Cálculo, prova e invariantes

João F. Ferreira*

Braga, 29 de Março de 2008

* Financiado pela Fundação para a Ciência e a Tecnologia

Introdução

Nesta sessão falaremos de:

- provas calculacionais
- construção vs. verificação
- invariantes

Noção de Prova

Objectivo: mostrar porque é que um teorema é verdadeiro, utilizando factos ou outros teoremas previamente provados.

Propriedades de uma boa prova

- relação clara entre os factos
- desenvolvimento explícito
- concisa (condição necessária para elegância)

Provas Informais

Teorema:

Para todos os conjuntos A, B e C:

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

Prova "convencional":

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C) \quad \text{e}$$

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

Prova:

Primeiro provamos que $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. Se $x \in A \cup (B \cap C)$, então $x \in A$ ou $x \in B \cap C$. Se $x \in A$, então $x \in A \cup B$ e $x \in A \cup C$; logo $x \in (A \cap B) \cap (A \cup C)$. Por outro lado, se $x \in B \cap C$, então $x \in B$ e $x \in C$; assim $x \in A \cup B$ e $x \in A \cup C$, por isso $x \in (A \cup B) \cap (A \cup C)$. Portanto, $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Conversamente, se $x \in (A \cup B) \cap (A \cup C)$, então $x \in A \cup B$ e $x \in A \cup C$. Consideramos dois casos: $x \in A$ e $x \notin A$. Se $x \in A$, então $x \in A \cup (B \cap C)$, e está provado. Se $x \notin A$, então, como $x \in A \cup B$, então $x \in B$. Da mesma forma, como $x \in A \cup C$ e $x \notin A$, então $x \in C$. Assim, $x \in B \cap C$; logo, $x \in A \cup (B \cap C)$. Portanto, $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

Provas Informais

A prova anterior poderia:

- ser mais calculacional, evitando interpretações desnecessárias;

- ser mais concisa, evitando a dupla inclusão e a análise de casos.

Formato de Prova

Se quisermos provar $A \leqslant D$ e se temos

$$A = B \quad , \quad B = C \quad e \quad C \leqslant D \quad ,$$

então registamos esta sucessão de igualdades como

$$\begin{array}{ll} & A \\ = & \{ \text{ razão pela qual } A = B \} \\ & B \\ = & \{ \text{ razão pela qual } B = C \} \\ & C \\ \leqslant & \{ \text{ razão pela qual } C = D \} \\ & D \end{array} .$$

Vantagens deste formato

- passos intermédios são omitidos
- cada passo está bem justificado
- podemos usar outras relações entre as expressões
- é fácil ver a relação entre cada duas expressões

Provas Calculacionais

Objectivo é provar:

$$x \in A \cup (B \cap C) \equiv x \in (A \cup B) \cap (A \cup C)$$

$$= \quad \{ \text{justif.} \}$$

verdadeiro.

$$
\begin{aligned}
& x \in A \cup (B \cap C) \\
= & \quad \{ \text{definição de } \cup \} \\
& x \in A \ \vee \ x \in (B \cap C) \\
= & \quad \{ \text{definição de } \cap \} \\
& x \in A \ \vee \ (x \in B \wedge x \in C) \\
= & \quad \{ \vee \text{ distribui pela } \wedge \} \\
& (x \in A \ \vee \ x \in B) \wedge (x \in A \ \vee \ x \in C) \\
= & \quad \{ \text{definição de } \cup \} \\
& x \in (A \cup B) \wedge x \in (A \cup C) \\
= & \quad \{ \text{definição de } \cap \} \\
& x \in (A \cup B) \cap (A \cup C) \ .
\end{aligned}
$$

Provas Formais

0. Se $a>0$ e $b>c>0$, então $a+b > a+c > 0$
1. se $a>b>0$, então $\sqrt{a} > \sqrt{b} > 0$
2. $224 > 9 > 0$
3. $\sqrt{224} > \sqrt{9} > 0$ (1 e 2)
4. $4\sqrt{14} > 3 > 0$ (3 e aritmética)
5. $57 + 4\sqrt{14} > 57 + 3 > 0$ (0 e 4)
6. $\sqrt{57 + 4\sqrt{14}} > \sqrt{57 + 3} > 0$ (1 e 5)
7. $1 + 2\sqrt{14} > 2\sqrt{15} > 0$ (6 e aritmética)
8. $8 + 1 + 2\sqrt{14} > 8 + 2\sqrt{15} > 0$ (0 e 7)
9. $\sqrt{8 + 1 + 2\sqrt{14}} > \sqrt{8 + 2\sqrt{15}} > 0$ (1 e 8)
10. $\sqrt{2} + \sqrt{7} > \sqrt{3} + \sqrt{5} > 0$ (9 e aritmética)

Construção vs. Verificação

Será $\sqrt{2} + \sqrt{7}$ superior ou inferior a $\sqrt{3} + \sqrt{5}$?

Construção vs. Verificação

Será $\sqrt{2} + \sqrt{7}$ superior ou inferior a $\sqrt{3} + \sqrt{5}$?

Incógnita: relação entre as expressões

$$(\sqrt{2} + \sqrt{7}) \quad R \quad (\sqrt{3} + \sqrt{5})$$

(Nota: R é uma relação de ordem)

Construção vs. Verificação

Será $\sqrt{2} + \sqrt{7}$ superior ou inferior a $\sqrt{3} + \sqrt{5}$?

Incógnita: relação entre as expressões

$a < b \equiv a^2 < b^2$

$$(\sqrt{2} + \sqrt{7}) \quad R \quad (\sqrt{3} + \sqrt{5})$$

(Nota: R é uma relação de ordem)

Para a e b positivos:

$$a^2 \; R \; b^2 \quad \equiv \quad a \; R \; b \; .$$

$$(\sqrt{2}+\sqrt{7}) \;\; R \;\; (\sqrt{3}+\sqrt{5})$$

$= \{ \text{cancelamento} \}$

$$(\sqrt{2}+\sqrt{7})^2 \;\; R \;\; (\sqrt{3}+\sqrt{5})^2$$

$= \{ \text{aritmética} \}$

$$(9 + 2\sqrt{14}) \;\; R \;\; (8 + 2\sqrt{15})$$

$= \{ \text{cancelamento} \}$ $+$

$$(1 + 2\sqrt{14}) \;\; R \;\; 2\sqrt{15}$$

$= \{ \text{cancelamento} \}^2$

$$(57 + 4\sqrt{14}) \;\; R \;\; 60$$

$= \{ \text{cancelamento} \}$ $+$

$$4\sqrt{14} \;\; R \;\; 3$$

$= \{ \text{cancelamento} \}$

$$224 \;\; R \;\; 9 \qquad .$$

$$(\sqrt{2}+\sqrt{7}) \quad R \quad (\sqrt{3}+\sqrt{5})$$

$=$ { cancelamento }

$$(\sqrt{2}+\sqrt{7})^2 \quad R \quad (\sqrt{3}+\sqrt{5})^2$$

$=$ { aritmética }

$$(9+2\sqrt{14}) \quad R \quad (8+2\sqrt{15})$$

$=$ { cancelamento }

$$(1+2\sqrt{14}) \quad R \quad 2\sqrt{15}$$

$=$ { cancelamento }

$$(57+4\sqrt{14}) \quad R \quad 60$$

$=$ { cancelamento }

$$4\sqrt{14} \quad R \quad 3$$

$=$ { cancelamento }

$$2274 \quad R \quad 9 \quad .$$

Conclusão:

R é >, i.e:

$$(\sqrt{2}+\sqrt{7}) > (\sqrt{3}+\sqrt{5}) \quad .$$

Invariantes

Um invariante é uma propriedade que se mantém constante.

Desde cedo que reconhecemos invariantes:

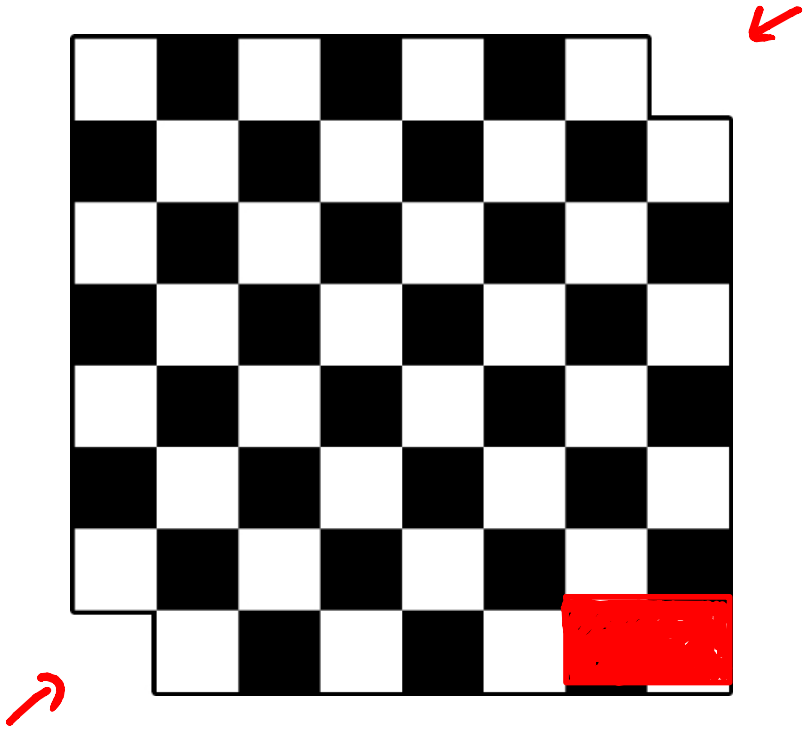
águas casas oficiais sinais

gata leitora vencedora

Mas:

~~mais~~ males ~~actora~~ actriz

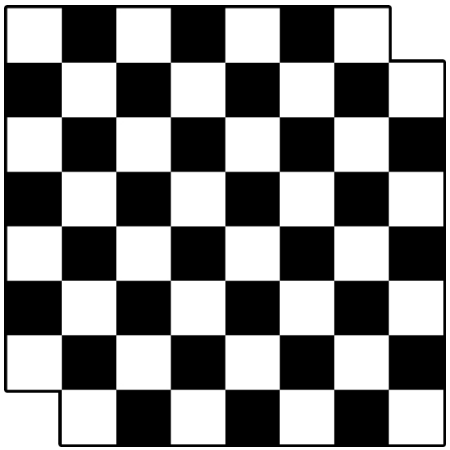
Tabuleiro de Xadrez Mutilado



Será possível cobrir este tabuleiro com dominós sem que estes se sobreponham nem saiam do tabuleiro ?

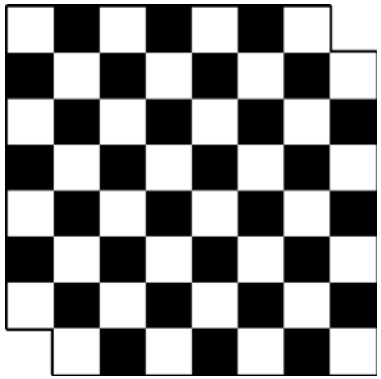
Tabuleiro de Xadrez Mutilado

Invariante: ao colocar um dominó cobrimos uma casa preta e uma casa branca



Tabuleiro de Xadrez Mutilado

Invariante: ao colocar um dominó cobrimos uma casa preta e uma casa branca



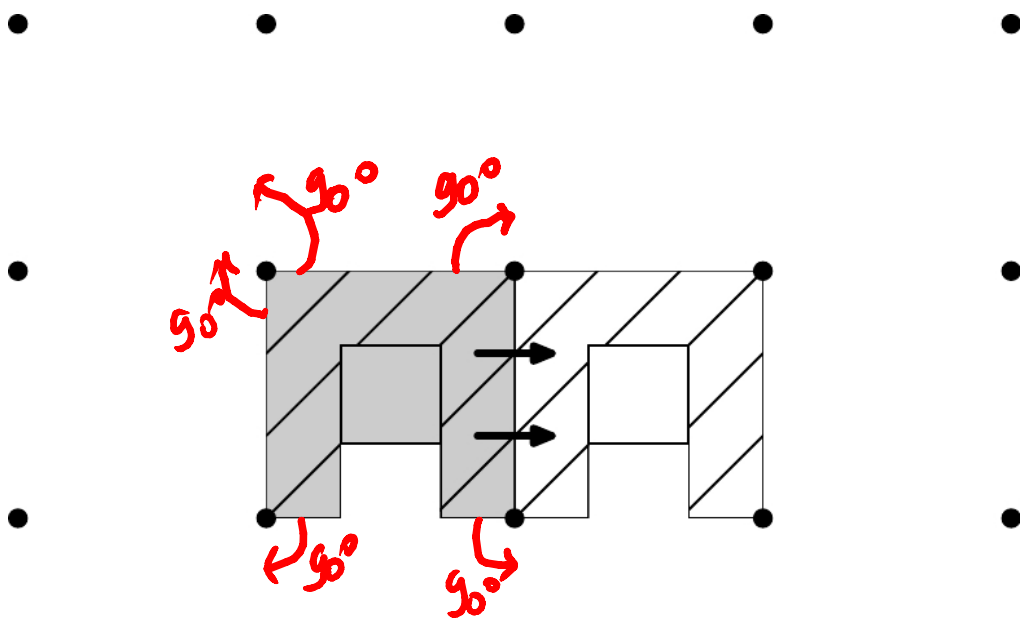
Não é possível!

O número de casas brancas e pretas ocupadas será sempre igual.

Mas, como removemos duas casas pretas, existem mais casas brancas que pretas.

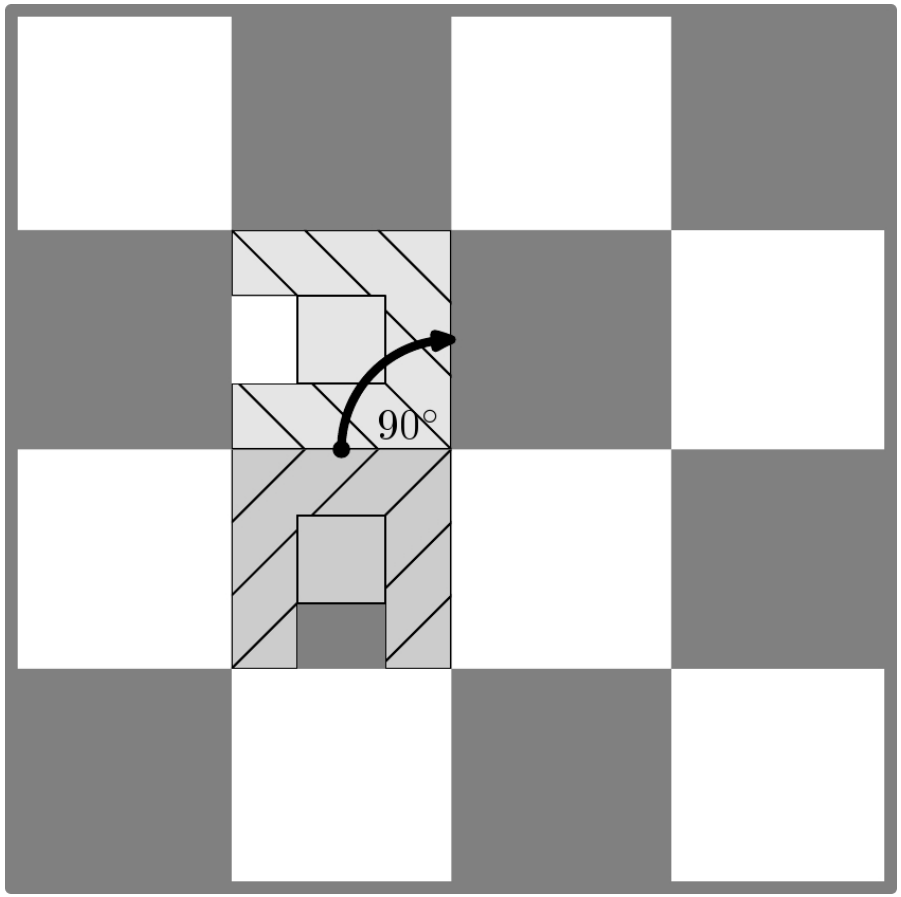
A Cadeira Pesada

Dada uma cadeira quadrada, o objectivo é movê-la para a direita uma distância igual ao seu próprio comprimento.



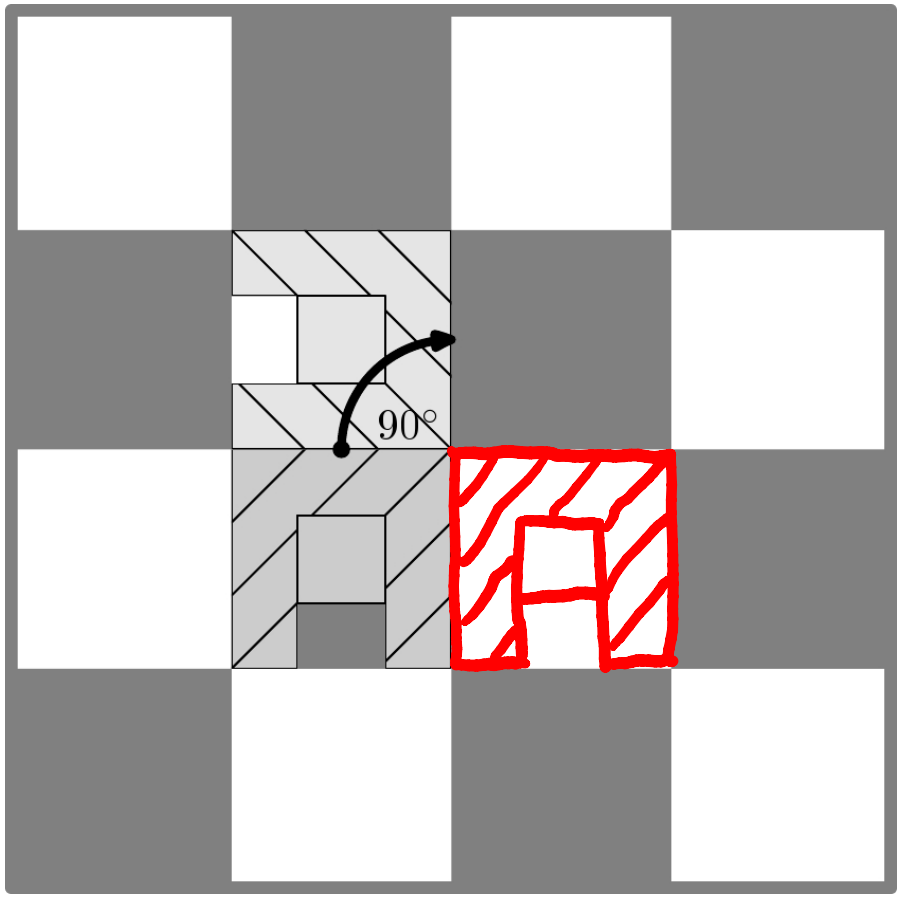
A Cadeira Pesada

Mas a cadeira é muito pesada e, como tal, só pode ser movida rodando-a 90° sobre um dos seus cantos.



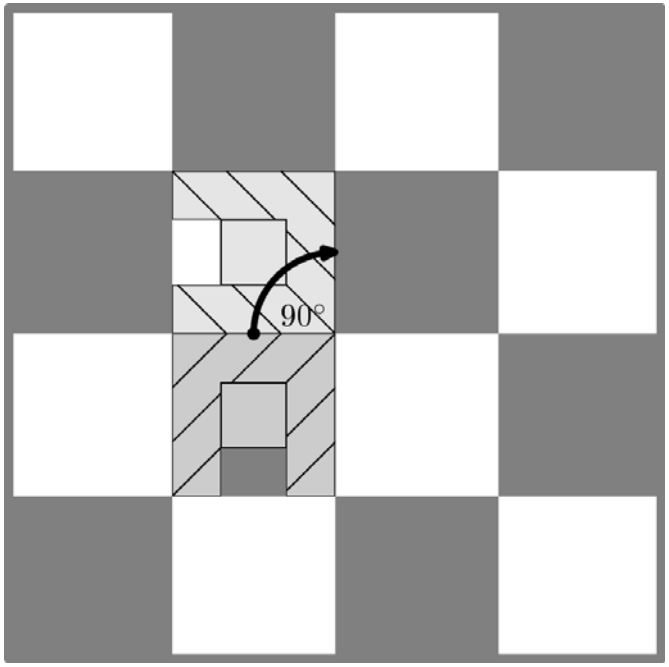
A Cadeira Pesada

Mas a cadeira é muito pesada e, como tal, só pode ser movida rodando-a 90° sobre um dos seus cantos.



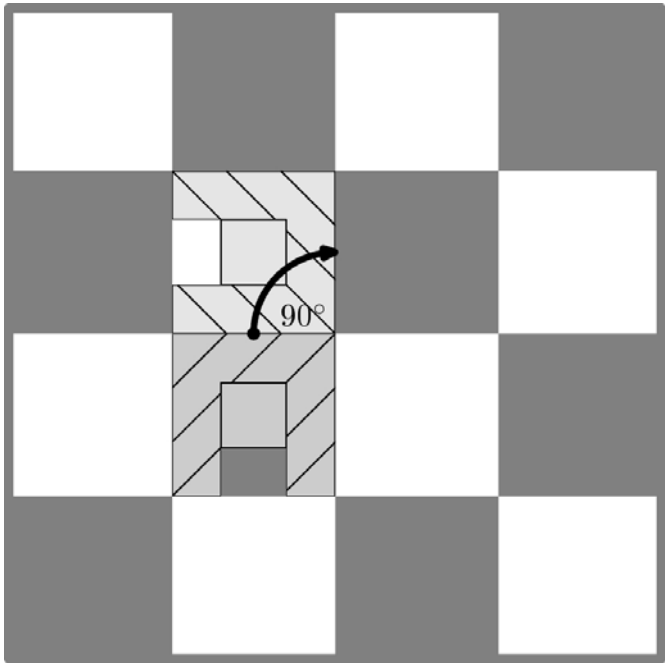
Será possível?

A Cadeira Pesada



- Pintamos o chão como um tabuleiro de xadrez
- Assumimos que a cadeira está numa casa preta
- Assumimos que a orientação inicial é Norte/Sul

A Cadeira Pesada



Não é possível!

- Pintamos o chão como um tabuleiro de xadrez
- Assumimos que a cadeira está numa casa preta
- Assumimos que a orientação inicial é Norte/Sul

Invariante: cadeira em casa preta

≡

orientação é Norte/Sul