Sistemas Lineares Diofantinos

Marcelo Hashimoto

mh@ime.usp.br

MAC5700 Seminários em Ciência da Computação

Instituto de Matemática e Estatística

Universidade de São Paulo

Sistemas lineares

Problema: encontrar $x_1, x_2, \ldots, x_n$ satisfazendo

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & \beta_1; \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & \beta_2; \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & \beta_m. \end{array}$$

Em forma matricial: encontrar x satisfazendo

$$Ax = b.$$

Sistemas lineares

Exemplo:

$$\begin{array}{rcrcrcrcl} 2x_1 & + & 3x_2 & + & 2x_3 & + & 6x_4 & = & 21 \\ 1x_1 & + & 2x_2 & + & 1x_3 & + & 4x_4 & = & 12 \\ 3x_1 & + & 5x_2 & + & 4x_3 & + & 10x_4 & = & 37 \end{array}$$

Em forma matricial:

$$\begin{bmatrix} 2 & 3 & 2 & 6 \\ 1 & 2 & 1 & 4 \\ 3 & 5 & 4 & 10 \end{bmatrix} x = \begin{bmatrix} 21 \\ 12 \\ 37 \end{bmatrix}$$

Problema

Problema de decisão: dada uma matriz A e um vetor b, existe solução para o sistema linear $Ax = b$?

Problema

Problema de decisão: dada uma matriz A e um vetor b, existe solução para o sistema linear $Ax = b$?

Usando eliminação gaussiana, pode-se demonstrar que:

Se sim, existe x tal que $Ax = b$.
Se não, existe y tal que $yA = 0$ e $yb \neq 0$.

Problema

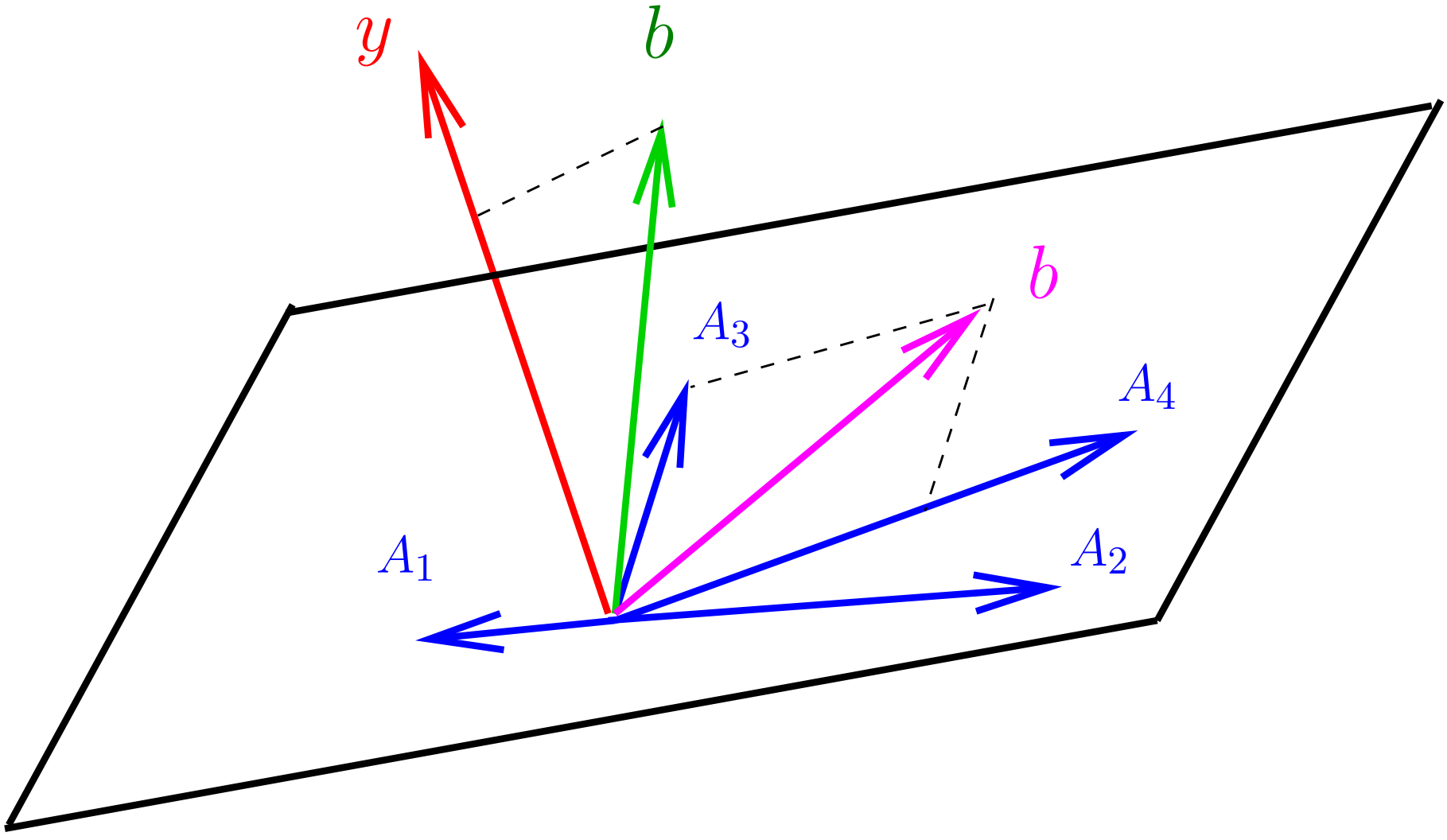
Problema de decisão: dada uma matriz A e um vetor b, existe solução para o sistema linear $Ax = b$?

Usando eliminação gaussiana, pode-se demonstrar que:

Se sim, existe x tal que $Ax = b$.
Se não, existe y tal que $yA = 0$ e $yb \neq 0$.

Para ambas as respostas existe um certificado.

Geometricamente



Certificado

Exemplo 1:

$$\begin{bmatrix} 2 & 3 & 2 & 6 \\ 1 & 2 & 1 & 4 \\ 3 & 5 & 4 & 10 \end{bmatrix} x = \begin{bmatrix} 21 \\ 12 \\ 37 \end{bmatrix}$$

Certificado

Exemplo 1:

$$\begin{bmatrix} 2 & 3 & 2 & 6 \\ 1 & 2 & 1 & 4 \\ 3 & 5 & 4 & 10 \end{bmatrix} x = \begin{bmatrix} 21 \\ 12 \\ 37 \end{bmatrix}$$

Certificado de sim:

$$\begin{bmatrix} 2 & 3 & 2 & 6 \\ 1 & 2 & 1 & 4 \\ 3 & 5 & 4 & 10 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \\ 4 \\ 3/2 \end{bmatrix} = \begin{bmatrix} 21 \\ 12 \\ 37 \end{bmatrix}$$

Certificado

Exemplo 2:

$$\begin{bmatrix} 2 & 1 & 1 & 2 \\ 6 & 5 & 4 & 7 \\ 2 & 3 & 2 & 3 \end{bmatrix} x = \begin{bmatrix} 2 \\ 1 \\ -2 \end{bmatrix}$$

Certificado

Exemplo 2:

$$\begin{bmatrix} 2 & 1 & 1 & 2 \\ 6 & 5 & 4 & 7 \\ 2 & 3 & 2 & 3 \end{bmatrix} x = \begin{bmatrix} 2 \\ 1 \\ -2 \end{bmatrix}$$

Certificado de não:

$$\begin{bmatrix} 2 & -1 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 & 1 & 2 \\ 6 & 5 & 4 & 7 \\ 2 & 3 & 2 & 3 \end{bmatrix} = 0 \qquad \begin{bmatrix} 2 & -1 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ -2 \end{bmatrix} = 1$$

Resumindo

Dados:

matriz A e vetor b.

Encontrar:

solução para $Ax = b$
ou certificado de inexistência.

Resumindo

Dados:

matriz A e vetor b.

Encontrar:

solução para $Ax = b$
ou certificado de inexistência.

Este problema pode ser resolvido em tempo polinomial.
(ex: eliminação gaussiana)

Resumindo

Dados:

matriz A e vetor b.

Encontrar:

solução para $Ax = b$
ou certificado de inexistência.

Este problema pode ser resolvido em tempo polinomial.
(ex: eliminação gaussiana)

O que acontece se exigirmos que a solução seja inteira?

Sistemas lineares diofantinos

Dados:

matriz A e vetor b.

Encontrar:

solução inteira para $Ax = b$
ou certificado de inexistência.

Sistemas lineares diofantinos

Dados:

matriz A e vetor b.

Encontrar:

solução inteira para $Ax = b$
ou certificado de inexistência.

Muitas vezes existe solução, mas não solução inteira.

Sistemas lineares diofantinos

Dados:

matriz A e vetor b.

Encontrar:

solução inteira para $Ax = b$
ou certificado de inexistência.

Muitas vezes existe solução, mas não solução inteira.

Um algoritmo que é capaz de encontrar uma solução pode não ser capaz de encontrar uma solução inteira, mesmo que ela exista. (ex: eliminação gaussiana)

Sistemas lineares diofantinos

Exemplo 1:

$$\begin{bmatrix} 2 & 3 & 2 & 6 \\ 1 & 2 & 1 & 4 \\ 3 & 5 & 4 & 10 \end{bmatrix} x = \begin{bmatrix} 21 \\ 12 \\ 37 \end{bmatrix}$$

Sistemas lineares diofantinos

Exemplo 1:

$$\begin{bmatrix} 2 & 3 & 2 & 6 \\ 1 & 2 & 1 & 4 \\ 3 & 5 & 4 & 10 \end{bmatrix} x = \begin{bmatrix} 21 \\ 12 \\ 37 \end{bmatrix}$$

Solução obtida com eliminação gaussiana:

$$\begin{bmatrix} 2 & 3 & 2 & 6 \\ 1 & 2 & 1 & 4 \\ 3 & 5 & 4 & 10 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \\ 4 \\ 3/2 \end{bmatrix} = \begin{bmatrix} 21 \\ 12 \\ 37 \end{bmatrix}$$

Sistemas lineares diofantinos

Exemplo 1:

$$\begin{bmatrix} 2 & 3 & 2 & 6 \\ 1 & 2 & 1 & 4 \\ 3 & 5 & 4 & 10 \end{bmatrix} x = \begin{bmatrix} 21 \\ 12 \\ 37 \end{bmatrix}$$

Existe solução inteira:

$$\begin{bmatrix} 2 & 3 & 2 & 6 \\ 1 & 2 & 1 & 4 \\ 3 & 5 & 4 & 10 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ 4 \\ 1 \end{bmatrix} = \begin{bmatrix} 21 \\ 12 \\ 37 \end{bmatrix}$$

Sistemas lineares diofantinos

Exemplo 2:

$$\begin{bmatrix} 4 & 4 & 3 & 18 \\ 3 & 4 & 3 & 18 \\ 2 & 2 & 3 & 12 \end{bmatrix} x = \begin{bmatrix} 12 \\ 11 \\ 7 \end{bmatrix}$$

Sistemas lineares diofantinos

Exemplo 2:

$$\begin{bmatrix} 4 & 4 & 3 & 18 \\ 3 & 4 & 3 & 18 \\ 2 & 2 & 3 & 12 \end{bmatrix} x = \begin{bmatrix} 12 \\ 11 \\ 7 \end{bmatrix}$$

Solução obtida com eliminação gaussiana:

$$\begin{bmatrix} 4 & 4 & 3 & 18 \\ 3 & 4 & 3 & 18 \\ 2 & 2 & 3 & 12 \end{bmatrix} \begin{bmatrix} 1 \\ 3/2 \\ 2/3 \\ 0 \end{bmatrix} = \begin{bmatrix} 12 \\ 11 \\ 7 \end{bmatrix}$$

Sistemas lineares diofantinos

Exemplo 2:

$$\begin{bmatrix} 4 & 4 & 3 & 18 \\ 3 & 4 & 3 & 18 \\ 2 & 2 & 3 & 12 \end{bmatrix} x = \begin{bmatrix} 12 \\ 11 \\ 7 \end{bmatrix}$$

Não existe solução inteira:

Como ter certeza disso?

Pergunta

Dado um sistema linear $Ax = b$ que não admite solução inteira, existe algum certificado de inexistência?

Caso particular

Vamos considerar uma única equação:

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta.$$

Fato 1

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta$$

admite solução inteira se e somente se

$$(\gamma_1\alpha_1)x_1 + (\gamma_2\alpha_2)x_2 + \cdots + (\gamma_n\alpha_n)x_n = \gamma\beta,$$

onde $\gamma_1, \gamma_2, \ldots, \gamma_n, \gamma \in \{+1, -1\}$,
também admite solução inteira.

Fato 1

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta$$

admite solução inteira se e somente se

$$(\gamma_1\alpha_1)x_1 + (\gamma_2\alpha_2)x_2 + \cdots + (\gamma_n\alpha_n)x_n = \gamma\beta,$$

onde $\gamma_1, \gamma_2, \ldots, \gamma_n, \gamma \in \{+1, -1\}$,
também admite solução inteira.

Conclusão 1: podemos supor valores não-negativos.

Fato 2

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta$$

admite solução inteira se e somente se

$$(\delta\alpha_1) x_1 + (\delta\alpha_2) x_2 + \cdots + (\delta\alpha_n) x_n = \delta\beta$$

também admite solução inteira.

Fato 2

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta$$

admite solução inteira se e somente se

$$(\delta\alpha_1) x_1 + (\delta\alpha_2) x_2 + \cdots + (\delta\alpha_n) x_n = \delta\beta$$

também admite solução inteira.

Conclusão 2: podemos supor valores inteiros.

Candidato a certificado de inexistência

Se d divide $\alpha_1, \alpha_2 \ldots, \alpha_n$ mas não divide β, então

$$\frac{\alpha_1}{d}x_1 + \frac{\alpha_2}{d}x_2 + \cdots + \frac{\alpha_n}{d}x_n = \frac{\beta}{d}$$

não admite solução inteira. Mas isso implica que

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta$$

também não admite solução inteira.

Candidato a certificado de inexistência

Se d divide $\alpha_1, \alpha_2 \ldots, \alpha_n$ mas não divide β, então

$$\frac{\alpha_1}{d}x_1 + \frac{\alpha_2}{d}x_2 + \cdots + \frac{\alpha_n}{d}x_n = \frac{\beta}{d}$$

não admite solução inteira. Mas isso implica que

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta$$

também não admite solução inteira.

Exemplo: $24x_1 + 4x_2 + 38x_3 + 16x_4 = 143$

Candidato a certificado de inexistência

Se d divide $\alpha_1, \alpha_2 \ldots, \alpha_n$ mas não divide β, então

$$\frac{\alpha_1}{d}x_1 + \frac{\alpha_2}{d}x_2 + \cdots + \frac{\alpha_n}{d}x_n = \frac{\beta}{d}$$

não admite solução inteira. Mas isso implica que

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta$$

também não admite solução inteira.

Poderíamos obter esse certificado em qualquer caso?

Caso particular do caso particular

Vamos considerar uma única variável:

$$\alpha_1 x_1 = \beta.$$

Caso particular do caso particular

Vamos considerar uma única variável:

$$\alpha_1 x_1 = \beta.$$

Caso 1: β/α_1 é inteiro.
Nesse caso, $x_1 := \beta/\alpha_1$ é uma solução inteira.

Caso 2: β/α_1 não é inteiro.
Nesse caso, $d := \alpha_1$ divide α_1 mas não divide β.

Caso particular do caso particular

Vamos considerar uma única variável:

$$\alpha_1 x_1 = \beta.$$

Caso 1: β/α_1 é inteiro.
Nesse caso, $x_1 := \beta/\alpha_1$ é uma solução inteira.

Caso 2: β/α_1 não é inteiro.
Nesse caso, $d := \alpha_1$ divide α_1 mas não divide β.

Em tempo polinomial, podemos encontrar uma solução inteira ou um certificado de inexistência nesse caso.

Voltando ao caso menos particular

Decidir se existem inteiros $x_1, x_2, \ldots, x_n$ satisfazendo

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta.$$

Voltando ao caso menos particular

Decidir se existem inteiros $x_1, x_2, \ldots, x_n$ satisfazendo

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta.$$

Idéia: tentar reduzir o problema ao caso fácil

$$\alpha_1 x_1 = \beta.$$

Voltando ao caso menos particular

Decidir se existem inteiros $x_1, x_2, \ldots, x_n$ satisfazendo

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta.$$

Idéia: tentar reduzir o problema ao caso fácil

$$\alpha_1 x_1 = \beta.$$

Supondo $\alpha_1 \leq \alpha_2, \ldots, \alpha_n$, considere a "versão reduzida"

$$\alpha_1 x'_1 + (\alpha_2 - \alpha_1) x'_2 + \cdots + (\alpha_n - \alpha_1) x'_n = \beta.$$

Equivalência da versão reduzida

Se temos inteiros $x'_1, x'_2, \ldots, x'_n$ satisfazendo

$$\alpha_1 x'_1 + (\alpha_2 - \alpha_1)x'_2 + \cdots + (\alpha_n - \alpha_1)x'_n = \beta,$$

podemos reformular a igualdade acima como

$$\alpha_1(x'_1 - x'_2 - \cdots - x'_n) + \alpha_2 x'_2 + \cdots + \alpha_n x'_n = \beta$$

e encontramos inteiros $x_1, x_2, \ldots, x_n$ satisfazendo

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = \beta.$$

Equivalência da versão reduzida

Se d não divide β e divide

$$\alpha_1, (\alpha_2 - \alpha_1), \ldots, (\alpha_n - \alpha_1),$$

então d não divide β e divide

$$\alpha_1, \alpha_2, \ldots, \alpha_n.$$

Equivalência da versão reduzida

Se d não divide β e divide

$$\alpha_1, (\alpha_2 - \alpha_1), \ldots, (\alpha_n - \alpha_1),$$

então d não divide β e divide

$$\alpha_1, \alpha_2, \ldots, \alpha_n.$$

Conclusão: resolver a versão reduzida é o suficiente.

Resumindo

“Enquanto há mais do que um coeficiente positivo, subtraia o menor dos coeficientes positivos de todos os outros.”

Resumindo

RESOLVE (α, β) $\quad \triangleright$ α, β inteiros não-negativos

1 $I \leftarrow \{i : \alpha_i \neq 0\}$

2 **enquanto** $|I| > 1$ **faça**

3 escolha i em I tal que α_i é mínimo

4 **para cada** j em I **faça**

5 $\alpha_j \leftarrow \alpha_j - \alpha_i$

6 **se** $\alpha_j = 0$

7 **então** $I \leftarrow I \setminus \{j\}$

8 seja i o único elemento de I

9 **se** α_i divide β

10 **então devolva** SIM

11 **senão devolva** NÃO

Redução mais eficiente

Idéia: subtrair o máximo possível de uma só vez.

$$\alpha_1 x'_1 + \left(\alpha_2 - \left\lfloor \frac{\alpha_2}{\alpha_1} \right\rfloor \alpha_1\right) x'_2 + \cdots + \left(\alpha_n - \left\lfloor \frac{\alpha_n}{\alpha_1} \right\rfloor \alpha_1\right) x'_n = \beta.$$

Redução mais eficiente

Idéia: subtrair o máximo possível de uma só vez.

$$\alpha_1 x'_1 + \left(\alpha_2 - \left\lfloor \frac{\alpha_2}{\alpha_1} \right\rfloor \alpha_1\right) x'_2 + \cdots + \left(\alpha_n - \left\lfloor \frac{\alpha_n}{\alpha_1} \right\rfloor \alpha_1\right) x'_n = \beta.$$

Podemos observar que:

$$\alpha_i - \left\lfloor \frac{\alpha_i}{\alpha_1} \right\rfloor \alpha_1 \leq \frac{\alpha_i}{2}.$$

Redução mais eficiente

Idéia: subtrair o máximo possível de uma só vez.

$$\alpha_1 x'_1 + \left(\alpha_2 - \left\lfloor \frac{\alpha_2}{\alpha_1} \right\rfloor \alpha_1\right) x'_2 + \cdots + \left(\alpha_n - \left\lfloor \frac{\alpha_n}{\alpha_1} \right\rfloor \alpha_1\right) x'_n = \beta.$$

Podemos observar que:

$$\alpha_i - \left\lfloor \frac{\alpha_i}{\alpha_1} \right\rfloor \alpha_1 \leq \frac{\alpha_i}{2}.$$

Conclusão: o algoritmo consome tempo polinomial.
(e nada mais é do que o algoritmo de Euclides)

Resumindo de novo

EUCLIDES (α, β) ▷ α, β inteiros não-negativos

1 $I \leftarrow \{i : \alpha_i \neq 0\}$

2 **enquanto** $|I| > 1$ **faça**

3 escolha i em I tal que α_i é mínimo

4 **para cada** j em I **faça**

5 $\alpha_j \leftarrow \alpha_j - \lfloor \alpha_j / \alpha_i \rfloor \alpha_i$ ▷ só mudou aqui

6 **se** $\alpha_j = 0$

7 **então** $I \leftarrow I \setminus \{j\}$

8 seja i o único elemento de I

9 **se** α_i divide β

10 **então devolva** SIM

11 **senão devolva** NÃO

Saindo do caso particular

Encontrar x inteiro satisfazendo

$$Ax = b.$$

Candidato a certificado de inexistência

Se existe algum y tal que

yA é inteiro e yb não é inteiro,

então não existe x inteiro tal que

$$Ax = b.$$

Candidato a certificado de inexistência

Se existe algum y tal que

yA é inteiro e yb não é inteiro,

então não existe x inteiro tal que

$$Ax = b.$$

Poderíamos obter esse certificado em qualquer caso?

Caso particular

Vamos supor que existe B não-singular tal que

$$A = [B\ 0].$$

Caso particular

Vamos supor que existe B não-singular tal que

$$A = [B\ 0].$$

Caso 1: $B^{-1}b$ é um vetor inteiro.
Nesse caso, temos uma solução inteira para $Ax = b$:

$$[B\ 0] \begin{bmatrix} B^{-1}b \\ 0 \end{bmatrix} = b$$

Caso particular

Vamos supor que existe B não-singular tal que

$$A = [B\ 0].$$

Caso 2: $B^{-1}b$ não é um vetor inteiro.
Nesse caso, existe y tal que yA é inteiro e yb não é inteiro:

$$B^{-1}A = B^{-1}[B\ 0] = [I\ 0]$$

Caso particular

Vamos supor que existe B não-singular tal que

$$A = [B\ 0].$$

Em tempo polinomial, podemos obter uma solução inteira para $Ax = b$ ou um certificado de inexistência nesse caso.

Redução ao caso fácil

Idéia: transformar A em $[B\ 0]$, com B não-singular.

Redução ao caso fácil

Idéia: transformar A em $[B\ 0]$, com B não-singular.

Podemos supor que A e b são ambos inteiros.

Podemos supor que A tem posto linha completo.
(é fácil eliminar as linhas linearmente dependentes)

Redução ao caso fácil

Idéia: transformar A em $[B\ 0]$, com B não-singular.

Podemos supor que A e b são ambos inteiros.

Podemos supor que A tem posto linha completo.
(é fácil eliminar as linhas linearmente dependentes)

Sendo $a_1, a_2, \ldots, a_n$ as colunas de A e sendo $x_1, x_2, \ldots, x_n$ os elementos de x, dizer que $Ax = b$ equivale a dizer que

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = b.$$

Redução ao caso fácil

Idéia: transformar A em $[B\ 0]$, com B não-singular, usando

(i) permutação de duas colunas;

(ii) multiplicação de uma coluna por -1;

(iii) soma do múltiplo inteiro de uma coluna a outra.

Todas as três operações preservam a existência (ou inexistência) de solução inteira para o sistema $Ax = b$.

Redução ao caso fácil

Idéia: transformar A em $[B\ 0]$, com B não-singular, usando

(i) permutação de duas colunas;

(ii) multiplicação de uma coluna por -1;

(iii) soma do múltiplo inteiro de uma coluna a outra.

Todas as três operações preservam a existência (ou inexistência) de solução inteira para o sistema $Ax = b$.

Conseguindo isso, o problema de decisão está resolvido.

Detalhe

Como podemos obter um certificado para a versão original a partir de um certificado para a versão reduzida?

A forma normal de Hermite

5	0	0	0	0	0	0	0
4	7	0	0	0	0	0	0
6	2	9	0	0	0	0	0
4	7	1	8	0	0	0	0
2	3	5	3	6	0	0	0

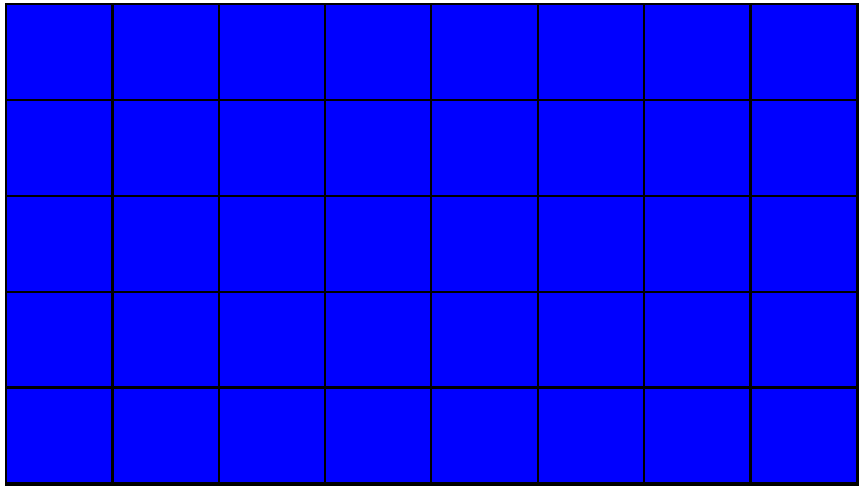
A está na forma normal de Hermite se $A = [B\ 0]$ e:

1. B é triangular inferior;
2. B é não-singular e não-negativa;
3. o maior elemento de uma linha de B está na diagonal.

Obtendo a forma normal de Hermite

Idéia: transformar A em uma matriz $[B\ 0]$ que satisfaz

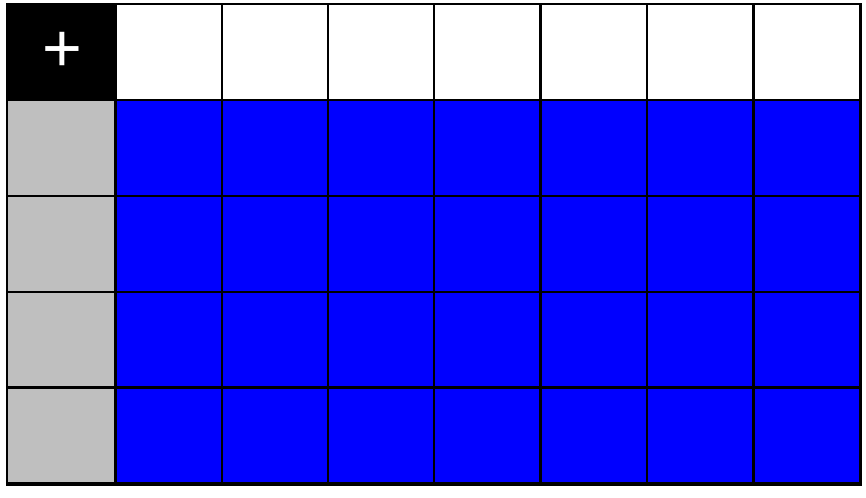
1. B é triangular inferior;
2. os elementos da diagonal de B são positivos.



Obtendo a forma normal de Hermite

Idéia: transformar A em uma matriz $[B\ 0]$ que satisfaz

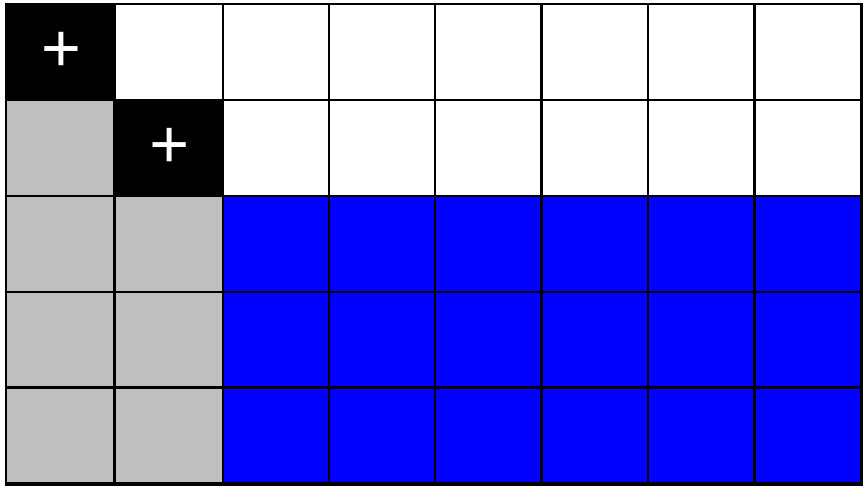
1. B é triangular inferior;
2. os elementos da diagonal de B são positivos.



Obtendo a forma normal de Hermite

Idéia: transformar A em uma matriz $[B\ 0]$ que satisfaz

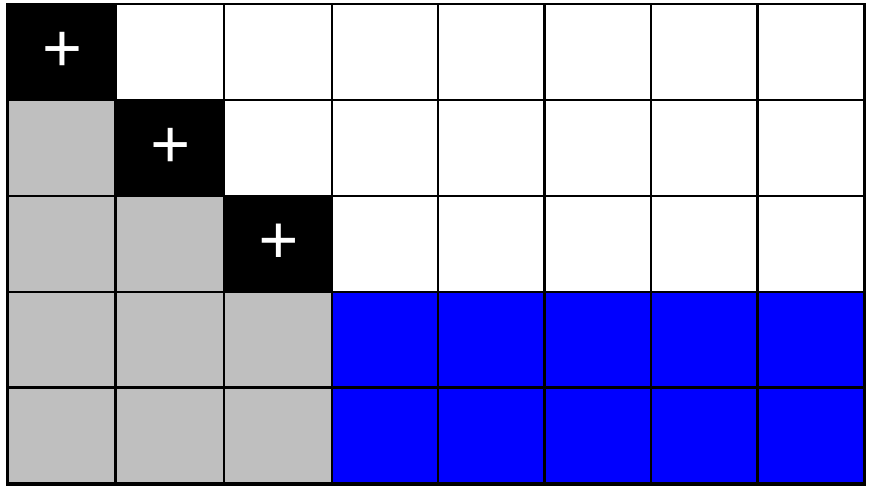
1. B é triangular inferior;
2. os elementos da diagonal de B são positivos.



Obtendo a forma normal de Hermite

Idéia: transformar A em uma matriz $[B\ 0]$ que satisfaz

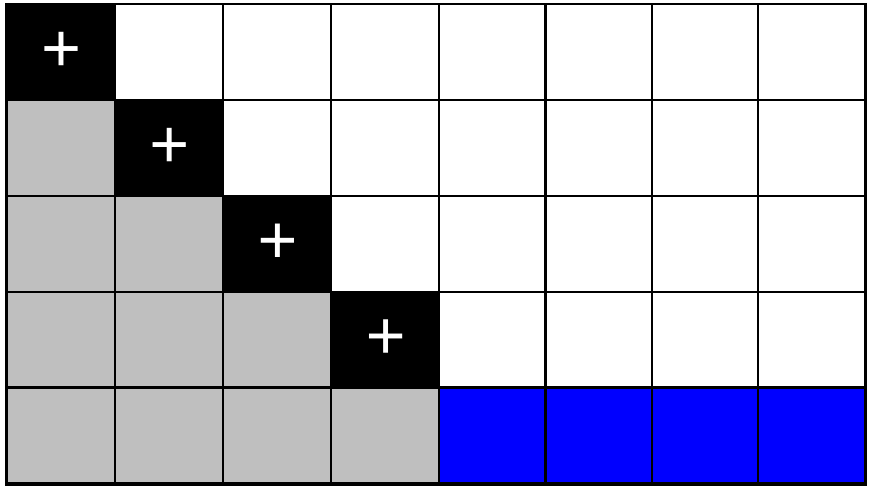
1. B é triangular inferior;
2. os elementos da diagonal de B são positivos.



Obtendo a forma normal de Hermite

Idéia: transformar A em uma matriz $[B\ 0]$ que satisfaz

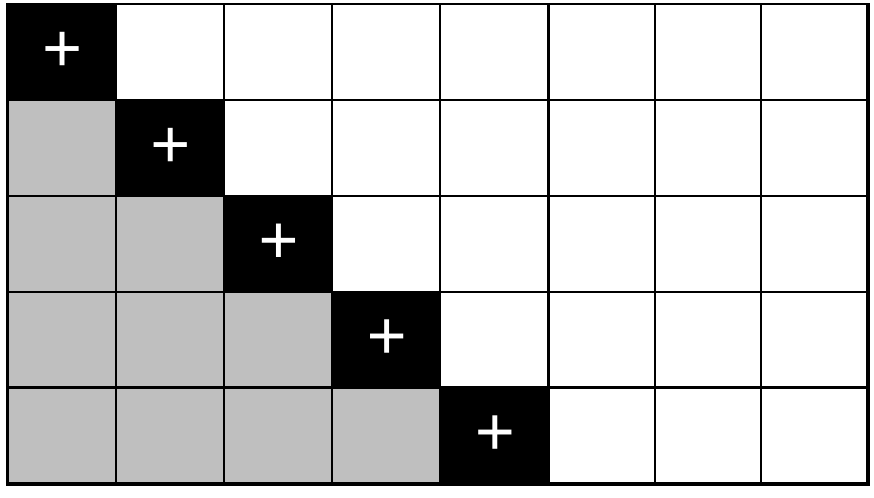
1. B é triangular inferior;
2. os elementos da diagonal de B são positivos.



Obtendo a forma normal de Hermite

Idéia: transformar A em uma matriz $[B\ 0]$ que satisfaz

1. B é triangular inferior;
2. os elementos da diagonal de B são positivos.



Obtendo a forma normal de Hermite

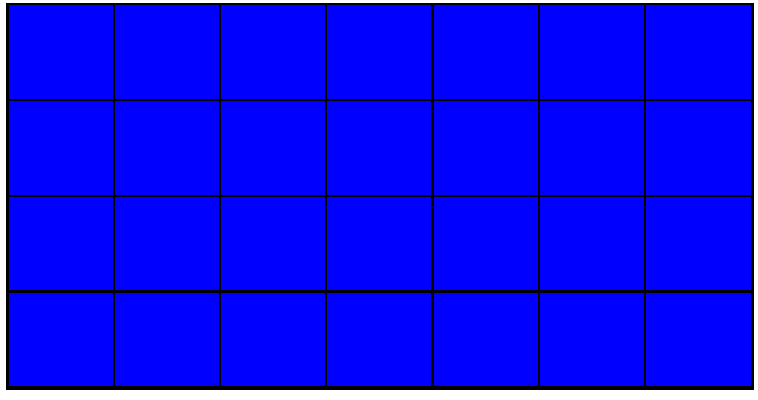
Idéia: transformar A em uma matriz $[B\ 0]$ que satisfaz

1. B é triangular inferior;
2. os elementos da diagonal de B são positivos.

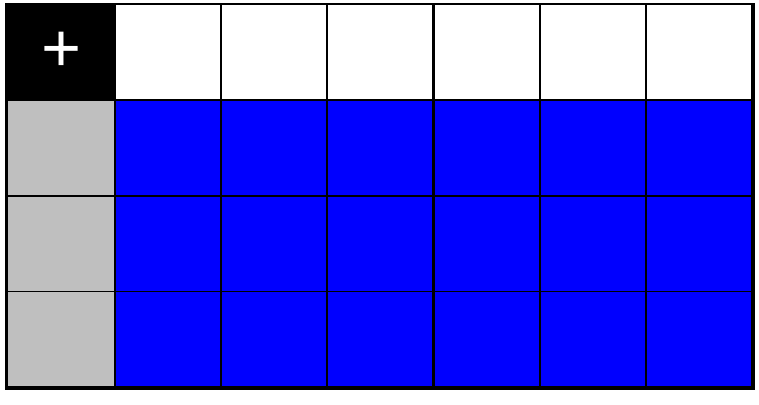
Trazer essa matriz para a forma normal de Hermite é trivial.
(usamos os elementos da diagonal para reduzir os outros)

Iteração

Queremos transformar uma matriz D



Em uma matriz na forma



Iteração

Vamos denotar as colunas da matriz D por

$$d_1, d_2, \ldots, d_l.$$

Com operações sobre as colunas, podemos garantir

$$D_{11}, D_{12}, \ldots, D_{1l} \geq 0 \quad \text{e} \quad D_{11} \leq D_{12}, \ldots, D_{1n},$$

e transformar D em uma matriz cujas colunas são

$$d_1, (d_2 - d_1), \ldots, (d_l - d_1).$$

Déjà Vu

“Enquanto há mais do que um elemento positivo na primeira linha, subtraia a coluna com o menor dos elementos positivos na primeira linha das outras.”

Déjà Vu

"Enquanto há mais do que um elemento positivo na primeira linha, subtraia a coluna com o menor dos elementos positivos na primeira linha das outras."

Mais eficiente: transformar D em uma matriz com colunas

$$d_1, \left(d_2 - \left\lfloor \frac{D_{12}}{D_{11}} \right\rfloor d_1 \right), \ldots, \left(d_l - \left\lfloor \frac{D_{1l}}{D_{11}} \right\rfloor d_1 \right).$$

Déjà Vu

"Enquanto há mais do que um elemento positivo na primeira linha, subtraia a coluna com o menor dos elementos positivos na primeira linha das outras."

Mais eficiente: transformar D em uma matriz com colunas

$$d_1, \left(d_2 - \left\lfloor \frac{D_{12}}{D_{11}} \right\rfloor d_1 \right), \ldots, \left(d_l - \left\lfloor \frac{D_{1l}}{D_{11}} \right\rfloor d_1 \right).$$

Moral da história: de novo o algoritmo de Euclides.

Resumindo

EUCLIDES (D) $\quad \triangleright$ D inteira

1 **para cada** i com $D_{1i} < 0$ **faça**
2 $\quad d_i \leftarrow -d_i$
3 $I \leftarrow \{i : D_{1i} \neq 0\}$
4 **enquanto** $|I| > 1$ **faça**
5 $\quad$ escolha i em I tal que D_{1i} é mínimo
6 $\quad$ **para cada** j em I **faça**
7 $\quad\quad d_j \leftarrow d_j - \lfloor D_{1j}/D_{1i} \rfloor d_i$
8 $\quad\quad$ **se** $D_{1j} = 0$
9 $\quad\quad\quad$ **então** $I \leftarrow I \setminus \{j\}$
10 seja i o único elemento de I
11 **se** $i \neq 1$
12 $\quad$ **então** permute d_i e d_1

Propriedade fundamental

Se $[B\ 0]$ é a matriz na forma normal de Hermite obtida a partir de A, então existe uma matriz U tal que

$$AU = [B\ 0]$$

e U é uma matriz unimodular.

Matrizes unimodulares

Uma matriz inteira U é unimodular se

$$|\det(U)| = 1.$$

Matrizes unimodulares

Uma matriz inteira U é unimodular se

$$|\det(U)| = 1.$$

Relembrando: a inversa de U é dada por

$$U^{-1}_{ij} = \frac{(-1)^{i+j}\det(\overline{U}_{ji})}{\det(U)}.$$

Matrizes Unimodulares

Uma matriz inteira U é unimodular se

$$|\det(U)| = 1.$$

Relembrando: a inversa de U é dada por

$$U^{-1}_{ij} = \frac{\text{alguma coisa inteira}}{\det(U)}.$$

Matrizes Unimodulares

Uma matriz inteira U é unimodular se

$$|\det(U)| = 1.$$

Relembrando: a inversa de U é dada por

$$U^{-1}_{ij} = \frac{\text{alguma coisa inteira}}{\det(U)}.$$

Conclusão: a matriz U^{-1} também é inteira.

Obtendo o certificado

Vamos supor que $AU = [B\ 0]$, onde $[B\ 0]$ é uma matriz na forma normal de Hermite e U é uma matriz unimodular.

Obtendo o certificado

Vamos supor que $AU = [B\ 0]$, onde $[B\ 0]$ é uma matriz na forma normal de Hermite e U é uma matriz unimodular.

Se $B^{-1}b$ é um vetor inteiro, como

$$[B\ 0]\begin{bmatrix} B^{-1}b \\ 0 \end{bmatrix} = b,$$

obtemos uma solução inteira para $Ax = b$:

$$AU\begin{bmatrix} B^{-1}b \\ 0 \end{bmatrix} = b$$

Obtendo o certificado

Vamos supor que $AU = [B\ 0]$, onde $[B\ 0]$ é uma matriz na forma normal de Hermite e U é uma matriz unimodular.

Se $B^{-1}b$ não é um vetor inteiro, como

$$B^{-1}[B\ 0] = [I\ 0],$$

e obtemos y tal que yA é inteiro e yb não é inteiro:

$$B^{-1}A = B^{-1}AUU^{-1} = B^{-1}[B\ 0]U^{-1} = [I\ 0]U^{-1}.$$

Não é só escolha de base

Existe solução inteira para

$$[2\ 3]x = 5,$$

mas não existe solução inteira para

$$2x = 5 \quad \text{e} \quad 3x = 5.$$

Reticulados

O reticulado gerado por um conjunto de vetores é o conjunto de combinações lineares inteiras desses vetores:

$$\{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n : \lambda_1, \lambda_2, \ldots, \lambda_n \text{ inteiros}\}.$$

Reticulados

O reticulado gerado por um conjunto de vetores é o conjunto de combinações lineares inteiras desses vetores:

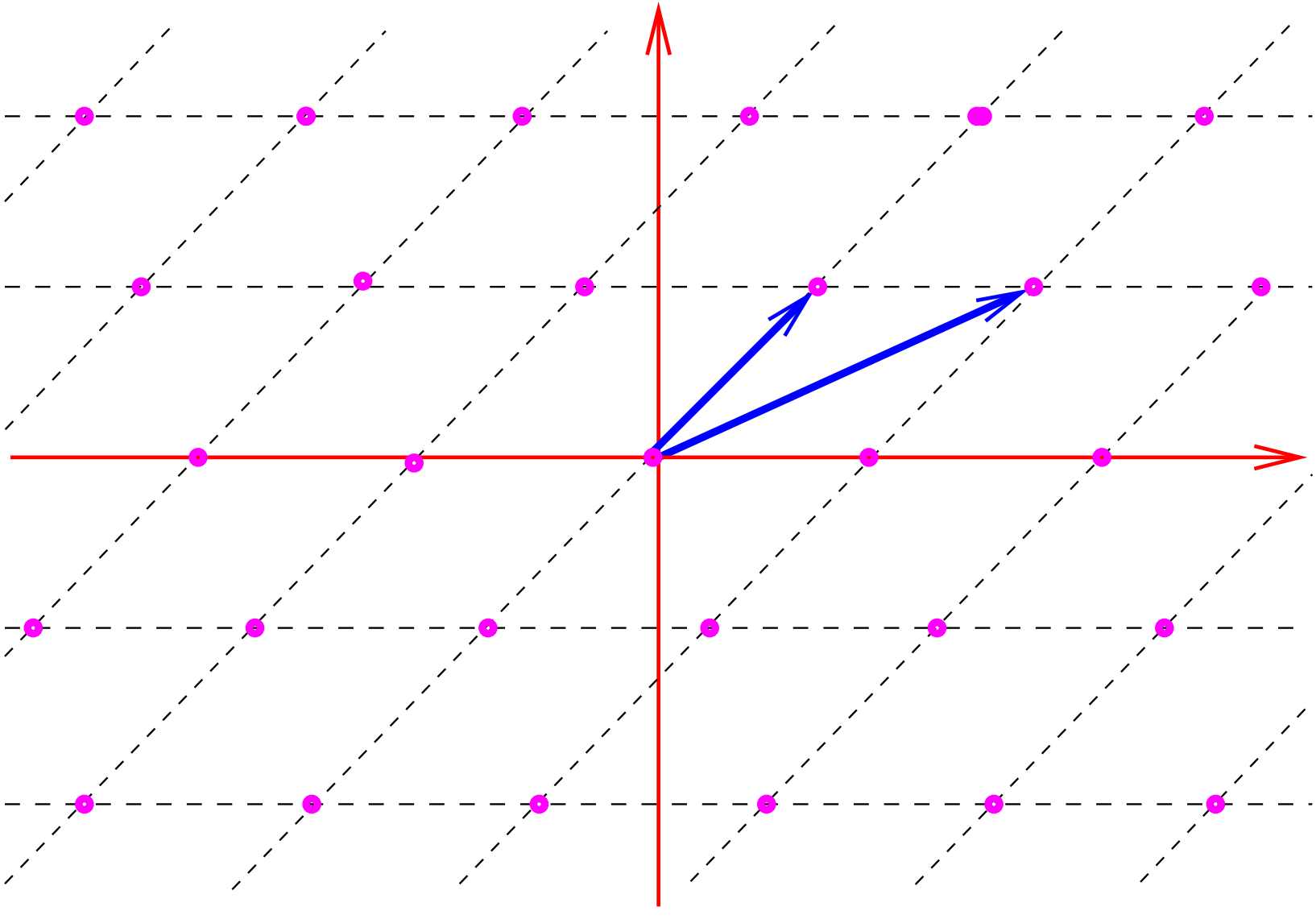
$$\{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n : \lambda_1, \lambda_2, \ldots, \lambda_n \text{ inteiros}\}.$$

"Existe solução inteira para $Ax = b$?"

$=$

"b está no reticulado gerado pelas colunas de A?"

Geometricamente



Reticulados

As operações feitas no algoritmo preservam o reticulado.

Reticulados

As operações feitas no algoritmo preservam o reticulado.

Se as colunas de A e A' geram o mesmo reticulado, as formas normais de Hermite $[B\ 0]$ e $[B'\ 0]$ são tais que

$$B = B'.$$

Reticulados

As operações feitas no algoritmo preservam o reticulado.

Se as colunas de A e A' geram o mesmo reticulado, as formas normais de Hermite $[B\ 0]$ e $[B'\ 0]$ são tais que

$$B = B'.$$

Conclusão: a forma normal de Hermite obtida é única.

Complexidade

A forma normal de Hermite e a matriz unimodular podem ser obtidas em tempo polinomial usando alguns “artifícios”.

Complexidade

A forma normal de Hermite e a matriz unimodular podem ser obtidas em tempo polinomial usando alguns “artifícios”.

É necessário adicionar colunas extras à matriz A para controlar o tamanho dos números durante o processo.

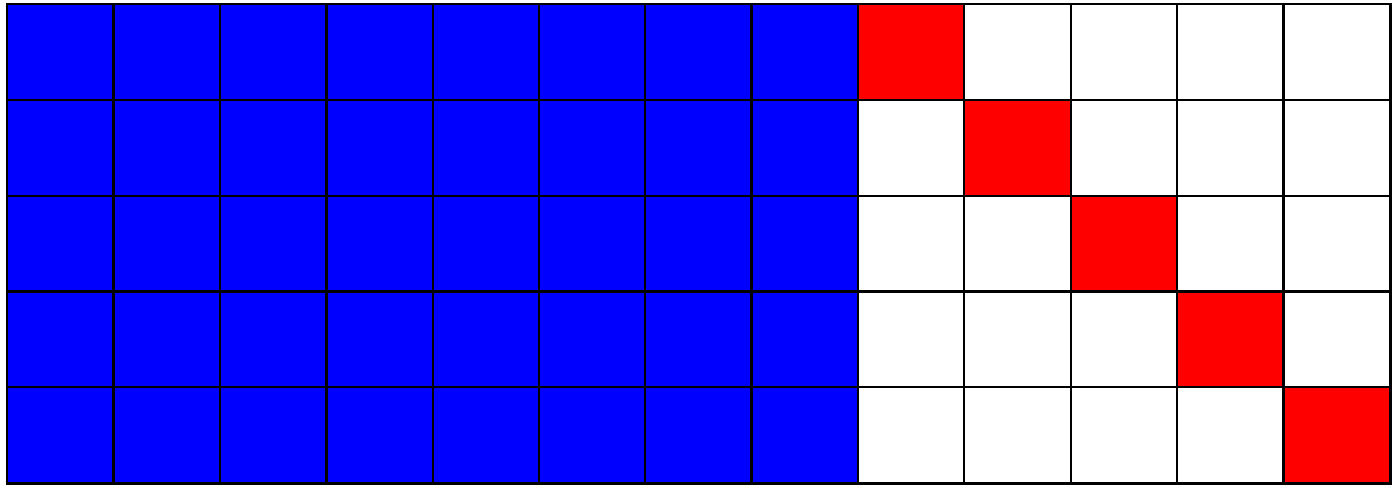
Complexidade

A forma normal de Hermite e a matriz unimodular podem ser obtidas em tempo polinomial usando alguns “artifícios”.

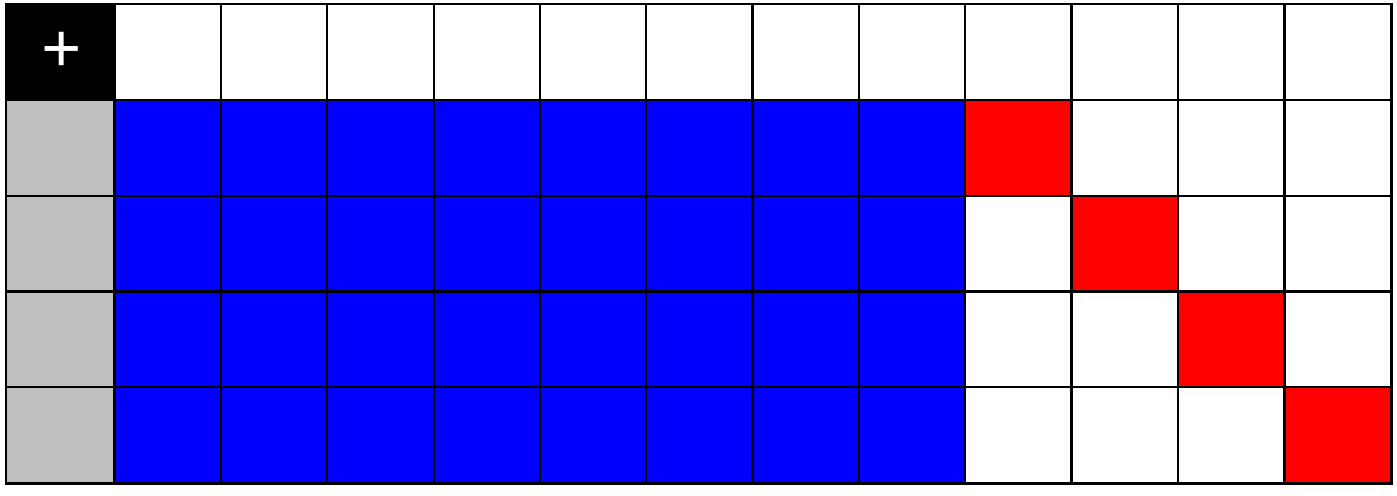
É necessário adicionar colunas extras à matriz A para controlar o tamanho dos números durante o processo.

Se as colunas extras pertencem ao reticulado gerado pelas colunas originais, a forma normal de Hermite é a mesma.

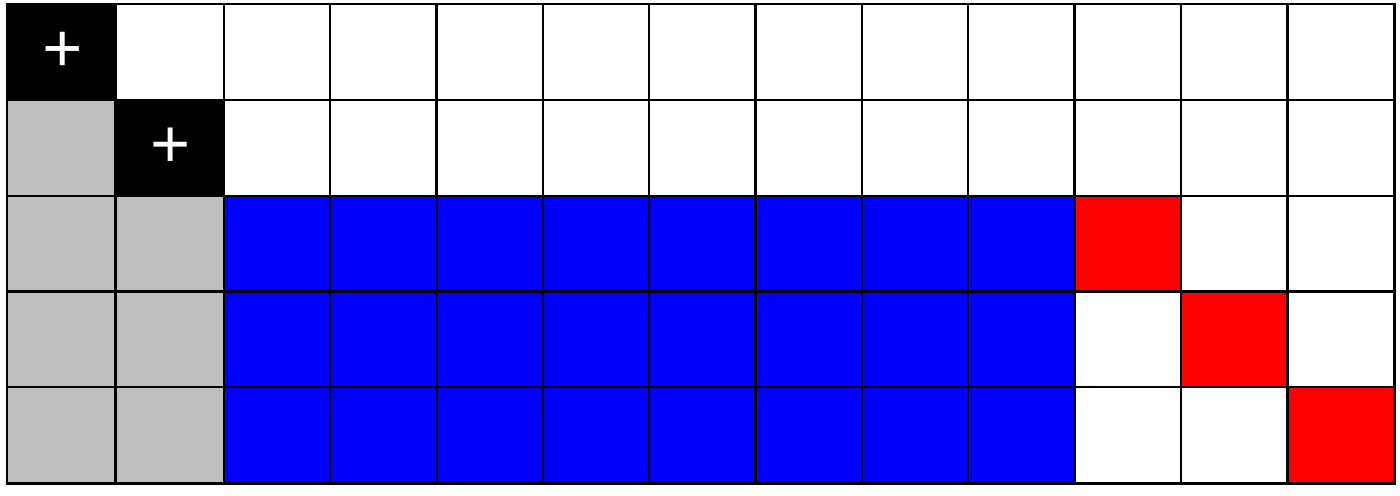
Colunas de controle



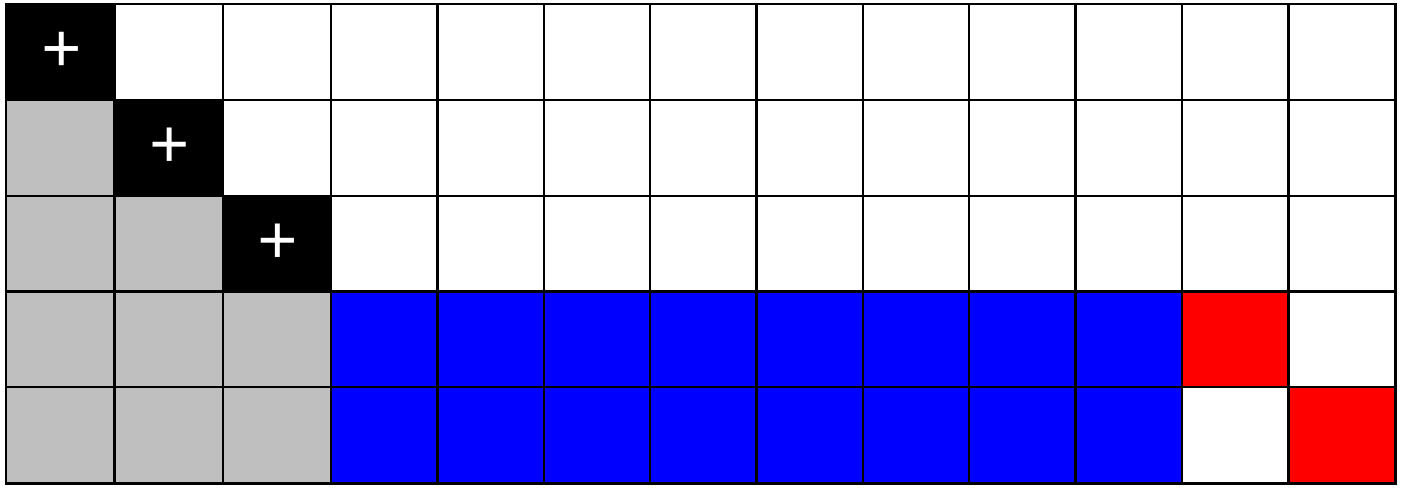
Colunas de controle



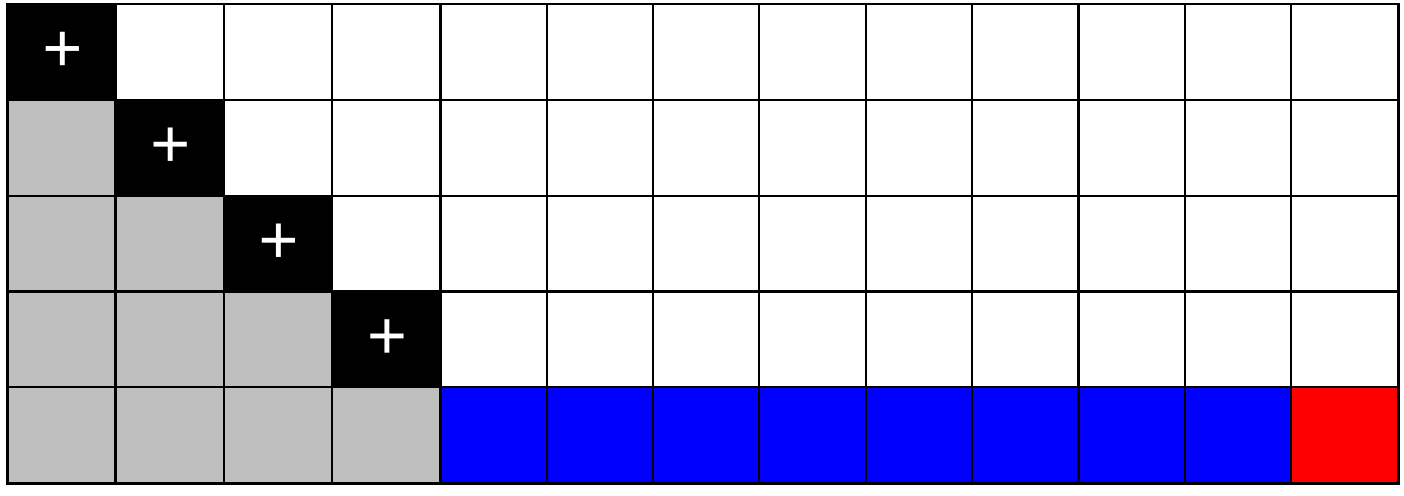
Colunas de controle



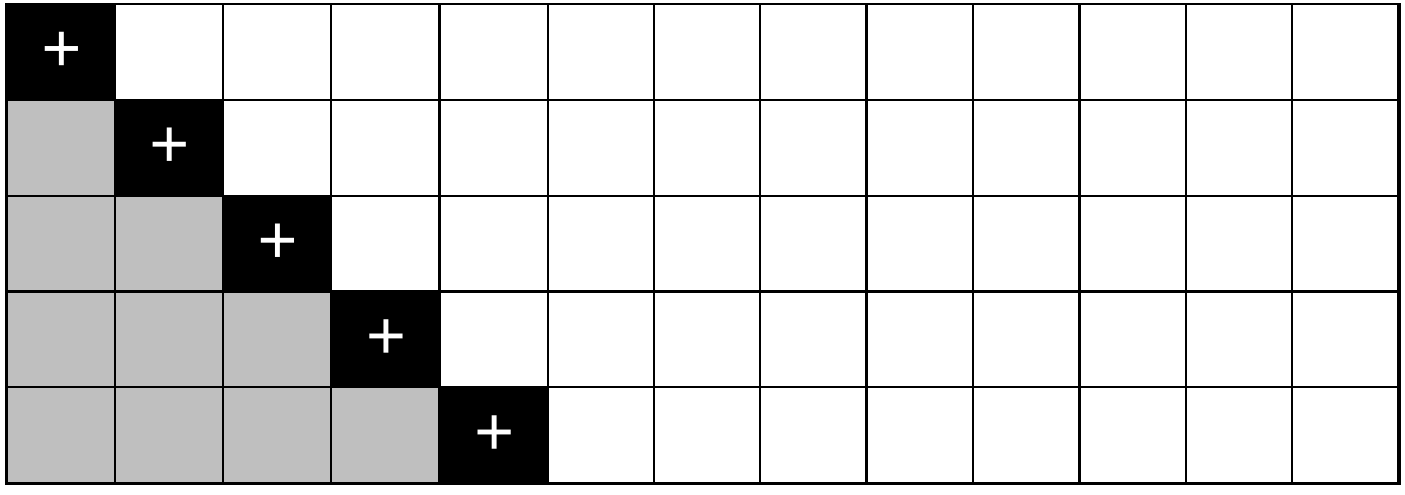
Colunas de controle



Colunas de controle



Colunas de controle



Família dos certificados de inexistência

Se não há solução para $Ax = b$, existe y com

$$yA = 0 \quad \text{e} \quad yb \neq 0.$$

Se não há solução inteira para $Ax = b$, existe y com

yA é inteiro e yb não é inteiro.

Se não há solução não-negativa para $Ax = b$, existe y com

$$yA \geq 0 \quad \text{e} \quad yb < 0.$$