. Suponga que, de contrera, fuera $q > \sqrt{n}$ (hay un error tipográfico en el texto de Johnsonbaugh). Entonces

$$\begin{aligned} d' &> \sqrt{n} \\ q &> \sqrt{n} \\ n = d'q &> \sqrt{n}\sqrt{n} \end{aligned} \tag{6.5}$$

en donde se obtiene la contradicción $n > n$. Por eso, debe ser $q \leq \sqrt{n}$.

Por eso, si n es un entero compuesto, entonces n tiene el divisor $d = q$ que satisface $2 \leq d \leq \sqrt{n}$.

ii) Si (n tiene un divisor d tal que $2 \leq d \leq \sqrt{n}$), entonces (n es un entero compuesto). *Demostración*. Si n tiene un divisor d tal que $2 \leq d \leq \sqrt{n}$, entonces, por la defininción de entero compuesto, n es compuesto.

Ejemplo. Algoritmo de la criba de Eratóstenes para determinar si un entero positivo n es primo o compuesto.

```python
import math
def es_primo (n):
    """ Devuelve True si el entero n es primo sino False. """
    # caso n < 2
    if (n < 2): # no es primo
        return False
    else:
        r = int (math.floor (math.sqrt (n)))
        for d in range (2,r+1):
            h = n %d
            if (h == 0):
                return False
        return True
```

Enunciado. Teorema fundamental de la aritmética: todo entero n mayor a 1 se puede expresar como el producto de primos. Si los primos se escriben en orden no decreciente, la factorización es única. En símbolos si $n = p_1 p_2 ... p_i$, donde todos son primos tales que $p_1 \leq p_2 \leq ... \leq p_i$, y si $n = p'_1 p'_2 ... p'_j$, donde todos son primos tales que $p'_1 \leq p'_2 \leq ... \leq p'_z$, entonces $i = j = z$, y $p_k = p'_k$, para $k = 1, 2, ..., z$.

Enunciado. El número de primos es infinito.

6.2. Máximo común divisor y mínimo común múltiplo

6.2.1. Máximo común divisor

Definición. Máximo común divisor (def.). Sean los enteros positivos α y β. Un divisor común de α y de β es un entero k que divide tanto a α como a β. El Máximo Común

Divisor (MCD) de α y β es el divisor común positivo más grande. **Notación**: el MCD de los enteros positivos α y β se denota con mcd(α,β).

Ejemplo. Calcular el mcd (30,105).

Solución. Primero usamos la definición:

$$\begin{aligned}\text{divisores\_positivos }(30) &= \{1,2,3,5,6,10,15,30\}\\ \text{divisores\_positivos }(105) &= \{1,3,5,5,7,15,21,35,105\}\\ \text{divisores\_comunes }(30{,}105) &= \{1,3,5,15\}\\ \text{mcd }(30{,}105) &= \max(\text{divisores\_comunes }(30{,}105)) = 15\end{aligned} \tag{6.6}$$

Por otra parte, notar que

$$\begin{aligned}\text{factorizacion\_factores\_primos }(30) &= 2\cdot 3\cdot 5 = 2\cdot 3\cdot 5\cdot 7^0\\ \text{factorizacion\_factores\_primos }(105) &= 3\cdot 5\cdot 7 = 2^0\cdot 3\cdot 5\cdot 7\\ \text{mcd }(30{,}105) &= 2^0\cdot 3\cdot 5\cdot 7^0 = 15\end{aligned} \tag{6.7}$$

Este segundo cómputo es un resultado general y que descripto por el enunciado del siguiente teorema:

Enunciado. Sean dos enteros α y β mayores a 1 con factorizaciones primas

$$\begin{aligned}\alpha &= p_1^{a_1}p_2^{a_2}...p_h^{a_h}\\ \beta &= p_1^{b_1}p_2^{b_2}...p_h^{b_h}\end{aligned} \tag{6.8}$$

en donde si el primo p_i no es factor del entero α, entonces se hace $a_i = 0$, y del mismo modo para β, mientras que h es el número total de primos juntando las factorizaciones en primos de α y de β. Entonces se cumple que

$$\text{mcd}(\alpha,\beta) = p_1^{\text{mín}\,(a_1,b_1)}p_2^{\text{mín}\,(a_2,b_2)}...p_h^{\text{mín}\,(a_h,b_h)} \tag{6.9}$$

Ejemplo. Calcular el mcd (82 320,950 796).

Solución: usando el teorema

$$\begin{aligned}\text{factorizacion\_factores\_primos }(82\,320) &= 2^4\cdot 3^1\cdot 5^1\cdot 7^3\cdot 11^0\\ \text{factorizacion\_factores\_primos }(950\,796) &= 2^2\cdot 3^2\cdot 5^0\cdot 7^4\cdot 11^1\\ \text{mcd }(82\,320{,}950\,796) &= 2^2\cdot 3^1\cdot 5^0\cdot 7^3\cdot 11^0 = 4116\end{aligned} \tag{6.10}$$

6.2.2. Mínimo común múltiplo

Definición. Mínimo común múltiplo (def.). Sean los enteros positivos α y β. Un múltiplo común de α y de β es un entero k que es divisible tanto por α como por β. El Mínimo Común Múltiplo (MCM) de α y n es el divisor común positivo más pequeño. **Notación**: el MCM de los enteros positivos α y β se denota con mcm(α,β).

Ejemplo. Calcular el mcm (30,105).

Solución: primero usamos la definición

- El 105 es divisible por 105 pero no por 30;
- El que le sigue es 210 que sí es divisible tanto por 105 como por 30;
- Como 210 es el divisible común a 105 y 30 más chico, entonces mcm (30,105) = 210.

Otra vez, podemos hacer

$$\begin{aligned} \text{factorizacion\_factores\_primos}\ (30) &= 2 \cdot 3 \cdot 5 = 2 \cdot 3 \cdot 5 \cdot 7^0 \\ \text{factorizacion\_factores\_primos}\ (105) &= 3 \cdot 5 \cdot 7 = 2^0 \cdot 3 \cdot 5 \cdot 7 \\ \text{mcm}\ (30{,}105) &= 2^1 \cdot 3 \cdot 5 \cdot 7^1 = 210 \end{aligned} \tag{6.11}$$

Notar que la factorización prima de mcm (30,105) debe contener a los factores 2, 3, 5 para que de ese modo 30 pueda dividir a mcm (30,105). Del mismo modo, la factorización prima de mcm (30,105) también debe contener a los factores 3, 5, 7 para que de ese modo 105 pueda dividir a mcm (30,105). Este segundo cómputo es un resultado general y que descripto por el enunciado del siguiente teorema:

Enunciado. Sean dos enteros α y β mayores a 1 con factorizaciones primas

$$\begin{aligned} \alpha &= p_1^{a_1} p_2^{a_2} ... p_h^{a_h} \\ \beta &= p_1^{b_1} p_2^{b_2} ... p_h^{b_h} \end{aligned} \tag{6.12}$$

en donde si el primo p_i no es factor del entero α, entonces se hace $a_i = 0$, y del mismo modo para β, mientras que h es el número total de primos juntando las factorizaciones en primos de α y de β. Entonces se cumple que

$$\text{mcm}(\alpha, \beta) = p_1^{\text{máx}\,(a_1, b_1)} p_2^{\text{máx}\,(a_2, b_2)} ... p_h^{\text{máx}\,(a_h, b_h)} \tag{6.13}$$

Ejemplo. Calcular el mcd (82 320,950 796).

Solución: usando el teorema

$$\begin{aligned} \text{factorizacion\_factores\_primos}\ (82\,320) &= 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^3 \cdot 11^0 \\ \text{factorizacion\_factores\_primos}\ (950\,796) &= 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^4 \cdot 11^1 \\ \text{mcd}\ (82\,320{,}950\,796) &= 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^4 \cdot 11^1 = 19\,015\,920 \end{aligned} \tag{6.14}$$

Ejemplo. Calcular el producto mcd (30,105) · mcd (30,105).

Solución:

$$\begin{aligned} \text{mcd}\ (30{,}105) &= 15 \\ \text{mcm}\ (30{,}105) &= 210 \\ \text{mcd}\ (30{,}105) \cdot \text{mcm}\ (30{,}105) &= 15 \cdot 210 = 3150 = 30 \cdot 105 \end{aligned} \tag{6.15}$$

Este segundo cómputo es un resultado general y que descripto por el siguiente teorema:

Teorema. Para todos los enteros positivos α y β se tiene que

$$\text{mcd}(\alpha, \beta) \cdot \text{mcm}(\alpha, \beta) = \alpha \cdot \beta \tag{6.16}$$

Demostración:

i) Si $\alpha = 1$, entonces $\text{mcd}(1,\beta) = 1$, y $\text{mcm}(1,\beta) = \beta$, entonces $\text{mcd}(\alpha,\beta)\cdot\text{mcm}(\alpha,\beta) = 1\cdot\beta = \alpha\cdot\beta$;
ii) Si $\beta = 1$, entonces $\text{mcd}(\alpha,1) = \alpha$, y $\text{mcm}(\alpha,1) = 1$, entonces $\text{mcd}(\alpha,\beta)\cdot\text{mcm}(\alpha,\beta) = \alpha\cdot 1 = \alpha\cdot\beta$;
iii) Por (i-ii) sólo basta analizar el caso $\alpha > 1$ y $\beta > 1$. Para eso, usando las Ecs. (6.9-6.13), y teniendo en cuenta que

$$\text{mín}(x,y) + \text{máx}(x,y) = x + y \tag{6.17}$$

se tiene que

$$\begin{aligned}\text{mcd}(\alpha,\beta)\cdot\text{mcm}(\alpha,\beta) &= \left[p_1^{\text{mín}\,(a_1,b_1)}p_2^{\text{mín}\,(a_2,b_2)}...p_h^{\text{mín}\,(a_h,b_h)}\right]\cdot\\ &\times\left[p_1^{\text{máx}\,(a_1,b_1)}p_2^{\text{máx}\,(a_2,b_2)}...p_h^{\text{máx}\,(a_h,b_h)}\right]\\ &= \left[p_1^{a_1}p_2^{a_2}...p_h^{a_h}\right]\cdot\left[p_1^{b_1}p_2^{b_2}...p_h^{b_h}\right] = \alpha\cdot\beta\end{aligned} \tag{6.18}$$

Observación. Si se tiene un algoritmo eficiente para hallar $\text{mcd}(\alpha,\beta)$, entonces se usa la Ec. (6.16) para hallar el $\text{mcm}(\alpha,\beta)$.

6.2.3. Teorema de Euclides y algoritmo de Euclides

Intro. El **algoritmo de Euclides** permite calcular rápidamente el **máximo común divisor** de dos enteros m y n, y se basa en que

$$\text{mcd}\,(a,b) = \text{mcd}\,(b,r) \qquad \text{donde } r = a \bmod b \tag{6.19}$$

Ejemplo. Calcular el mcd (30,105).

Solución: para usar reiteradamente la Ec. (6.19), primero hacemos mcd (30,105) = mcd (105,30).

$$\begin{aligned}&\text{mcd (105,30) = mcd (30,15), pues 105 mod 30 = 15}\\ &\text{mcd (30,15) = mcd (15,0) , pues 30 mod 15 = 0}\\ &\text{mcd (15,0) = 15, pues 15 es el mayor entero que divide a 15 y a 0}\end{aligned} \tag{6.20}$$

Teorema. Sean a un entero no negativo, b un entero positivo, y $r = a \bmod b$, entonces $\text{mcd}\,(a,b) = \text{mcd}\,(b,r)$. *Demostración*:

- Por el teorema cociente-residuo, existen enteros q y r que satisfacen $a = bq+r$, donde $0 \le r < b$.
- Sea un entero c un divisor común de a y b. Por teorema auxiliar, si $c|b$, entonces $c|bq$;
- Por teorema auxiliar, si $c|a$ y $c|bq$, entonces $c|a-bq$, es decir, $c|r$;
- Si $c|b$ y $c|r$, entonces c es un divisor común de b y de r;
- Recíprocamente, si c es un divisor común de b y de r, entonces $c|b$ y $c|r$, por lo que $c|bq$ y $c|bq+r$, o sea $c|a$;
- Por eso, c es un divisor común de a y de b;
- Luego, el conjunto de divisores comunes de a y de b es igual al conjunto de divisores comunes de b y de r, por ende $\text{mcd}\,(a,b) = \text{mcd}\,(b,r)$.

6.2.4. Algoritmo de Euclides

Se incluyen dos versiones del algoritmo de Euclides: una secuencial y otra recursiva. Una versión secuencial está dada por

```python
def mcd_s (a,b): # maximo comun divisor
    """
    Maximo Comun Divisor de los enteros a y b, version secuencial.
    """
    # nos ponemos en el caso donde ambos son no negativos
    a = abs (a)
    b = abs (b)
    k = 0                   # inicia contadora
    # lazo principal
    while (b != 0):
        r = a % b           # resto
        a = b               # nuevo "a" para el procimo ciclo
        b = r               # nuevo "b" para el procimo ciclo
        k = k + 1           # incrementa contadora
    # aqui b == 0
    return (a,k)
```

mientras que una versión recursiva es la siguiente

```python
def mcd_r (a,b): # maximo comun divisor
    """
    Maximo Comun Divisor de los enteros a y b, version recursiva.
    """
    if   (a > b): # paso recursivo
       z = mcd_r (a-b, b)
    elif (b > a): # paso recursivo
       z = mcd_r (b-a, a)
    else:         # paso base
       z = a
    return z
```

6.2.5. Sucesión de Fibonacci

La sucesión de Fibonacci $\{f_n\}$ está definida por

$$f_n = \begin{cases} \mathrm{f}_{n-1} + f_{n-2} & \text{si } n \geq 3; \\ 1 & \text{si } n = 1 \text{ o } n = 2; \end{cases} \tag{6.21}$$

Sus primeros términos son $\{1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...\}$.

6.2.6. Análisis del algoritmo de Euclides

Teorema. Suponga los enteros a, b requieren n operaciones módulo cuando se introducen en el algoritmo de Euclides, con $a > b$, y con $n \geq 1$. Entonces $a \geq f_{n+2}$ y $b \geq f_{n+1}$, donde $\{f_n\}$ es la sucesión de Fibonacci. *Demostración* (por inducción):

- PB ($n = 1$): cuando $a = 2$ y $b = 1$, es $n = 1$. Por otra parte $f_3 = 2$ y $f_2 = 1$, y se verifica el PB;
- Suponga que el par a, b, con $a > b$, requieran $n + 1$ operaciones módulo en el AE;

- Primero se calcula $r = a \bmod b$, es decir $a = bq + r$, con $0 \leq r < b$;
- Luego se repite usando b y r, con $b > r$.
- Cuando se hicieron n operaciones módulo, usamos la HI para obtener $b \geq f_{n+2}$ y $r \geq f_{n+1}$.
- En $a = bq + r$, dado que $q > 0$ cuando $a > b$, reemplazamos

$$a = bq + r \geq b + r \geq f_{n+2} + f_{n+1} = f_{n+3} \tag{6.22}$$

es decir, $a \geq f_{n+3}$ y $b \geq f_{n+2}$.

Teorema. Sean los enteros $a \geq m$ y $b \geq m$, con $m \geq 8$. Cuando a, b se los introduce en el AE se cumple que el número n de operaciones módulo verifica $n < \log_{3/2}(m/(3/2))$. Suponga que $a > b$. *Demostración*:

- Sean los enteros a y b que requieren como máximo n operaciones módulo cuando se introducen en el algoritmo de Euclides;
- Como $a > b$ se puede emplear el teorema anterior, i.e. se cumple que $f_{n+2} \leq a$. Como además $a \leq m$, se tiene que $f_{n+2} \leq m$;
- Se puede demostrar que $(3/2)^{n+1} < f_{n+2}$ para $n \geq 4$;
- Combinando vemos que $(3/2)^{n+1} < f_{n+2} \leq m$, o sea, $(3/2)^{n+1} < m$;
- Tomando logaritmos en base 3/2 queda

$$\begin{aligned} (n+1)\log_{3/2}(3/2) &< \log_{3/2} m \\ n+1 &< \log_{3/2} m \\ n &< \log_{3/2} m - 1 \\ n &< \log_{3/2} m - \log_{3/2}(3/2) \\ n &< \log_{3/2} \frac{m}{3/2} \end{aligned} \tag{6.23}$$

6.3. Representaciones de enteros

Intro. Es usual usar notación decimal para representar números enteros, e.g. 987 significa $9 \cdot 10^2 + 8 \cdot 10^1 + 7 \cdot 10^0$. No obstante, a veces, conviene usar una base distinta de la decimal, en particular: binario (base 2), octal (base 8), hexadecimal (base 16). De hecho se puede usar cualquier base $B > 0$, dando lugar al enunciado del siguiente teorema.

Enunciado. Expresión de un entero positivo en una base B positiva: sea un entero positivo B mayor a 1. Si n es un entero positivo, entonces se lo puede expresar como

$$n = a_k B^k + a_{k-1} B^{k-1} + \dots + a_1 B^1 + a_0 \tag{6.24}$$

de una única forma, donde k es un entero no negativo, $a_0, a_1, \dots, a_k$ son enteros no negativos menores a B, y $a_k \neq 0$.

Definición. Expresión binaria (def.): cuando se elige base $B = 2$, con lo cual bastan 2 símbolos, cada símbolo es 0 o 1. En consecuencia la expresión binaria de un entero es una cadena de bits.

Ejemplo. Obtener la expresión decimal del binario $z = (1\ 0101\ 1101)_2$.

Solución:

$$z = 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = (349)_{10} \quad (6.25)$$

Definición. Expresión hexadecimal (def.): cuando se elige base $B = 16$, con lo cual hacen falta 16 símbolos. Normalmente se emplean 0-9 y A-F, e.g. ver Tabla 6.1.

decimal	binario	hexadecimal
1	00001	1
2	00010	2
3	00011	3
4	00100	4
5	01001	5
6	01010	6
7	01011	7
8	01000	8
9	01001	9
10	01010	A
11	01011	B
12	01100	C
13	01101	D
14	01110	E
15	01111	F
16	10000	10

Tabla 6.1: Enteros desde 1 hasta 16 en base decimal, binaria, y hexadecimal..

Ejemplo. Obtener la expresión decimal del hexadecimal $z = (2AE0B)_{16}$.

Solución:

$$\begin{aligned} z &= 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^0 + 11 \cdot 16^0 \\ &= (175\ 627)_{10} \end{aligned} \quad (6.26)$$

Ejemplo. Obtener la expresión decimal del hexadecimal $z_1 = (21)_{16}$, y $z_2 = (30)_{16}$.

Solución:

$$\begin{aligned} z_1 &= 2 \cdot 16^1 + 1 \cdot 16^0 = (33)_{10} \\ z_2 &= 3 \cdot 16^1 + 0 \cdot 16^0 = (48)_{10} \end{aligned} \quad (6.27)$$

Observación. cada digito hexadecimal puede expresarse usando 4 bits lo cual, con experiencia, facilita las conversiones.

Ejemplo. Como $(1110)_2 = (14)_{10} = (E)_{16}$, y como $(0101)_2 = (05)_{10} = (5)_{16}$, se tiene que $(1110\ 0101)_2 = (E5)_{16}$.

Definición. Byte, palabra, octeto (def.): son cadenas de bits de longitud 8. Notar que un byte se puede representar usando 2 números hexadecimales.

6.3.1. Cambios de base

Lo haremos con ejemplos.

Ejemplo. Calcular $z = (12\,345)_{10}$ en octal.

Solución:

$$\begin{aligned}
12\,345 &= 8 \cdot 1\,543 + 1 & (1)\\
1\,543 &= 8 \cdot 192 + 7 & (7)\\
192 &= 8 \cdot 24 + 0 & (0)\\
24 &= 8 \cdot 3 + 0 & (0)\\
3 &= 8 \cdot 0 \text{ (end)} + 3 & (3)\\
(12\,345)_{10} &= (30\,071)_8
\end{aligned} \tag{6.28}$$

Ejemplo. Calcular $z = (177\,130)_{10}$ en hexadecimal.

Solución:

$$\begin{aligned}
177\,130 &= 16 \cdot 11\,070 + 10 & (A)\\
11\,070 &= 16 \cdot 691 + 14 & (E)\\
691 &= 16 \cdot 43 + 3 & (3)\\
43 &= 16 \cdot 2 + 11 & (B)\\
2 &= 16 \cdot 0 \text{ (end)} + 2 & (2)\\
(177\,130)_{10} &= (2B3EA)_{16}
\end{aligned} \tag{6.29}$$

Ejemplo. Calcular $z = (241)_{10}$ en binario.

Solución:

$$\begin{aligned}
241 &= 2 \cdot 120 + 1\\
120 &= 2 \cdot 60 + 0\\
60 &= 2 \cdot 30 + 0\\
30 &= 2 \cdot 15 + 0\\
15 &= 2 \cdot 7 + 1\\
7 &= 2 \cdot 3 + 1\\
3 &= 2 \cdot 1 + 1\\
1 &= 2 \cdot 0 \text{ (end)} + 1\\
(241)_{10} &= (1111\,0001)_2
\end{aligned} \tag{6.30}$$

6.3.2. Ejercicios con enteros

Ejemplo. (ex-GTP de la FIQ, intermedio) Sea T_n la mayor potencia de 2 que divide al entero positivo n. Demuestre que

$$T_{mn} = T_m + T_n \qquad \text{para todos los enteros positivos } m, n \tag{6.31}$$

Solución:

- PB ($m = n = 1$): en el lado izquierdo $I_1 = T_{1\cdot 1} = T_1$, mientras que en el lado derecho $D_1 = T_1 + T_1$. Como $2^0 = 1$ es la mayor potencia de 2 que divide a $n = 1$, se tiene que $T_1 = 0$, por lo que se cumple la igualdad $I_1 = D_1 = 0$.

- PI (Zarza, LMA, 2008):

$$n = \begin{cases} \text{par} & n = 2^k p, \text{ con algún entero } k > 0; \\ \text{impar} & n = 2^0 p; \end{cases} \tag{6.32}$$

donde p es entero impar. Ahora

$$\begin{aligned} \text{sea } m = 2^k p &\quad \text{entonces } T_m = k; \\ \text{sea } n = 2^h q &\quad \text{entonces } T_n = h; \end{aligned} \tag{6.33}$$

Calculando el producto de m y n se tiene

$$m \cdot n = 2^{k+h} \tilde{p} \tag{6.34}$$

donde $\tilde{p} = p \cdot q$. Como p y q son impares, entonces su producto $\tilde{p}$ también lo es, por lo que

$$T_{m \cdot n} = k + h \tag{6.35}$$

Comparando las Ecs. (6.33-6.35) se concluye que se cumple la Ec. (6.31) para todos los enteros positivos m, n.

Ejemplo. (ex-GTP de la FIQ, avanzado) Sea T_n la mayor potencia de 2 que divide al entero positivo n, y sea S_n el número de unos en la representación binaria de n. Sabiendo que $T_{mn} = T_m + T_n$ para todos los enteros positivos m, n, demuestre que

$$T_{n!} = n - S_n \qquad \text{para todo entero positivo } n \tag{6.36}$$

Solución:

- De la Tabla 6.2 se observa que

$$T_n = \begin{cases} 0 & \text{cuando } n = 2k + 1 \text{ (impar);} \\ j & \text{cuando } n = 2k \text{ (par) con } j \text{ unos;} \end{cases} \tag{6.37}$$

- De la Tabla 6.2 se también se observa que, por ejemplo,

$$T_{16} = T_{8 \cdot 2} = T_8 + T_2 = 3 + 1 = 4 \tag{6.38}$$

- PB ($n = 1$):

$$\begin{aligned} I_1 &= T_{1!} = T_1 = 0 & D_1 &= 1 - S_1 = 1 - 1 = 0 \\ I_3 &= T_{3!} = T_6 = 1 & D_6 &= 3 - S_6 = 3 - 2 = 1 \\ I_4 &= T_{4!} = T_{24} = 3 & D_4 &= 4 - S_4 = 4 - 1 = 3 \end{aligned} \tag{6.39}$$

En la primera línea de la Ec. (6.39) se cumple la igualdad $I_1 = D_1 = 0$, por lo que se verifica el PB.
- Cuenta auxiliar

- Sea n par:

$$\begin{array}{rll} & n = 101...1...00000000 & \text{hay } j \text{ ceros} \\ + & & \\ & 1 = 000...0...00000001 & \\ \hline & n+1 = 101...1...00000001 & \text{nuevo } 1 \end{array}$$

Entonces $S_{n+1} = S_n + 1$ y $T_{n+1} = 0$ cuando n es par;

- Sea n impar:

$$\begin{array}{rll} & n = 101...1...01111111 & \text{hay } j \text{ unos} \\ + & & \\ & 1 = 000...0...00000001 & \\ \hline & n+1 = 101...1...10000000 & \text{nuevo } 1 \text{ y } j \text{ ceros} \end{array}$$

Entonces $S_{n+1} = S_n - j + 1$ y $T_{n+1} = j$ cuando n es impar;

- PI: asumimos que la HI dada por la Ec. (6.36) es T para algún entero $n \geq 1$ arbitrario pero fijo, y planteamos:

$$\begin{aligned} I_{n+1} &= T_{(n+1)!} && ; \\ &= T_{(n+1)n!} && ; \text{por definición del factorial} \\ &= T_{n+1} + T_{n!} && ; \text{por Ec. (6.31)} \\ &= T_{n+1} + (n - S_n) && ; \text{introducimos la HI} \end{aligned} \tag{6.40}$$

Usando resultados de la cuenta auxiliar

$$\begin{aligned} S_n = S_{n+1} - 1 \text{ y } T_{n+1} = 0 \quad & \text{si } n = 2k \text{ (par)}; \\ S_n = S_{n+1} + j - 1 \text{ y } T_{n+1} = j \quad & \text{si } n = 2k+1 \text{ (impar)}; \end{aligned} \tag{6.41}$$

es decir,

$$T_{n+1} + n - S_n = \begin{cases} 0 + n - S_{n+1} + 1 = (n+1) - S_{n+1} & \text{si } n = 2k \text{ (par)}; \\ j + n - S_{n+1} - j + 1 = (n+1) - S_{n+1} & \text{si } n = 2k+1 \text{ (impar)}; \end{cases} \tag{6.42}$$

por lo que $I_{n+1} = D_{n+1}$, y se cumple el PI.

6.4. Sucesiones y sumatorias

Definición. (Sec. 3.2, p. 210, Rosen):

1) Una sucesión $S = S(n)$ es una función cuyo dominio es algún subconjunto $\mathbb{Z}_a^b$ de los enteros $\mathbb{Z}$, donde n es el índice entero de la sucesión tal que $a \leq n \leq b$;
2) Notación: $S = \{s_n\}$ denota la sucesión, donde s_n es enésimo término de la sucesión;
3) Sucesión infinita: cuando el dominio es infinito. Sucesión finita: cuando el dominio es finito;

4) Sucesión creciente: cuando $a_{n+1} > a_n$ para todo n;
5) Sucesión decreciente: cuando $a_{n+1} < a_n$ para todo n;
6) Sucesión no decreciente: cuando $a_{n+1} \geq a_n$ para todo n;
7) Sucesión no creciente: cuando $a_{n+1} \leq a_n$ para todo n.

Definición.

1) Sumatoria: $\sum_{i=m}^{n} a_i = a_m + a_{m+1} + ... + a_m$;
2) Productoria: $\prod_{i=m}^{n} a_i = a_m a_{m+1} ... a_m$.

Ejemplo. Cambio de índice y de límites en una sumatoria. En $A = \sum_{i=0}^{n} i r^{n-i}$ introducir el cambio de índice $i = j-1$. Solución: como $i = j-1$, se tiene que, cuando $i = 0$ es $j = 1$, y cuando $i = n$ es $j = n+1$. Por otra parte $n - i = n - j + 1$. Finalmente, reemplazando, se tiene $A = \sum_{j=1}^{n+1} (j-1) r^{n-j+1}$.

Definición.

1) Una cadena α sobre un conjunto finito X es una sucesión ordenada de elementos de X. Nota: frecuentemente X es el conjunto de los caracteres alfa numéricos;
2) Cadena nula: es la cadena sin elementos y suele simbolizarse con λ;
3) Subcadena β de una cadena α: se obtiene eligiendo alguno o todos los elementos *consecutivos* de α;
4) Longitud de una cadena α: es igual al número de elementos de α y se denota $|\alpha|$;
5) Concatenación de 2 cadenas: la concatenación de las cadenas α y β se denota con $\alpha\beta$. En general, $\alpha\beta \neq \beta\alpha$;
6) Notación: sea X un conjunto finito, X^* es el conjunto de todas las cadenas posibles de X incluyendo la cadena nula λ.

Ejemplo. Sea $X = \{a, b, c, d\}$, entonces $\alpha = baac$, $\beta = acab$, donde $\alpha \neq \beta$, y con $|\alpha| = 4$.

6.5. Crecimiento de funciones enteras

Comentario. En el análisis de algoritmos hacen falta obtener estimaciones de tiempo de ejecución y espacio en memoria necesarios para resolver una tarea de tamaño n, donde n es, por ejemplo, el número de datos del problema (Sec. 2.2, p. 120, Rosen). Los tiempos de ejecución y el espacio en memoria suelen contemplar el mejor caso, el peor caso, y/o el caso promedio.

Definición. Sean dos funciones $f(n)$ y $g(n)$, ambas con dominio $n \in \mathbb{Z}^+$.

1) *Cota inferior*: se escribe $f(n) = \Omega(g(n))$ y se dice que $f(n)$ es orden omega de $g(n)$, si existe una constante positiva C_1 tal que $C_1|g(n)| \leq |f(n)|$ para todo $n \in Z^+$. Cuando $f(n) = \Omega(g(n))$ también se dice que $g(n)$ es una cota inferior.
2) *Cota superior*: Se escribe $f(n) = O(g(n))$ y se dice que $f(n)$ es orden O mayúscula de $g(n)$, si existe una constante positiva C_2 tal que $|f(n)| \leq C_2|g(n)|$ para todo $n \in Z^+$. Cuando $f(n) = O(g(n))$ también se dice que $g(n)$ es una cota superior.

3) *Cota estrecha*: Se escribe $f(n) = \Theta(g(n))$ y se dice que $f(n)$ es orden tita de $g(n)$ si $f(n) = \Omega(g(n))$ y $f(n) = O(g(n))$, o sea, existen constantes positivas C_1 y C_2 tales que $C_1|g(n)| \leq |f(n)| \leq C_2|g(n)|$ para todo $n \in Z^+$. Cuando $f(n) = \Theta(g(n))$ también se dice que $g(n)$ es una cota estrecha.

Ejemplo. Obtener cotas inferior, superior y estrecha para la función $f(n) = 60n^2 + 5n + 1$ con $n \in Z^+$. Solución:

1) *Cota inferior*: como $f(n) = 60n^2 + 5n + 1 \geq 60n^2$, elegimos $C_1 = 60$ con lo que $f(n) = \Omega(n^2)$.
2) *Cota superior*: $f(n) = 60n^2 + 5n + 1 \leq 60n^2 + 5n^2 + n^2 = 66n^2$, elegimos $C_2 = 66$ con lo que $f(n) = O(n^2)$.
3) *Cota estrecha*: Finalmente, como $f(n) = \Omega(g(n))$ y $f(n) = O(g(n))$, también es $f(n) = \Theta(n^2)$.

Teorema. Sea $p(n) = a_k n^k + a_{k-1}n^{k-1} + ... + a_1 n + a_0$ un polinomio en n de grado k donde cada a_i es no-negativa para $0 \leq i \leq k$. Entonces $p(n) = \Theta(n^k)$. Demostración:

1) Para todo n:
$$p(n) = a_k n^k + a_{k-1}n^{k-1} + ... + a_1 n + a_0 \geq a_k n^k = C_1 n^k \tag{6.43}$$
donde $C_1 = a_k$. Por lo tanto $p(n) = \Omega(n^k)$.
2) Para todo n:
$$\begin{aligned} p(n) &= a_k n^k + a_{k-1}n^{k-1} + ... + a_1 n + a_0 \\ &\leq a_k n^k + a_{k-1}n^k + ... + a_1 n^k + a_0 n^k \\ &= (a_k + a_{k-1} + ... + a_1 + a_0)n^k \\ &= C_2 n^k \end{aligned} \tag{6.44}$$
donde $C_2 = a_k + a_{k-1} + ... + a_1 + a_0$. Por lo tanto $p(n) = O(n^k)$.
3) Finalmente, como $p(n) = \Omega(n^k)$ y $p(n) = O(n^k)$, es $p(n) = \Theta(n^k)$.

Ejemplo. Obtener cotas inferior, superior y estrecha para la función $f(n) = 2n + 3\lg(n)$, donde $n \in Z^+$. Solución:

1) *Cota inferior*: Como $f(n) = 2n + 3\lg(n) \geq 2n$, elegimos $C_1 = 2$ con lo que $f(n) = \Omega(n)$.
2) *Cota superior*: Como $f(n) = 2n + 3\lg(n) < 2n + 3n = 5n$, donde $\lg(n) < n$, elegimos $C_2 = 5$ con lo que $f(n) = O(n)$.
3) *Cota estrecha*: Finalmente, como $f(n) = \Omega(n)$ y $f(n) = O(n)$, también es $f(n) = \Theta(n)$.

Ejemplo. Obtener cotas inferior, superior y estrecha para la suma de Gauss $f(n) = 1 + 2 + ... + n$, donde $n \in Z^+$. Solución:

1) *Cota superior*: Como $f(n) = 1 + 2 + ... + n \leq n + n + ... + n = n \cdot n = n^2$, elegimos $C_2 = 1$ con lo que $f(n) = O(n^2)$.
2) *Cota inferior*: Como $f(n) = 1 + 2 + ... + n \geq 1 + 1 + ... + 1 = n$, primero intentamos elegir $C_1 = 1$, con lo que $f(n) = \Omega(n)$. Pero esta cota inferior no es igual a la superior,

i.e. las funciones $g(n)$ son diferentes: en la primera es n^2 mientras que en la segunda es n, por lo que no puede deducirse una estimación para la cota estrecha Θ. Por esto, buscamos otra cota inferior. Para simplificar lo que sigue, solo consideremos los casos en que n sea un entero **par**.

a] Ejemplo previo: sea $n = 6$ (par), entonces hacemos

$$1 + 2 + 3 + \underbrace{(4 + 5 + 6)}_{\text{tomo la 2da mitad}} \geq \underbrace{4 + 5 + 6}_{\text{los igualo al 1er sumando}} \geq \underbrace{4 + 4 + 4}_{\text{como hay 3 sumandos}} = 3 \cdot 4 \tag{6.45}$$

donde el primer sumando vale $\alpha = n/2 + 1 = 4$, mientras que el número de sumandos es $z = n/2 = 3$, cuando $n = 6$;

b] En general, el valor del primer sumando α y el número de sumandos z de la suma parcial de Gauss valen

$$\begin{aligned} \alpha &= n/2 + 1 \quad &&\text{; porque es el entero siguiente a } n/2 \\ z &= (\text{entero final} - \text{entero inicial} + 1) = n - (n/2 + 1) + 1 = n/2 \end{aligned} \tag{6.46}$$

Teniendo en cuenta la Ec. (6.46) hacemos

$$\begin{aligned} 1 + 2 + \ldots + n &\geq \alpha + (\alpha + 1) + \ldots + n && \text{; dejo la 2da mitad} \\ &\geq \alpha + \alpha + \ldots + \alpha && \text{; la desigualdad no cambia} \\ &= z\alpha && \text{; suma de } z \text{ términos iguales a } \alpha \\ &= \left(\frac{n}{2}\right)\left(\frac{n}{2} + 1\right) \geq \left(\frac{n}{2}\right)\left(\frac{n}{2}\right) = \frac{n^2}{4} \end{aligned} \tag{6.47}$$

De la Ec. (6.47) elegimos $C_1 = 1/4$, con lo que $f(n) = \Omega(n^2)$.

3) *Cota estrecha*: Finalmente, como ahora $f(n) = \Omega(n^2)$ y $f(n) = O(n^2)$, ahora sí se puede concluir que $f(n) = \Theta(n^2)$.

Observación. Un algoritmo iterativo para la suma de Gauss $f(n) = 1 + 2 + \ldots + n$, con entero n positivo, se muestra en la función `suma_gauss(n)`. Nota: el intervalo del `range` usado en el lazo `for` es cerrado a la izquierda y es abierto a la derecha, por eso sumamos uno para que ejecute el entero final n.

```
def suma_gauss(n): # retorna la suma de Gauss para entero n positivo
    suma = 0        # inicializo acumulador de la suma
    for i in range (1,n+1): # cerrado a la izq. y abierto a la derecha
        suma = suma + i      # acumulo el i actual
    return suma              # retorno resultado
```

Observación. La expresión $z = (\text{entero final} - \text{entero inicial} + 1)$ dada en la Ec. (6.46) es la misma que empleamos para saber cuántas veces se ejecuta un ciclo `for i` en el rango de enteros $[i_{\text{inicial}}, i_{\text{final}}]$, mostrado en la función `lazo_for(entero_inicial,entero_final)`.

```
def lazo_for(entero_inicial,entero_final):
    for i in range (entero_inicial,entero_final+1):
        z = alguna_cuenta
    return z
```

n	$(n)_2$	T_n	Z_n
1	1	0	0
2	10	1	1
3	11	0	0
4	100	2	2
5	101	0	0
6	110	1	1
7	111	0	0
8	1000	3	3
9	1001	0	0
10	1010	1	1
11	1011	0	0
12	1100	4	4
13	1101	0	0
14	1110	1	1
15	1111	0	0
16	10000	5	5
17	10001	0	0
18	10010	1	1
19	10011	0	0
20	10100	2	2
21	10101	0	0
22	10110	1	1
23	10111	0	0
24	11000	3	3

Tabla 6.2: Primeros valores de n en base 10, en donde $(n)_2$ es el entero n en base 2, T_n la mayor potencia de 2 que divide a n, y Z_n el número de ceros consecutivos al final de $(n)_2$.

CAPÍTULO 7

Métodos de conteo

Contents

7.1. Principios básicos de conteo

7.1.1. Regla del producto (o principio de la multiplicación)

Definición. Regla del producto (o **principio de la multiplicación**) (PM). Si se tiene una serie de t tareas tales que se puedne hacer en t etapas sucesivas, en donde

- La etapa 1 se puede hacer de n_1 maneras;
- La etapa 2 se puede hacer de n_2 maneras; etc.;
- La etapa t se puede hacer de n_t maneras;

y las tareas son compatibles dos a dos, i.e. si se hace la tarea T_i también se puede hacer la tarea T_j, con $i \neq j$, entonces, el número de opciones z para hacer toda la tarea es $z = n_1 n_2 ... n_t$.

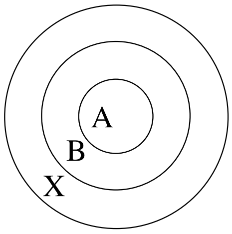

Figura 7.1: Diagrama de Venn cuando $A \subset B \subset X$.

Ejemplo. Para contar el número de opciones en el menú de un bar, o para combinar la ropa (e.g. camisa, pantalón), etc., hay que emplear el PM, ver los ejemplos del libro.

Ejemplo. Etiquetar las butacas de un auditorio con una letra y un número entero positivo menor o igual a 100. ¿Cuántas formas distintas existen para etiquetar una butaca? Considere un alfabeto de 26 letras. Solución: el proceso de etiquetar las butacas consiste en 2 tareas: asignar una de las 26 letras del alfabeto, y luego asignar uno de los 100 números disponibles. Usando el PM hay $z = 26 \cdot 100 = 2600$ formas distintas de etiquetar una butaca.

Ejemplo. Sean los 5 caracteres A, B, C, D, E. El número de cadenas que se pueden construir cuando:

i) De longitud 4, sin repetir caracteres: usamos el PM en 4 pasos sucesivos $z_{ABCD} = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ opciones;
ii) De longitud 4, sin repetir caracteres, y que empiezan con B: otra vez usamos el PM en 4 pasos sucesivos $z_B = 1 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 24$ opciones;
iii) De longitud 4, sin repetir caracteres, y sin empezar con B: hay dos opciones para hacerlo:
    a) Contar las opciones que empiezan con A, luego con C, luego con D, luego con E, y sumarlas. En cada uno se tiene el mismo número de opciones $z_0 = 1{\cdot}4{\cdot}3{\cdot}2 = 24$, por lo que en total habrán $z_{ACDE} = 4z_0 = 4 \cdot 24 = 96$ opciones;
    b) Hacerlo por diferencia entre los números de opciones en total y las que empiezan con B. Se tiene $z_{ACDE} = z_{ABCDE} - z_B = 120 - 24 = 96$ opciones.

Ejemplo. ¿Cuántas cadenas de bits diferentes hay de longitud 7? Solución: hay que llenar 7 casilleros, en cada uno hay 2 opciones, por lo que usando el PM hay $z = 2^7$.

Ejemplo. ¿Cuántas patentes diferentes hay si cada una consiste en una serie de 3 letras seguidas de 4 dígitos, y se permiten las repeticiones de letras o dígitos? Considere un alfabeto de 26 letras. Solución: considerando un alfabeto de 26 letras, los 10 dígitos, y usando el PM hay en total $z = 26^3 \cdot 10^4$.

Observación. Una demostración basada en un argumento combinatorio es una demostración que emplea un argumento de conteo.

Teorema. Utilizando un argumento de conteo demuestre que en un conjunto finito A de n elementos, se cumple que $|\mathcal{P}(A)| = 2^n$, donde $\mathcal{P}(A)$ es el conjunto potencia (o conjunto de partes) del conjunto A.

etapa 1: colocar elemento x_1	etapa 2: colocar elemento x_2	A	$B-A$	$X-B$	par ordenado (A,B) resultante
en A	en A	$\{1,2\}$	$\emptyset$	$\emptyset$	$(\{1,2\},\{1,2\})$
	en $B-A$	$\{1\}$	$\{2\}$	$\emptyset$	$(\{1\},\{1,2\})$
	en $X-B$	$\{1\}$	$\emptyset$	$\{2\}$	$(\{1\},\{1\})$
en $B-A$	en A	$\{2\}$	$\{1\}$	$\emptyset$	$(\{2\},\{1,2\})$
	en $B-A$	$\emptyset$	$\{1,2\}$	$\emptyset$	$(\emptyset,\{1,2\})$
	en $X-B$	$\emptyset$	$\{1\}$	$\{2\}$	$(\emptyset,\{1\})$
en $X-B$	en A	$\{2\}$	$\emptyset$	$\{1\}$	$(\{2\},\{2\})$
	en $B-A$	$\emptyset$	$\{2\}$	$\{1\}$	$(\emptyset,\{2\})$
	en $X-B$	$\emptyset$	$\emptyset$	$\{1,2\}$	$(\emptyset,\emptyset)$

Tabla 7.1: Cada uno de los pares ordenados (A,B) que verifican $A \subseteq B \subseteq X$ cuando $X = \{1,2\}$.

Demostración:

Un subconjunto del conjunto $A = \{a_1, a_2, ..., a_n\}$ se puede construir en n pasos sucesivos:

- Se elige (o no) el elemento a_1;
- Se elige (o no) el elemento a_2; etc.;
- Se elige (o no) el elemento a_n;

en donde cada etapa se puede realizar de 2 maneras por lo que, usando el PM, el número de subconjuntos posibles es $z = 2 \cdot 2 \cdot ... \cdot 2$, n veces, o sea $z = 2^n$.

Teorema. Sea un conjunto finito X de n elementos, y los subconjuntos A y B de X. Utilizando un argumento de conteo demuestre que el número de pares ordenados (A,B) tales que $A \subseteq B \subseteq X$ es $z = 3^n$. *Demostración*: Sea el par ordenado (A,B) tal que $A \subseteq B \subseteq X$. Convine trazar un diagrama de Venn, ver Fig. 7.1, para ver lo siguiente: (i) Si se asigna cada elemento de X a uno de los conjuntos A, $B-A$ o $X-B$, se tendrá un par ordenado único (A,B) que satisface $A \subseteq B \subseteq X$; (ii) Recíprocamente, cada elemento de X debe estar en uno solo de los conjuntos A, $B-A$ o $X-B$. Por eso podemos emplear el siguiente proceso por etapas:

- Se asigna el elemento x_1 de X a alguno de los conjuntos A, $B-A$, o $X-B$;
- Se asigna el elemento x_2 de X a alguno de los conjuntos A, $B-A$, o $X-B$, etc.;
- Se asigna el elemento x_n de X a alguno de los conjuntos A, $B-A$, o $X-B$;

En cada una de estas etapas hay 3 opciones por lo que, usando el PM, el número total de opciones es $z = 3 \cdot 3 \cdot ... \cdot 3$, n veces, o sea $z = 3^n$.

Ejemplo. Sea un conjunto finito $X = \{1,2\}$, y los subconjuntos A y B de X tales que verifican $A \subseteq B \subseteq X$. Aplique el teorema anterior. Luego, liste cada uno de los pares ordenados (A,B) que verifican $A \subseteq B \subseteq X$. Solución: tenemos $n = 2$, por lo que $z = 3^2 = 9$, i.e. hay 9 pares ordenados (A,B) que verifican $A \subseteq B \subseteq X$. Cada uno está listado en la Tabla 7.1.

Ejemplo. ¿Cuántas cadenas de bits diferentes hay de longitud 6? Solución: usando el PM hay $z = 2^7$.

Ejemplo. ¿Cuántas funciones se pueden definir desde un conjunto $A = \{a_1, a_2, ..., a_m\}$ de m elementos (dominio) a otro conjunto $B = \{b_1, b_2, ..., b_n\}$ de n elementos (codominio)?

Solución: una función $f\colon A \to B$ se corresponde con una elección de los n elementos del codominio B, para cada uno de los elementos del dominio A. Usando el PM hay $z = n \cdot n ... \cdot n$ (m veces), o sea, $z = |B|^{|A|}$. Notar que cuando $|A| = 1$ (o $m = 1$), se tiene $z_1 = n$ y, además, si bien serán funciones, no serán funciones inyectivas.

Tarea. Escriba cada una de las funciones que se pueden definir entre los conjuntos: (i) $A = \{a\}$ y $B = \{1, 2, 3\}$; (ii) $A = \{a, b\}$ y $B = \{\delta\}$. En cada caso ¿hay inyectivas? ¿cuáles?

Ejemplo. ¿Cuántas funciones inyectivas se pueden definir desde un conjunto $A = \{a_1, a_2, ..., a_m\}$ de m elementos (dominio) a otro conjunto $B = \{b_1, b_2, ..., b_n\}$ de n elementos (codominio)? Solución:

i) Sea una función $f\colon A \to B$. Si $|A| > |B|$ entonces no hay unicidad de la preimagen, por lo que f no será inyectiva;
ii) Sabemos que $|A| \leq |B|$ (i.e. $m \leq n$). Si f debe ser inyectiva, entonces se la puede construir en m pasos sucesivos:
   - Elijo la imagen de a_1, para lo cual dispongo de n opciones;
   - Elijo la imagen de a_2, para lo cual dispongo de $(n - 1)$ opciones;
   - Elijo la imagen de a_3, para lo cual dispongo de $(n - 2)$ opciones; etc.;
   - Elijo la imagen de a_m, para lo cual dispongo de $(n - m + 1)$ opciones;

   por lo que, usando el PM, en total hay

$$z = n \cdot (n - 1)...(n - m + 1) \tag{7.1}$$

   funciones inyectivas posibles $f\colon A \to B$, siempre que $|A| \leq |B|$;
ii) Caso particular: cuando $m = n$ entonces hay $n!$ funciones inyectivas.

Observación. El PM en términos de conjuntos finitos. Por una parte, si A_1, A_2, ..., A_n son conjuntos finitos, entonces el número de elementos del producto cartesiano $A_1 \times A_2 ... \times A_n$ es igual al producto del números de elementos de cada conjunto. Por otra parte, la tarea de elegir un elemento del producto cartesiano $A_1 \times A_2 ... \times A_n$ consiste en elegir un elemento de A_1, un elemento de A_2, ..., un elemento de A_n. Luego, sumando el PM se tiene que $|A_1 \times A_2 ... \times A_n| = |A_1||A_2|...|A_n|$.

7.1.2. Regla de la suma (o principio de la suma)

Definición. Regla de la suma (o **principio de la suma**) (PS) (enunciado). Si se tiene una serie de t tareas tales que

- La tarea 1 se puede hacer de n_1 maneras;
- La tarea 2 se puede hacer de n_2 maneras; etc.;
- La tarea t se puede hacer de n_1 maneras;

y las tareas son incompatibles dos a dos, i.e. si se hace la tarea T_i no se hace la tarea T_j, con $i \neq j$, entonces el número de opciones z para hacer toda la tarea es $z = n_1 + n_2 + ... + n_t$.

Ejemplo. Un alumno puede legir un tema proyecto entre 3 listas de temas. Si cada lista tiene 23, 17 y 13 propuestas, entonces ¿cuántas opciones dispone el alumno para elegir? (asuma un alumno normal). Solución:

- De la primera lista dispone de 23 opciones;
- De la segunda lista dispone de 17 opciones; etc.;
- De la tercera lista dispone de 13 opciones.

Como las tareas incompatibles dos a dos entonces, por el PS, el alumno dispone de $z = 23 + 17 + 13 = 53$ opciones.

Observación. El PS en términos de conjuntos finitos. Por una parte, si $A_1, A_2, ..., A_n$ son conjuntos finitos dsjuntos dos a dos, i.e. $A_i \cap A_j = \emptyset$ cuando $i \neq j$, entonces el número de elementos de la unión $A_1 \cup A_2 ... \cup A_n$ es igual a la suma del números de elementos de cada conjunto. Por otra parte, sea T_i la tarea de elegir un elemento del conjunto A_i, para $i = 1, 2, ..., n$. Como las tareas son incompatibles dos a dos, el número de formas de elegir un elemento de la unión, que coincide con el número de elementos de la unión, es $z = |A_1| + |A_2| ... + |A_n|$.

Observación. El PIE en conteo. Cuando algunas tareas se pueden hacer simultáneamente, no se puede usar el PS para hallar el número de opciones de hacer toda la tarea pues estamos contando 2 veces las tareas que se pueden hacer simultáneamente. Una forma de resolverlo, es sumando el número de maneras de realizar cada una de las tareas, y luegos restamos el número de opciones de realizar las tareas que se pueden hacer simultáneamente, es decir, aplicamos el PIE.

Ejemplo. ¿Cuántas cadenas de 8 bits comienzan con 1 o terminan con 10? Solución. Usamos el PIE para 2 conjuntos:

$$\begin{gathered} |A \cup B| = |A| + |B| - |A \cap B| \\ z_{A\cup B} = z_A + z_B - z_{A\cap B} \end{gathered} \tag{7.2}$$

a) Tarea A: el úmero de cadenas de 8 bits que empiezan con 1 es $z_A = 1{\cdot}2{\cdot}2{\cdot}2{\cdot}2{\cdot}2{\cdot}2{\cdot}2 = 2^7$;
b) Tarea B: el úmero de cadenas de 8 bits que terminan con 10 es $z_B = 2{\cdot}2{\cdot}2{\cdot}2{\cdot}2{\cdot}2{\cdot}1{\cdot}1 = 2^6$;
iii) Tarea $A \cap B$: el úmero de cadenas de 8 bits que empiezan con 1 y terminan con 10 es $z_2 = 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 1{\cdot}1 = 2^5$;
iv) Tarea $A \cup B$: entonces $z_{A\cup B} = z_A + z_B - z_{A\cap B} = 2^7 + 2^6 - 2^5 = 128 + 64 - 32 = 160$ opciones. Notar que, en general, $z \geq 0$.

7.1.3. Diagrama en árbol

Intro.
- Algunos problemas de conteo se pueden resolver usando un DA;
- Un digrama en árbol está formado por una raíz, un cierto número de ramas que parte de la raíz y, quizás, por otras ramas que empiezan en los extremos libres de las ramas, y así sucesivamente, hasta llegar a las hojas, las cuales son los extremos de las ramas en donde no empieza otra rama;
- Si utilizamos un árbol para contar, entonces usamos las ramas para representar cada posible elección. Los resultados posibles están en las hojas.

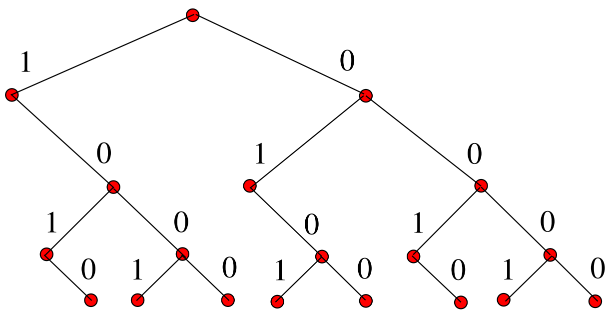

Figura 7.2: Diagrama en árbol para hallar el número de cadenas de 4 bits sin dos unos consecutivos.

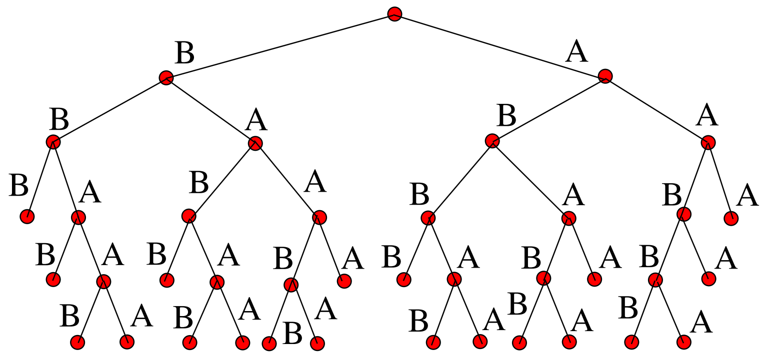

Figura 7.3: Eliminatoria entre 2 equipos con no más de 5 partidos, en donde el primero que gane 3 partidos es el campeón.

Ejemplo. ¿Cuántas cadenas de 4 bits sin dos unos consecutivos hay, y cuáles son? Solución: hay 8 cadenas que se muestran en el diagrama en árbol de la Fig. 7.2.

Ejemplo. Una eliminatoria entre 2 equipos con, a lo más, 5 partidos, en donde el primero que gane 3 partidos es el campeón. ¿Cuáles son las posibles historias de la eliminatoria. Solución: los posibles historiales se muestran en el diagrama en árbol de la Fig. 7.3.

Ejemplo. ¿Cuántas opciones hay para elegir 2 libros de temas diferentes de la siguiente lista de libros: 5 de Computación (C), 3 de Matemática (M), y 2 de Arte (A), donde todos son libros distintos. Solución. Hay que elegir 2 libros de temas diferentes. Primero contamos las opciones por separado con 2 temas usando el PM. Tenemos:

- Computación-Matemática $z_{CM} = 5 \cdot 3 = 15$;
- Computación-Arte $z_{CA} = 5 \cdot 2 = 10$;
- Matemática-Arte $z_{MA} = 3 \cdot 2 = 6$;

Estas selecciones son incompatibles entre si, i.e. corresponden a conjuntos ajenos entre si, por lo que usamos el PS resultando $z = z_{CM} + z_{CA} + z_{MA} = 15 + 10 + 6$.

7.2. Permutaciones y combinaciones

7.2.1. Permutaciones

Definición. Permutación (o **n-permutación**). Una permutación (o n-permutación) de n

elementos DISTINTOS x_1, x_2, ..., x_n es un ordenamiento de sus n elementos. Notación: el número de permutaciones de n elementos tomados de un conjunto de n elementos distintos lo denotamos con $P(n)$ (o con $P(n,n)$).

Ejemplo. Encuentre todas las permutaciones posibles de las letras A, B, C. Solución: se tienen 6 posibilidades

- ABC, BCA, CAB (obtenida con permutaciones circulares);
- ACB, BAC, CBA (fija la primera letra del caso anterior y una permutación de las 2 restantes).

Teorema. El número de permutaciones con n elementos tomados de un conjunto de n elementos distintos está dado por $P(n) = n!$. *Demostración*: Usamos el PM para construir una permutación en n etapas sucesivas:

- Se elige el 1er elemento, para lo cual hay n opciones;
- Se elige el 2do elemento, para lo cual quedan $(n-1)$ opciones;
- Se elige el 3er elemento, para lo cual quedan $(n-2)$ opciones; etc.;
- Se elige el último elemento, para lo cual queda 1 opción;

por lo que, usando el PM, el número de permutaciones posibles es

$$P(n,n) = n(n-1)(n-2)...2 \cdot 1 = n! \tag{7.3}$$

Ejemplo. Sean las 6 letras $ABCDEF$. Determine el número de permutaciones que contienen

- La subcadena DEF. Solución: hay que contar todas las permutaciones de los caracteres A, B, C, y DEF (fija). Vemos que para el conteo tenemos 4 cadenas efectivas, por lo que se tiene $z = 4!$
- Las letras DEF juntas pero en cualquier orden. Solución: a la solución del caso anterior hay que agregarle las permutaciones de los caracteres D, E, y F, lo cual agrega $3!$ por lo que en total se tiene $z = 4! \cdot 3! = 6 \cdot 24 = 144$.

Ejemplo. Sean 6 personas distinguibles (i.e. no gemelos ni clones). Determine el número de opciones para sentarlas alrededor de una mesa circular. Solución: notar que los arreglos obtenidos por rotación se consideran iguales, una vez sentados en alguna forma los podemos correr a todos juntos sin cambiar la disposición relativa. En este caso, sentamos a A en cualquier lugar, luego sentamos a las $5 = 6 - 1$ personas restantes en alguna forma, para lo cual hay $(6-1)!$ opciones.

Observación. En general tenemos $P(n, \text{lineal}) = n!$ y $P(n, \text{circular}) = (n-1)!$

Definición. Permutación de r elementos (r-permutación). Una permutación de r elementos (o r-permutación) tomados de entre n elementos DISTINTOS x_1, x_2, ... x_n, es un ordenamiento de r elementos, donde $0 \leq r \leq n$. Notación: el número de permutaciones de r elementos tomados de un conjunto de n elementos distintos, con $0 \leq r \leq n$, lo denotamos con $P(n,r)$.

Ejemplo. Determine todas las permutaciones con 2 elementos tomados del conjunto $\{A, B, C, D\}$. Solución. Por fuerza bruta obtenemos:

- AB, AC, AD (la 1ra con la 2da, con la 3ra, etc.);
- BC, BD (la 2da con la 3ra, con la 4ta, etc.);
- CD (la 3ra con la 4ta, con la 5ta, etc.);
- BA, CA, DA, CB, DB, DC (todas las permutaciones de los casos anteriores).

con un total de 12 alternativas.

Teorema. El número de permutaciones con r elementos tomados de un conjunto de n elementos distintos, con $0 \leq r \leq n$, está dado por $P(n, r) = n \cdot (n-1)....(n-r+1)$. *Demostración*: Usamos el PM para construir una permutación con r elementos tomados de un conjunto de n elementos, donde $0 \leq r \leq n$, lo hacemos en r etapas sucesivas:

- Se elige el elemento 1, para lo cual hay n opciones;
- Se elige el elemento 2, para lo cual hay $(n-1)$ opciones;
- Se elige el elemento 3, para lo cual hay $(n-2)$ opciones; etc.;
- Se elige el elemento r, para lo cual hay $(n-r+1)$ opciones;

por lo que, usando el PM, el número de permutaciones posibles con r elementos es

$$P(n, r) = n(n-1)(n-2)...(n-r+1) \tag{7.4}$$

Notar que si $r = n$, entonces se recupera el caso anterior.

Ejemplo. Determine el número de permutaciones con 2 elementos tomados del conjunto $\{A, B, C, D\}$. Solución: tenemos $n = 4$ y $r = 2$, por lo que $n-r+1 = 4-2+1 = 3$, y el número de permutaciones posibles de 2 elementos tomados de un conjunto de 4 elementos es $P(4, 2) = 4 \cdot 3 = 12$, cada una de las cuales fueron listadas en el ejemplo anterior.

Observación. Fórmula alternativa de cómputo para $P(n, r)$. Notar que:

$$\begin{aligned} P(n, r) &= n(n-1)(n-2)...(n-r+1) \\ &= \frac{n(n-1)(n-2)...(n-r+1)(n-r)(n-r-1)...2 \cdot 1}{(n-r)(n-r-1)...2 \cdot 1} \\ &= \frac{n!}{(n-r)!} \end{aligned} \tag{7.5}$$

Ejemplo. Determine el número de opciones para ubicar sentar a una mesa (recta) a 7 Marcianos (M) y a 5 Venusianos (V), todos distinguibles (i.e. no gemelos ni clones), si 2 V no pueden sentarse juntos. Solución. Una sentada la podemos hacer en 2 etapas:

i) Sentamos primero a los 7 de Marte dejando un lugar libre por medio, para lo cual hay $z_M = P(7) = 7!$ opciones. Notar que de este modo se generaron 7+1=8 lugares libres, i.e. _M1_M2_M3_M4_M5_M6_M7_;
ii) Luego sentamos a los 5 de Venus en esos 8 lugares libres, para lo cual hay $z_V = P(8, 5)$ opciones;

Finalmente, usando el PM, se tienen $z = z_M z_V = P(7)P(8, 5) = 7!P(8, 5)$ opciones.

7.2.2. Combinaciones

Definición. Combinación. Una combinación de r elementos tomados de entre n elementos DISTINTOS x_1, x_2, ... x_n, es una selección NO-ORDENADA de r elementos, donde $0 \leq r \leq n$. Notación: el número de combinaciones de r elementos tomados de un conjunto de n elementos distintos, con $0 \leq r \leq n$, lo denotamos con $\binom{n}{r}$ (notación de Newton), o con $C(n, r)$.

Ejemplo. Determine todas las combinaciones con 2 elementos tomados del conjunto $\{A, B, C, D\}$. Solución. Por fuerza bruta obtenemos 6 posibilidades:

- AB, AC, AD (la 1ra con la 2da, con la 3ra, etc.);
- BC, BD (la 2da con la 3ra, con la 4ta, etc.);
- CD (la 3ra con la 4ta, con la 5ta, etc.);

Teorema. El número de combinaciones con r elementos tomados de un conjunto A de n elementos distintos, con $0 \leq r \leq n$, está dado por

$$C(n, r) = \frac{n!}{r!(n-r)!} \tag{7.6}$$

Demostración. Podemos construir las permutaciones con r elementos tomados de un conjunto de n elementos, con $0 \leq r \leq n$, en 2 etapas sucesivas:

- Construimos todas las combinaciones con r elementos tomados de un conjunto de n elementos;
- Para cada combinación con r elementos obtenemos todas sus permutaciones posibles.

Luego, usando el PM, el número de permutaciones con r elementos es igual al producto del número de combinaciones con r elementos tomados de una conjunto de n elementos, por el número de sus permutaciones, i.e.

$$\begin{aligned} P(n, r) &= C(n, r)P(r) \\ \therefore \quad C(n, r) &= \frac{P(n, r)}{P(r)} \\ &= \frac{n(n-1)(n-2)...(n-r+1)}{r(r-1)...1} \\ &= \frac{n!}{r!(n-r)!} \end{aligned} \tag{7.7}$$

Ejemplo. Si $\{A, B, C, D\}$, y $r = 2$, tendremos

- AB, AC, AD, BC, BD, CD (todas las combinaciones con 2 elementos);
- BA, CA, DA, CA, DB, DC (todas las permutaciones de las combinaciones anteriores);
- Aqui tenemos $P(4, 2) = 12$ y $P(2) = 2! = 2$, con lo que $C(4, 2) = P(4, 2)/P(2) = 12/2 = 6$, y que ya fueron listadas.

Ejemplo. Si $\{A, B, C, D\}$, y $r = 2$, tendremos

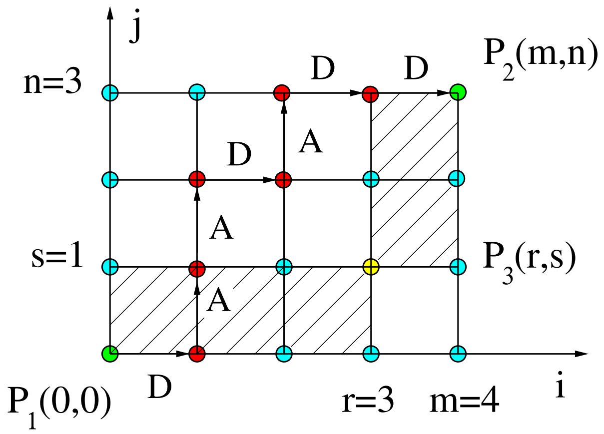

Figura 7.4: Grilla rectangular entre los vértices $P_1(0,0)$ y $P_2(m,n)$. Incluye un vértice intermedio $P_3(r,s)$, y la ruta *DAADADD*.

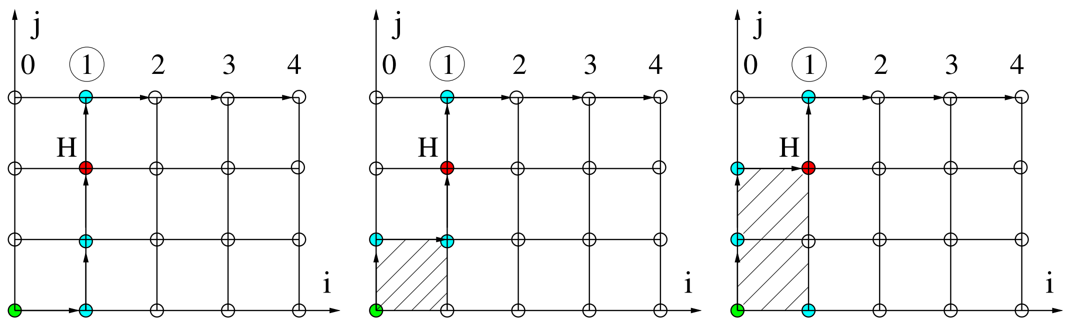

Figura 7.5: La clase de las rutas que llegan al borde superior por primera vez en la posición $i = 1$ en la grilla $n = 3 \times m = 4$.

- AB, AC, AD, BC, BD, CD (todas las combinaciones con 2 elementos);
- BA, CA, DA, CA, DB, DC (todas las permutaciones de las combinaciones anteriores);
- Aquí tenemos $P(4,2) = 12$ y $P(2) = 2! = 2$, con lo que $C(4,2) = P(4,2)/P(2) = 12/2 = 6$, y que ya fueron listadas.

Ejemplo. Conteo de rutas posibles en una grilla rectangular entre vértices $P_1(0,0)$ y $P_2(m,n)$ dados, y posiblemente un vértice intermedio $P_3(r,s)$, con $0 \leq r \leq m$ y $0 \leq s \leq n$. Demuestre, incluyendo el uso de argumentos de conteo, que:

i) Existen $\binom{m+n}{m}$ rutas para ir desde el vértice $P_1(0,0)$ hacia el $P_2(m,n)$, yendo siempre hacia la Derecha (D) y hacia arriba (A);

ii) Se verifican las identidades combinatorias

$$\begin{aligned} \binom{m+n}{m} &= \binom{m+n}{n} \\ \binom{m+n}{m} &= \sum_{k=0}^{m} \binom{k+(n-1)}{k} \end{aligned} \tag{7.8}$$

Solución:

i) Cada ruta desde $P_1(0,0)$ hacia $P_2(m,n)$ se puede representar como una cadena de $(m+n)$ letras A (hacia Arriba) y D (hacia a la Derecha). Por ejemplo, en la Fig. 7.4

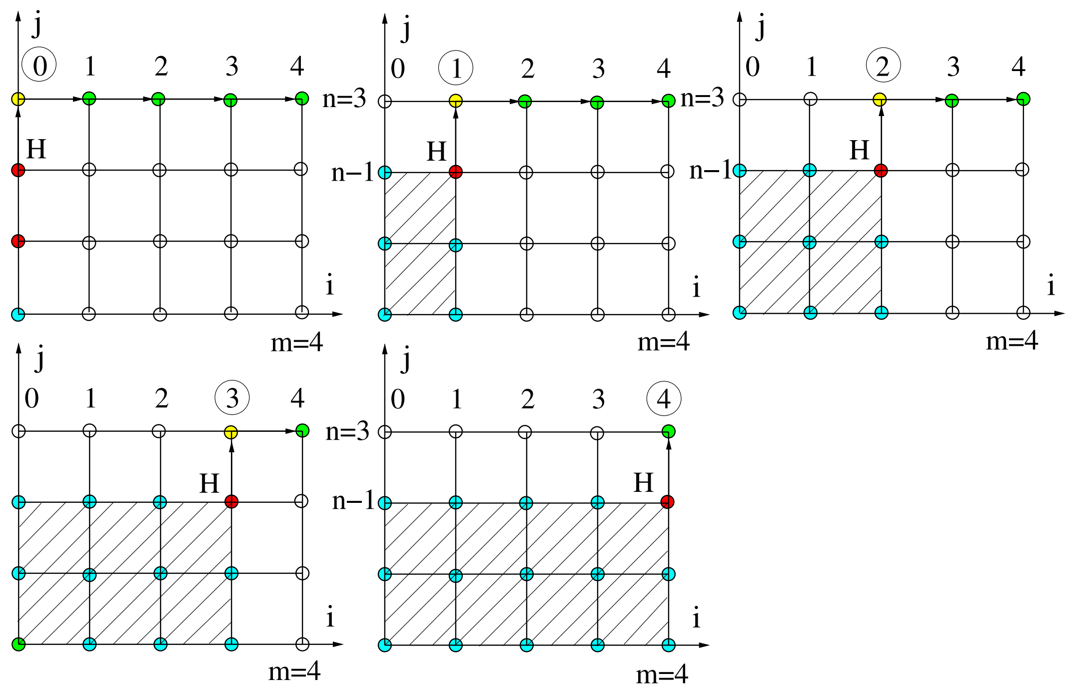

Figura 7.6: División de las rutas en clases según la primera vez que tocan el borde superior. Una ruta toca al borde superior por primera vez en cualquiera de las líneas verticales $i = 0, 1, 2, 3, 4$.

se muestra el caso $m = 4$ y $n = 3$, en donde la cadena de cualquier ruta tiene 7 caracteres, e.g. en la dicha figura se ha marcado la ruta *DAADADD*, con 4 letras D y 3 letras A. Entonces, contar el números de rutas en esas condiciones equivale al número de cadenas que se pueden construir, para lo cual hay 2 opciones:

- Elegimos primero las m posiciones para las letras D, en cualquier orden, entre los $(m + n)$ lugares en la cadena, y luego completamos las posiciones restantes con las letras D. Luego, el número total de rutas posibles debe ser $\binom{m+n}{m}$;
- Elegimos primero las n posiciones para las letras A, en cualquier orden, entre los $(m + n)$ lugares en la cadena, y luego completamos las posiciones restantes con letras A. Luego, el número total de rutas posibles debe ser $\binom{m+n}{n}$;
- El resultado de los conteos anteriores debe ser el mismo, por lo que $\binom{m+n}{m} = \binom{m+n}{n}$.

Observaciones:

- Las posiciones elegidas para las letras A y D se pueden distinguir, por eso, no incide que las letras sean indistinguibles;
- La primera Ec. (7.8) también se puede comprobar usando la definición de número combinatorio y un poco de álgebra

$$\begin{aligned}\binom{m+n}{m} &= \frac{(m+n)!}{m!(m+n-m)!} = \frac{(m+n)!}{m!n!}\\ \binom{m+n}{n} &= \frac{(m+n)!}{n!(m+n-n)!} = \frac{(m+n)!}{n!m!}\end{aligned} \tag{7.9}$$

ii) - Dividimos las rutas en clases basándonos en la primera vez que tocan el borde superior. Una ruta puede tocar el borde superior por primera vez en cualquiera de las $m + 1$ líneas verticales;

- Notar que (i) las clases son ajenas porque una ruta no puede llegar al borde superior por primera vez en más de una ocasión; y (ii) cada ruta pertenece a alguna clase;
- Es decir, esas clases definan una partición del conjunto de rutas, por lo cual podemos emplear el PS, según el cual la suma del número de rutas en cada clase es igual al número total de rutas, pues (i) ninguna ruta se cuenta 2 veces (porque están en clases disjuntas); y (ii) cada ruta pertenece a alguna clase;
- Por ejemplo, en la Fig. 7.5 se muestran las 3 rutas que existen para llegar al borde superior por primera vez en la línea vertical $i = 2$. Notar que las rutas alternativas se dan antes de llegar al vértice H marcado, i.e. una vez llegado a H sólo hay una forma de terminar la ruta: subiendo un cuadro (una A). Por eso basta contar el número de rutas en la subgrilla sombreada 1×2 y, por el inciso anterior, se obtiene $z_2 = \binom{1+2}{1} = \binom{3}{1} = 3$, valor ya obtenido;
- Haciendo lo mismo en cada una de las líneas verticales $i = 0, 1, 2, 3, 4$, ver Fig. (7.6), se tiene

$$\begin{aligned}
\text{en } i = 0:\quad & \binom{0+2}{0} = \binom{2}{0} = 1 \\
\text{en } i = 1:\quad & \binom{1+2}{1} = \binom{3}{1} = 3 \\
\text{en } i = 2:\quad & \binom{2+2}{2} = \binom{4}{2} = 6 \\
\text{en } i = 3:\quad & \binom{3+2}{3} = \binom{5}{3} = 10 \\
\text{en } i = 4:\quad & \binom{4+2}{4} = \binom{6}{4} = 15
\end{aligned} \tag{7.10}$$

cuya suma z_D es el lado derecho de la Ec. (7.8) y es igual al lado izquierdo z_I de la misma ecuación

$$\begin{aligned}
z_D &= 1 + 3 + 6 + 10 + 15 = 35 \\
z_I &= \binom{4+3}{3} = \binom{7}{3} = 35
\end{aligned} \tag{7.11}$$

- Generalizando la ley que se va generando en la Ec. (7.10) se tiene

$$\begin{aligned}
z_D &= \sum_{k=0}^{m} \binom{k + (n-1)}{k} \\
z_I &= \binom{m+n}{m}
\end{aligned} \tag{7.12}$$

y como debe ser $z_I = z_D$, se obtiene la segunda identidad de la Ec. (7.8).

7.3. Permutaciones y combinaciones generalizadas

7.3.1. Permutaciones generalizadas

Ejemplo. Encuentre todas las cadenas que se pueden formar usando todas las letras de la palabra MISSISSIPPI. Solución: tenemos $n = 11$ letras pero, como hay letras repetidas, la respuesta no es $z = (11 \cdot 10...2 \cdot 1) = 11! = 39\,916\,800$, sino que son muchas menos. Notar que

- Hay $C(11, 2)$ lugares para las 2 letras P, y pierdo 2 lugares;
- Hay $C(11 - 2, 4) = C(9, 4)$ lugares para las 4 letras S, y pierdo 4 lugares;
- Hay $C(9 - 4, 4) = C(5, 4)$ lugares para las 4 letras I, y pierdo 4 lugares;
- Hay $C(5 - 4, 1) = C(1, 1)$ lugares para la letra M (una sola);

y usando el PM se tiene

$$\begin{aligned} z &= \binom{11}{2} \cdot \binom{9}{4} \cdot \binom{5}{4} \cdot \binom{1}{1} \\ &= \frac{11!}{2!9!} \cdot \frac{9!}{4!5!} \cdot \frac{5!}{4!1!} \cdot \frac{1!}{1!0!} \\ &= \frac{11!}{2!4!1!} = 831\,600 \end{aligned} \tag{7.13}$$

y que es mucho menor (en una relación 48 a 1) con respecto a una permutación de 11 elementos distinguibles.

Teorema. El número de permutaciones de n elementos tomados de una colección con:

- n_1 elementos idénticos del tipo 1;
- n_2 elementos idénticos del tipo 2; etc.
- n_t elementos idénticos del tipo t;

tal que hay $n = n_1 + n_2 + ... + n_t$ elementos en total, está dado por

$$z = \frac{n!}{n_1!n_2!...n_t!} \qquad \text{con } n = n_1 + n_2 + ... + n_t \tag{7.14}$$

Demostración: Hay que asignar las posiciones a cada uno de los n elementos, en donde

- Para los n_1 elementos idénticos del tipo 1, hay $C(n, n_1)$ opciones, y se pierden n_1 lugares;
- Para los n_2 elementos idénticos del tipo 2, hay $C(n - n_1, n_2)$ opciones, y se pierden otros n_2 lugares;
- Para los n_3 elementos idénticos del tipo 3, hay $C(n-n_1-n_2, n_3)$ opciones, y se pierden otros n_3 lugares; etc.

por lo que, usando el PM, el número total de permutaciones posibles es

$$\begin{aligned} z &= C(n, n_1) \cdot C(n - n_1, n_2) \cdot C(n - n_1 - n_2, n_3) \ldots C(n - n_1 - n_2 ... - n_{t-1}, n_t) \\ &= \frac{n!}{n_1!(n - n_1)!} \cdot \frac{(n - n_1)!}{n_2!(n - n_1 - n_2)!} \cdots \frac{(n - n_1 - n_2... - n_{t-1})!}{n_t!} \\ &= \frac{n!}{n_1!n_2!...n_t!} \end{aligned} \tag{7.15}$$

7.3.2. Combinaciones generalizadas

Ejemplo. Se tienen libros de Computación (C), Física (F), e Historia (H), con al menos 6 copias idénticas (clones) de cada uno. Determine el número de opciones para elegir 6 libros. Solución:

- Hay que elegir, en cualquier orden, 6 libros del conjunto $\{C, F, H\}$ con 3 clases, o **colores**;
- Una selección queda definida indicando el número de libros de cada tipo, para lo cual conviene un esquema con círculos $\circ$ para los libros de cada clase (o de cada color), posiblemente repetidos, y 2 rectángulos $\square$ como **separadores** que separan a las 3 clases de libros, e.g.

Computación (C)		Física (F)		Historia (H)		
$\circ\circ\circ$	$\square$	$\circ\circ$	$\square$	$\circ$	3 de C, 2 de F, 1 de H	(7.16)
	$\square$	$\circ\circ\circ\circ$	$\square$	$\circ\circ$	0 de C, 4 de F, 2 de H	

- Notar que para separar las 3 clases de libros (o colores), hacen falta 2 separadores $\square$, i.e. es el número de clases (o de colores) menos 1;
- Cada ubicación de 6 círculos y 2 separadores $\square$ define una selección, en donde hay 8 símbolos en total (entre círculos y rectángulos);
- Notar que basta definir la ubicación de los 2 separadores, por lo que tendremos $z = C(8, 2) = 28$ formas para elegir 6 libros de C, F e H.

Teorema. "Teorema de pelotero". El número de opciones para elegir uan combinación de k elementos posiblemente repetidos (y en cualquier orden) tomados de un conjunto con t clases (o colores, asumidos ditinguibles), está dado por

$$z = \binom{k + (t-1)}{t-1} \tag{7.17}$$

Además

$$\binom{k + (t-1)}{t-1} = \binom{k + (t-1)}{k} \tag{7.18}$$

Demostración:

- Sea el conjunto de las t clases (o colores) asumidos como distinguibles;
- Consideremos k círculos (para los elementos) y $t - 1$ separadores (para los colores). En total tenemos $k + (t - 1)$ símbolos;
- Cada distribución de estos símbolos define una combinación;
- El número de símbolos hasta encontrar al separador 1, define una selección de elementos de la clase (o color) 1;
- El número de símbolos entre los separadores 1 y 2, define una selección de elementos de la clase (o color) 2; etc.
- Como hay $C(k + (t - 1), t - 1)$ opciones para elegir las posiciones de los separdores, también habrán $z_1 = C(k + (t - 1), t - 1)$ selecciones;
- Como hay $C(k+(t-1), k)$ opciones para elegir las posiciones de los círculos, también habrán $z_2 = C(k + (t - 1), k)$ selecciones;

i	j	k
0	0	0
1	0	0
1	1	0
1	1	1

Tabla 7.2: Valores de i, j, k en el algoritmo de 3 lazos anidados, con $n = 2$ y $k = 3$.

- Como es la misma tarea se concluye que $z_1 = z_2$.

Ejemplo. Hay 3 pilas de pelotas: Rojas (R), Verde (V), y Amarillas (A). Cada pila tiene al menos 6 pelotas. Determine el número de opciones para:

- Elegir 8 pelotas, sin restricciones;
- Elegir 8 pelotas con al menos una de cada color.

Solución:

- Es una elección de $k = 8$ elementos, posiblemente repetidos, en cualquier orden, por lo que podemos aplicar el "teorema del pelotero", con $t = 3$ clases (los 3 colores de las pelotas), resultando $z = C(8 + (3 - 1), (3 - 1) = C(10, 2) = 45$;
- Primero elegimos 1 pelota de cada color y, para completar, hay que agregar las que falta, i.e. $k = 8 - 3 = 5$ pelotas de cualquier color, i.e. $z = C(5 + (3 - 1), (3 - 1) = C(7, 2) = 21$.

```python
def QueHace (n):
    for i in range (n):
        for j in range (i):
            for k in range (j):
                print (i,j,k)
    return None
```

Ejemplo. Determine el número de veces en que se ejecuta la impresión de la túpla (i, j, k) en el algoritmo dado.
Solución:

- Cada `print` muestra los valores de los enteros (i, j, k), donde $0 \leq i \leq j \leq k \leq (n-1)$;
- Cada sucesión de los tres enteros i, j, k satisface dicha desigualdad. Hay que contar el número de opciones de elegir 3 enteros, permitiendo las respeticiones, tomados del conjunto $\{0, 1, ..., n - 1\}$, por lo que el número de clases (colores) distinguibles es $t = n$, mientras que la cantidad de elementos en cada selección es $k = 3$, es decir, $z = C(k + (t - 1), (t - 1)) = C(n + 2, n - 1)$
- Por ejemplo, si $n = 2$ es $z = C(2 + 2, 2 - 1) = C(4, 1) = 4$ se tienen los valores i, j, k mostrados en la Tabla 7.2.

Ejemplo. Contar el número de soluciones de la ecuación diofántica

$$x_1 + x_2 + x_3 + x_4 = 29 \tag{7.19}$$

sujeta a las siguientes restricciones:

i) Cuando $x_1, x_2, x_3, x_4 \geq 1$. Solución: es equivalente a elegir 29 elementos x_i de tipo i, con $i = 1, 2, 3, 4$. En este caso, el número de clases (colores) es $t = 4$, y el número de elementos en cada selección es $k = 29$ (la suma de k valores uno). Se tiene $z_1 = C(k + (t - 1), (t - 1) = C(29 + (4 - 1), (4 - 1) = C(32, 3) = 4960$

ii) Cuando $x_1 > 0$, $x_2 > 1$, $x_3 > 2$, $x_4 \geq 0$. Solución: es equivalente a elegir 29 elementos con, al menos, 1 elemento del tipo 1, 2 elementos del tipo 2, y 3 elementos del tipo 3. Después hay que completar eligiendo $k = 29 - 1 - 2 - 3 = 23$ elementos adicionales. Escribimos:

$$\begin{gathered}(x_1 - 1) + (x_2 - 2) + (x_3 - 3) + (x_4 - 0) = 29 - 1 - 2 - 3 - 0 \\ y_1 + y_2 + y_3 + y_4 = 23\end{gathered} \tag{7.20}$$

donde $y_1, y_2, y_3, y_4 \geq 0$, y ahora puede aplicarse el teorema del pelotero con los nuevos valores: $z_2 = C(23 + (4 - 1), (4 - 1) = C(26, 3) = 2600$

Ejemplo. Contar el número de soluciones de la ecuación diofántica

$$x_1 + x_2 + x_3 + x_4 = 12 \tag{7.21}$$

con $0 \leq x_1 \leq 4$, $0 \leq x_2 \leq 5$, $0 \leq x_3 \leq 8$, $0 \leq x_4 \leq 9$. Solución:

- Introducimos los conjuntos
  - X: conj. de enteros no negativos, sin otras restricciones, es el conjunto universal;
  - A: conj. de enteros $0 \leq x_1 \leq 4$;
  - B: conj. de enteros $0 \leq x_2 \leq 5$;
  - C: conj. de enteros $0 \leq x_3 \leq 8$;
  - D: conj. de enteros $0 \leq x_4 \leq 9$;
- Entonces, el conjunto solución es

  $$I = A \cap B \cap C \cap D \tag{7.22}$$

  cuya cantidad de elementos $z_I = |I|$ es la respuesta pedida. Pero, para calcular z, haremos un rodeo empezando con

  $$X = I \cup \overline{I} \tag{7.23}$$

  donde

  $$\overline{I} = \overline{A \cap B \cap C \cap D} \tag{7.24}$$

  Como I e $\overline{I}$ son conjuntos disjuntos se tiene que

  $$|X| = |I| + |\overline{I}| \qquad \therefore \qquad |I| = |X| - |\overline{I}| \tag{7.25}$$

  usando una de las leyes de De Morgan

  $$\overline{I} = \overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{D} \tag{7.26}$$

  pero

  $$\begin{aligned}\overline{A} &= X - A \\ \overline{B} &= X - B \\ \overline{C} &= X - C \\ \overline{D} &= X - D\end{aligned} \tag{7.27}$$

en donde

$$\begin{aligned} X-A&: \text{conjunto con } x_1 \geq 5 \text{ y } x_2, x_3, x_4 \geq 0;\\ X-B&: \text{conjunto con } x_2 \geq 6 \text{ y } x_1, x_3, x_4 \geq 0;\\ X-C&: \text{conjunto con } x_3 \geq 9 \text{ y } x_1, x_2, x_4 \geq 0;\\ X-D&: \text{conjunto con } x_4 \geq 10 \text{ y } x_1, x_2, x_3 \geq 0; \end{aligned} \tag{7.28}$$

por lo que

$$\begin{aligned} |I| &= |X| - |\overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{D}|\\ |I| &= |X| - |(X-A) \cup (X-B) \cup (X-C) \cup (X-D)|\\ z_I &= z_0 - (z_1 + z_2 + z_3 + z_4) \end{aligned} \tag{7.29}$$

donde

$$\begin{aligned} z_0 &= |X|;\\ z_1 &= |X-A|;\\ z_2 &= |X-B|;\\ z_3 &= |X-C|;\\ z_4 &= |X-D|; \end{aligned} \tag{7.30}$$

- Conteo para el conjunto X: la ecuación es

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 12 \quad \text{con } x_1, x_2, x_3, x_4 \geq 0.\\ z_0 &= \binom{12+3}{3} = \binom{15}{3} = 455 \end{aligned} \tag{7.31}$$

- Conteo para el conjunto $X - A$: la ecuación es

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 12 \quad \text{con } x_1 \geq 5 \text{ y } x_2, x_3, x_4 \geq 0.\\ (x_1 - 5) + x_2 + x_3 + x_4 &= (12 - 5)\\ y_1 + x_2 + x_3 + x_4 &= 7 \quad \text{con } y_1, x_2, x_3, x_4 \geq 0.\\ z_1 &= \binom{7+3}{3} = \binom{10}{3} = 120 \end{aligned} \tag{7.32}$$

- Conteo para el conjunto $X - B$: la ecuación es

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 12 \quad \text{con } x_2 \geq 6 \text{ y } x_1, x_3, x_4 \geq 0.\\ x_1 + (x_2 - 6) + x_3 + x_4 &= (12 - 6)\\ x_1 + y_2 + x_3 + x_4 &= 6 \quad \text{con } x_1, y_2, x_3, x_4 \geq 0.\\ z_2 &= \binom{6+3}{3} = \binom{9}{3} = 84 \end{aligned} \tag{7.33}$$

- Conteo para el conjunto $X - C$: la ecuación es

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 12 \quad \text{con } x_3 \geq 9 \text{ y } x_1, x_2, x_4 \geq 0.\\ x_1 + x_2 + (x_3 - 9) + x_4 &= (12 - 9)\\ x_1 + x_2 + y_3 + x_4 &= 3 \quad \text{con } x_1, x_2, y_3, x_4 \geq 0.\\ z_3 &= \binom{3+3}{3} = \binom{6}{3} = 20 \end{aligned} \tag{7.34}$$

selección en el 1er factor $(a+b)$	selección en el 2do factor $(a+b)$	selección en el 3er factor $(a+b)$	producto
a	a	a	$aaa = a^3$
a	a	b	$aab = a^2b$
a	b	a	$aba = a^2b$
a	b	b	$abb = ab^2$
b	a	a	$baa = a^2b$
b	a	b	$bab = ab^2$
b	b	a	$bba = ab^2$
b	b	b	$bbb = b^3$

Tabla 7.3: Tarea de selección de los símbolos a y b, en cualquier orden y permitiendo las repeticiones.

- Conteo para el conjunto $X - D$: la ecuación es

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 12 \quad \text{con } x_4 \geq 10 \text{ y } x_1, x_2, x_3 \geq 0. \\ x_1 + x_2 + x_3 + (x_4 - 10) &= (12 - 10) \\ x_1 + x_2 + x_3 + y_4 &= 2 \quad \text{con } x_1, x_2, x_3, y_4 \geq 0. \\ z_4 &= \binom{2+3}{3} = \binom{5}{3} = 10 \end{aligned} \tag{7.35}$$

- Juntando resultados parciales

$$\begin{aligned} z_I &= z_0 - (z_1 + z_2 + z_3 + z_4) \\ &= 455 - (120 + 84 + 20 + 10) = 221 \end{aligned} \tag{7.36}$$

7.4. Coeficientes binomiales e identidades combinatorias

Ejemplo. Evaluar a partir de primeros principios $(a+b)^3$.
Solución:

$$\begin{aligned} (a+b)^3 &= (a+b)(a+b)(a+b) \\ &= (a+b)(aa + ab + ba + bb) \\ &= (aaa + aab + aba + abb)(baa + bab + bba + bbb) \\ &= a^3 + a^2b + a^2b + ab^2 + a^2b + ab^2 + ab^2 + b^3 \\ &= a^3 + 3a^2b + 3ab^2 + b^3 \end{aligned} \tag{7.37}$$

Se puede repensar como una tarea de selección de símbolos a o b, en cualquier orden, permitiendo las repeticiones, lo cual se muestra en la Tabla 7.3.

7.4.1. Teorema de Newton (o teorema de binomio)

Teorema. Teorema de Newton (o teorema de binomio). Si $a, b \in \mathbb{R}$ y n es un entero positivo, entonces

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \tag{7.38}$$

i) Demostración 1 (usando un argumento de conteo):

- En el desarrollo de $(a+b)^n$, un término de la forma $a^{n-k}b^k$ surge de elegir b en k factores, y elegir a en $(n-k)$ factores adicionales;
- Pero esto se puede hacer de $C(n,k)$ modos pues $C(n,k)$ cuenta el número de opciones para elegir k elementos de entre n disponibles;
- Entonces $a^{n-k}b^k$ debe aparecer $C(n,k)$ veces. Esto vale para $0 \leq k \leq n$ y, aplicando el PS,

$$(a+b)^n = \binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + ... + \binom{n}{n}a^0 b^n \tag{7.39}$$

ii) Demostración 2 (usando inducción): para alumnos libres.

Tarea. Re-hacer ejemplos 6.7.2, 6.7.3, y 6.7.5.

Observación. Los coeficientes binomiales son los números combinatorios.

Ejemplo. Encontrar el coeficiente de a^5b^4 de $(a+b)^9$.
Solución: con $n = 9$, y $k = 4$ en el binomio de Newton se tiene que $C(n,k)a^{n-k}b^k = C(9,5)a^5b^4 = 126a^5b^4$.

7.4.2. Teorema y triángulo de Pascal (o de Tartaglia)

Permite obtener rápidamente los coeficientes binomiales construyendo la siguiente disposición de enteros

$$\begin{array}{lccccccccc}
n=0: & & & & & 1 & & & & \\
n=1: & & & & 1 & & 1 & & & \\
n=2: & & & 1 & & 2 & & 1 & & \\
n=3: & & 1 & & 3 & & 3 & & 1 & \\
n=4: & 1 & & 4 & & 6 & & 4 & & 1
\end{array}$$

En esta construcción se pueden identificar

$$\begin{array}{lccc}
\text{horizontal } n: & \binom{n}{k-1} & & \binom{n}{k} \\
\text{horizontal } (n+1): & & \binom{n+1}{k} & \\
& \text{diag } (k-1) & \text{diag } k &
\end{array}$$

Teorema. Teorema. El triángulo de Pascal se justifica con la identidad combinatoria

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \qquad \text{donde } 1 \leq k \leq n \tag{7.40}$$

i) Demostración (usando un argumento de conteo):

- Sea un conjunto A con n elementos. Al agregarle un nuevo elemento x, entonces el número de subconjuntos de k elementos que se pueden formar a partir del conjunto $B = A \cup \{x\}$ está dado por $C(n+1,k)$.

- Los subconjuntos de k elementos de B se pueden dividir en 2 clases ajenas, a saber, los de la clase 1, dados por los subconjuntos de B que no contienen al elemento x, y los de la clase 2, que sí lo contienen.
- Cada subconjunto de la clase 1 es un conjunto de k elementos tomados del conjunto A, por lo que hay $C(n, k)$ opciones;
- Cada subconjunto de la clase 2 consiste en la unión de un subconjunto de $k - 1$ elementos de A, y el conjunto $\{x\}$, formado por el elemento x, por lo que hay $C(n, k - 1)$ opciones;
- Luego, usando el PS, se tiene que $C(n + 1, k)$ debe ser igual a la suma $C(n, k) + C(n, k - 1)$.

ii) Demostración 2 (usando la definición): es un ejercicio en la GTP.

Ejemplo. Demostrar que para todo entero n positivo se tiene que

$$\sum_{k=1}^{n} \binom{n}{k} = 2^n \tag{7.41}$$

Solución:

i) Demostración 1 (usando un argumento de conteo):

- Dado un conjunto A de n elementos, hay $C(n, k)$ subconjuntos de k elementos, y la suma de todos ellos cuenta el número de subconjuntos posibles de A;
- Por otra parte, se sabe que hay 2^n subconjuntos posibles de un conjunto A de n elementos;
- Dado que se trata de la misma tarea, ambas expresiones deben ser iguales.

ii) Demostración 2 (usando inducción). A partir de:

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \tag{7.42}$$

si $a = b = 1$, entonces se obtiene la Ec. 7.41.

Ejemplo. Demostrar que para todo entero n positivo se tiene que

$$\sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1} \tag{7.43}$$

Solución:

- Re-escribimos la identidad de Pascal

$$\binom{i}{k} = \binom{i+1}{k+1} - \binom{i}{k+1} \qquad \text{donde } 1 \le k \le n \tag{7.44}$$

- Antes hacemos el caso particular

$$\begin{aligned}\sum_{i=3}^{6}\binom{i}{3} &= \binom{3}{3}+\binom{4}{3}+\binom{5}{3}+\binom{6}{3}\\ &= \binom{3}{3}+\left[\binom{5}{4}-\binom{4}{4}\right]+\left[\binom{6}{4}-\binom{5}{4}\right]+\left[\binom{7}{4}-\binom{6}{4}\right]\\ &= \binom{3}{3}-\binom{4}{4}+\binom{7}{4}=\binom{7}{4}\end{aligned} \tag{7.45}$$

- Ahora, en general,

$$\begin{aligned}\sum_{i=k}^{n}\binom{i}{k} &= \binom{k}{k}+\binom{k+1}{k}+...+\binom{n}{k}\\ &= 1+\left[\binom{k+2}{k+1}-\binom{k+1}{k+1}\right]\\ &+\left[\binom{k+3}{k+1}-\binom{k+2}{k+1}\right]+...\\ &+\left[\binom{n+1}{k+1}-\binom{n}{k+1}\right]\\ &= \binom{n+1}{k+1}\end{aligned} \tag{7.46}$$

Ejemplo. Demostrar que para todo entero n positivo se tiene que

$$\binom{1}{1}+\binom{2}{1}+...+\binom{n}{1}=\frac{n+1}{2} \tag{7.47}$$

Solución:

$$\binom{n+1}{2}=\frac{(n+1)!}{2!(n-1)!}=\frac{(n+1)n(n-1)!}{2(n-1)!}=\frac{n(n+1)}{2} \tag{7.48}$$

$$\binom{n+1}{1}=\frac{n!}{1!(n-1)!}=\frac{n(n-1)!}{1(n-1)!}=n \tag{7.49}$$

Teorema. El número de combinaciones con r elementos tomados de un conjunto A de n elementos distintos, con $0 \leq r \leq n$, está dado por

$$C(n,r)=\frac{n!}{r!(n-r)!} \tag{7.50}$$

Demostración. Podemos construir las permutaciones con r elementos tomados de un conjunto de n elementos, con $0 \leq r \leq n$, en 2 etapas sucesivas:

- Construimos todas las combinaciones con r elementos tomados de un conjunto de n elementos;
- Para cada combinación con r elementos obtenemos todas sus permutaciones posibles.

Luego, usando el PM, el número de permutaciones con r elementos es igual al producto del número de combinaciones con r elementos tomados de una conjunto de n elementos, por el número de sus permutaciones, i.e.

$$\begin{aligned} P(n,r) &= C(n,r)P(r) \\ \therefore \quad C(n,r) &= \frac{P(n,r)}{P(r)} \\ &= \frac{n(n-1)(n-2)...(n-r+1)}{r(r-1)...1} \\ &= \frac{n!}{r!(n-r)!} \end{aligned} \tag{7.51}$$

Teorema. Teorema multimonial (caso $m = 3$. Si $a, b, c \in \mathbb{R}$ y n es un entero positivo, entonces

$$(a+b+c)^n = \sum_{i+j+k=n}^{n} \binom{n}{i\ j\ k} a^i b^j c^k \tag{7.52}$$

Demostración:

- Para concretar, primero evaluemos $(a+b+c)^{17}$. En ese caso, hay que evaluar $(a+b+c)^{17} = (a+b+c)...(a+b+c)$, con 17 factores idénticos. Entre otros estará el término $a^4b^6c^7$ pues la suma de esos exponentes es $4+6+7 = 17$, de donde

$$\begin{aligned} &\text{Como } a \text{ puede ser elegido en 4 de los 17 factores:} \\ &\text{Como } b \text{ puede ser elegido en 6 de los 17 factores:} \\ &\text{Como } c \text{ puede ser elegido en 7 de los 17 factores:} \end{aligned} \tag{7.53}$$

  tendremos

$$\binom{17}{4}\binom{13}{6}\binom{7}{7} = \frac{17!}{4!13!}\frac{13!}{6!7!}\frac{7!}{7!0!} = \frac{17!}{4!6!7!} \tag{7.54}$$

  entonces, en el desarrollo de $(a+b+c)^{17}$ está el el término

$$\frac{17!}{4!6!7!}a^4b^6c^7 \tag{7.55}$$

  Lo que se está haciendo es calcular el número de formas de ordenar las 17 letras *aaaabbbbbbccccccc*. Se concluye que el desarrollo de $(a+b+c)^{17}$ es la suma de todos los términos de la forma

$$\frac{17!}{i!j!k!}a^ib^jc^k \tag{7.56}$$

  donde i, j, k recorren todos los posibles enteros no-negativos tales que $i + j + k = 17$.
- En general, se tiene

$$(a+b+c)^n = \sum_{i+j+k=n}^{n} \binom{n}{i\ j\ k} a^i b^j c^k \tag{7.57}$$

número de solución	i	j	k
1	3	0	0
2	0	3	0
3	0	0	3
4	2	1	0
5	2	0	1
6	1	2	0
7	0	2	1
8	0	1	2
9	1	0	2
10	1	1	1

Tabla 7.4: Valores de i, j, k tales que $i + j + k = 3$.

Ejemplo. Evaluar $(x + y + z)^3$. Solución:

$$(x + y + z)^3 = \sum_{i+j+k=3}^{3} \binom{3}{i\ j\ k} x^i y^j z^k \tag{7.58}$$

donde el número de soluciones de $i + j + k = 3$ se obtiene con el teorema del pelotero con $k = 3$ y $t = 3$, resultando $z = C(k + (t-1), (t-1)) = C(3 + 2, 2) = C(5, 2) = 10$ sumandos. Los valores i, j, k son mostrados en la Tabla 7.4. Tenemos

$$\begin{aligned}(x + y + z)^3 &= \frac{3!}{3!0!0!}x^3y^0z^0 + \frac{3!}{0!3!0!}x^0y^3z^0 + \frac{3!}{0!0!3!}x^0y^0z^3 \\ &+ \frac{3!}{2!1!0!}x^2y^1z^0 + \frac{3!}{2!0!1!}x^2y^0z^1 + \frac{3!}{1!2!0!}x^1y^2z^0 \\ &+ \frac{3!}{0!2!1!}x^0y^2z^1 + \frac{3!}{0!1!2!}x^0y^1z^2 + \frac{3!}{1!0!2!}x^1y^0z^2 + \frac{3!}{1!1!1!}x^1y^1z^1\end{aligned} \tag{7.59}$$

operando y simplificando

$$\begin{aligned}(x + y + z)^3 &= x^3 + y^3 + z^3 \\ &+ 3x^2y^1 + 3x^2z^1 + 3x^2y^2 \\ &+ 3y^2z^1 + 3y^1z^2 + 3x^1z^2 + 6x^1y^1z^1\end{aligned} \tag{7.60}$$

7.5. Ejemplos usando principios básicos de conteo

Ejemplo. ¿De cuántas maneras puede un fotógrafo de boda ordenar un grupo de 6 personas si los novios deben salir juntos en la foto.

a) Los novios deben salir juntos en la foto;
b) Los novios no deben salir juntos en la foto;
c) La novia debe salir en algún puesto a la izquierda del novio.

Solución.

a) Los ordenamientos posibles se pueden representar con el siguiente esquema:

$$\begin{array}{cccccccl}
n & n & _ & _ & _ & _ & & \text{fila 1} \\
_ & n & n & _ & _ & _ & & \text{fila 2} \\
_ & _ & n & n & _ & _ & & \text{fila 3} \\
_ & _ & _ & n & n & _ & & \text{fila 4} \\
_ & _ & _ & _ & n & n & & \text{fila 5}
\end{array}$$

en donde n denota novio o novia, y $\_$ es un lugar para las restantes 6-2=4 personas. Cada fila representa una ubicación con los dos novios juntos. En cada fila hay 2! opciones para ubicar a los 2 novios juntos, y otras 4! opciones para ubicar a las demás personas, por lo que, usando el PM, se tienen $2! \cdot 4!$ opciones en cada fila. El número total de opciones para dicha foto será la suma de todos estos casos que, por ser sumandos iguales, se reduce al producto del número de opciones en cada fila por el número de filas. Lo que falta es determinar el número de filas posibles sin tener que hacer este esquema. Para ese fin, notar que la fila 1 es una cadena de la forma $n_1n_2x_3...x_6$, donde n_1n_2 son los novios que van juntos, mientras que $x_3, ..., x_6$ son las restantes $6 - 2 = 4$ personas. La fila 2 se puede obtener de la 1 desplazando un lugar hacia la derecha, la fila 3 se puede obtener de la fila 2 desplazando un lugar hacia la derecha, etc. Para llegar hasta el final, hay que hacer $6 - 2 = 4$ desplazamientos hacia la derecha. El número total de filas es igual al número total de desplazamientos hacia la derecha más la fila 1, o sea $6 - 2 + 1 = 5$. Finalmente, el número total de opciones para dicha foto es $z = 2! \cdot (6 - 2)! \cdot (6 - 2 + 1)$ y, sacando cuentas, $z = 2! \cdot 4! \cdot 5 = 240$.

b) Para el hogar.

c) Para el hogar.

d) Para el hogar.

Ejemplo. Determinar el número de ordenamientos posibles de un grupo de q personas donde p personas deben quedar juntas, con $p \leq q$. Solución. Generalizando el ejemplo anterior se tiene que:

- La primera fila está dada por la cadena $n_1n_2...n_px_{p+1}x_{p+2}...x_q$, que representa una selección de q personas ubicadas al inicio, donde $n_1n_2...n_p$ es la subcadena con las p personas que van juntas, mientras que $x_{p+1}x_{p+2}...x_q$ es la subcadena con las restantes $q - p$ personas;
- En cada fila hay $p!$ opciones para ubicar a las p personas que van juntas, y otras $(q - p)!$ opciones para ubicar a las restantes $q - p$ personas;
- El número de filas posibles con p personas juntas en cada una es $(q - p + 1)$;
- Finalmente, el número total de opciones está dado por: $z = p! \cdot (q - p)! \cdot (q - p + 1)$

Ejemplo. Consigna: elegir una delegación de 4 personas de entre un total de 12 estudiantes para asistir a un congreso. Hallar:

a) De cuántas maneras se puede elegir la delegación? (sin restricciones);

b) Idem pero considerando que hay 2 estudiantes que quieren ir pero se niegan a estar en la delegación simultáneamente;

c) Idem pero considerando que hay 2 estudiantes que asistirán al congreso sólo si van juntos;

d) Idem pero considerando que hay 2 estudiantes que no les preocupa mucho asistir pero, si van, se niegan a estar en la delegación simultáneamente.

Solución:

a) Se tiene $z_a = C(12, 4) = 495$;

b) Sean los estudiantes A y B que quieren ir pero se niegan a estar juntos. Hacemos 2 etapas. Primero incluimos al estudiante A en la delegación y excluimos al estudiante B. Entonces restan elegir 4 - 1 = 3 delegados de un total de 12 - 1 (pues A que ya está) - 1 (pues a B lo echamos), o sea, $z_1 = C(10, 3) = 120$. Ahora incluimos al estudiante B en la delegación y excluimos al estudiante A. Es lo mismo que antes por lo que $z_2 = C(10, 3) = 120$. Finalmente usando el Principio de la Suma (PS), el total de opciones es $z_b = z_1 + z_2 = 2C(10, 3) = 240$.

c) Sean los estudiantes A y B los que solo irán si van juntos. Hacemos 2 etapas. Primero, si incluimos a ambos estudiantes A y B en la delegación, entonces sólo restan elegir a otros 2 delegados de un total de 12-2=10 (porque A y B que ya están), lo que da $z_3 = C(10, 2) = 45$ opciones. Luego excluimos a ambos estudiantes A y B en la delegación, por lo que hay que elegir a 4 delegados de un total de 12-2=10 (porque A y B fueron excluidos), lo que se agregan otras $z_4 = C(10, 4) = 210$ opciones. Finalmente, usando el PS, el total es $z_c = z_3 + z_4 = C(10, 2) + C(10, 4) = 45 + 210 = 255$.

d) Sean los estudiantes A y B que no les preocupa mucho asistir pero, si van, se niegan a estar en la delegación simultáneamente. Una manera de resolver esto es usar el PIE, *i.e.* considerar el total de las combinaciones sin restricciones (inciso-a), es decir, $z_a = C(12, 4) = 495$, y a ese total le restamos el número de delegaciones en las que A y B aparecen juntos, dado por $z_3 = C(10, 2) = 45$ ya hallado. Con todo esto se obtiene $z_d = 495 - 45 = 450$. Verificación: otro razonamiento es sumar el número de opciones cuando A y B quieren ir pero se niegan a estar juntos (inciso-b) con el número de opciones cuando excluimos A y B de la delegación, o sea, $z'_d = z_b + z_4 = 2C(10, 3) + C(10, 4) = 240 + 210 = 450$, y se llega al mismo resultado.

Ejemplo. [Rosen: ejemplo 16 (pág. 444), y Problema 45 (pág. 448)]. Sea R una relación en un conjunto finito A de n elementos. Utilice un argumento de conteo para demostrar que el número máximo de:

- Relaciones $z_1 = 2^{n^2}$;
- relaciones reflexivas $z_2 = 2^{(n^2-n)}$;
- relaciones simétricas $z_3 = 2^n \cdot 2^{(n^2-n)/2}$;
- relaciones antisimétricas $z_4 = 2^n \cdot 3^{(n^2-n)/2}$.

Solución.

- La base 2 surge porque cada par ordenado (x, y) del producto cartesiano $A \times A$ tiene 2 posibilidades en una relación dada, o bien estar, o bien no estar. Como hay $n \cdot n$ pares ordenados en el producto cartesiano $A \times A$, se concluye que hay 2^{n^2} opciones;
- En una relación R en un conjunto A de n elementos, los pares ordenados que tienen componentes iguales (de la forma (x, x)) son n, y los restantes serán $(n^2 - n)$. Al formar todas las relaciones reflexivas posibles, esos pares remanentes pueden o no estar y por eso hay $2^{(n^2-n)}$ opciones;

- En una relación R en un conjunto A de n elementos, los pares ordenados que tienen componentes iguales (de la forma (x, x)) son n, estos pueden (o no) estar en una relación simétrica, por lo que tenemos un factor 2^n. Los restantes pares ordenados que se pueden formar de $A \times A$ son $(n^2 - n)$. Al contar todas las relaciones simétricas posibles, si un par ordenado $(x, y) \in R$, con $x \neq y$, entonces también hay que incluir al par simétrico (y, x). Luego, sólo disponemos de la mitad de los pares iniciales, i.e. $(n^2 - n)/2$, los cuales pueden (o no) estar. En total tenemos $2^n \cdot 2^{(n^2-n)/2}$ opciones;
- Por empezar, podemos (o no) incluir los pares reflexivos (x, x)en una relación antisimétrica, por lo que tenemos un factor 2^n. En los restantes pares ordenados (x, y), con $x \neq y$, hay 3 opciones: o bien colocar (x, y) sólo, o bien colocar (y, x) sólo, o bien no colocar (x, y) ni (y, x). En total tenemos $2^n \cdot 3^{(n^2-n)/2}$ opciones.

Ejemplo. Sea R una relación definida en el conjunto $A = \{a\}$. Aplique las fórmulas de conteo del ejemplo anterior, y obtenga cada relación posible.
Solución.

- El número de relaciones posibles R es $z_1 = 2^{1^2} = 2^1 = 2$, y están dadas por $R_1 = \emptyset$, $R_2 = \{(a, a)\}$;
- El número de relaciones R reflexivas es $z_2 = 2^{(1^2-1)} = 2^{1-1} = 2^0 = 1$;
- El número de relaciones R simétricas es $z_3 = 2^1 \cdot 2^{(1^2-1)/2} = 2 \cdot 2^{0/2} = 2$;
- El número de relaciones R antisimétricas es $z_4 = 2^1 \cdot 3^{(1^2-1)/2} = 2 \cdot 3^{0/2} = 2$.

Ejemplo. Sea R una relación definida en el conjunto $A = \{a, b\}$. Aplique las fórmulas de conteo del ejemplo anterior, y obtenga cada relación posible.
Solución.

- El número de relaciones R que se pueden definir en el conjunto A dado es $z_1 = 2^{2^2} = 2^4 = 16$, y son las mostradas en la Tabla 7.5.
- El número de relaciones R reflexivas que se pueden definir en el conjunto A dado es $z_2 = 2^{(2^2-2)} = 2^{4-2} = 2^2 = 4$;
- El número de relaciones R simétricas que se pueden definir en el conjunto A dado es $z_3 = 2^2 \cdot 2^{(2^2-2)/2} = 4 \cdot 2^{(4-2)/2} = 4 \cdot 2^1 = 8$;
- El número de relaciones R antisimétricas que se pueden definir en el conjunto A dado es $z_4 = 2^2 \cdot 3^{(2^2-2)/2} = 4 \cdot 3^{(4-2)/2} = 4 \cdot 3^1 = 12$.

7.6. Principios del palomar

Veremos a continuación 3 formas del Principio del Palomar (PP).

7.6.1. Primera forma del principio del palomar

Definición. Primera forma del PP. Suponga que m palomas vuelan a n palomares. Si hay más palomas que palomares (i.e. $m > n$), entonces algún palomar debe contener, al menos, a 2 palomas.

relacioón R	matriz $M(R)$	reflexiva	simétrica	antisimétrica
$R_1 = \emptyset$	$M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	-	1	1
$R_2 = \{(a,a)\}$	$M_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$	-	2	2
$R_3 = \{(a,b)\}$	$M_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$	-	-	3
$R_4 = \{(b,a)\}$	$M_4 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$	-	-	4
$R_5 = \{(b,b)\}$	$M_5 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$	-	3	5
$R_6 = \{(a,a),(a,b)\}$	$M_6 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$	-	-	6
$R_7 = \{(a,a),(b,a)\}$	$M_7 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$	-	-	7
$R_8 = \{(a,a),(b,b)\}$	$M_8 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	4	8
$R_9 = \{(a,b),(b,a)\}$	$M_9 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	-	5	-
$R_{10} = \{(a,b),(b,b)\}$	$M_{10} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$	-	-	9
$R_{11} = \{(b,a),(b,b)\}$	$M_{11} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$	-	-	10
$R_{12} = \{(a,a),(a,b),(b,a)\}$	$M_{12} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	-	6	-
$R_{13} = \{(a,a),(a,b),(b,b)\}$	$M_{13} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	2	-	11
$R_{14} = \{(a,a),(b,a),(b,b)\}$	$M_{14} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	3	-	12
$R_{15} = \{(a,b),(b,a),(b,b)\}$	$M_{15} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	-	7	-
$R_{16} = \{(a,a),(a,b),(b,a),(b,b)\}$	$M_{16} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$	4	8	-

Tabla 7.5: Todas las relaciones R posibles sobre el conjunto $A = \{a, b\}$ y su clasificación.

Observación. El PP, en cualquiera de sus formas, no dice cómo localizar el palomar con al menos 2 palomas, solo asegura su existencia.

Observación. Para usar el PP hay que decidir quiénes son las palomas y quiénes son los palomares.

Ejemplo. Hay 10 personas con los nombre Germán (G), Javier (J), Luciana (L), y los apellidos Aimar (A), Ciaraviglio, y Mascherano (M). Probar que, al menos, 2 personas tienen el mismo nombre y apellido.
Solución: vemos que hay $3 \cdot 3 = 9$ nombres completos para las 10 personas (e.g. tres posibles son LA, GC, y JM). En este caso, las palomas son las personas $m = 10$, y los palomares son los nombres completos $n = 9$. Entonces, usando el PP, algún mismo nombre completo se asigna, al menos, a 2 personas.

7.6.2. Segunda forma del principio del palomar

Definición. Segunda forma del PP. Sean los conjuntos finitos X e Y, con $m = |X|$ y $n = |Y|$, y una función $f\colon X \to Y$. Si el número de elementos del dominio fuera mayor al del codominio (i.e. $m > n$), entonces debe ser $f(x_i) = f(x_j)$ para, al menos, algún par de elementos $x_i, x_j \in X$, con $x_i \neq x_j$.

Observación. Cuando el número de elementos del dominio es mayor al del codominio (i.e. $m > n$), entonces la función $f(x)$ no es inyectiva pues $y = f(x_i) = f(x_j)$ para, al menos un par de elementos $x_i, x_j \in X$, con $x_i \neq x_j$, indica que la preimagen de y no es única.

Observación. La segunda forma se reduce a la primera forma si X es el conjunto de las palomas, Y es el conjunto de palomares, y la funcón f es la función que asigna la paloma x a un palomar $f(x)$, con $m = |X|$ y $n = |B|$. En ese caso, por el PP en su primera forma, si $m > n$, entonces al menos 2 palomas $x_1, x_2 \in X$ se asignan a un mismo palomar $f(x)$, i.e. $f(x_1) = f(x_2)$ con $x_1 \neq x_2$.

7.6.3. Tercera forma del principio del palomar

Teorema. Tercera forma del PP. Sean los conjuntos finitos X e Y, y una función $f : X \to Y$, con $m = |X|$ y $n = |Y|$. Sea $k =$ techo (n/m), entonces hay k elementos del dominio $x_1, x_2, ..., x_k$ tales que $f(x_1) = f(x_2) = ... = f(x_k)$.

Demostración (por contradicción):

Suponemos que la conclusión fuera falsa, i.e. cuando mucho hay

- $(k-1)$ valores del dominio tales que $f(x) = y_1$;
- $(k-1)$ valores del dominio tales que $f(x) = y_2$; etc.;
- $(k-1)$ valores del dominio tales que $f(x) = y_n$;

Entonces, la cantidad de elementos del codominio seria $(k-1)n$. En ese caso, y como $k = \lceil m/n \rceil \leq m/n$, se tiene

$$n(k-1) = nk - n < nk \leq n(m/n) = m \qquad \therefore \qquad n(k-1) < m \tag{7.61}$$

O sea, el número de elementos en el dominio de la función f sería menor a la cantidad de elementos del conjunto X. Pero esto no es posible pues, en ese caso, f no sería una función.

Ejemplo. Demostrar que en cualquier grupo de 6 personas o más hay, al menos, 3 personas que mutuamente, o bien se conocen, o bien no se conocen.
Solución: sean las 6 personas P_1, P_2, ..., P_6. Hay 5 pares posibles (P_1, P_2), (P_1, P_3), (P_1, P_4), (P_1, P_5), (P_1, P_6), que, o bien se conocen, o bien no se conocen. Por la tercera forma del PP hay $\lceil 5/2 \rceil = 3$ pares de personas (P_1, P_i), (P_1, P_j), (P_1, P_k) con un mismo valor (o bien se conocen, o bien no se conocen). Ahora ubicamos a esos 3 pares de personas en 2 habitaciones:

- En la habitación A ubicamos a las 3 personas P_i, P_j, P_k que conocen a P_1:
  - Si, al menos, un par entre P_i, P_j, P_k se conocen entre si, entonces, ese par más P_1 constituye un grupo de 3 personas que se conocen;
  - En caso contrario, P_i, P_j, P_k no se conocen entre si, por lo que ahora tenemos un grupo de 3 personas que no se conocen entre si.

- En la habitación B ubicamos a las 3 personas P_i, P_j, P_k que no conocen a P_1:
  - Si, al menos, un par entre P_i, P_j, P_k no se conocen entre si, entonces, ese par más P_1 constituye un grupo de 3 personas que no se conocen;
  - En caso contrario, P_i, P_j, P_k se conocen entre si, por lo que otra vez tenemos 3 pares de personas que se conocen entre si.

CAPÍTULO 8

Relaciones

Contents

8.1. Relaciones binarias y relaciones

8.1.1. Relación binaria

Definición. Sean dos conjuntos A y B. *Relación Binaria* (Relación Binaria (RB)) (def.): una relación binaria R de A en B es un subconjunto del producto cartesiano $A \times B$.

Notación: $R = \{(a, b) \mid (a, b) \in A \times B\}$, donde $a \in A$ y $b \in B$. Se denota aRb cuando $(a, b) \in R$, y se dice que el elemento a está relacionado con el elemento b mediante R. En caso contrario, se denota con $a \not R b$ cuando $(a, b) \notin R$.

Observación. Una función $f : A \to B$ es un caso especial de una RB, en donde R asigna exactamente **un** elemento $b \in B$ a **cada** elemento $a \in A$.

8.1.2. Relación en un conjunto

Definición. *Relación* (def.): una relación en un conjunto A es una RB de A en A, i.e. $R = \{(a, b) \mid (a, b) \in A \times A\}$, donde $a, b \in A$.

8.2. Propiedades de una relación

8.2.1. Relación reflexiva

Definición. Relación reflexiva (def.): una relación R en un conjunto A es reflexiva si todos los pares ordenados de la forma (a, a) pertenecen a la relación R. **Notación**: una relación R en un conjunto A es reflexiva si $(a, a) \in R$, para todo $a \in A$.

Ejemplo. Como $n|n$ para cada entero positivo n, se concluye que la relación "divide a" en el conjunto de los enteros positivos es reflexiva.

8.2.2. Relación simétrica

Definición. Relación simétrica (def.): una relación R en un conjunto A es simétrica si $(a, b) \in R$, entonces $(b, a) \in R$, para todo $a, b \in A$. **Notación**: una relación R en un conjunto A es simétrica si $(a, b) \in R \to (b, a) \in R$, para todo $a, b \in A$. **Observación**: en una relación simétrica no importan la presencia o ausencia de los pares reflexivos.

8.2.3. Relación antisimétrica

Definición. Relación antisimétrica (def. 1): una relación R en un conjunto A es antisimétrica si $(a, b) \in R \wedge a \neq b$, entonces $(b, a) \notin R$, para todos $a, b \in A$. **Relación antisimétrica** (def. 2): una relación R en un conjunto A es antisimétrica si $(a, b) \in R \wedge (b, a) \in R$, entonces $a = b$, para todo $a, b \in A$. **Observación**: en una relación antisimétrica no importan la presencia o ausencia de los pares reflexivos. **Notación**: una relación R en un conjunto A es antisimétrica si $((a, b) \in R \wedge (b, a) \in R) \to a = b$, para todo $a, b, c \in A$.

Ejemplo. Como $n|n$ para cada entero positivo n, se concluye que la relación "x divide a y" es reflexiva cuando x, y pertenecen al conjunto de los enteros positivos.

Observación.

a) Los términos simétrico y antisimétrico no son opuestos entre si. Una relación R en un conjunto A puede tener simultáneamente ambas propiedades (poco frecuente), o carecer de ambas (bastante más frecuente);
b) Si una relación R en un conjunto A contiene algún par ordenado (a, b) tal que $a \neq b$, entonces no puede se simétrica y antisimétrica a la vez.

Ejemplo. Analizar las siguientes relaciones R en el conjunto $A = \{a, b, c\}$ dadas por la Ec. (8.1).

$$\begin{aligned} R_1 &= \{(a,a),(b,b),(c,c)\} : \text{es reflexiva, es simétrica, y es antisimétrica;} \\ R_2 &= \{(a,a),(b,b)\} : \text{no es reflexiva, es simétrica, y es antisimétrica;} \\ R_3 &= \{(a,a),(a,b)\} : \text{no es reflexiva, no es simétrica, y es antisimétrica;} \\ R_4 &= \{(a,a),(a,b),(b,a)\} : \text{no es reflexiva, es simétrica, pero no es antisimétrica.} \end{aligned} \tag{8.1}$$

Ejemplo. Contrapositiva de la definición de relación antisimétrica. Escriba la contrapositiva de: una relación R en un conjunto A es antisimétrica si $(a, b) \in R \wedge (b, a) \in R$, entonces $a = b$, para todo $a, b \in A$.

Solución: una relación R en un conjunto A es antisimétrica si $a \neq b$, entonces $(a, b) \notin R \vee (b, a) \notin R$, para todo $a, b \in A$. En otras palabras, R no es antisimétrica cuando $a \neq b$, y se tiene que tanto aRb como bRa son T, para todo $a, b \in A$. Esto equivale al caso T $\rightarrow$ F, que es F (verlo escribiendo una TV).

8.2.4. Relación transitiva

Definición. Relación transitiva (def.): una relación R en un conjunto A es transitiva, si $(a, b) \in R$ y $(b, c) \in R$, entonces se tiene también $(a, c) \in R$, para todo $a, b, c \in A$. **Notación**: una relación R en un conjunto A es transitiva si $((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R$, para todo $a, b, c \in A$.

Ejemplo. Sea la relación $R = \{(a, b) \mid a$ divide a b para todo $a, b \in \mathbb{Z}$. Se tiene:

i) Si a divide a b, usando la definición de divide se tiene: como aRb, entonces $b = \alpha a$, con $\alpha \in \mathbb{Z}$;
ii) Si b divide a c, usando la definición de divide se tiene: como bRc, entonces $c = \beta b$, con $\beta \in \mathbb{Z}$;
iii) Reemplazando $c = \beta b = \beta\alpha a = \gamma a$, o sea, $c = \gamma a$, es decir, c divide a a, donde $\gamma = \alpha\beta$, con $\gamma \in \mathbb{Z}$;
iv) Eso ocurre para todo aRb y bRc, por lo que la relación "a divide a b" es transitiva en $\mathbb{Z}$.

Ejemplo. Sean R y S relaciones en un conjunto A. Demuestre o dé un contraejemplo en cada caso:

1) Si R y S son transitivas, entonces $R \cup S$ ¿es también transitiva? Rpta: es F, contraejemplo: sea el conjunto $A = \{1, 2, 3\}$, y las relaciones transitivas $R = \{(1, 2)\}$ y $S = \{(2, 3)\}$. Se tiene $R \cup S = \{(1, 2), (2, 3)\}$ que no es transitiva.

2) Si R y S son transitivas, entonces $R \cap S$ ¿es también transitiva?
3) Si R y S son transitivas, entonces $R \circ S$ ¿es también transitiva?
4) Si R es transitiva, entonces R^{-1} ¿es también transitiva? Rpta. Para todo $a, b, c \in A$ se tiene
   - Si $aR^{-1}b$ y $bR^{-1}c$, entonces, por definición de R^{-1}, debe ser bRa y cRb, o sea, cRb y bRa;
   - Como R es transitiva, debe ser cRa;
   - Por definición de relación inversa, debe ser $aR^{-1}c$;
   - Se concluye que toda vez que $aR^{-1}b$ y $bR^{-1}c$, debe ser $aR^{-1}c$, por lo que R^{-1} también es transitiva.
5) Si R es reflexiva, entonces R^{-1} ¿es también reflexiva? Rpta. Para todo $a \in A$ se tiene
   - Si R es reflexiva, entonces aRa para todo $a \in A$. Por definición de R^{-1}, debe ser $aR^{-1}a$ para todo $a \in A$, por lo que $R \subseteq R^{-1}$;
   - Si R^{-1} es reflexiva, entonces $aR^{-1}a$ para todo $a \in A$. Por definición de R^{-1}, debe ser aRa para todo $a \in A$, por lo que $R^{-1} \subseteq R$. Por eso, $R = R^{-1}$;
   - Por último, si R es reflexiva, entonces aRa para todo $a \in A$. Y como $R = R^{-1}$, debe ser $aR^{-1}a$ para todo $a \in A$.
6) Si R y S son reflexivas, entonces $R \cup S$ ¿es también reflexiva? Rpta. Para todo $a, b \in A$ se tiene
   - Si $R \cup S$ es reflexiva, entonces $(a, a) \in (R \cup S)$ para todo $a \in A$;
   - Por definición de la unión se tiene $(a, a) \in R \vee (a, a) \in S$ para todo $a \in A$;
   - Como R y S son reflexivas, cada una es T;
7) Si R y S son reflexivas, entonces $R \cap S$ ¿es también reflexiva? Rpta. Para todo $a, b \in A$ se tiene
   - Si $R \cap S$ es reflexiva, entonces $(a, a) \in (R \cap S)$ para todo $a \in A$;
   - Por definición de la intersección se tiene $(a, a) \in R \wedge (a, a) \in S$ para todo $a \in A$;
   - Y como R y S son reflexivas, cada una es T;
8) Si R y S son reflexivas, entonces $R \circ S$ ¿es también reflexiva? Rpta. Para todo $a \in A$ se tiene
   - Como R es reflexiva, entonces $(a, a) \in R$ para todo $a \in A$;
   - Como S es reflexiva, entonces $(a, a) \in S$ para todo $a \in A$;
   - En esas condiciones, $R \circ S$ se reduce a $\{(a, a) \mid \forall a \in A$, por lo que $R \circ S$ también es reflexiva.

8.3. Relaciones de orden parcial y total

8.3.1. Relación de orden parcial

Definición. se dice que una relación R en un conjunto A es una Relación de Orden Parcial (ROP) si es reflexiva, antisimétrica, y transitiva.

8.3.2. Relación de orden total

Definición. Elementos comparables e incomparables. Sea una ROP R sobre un conjunto A, y sean los elementos $a, b \in A$. Se denota con $a \preceq b$ para indicar que $(a, b) \in R$, notación que sugiere interpretar a la ROP R como un ordenamiento de los elementos de A. Si en una ROP R en un conjunto A se verifica que $a \preceq b$ o bien $b \preceq a$, entonces se dice que los elementos a y b de A son comparables y, en el caso contrario se dice que son elementos incomparables.

Definición. Relación de orden total: una relación R en un conjunto A es una Relación de Orden Total (ROT) cuando todos los elementos de A son comparables.

Ejemplo.

1) **Ejemplo de orden total**: la relación $\leq$ en los enteros positivos es una ROT, pues para todos los enteros $a, b \in \mathbb{Z}$ se tiene, o bien $x \leq y$, o bien $y \leq x$;

2) **Ejemplo de orden parcial**: la relación $a|b$ en los enteros positivos es una ROP porque tiene elementos tanto comparables como incomparables, e.g. 3 y 6 son comparables (pues 3 divide a 6), pero 2 y 3 son incomparables (pues 2 no divide a 3).

8.4. Relación inversa y composición de relaciones

8.4.1. Relación inversa

Definición. Relación inversa. Sea una relación R de un conjunto A en otro B. La relación inversa se denota con R^{-1} y es la relación de B en A definida por $R^{-1} = \{(b, a) \mid (a, b) \in R\}$, con $a \in A$ y $b \in B$.

Ejemplo. Sean los conjuntos $A = \{2, 3, 4\}$ y $B = \{3, 4, 5, 6, 7\}$, y las relaciones:

a) $R = \{(a, b) \mid \text{si } a \text{ divide a } b\}$. En este caso queda R = { (2,4), (2,6), (3,3), (3,6), (4,4) }.
b) $R^{-1} = \{(b, a) \mid \text{si } b \text{ es divisible por } a\}$. Ahora R^{-1} = { (4,2), (6,2), (3,3), (6,3), (4,4) }.

8.4.2. Composición de dos relaciones

Definición. Composición de dos relaciones. Sean los conjuntos A, B, y C, y sean las relaciones R_1, de A hacia B, y R_2, de B hacia C. La composición de R_1 y R_2 se denota con $R_2 \circ R_1$, y es la relación de A hacia C definida con $R_2 \circ R_1 = \{(a, c) \mid (a, b) \in R_1 \wedge (b, c) \in R_2\}$, con $a \in A$, $b \in B$, y $c \in C$.

Ejemplo. Sean los conjuntos $A = \{\alpha, \beta, \gamma\}$, $B = \{1, 2, 3, 4\}$, y $C = \{t, u\}$, y las relaciones: $R_1 = \{(\alpha, 2), (\alpha, 4), (\beta, 1), (\gamma, 2), (\gamma, 3), (\gamma, 4)\}$, $R_2 = \{(1, t), (2, t), (4, u)\}$. En este caso, resulta la composición $R_2 \circ R_1 = \{(\alpha, t), (\alpha, u), (\beta, t), (\gamma, t), \gamma, u)\}$, ver Fig. 8.1.

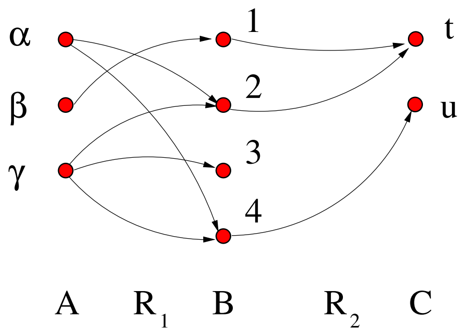

Figura 8.1: Diagramas de flechas de las relaciones R_1, R_2, y de la composición $R_2 \circ R_1$.

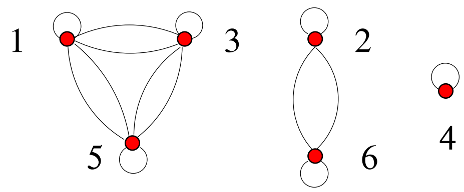

Figura 8.2: La relación R es una RE.

8.5. Relaciones de equivalencia

8.5.1. Relación de equivalencia

Definición. *Relación de Equivalencia*: es una relación R sobre un conjunto A que es reflexiva, simétrica, y transitiva.

Ejemplo. Sea el conjunto $A = \{1, 2, 3, 4, 5, 6\}$ y la Relación de Equivalencia (RE) dada por la Ec. (8.2). Se tiene que esta R es una RE. Verlo más rápidamente analizando la Fig. 8.2.

$$R = \{(1,1),(1,3),(1,5),(2,2),(2,6),(3,5), (4,4),(5,5),(6,6),(3,1),(5,1),(6,2),(5,3)\} \tag{8.2}$$

8.5.2. Partición

Definición. *Partición* (def.): una partición $\mathcal{S}$ de un conjunto A es una colección de n subconjuntos A_k para $k = 1, 2, ..., n$, llamados también como bloques, tales que: (i) cada bloque A_k es no vacío; (ii) los bloques son disjuntos dos a dos; y (iii) la unión de todos los bloques recupera al conjunto A.

Notación: los subconjuntos (bloques) A_k definen la partición

$$\mathcal{S} = \{A_k \mid \text{para } k = 1, 2, ..., n\}$$

con n entero positivo, cuando

$$\begin{cases} A_k \neq \emptyset & \text{para } k = 1, 2, ..., n; \\ A_i \cap A_j = \emptyset & \text{con } i \neq j \text{, para } i, j = 1, 2, ..., n; \\ \bigcup_{k=1}^{n} A_k = A & . \end{cases} \tag{8.3}$$

Ejemplo. Sea el conjunto $A = \{a, b, c, d, e, f, g, h, i, j\}$, con $|A| = 10$, y los subconjuntos (bloques) $A_1 = \{a, b, c\}$, $A_2 = \{d, e\}$, $A_3 = \{f\}$, y $A_4 = \{g, h, i, j\}$. Como se cumplen las tres condiciones

- Cada bloque A_k es no vacío, para $k = 1, 2, 3, 4$;
- Todas las intersecciones de los bloques de a pares son vacías, i.e. $A_1 \cap A_2 = A_1 \cap A_3 = A_1 \cap A_4 = \emptyset$, $A_2 \cap A_3 = A_2 \cap A_4 = \emptyset$, y $A_3 \cap A_4 = \emptyset$;
- $A_1 \cup A_2 \cup A_3 \cup A_4 = A$;

entonces la colección de conjuntos (bloques) A_1, A_2, A_3, y A_4, define una partición $\mathcal{S}$ del conjunto A.

8.5.3. Relaciones de equivalencia y particiones

Observación. Si $\mathcal{S}$ es una partición de un conjunto A, entonces se la puede emplear para construir una RE en el conjunto A.

Ejemplo. Sea el conjunto de 6 pelotas $A = \{1, 2, 3, 4, 5, 6\}$, numeradas y pintadas con los colores rojo (*red*, pelotas 1, 3, 5), verde (*green*, pelotas 2,6), y amarillo (*yellow*, pelota 4). Si las separamos en los bloques obtenemos la Ec. (8.4). entonces la colección $S = \{A_1, A_2, A_3\}$ define una partición de A, donde la relación aRb indica que las pelotas a y b son del mismo color, donde R está dada por la Ec. (8.5). Se observa que R es una RE. Verlo quizás más rápidamente analizando la Fig. 8.2.

$$\begin{aligned} A_1 &= \{x \mid x \text{ es una pelota roja }\} \\ A_2 &= \{x \mid x \text{ es una pelota verde }\} \\ A_3 &= \{x \mid x \text{ es una pelota amarilla}\} \end{aligned} \tag{8.4}$$

$$R = \{(1,1), (1,3), (1,5), (2,2), (2,6), (3,5), (4,4), (5,5), (6,6), (3,1), (5,1), (6,2), (5,3)\} \tag{8.5}$$

Teorema. (teor. 3.2.1, pág. 125 Johnsonbaugh). Sea $\mathcal{S}$ una partición en un conjunto A. Se define la relación R en A como sigue: aRb si y solo si los elementos a y b pertenecen a un mismo bloque A_k de la partición $\mathcal{S}$. En esas condiciones, la relación R es una RE. *Demostración*:

- Sea un elemento $a \in A$. Por la definición de partición $\mathcal{S}$, un elemento a debe pertenecer a algún conjunto A_k de la partición $\mathcal{S}$, por lo que aRa. Además, se observa que eso ocurre para todo elemento $a \in A$. Por eso, la relación R es reflexiva;

- Suponga que aRb. Eso significa que ambos elementos a y b están en un mismo bloque A_k de la partición $\mathcal{S}$. Por eso, se concluye que también bRa. Otra vez, eso vale para todo $a, b \in A$, por lo que la relación R es simétrica;
- Suponga que aRb y que bRc. En el primer caso, significa que ambos elementos a y b pertenecen a un mismo bloque A_i de la partición $\mathcal{S}$, mientras que en el segundo caso significa que los elementos b y c pertenecen a algún otro bloque A_j, posiblemente con $i \neq j$. Pero el elemento b pertenece exactamente a un bloque de la partición $\mathcal{S}$, por lo que debe ser $i = j$. En consecuencia, ambos elementos a y c estarán en el mismo bloque A_i y, por ende, aRc. Otra vez, esto vale para todo $a, b, c \in A$, por lo que la relación R es transitiva.

8.5.4. Conjunto relativo de un elemento en una relación de equivalencia

Si $\mathcal{S}$ es una partición de un conjunto A, y R es una RE determinada por $\mathcal{S}$, entonces los bloques de la partición $\mathcal{S}$ pueden ser descriptos en términos de la RE expresada por R. Si A_k es un bloque genérico de la partición $\mathcal{S}$, y $a \in A_k$ le pertenece, entonces, por definición de partición, se tiene que A_k consta de todos los elementos x que están relacionados con a.

Definición. *Conjunto relativo en una* RE *de un elemento*: sea R una RE sobre un conjunto A, y un elemento p de A. El conjunto relativo en R del elemento p de A es el conjunto formado por todos los elementos $x \in A$ tales que xRp, y se denota con la Ec. (8.6).

$$[p] = \{x \mid xRp\} \tag{8.6}$$

Definición. *Clases de Equivalencia*: sea R una RE sobre un conjunto A. Los conjuntos relativos $[a]$ definidos por la partición $\mathcal{S}$ asociada con R se llaman las CE sobre el conjunto A.

Ejemplo. En el ejemplo de las pelotas numeradas y pintadas con los colores rojo (*red*, pelotas 1, 3, 5), verde (*green*, pelotas 2,6), y amarillo (*yellow*, pelota 4), tenemos la tres CE dadas en la Ec. (8.7). En general, los números de elementos en cada CE son diferentes entre si. Sugerencia: omitir el ter. 3.2.15 por inducir a confusión.

$$\begin{aligned} C_1 &= \{1, 3, 5\} = [1] = [3] = [5] \\ C_2 &= \{2, 6\} = [2] = [6] \\ C_3 &= \{4\} = [4] \end{aligned} \tag{8.7}$$

8.5.5. Clases de equivalencia y particiones

Teorema. Se R una RE en el conjunto A. Las afirmaciones listadas en la Ec. (8.8) son equivalentes.

$$\begin{array}{rll} \text{(i)} & aRb & ; \\ \text{(ii)} & [a] = [b] & ; \\ \text{(iii)} & [a] \cap [b] \neq \emptyset & ; \end{array} \tag{8.8}$$

Demostración:

1) (i) → (ii) Suponga que aRb. Para probar que $[a] = [b]$ mostraremos que $[a] \subseteq [b]$ y que $[b] \subseteq [a]$. Para eso hacemos:
   - Sea $x \in [a]$, entonces, por la definición de $[a]$, se concluye que xRa;
   - Como xRa, aRb, y R es transitiva, debe ser xRb, por lo que $x \in [b]$;
   - Como $x \in [a]$ y $x \in [b]$, para todo $x \in [a]$, debe ser $[a] \subseteq [b]$;
   - Al revés, sea $z \in [b]$, entonces, por la definición de $[b]$, se tiene que zRb;
   - Como R es simétrica, si aRb debe ser bRa;
   - Como zRb, bRa, y R es transitiva, debe ser zRa, con lo que $z \in [a]$;
   - Como $z \in [b]$ y $x \in [a]$, para todo $z \in [b]$, debe ser $[b] \subseteq [a]$;
   - Se concluye que $[a] = [b]$.
2) (ii) → (iii) Suponga que $[a] = [b]$. Como R es reflexiva, se tiene que aRa para todo $a \in A$. En ese caso, como $[a]$ es no vacia, se concluye $[a] \cap [b] \neq \emptyset$;
3) (iii) → (i) Suponga que $[a] \cap [b] \neq \emptyset$. Entonces existe un elemento c tal que $c \in [A] \wedge c \in [b]$, es decir, aRc y bRc. Por simetría, si bRc debe ser cRb. Entonces tenemos aRc, cRb, y R transitiva, por lo que debe ser aRb;
4) Como se cumplen (i) → (ii), (ii) → (iii), y (iii) → (i), las 3 afirmaciones son equivalentes.

8.6. Matrices en relaciones

8.6.1. Matriz de una relación binaria

Definición. *Matriz de una relación binaria* (def.). Sean los conjuntos finitos A y B, donde $m = |A|$ y $m = |B|$. La matriz de una relación binaria R de A en B es la matriz de bits $\boldsymbol{M}(R)$ de $m \times n$ definida por la Ec. (8.9).

$$[\boldsymbol{M}]_{i,j} = \begin{cases} 1 & \text{si } (a_i, b_j) \in R; \\ 0 & \text{si } (a_i, b_j) \notin R; \end{cases} \tag{8.9}$$

para $i = 1, 2, ..., m$ y $j = 1, 2, ..., n$.

Observación.

- Las filas de $\boldsymbol{M}$ se corresponden con los elementos del conjunto A en algún orden arbitrario pero fijo;
- Las columnas de $\boldsymbol{M}$ se corresponden con los elementos del conjunto B en algún orden arbitrario pero fijo;
- En general la matriz $\boldsymbol{M}$ de una relación binaria es rectangular excepto en una relación R definida sobre un conjunto A.

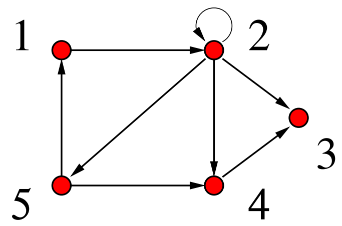

Figura 8.3: Diagrafo asociado a la relación R del ejemplo 8.6.3.

Ejemplo. Sea los conjuntos $A = \{\beta, \gamma, \delta\}$ y $B = \{a, b, c, d\}$, y la relación binaria $R = \{(\beta, b), (\beta, d), (\gamma, b), (\gamma, d)\}$, entonces la matriz de la relación binaria está dada por la Ec. (8.10).

$$\boldsymbol{M} = \begin{array}{c c} & \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{array}{c} \beta \\ \gamma \\ \delta \end{array} & \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array} \tag{8.10}$$

8.6.2. Matriz de una relación en un conjunto

Es un caso particular de la matriz de una relación binaria.

Definición. *Matriz de una relación en un conjunto* (def.). Sea una relación R en un conjunto finito A de n elementos. La matriz de la relación R es la matriz de bits $\boldsymbol{M}$, cuadrada de $n \times n$, dada por la Ec. (8.11).

$$[\boldsymbol{M}]_{i,j} = \begin{cases} 1 & \text{si } (a_i, a_j) \in R; \\ 0 & \text{en caso contrario;} \end{cases} \tag{8.11}$$

donde $i, j = 1, 2, ..., n$, y los elementos $a_i, a_j \in A$.

8.6.3. Relaciones, digrafos, y trayectorias

Definición. Digrafo asociado a una relación finita. Sea R una relación en un conjunto finito A. El digrafo G asociado con la relación R se traza de la siguiente manera: (i) se representa cada elemento a de A con un vértice (o punto); (ii) para cada par ordenado $(a, b) \in R$ se traza una flecha (lado o arco orientado) desde el vértice a hacia el b, con $a, b \in A$.

Definición. Trayectoria. Sea R una relación en un conjunto A. Una trayectoria (o camino, o ruta) de longitud n en R desde el elemento a hacia el b es una sucesión finita P : $a, x_1, x_2, ..., x_{n-1}, b$ que empieza en a, termina en b, y tal que $aRx_1 \wedge x_1Rx_2 ... \wedge x_{n-1}Rb$. **Ciclo**: es una trayectoria que empieza y termina en un mismo vértice.

Observación. Una ruta de longitud n involucra $(n + 1)$ elementos de A aunque no necesariamente distintos.

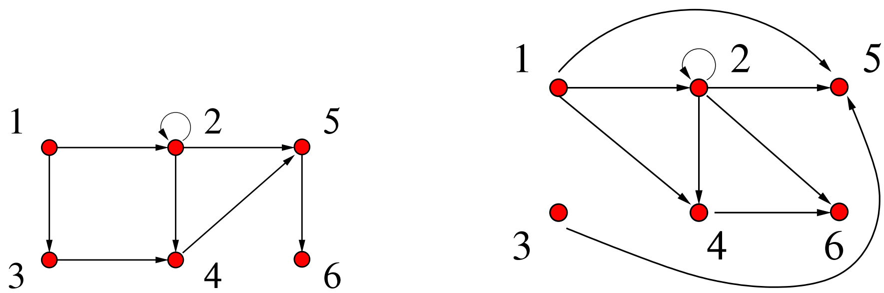

Figura 8.4: Digrafos asociados a las relaciones R y R^2 del ejemplo 8.6.3.

Ejemplo. Sea el conjunto $A = \{1, 2, 3, 4, 5\}$, y la relación $R = \{(1, 2), (2, 2), (2, 3), (2, 4), (4, 3), (5, 1), (5, 4)\}$, ver Fig. 8.3. Tres trayectorias cualesquiera en R son: P_1: 1, 2, 5, 4, 3, P_2: 1, 2, 5, 1, y P_3: 2,2, donde $|P_1| = 4$, $|P_2| = 3$, y $|P_3| = 1$.

Observación. Las trayectorias de longitud 1 están asociadas con los pares ordenados $(a, b) \in R$. Las trayectorias en una relación R permiten definir nuevas relaciones a partir de R.

Definición. Relación R^n sobre un conjunto finito A. La relación R^n, con entero positivo n está formada con los pares ordenados $(a, b) \in R^n$, en donde aR^nb indica que existe una trayectoria de longitud n entre los elementos a y b pertenecientes al conjunto A.

Para obtener R^n puede ser más cómodo hacerlo a través de la matriz $\boldsymbol{M}(R^n)$ asociada, la cual se obtiene mediante la potencia n de la matriz $\boldsymbol{M}(R)$ dada por

$$\boldsymbol{M}(R^n) = \underbrace{\boldsymbol{M}(R) \odot \boldsymbol{M}(R) ... \odot \boldsymbol{M}(R)}_{n \text{ factores}} \tag{8.12}$$

realizada con n factores, en donde $\odot$ denota el producto matricial de bits (o producto matricial booleano) definido a continuación.

Definición. Producto matricial de bits (o producto matricial booleano). Sean los conjuntos finitos A, B y C, con p, q y r elementos, respectivamente, las relaciones R_1 de A en B, y R_2 de B en C, respectivamente, y las matrices de relaciones $\boldsymbol{M}(R_1)$ de $p \times q$ y $\boldsymbol{B}(R_2)$ de $q \times r$, se define el producto matricial de bits $\boldsymbol{M}(R_1 \circ R_2) = \boldsymbol{M}(R_1) \odot \boldsymbol{M}(R_2)$ a la matriz obtenida realizando primero el producto matricial usual, y a continuación reemplazar cada entrada no nula de $\boldsymbol{M}(R_1 \circ R_2)$ por 1, mientras que las entradas nulas siguen siendo nulas.

Ejemplo. Sea el conjunto $A = \{1, 2, 3, 4, 5, 6\}$, y la relación $R = \{$ (1,2), (1,3), (2,2), (2,4), (2,5), (3,4), (4,5), (5,6) $\}$, ver Fig. 8.4. Calculando $R^2 = R \circ R$ mediante la definición se obtiene: $R^2 = \{$ (1,2), (1,4), (1,5), (2,2), (2,4), (2,5), (2,6), (3,5), (4,6) $\}$, y que son todas las trayectorias de longitud 2 en A obtenidas a partir de R, verlo en la Fig. 8.4. Tarea: obtener R^2 mediante el producto matricial de bits $\boldsymbol{M}(R^2) = \boldsymbol{M}(R) \odot \boldsymbol{M}(R)$.

8.6.4. Relaciones, conjuntos, y matrices

En la Tabla 8.1 se resumen recetas prácticas para chequear en una relación R en un conjunto finito A de n elementos las propiedades: reflexiva, simétrica, antisimétrica, y transitiva, en donde

$$\begin{aligned} I_A &= \{(x_1, x_1), (x_1, x_1)..., (x_n, x_n)\} && \text{relación identidad en } A; \\ R^2 &= R \circ R && \text{composición de } R \text{ con } R; \\ R^{-1} &= \{(y, x) \mid (x, y) \in R\} && \text{relación inversa de } R; \end{aligned} \tag{8.13}$$

propiedad	como conjunto	en la matriz de R
R es reflexiva	$I_A \subseteq R$	$\boldsymbol{M}(I_A) \leq \boldsymbol{M}(R)$
R es simétrica	$R = R^{-1}$	$\boldsymbol{M}(R) = \boldsymbol{M}(R^{-1})$
R es antisimétrica	$R \cap R^{-1} \subseteq I_A$	$\boldsymbol{M}(R) \odot \boldsymbol{M}(R^{-1}) \leq \boldsymbol{M}(I_A)$
R es transitiva	$R^2 \subseteq R$	$\boldsymbol{M}(R^2) \leq \boldsymbol{M}(R)$

Tabla 8.1: Recetas para chequear algunas propiedades de una relación R en un conjunto A.

Ejemplo. Sea el conjunto $A = \{a, b, c\}$ y la matriz de la relación R dada por la Ec. (8.14). Usar el producto matricial de bits (o producto booleano) para decidir si R es transitiva (o no).

$$\boldsymbol{M}(R) = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \end{array} \tag{8.14}$$

Solución. Calculando:

$$\boldsymbol{M}(R^2) = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array} \tag{8.15}$$

A partir de las Ecs. (8.14-8.15) se concluye que no se cumple que $\boldsymbol{M}(R^2) \leq \boldsymbol{M}(R)$, por lo que R no es transitiva.

Ejemplo. Sea el conjunto $A = \{a, b, c\}$ y la matriz de la relación R dada por la Ec. (8.16). Usar el producto matricial de bits (o producto booleano) para decidir si R es transitiva (o no).

$$\boldsymbol{M}(R) = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{array} \tag{8.16}$$

Solución. Calculando:

$$\boldsymbol{M}(R^2) = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{array} \tag{8.17}$$

A partir de las Ecs. (8.16-8.17) se concluye que se cumple que $\boldsymbol{M}(R^2) \leq \boldsymbol{M}(R)$, por lo que R es transitiva.

Observación. Implementaciones de tests para determinar si una relación R en un conjunto A es: reflexiva, simétrica, antisimétrica, transtiva, relación de equivalencia, relación de orden parcial, o ninguna, analizando la matriz M asociada a R, son mostradas a continuación.

```
def es_reflexiva (M):
    n = len(M)
    for i in range (n):
        if not M[i,i]:
            return False
    return True
```

```
def es_simetrica_vainilla (M):
    n = len (M)
    for i in range (n):
        for j in range (n):
            if (M[i,j] and not M[j,i]):
                return False
    return True
```

```
def es_simetrica(M):
    n = len (M)
    for i in range (n):
        for j in range (i+1,n):
            if (M[i,j] and not M[j,i]):
                return False
            if (M[j,i] and not M[i,j]):
                return False
    return True
```

```
def es_antisimetrica (M):
    n = len (M)
    for i in range (n):
        for j in range (i+1,n):
            if (M[i,j] and M[j,i]):
                return False
    return True
```

```
def es_transitiva (M):
    n = len (M)
    for k in range (n):
        for i in range (n):
            for j in range (n):
                if ((M[i,k] and M[k,j]) and not M[i,j]):
                    return False
    return True
```

```
def es_relacion_de_equivalencia (M):
    return (es_reflexiva (M) and
            es_simetrica (M) and
            es_transitiva(M))
```

```
def es_relacion_de_orden_parcial (M):
    return (es_reflexiva     (M) and
            es_antisimetrica(M) and
            es_transitiva    (M))
```

CAPÍTULO 9

Relaciones de Recurrencia

Contents

9.1. Intro a relaciones de recurrencia

Definición. Relación de Recurrencia (RR) y Condiciones Iniciales (CI). Una RR para la sucesión a_0, a_1, ... a_n, ... es una ecuación que relaciona el término genérico con un cierto número de términos predecesores. Para que la RR sea unívoca, se debe especificar las CI dadas por un número finito de términos de la sucesión conocidos expliícitamente.

Observación.

i) A veces el término genérico es a_n, en ese caso sus predecesores son a_{n-1}, a_{n-2}, ..., etc;
ii) Otras veces el término genérico es a_{n+1}, por lo que sus predecesores son a_n, a_{n-1}, ..., etc;

Ejemplo. La RR y las CI para la sucesión de Fibonacci se puede escribir en diversas formas, e.g.:

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} \quad \text{para } n = 3, 4, ... \\ f_1 &= f_2 = 1 \end{aligned} \tag{9.1}$$

que puede re-escribirse como

$$f_n = \begin{cases} f_{n-1} + f_{n-2} & \text{para } n = 3, 4, ... \\ 1 & \text{para } n = 1 \text{ o } n = 2 \end{cases} \tag{9.2}$$

y que puede resescribirse como

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \quad \text{para } n = 2, 3, ... \\ f_1 &= f_2 = 1 \end{aligned} \tag{9.3}$$

Ejemplo. Sea A_n la cantidad de dinero al final de n años, y suponga una persona que invierte $A_0 = 1000$ al 12 % anual compuesto. Escriba una RR y un algoritmo para obtener la cantidad de dinero al cabo de n años. Solución.

- Sea $t = 12/100$ la tasa tanto por 1. Tenemos

$$\begin{aligned} A_n &= A_{n-1} + tA_{n-1} = (1+t)A_{n-1} = pA_{n-1} \\ A_n &= pA_{n-1} \quad \text{con todo entero } n \geq 1 \text{ y } A_0 = 1000 \end{aligned} \tag{9.4}$$

- Resolviendo por iteración:

$$\begin{aligned} A_n &= pA_{n-1} = p(pA_{n-2}) = p^2 A_{n-2} = \ldots = p^n A_0 \\ A_n &= p^n A_0 \end{aligned} \tag{9.5}$$

Ejemplo. Hallar una RR y las CI para el número de subconjuntos de un conjunto de n elementos. Solución: sea S_n el número de subconjuntos de un conjunto de n elementos. Como al pasar de un conjunto de $(n-1)$ elementos a otro conjunto de n elementos se duplica el número de subconjuntos disponibles (pues $|\mathbb{P}(\mathbb{X})| = 2^n$, con $n = |X|$), obtenemos la RR

$$S_n = 2S_{n-1} \quad \text{con } n \geq 1 \text{ y } S_0 = 1 \tag{9.6}$$

Ejemplo. Hallar una RR y las CI para el número on de cadenas de n bits que no contienen la subcadena 111. Solución: sea S_n el número de cadenas de n bits que no contienen la subcadena 111. La cadena de n bits que no contiene la subcadena 111 puede provenir de las subcadenas:

- Con $(n-1)$ bits tales que terminan en 0, 1;
- Con $(n-2)$ bits tales que terminan en 00, 01, 10;
- Con $(n-3)$ bits tales que terminan en 000, 001, 010, 100, 101, 110;
- Usando el PS obtenemos la RR y las CI dadas por

$$\begin{aligned} S_n &= S_{n-1} + S_{n-2} + S_{n-3} \quad \text{con } n \geq 4 \\ S_1 &= 2 \quad \text{son 0 y 1} \\ S_2 &= 3 \quad \text{son 00, 01, 10} \\ S_3 &= 5 \quad \text{son 000, 001, 010, 100, 101} \end{aligned} \tag{9.7}$$

Ejemplo. Torres de Hanoi. Encontrar la RR y la CI para el número de movimientos H_n que resuelve el problema del juego de las Torres de Hanoi (TH) con n discos, con al menos un disco. Solución:

- Consigna: mover los discos, de a uno por vez, desde la estaca A hacia la C, pero nunca colocando un disco más grande sobre otro más pequeño, usando la estaca B como auxiliar;
- Por ejemplo, en la Fig. 9.1 se muestran los movimientos para resolver este juego con $n = 3$ discos;
- Si hay un disco ($n = 1$), el juego se resuelve con un movimiento, por lo que $c_1 = 1$;

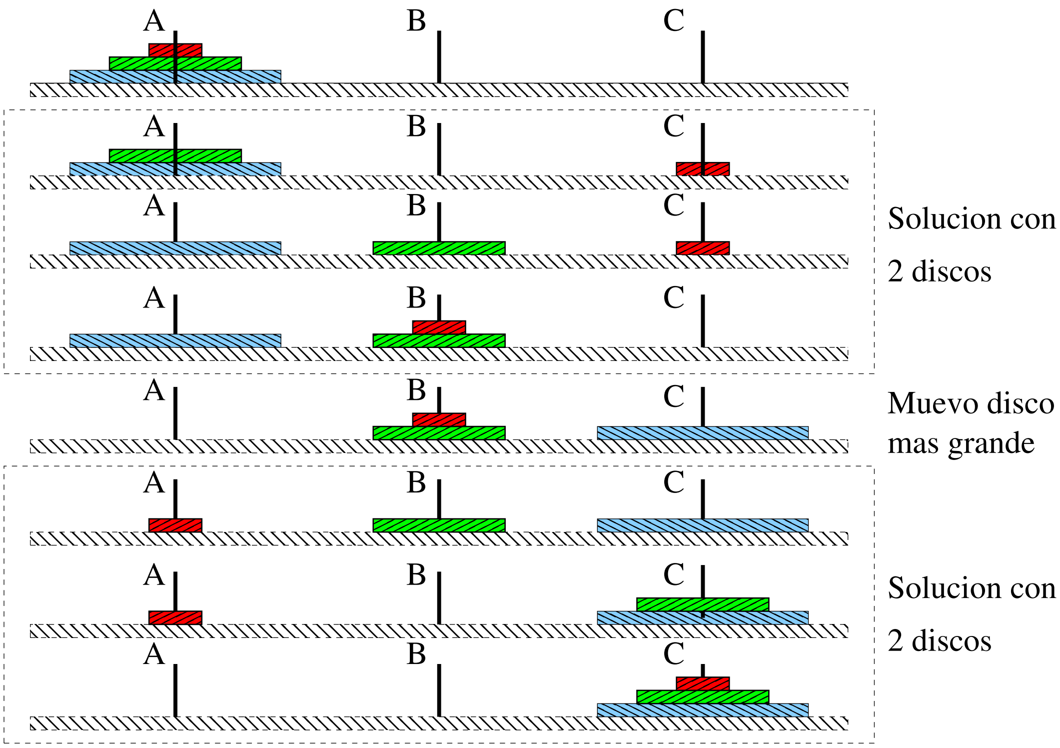

Figura 9.1: Movimientos en el juego de las TH con $n = 3$ discos.

- Si hay más de un disco, $n > 1$, el juego se divide en 3 etapas: (i) se pasan $n-1$ discos de la estaca A hacia la auxiliar B, lo cual involucra H_{n-1} movimientos; (ii) luego se mueve el disco más grande de manera explíta a la estaca C (con un movimiento); y (iii) se vuelven a pasar los $n-1$ discos de la estaca auxiliar B hacia la C, lo cual involucra otros H_{n-1} movimientos. Sumando, se tiene la RR y la condición inicial

$$\begin{aligned} H_n &= 2H_{n-1} + 1 \quad \text{con } n \geq 2 \\ H_1 &= 1 \end{aligned} \tag{9.8}$$

9.2. Solución de las relaciones de recurrencia

Ejemplo. Resolver la RR dada por $a_n = a_{n-1} + 3$, para todo entero $n \geq 2$, con la CI dada por $a_1 = 2$. Solución:

$$\begin{aligned} a_n &= a_{n-1} + 3 \quad \text{con } n \geq 2 \\ a_{n-1} &= a_{n-2} + 3 \\ a_n &= (a_{n-1}) + 3 = ((a_{n-2} + 3) + 3) = (a_{n-3} + 3) + 3 + 3 = a_{n-4} + (3 + 3 + 3 + 3) \end{aligned} \tag{9.9}$$

Para hallar k hacemos

$$\begin{aligned} n - k = 1 \quad &\therefore \quad k = n - 1 \\ a_n &= a_1 + 3(n-1) \\ a_n &= 2 + 3(n-1) \quad \text{con } n \geq 1 \end{aligned} \tag{9.10}$$

Ejemplo. Resolver la RR que resuelve el número mínimo de movimientos para resolver el juego de las TH, dada por $H_n = 2H_{n-1} + 1$, para todo entero $n \geq 2$, con la CI para un disco $H_1 = 1$. Solución: por iteración (en donde el último valor de k está dado cuando $n - k = 1$, por lo que $k = n - 1$)

$$\begin{aligned} H_n &= 2H_{n-1} + 1 \quad \text{con } n \geq 2 \\ &= 2(2H_{n-2} + 1) + 1 \\ &= 2^2(H_{n-2}) + 2 + 1 \\ &= 2^2(2H_{n-3} + 1) + 2 + 1 \\ &= 2^3H_{n-3} + 2^2 + 2^1 + 2^0 \\ &= 2^3(2H_{n-4} + 1) + 2^2 + 2^1 + 2^0 \\ &= 2^4H_{n-4} + 2^3 + 2^2 + 2^1 + 2^0 = ... \\ &= 2^k(2H_{n-k} + 1) + 2^{k-1} + ... + 2^1 + 2^0 \\ &= 2^{n-1}H_1 + 2^{n-2} + ... + 2^1 + 2^0 = ... \\ &= 2^{n-1} + 2^{n-2} + ... + 2^1 + 2^0 \end{aligned} \tag{9.11}$$

que es una forma particular de la serie geométrica

$$a + ar + ar^2 + ... + ar^m = \frac{a(r^{m+1} - 1)}{r - 1} \quad \text{con } r \neq 1 \tag{9.12}$$

cuando $r = 2$, $a = 1$, y $m = n - 1$, resulta

$$1 + 2 + 4 + 8 + ... + 2^{n-1} = \frac{1 \cdot (2^n - 1)}{2 - 1} \tag{9.13}$$

por lo que la solución no-recursiva es

$$H_n = 2^n - 1 \tag{9.14}$$

Definición. Una Relación de Recurrencia Homogénea, Lineal, de Coeficientes Constantes (RRHLCC), de orden k, es una relación de recurrencia de la forma

$$a_n = c_1a_{n-1} + c_2a_{n-2} + ... + c_ka_{n-k} \quad \text{con, al menos, } c_k \neq 0 \tag{9.15}$$

en donde la unicidad se logra definiendo k condiciones iniciales

$$a_0 = c_0 \quad a_1 = c_1 \quad ... \quad a_k = c_k \tag{9.16}$$

Ejemplo. Clasificar cada una de las siguientes RR.

- $s_n = 2s_{n-1}$: es una RRHLCC, de orden 1;
- $f_n = f_{n-1} + f_{n-2}$ (Fibonacci): es una RRHLCC, de orden 2;
- $a_n = 3a_{n-1}a_{n-2}$: es una RRH no-lineal, de CC, de orden 2;
- $a_n - a_{n-1} = 2n$: es una RR lineal, no-homogénea, de CC, y de orden 1;
- $a_n = 3na_{n-1}$: es una RR lineal, homogénea, y de coeficientes no-constantes.

Ejemplo. Procedimiento básico para resolver una RRHLCC. Resolver la RRHLCC dada por $a_n = 5a_{n-1} - 6a_{n-2}$, para todo entero $n \geq 2$, con las CI particulares $a_0 = 7$ y $a_1 = 16$. Solución: Sea $a_n = r^n$, donde r se asume como una constante real. Reemplazando

$$
\begin{aligned}
r^n &= 5r^{n-1} - 6r^{n-2} \\
r^n - 5r^{n-1} + 6r^{n-2} &= 0 \\
r^{n-2}(r^2 - 5r + 6) &= 0 \quad \text{si } r^{n-2} \neq 0, \text{ debe ser } (r^2 - 5r + 6) = 0 \\
\therefore \quad r_{1,2} &= \frac{5 \pm \sqrt{25 - 24}}{2} \quad \therefore \quad r_1 = 2 \quad , \quad r_2 = 3
\end{aligned}
\tag{9.17}
$$

entonces hay 2 soluciones linealmente independientes $S_n = r_1^n$ y $T_n = r_2^n$, por lo que la solución general es una combinación lineal de ambas soluciones

$$
\begin{aligned}
a_n &= \alpha S_n + \beta T_n \\
&= \alpha r_1^n + \beta r_2^n \\
&= \alpha 2^n + \beta 3^n
\end{aligned}
\tag{9.18}
$$

donde α y β son constantes a determinar a partir de las condiciones iniciales

$$
\begin{aligned}
a_0 &= \alpha 2^0 + \beta 3^0 = 7 \\
a_1 &= \alpha 2^1 + \beta 3^1 = 16
\end{aligned}
\tag{9.19}
$$

con lo que se tiene un sistema lineal de dos ecuaciones para las incógnitas α y β

$$
\begin{aligned}
\alpha + \beta &= 7 \\
2\alpha + 3\beta &= 16
\end{aligned}
\tag{9.20}
$$

cuya solución da $\alpha = 5$ y $\beta = 2$. Finalmente, la solución particular es $a_n = 52^n + 23^n$ para $n = 0, 1, 2, ...$

Teorema. Sea $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ una RRHL de segundo orden.

- Si S y T son soluciones, entonces $U = \alpha S + \beta T$ también es solución;
- Si r es una raíz de $t^2 - c_1 t - c_2 = 0$, entonces r^n es solución, para $n = 0, 1$;
- Si $\{a_n\}$ es la sucesión $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ tal que $a_0 = c_0$, $a_1 = c_1$, y si r_1, r_2 son raíces reales y distintas, i.e. $r_1 \neq r_2$, entonces existen constantes α y β tales que $a_n = \alpha r_1^n + \beta r_2^n$, para $n = 0, 1, ...$;

Demostración:

- Como S y T son soluciones de la RR, debe ser

$$
\begin{aligned}
S_n &= c_1 S_{n-1} + c_2 S_{n-2} \quad \therefore \quad \alpha S_n = \alpha(c_1 S_{n-1} + c_2 S_{n-2}) \\
T_n &= c_1 T_{n-1} + c_2 T_{n-2} \quad \therefore \quad \beta T_n = \beta(c_1 T_{n-1} + c_2 T_{n-2})
\end{aligned}
\tag{9.21}
$$

  sumando ambas ecuaciones

$$
\begin{aligned}
U_n &= \alpha S_n + \beta T_n \\
&= c_1(\alpha S_{n-1} + \beta T_{n-1}) + c_2(\alpha S_{n-2} + \beta T_{n-2}) \\
&= c_1 U_{n-1} + c_2 U_{n-2}
\end{aligned}
\tag{9.22}
$$

  por lo que U también es una solución.

- Si r es una raíz de la EC dada por $t^2 - c_1 t - c_2 = 0$, entonces se cumple $r^2 = c_1 t + c_2$, y hacemos
$$c_1 r^{n-1} + c_2 r^{n-2} = r^{n-2}(c_1 r + c_2) = r^{n-2} r^2 = r^n \tag{9.23}$$
por lo que la sucesión r^n, con $n = 0, 1, ...,$ verifica la EC;
- Sea $U_n = \alpha r_1^n + \beta r_2^n$, entonces U es solución y para cumplir con las CI dadas, planteamos
$$\begin{aligned} U_0 &= \alpha r_1^0 + \beta r_2^0 = C_0 \\ U_1 &= \alpha r_1^1 + \beta r_2^1 = C_1 \end{aligned} \tag{9.24}$$
es decir,
$$\begin{aligned} \alpha + \beta &= C_0 \\ \alpha r_1 + \beta r_2 &= C_1 \end{aligned} \tag{9.25}$$
Para igualar el primer término de ambas ecuaciones hacemos
$$\begin{aligned} r_1\alpha + r_1\beta &= r_1 C_0 \\ r_1\alpha + r_2\beta &= C_1 \end{aligned} \tag{9.26}$$
restando lado a lado se obtiene $(r_1 - r_2)\beta = r_1 C_0 - C_1$, y sólo cuando $r_1 \neq r_2$ se puede obtener $\beta = (r_1 C_0 - C_1)/(r_1 - r_2)$, y luego $\alpha = C_0 - \beta$.

Teorema. Sea $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ una RRHL de segundo orden.

- Si S y T son soluciones, entonces $U = \alpha S + \beta T$ también es solución;
- Si $\{a_n\}$ es la sucesión $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ tal que $a_0 = c_0$, $a_1 = c_1$, y si ambas raíces de $r^2 - c_1 r - c_2 = 0$ son iguales a r_0, entonces existen constantes α y β tales que $a_n = \alpha r_0^n + \beta n r_0^n$, con $n = 0, 1, ...;$

Demostración:

- El teorema anterior prueba que la sucesión r_0^n, para $n = 1, 2, ...,$ es solución de la RR;
- Por lo que resta demostrar que la sucesión $n r_0^n$, para $n = 1, 2, ...,$ también es una solución de la RR.
- Como r_0 es la única solución real de la EC, se tiene
$$r^2 - c_1 r - c_2 = (r - r_0)(r - r_0) = (r - r_0)^2 \tag{9.27}$$
Las raíces x_1 y x_2 de la ecuación cuadrática general $ax^2 + bx + c = 0$ verifican las propiedades $x_1 + x_2 = -b/a$ y $x_1 \cdot x_2 = c/a$. Dichas propiedades en este caso se re-expresan como $c_1 = 2r_0$ y $c_2 = -r_0^2$, por lo que
$$\begin{aligned} c_1(n-1)r_0^{n-1} + c_2(n-2)r_0^{n-2} &= 2r(n-1)r_0^{n-1} - r_0^2(n-2)r_0^{n-2} \\ &= r_0^n[2(n-1) - (n-2)] = n r_0^n \end{aligned} \tag{9.28}$$
entonces la sucesión $n r_0^n$ es solución.

Ejemplo. Resolver $a_n = 4a_{n-1} - 4a_{n-2}$ para todo entero $n \geq 2$, con $a_0 = 1$ y $a_1 = 1$. Solución: Sea $a_n = r^n$, donde r se asume como una constante real no nula. Reemplazando
$$\begin{aligned} & r^n - 4r^{n-1} + 4r^{n-2} = 0 \\ & r^{n-2}(r^2 - 4r + 4) = 0 \quad \text{si } r^{n-2} \neq 0, \text{ debe ser } (r^2 - 4r + 4) = 0 \\ & \therefore \quad r_{1,2} = \frac{4 \pm \sqrt{16 - 16}}{2} \qquad \therefore \quad r_1 = r_2 = r_0 = 2 \end{aligned} \tag{9.29}$$

entonces las 2 soluciones linealmente independientes son $S_n = r_0^n$ y $T_n = nr_0^n$, por lo que la solución general es una combinación lineal de ambas soluciones

$$\begin{aligned} a_n &= \alpha S_n + \beta T_n \\ &= \alpha r_0^n + \beta n r_0^n \\ &= \alpha 2^n + \beta n 2^n \end{aligned} \tag{9.30}$$

donde α y β son constantes a determinar a partir de las condiciones iniciales

$$\begin{aligned} a_0 &= \alpha 2^0 + \beta \cdot 0 \cdot 2^0 = 1 \\ a_1 &= \alpha 2^1 + \beta \cdot 1 \cdot 3^1 = 1 \end{aligned} \tag{9.31}$$

con lo que se tiene un sistema lineal de dos ecuaciones para las constantes α y β

$$\begin{aligned} \alpha &= 1 \\ 2\alpha + 2\beta &= 1 \end{aligned} \tag{9.32}$$

cuya solución da $\alpha = 1$ y $\beta = -1/2$. Finalmente, la solución particular es $a_n = 2^n - \frac{1}{2} n 2^n$ para $n = 0, 1, 2, ...$

CAPÍTULO 10

Grafos

Contents

10.1. Primeras definiciones y terminología en grafos

Definición.

- *Grafo*: un grafo se denota con la dupla $G = (V, E)$, y está formado por un conjunto V de *vértices* (o nodos), y de un conjunto E de *aristas*, tal que cada arista $e \in E$ se asocia a un par no-ordenado de vértices;
- Si existe una *única* arista e asociada a los vértices u y v se escribe $e = (u, v)$ o $e(v, u)$ en donde, en este contexto, (u, v) no-representa un par ordenado;
- Se dice que una arista e en un grafo asociada con el par de vértices u y v *es incidente* sobre u y sobre v, y se dice que u y v son *incidentes* sobre la arista e, y que u y v son *vértices adyacentes* (o primeros vecinos). También se dice que u es adyacente a v, y que v es adyacente a u;
- Supondremos (suposición más frecuente en literatura) que el conjunto de vértices V es no-vacío, el de aristas E puede ser vacío, y que ambos son finitos;
- Se dice que dos o más aristas son *aristas paralelas* cuando están asociadas a un mismo par de vértices;
- *Lazo*: es una arista incidente en un mismo vértice;
- Vértice *aislado*: es un vértice que no incide en ninguna arista;

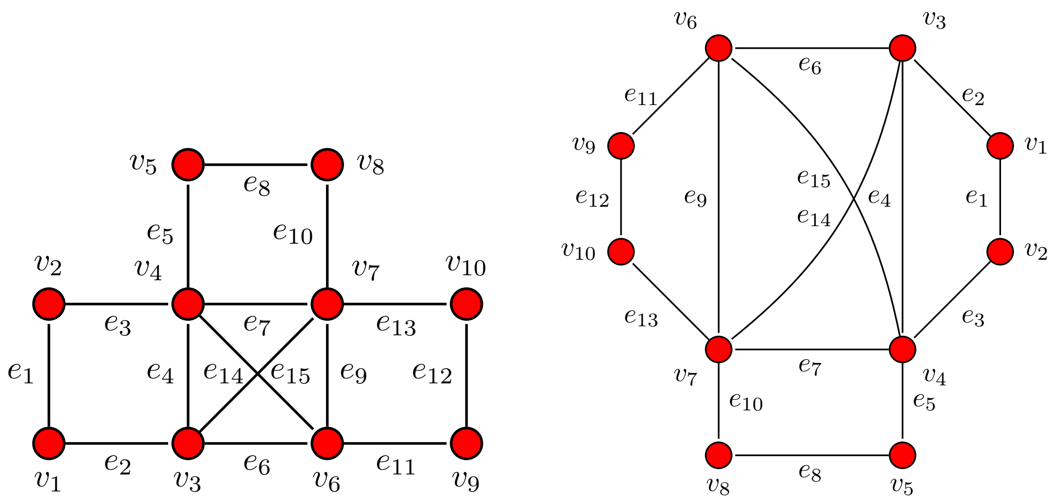

Figura 10.1: Dos grafos isomorfos: un mismo grafo dibujado en dos formas distintas pero con, exactamente, la misma información.

- Un *grafo simple* es un grafo $G = (V, E)$ *sin lazos ni aristas paralelas*;

Observación.

- En los textos [2] y [4]: omitir todo lo relacionado con "grafos orientados" o "grafos dirigidos";
- En [2] se utiliza la palabra "gráfica" en lugar de *grafo*, término que no usaremos;
- Cada vez que se pueda conviene trazar un dibujo representativo del gafo, usando los vértices como puntos y cada arista como una línea que une los vértices incidentes;
- Pero un "mismo" grafo se puede dibujar de muchas maneras, dando lugar a la noción de *grafos isomorfos*;
- En literatura (y libros) no hay un acuerdo general en las definiciones, e.g. en Rosen, además introduce: Multigrafo: es un grafo que admite aristas paralelas; Pseudografo: es un grafo que admite lazos.

Ejemplo. Sea el grafo $G = (V, E)$ dado por los vértices $V = \{v_1, v_2, ..., v_{10}\}$, y las aristas $E = \{e_1, e_2, ..., e_{13}\}$, y trazado en la Fig. 10.1 en dos formas distintas pero completamente equivalentes: son dos grafos isomorfos.

Ejemplo. Sean los tres grafos mostrados en la Fig. 10.2:

$G_1 = (V_1, E_1)$: como no tiene lazos ni aristas paralelas, es un grafo simple;

$G_2 = (V_2, E_2)$: como tiene las aristas paralelas e_1, e_6, y e_7, y el lazo e_8: no es un grafo simple;

$G_3 = (V_3, E_3)$: como no tiene lazos ni aristas paralelas, es un grafo simple, con vértice aislados v_7 y v_8.

10.2. Algunas familias distinguidas de grafos simples

Definición.

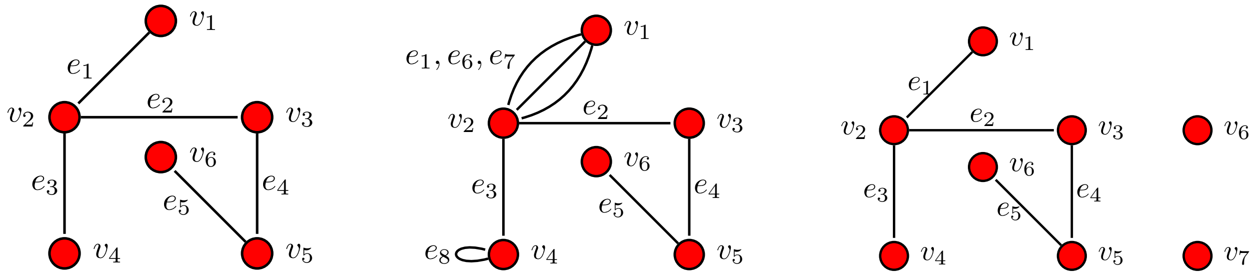

Figura 10.2: Grafos G_1, G_2, y G_3.

- Grafo *completo*: el grafo completo de n vértices, con $n \geq 1$, es el grafo *simple* que contiene exactamente una arista entre cada par de vértices distintos. Se denota con K_n;
- Grafo *bipartito*: un grafo $G = (V, E)$ es bipartito si es un grafo simple en donde existen dos conjuntos de vértices V_1 y V_2 de V, cualesquiera posiblemente vacío, tales que $V_1 \cap V_2 = \emptyset$, y $V_1 \cup V_2 = V$, y donde cada arista de E es incidente en un vértices de V_1 y en un vértice de V_2;
- Grafo *bipartito completo*: un grafo $G = (V, E)$ es bipartito si es un grafo simple en donde el conjunto de vértices tiene una partición en V_1 con m vértices, y V_2 de n vértices, y el conjunto de aristas de E consiste en *todas* las aristas de la forma (v_i, v_j), con $v_i \in V_1$ y $v_j \in V_2$. Se denota con $K_{m,n}$;
- *Grafo ciclo*: el grafo ciclo para $n \geq 3$ vértices es un grafo simple que consta de n vértices $\{v_1, v_2, v_3, ..., v_n\}$, y las aristas $\{(v_1, v_2), (v_2, v_3), ..., (v_{n-1}, v_n)\}$. Se denota con C_n;
- *Grafo rueda* (*wheel*): el grafo rueda es el grafo simple que se obtiene cuando se agrega un vértice adicional al ciclo C_n y lo conectamos con cada uno de los vértices de C_n. Se denota con W_n;
- *Grafo n-cubo* (o hipercubo): el cubo n dimensional es el grafo simple cuyos vértices representan a las 2^n cadenas de bits de longitud n, en donde 2 vértices son adyacentes ssi las cadenas de bits a las que representan difieren exactamente en 1 bit. Se denota con Q_n. Para construir en forma *recursiva* de Q_{n+1} a partir de Q_n: se hacen dos copias de Q_n, anteponiendo un 0 a cada una de las etiquetas de los vértices de una de las copias de Q_n, anteponiendo un 1 a cada una de las etiquetas de los vértices de la otra copia, y agregando aristas que conectan 2 vértices cuyas etiquetas difieran únicamente en el primer bit.

Ejemplo. Los grafos completos K_1, K_2, K_3, y K_4 se muestran en la Fig. 10.3.

Ejemplo. En la Fig. 10.4 se muestran un grafo bipartito $G_{3,4}$, y el grafo bitartito completo $K_{3,4}$.

Ejemplo. Los grafos ciclo C_3, C_4, y C_5 se muestran en la Fig. 10.5.

Ejemplo. Los grafos rueda W_3, W_4, y W_5 se muestran en la Fig. 10.6.

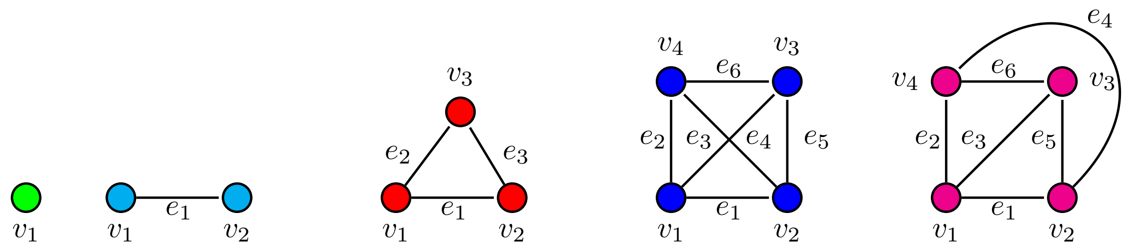

Figura 10.3: Los grafos completos K_1, K_2, K_3, y K_4, en donde K_4 graficado de dos maneras.

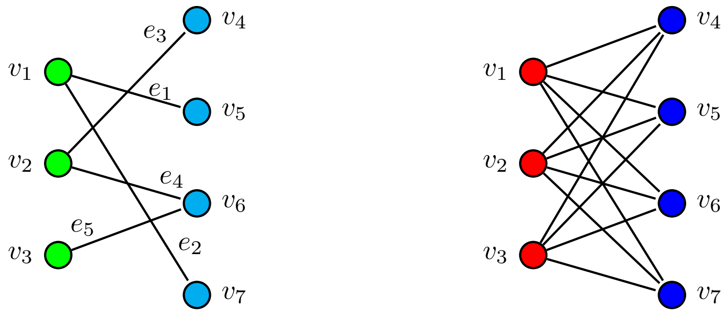

Figura 10.4: Un grafo bipartito $G_{3,4}$, y el grafo bitartito completo $K_{3,4}$.

Ejemplo. Los hipercubos Q_1, Q_2, y Q_3, obtenidos en forma recursiva, se muestran en la Fig. 10.7.

Tarea. Obtener: el hipercubo Q_2 a partir de Q_1, y el hipercubo Q_3 a partir de Q_2, en forma recursiva.

Observación.

- El grafo completo K_1 es bipartito: donde V_1 es el conjunto que contiene al único vértice, y V_2 es el conjunto vacío, donde cada arista, en realidad ninguna, incide en un vértice de V_1 y en un vértice de V_2. [4]: omitir todo lo relacionado con "grafos orientados" o "grafos dirigidos";

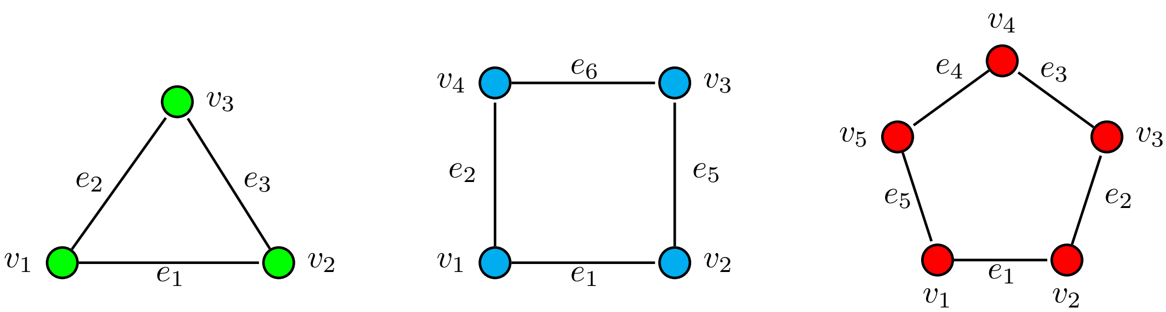

Figura 10.5: Los grafos ciclo C_3, C_4, y C_5.

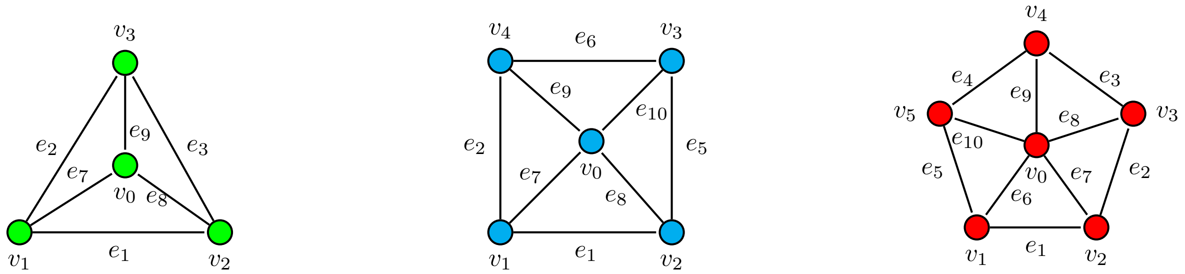

Figura 10.6: Los grafos rueda W_3, W_4, y W_5.

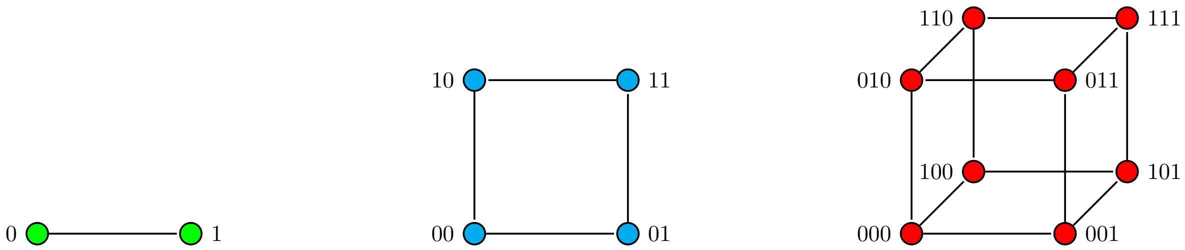

Figura 10.7: Los hipercubos Q_1, Q_2, y Q_3.

- En [2] se utiliza la palabra "gráfica" en lugar de *grafo*, término que no usaremos;
- Cada vez que se pueda conviene trazar un dibujo representativo del gafo, usando los vértices como puntos y cada arista como una línea que une los vértices incidentes;
- Pero un mismo grafo se puede dibujar de muchas maneras, dando lugar a la noción de *grafos isomorfos* (descripción informal);
- En la literatura (y libros) no hay un acuerdo general en las definiciones, e.g. en Rosen, además introduce:
  - Multigrafo: es un grafo que admite aristas paralelas;
  - Pseudografo: es un grafo que admite lazos;

Definición.

- *Grado* de un vértice en un grafo $G = (V, E)$: se denota con $\delta(v)$, y es igual al número de aristas incidentes en el vértice v de G, excepto en los lazos en donde cada lazo contribuye en 2 unidades al grado del vértice;
- *Vértice aislado* en un grafo $G = (V, E)$: es todo vértice de grado 0. Un vértice aislado no es adyacente a ningún otro vértice.
- *Vértice hoja* en un grafo $G = (V, E)$: es todo vértice de grado 1. Una hoja es adyacente a exactamente un vértice distinto de si mismo.

10.3. Trayectorias y ciclos

Definición.

- *Trayectoria* (o ruta): sean un grafo $G = (V, E)$, y los vértice v_0 y v_n en G. Una *trayectoria* (o ruta) de v_0 a v_n, de *longitud* n, es una sucesión alternada de $n + 1$ vértices y n

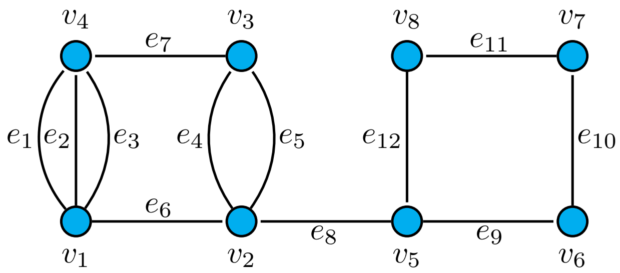

Figura 10.8: Un grafo conexo $G = (V, E)$ porque existe, al menos, una ruta entre cada par de vértices de G. Además, no es un grafo simple porque tiene las aristas paralelas e_1, e_2, e_3 y e_4, e_5
.

aristas que comienza en el vértice v_0 y termina en el vértice v_n, donde la arista e_i es incidente sobre los vértices v_{i-1} y v_i para $i = 1, ..., n$;

- Grafo *conexo*: un grafo $G = (V, E)$ es un grafo *conexo* si dados cualesquiera dos vértices u y v en V, existe al menos una ruta de u a v;
- *Subgrafo*: sea un grafo $G = (V, E)$. Se dice que $G' = (V', E')$ es un subgrafo de G si: (i) $V' \subseteq V$ y $E' \subseteq E$; y (ii) para toda arista $e' \in E'$, si e' incide en los vértices u' y v', entonces $u', v' \in V'$;
- *Componente* (o *componente conexa*): sea un grafo $G = (V, E)$ y un vértice u en G. El subgrafo G' de G formado por todas las aristas y vértices de G que están contenidos en alguna ruta que comienza en el vértice u se llama *componente* de G que contiene a u;
- *Vértice de articulación*: un vértice v en un grafo conexa G es un vértice de articulación si la eliminación de v y todas las aristas incidentes en v desconecta a G;
- *Arista puente*: una arista e en un grafo conexa G es una arista puente si la eliminación de e (pero conservando los vértices incidentes en e), desconecta a G.

Observación.

- La idea de la definición de trayectoria o ruta es la siguiente: comience en el vértice v_0, recorra la arista e1 hasta v_1, siga por la arista e_2 hasta el v_2, etc., hasta llegar al v_n;
- En ausencia de aristas paralelas, cuando se lista una ruta usualmente se suprimen las aristas.

Ejemplo. El grafo $G = (V, E)$ trazado en la Fig. 10.8 es un grafo conexo porque existe, al menos, una ruta entre cada par de vértices en G. Por eso, se puede listar las rutas sin las aristas. Por ejemplo, la ruta $T_1 = (v_8, e_{12}, v_5, e_8, v_2, e_5, v_3, e_7, v_4, e_3, v_1)$, o la ruta $T_2 = (v_8, e_{12}, v_5, e_8, v_2, e_4, v_3, e_7, v_4, e_1, v_1)$, ambas de longitud 5. Además, la ruta $T_3 = (v_8, e_{12}, v_5, e_6, v_1)$, de longitud 3, y la $T_4 = (v_6)$ de longitud 0.

Ejemplo. El grafo $G = (V, E)$ trazado en la Fig. 10.9 es un grafo simple (sin lazos ni aristas paralelas), y también es conexo (existe al menos una ruta entre cada par de vértices de G). En particular, entre los vértices v_8 y v_1 se pueden listar las rutas sin incluir las aristas, e.g. $T_1 = (v_8, v_5, v_2, v_3, v_4, v_1)$ de longitud 5, y la $T_2 = (v_8, v_5, v_2, v_1)$, de longitud 3.

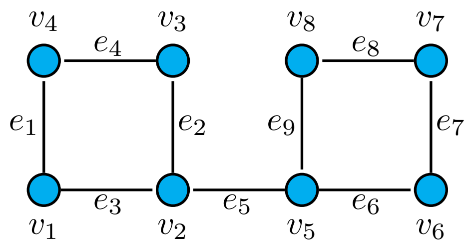

Figura 10.9: Un grafo conexo $G = (V, E)$ porque tiene, al menos, una ruta entre cada par de vértices de G. Además, no es un grafo simple porque tiene las aristas paralelas e_1, e_2, e_3 y e_4, e_5
.

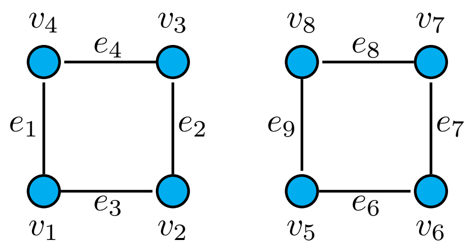

Figura 10.10: Un grafo $G = (V, E)$ que no es conexo porque, por ejemplo, no hay una ruta entre los vértices v_8 y v_1.

Ejemplo. El grafo $G = (V, E)$ trazado en la Fig. 10.10 no es conexo porque entre otros, por ejemplo, no hay una ruta entre los vértices v_8 y v_1.

Ejemplo. El grafo conexo $G = (V, E)$ trazado en la Fig. 10.11 (arriba, izquierda o derecha) particionado mediante: las aristas puente e_4 y e_8 (mitad-izq.), o con los vértices de articulación v_4 y v_9 (mitad-der.), la elección de los mismos es arbitraria, resultando dos componentes conexas (abajo-izq. y abajo-der.).

Definición. Sea un grafo $G = (V, E)$, y dos vértices u y v de G:

- *Trayectoria simple* (o *ruta simple*) de u a v: es una trayectoria (o ruta) de u a v *sin vértices* repetidos;
- *Ciclo* (o *circuito*) de u a u: es una trayectoria (o ruta) de u a u con longitud mayor a cero y *sin aristas* repetidas;
- *Ciclo simple* (o *circuito simple*) de u a u: es un ciclo (o circuito) *sin vértices* repetidos excepto el inicial y el final, y que son iguales a u.

Ejemplo. En el grafo conexo $G = (V, E)$ trazado en la Fig. 10.11 (izquierda o derecha):

- $T_1 = (v_4, v_5, v_7, v_6, v_8, v_7, v_9)$: no es una ruta simple, tampoco un ciclo, ni un ciclo simple;
- $T_2 = (v_4, v_5, v_7, v_9)$: sí es una ruta simple, pero no es un ciclo, ni un ciclo simple;
- $T_3 = (v_7, v_6, v_8, v_7, v_9, v_3, v_2, v_4, v_5, v_7)$: no es una ruta simple, sí es un ciclo, pero no un ciclo simple;

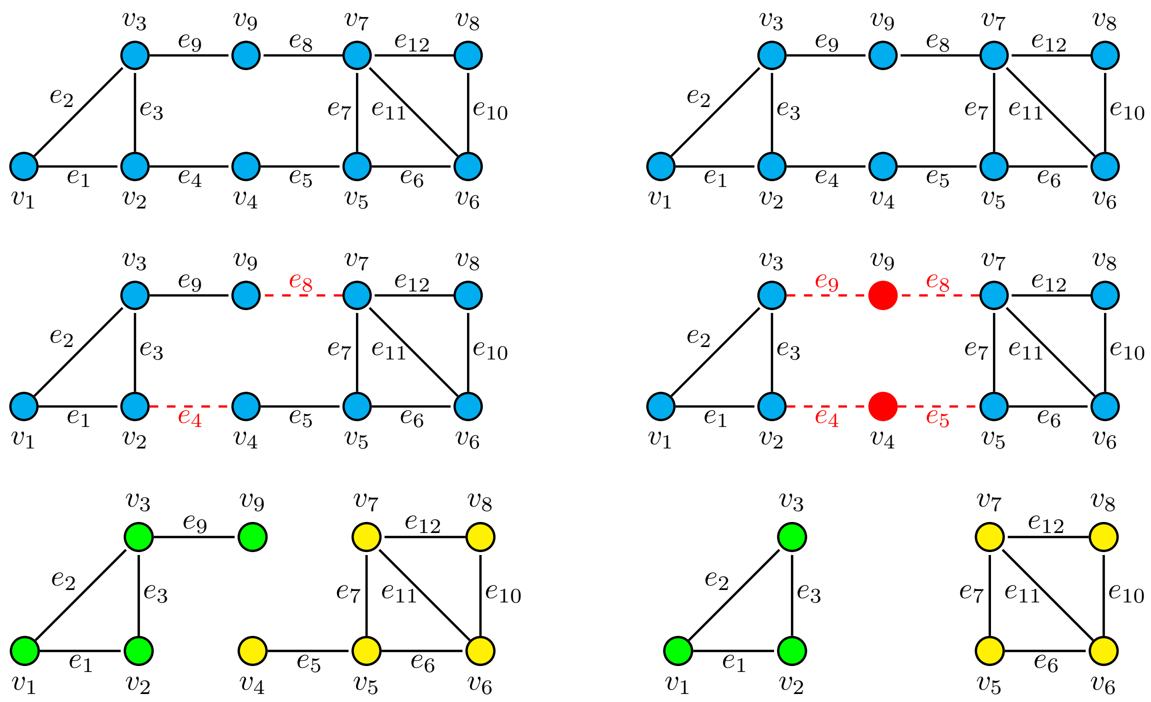

Figura 10.11: Un grafo conexo $G = (V, E)$ (arriba, izq. o der.) particionado mediante: las aristas puente e_4 y e_8 (mitad-izq.), o los con los vértices de articulación v_4 y v_9 (la elección de los mismos es arbitraria), resultando dos componentes conexas (abajo-izq. y abajo-der.).

- $T_4 = (v_7, v_9, v_3, v_2, v_4, v_5, v_7)$: no es una ruta simple, sí es un ciclo, y sí es un ciclo simple;
- $T_5 = (v_7)$: sí es una ruta simple, pero no es un ciclo, ni un ciclo simple.

10.4. Trayectoria y ciclo de Euler

Definición. Sea un grafo $G = (V, E)$ y un vértice u cualquiera de G:

- *Ciclo de Euler* (o *circuito de Euler*) [CE]: un CE es un ciclo (ruta de u a u de longitud mayor a cero sin aristas repetidas), y que contiene a **todas** las aristas del grafo G;
- Es decir, en un grafo G, un CE comienza en algún vértice, recorre todas las aristas exactamente una vez y regresa al vértice de partida;
- *Trayectoria de Euler*: es una trayectoria desde u que no repite aristas e incluye a todas las aristas del grafo G;

Observación.

- Entre los textos de Johnsonbaugh [2] y de Rose [4]: hay diferencias sutiles en las definiciones, e.g. trayectoria, ciclo, trayectoria simple, ciclo simple, circuito de Euler, etc.
- De todos modos, cada libro es consistente pero atención cuando se consultan ambos textos.

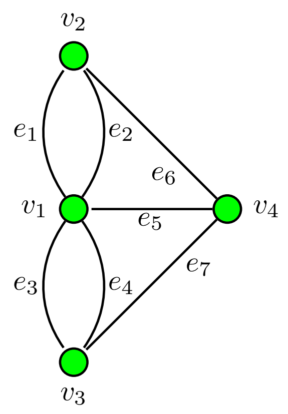

Figura 10.12: Grafo para el problema de los siete puentes de Königsberg: no tiene un ciclo de Euler, ni un circuito de Euler.

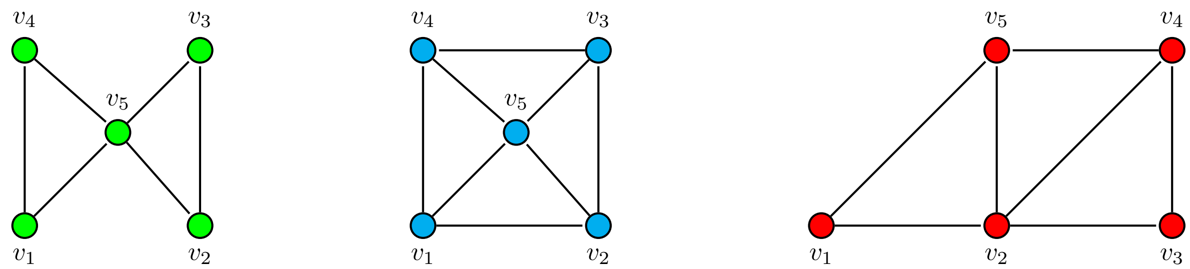

Figura 10.13: Grafo G_1 (izq.): con ciclo de Euler; grafo G_2 (med.): no tiene un ciclo de Euler ni una trayectoria de Euler; grafo G_3 (der.): no tiene un ciclo de Euler, pero si una trayectoria de Euler.

Ejemplo. En la Fig. 10.12 se muestra el grafo G que describe el problema de los siete puentes de Königsberg, donde G no tiene un ciclo de Euler ni un circuito de Euler.

Ejemplo. En los grafos conexos trazados en la Fig. 10.13:

- En el grafo G_1 (izq.): un ciclo de Euler es $C_1 = (v_1, v_5, v_3, v_2, v_5, v_4, v_1)$;
- En el grafo G_2 (med.): no tiene un ciclo de Euler ni una trayectoria de Euler;
- En el grafo G_3 (der.): no tiene un ciclo de Euler, pero si una trayectoria de Euler, e.g. $T_3 = (v_5, v_2, v_3, v_4, v_2, v_5, v_4)$.

Teorema. Sea $G = (V, E)$ un grafo, y los vértices u y v arbitrarios en G. Se cumple que: *Si G tiene un Ciclo de Euler (CE), entonces G es conexo y todo vértice tiene grado par.* Demostración: suponga que G tiene un CE, entonces G tiene una trayectoria de u a u que recorre todas las aristas exactamente una vez, por lo que en cada vértice debe haber un número par de aristas (la ruta entra y sale en cada vértice), o sea, cada vértice tiene grado par. La porción del CE que lleva de u a v sirve como ruta de u a v, y como u y v son arbitrarios, hay una ruta entre cada par de vértices de G, por lo que G es conexa.

Teorema. Sea $G = (V, E)$ un grafo, y los vértices u y v arbitrarios en G. Se cumple que: *Si G es conexo y todo vértice tiene grado par, entonces G tiene un Ciclo de Euler (CE).* Demostración por inducción en el número n de aristas en G.

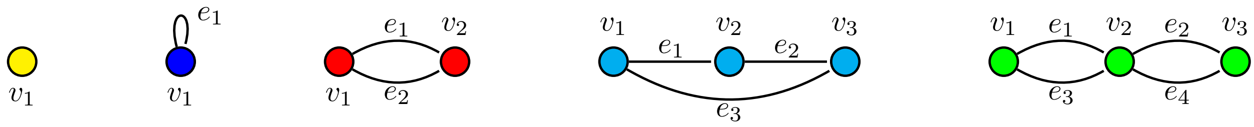

Figura 10.14: Primeros grafos conexos G, con todos sus vértices de grado par y con aristas: $n = 0$ y $n = 1$ (izq.), $n = 2$ (centro-izq.), $n = 3$ (centro-der.), y $n = 4$ (der.).
.

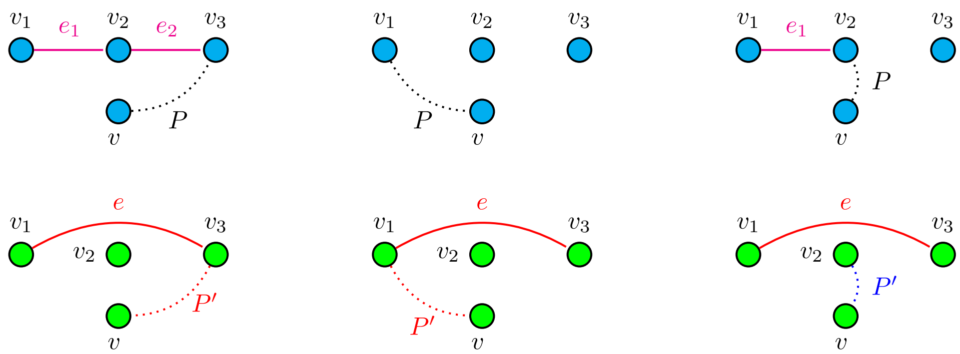

Figura 10.15: Grafos conexos G con todos sus vértices de grado par y con: $n = 3$ aristas (arr-izq.), $n = 4$ aristas (arr-der.), y sus versiones modificadas G' según construcción auxiliar del teorema: con $n = 3$ aristas y 2 componentes conexas (abajo-izq.), y con $n = 4$ aristas y 1 componente conexa (abajo-der.).

- Paso Base ($n = 0$): si G es un grafo con 0 aristas, entonces G se reduce a un único vértice. En este caso, el CE consta de un vértice sin aristas.
- Paso Inductivo: sea un grafo G con n aristas, donde n es positivo, arbitrario pero fijo. HI: suponemos que todo grafo conexo con k aristas y todos sus vértices tienen grado par, tiene un CE, para algún entero $k < n$:
  - Si G es conexo, tiene 1 o 2 vértices, y cada uno tiene grado par, ver Fig. 10.14 (izq. y centro-izq.), en forma directa se comprueba que cada grafo en esas condiciones tiene un CE;
  - Si G es conexo, tiene al menos 3 vértices, y cada vértice tiene grado par, rotulamos tres vértices con v_1, v_2 y v_3, y las aristas $e_1 = (v_1, v_2)$, $e_2 = (v_2, v_3)$, e.g. ver Fig. 10.14 (centro-der. o der.);
  - Eliminamos las aristas e_1 y e_2 pero conservamos sus vértices adyacentes, y agregamos la arista $e = (v_1, v_3)$, para obtener un grafo G';
  - Con esta modificación:
    - Antes los vértices v_1 y v_3 estaban conectados a través de v_2, y ahora son adyacentes a través de la arista agregada e;
    - No se alteran los grados de v_1 ni v_3;
    - El grado de v_3 se reduce en 2 unidades;

    Por lo que G' tiene una arista menos, y cada vértice sigue teniendo grado par;
  - Todavía no sabemos si G' se mantiene conexo, aunque notamos que en caso de $n = 3$ aristas resulta que G' puede tener una o dos componentes (donde cada una es conexa, por definición), ver Fig. 10.15 (izq. o der.);

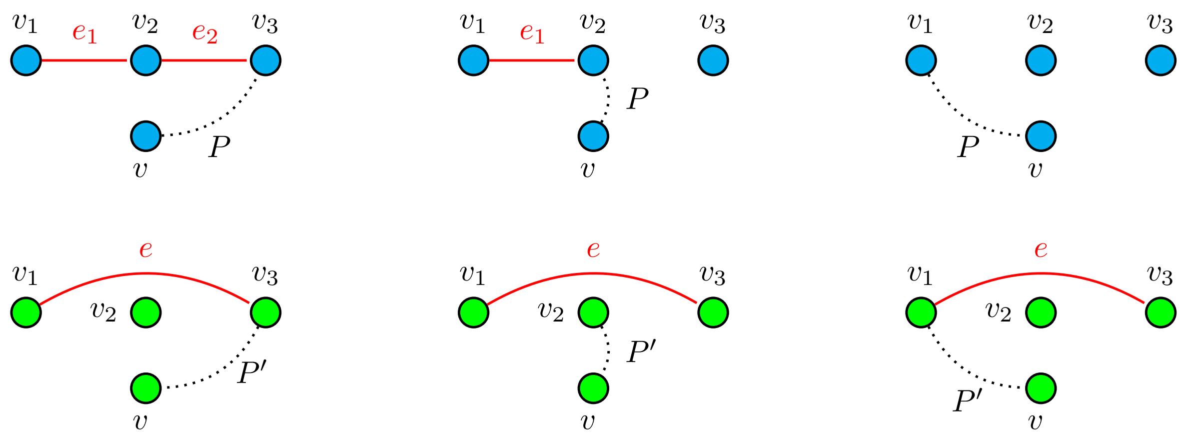

Figura 10.16: Trayectorias P en G: $P = (v, v_3, e_2, v_2, e_1, v_1)$ [arriba-izq.], $P = (v, v_1)$ [arriba-cen.], y $P = (v, v_2, e_1, v_1)$ [arriba-der.]. Trayectorias P' en G': $P' = (v, v_3, e, v_1)$ [abajo-izq.], $P' = (v, v_1)$ [abajo-cen.], y $P' = (v, v_2)$ [abajo-der.]. Componentes conexas en G': o bien 1 (izq. y cen.), o bien 2 (der.).

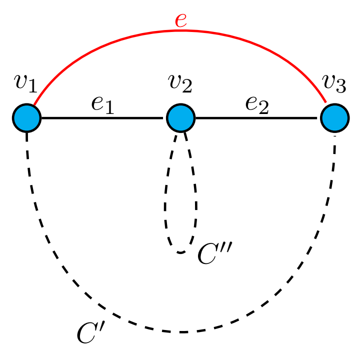

Figura 10.17: Si G' tiene 1 Componente Conexa (CC) con un ciclo de Euler C': se sustituye e en C' por e_1 y por e_2. Pero si G' tiene 2 CC, la CC que contiene a v_1 tiene un ciclo de Euler C', y la CC que contiene a v_2 tiene otro C''. Entonces se modifica C': sustituir e en C' por (v_1, v_2), seguido de C'', y seguido de (v_2, v_3).

- Sea P una ruta en G (pues G es conexo), desde un vértice v arbitrario hacia v_1, ver Fig. 10.16 (izq.).;
- Sea P' la parte de la ruta P que comienza en v pero cuyas aristas están en G', ver Fig. 10.16 (der.);
- Notar que la arista agregada e puede estar en P' pero no en P. Por otra parte, la ruta P' puede terminar ya sea en v_1, en v_2, o en v_3:
  - Si P' termina en v_3 o en v_1, y por la arista agregada e, entonces el vértice v está en la misma componente en G' que contiene a v_3 y a v_1;
  - Pero si P' termina en v_2, entonces v está en la misma componente que v_2;

  Por eso, todo vértice en G' está en una misma componente, o bien de v_1 y v_3, o bien de v_2;
- En definitiva, G' puede tener una o dos componentes, que se analizan por separado:
  - Si G' tiene una componente, entonces G' es conexa, y usamos la HI para concluir que G' tiene un ciclo de Euler C', ver Fig. 10.15, que se puede modificar

para obtener un CE en G: sustituir la arista e en C' por e_1 y por e_2;
- Si G' tiene dos componentes entonces, por la HI, la componente que contiene a v_1 tiene un ciclo de Euler C', y la componente que contiene a v_2 tiene otro ciclo de Euler C'' (que comienza y termina en v_2), ver Fig. 10.15. Pero C' se lo puede modificar: sustituyendo e en C' por (v_1, v_2), seguido de C'', y seguido de (v_2, v_3).

Teorema. [en el texto de Rosen: "teorema de los apretones de manos"]. Sea $G = (V, E)$ un grafo con $n = |V|$ vértices y $m = |E|$ aristas. Se cumple que

$$\sum_{i=1}^{n} \delta(v_i) = 2m \tag{10.1}$$

En particular, la suma de los grados de todos los vértices de un grafo es un número par. Demostración: cada arista contribuye en 2 unidades a la suma de los grados de los vértices, pues cada arista incide en 2 vértices, posiblemente iguales. Eso significa que la suma de los grados de todos los vértices, debe ser igual al doble del número de aristas. Demostración:

Teorema. [en el texto de Johnsonbaugh figura como un corolario del teorema anterior]. Todo grafo $G = (V, E)$ tiene un número par de vértices de grado impar. Demostración: sean V_P y V_I los conjuntos de vértices de grado par e impar, respectivamente, de G. Entonces, descomponemos la suma de los grados de todos los vértices en 2 sumas:

$$\sum_{v \in V_P} \delta(v) + \sum_{v \in V_I} \delta(v) = 2M \tag{10.2}$$

- Como $\delta(v)$ es par si $v \in V_P$, la primera sumatoria es la suma de números pares, por lo que es un número par.
- Además la suma de ambas sumatorias es otro número par, e igual a $2M$. En consecuencia la segunda sumatoria debe ser otro número par.
- Pero todos los términos en la segunda sumatoria son números impares, por lo que debe haber un número par de sumandos. En conclusión, debe haber un número par de vértices de grado impar.

Teorema. Sea $G = (V, E)$ un grafo, y dos vértices u y v cualesquiera de G, con $u \neq v$. Se tiene que: el grafo G tiene una ruta sin aristas repetidas de u a v que contiene todas las aristas y vértices ssi es conexa y u y v son los únicos vértices de grado impar. Demostración (primera parte): suponemos que el grafo G tiene una ruta P sin aristas repetidas de u a v que contiene todas las aristas y vértices. Entonces, el grafo G debe ser conexo. Si se agrega una arista (u, v), el grafo G' tiene un ciclo de Euler, i.e. la ruta P junto con la arista agregada (u, v). Por teorema anterior, cada vértice tiene grado par. Al eliminar la arista agregada solo afecta a los grados de u y v, que se reducen en 1. Entonces, en la ruta original, u y v tienen grado impar y todos los otros vértices tienen grado par. Demostración (segunda parte): suponemos que el grafo G es conexo y tiene exactamente dos vértices u y v de grado impar. Provisoriamente, se agrega la arista $e = (u, v)$ resultando el grafo G', el cual es conexo y cada vértice tiene grado par. Por teorema anterior, G' tiene un ciclo

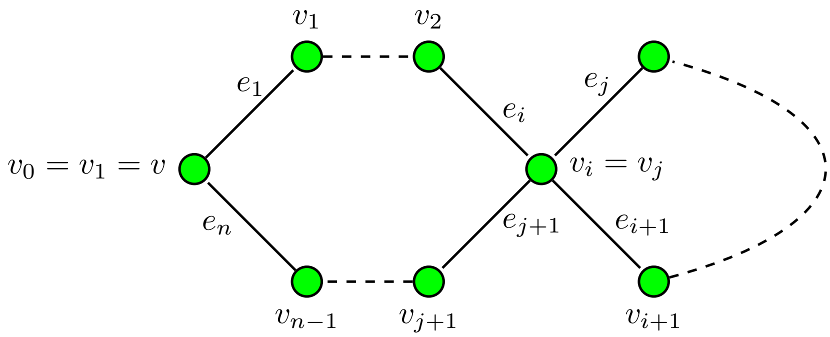

Figura 10.18: Un ciclo C que, o bien es simple, o bien se puede reducir a uno ciclo simple.

de Euler. Si se elimina la arista e de este ciclo de Euler, se obtiene una ruta sin aristas repetidas de u a v que contiene todas las aristas y vértices de G.

Teorema. Sea $G = (V, E)$ un grafo, y un vértice u cualequiera de G. El grafo G contiene un ciclo de v a v, entonces G contiene un ciclo simple de v a v. Demostración: sea el ciclo $C = (v_0, e_1, v_1, ..., e_i.v_i, e_{i+1}, ..., e_j, v_j, e_{j+1}, ..., e_n, v_n)$ de v a v, donde $v = v_0 = v_n$, ver Fig. 10.16. Si C no es un ciclo simple, entonces $v_i = v_j$ para algún $i < j < n$. Se sustituye C por el ciclo $C' = (v_0, e_1, v_1, ..., e_i.v_i, e_{j+1}, ..., e_n, v_n)$. Si C' no es un ciclo simple de v a v, entonces se repite el procedimiento hasta obtener un ciclo simple de v a v.

10.5. Ciclo y trayectoria de Hamilton

Definición. Sea un grafo $G = (V, E)$, y un vértice u cualquiera de G:

- *Ciclo de Hamilton* (o *circuito de Hamilton*) [CH]: un CH es un ciclo (ruta de u a u de longitud mayor a cero sin aristas repetidas), y que contiene a **todos** los vértices del grafo G;
- Es decir, en un CH comienza en un vértice, visita cada vértice exactamente una vez (excepto por el inicial que se visita dos veces: al inicio y al final de ciclo), y regresa al vértice de inicio;
- *Trayectoria de Hamilton* [TH]: es una trayectoria que pasa por cada vértice de G exactamente sólo una vez;

Ejemplo. En los grafos conexos trazados en la Fig. 10.19:

- En el grafo G_1 (izq.): un ciclo de Hamilton es $C_1 = (v_1, v_2, v_3, v_4, v_5, v_1)$, y una trayectoria de Hamilton es $T_3 = (v_1, v_2, v_3, v_4, v_5)$;
- En el grafo G_2 (med.): no tiene ciclo de Hamilton ni trayectoria de Hamilton;
- En el grafo G_3 (der.): no tiene un ciclo de Hamilton, pero si trayectoria de Hamilton, e.g. $T_3 = (v_1, v_2, v_3, v_4)$.

Observación. Sobre la existencia de los ciclos de Hamilton:

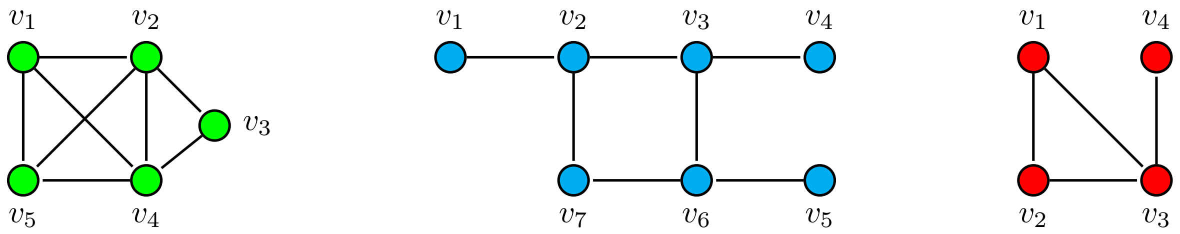

Figura 10.19: Grafo G_1 (izq.): con ciclo de Hamilton y con trayectoria de Hamilton; grafo G_2 (med.): no tiene ciclo de Hamilton ni trayectoria de Hamilton; grafo G_3 (der.): no tiene ciclo de Hamilton, pero si una trayectoria de Hamilton.

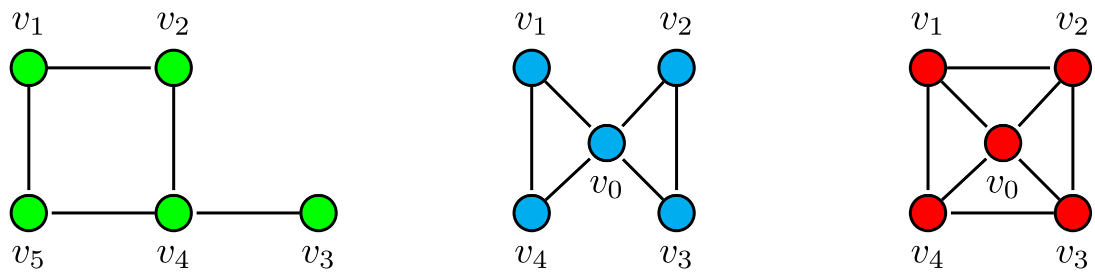

Figura 10.20: Grafo G_1 (izq.) y grafo G_2 (cen.): ninguno tiene un ciclo de Hamilton. Pero el grafo G_3 (der.) sí tiene un ciclo de Hamilton.

- No se conoce una manera sencilla de determinar si un grafo G tiene un ciclo o una trayectoria de Hamilton, lo cual contrasta fuertemente con la tarea de determinar si un grafo tiene un ciclo de Euler porque ahí, simplemente, aplicamos el teorema de Euler. Es decir, para determinar la existencia de los ciclos de Hamilton en G no se conocen criterios simples (necesarios y suficientes);
- Sin embargo, se conocen diversos resultados parciales que dan condiciones suficientes para la existencia de los ciclos de Hamilton;
- Por otra parte, ciertas propiedades pueden usarse para mostrar que un grafo G no tiene un ciclo de Hamilton. Por ejemplo:
  - Un grafo con un vértice de grado 1 no puede tener un ciclo de Hamilton, porque en un ciclo de Hamilton cada vértice es incidente en otros dos vértices del ciclo;
  - Si un vértice en el grafo G tiene grado 2, entonces ambas aristas que inciden con ese vértice deben ser parte de cualquier ciclo de Hamilton;
  - Cuando se va construyendo un ciclo de Hamilton y el mismo ha pasado a través de un vértice, entonces todas las aristas incidentes en ese vértice que no se usaron (distintas de las dos utilizados en el ciclo que se intenta construir), pueden ser eliminadas en la subsiguiente búsqueda;
  - Un ciclo de Hamilton no puede contener otro ciclo de Hamilton más pequeño dentro del mismo.

Ejemplo. En los grafos conexos trazados en la Fig. 10.20:

- En el grafo G_1 (izq.): no tiene un ciclo de Hamilton porque G_1 tiene un vértice de grado 1;

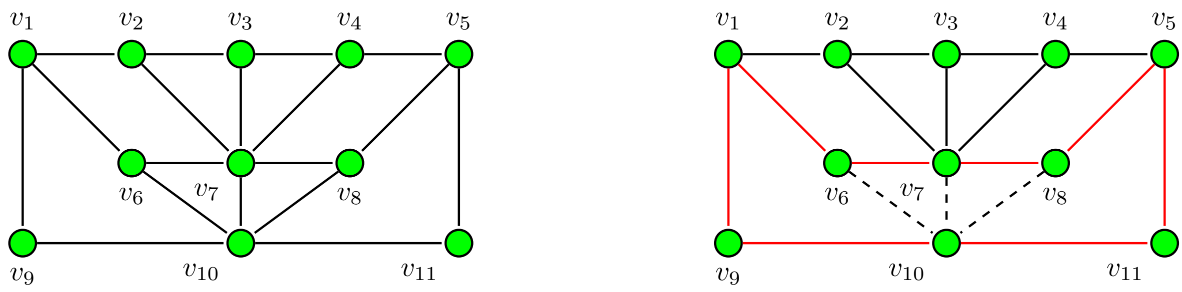

Figura 10.21: Grafo G (izq.). Se traza un ciclo C en G (en rojo a la der.): todos sus vértices tienen grado 2, pero al intentar agregar una arista algún vértice v pasa a $\delta(v) > 2$, por lo que G no tiene un CH.

- En el grafo G_2 (cen.): los vértices v_1, v_2, v_3, v_4 tienen grado 2, por lo que las aristas incientes en esos vértices deben ser parte del ciclo de Hamilton, pero entonces todo CH debe tener las 4 aristas incidentes en v_0, entonces hay que pasar dos veces por v_0. Por eso, G_2 tampoco tiene un ciclo de Hamilton;
- En cambio, en el grafo G_3 (der.): un ciclo de Hamilton es $C_1 = (v_1, v_2, v_3, v_4, v_0, v_1)$.

Ejemplo. En el grafo conexo G trazado en la Fig. 10.21 (izq.):

- Como v_9 tiene grado 2, sus aristas incidentes (v_9, v_1) y (v_9, v_{19}) son parte del CH que se intenta trazar, marcadas en rojo en la Fig. 10.21 (der.);
- Como v_{11} tiene grado 2, sus aristas incidentes (v_{11}, v_{10}) y (v_{11}, v_5) también son parte del CH que se intenta trazar, marcadas en rojo en la Fig. 10.21 (der.);
- Dado las dos aristas ocupadas en v_{10}, las restantes aristas incidentes en v_{10} no pueden estar en el CH que se intenta trazar, marcado en punteado en la Fig. 10.21 (der.);
- Entonces, las aristas (v_1, v_6), (v_6, v_7), y (v_7, v_8), (v_8, v_5), también deben estar en el CH, con lo que resulta el ciclo C trazado en la Fig. 10.21 (der.);
- Ahora, al intentar alguna arista adicional a C, se obtiene un ciclo con algún vértice v con grado $\delta(v) > 2$, lo que no es posible en un CH. Por eso, este grafo no tiene un CH.

10.6. Algoritmo de Dijkstra

Enunciado. Algoritmo de Dijkstra: sea un grafo ponderado $G = (V, E, W)$, donde V es el conjunto de vértices, V es el conjunto de aristas, y W es el conjunto de pesos de las aristas (valores no-negativos), y un par de vértces inicial (o de partida) v_a y final v_z (o de llegada) en G:

- El Algoritmo de Dijkstra (AD) permite encontrar una trayectoria de menor peso (o Ruta de Peso Mínimo (RPM)) entre los vértices v_a y v_z.
- Con una modificación simple en el algoritmo básico incluso se admite grafos G no-conexos (ver ejercicio de la GTP, y se pregunta en examen), resultando un AD Modificado (ADM).

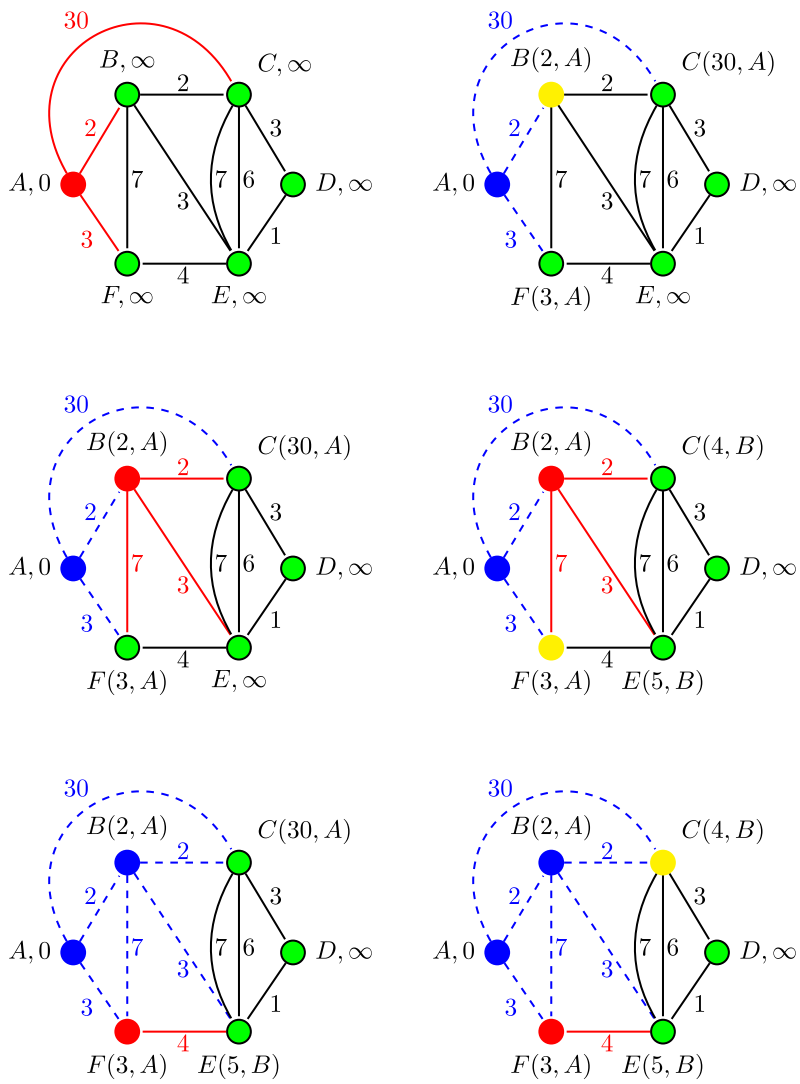

Figura 10.22: AD para hallar una RPM desde el vértice A hacia el D. Vértice de peso mínimo u elegido y aristas adyacentes a u (en rojo) [izq.]. Eventual cambio de los pesos de los vértices adyacentes a u, y siguienteo vértice de peso mínimo (en amarillo) [der.].

- El ADM asigna una etiqueta $L(v)$ a cada vértice v. En cada iteración, algunos vértices tienen etiquetas *temporales* y otros tienen etiquetas *permanentes*.
- Sean T y P los conjuntos de vértices con etiquetas *temporales* y *permanentes*, respectivamente.
- Se puede demostrar que si $L(v)$, con $v \in P$, es la etiqueta permanente del vértice v, entonces $L(v)$ es la longitud de una RMC desde v_a hacia v.
- Al inicio, como *condición inicial* para **todo** el grafo, el vértice de partida v_a tiene etiqueta temporal 0, y los demás vértices tienen etiquetas temporales ∞.
- En el caso en que los vértices de partida v_a y de llegada v_z están en una misma componente conexa, el AD terminará cuando el vértice de llegada v_z se le asigne una etiqueta *permanente*. Cuando eso ocurre, $L(v_z)$ es la longitud de una RPM desde v_a hacia v_z. En ese caso, como una verificación en examen, $L(v_z)$ debe coincidir con la

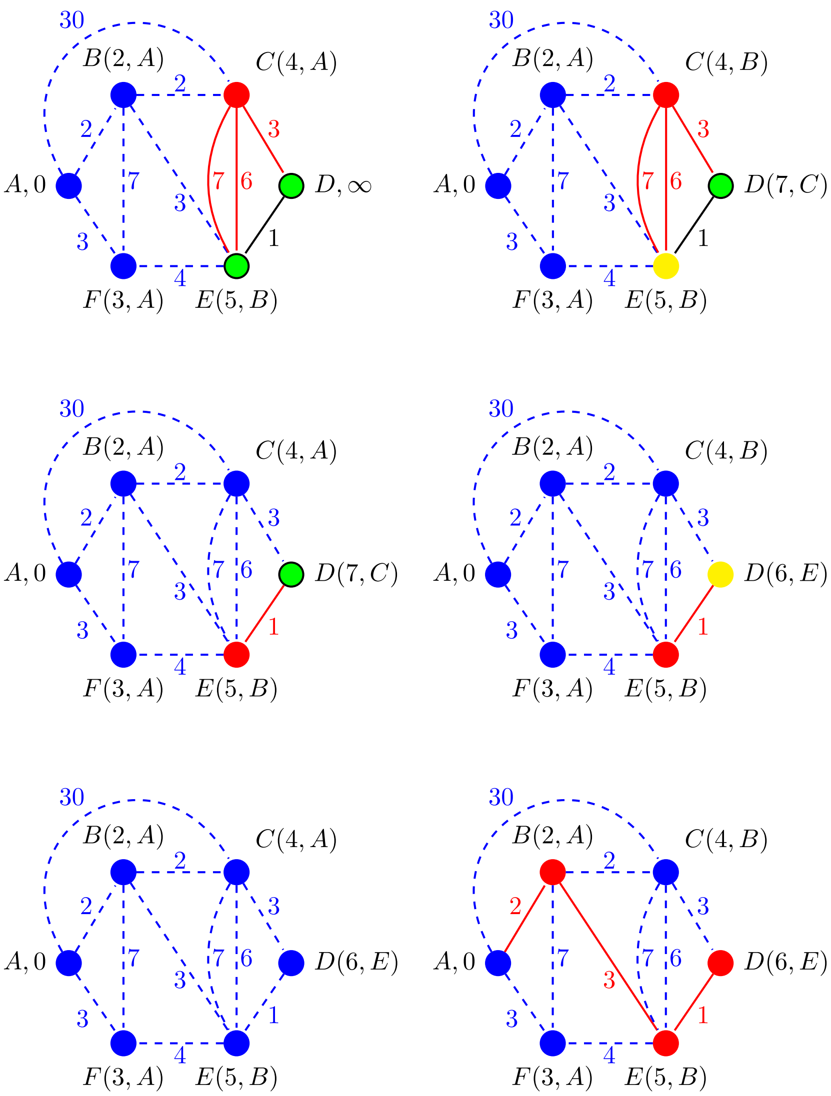

Figura 10.23: Algoritmo de Dijkstra (continuación de la Fig. 10.22.

suma de los pesos de todas las aristas de la RPM hallada.

- En cada iteración del ADM se cambia el estado de alguna etiqueta de vértice de *temporal* a *permanente* de la siguiente manera:
  - En el grafo actual, se busca el vértice temporal $u = v_{\text{min}}$ con el *menor* peso $L(u)$, y se lo marca como un vértice con peso *permanente* (en color rojo en la Fig. del ejemplo siguiente);
  - Si $u = v_z$, entonces fin del ADM, retornando $L(v_z)$ y la RPM;
  - En cambio, si el peso del vértice u es $L(u) = \infty$, entonces se aborta;
  - En otro caso, para **todos** los vértices *temporales v adyacentes* a u, se calcula el peso test
  $$L_{\text{test}}(v) = L(u) + L[(u, v)] \tag{10.3}$$
  y, solo si es menor que el peso actual $L(v)$, entonces se cambia $L(v)$ con el peso test $L_{\text{test}}(v)$;

- Además, para recordar de donde provino el cambio del peso y poder re-construir la RPM, se recuerda en el vértice v al vértice u que ocasionó el decremento mediante la dupla $(L_{\text{test}}(v), u)$.

- Explicación del caso $L(u) = \infty$:
  - Dado que existe al menos una trayectoria entre cada par de vértices ubicados dentro de una misma CC, el test de la Ec. (10.3) siempre dispondrá de vértices adyacentes, y cambiará gradualmente los pesos iniciales ∞ de algunos vértices por otros valores menores;
  - Si los vértices de partida v_a y de llegada v_z están en una misma CC, entonces existe al menos una trayectoria entre v_a y v_z, por lo que siempre habrán vértices adyacentes disponibles para el test de la Ec. (10.3);
  - Como entre CC diferentes no hay aristas que las vinculen, el test de la Ec. (10.3) no-podrá cambiar los pesos temporales de los vértices ubicados en otras CC;
  - Cuando todos los vértices temporales disponibles en la CC del vértice de partida v_a se eligieron como vértices de peso mínimo, y ninguno corresponde al de llegada v_z, en la siguiente iteración se elegirá un vértice ubicado en otra CC;
  - Pero, como no hay conexón entre la CC del v_a y las restantes CC, entonces todos los vértices temporales de las restantes CC mantuvieron el peso inicial ∞;
  - Entonces, cuando se elige un vértice u con peso $L(u) = \infty$, se está eligiendo por primera vez un vértice ubicado en otra componente conexa, y no será posible continuar.

Ejemplo. En el grafo conexo G trazado en la Fig. 10.22 (arriba-izq.), encontrar una RPM desde el vértice A hacia el D. Solución: el desarrollo del AG se muestra con los grafos trazados en las Figs. 10.22-10.23. Luego de finalizar, una RPM es $R = (D, G, B, A)$, y su peso es $L(D) = 5$, y se marca en rojo en la Fig. 10.23 (abajo-derecha). Se verifica que $L(D) = 1 + 3 + 2 = 5$, i.e. es igual a la suma de los pesos $L[(D, E)]$, $L[(E, B)]$, y $L[(B, A)]$ de esas aristas.

10.7. Representaciones de grafos

Definición. Sea un $G = (V, E)$, con $n = |V|$ vértices y $m = |E|$ aristas, con un orden arbitrario dado para los vértices y aristas, posiblemente no-simple (con lazos o aristas paralelas):

- Matriz de *adyacencia*: la matriz de *adyacencia* $\boldsymbol{A}$ de G tiene n filas y n columnas, siguiendo el orden dado a los vértices, y con valores enteros según:

$$[\boldsymbol{A}]_{i,j} = \begin{cases} k & \text{si hay } k \text{ aristas paralelas } (v_i, v_j)\text{, con } i \neq j \\ 2z & \text{si hay } z \text{ lazos } (v_i, v_i) \\ 0 & \text{en otro caso} \end{cases} \tag{10.4}$$

  Nota: cuando G es un grafo *simple*, la Ec. (10.4) se reduce a la dada en el texto de

Johnsonbaugh:

$$[\boldsymbol{A}]_{i,j} = \begin{cases} 1 & \text{si la arista } (v_i, v_j) \in E, \text{ con } i \neq j \\ 2z & \text{si hay } z \text{ lazos } (v_i, v_i) \\ 0 & \text{en otro caso} \end{cases} \tag{10.5}$$

- Matriz de *incidencia*: la matriz de *incidencia* $\boldsymbol{I}$ de G tiene n filas y m columnas, siguiendo el orden dado, y con valores enteros según:

$$[\boldsymbol{I}]_{i,j} = \begin{cases} 1 & \text{si el vértice } v_i \text{ es incidente en la arista } e_j \\ 0 & \text{en otro caso} \end{cases} \tag{10.6}$$

Observación.

- La matriz de adyacencia $\boldsymbol{A}$ es cuadrada y simétrica;
- La suma de la fila o de la columna del vértice v_i es igual al grado $\delta(v_i)$;
- La matriz de adyacencia depende del ordenamiento dado a los vértices, y como hay $n!$ formas de enumerar los vértices, hay $n!$ matrices de adyacencia distintas para mismo un grafo G dado de n vértices;

Ejemplo. En los grafos trazados en la Fig. 10.24:

- En el grafo simple G_1 (izq.):

$$\boldsymbol{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ \delta(v_i) \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} \\ \begin{array}{ccccc} 3 & 3 & 2 & 3 & 3 \end{array} \end{array} \begin{array}{c} \delta(v_i) \\ 3 \\ 3 \\ 2 \\ 3 \\ 3 \\ \\ \end{array} \tag{10.7}$$

- En el grafo no-simple G_2 (der.):

$$\boldsymbol{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ \delta(v_i) \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \begin{bmatrix} 0 & 3 & 0 & 1 & 2 \\ 3 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 2 \\ 2 & 0 & 0 & 2 & 4 \end{bmatrix} \\ \begin{array}{ccccc} 6 & 6 & 0 & 4 & 8 \end{array} \end{array} \begin{array}{c} \delta(v_i) \\ 6 \\ 6 \\ 0 \\ 4 \\ 8 \\ \\ \end{array} \tag{10.8}$$

Observar la fila y columna nulas del vértice v_3.

Teorema. [**Conteo de trayectorias de longitud** p **en un grafo** G]: sea $G = (V, E)$ un grafo *simple* de n vértices, y la matriz de adyacencia $\boldsymbol{A}$ asociada a G, con respecto a un orden dado. Se cumple que: la entrada ij (en la fila i y columna j) de la potencia $\boldsymbol{A}^p$ es igual al número de trayectorias de longitud p entre los vértices i y j, para $p = 1, 2, ...$
Demostración (por inducción sobre p).

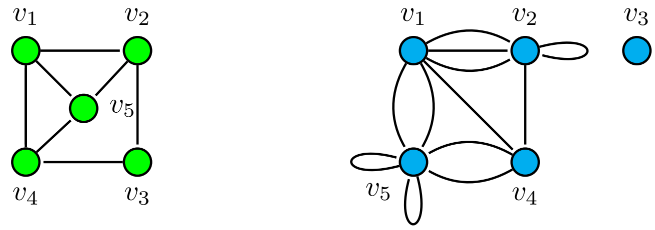

Figura 10.24: G_1: grafo simple (sin lazos ni aristas paralelas) (izq.). G_2: grafo no-simple (con lazos o aristas paralelas) (der).

- Paso Base ($p = 1$): si $p = 1$, $\boldsymbol{A}^1$ se reduce a $\boldsymbol{A}$. La entrada ij es 1 si hay una arista de i a j, lo cual representa una trayectoria de longitud 1, y 0 en otro caso, entonces se verifica el PB.
- Paso Inductivo: suponemos que el teorema es cierto para algún entero p, positivo y abitrario pero fijo, y vemos qué sucede con $p + 1$. Calculamos $\boldsymbol{A}^{p+1}$ con el producto matricial $\boldsymbol{A}^{p+1} = \boldsymbol{A}^p\boldsymbol{A}$, i.e. la entrada ij en $\boldsymbol{A}^{p+1}$ se obtiene al multiplicar por pares los elementos en la fila i de $\boldsymbol{A}^p$ por los elementos de la columna j de $\boldsymbol{A}$, y después sumamos:

$$\begin{array}{c} \\ \text{fila } i \text{ de } \boldsymbol{A}^p : \end{array} \begin{array}{c} \\ \begin{bmatrix} s_1 & s_2 & \dots & s_k & \dots & s_n \end{bmatrix} \times \end{array} \begin{array}{c} \text{columna } j \text{ de } \boldsymbol{A} \\ \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_k \\ \vdots \\ t_n \end{bmatrix} \end{array} \tag{10.9}$$

$$= s_1t_1 + s_2t_2 + \dots + s_kt_k + \dots s_nt_n$$
$$= \text{entrada } ij \text{ de } \boldsymbol{A}^{p+1}$$

Por la HI, s_k es el número de trayectorias de longitud p de i a k en el grafo G. Como la última arista es (k, j), Fig. 10.25, y t_k vale 0 o 1:
  - Si $t_k = 0$ no hay arista (k, j), por lo que hay $s_kt_k = s_k \cdot 0 = 0$ trayectorias de longitud $p + 1$ de i a j;
  - Si $t_k = 1$, hay una arista (k, j). Como hay s_k trayectorias de longitud p del vértice i al k, entonces hay $s_kt_k = s_k \cdot 1 = s_k$ trayectorias de longitud $p + 1$ de i a j;
  - Al sumar sobre k se cuentan todas las trayectorias de longitud $p + 1$ de i a j. Entonces, la entrada ij en $\boldsymbol{A}^{p+1}$ es igual al número de trayectorias de longitud $p + 1$ de i a j, y se prueba el paso inductivo.

10.8. Isomorfismo de grafos (nociones)

Definición.

- Los grafos G_1 y G_2 son *isomorfos* si existe una dupla de funciones (f, g) *biyectivas*, en donde f mapea los vértices de G_1 a los vértices de G_2, y f mapea las aristas de G_1

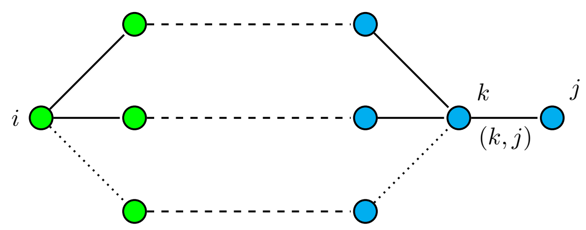

Figura 10.25: Una trayectoria de i a j de longitud $p + 1$ cuyo penúltimo vértice es k consiste en una trayectoria de longitud p de i a k, seguida de la arista (k, j). Si hay s_k trayectorias de longitud p de i a k, y t_k vale 1 si está la arista (k, j) y 0 en otro caso, entonces la suma de $s_k t_k$ sobre toda k da el número de trayectorias de longitud $p + 1$ de i a j.

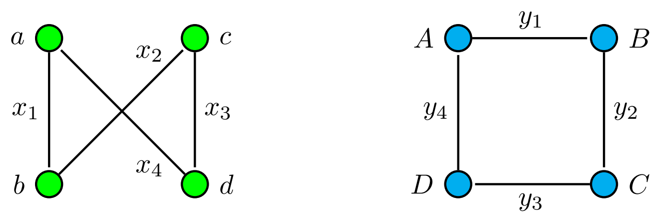

Figura 10.26: Los grafos G_1 (izq.) y G_2 son isomorfos.

a las aristas de G_2, de modo tal que que una arista e es incidente en los vértices u y v de G_1 ssi la arista $g(e)$ es incidente en $f(u)$ y en $f(v)$ en G_2.

- La tupla de funciones $f, g)$ definen el *isomorfismo* de G_1 en G_2.

Ejemplo. En la Fig. 10.26 se muestran los grafos G_1 (izq.) y G_2 (der.):

- El grafo G_1 tiene los 4 vértices: a, b, c, d, y las 4 aristas: (a, b), (b, c), (c, d), y (d, a);
- El grafo G_2 tiene los 4 vértices: A, B, C, D, y las 4 aristas: (A, B), (B, C), (C, D), y (D, A).
- Los grafos G_1 y G_2 son isomorfos, en donde el isomorfismo es descripto por la tupla de funciones:

$$\begin{array}{cccc} f(a) = A & f(b) = B & f(c) = C & f(d) = D \\ g(x_1) = y_1 & g(x_2) = y_2 & g(x_3) = y_3 & g(x_4) = y_4 \end{array} \tag{10.10}$$

Observación.

- En general, la matriz de adyacencia de un grafo cambia cuando se modifica el orden de los vértices.
- No obstante, los grafos $_1$ y G_2 resultan isomorfos ssi para algún orden de sus vértices, sus matrices de adyacencia son iguales.

Teorema. Sean los grafos G_1 y G_2 ambos de n vértices. Entonces, G_1 y G_2 son isomorfos ssi, para algún orden de sus vértices, sus matrices de adyacencia $\boldsymbol{A}_1$ y $\boldsymbol{A}_2$ son iguales. Demostración:

- Suponemos que G_1 y G_2 son isomorfos, por lo que existe una tupla de funciones biyectivas (f, g), con una función f de los vértices de G_1 a los de G_2, y una función g de las aristas de G_1 a las de G_2, de modo tal que una arista e incide en los vértices u y v ssi la arista $g(e)$ incide en $f(u$ y en $f(v)$ en G_2;

- Sea $u_1, u_2, ..., u_n$ un orden de los vértices de G_1, y $\boldsymbol{A}_1$ la matriz de adyacencia de G_1 relativa a dicho orden;
- Sea $\boldsymbol{A}_2$ la matriz de adyacencia de G_2 relativa al orden $f(u_1), f(u_2), ..., fu_n$ un orden de los vértices de G_2;
- Supongamos que la entrada i, j (fila i, columna j, con $i \neq j$) de $\boldsymbol{A}_1$ es igual k. Entonces existen k aristas $e_1, e_2, ...e_k$ incidentes en u_i y en u_j;
- En ese caso, hay otras k aristas $g(e_1), ..., g(e_k)$ incidentes en $f(u_i)$ y en $f(u_j)$ en G_2;
- Por eso, la entrada i, j en $\boldsymbol{A}_2$, que cuenta el número de aristas que inciden en $f(u_i)$ y en $f(u_j)$ también es igual k;
- Un razonamiento similar muestra que las entradas diagonales de $\boldsymbol{A}_1$ y $\boldsymbol{A}_2$ también son iguales;
- Por lo que debe ser $\boldsymbol{A}_1 = \boldsymbol{A}_2$.

Enunciado. Sean los grafos $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ isomorfos. Entonces las siguientes enunciados son equivalentes:

- G_1 y G_2 son isomorfos;
- Existe una función biyectiva f de V_1 a V_2 en donde: los vértices u y v son adyacentes en G_1, ssi los los vértices $f(u)$ y $f(v)$ son adyacentes en G_2.

Ejemplo. Para los grafos G_1 y G_2 mostrados en la Fig. 10.26 (izq. y der.) se tiene que la matriz de adyacencia de G_1 relativa al orden a, b, c, d es

$$\boldsymbol{A}_1 = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{array} \tag{10.11}$$

y que es igual a la matriz de adyacencia de G_2, relativa al orden A, B, C, D, i.e.

$$\boldsymbol{A}_2 = \begin{array}{c} \\ A \\ B \\ C \\ D \end{array} \begin{array}{c} \begin{array}{cccc} A & B & C & D \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{array} \tag{10.12}$$

por lo que G_1 y G_2 son grafos isomorfos.

Definición. Invariante: sean dos grafos G_1 y G_2 isomorfos. Se dice que la propiedad P es un *invariante* si G_1 tiene la propiedad P, entonces G_2 también tiene la propiedad P.

Observación. Si G_1 y G_2 son isomorfos, entonces G_1 y G_2 tienen:

- Un mismo número de vértices, por lo que la propiedad "tiene n vértices" es un invariante, con $n \geq 0$;
- Un mismo número de aristas, por lo que la propiedad "tiene e aristas" es un invariante, con $e \geq 0$;;

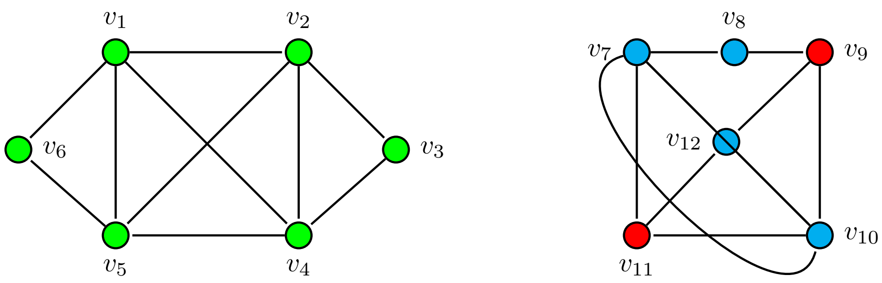

Figura 10.27: Los grafos G_1 (izq.) y G_2 tienen 6 vértices y 10 aristas cada uno, pero G_1 no tiene vértices de grado 3 mientras que G_2 tiene 2 (en rojo), por lo que no son isomorfos.

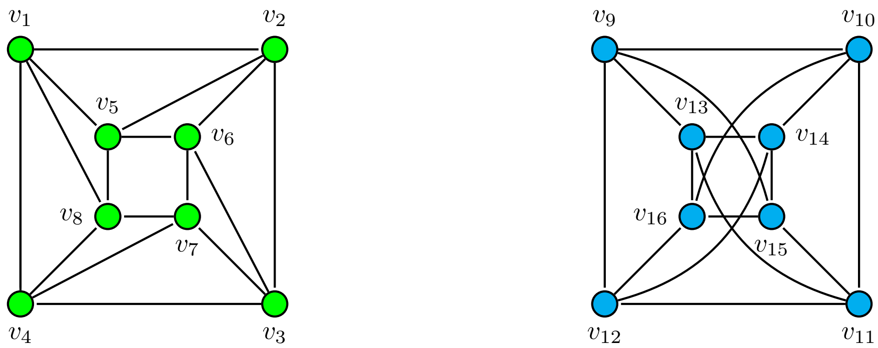

Figura 10.28: Los grafos G_1 (izq.) y G_2 tienen 8 vértices, 16 aristas, y 8 vértices de grado 4 cada uno, pero G_1 tiene ciclos simples de longitud 3 mientras que G_2 no, por lo que no son isomorfos.

- La misma cantidad de vértices de igual grado, por lo que la propiedad ”tiene un vértice de grado k” es un invariante, con $k \geq 0$;
- La misma cantidad de ciclos simples de longitud k, por lo que la propiedad ”tiene un ciclo simple de longitud k” es un invariante, con $k \geq 3$;
- Nota: hay muchos otros invariantes que no veremos.

Ejemplo. En la Fig. 10.27 se muestran los grafos G_1 (izq.) y G_2 (der.), en donde:

- Ambos tienen 6 vértices cada uno;
- Ambos tienen 10 aristas cada uno;
- G_1 no tiene vértices de grado 3, pero G_2 tiene 2, por lo que G_1 y G_2 no son isomorfos.

Ejemplo. En la Fig. 10.28 se muestran los grafos G_1 (izq.) y G_2 (der.), en donde:

- Ambos tienen 8 vértices cada uno;
- Ambos tienen 16 aristas cada uno;
- Cada vértice en G_1 y en G_2 tiene grado 4;
- Los ciclos simples en G_1 son de longitud 3, pero en G_2 los ciclos simples son de longitud 4, por lo que G_1 y G_2 no son isomorfos.

10.9. Grafos planos (nociones)

Definición.

- Grafo *plano*: un grafo $G = (V, E)$ conexo y simple (simple: no hay lazos ni aristas paralelas), es un grafo *plano* si puede trazarse sobre una superficie sin que se crucen sus aristas. Tal trazado se denomina una *representación planar* del grafo.
- *Cara* o *región* f: es cada una de las regiones contiguas en que queda dividida una superficie por un grafo plano (incluyendo la región no-acotada), y queda delimitada por el ciclo de frontera;
- Cara exterior (o región exterior): está definida por la región no-acotada.
- Grado de una cara G_f (o región G_r): es igual al número de aristas que hay en el ciclo de frontera;
- En un grafo plano, cada arista pertenece al menos a 2 ciclos frontera (e.g. verlo en K_3);
- *Fórmula de Euler* (FE) para un grafo plano: si G es un grafo conexo, simple, y plano, tiene v vértices, e aristas, y f caras, entonces se verifica que:

$$f = e - v + 2 \tag{10.13}$$

  esto es: todas las representaciones planares de un grafo dividen al plano en un mismo número de regiones.

Observación.

- El grafo completo K_4 (Fig. 10.29, arriba), y el hipercubo Q_3 (Fig. 10.29, abajo), son grafos planos;
- El grafo bipartito completo $K_{3,3}$ no es plano. Demostración:
  - Los ciclos en el grafo bipartito completo $K_{3,3}$ tienen al menos longitud 4, e.g. ver ciclo (v_1, v_3, v_2, v_1) trazado en color rojo en Fig. 10.30 (izq.);
  - Entonces cada cara en $K_{3,3}$ estará delimitada al menos por 4 aristas, y el número e_f de aristas que acotan las caras debe ser $e_f \geq 4f$;
  - En un grafo plano, cada arista contribuye en 2 al grado de cada cara, por lo que $e_f = 2e$ (donde e es el número total de aristas en G);
  - *Suponiendo* que $K_{3,3}$ *fuera* plano, podemos introducir la FE dada por la Ec. (10.13):

$$\begin{aligned} e_f &\geq 4f \\ e_f &= 2e \end{aligned} \quad \therefore \quad 2e \geq 4f = 4(e - v + 2) \tag{10.14}$$

    Como en $K_{3,3}$ hay $v = 6$ vértices, y $e = 9$ aristas, resulta

$$\begin{aligned} 2(9) &\geq 4(9 - 6 + 2) \\ 18 &\geq 20 \end{aligned} \tag{10.15}$$

    lo que no es posible, por lo que $K_{3,3}$ debe ser un grafo no-plano;
- También se puede demostrar que el grafo completo K_5 tampoco es plano, ver Fig. 10.30;

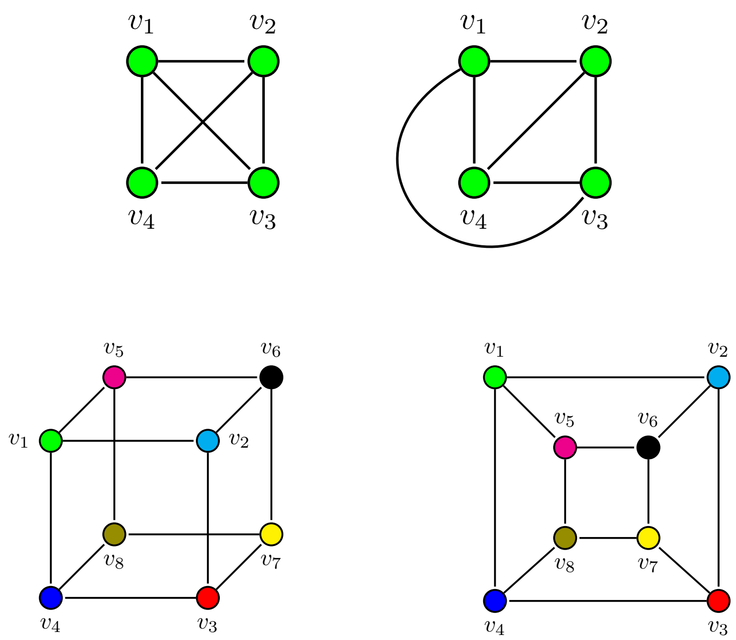

Figura 10.29: El grafo completo K_4 (arriba, izq. y der.), y el hipercubo Q_3 (abajo, izq. y der.) son grafos planos.

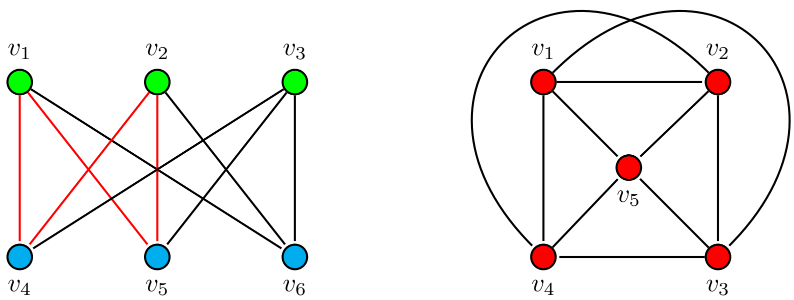

Figura 10.30: El grafo bipartito completo $K_{3,3}$ (izq.) y el completo K_5 (der.) no son grafos planos.

- Además, si un grafo G contiene a $K_{3,3}$ o a K_5 como subgrafos,entonces G no puede ser un grafo plano.

Definición.

- Aristas *en serie*: si un grafo $G = (V, E)$ tiene un vértice v de grado 2, y aristas (v, v_1) y (v, v_2), con $v_1 \neq v_2$, se dice que las aristas (v, v_1) y (v, v_2) están en *serie*;
- *Subdivisión elemental* (en Rosen) o *reducción de una serie* (en Johnsonbaugh): consiste en eliminar el vértice v, y sustitur las aristas (v, v_1) y (v, v_2), con (v_1, v_2), ver Fig. 10.31, yendo de izq. a der.;
- *Suavizado* (o *alisado*): es la operación inversa de la anterior, i.e. introducir el vértice v, y sustitur la arista (v_1, v_2) con (v, v_1) y (v, v_2), ver Fig. 10.31, yendo de der. a izq.;
- Se dice que los grafos G_1 y G_2 son un *homomorfismo* si G_1 y G_2 se pueden obtener mediante una serie de subdivisiones elementales.

Figura 10.31: Subdivisión elemental: de izq. a der.; suavizado (o alisado): de der. a izq.

Figura 10.32: Los grafos G_1 (izq.) y G_2 (der.) son homomorfos: G_2 puede obtenerse de G_1 con 2 subdisiones elementales, y G_1 puede obtenerse de G_2 con 2 suavizados.

Ejemplo. Los grafos G_1 y G_2 mostrados en la Fig. 10.32 son homomorfos porque mediante subdisiones elementales se reducen a G'.

Teorema de Kuratowski: un grafo G no-es plana, ssi G contiene un subgrafo homomorfo a $K_{3,3}$ o a K_5.

APÉNDICE A

Acrónimos y abreviaturas empleadas

A.1. Lista de acrónimos

AE Algoritmo de Euclides

CE Clases de Equivalencia

CI Condiciones Iniciales

DA Diagrama en Arbol

DD Dominio de Discurso

DeD Demostración Directa

DeI Demostración Indirecta

DrA Demostración por Reducción al Absurdo

EC Ecuación Característica

EL Equivalencia Lógica

F Falso (por *False*)

GPL Licencia Pública General de GNU

FP Función Proposicional

GTP Guía de Trabajos Prácticos

idle Integrated DeveLopment Environment

HI Hipótesis Inductiva

LE lógicamente equivalentes

MCD Máximo Común Divisor

MCM Mínimo Común Múltiplo

PB Paso Base

PB Paso Base

PIE Principio de Inclusión-Exclusión

PIF Principio de Inducción Fuerte

PIM Principio de Inducción Matemática

PI Paso de Inducción

PR Paso Recursivo

PS Principio de la Suma

PP Principio del Palomar

PM Principio de la Multiplicación

RB Relación Binaria

RP Reglas de precedencia

RE Relación de Equivalencia

ROP Relación de Orden Parcial

ROT Relación de Orden Total

RR Relación de Recurrencia

RRHLCC Relación de Recurrencia Homogénea, Lineal, de Coeficientes Constantes

T Verdadero (por *True*)

TH Torres de Hanoi

TV Tabla de Verdad

TP Tablas de Pertenencia

VV Valor de Verdad

V Verdadero

A.2. Lista de abreviaturas

i.e. es decir, o esto es, del latín *id est*

e.g. por ejemplo, del latín *exempli gratia*

Bibliografía

[1] N. Biggs. *Matemática discreta*. Ediciones Vicens Vives, S.A., España, 2 edition, 1998.

[2] R. Johnsonbaugh. *Matemáticas discretas*. ISBN 9789702606376. Prentice Hall, Mexico, 6 edition, 2005.

[3] Python. http://www.python.org/, 2014.

[4] K. H. Rosen. *Matemática Discreta y sus Aplicaciones*. ISBN 9788448140731. Mc Graw Hill, Colombia, 5 edition, 2004.

Nomenclatura

Indice alfabético