Problema 1

Para p, q, r proposições elementares, mostre que:

(a) $p \oplus q \iff (p \wedge \neg q) \vee (\neg p \wedge q) \iff \neg(p \leftrightarrow q)$

Usando a definição de que $p \oplus q$ (*xor*) é verdadeiro quando uma ou outra variável for verdadeira, mas não ambas (ou exclusivo), pode-se prosseguir por construção de tabela-verdade:

p	q	$p \wedge \neg q$	$\neg p \wedge q$	$(p \wedge \neg q) \vee (\neg p \wedge q)$	$\neg(p \leftrightarrow q)$	$p \oplus q$
1	1	0	0	0	0	0
1	0	1	0	1	1	1
0	1	0	1	1	1	1
0	0	0	0	0	0	0

em que foram usados atalhos para os NOTs e o fato de que se $p \leftrightarrow q$ é verdadeiro quando p, q tem o mesmo-valor verdade, então $\neg(p \leftrightarrow q)$ é verdadeiro quando tem valores *distintos*. Sabíamos de antemão que teríamos $2^2 = 4$ linhas devido às duas variáveis lógicas p, q. Basta então comparar as últimas três colunas para constatar a equivalência lógica entre elas.

(b) $((p \leftrightarrow q) \wedge (q \leftrightarrow r) \wedge (r \leftrightarrow p)) \iff ((p \rightarrow q) \wedge (q \rightarrow r) \wedge (r \rightarrow p))$

Novamente, com o uso de tabelas-verdade, para o lado esquerdo:

p	q	r	$p \leftrightarrow q$	$q \leftrightarrow r$	$r \leftrightarrow p$	$((p \leftrightarrow q) \wedge (q \leftrightarrow r) \wedge (r \leftrightarrow p))$
1	1	1	1	1	1	1
1	1	0	0	0	0	0
1	0	1	0	0	1	0
1	0	0	0	1	0	0
0	1	1	0	1	0	0
0	1	0	0	0	1	0
0	0	1	1	0	0	0
0	0	0	1	1	1	1

e agora para o lado direito da implicação dupla:

p	q	r	$p \rightarrow q$	$q \rightarrow r$	$r \rightarrow p$	$((p \rightarrow q) \wedge (q \rightarrow r) \wedge (r \rightarrow p))$
1	1	1	1	1	1	1
1	1	0	1	0	1	0
1	0	1	0	1	0	0
1	0	0	0	1	1	0
0	1	1	1	1	0	0
0	1	0	1	0	1	0
0	0	1	1	1	0	0
0	0	0	1	1	1	1

de onde se conclui que as duas expressões lógicas são equivalentes. Novamente, sabíamos de antemão que para cada tabela teríamos $2^3 = 8$ linhas em razão de três variáveis p, q, r.

Problema 2

Sem construir tabelas verdade, mostre que:

[Notação:] *underbraces* indicam a sugestão visual pro próximo passo da dedução, o texto entre colchetes indica a propriedade usada na passagem. Em geral a indicação e o texto em colchetes *não* corresponderão à mesma linha da dedução.

(a) $p \vee (p \wedge (p \vee q)) \iff p$

$$\begin{aligned} p \vee \underbrace{(p \wedge (p \vee q))} &\iff p \wedge p && \text{[Absorção]} \\ &\iff p && \text{[Idempotência]} \end{aligned}$$

(b) $p \vee q \vee (\neg p \wedge \neg q \wedge r) \iff p \vee q \vee r$

$$\begin{aligned} \underbrace{p \vee q} \vee (\underbrace{\neg p \wedge \neg q} \wedge r) &\iff (p \vee q) \vee \big(\underbrace{(\neg p \wedge \neg q)} \wedge r\big) && \text{[Associatividade]} \\ &\iff \underbrace{(p \vee q)} \vee \big(\neg(p \vee q) \wedge r\big) && \text{[De Morgan]} \\ &\iff \underbrace{\big((p \vee q) \vee \neg(p \vee q)\big)} \wedge \big((p \vee q) \wedge r\big) && \text{[Distributividade]} \\ &\iff 1 \wedge \big((p \vee q) \vee r\big) && \text{[Tautologia]} \\ &\iff (p \vee q) \vee r && \text{[Identidade]} \\ &\iff p \vee q \vee r && \text{[Associatividade]} \end{aligned}$$

(c) $((\neg p \vee \neg q) \to (p \wedge q \wedge r)) \iff p \wedge q$

$$\begin{aligned} \big((\neg p \vee \neg q) \to (p \wedge q \wedge r)\big) &\iff \Big(\underbrace{\neg(\neg p \vee \neg q)} \vee (p \wedge q \wedge r)\Big) && \text{[Equivalência lógica]} \\ &\iff \underbrace{(p \wedge q)} \vee (p \wedge q \wedge r) && \text{[De Morgan]} \\ &\iff (p \wedge q) && \text{[Absorção em } p \wedge q\text{]} \end{aligned}$$

Talvez a última passagem pareça obscura. Seja $\phi = p \wedge q$. Então se lê:

$$\phi \vee (\phi \wedge r) \iff \phi,$$

como desejado.

Problema 3

Utilizando as regras de equivalências lógicas (indique-as), simplifique a expressão na CNF[a]:

$$\phi = (p \vee q \vee r) \wedge (p \vee t \vee \neg q) \wedge (p \vee \neg t \vee r)$$

Determine uma ψ na DNF[b] tal que $\phi \iff \psi$. É o caso em que $\psi = \phi^d$, o dual de ϕ? Justifique!

Solução:

$$\begin{aligned}
&(p \vee \underbrace{q \vee r}) \wedge (p \vee \underbrace{t \vee \neg q}) \wedge (p \vee \neg t \vee r) \\
&\qquad \iff \underbrace{p \vee}\,[(q \vee r) \wedge (t \vee \neg q)] \wedge \underbrace{(p \vee}\,\neg t \vee r) && \text{[Distributiva]} \\
&\qquad \iff p \vee \big[\underbrace{(q \vee r)} \wedge (t \vee \neg q) \wedge \underbrace{(\neg t \vee r)}\big] && \text{[Distributiva]} \\
&\qquad \iff p \vee \big[\underbrace{(q \vee r)} \wedge \underbrace{(\neg t \vee r)} \wedge (t \vee \neg q)\big] && \text{[Comutativa]} \\
&\qquad \iff p \vee \big[\underbrace{(r \vee q)} \wedge \underbrace{(r \vee \neg t)} \wedge (t \vee \neg q)\big] && \text{[Comutativa]} \\
&\qquad \iff p \vee \big[\big(r \vee \underbrace{(q \wedge \neg t)}\big) \wedge \underbrace{(t \vee \neg q)}\big] && \text{[Distributiva]} \\
&\qquad \iff p \vee \big[\big(r \vee \underbrace{\neg(t \vee \neg q)}\big) \wedge \underbrace{(t \vee \neg q)}\big] && \text{[De Morgan e Comut.]} \\
&\qquad \iff p \vee \big[\underbrace{\big((t \vee \neg q) \wedge \neg(t \vee \neg q)\big)} \vee \big((t \vee \neg q) \wedge r\big)\big] && \text{[Comut. e Distr.]} \\
&\qquad \iff p \vee \underbrace{\big[0 \vee \big((t \vee \neg q) \wedge r\big)\big]} && \text{[Contradição]} \\
&\qquad \iff p \vee [r \wedge \underbrace{(\neg q \vee t)}] && \text{[Ident. e Comut.]} \\
&\qquad \iff p \vee [r \wedge (q \to t)] && \text{[Implicação]}
\end{aligned}$$

Pela definição de CNF e DNF (notação adaptada das notas de aula), usando que $\bigvee_j x_i = x_1 \vee \cdots \vee x_n$ e o equivalente para $\wedge$, vejamos que a CNF proposta é da forma:

$$\begin{aligned}
\phi = \bigwedge_i \left(\bigvee_j x_j^{a_{ij}} \right) &\iff \phi = \bigwedge_i \left(\bigvee_j x_j^{a_{ij}} \right) && \text{[Comutatividade - indutivo]} \\
&\iff \phi = \neg \left[\bigvee_i \left(\bigwedge_j \neg x_j^{a_{ij}} \right) \right] && \text{[De morgan - indutivo]} \\
&\iff \phi = \neg \left[\bigvee_i \left(\bigwedge_j x_j^{\bar{a}_{ij}} \right) \right] && \text{[Complementação de } a_{ij}\text{]}
\end{aligned}$$

em que cada a_{ij} especifica o valor-verdade de x_j (um valor booleano). Então a negação seria $\neg\phi = \bigvee_i \left(\bigwedge_j x_j^{\bar{a}_{ij}} \right)$ e, por sua vez, a dual seria apenas complementar os expoentes dessa negação, $\phi^d = \bigvee_i \left(\bigwedge_j x_j^{a_{ij}} \right)$. Logo, para as mesmas variáveis, podemos escrever ϕ^d já na DNF:

$$\phi^d = (p \wedge q \wedge r) \vee (p \wedge t \wedge \neg q) \vee (p \vee \neg t \wedge r),$$

em que prontamente se nota a dualização por troca das conjuções por disjunções. Vejamos a dualização da expressão já reduzida (ver penúltimo passo, com identidade e comutação):

$$\phi^d = p \wedge [r \vee (\neg q \wedge t)].$$

Vejamos ainda que tomando $p = 1$, $q = 0$, $r = 0$ e $t = 0$, ϕ assume valor 1 (basta p ser 1) enquanto a dual assume 0 (0 na conjunção mais interna devido ao valor de t, $r = 0$ força outro 0 na disjunção que é anulada e que, por sua vez, zera a conjunção mais externa). Logo qualquer expressão logicamente equivalente à dual ϕ^d *não* será logicamente equivalente a ϕ (e vice-versa), bastando repetir a escolha acima para mostrar.

Em particular, isso é irrespectivo da forma a representar as funções, como por exemplo uma CNF ψ logicamente equivalente a ϕ. Esta ψ, por sua vez, pode ser obtida através da negação das variáveis cujas linhas na tabela-verdade de ϕ resultem em falsidades (método mostrado em [Lehman et al., 2018]).

Tem-se 4 variáveis, portanto, esperamos no total $2^4 = 16$ linhas na tabela-verdade. Expandiremos a expressão inicial para a CNF completa:

$$\begin{aligned}\phi = (p \vee q \vee r \vee t) \wedge (p \vee q \vee r \vee \neg t) \wedge (p \vee \neg q \vee r \vee t) \wedge (p \vee \neg q \vee \neg r \vee t) \wedge \\ \wedge (p \vee \neg q \vee r \vee \neg t)\end{aligned}$$

Indica valor verdade em 5 entradas da tabela-verdade, por 5 cláusulas, a saber (representação vetorial):

$$\mathbf{x}_\phi \in \{(1,1,1,1), (1,1,1,0), (1,0,1,1), (1,0,0,1), (1,0,1,0)\}.$$

Logo, esperamos que a DNF completa possua 11 termos correspondentes aos casos de falsidade da tabela-verdade dados a seguir:

$$\begin{aligned}\bar{\mathbf{x}}_\psi \in \{&(1,1,0,1), (1,1,0,0), (1,0,0,0), (0,1,1,1), (0,1,1,0), (0,1,0,1), \\ &(0,1,0,0), (0,0,1,1), (0,0,1,0), (0,0,0,1), (0,0,0,0)\},\end{aligned}$$

portanto,

$$\begin{aligned}\psi = &(\neg p \wedge \neg q \wedge r \wedge \neg t) \vee (\neg p \wedge \neg q \wedge r \wedge t) \vee (\neg p \wedge q \wedge r \wedge t) \vee (p \wedge \neg q \wedge \neg r \wedge \neg t) \\ &\vee (p \wedge \neg q \wedge \neg r \wedge t) \vee \vee (p \wedge \neg q \wedge r \wedge \neg t) \vee (p \wedge \neg q \wedge r \wedge t) \vee (p \wedge q \wedge \neg r \wedge \neg t) \\ &\vee (p \wedge q \wedge \neg r \wedge t) \vee (p \wedge q \wedge r \wedge \neg t) \vee (p \wedge q \wedge r \wedge t)\end{aligned}$$

que poderia ser simplificada, mas não o faremos.

[a] *Conjunctive Normal Form*.
[b] *Disjunctive Normal Form*.

Problema 4

Defina o operador *nand* de *not . . . and . . .*, por $p \uparrow q \iff \neg(p \wedge q)$, para proposições p, q. Represente as operações abaixo utilizanndo somente este novo operador.

Nota: o presente exercício (ou variações, ou partes dele) é comum em bibliografias sobre Eletrônica Digital/Sistemas Digitais (a exemplo de [Widmer et al., 2017]). O exercício será então feito constatando a expressão desejada e mostrando que se reduz ao item (o processo de dedução manual, feita em um caderno, é usualmente feito na direção contrária).

(a) $\neg p$

$$\begin{aligned} p \uparrow p &\iff \neg(p \wedge p) && \text{[Definição]} \\ &\iff \neg p && \text{[Idempotência]} \end{aligned}$$

(b) $p \vee q$

$$\begin{aligned} (p \uparrow p) \uparrow (q \uparrow q) &\iff \neg(\neg p \wedge \neg q) && \text{[Definição e Item a)]} \\ &\iff p \vee q && \text{[De Morgan]} \end{aligned}$$

(c) $p \wedge q$

$$\begin{aligned} (p \uparrow q) \uparrow (p \uparrow q) &\iff \neg(p \uparrow q) && \text{[Item a)]} \\ &\iff \neg\big(\neg(p \wedge q)\big) && \text{[Definição]} \\ &\iff p \wedge q && \text{[Negação dupla]} \end{aligned}$$

(d) $p \to q$

$$\begin{aligned} [(p \uparrow p) \uparrow (p \uparrow p)] \uparrow (q \uparrow q) &\iff (\neg p \uparrow \neg p) \uparrow (q \uparrow q) && \text{[Item a) duas vezes]} \\ &\iff \neg p \vee q && \text{[Item b)]} \\ &\iff p \to q && \text{[Implicação]} \end{aligned}$$

(e) $p \leftrightarrow q$

A sequência de passos é bastante extensa, mas basta notar que:

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$

e usar os itens d) e c):

$$\big((p \to q) \uparrow (q \to p)\big) \uparrow \big((p \to q) \uparrow (q \to p)\big)$$

$$\Big(\Big\{\big[(p\uparrow p)\uparrow(p\uparrow p)\big]\uparrow(q\uparrow q)\Big\}\uparrow\Big\{\big[(q\uparrow q)\uparrow(q\uparrow q)\big]\uparrow(p\uparrow p)\Big\}\Big)\uparrow$$
$$\uparrow\Big(\Big\{\big[(p\uparrow p)\uparrow(p\uparrow p)\big]\uparrow(q\uparrow q)\Big\}\uparrow\Big\{\big[(p\uparrow p)\uparrow(p\uparrow p)\big]\uparrow(q\uparrow q)\Big\}\Big)$$

Agora, faça o mesmo para *nor*, de *not* ... *or* ..., dado por $p\downarrow q \iff \neg(p\vee q)$

(a) $\neg p$

$$\begin{aligned} p\downarrow p &\iff \neg(p\wedge p) && \text{[Definição]}\\ &\iff \neg p && \text{[Idempotência]}\end{aligned}$$

Nota-se a analogia com o primeiro caso.

(b) $p\vee q$

$$\begin{aligned} (p\downarrow q)\downarrow(p\downarrow q) &\iff \neg(p\downarrow q) && \text{[Item a)]}\\ &\iff \neg[\neg(p\vee q)] && \text{[Definição]}\\ &\iff p\vee q && \text{[Negação dupla]}\end{aligned}$$

(c) $p\wedge q$

$$\begin{aligned} (p\downarrow p)\downarrow(q\downarrow q) &\iff (\neg p)\downarrow(\neg q) && \text{[Definição]}\\ &\iff \neg(\neg p\vee\neg q) && \text{[Definição]}\\ &\iff p\wedge q && \text{[De Morgan]}\end{aligned}$$

Nota-se a semelhança (mas não é a mesma coisa!) do caso *nand*.

(d) $p\to q$

$$\begin{aligned} \big[(p\downarrow p)\downarrow q\big]\downarrow\big[(p\downarrow p)\downarrow q\big] &\iff (\neg p\downarrow q)\downarrow(\neg p\downarrow q) && \text{[Item a)]}\\ &\iff \neg p\vee q && \text{[Item b)]}\\ &\iff p\to q && \text{[Implicação]}\end{aligned}$$

(e) $p\leftrightarrow q$

Novamente, notemos que:

$$p\leftrightarrow q\equiv(p\to q)\wedge(q\to p)$$

e, mais uma vez, os itens c) e d):

$$\big((p\to q)\downarrow(p\to q)\big)\downarrow\big((q\to p)\downarrow(q\to p)\big)$$

$$\left(\left\{\left[(p\downarrow p)\downarrow(p\downarrow p)\right]\downarrow(q\downarrow q)\right\}\downarrow\left\{\left[(p\downarrow p)\downarrow(p\downarrow p)\right]\downarrow(q\downarrow q)\right\}\right)\downarrow$$
$$\downarrow\left(\left\{\left[(q\downarrow q)\downarrow(q\downarrow q)\right]\downarrow(p\downarrow p)\right\}\downarrow\left\{\left[(q\downarrow q)\downarrow(q\downarrow q)\right]\downarrow(p\downarrow p)\right\}\right)$$

Problema 5

Determine se cada uma das expressões abaixo são satisfatíveis:

(a) $(p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg s) \wedge (p \vee \neg r \vee \neg s) \wedge (\neg p \vee \neg q \vee \neg s) \wedge (p \vee q \vee \neg s)$

Nota-se o p disponível para a quase todas as cláusulas, à exceção da penúltima. Nesta, basta assumir $q = 0$ e quaisquer valores de s e r. Logo um exemplo que satisfaz é $p = 1$, $q = 0$, $s = 1$ e $r = 1$. A saber:

$$\underbrace{(p \vee q \vee \neg r)}_{p=1 \text{ satisfaz}} \wedge \underbrace{(p \vee \neg q \vee \neg s)}_{p=1 \text{ satisfaz}} \wedge \underbrace{(p \vee \neg r \vee \neg s)}_{p=1 \text{ satisfaz}} \wedge \underbrace{(\neg p \vee \neg q \vee \neg s)}_{q=0 \text{ satisfaz}} \wedge \underbrace{(p \vee q \vee \neg s)}_{p=1 \text{satisfaz}}$$

(b) $(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg s) \wedge (p \vee \neg q \vee \neg s) \wedge (\neg p \vee \neg r \vee \neg s) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg r \vee \neg s)$

O mesmo raciocínio, porém agora há três cláusulas satisfeitas por $p = 1$. Uma delas é satisfeita com $q = 1$, outra com $r = 1$ e outra com $s = 0$. Como exemplo, $p = 1$, $q = 1$, $r = 1$ e $s = 0$. Vejamos:

$$\underbrace{(\neg p \vee \neg q \vee r)}_{r=1 \text{ satisfaz}} \wedge \underbrace{(\neg p \vee q \vee \neg s)}_{q=1 \text{ satisfaz}} \wedge \underbrace{(p \vee \neg q \vee \neg s)}_{p=1 \text{ satisfaz}} \wedge \underbrace{(\neg p \vee \neg r \vee \neg s)}_{s=0 \text{ satisfaz}} \wedge \underbrace{(p \vee q \vee \neg r)}_{p=1 \text{ satisfaz}} \wedge \underbrace{(p \vee \neg r \vee \neg s)}_{p=1 \text{ satisfaz}}$$

(c)

$$(p \vee q \vee r) \wedge (p \vee \neg q \vee \neg s) \wedge (q \vee \neg r \vee s) \wedge (\neg p \vee r \vee s) \wedge (\neg p \vee q \vee \neg s) \wedge$$
$$\wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee \neg q \vee s) \wedge (\neg p \vee \neg r \vee \neg s)$$

Inicia-se com $p = 0$ para satisfazer quatro cláusulas e se nota que a terceira é indiferente ao valor de p. Dessas, duas são satisfeitas com $q = 1$. Das restantes, uma é satisfeita com $s = 0$ e indiferente ao valor de r. A final é, por fim, satisfeita com $r = 0$. A saber:

$$\underbrace{(p \vee q \vee r)}_{q=1 \text{ satisfaz}} \wedge \underbrace{(p \vee \neg q \vee \neg s)}_{s=0 \text{ satisfaz}} \wedge \underbrace{(q \vee \neg r \vee s)}_{q=1 \text{ satisfaz}} \wedge \underbrace{(\neg p \vee r \vee s)}_{p=0 \text{ satisfaz}} \wedge \underbrace{(\neg p \vee q \vee \neg s)}_{p=0 \text{ satisfaz}} \wedge$$
$$\wedge \underbrace{(p \vee \neg q \vee \neg r)}_{r=0 \text{ satisfaz}} \wedge \underbrace{(\neg p \vee \neg q \vee s)}_{p=0 \text{ satisfaz}} \wedge \underbrace{(\neg p \vee \neg r \vee \neg s)}_{p=0 \text{ satisfaz}}$$

Mostrou-se para cada expressão um conjunto de valores que as variáveis booleanas podem assumir para que se mostrem serem expressões satisfatíveis.

Problema 6

Em português e em lógica proposicional, escreva a recíproca, contra-positiva e inversa das condicionais abaixo.

(a) Se nevar hoje, eu irei esquiar amanhã.

Seja P : "Hoje neva"e Q : "Esquiarei amanhã". Então a frase acima é $P \to Q$ e:

- Recíproca: $Q \to P$: "Se eu esquiar amanhã, hoje nevará".
- Contra-positiva: $\neg Q \to \neg P$: "Se eu não esquiar amanhã, então hoje não nevou".
- Inversa: $\neg P \to \neg Q$: "Se não nevar hoje, não irei esquiar amanhã".

(b) Eu vou à aula sempre que terá uma prova.

Seja P : "Haverá uma prova"e Q : "Eu vou à aula". Então a frase acima é $P \to Q$ e:

- Recíproca: $Q \to P$: "Se eu for à aula, haverá uma prova". Ou ainda "Sempre que eu for à aula, haverá uma prova"(o ponto aqui é sutil na língua portuguesa, mas inverte a ordem de causalidade: indica-se que a ocorrência de prova é deflagrada pela minha ida à aula e não o contrário, como na direta).
- Contra-positiva: $\neg Q \to \neg P$: "Se eu não fui à aula, então é porque não haverá uma prova". Novamente, aqui o ponto foi reforçado de que a ocorrência de provas sempre deflagra minha ida às aulas.
- Inversa: $\neg P \to \neg Q$: "Se não houver uma prova, não irei à aula". Já aqui o ponto (contando que não valha a direta) é que, se houver provas, talvez eu vá à aula. Mas caso contrário, certamente não irei.

(c) Um inteiro positivo é primo somente se ele não possui divisores além de 1 e si próprio.

Seja P : "n é primo"e Q : "n não possui divisores além de 1 e si próprio". Então a frase acima é $P \to Q$ e:

- Recíproca: $Q \to P$: "n é primo se ele não possui divisores além de 1 e si próprio".
- Contra-positiva: $\neg Q \to \neg P$: "Se n possui divisores além de 1 e si próprio, então n não é primo".
- Inversa: $\neg P \to \neg Q$: "Se n não é primo, então possui divisores além de 1 e si próprio".

Problema 7

Sejam A, B, C três conjuntos e suponha que $A \subseteq C$. Prove que:

$$A \cup (B \cap C) = (A \cup B) \cap C.$$

Forneça um exemplo que mostre que a condição $A \subseteq C$ não pode ser ignorada.

Solução:

($\Rightarrow$) Seja $x \in A \cup (B \cap C)$. Então $x \in A$ ou $x \in B \cap C$. Se $x \in A$, naturalmente $x \in A \cup B$ e então como $A \subseteq C$, $x \in C$. Daí procede que $x \in A \cup B$ e $x \in C$, ou seja, $x \in (A \cup B) \cap C$.

($\Leftarrow$) Seja $x \in (A \cup B) \cap C$. Então $x \in (A \cup B)$ e $x \in C$. Se $x \in A$, naturalmente $x \in A \cup (B \cap C)$ e não há mais o que mostrar. Vejamos o caso que $x \notin A$. Se $x \notin A$, deve ocorrer que $x \in B$, do contrário não poderia ocorrer que $x \in A \cup B$, o que foi dado por hipótese. Como $x \in B$ e $x \in C$, $x \in B \cap C$. Desse último fato, procede naturalmente que $x \in A \cup (B \cap C)$.

Como foi mostrado que $A \cup (B \cap C) \subseteq (A \cup B) \cap C$ e $(A \cup B) \cap C \subseteq A \cup (B \cap C)$, conclui-se que $A \cup (B \cap C) = (A \cup B) \cap C$.

Nota: foi usado abundamentemente o fato de que $A \subseteq A \cup B$ para quaisquer A, B. Expressando de forma lógica o pertencimento de um x arbitrário, procede que:

$$x \in A \to (x \in A) \vee (x \in B) \iff \underbrace{\neg(x \in A) \vee (x \in A)}_{\text{tautologia}} \vee (x \in B) \iff 1 \vee B \equiv 1$$

é, como mostrado, uma tautologia.

Nota 2: é pedido um comentário sobre a importância de $A \subseteq C$ na identidade acima. Vejamos primeiro como foi usada no passo da proposição direta. Suponhamos o caso em que exista $x \in A$ tal que $x \notin C$ (se não for o caso, A é vazio e a identidade continua válida pois $A \subseteq C$). Como $x \notin C$, $x \notin B \cap C$ e o lado direito da expressão se reduz (por distributiva da união e notando a intersecção vazia entre A e C) a $B \cap C$. Isso é absurdo, pois já vimos que $x \in A$ mas não poderia ocorrer que $x \in C$. Logo o que não se verificaria é o lado direito da expressão, que deixaria de valer. Portanto, a condição $A \subseteq C$ é necessária para a validade da igualdade.

Problema 8

Sejam $B \subseteq A$ conjuntos tais que $|A| = n$ e $|B| = k$. Quantos subconjuntos de A possuem intersecção unitária (um único elemento) com B?

$$|\{C \subseteq A : |C \cap B| = 1\}| = ?$$

Solução: da condição de subconjunto, procede que $|B| \leq |A|$, ou seja, $k \leq n$. Um subconjunto de A tal que $|C \cap B| = 1$ pode ser construído tomando um elemento de B e os demais elementos a partir dos $n - k$ elementos que estão em A, mas não em B.

Há $2^{n-k} = \sum_{i=0}^{n-k} \binom{n-k}{i}$ formas de construir esses conjuntos com valores remanescentes, desde nenhum (ou seja, contendo apenas o elemento escolhido de B) até todos os $n - k$. Independentemente e para cada uma dessas escolhas, podemos escolher agora um dentre os k elementos de B.

Por regra do produto em Princípio Fundamental da Contagem (doravante, PFC) há, portanto, $k2^{n-k}$ formas de escolher esses subconjuntos.

Problema 9

Quantas tabelas verdade distintas de proposições compostas existem envolvendo as variáveis proposicionais p e q? Justifique!

Solução: cada linha da tabela verdade é gerada a partir de um valor 1 ou 0 de cada uma das varáveis proposicionais. Sendo assim há $2^2 = 4$ linhas para o caso de duas variáveis.

Para o presente caso, tomemos os vetores característicos (ou seja, assume-se *ordem*) $\mathbf{x}_i = (a_{i1}, a_{i2}, a_{i3}, a_{i4})$ correspondentes à i-ésima tabela verdade passível de ser construída. Não é necessário especificar para a presente solução, mas se pode pensar que a_{i1} corresponde à linha $p = 1$, $q = 1$; a_{i2} a $p = 1$, $q = 0$; a_{i3} a $p = 0$, $q = 1$; por fim, a_{i4} a $p = 0$, $q = 0$.

Agora procederemos por PFC: para a_{i1} se tem duas escolhas (1 ou 0) que independem das escolhas do próximo, a_{i2}, que também tem duas escolhas e assim sucessivamente. Sendo assim, por regra do produto (aplicada $3 = n - 1$ vezes), o total de escolhas possíveis distintas para $\mathbf{x_i}$ é $2^4 = 16$.

Problema 10

De quantas maneiras podemos distribuir k bolas em n caixas de forma que cada caixa tenha no máximo uma bola?

Solução: vejamos primeiramente que é necessário que $n \geq k$. Se não fosse o caso, após inserir as primeiras n bolas, não haveria mais caixas distintas para colocar e seríamos obrigados a repetir a caixa.

Vejamos então que ao alocar as k bolas em n caixas, estamos na realidade escolhendo uma combinação de k caixas dentre n possíveis, o que é possível de $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ formas distintas.

Problema 11

Seja $k \geq 2n$. De quantas formas podemos distribuir k moedas idênticas a n pessoas se cada uma deve receber ao menos 2 moedas?

Solução: de início, podemos pensar da seguinte maneira: podemos dar as 2 moedas que devemos minimamente a cada pessoa e então decidir o que fazer com as $k-2n$ restantes.

Outra forma de pensar é a seguinte: dar uma moeda para as n pessoas (só há uma forma de fazer isso, já que as moedas são idênticas) e então distribuir $k-n$ moedas de modo que cada pessoa receba no mínimo uma (nova).

Este último problema foi mencionado em aula como um dos problemas modificados em [Lovász et al., 2003]. Sua solução é então que há $\binom{r-1}{n-1}$ com $r = k-n$, ou seja, $\binom{k-n-1}{n-1}$ formas de distribuir para o presente problema.

Problema 12

Forneça provas combinatórias para as relações:

Nota: em razão de buscar literatura para me preparar para os exercícios, deparei-me com a solução de um dos exercícios (que indicarei, os que não indiquei significa que fiz por conta, sem consulta).

(a) Para $0 \leq k \leq n$, $\binom{n}{2} = \binom{k}{2} + k(n-k) + \binom{n-k}{2}$

O lado esquerdo da relação corresponde a todas as formas escolher, num conjunto com n elementos, apenas dois deles. Vejamos que isso pode ser pensado da seguinte forma: escolhe-se um subconjunto de k elementos de n.

Podemos pegar dois elementos dele, um elemento dele e outro que esteja fora e, por fim, dois que não estejam nele. Essas escolhas são todas independentes e "em paralelo", logo pelo PFC na forma de regra de soma, podemos somar.

- $\binom{k}{2}$: representa as possibilidades distintas de escolher 2 dentre k elementos.
- $k(n-k)$: representa as possibilidades distintas de escolher um elemento dentre k e, feita essa escolha e independente da ordem, escolher outro nos $n-k$ faltantes.
- $\binom{n-k}{2}$: representa as possibilidades de escolher 2 dentre $n-k$ elementos.

em que se chega, então, ao lado direito da equação.

(b) $\binom{n}{2} + \binom{n+1}{2} = n^2$

O lado direito da expressão representa, por exemplo, escolher *em ordem* dois elementos, sem repetição, com a restrição de que um deles, digamos, o k-ésimo, seja proibido na primeira escolha. Sabe-se de antemão qual o elemento proibido.

Isso pode ser expresso de outra forma: deseja-se dois elementos dos $n+1$, entretanto não se importaria com a ordem desde que sejam aqueles dois previamente indicados (não se sabe qual o elemento proibido antes de escolher). Há duas possibilidades: ou um dos elementos era o proibido no início ou, de forma completamente independente, nenhum dos dois era o elemento proibido.

Caso um deles seja o proibido, só há uma ordem que contemple os dois desejados e então houve, equivalentemente, $\binom{n}{2}$ escolhas viáveis. Caso contrário, quaisquer das escolhas de 2 em $n+1$, ou seja, $\binom{n+1}{2}$ era viável.

(c) $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$

Suponhamos o seguinte problema (baseei-me na solução do item *e)* mas não consultei o material): desejo formar um comitê de exatamente k alunos e escolher um deles para ser representante.

Uma das formas de formar é escolher k dentre n alunos e, entre esses, um deles para ser representante. Temos então por PFC, regra do produto $\binom{n}{k}\binom{k}{1} = k\binom{n}{k}$.

Outra forma de fazer é, dentre todos os n alunos, escolher o representante e então proceder à escolha dos $k-1$ dentre $n-1$ aqueles que irão compor o comitê. Analogamente ao caso anterior, $\binom{n}{1}\binom{n-1}{k-1} = n\binom{n-1}{k-1}$.

Logo temos a igualdade:

$$k\binom{n}{k} = n\binom{n-1}{k-1} \Rightarrow \binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}.$$

(d) Para $0 \leq l \leq k \leq n$, $\binom{n}{k}\binom{k}{l} = \binom{n}{l}\binom{n-l}{k-l}$

O lado esquerdo corresponde a: tomar k elementos dentre n e, feita a escolha desse conjunto, escolher l dentro de k. No fim, são feitas duas escolhas: l elementos dentro de um conjunt k.

Isso pode ser feito também da seguinte forma: escolher diretamente os l elementos desejados e, depois, o conjunto faltante para completar k. Vejamos que se l já foram escolhidos, o total a escolher é $n - l$, assim como o faltante para completar k é $k - l$.

Logo, por PFC na lei de produtos, obtém-se a igualdade proposta (notando que são sequenciais e dependentes uma da outra, na ordem que foram enunciadas aqui).

(e) $\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$

Solução de [Benjamin and Quinn, 2003]: escolher dentre n estudantes comitês de k estudantes de modo que um deles seja um representante.

A solução do lado esquerdo é, dado um comite de k alunos foram escolhidos $\binom{n}{k}$, no qual há k possibilidades de escolha do representante. Como essas escolhas para diferentes k são independentes, obtemos a soma (PFC, regra da soma).

A solução do lado direito corresponde a escolher o representante dentre os n estudantes e, depois, formar os comitês possíveis com até k estudantes. Isso é dado por $\sum_{k=0}^{n-1}\binom{n-1}{k} = 2^{n-1}$. Como essas escolhas são sequênciais (a escolha do estudante determina as escolhas seguintes dos comitês), então por PFC, regra do produto, tem-se $n2^{n-1}$

(f) $\sum_{k=0}^{m}\binom{p}{k}\binom{q}{m-k} = \binom{p+q}{m}$

Suponhamos o seguinte problema: escolher m dentre $p + q$ objetos.

O lado direito dessa equação é justamente o total de possibilidades em que isso pode ser feito diretamente do montante de $p + q$ elementos.

O lado esquerto representa o seguinte: podemos tomar k elementos em p e $m - k$ elementos em q a fim de conseguir a totalidade dos m elementos. Vejamos que podemos fazer isso com $k = 0$, $k = 1$, $\ldots$, $k = m$ elementos. Dado k, por PFC/produto temos a escolha $\binom{p}{k}\binom{q}{m-k}$

Cada uma dessas escolhas é independente e ocorrem “em paralelo", pois não podemos ao mesmo tempo tomar duas quantidades distintas de elementos de cada conjunto.

Logo, por PFC/soma:

$$\binom{p}{0}\binom{q}{m} + \binom{p}{1}\binom{q}{m-1} + \cdots + \binom{p}{m}\binom{q}{0} = \sum_{k=0}^{p}\binom{p}{k}\binom{q}{m-k}$$

Problema 13

Sejam $m, n \geq 1$ inteiros. Quantas funções $f : [m] \to [n]$

(a) Existem?

Cada elemento do domínio deve levar a um único elemento do contradomínio. Uma das formas de pensar é que podemos, para cada $x \in [m]$ escolher $y \in [n]$ tal que $y = f(x)$. Podemos pensar que definir a função f_i é como a alocação de valores de $[n]$ no vetor característico $\mathbf{y}_i = (y_{i1}, y_{i2}, \ldots, y_{im})$, ou seja, $y_{ij} = f_i(x_j)$.

Essa notação ainda reforça o fato de que cada valor do domínio *deve* levar a um único valor da imagem. De fato, Im$f_i = \{y_{ij} : y_{ij} \in \mathbf{y}_i\}$.

Como para cada índice desse vetor alocado um valor possível dentre n de forma independente em m posições, pelo PFC/regra do produto, podemos então propor que há n^m possibilidades.

(b) São injetoras?

Para que as funções sejam injetoras, é necessário que dois valores distintos do domínio mapeiem a valores distintos do contradomínio. Isso significa que, usando a mesma construção do vetor acima, após a escolha do i-ésimo componente, seja reduzida uma das possibilidades de valores admissíveis de $[n]$ que se pode tomar para o índice seguinte. Logo há n escolhas possíveis para o primeiro índice do vetor, $n - 1$ para o segundo e assim sucessivamente.

Há, portanto,

$$\underbrace{n(n-1)\ldots(n-(m-1))}_{m \text{ valores}} = \frac{n!}{(n-m)!}$$

possibilidades. Vejamos que se $n < m$, será necessário repetir valores do domínio e então não há possibilidade de construir funções injetoras.

(c) São bijetoras?

Agora vejamos que para que haja bijeção entre domínio e contradomínio (no caso de função bijetora é necessária também a sobrejeção), é necessário primeiro a injeção, ou seja, $n \geq m$ (ver item anterior). Como é bijetora, existe para cada f_i uma $f_i^{-1} : [n] \to [m]$ que é sua inversa, também é bijetora e, em particular, é injetora. Logo deve ocorrer também que $m \geq n$ e, por fim, que $m = n$.

Sendo assim, para cada elemento do vetor $\mathbf{y_i}$ temos escolhas distintas, como no caso anterior, e elas esgotam as possibilidades de valores do contradomínio. Logo o total de funções é:

$$n!\delta_{nm} = m!\delta_{nm} = \begin{cases} n! = m!, & \text{se } n = m \\ 0, & \text{se } n \neq m \end{cases}$$

(d) São sobrejetoras?

Para que seja sobrejetora, todos os n elementos do contradomínio devem receber algum valor do mapeamento. Se $n > m$ isso se tornaria impossível, pois no cenário em que cada valor do domínio fosse associado a um valor distinto na imagem, faltaria elementos na imagem. Logo todas as possibilidades ocorrem com $n \leq m$.

Uma forma de pensar é a seguinte: podemos pegar cada valor do contradomínio e associar a um valor do domínio. Como a cada escolha não podemos repetir o valor do domínio usado (do contrário não seria uma função), temos as primeiras $n!$ escolhas. Para cada uma dessas escolhas, tendo restado $m - n$ elementos do domínio para decidir como alocar, as escolhas de valores em $[n]$ são quaisquer, não há mais restrição. Logo o total de escolhas é $n^{m-n}n!$, notando que as $m-n$ remanescentes foram tratadas como no caso do item a).

Agora com $m = n$ e para um único $i \in [n]$, quantas:

(e) satisfazem $f(i) = i$?

Fixou-se a ocorrência de um elemento do domínio e de um elemento do contradomínio. O restante dos valores é uma redução dos casos anteriores, em particular $(n-1)^{n-1}$ para funções quaisquer, $(n-1)!$ para funções injetoras, bijetoras e sobrejetoras.

Problema 14

Determine todos os inteiros positivos a, b, c para os quais

$$\binom{a}{b}\binom{b}{c} = 2\binom{a}{c}$$

Solução: usando a definição algébrica dos coeficientes binomiais,

$$\binom{a}{b}\binom{b}{c} = \frac{a!}{\cancel{b!}(a-b)!}\frac{\cancel{b!}}{c!(b-c)!} = \frac{a!}{c!(b-c)!},$$

$$\binom{a}{c} = \frac{a!}{c!(c-a)!},$$

teremos a igualdade quando:

$$\frac{\cancel{a!}}{\cancel{c!}(b-c)!} = 2\frac{\cancel{a!}}{\cancel{c!}(a-c)!} \Leftrightarrow (a-c)! = 2(b-c)!.$$

Agora vejamos os casos de interesse em que $c \leq b \leq a$, ou seja, $0 \leq b-c \leq a-c$. Fatoriais são, pela definição recursiva, tais que um fatorial pode ser expresso por outro de inteiro menor multiplicado por uma sequência de inteiros até chegar a esse valor (que é o maior).

Na expressão dada, as única possibilidade são as que:

$$(a-c)! = 2! = 2, \quad (b-c)! = 1! = 1,$$

ou seja,

$$b = c+1, \quad a = c+2 = b+1 \quad \text{para } c \in \mathbb{Z}, c > 0.$$

Problema 15

Temos um conjunto $V = [n]$ de compostos químicos, $n \geq 1$ inteiro, que precisam ser acondicionados em caixas. Certos pares (não ordenados) de compostos, descritos por $E \subseteq \binom{V}{2}$, não podem compartilhar uma mesma caixa sob o risco de reagirem e causarem explosões. Obviamente, queremos utilizar o menor número $m \leq n$ de caixas possível. Formule o problema como uma questão de satistatifibilidade de expressões proposicionais (isto é, apresente uma redução ao SAT), descrevendo em detalhes cada cláusula adotada. Mostre que cada solução à satisfatibilidade corresponde a uma solução de empacotamento e vice-versa.

Solução: tem-se pelo enunciado uma quantidade $p = \binom{|E|}{2}$ pares que não podem ser formados, ou ainda, de pares que não podem constar juntos numa mesma caixa.

Seja dada uma quantidade m de caixas com capacidade de armazenamento q, ou seja, um total de mq frascos poderiam, em tese, ser alocada nessas caixas (sem levar em conta as p impossibilidades) e que deve ser maior que n, do contrário simplesmente não haveria caixas suficientes para conter todos os frascos. Logo a primeira restrição é que $P_1 : mq \geq n$.

Pensemos agora em cada composto dentro da caixa. Seja:

$$\phi(x, y) = \begin{cases} 1, & \text{se } x \text{ ou } y \text{ (ou ambos) não são frascos ou } \{x, y\} \notin E \\ 0, & \text{se } \{x, y\} \in E \end{cases}$$

logo é necessário que em cada caixa não estejam pares proibidos, o que pode ser verificado fazendo, "para cada caixa, entre quaiquer dois elementos da caixa, não pode ocorrer que $\phi = 0$". Em linguagem lógica:

$$P_2 : \bigwedge_{i=1}^{m} \bigwedge_{\substack{j,k \\ j \neq k}} \phi(j, k) = \bigwedge_{i=1}^{m} \bigwedge_{j} \bigwedge_{k>j} \phi(j, k)$$

é uma proposição que precisa ser satisfeita. Como não há qualquer ordem nas alocações, uma estratégia possível para não incorrer em ter de verificar pares de frascos/espaços que não estejam nem na mesma caixa é a convenção de indices tal que $r(i, j) = (i - 1)q + j$ com $i = 1, \ldots, m$, $j = 1, \ldots, q$ é o j-ésimo frasco/espaço da i-ésima caixa. Logo a proposição pode ser reduzida a:

$$P_2 : \bigwedge_{i=1}^{m} \bigwedge_{j}^{q} \bigwedge_{k=j+1}^{q} \phi(r(i, j), r(i, k)).$$

A restrição remanescente agora é apenas garantir que todos os compostos precisam ser inseridos nas caixas e assim eliminar soluções ineficientes em que espaços vazios são alocados indiscrimidamente. Também recai em garantir que um composto não seja erroneamente alocado múltiplas vezes (consideremos frascos de compostos repetidos, se houver, como valores distinto sem $[n]$ e que formam repetidos pares em E, casso seja

necessário). Seja:

$$\psi(x, y, z) = \begin{cases} 1, & \text{se } z \in [n] \text{ é } y\text{-ésimo elemento da caixa } x \\ 0, & \text{caso contrário} \end{cases}$$

Garantir que todos os compostos ocorram ao menos e no máximo uma vez é dado por uma expressão mais complicada. Primeiro, tomemos a convenção de que todos os números de $n+1$ a mq, se houver, são espaços vazios (distintos, para fins de índice) que precisam necessariamente ser alocados devido à natural incompatibilidade das dimensões. Então famços:

$$P3 : \bigvee_{i=1}^{m} \bigvee_{j=1}^{q} (\psi(i,j,1) \oplus \psi(i,j,2) \cdots \oplus \psi(i,j,n) \cdots \oplus \psi(i,j,mq)) = \bigvee_{i=1}^{m} \bigvee_{j=1}^{q} \bigoplus_{k=1}^{mq} \psi(i,j,k),$$

em que $\oplus$ é chamada disjunção exclusiva ou, ainda, *xor*. Seu uso é feito para que cada cláusula se torne satisfatível com apenas um valor de k por vez globalmente.

Por fim, o problema final se escreve na forma SAT como:

$$P_{SAT} = P_1 \wedge P_2 \wedge P_3.$$

Correspondência SAT-empacotamento: Agora suponhamos que um empacotamento tenha sido feito. Isso significa que os valores de $[n]$ foram alocados aos mq espaços, possivelmente com repetições de 0 correspondendo aos espaços vazios deixados. Se os frascos couberam nas caixas, os mq espaços vazios iniciais foram suficientes e se verifica P_1

Se o empacotamento é viável, nenhum frasco dos pares $\{x, y\} \in E$ foram alocados na mesma caixa, logo dada uma caixa i, temos certeza de que $\bigwedge_j^q \bigwedge_{k=j+1}^q \phi(r(i,j), r(i,k))$ e variando nos índices i, obtemos a validade de P_2.

Vamos por fim argumentar que P_3 se comporta como esperamos. Cada grande *xor* garante que constará em cada espaço (j-ésimo espaço na i-ésima caixa) ou um dos $mq - n$ espaços vazios necessários para compatibilizar o problema ou um, e apenas um, dos compostos químicos.

Para fins de SAT, essa formulação será o suficiente e se presume retornar 1 quando corresponder a um empacotamento possível dados n, E, m, q. Entretanto, para fins de computar as soluções disponíveis, deve-se considerar os $mq - n$ espaços vazios como idênticos, ou seja, dividir o total de soluções encontradas por $(mq - n)!$.

Referências

[Benjamin and Quinn, 2003] Benjamin, A. T. and Quinn, J. J. (2003). *Proofs that Really Count: The Art of Combinatorial Proof*, volume 27. Mathematical Association of America, 1 edition.

[Lehman et al., 2018] Lehman, E., Leighton, F. T., and Meyer, A. R. (2018). *Mathematics for Computer Science*.

[Lovász et al., 2003] Lovász, L., Pelikán, J., and Vesztergombi, K. (2003). *Discrete Mathematics: Elementary and Beyond*. Undergraduate Texts in Mathematics. Springer New York.

[Widmer et al., 2017] Widmer, N., Tocci, R., and Moss, G. (2017). *Digital Systems: Principles and Applications*. Pearson.