The Multi-Dimensional Frobenius Problem and Vector GCDs

Vadim Ponomarenko

Department of Mathematics and Statistics
San Diego State University

Fachbereich Mathematik/Informatik Universität Bremen
April 19, 2011

http://www-rohan.sdsu.edu/∼vadim/frob-gcd.pdf

SAN DIEGO STATE UNIVERSITY

Acknowledgments

- Ulrich Krause
- National Science Foundation
- Jeffrey Amos, Iuliana Pascu, Enrique Treviño, Yan Zhang

Two Puzzles

If this talk becomes boring…

Let $A = \left\{ \binom{6}{2}, \binom{1}{1}, \binom{-1}{3} \right\}$. Question: Is $Span(A) = \mathbb{Z}^2$?

$Span(A) = \left\{ k_1 \binom{6}{2} + k_2 \binom{1}{1} + k_3 \binom{-1}{3} : k_i \in \mathbb{Z} \right\}$.

Also for $B = \left\{ \binom{6}{2}, \binom{1}{1}, \binom{-2}{3} \right\}$.

Starting Point

Fix a set A of positive integers. Usually, the Frobenius number is defined via:

$$g(A) = \max\ \mathbb{Z} \setminus \mathbb{N}_0[A]$$

This does not generalize "correctly" to vectors. Instead:

$$g(A) = \inf\{x : \text{if } y > x \text{ then } y \in \mathbb{N}_0[A]\}$$

Note: For $A = \{4, 6\}$, $g(A)$ is undefined.

SAN DIEGO STATE UNIVERSITY

Starting Point

Fix a set A of positive integers. Usually, the Frobenius number is defined via:

$$g(A) = \max\ \mathbb{Z} \setminus \mathbb{N}_0[A]$$

This does not generalize "correctly" to vectors. Instead:

$$g(A) = \inf\{x : \text{if } y > x \text{ then } y \in \mathbb{N}_0[A]\}$$

Note: For $A = \{4, 6\}$, $g(A)$ is undefined.

Starting Point

Fix a set A of positive integers. Usually, the Frobenius number is defined via:

$$g(A) = \max\ \mathbb{Z} \setminus \mathbb{N}_0[A]$$

This does not generalize "correctly" to vectors. Instead:

$$g(A) = \inf\{x : \text{if } y > x \text{ then } y \in \mathbb{N}_0[A]\}$$

Note: For $A = \{4, 6\}$, $g(A)$ is undefined.

Definition

Fix a set A of vectors from $\mathbb{N}_0^d$, with $|A| \geq d$.

Set $C = \mathbb{R}^{>0}[A]$, an open cone in the first orthant.

C is *simple* if d vectors determine it. We assume this.

Define a partial order on vectors via $y > x$ if $y - x \in C$.

$g(A) = \inf \left\{ x \in \mathbb{Q}^d : \text{if } y \in \mathbb{Z}^d \text{ and } y > x, \text{ then } y \in \mathbb{N}_0[A] \right\}$

Definition

Fix a set A of vectors from $\mathbb{N}_0^d$, with $|A| \geq d$.

Set $C = \mathbb{R}^{>0}[A]$, an open cone in the first orthant.

C is *simple* if d vectors determine it. We assume this.

Define a partial order on vectors via $y > x$ if $y - x \in C$.

$g(A) = \inf \left\{ x \in \mathbb{Q}^d : \text{if } y \in \mathbb{Z}^d \text{ and } y > x, \text{ then } y \in \mathbb{N}_0[A] \right\}$

San Diego State University

Definition

Fix a set A of vectors from $\mathbb{N}_0^d$, with $|A| \geq d$.

Set $C = \mathbb{R}^{>0}[A]$, an open cone in the first orthant.

C is *simple* if d vectors determine it. We assume this.

Define a partial order on vectors via $y > x$ if $y - x \in C$.

$$g(A) = \inf\left\{x \in \mathbb{Q}^d : \text{if } y \in \mathbb{Z}^d \text{ and } y > x, \text{ then } y \in \mathbb{N}_0[A]\right\}$$

Definition

Fix a set A of vectors from $\mathbb{N}_0^d$, with $|A| \geq d$.

Set $C = \mathbb{R}^{>0}[A]$, an open cone in the first orthant.

C is *simple* if d vectors determine it. We assume this.

Define a partial order on vectors via $y > x$ if $y - x \in C$.

$g(A) = \inf \left\{ x \in \mathbb{Q}^d : \text{if } y \in \mathbb{Z}^d \text{ and } y > x, \text{ then } y \in \mathbb{N}_0[A] \right\}$

SAN DIEGO STATE UNIVERSITY

Definition

Fix a set A of vectors from $\mathbb{N}_0^d$, with $|A| \geq d$.

Set $C = \mathbb{R}^{>0}[A]$, an open cone in the first orthant.

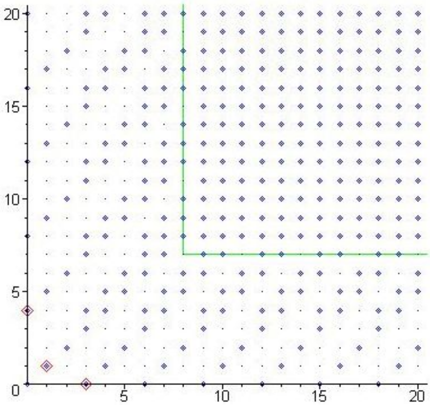
C is *simple* if d vectors determine it. We assume this.

Define a partial order on vectors via $y > x$ if $y - x \in C$.

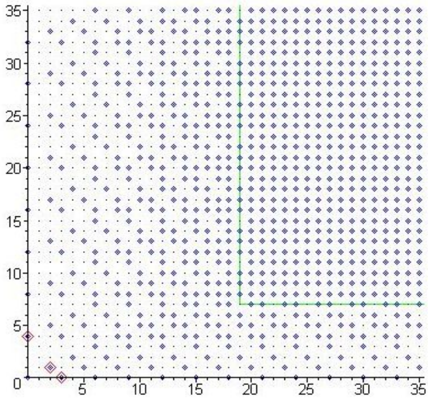
$$g(A) = \inf \left\{ x \in \mathbb{Q}^d : \text{if } y \in \mathbb{Z}^d \text{ and } y > x, \text{ then } y \in \mathbb{N}_0[A] \right\}$$

Pictures

$A = \{(0,4),(1,1),(3,0)\}$

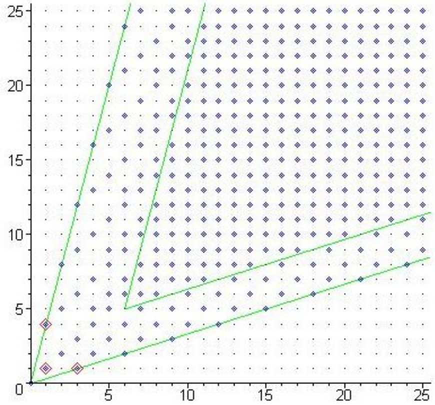


$A = \{(0,4),(2,1),(3,0)\}$

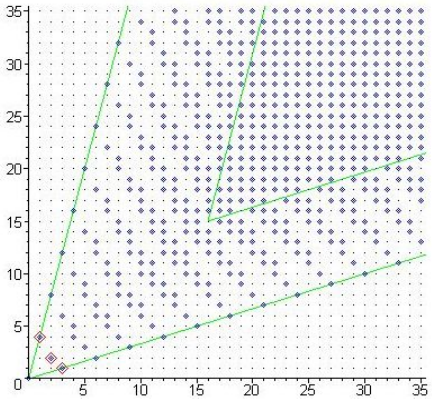


More Pictures

$A = \{(1,4),(1,1),(3,1)\}$



$A = \{(1,4),(2,2),(3,1)\}$



Just One Vector?

Thm [Simpson Tijdeman 2003]: Suppose $|A| = d + 1$, $g(A)$ is nonempty, and $a_1, \ldots, a_d$ determine C. Then

$$g(A) = \{|a_1 a_2 \cdots a_d| a_{d+1} - \sum A\}.$$

Generalizes the 1-d: $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

In particular, $|g(A)| = 1$, and $g(A) \subseteq \mathbb{Z}^d$.

(converse) Thm: Given $x \in \mathbb{N}^d$, there is an A with $|A| = d + 1$ and $g(A) = \{x\}$, if and only if at least one coordinate of x is odd.

Just One Vector?

Thm [Simpson Tijdeman 2003]: Suppose $|A| = d + 1$, $g(A)$ is nonempty, and $a_1, \ldots, a_d$ determine C. Then

$$g(A) = \{|a_1 a_2 \cdots a_d| a_{d+1} - \sum A\}.$$

Generalizes the 1-d: $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

In particular, $|g(A)| = 1$, and $g(A) \subseteq \mathbb{Z}^d$.

(converse) Thm: Given $x \in \mathbb{N}^d$, there is an A with $|A| = d + 1$ and $g(A) = \{x\}$, if and only if at least one coordinate of x is odd.

Just One Vector?

Thm [Simpson Tijdeman 2003]: Suppose $|A| = d + 1$, $g(A)$ is nonempty, and $a_1, \ldots, a_d$ determine C. Then

$$g(A) = \{|a_1 a_2 \cdots a_d| a_{d+1} - \sum A\}.$$

Generalizes the 1-d: $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

In particular, $|g(A)| = 1$, and $g(A) \subseteq \mathbb{Z}^d$.

(converse) Thm: Given $x \in \mathbb{N}^d$, there is an A with $|A| = d + 1$ and $g(A) = \{x\}$, if and only if at least one coordinate of x is odd.

Just One Vector?

Thm [Simpson Tijdeman 2003]: Suppose $|A| = d+1$, $g(A)$ is nonempty, and $a_1, \ldots, a_d$ determine C. Then

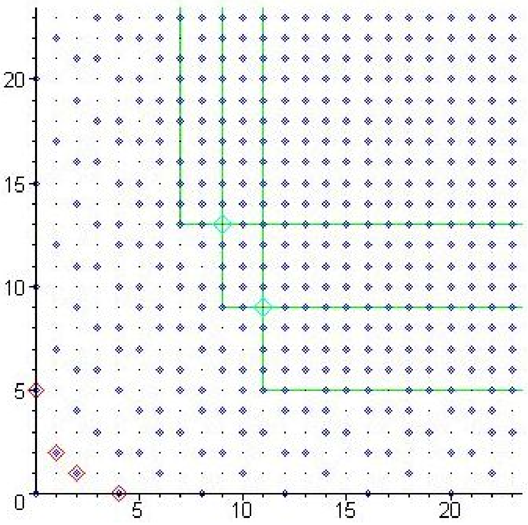
$$g(A) = \{|a_1 a_2 \cdots a_d| a_{d+1} - \sum A\}.$$

Generalizes the 1-d: $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

In particular, $|g(A)| = 1$, and $g(A) \subseteq \mathbb{Z}^d$.

(converse) Thm: Given $x \in \mathbb{N}^d$, there is an A with $|A| = d+1$ and $g(A) = \{x\}$, if and only if at least one coordinate of x is odd.

$|g(A)| > 1$



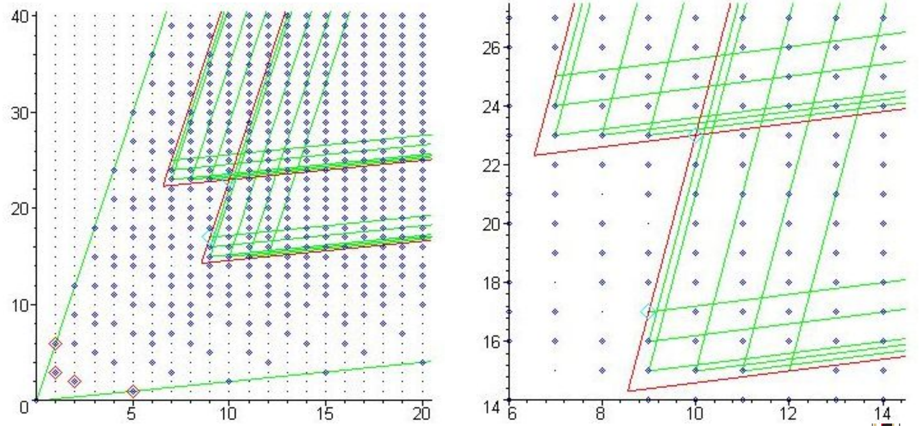
$A = \{(0,5), (1,2), (2,1), (4,0)\}$

$g(A) =$
$\{(7,13), (9,9), (11,5)\}$

Missing from $\mathbb{N}_0[A]$: (9,13),(11,9), as indicated, and infinitely many points on $x = 7, y = 5$

$g(A) \not\subset \mathbb{Z}^d$

$A = \{(1,6),(2,2),(1,3),(5,1)\}$. $g(A) = \left\{\left(\frac{190}{29}, \frac{647}{29}\right), \left(\frac{248}{29}, \frac{415}{29}\right)\right\}$
(2 Frobenius vectors are better than 11) Why 29?



Miscellaneous Results

Assume $A \subseteq \mathbb{N}_0^d$, $a_1, a_2, \ldots, a_d$ determine C, $g(A) \neq \emptyset$.

Thm: $|a_1 a_2 \cdots a_d| g(A) \subseteq \mathbb{Z}^d$. (not too far from $\mathbb{Z}^d$)

Thm:
$g(A) \leq (|a_1 a_2 \cdots a_d| - 1) LUB(a_{d+1}, \ldots, a_k) - a_1 - \cdots - a_d$

Note: generalizes a one-dimensional bound of Schur 1935:
$g(A) \leq (a_1 - 1) \max\{a_2, \ldots, a_k\} - a_1$

Miscellaneous Results

Assume $A \subseteq \mathbb{N}_0^d$, $a_1, a_2, \ldots, a_d$ determine C, $g(A) \neq \emptyset$.

Thm: $|a_1 a_2 \cdots a_d| g(A) \subseteq \mathbb{Z}^d$. (not too far from $\mathbb{Z}^d$)

Thm:
$g(A) \leq (|a_1 a_2 \cdots a_d| - 1) LUB(a_{d+1}, \ldots, a_k) - a_1 - \cdots - a_d$

Note: generalizes a one-dimensional bound of Schur 1935:
$g(A) \leq (a_1 - 1) \max\{a_2, \ldots, a_k\} - a_1$

Miscellaneous Results

Assume $A \subseteq \mathbb{N}_0^d$, $a_1, a_2, \ldots, a_d$ determine C, $g(A) \neq \emptyset$.

Thm: $|a_1 a_2 \cdots a_d| g(A) \subseteq \mathbb{Z}^d$. (not too far from $\mathbb{Z}^d$)

Thm:
$g(A) \leq (|a_1 a_2 \cdots a_d| - 1) LUB(a_{d+1}, \ldots, a_k) - a_1 - \cdots - a_d$

Note: generalizes a one-dimensional bound of Schur 1935:
$g(A) \leq (a_1 - 1) \max\{a_2, \ldots, a_k\} - a_1$

Miscellaneous Results

Assume $A \subseteq \mathbb{N}_0^d$, $a_1, a_2, \ldots, a_d$ determine C, $g(A) \neq \emptyset$.

Thm: $|a_1 a_2 \cdots a_d| g(A) \subseteq \mathbb{Z}^d$. (not too far from $\mathbb{Z}^d$)

Thm:
$g(A) \leq (|a_1 a_2 \cdots a_d| - 1) LUB(a_{d+1}, \ldots, a_k) - a_1 - \cdots - a_d$

Note: generalizes a one-dimensional bound of Schur 1935:
$g(A) \leq (a_1 - 1) \max\{a_2, \ldots, a_k\} - a_1$

Existence of $g(A)$

Schur's Thm: $g(A)$ is nonempty if and only if $GCD(A) = 1$

Novikov 92/94, Halter-Koch 93, found technical conditions for $g(A) \neq \emptyset$, but not this nice.

Need to define $GCD(A)$ for $A \subseteq \mathbb{N}_0^d$.

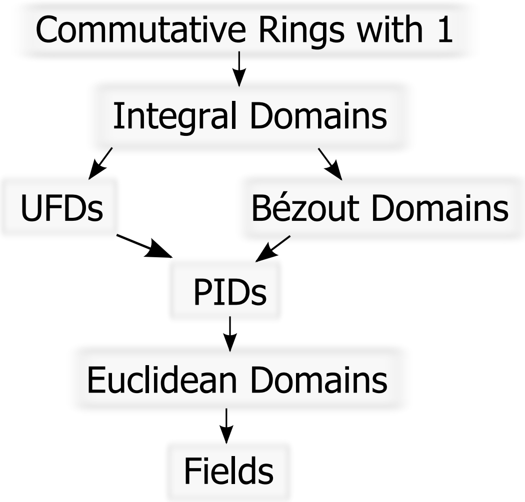
Existence of $g(A)$

Schur's Thm: $g(A)$ is nonempty if and only if $GCD(A) = 1$

Novikov 92/94, Halter-Koch 93, found technical conditions for $g(A) \neq \emptyset$, but not this nice.

Need to define $GCD(A)$ for $A \subseteq \mathbb{N}_0^d$.

Algebraic Context for GCDs



1. Commutative Rings: anything goes
2. Integral Domains: GCD's are associates
3. UFDs: GCD's exist
4. Bézout Domains: GCD's exist, in span
5. PIDs: Smith normal form
6. Euclidean Domains: good computation
7. Fields: GCD's trivial

Definition

$A \subseteq \mathbb{Z}^d$. Set $n = |A|$. We will define $GCD(A) \in \mathbb{N}_0$.

Let $[A]$ be the $d \times n$ matrix whose columns are A.

Choose d columns of $[A]$, take determinant.

Let $\overline{A}$ be a list of all these $\binom{n}{d}$ determinants.

Define $GCD(A) = GCD(\overline{A})$.

Note: "d^{th} determinantal divisor" of $[A]$.

Definition

$A \subseteq \mathbb{Z}^d$. Set $n = |A|$. We will define $GCD(A) \in \mathbb{N}_0$.

Let $[A]$ be the $d \times n$ matrix whose columns are A.

Choose d columns of $[A]$, take determinant.

Let $\overline{A}$ be a list of all these $\binom{n}{d}$ determinants.

Define $GCD(A) = GCD(\overline{A})$.

Note: "d^{th} determinantal divisor" of $[A]$.

Definition

$A \subseteq \mathbb{Z}^d$. Set $n = |A|$. We will define $GCD(A) \in \mathbb{N}_0$.
Let $[A]$ be the $d \times n$ matrix whose columns are A.
Choose d columns of $[A]$, take determinant.
Let $\overline{A}$ be a list of all these $\binom{n}{d}$ determinants.

Define $GCD(A) = GCD(\overline{A})$.

Note: "d^{th} determinantal divisor" of $[A]$.

Definition

$A \subseteq \mathbb{Z}^d$. Set $n = |A|$. We will define $GCD(A) \in \mathbb{N}_0$.
Let $[A]$ be the $d \times n$ matrix whose columns are A.
Choose d columns of $[A]$, take determinant.
Let $\overline{A}$ be a list of all these $\binom{n}{d}$ determinants.

Define $GCD(A) = GCD(\overline{A})$.

Note: "d^{th} determinantal divisor" of $[A]$.

Some GCD Properties

Increasing: Let $B \subseteq A$. Then $GCD(A)|GCD(B)$

Similarity: Suppose there are invertible matrices L, R with $[A] = L[B]R$. Then $GCD(A) = GCD(B)$.

"Common" Divisor: For all $A \subseteq \mathbb{Z}^d$ there exists $B \subseteq \mathbb{Z}^d$ and $M \in M_d(\mathbb{Z})$ with $A = MB$ and $GCD(A) = det(M)$.

"Greatest" Common Divisor: For all $A \subseteq \mathbb{Z}^d$, $M \in M_d(\mathbb{Z})$, $GCD(MA) = |det(M)|GCD(A)$.

Proof hint: Smith normal form

Some GCD Properties

Increasing: Let $B \subseteq A$. Then $GCD(A)|GCD(B)$

Similarity: Suppose there are invertible matrices L, R with $[A] = L[B]R$. Then $GCD(A) = GCD(B)$.

"Common" Divisor: For all $A \subseteq \mathbb{Z}^d$ there exists $B \subseteq \mathbb{Z}^d$ and $M \in M_d(\mathbb{Z})$ with $A = MB$ and $GCD(A) = det(M)$.

"Greatest" Common Divisor: For all $A \subseteq \mathbb{Z}^d$, $M \in M_d(\mathbb{Z})$, $GCD(MA) = |det(M)|GCD(A)$.

Proof hint: Smith normal form

Some GCD Properties

Increasing: Let $B \subseteq A$. Then $GCD(A) | GCD(B)$

Similarity: Suppose there are invertible matrices L, R with $[A] = L[B]R$. Then $GCD(A) = GCD(B)$.

"Common" Divisor: For all $A \subseteq \mathbb{Z}^d$ there exists $B \subseteq \mathbb{Z}^d$ and $M \in M_d(\mathbb{Z})$ with $A = MB$ and $GCD(A) = det(M)$.

"Greatest" Common Divisor: For all $A \subseteq \mathbb{Z}^d$, $M \in M_d(\mathbb{Z})$, $GCD(MA) = |det(M)| GCD(A)$.

Proof hint: Smith normal form

Some GCD Properties

Increasing: Let $B \subseteq A$. Then $GCD(A)|GCD(B)$

Similarity: Suppose there are invertible matrices L, R with $[A] = L[B]R$. Then $GCD(A) = GCD(B)$.

"Common" Divisor: For all $A \subseteq \mathbb{Z}^d$ there exists $B \subseteq \mathbb{Z}^d$ and $M \in M_d(\mathbb{Z})$ with $A = MB$ and $GCD(A) = det(M)$.

"Greatest" Common Divisor: For all $A \subseteq \mathbb{Z}^d$, $M \in M_d(\mathbb{Z})$, $GCD(MA) = |det(M)|GCD(A)$.

Proof hint: Smith normal form

Some GCD Properties

Increasing: Let $B \subseteq A$. Then $GCD(A)|GCD(B)$

Similarity: Suppose there are invertible matrices L, R with $[A] = L[B]R$. Then $GCD(A) = GCD(B)$.

"Common" Divisor: For all $A \subseteq \mathbb{Z}^d$ there exists $B \subseteq \mathbb{Z}^d$ and $M \in M_d(\mathbb{Z})$ with $A = MB$ and $GCD(A) = det(M)$.

"Greatest" Common Divisor: For all $A \subseteq \mathbb{Z}^d$, $M \in M_d(\mathbb{Z})$, $GCD(MA) = |det(M)|GCD(A)$.

Proof hint: Smith normal form

Bézout's identity

Thm: $Span(A) = GCD(A)\mathbb{Z}$ (1-d)

Thm: $[\mathbb{Z}^d : Span(A)] = GCD(A)$ $(\neq 0)$. submodule index

Cor: $g(A)$ is nonempty if and only if $GCD(A) = 1$

Bézout's identity

Thm: $Span(A) = GCD(A)\mathbb{Z}$ (1-d)

Thm: $[\mathbb{Z}^d : Span(A)] = GCD(A)$ $(\neq 0)$. submodule index

Cor: $g(A)$ is nonempty if and only if $GCD(A) = 1$

Bézout's identity

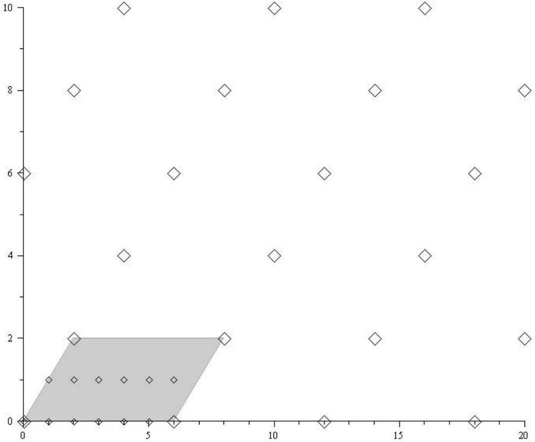
Thm: $Span(A) = GCD(A)\mathbb{Z}$ (1-d)

Thm: $[\mathbb{Z}^d : Span(A)] = GCD(A)$ $(\neq 0)$. submodule index

Cor: $g(A)$ is nonempty if and only if $GCD(A) = 1$

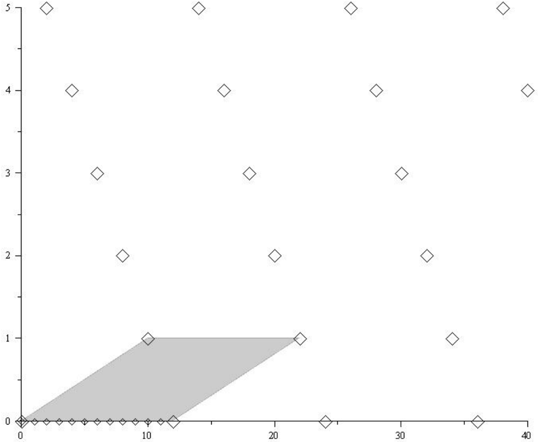
Pictures

Let $A = \left\{ \begin{pmatrix} 10 \\ 4 \end{pmatrix}, \begin{pmatrix} 8 \\ 2 \end{pmatrix} \right\}$. $[A] = L \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix} R$. $GCD(A) = 12$.



Pictures

Let $A = \left\{ \begin{pmatrix} 10 \\ 1 \end{pmatrix}, \begin{pmatrix} 8 \\ 2 \end{pmatrix} \right\}$. $[A] = L \begin{pmatrix} 1 & 0 \\ 0 & 12 \end{pmatrix} R$. $GCD(A) = 12$.



Original Two Puzzles

Let $A = \left\{ \binom{6}{2}, \binom{1}{1}, \binom{-1}{3} \right\}$. Question: Is $Span(A) = \mathbb{Z}^2$?
$\overline{A} = \{4, 20, 4\}$ so $GCD(A) = 4 = [\mathbb{Z}^2 : Span(A)]$. NO

Also for $B = \left\{ \binom{6}{2}, \binom{1}{1}, \binom{-2}{3} \right\}$.
$\overline{B} = \{4, 22, 5\}$ so $GCD(A) = 1$ and $Span(B) = \mathbb{Z}^2$. YES

Original Two Puzzles

Let $A = \left\{ \binom{6}{2}, \binom{1}{1}, \binom{-1}{3} \right\}$. Question: Is $Span(A) = \mathbb{Z}^2$?
$\overline{A} = \{4, 20, 4\}$ so $GCD(A) = 4 = [\mathbb{Z}^2 : Span(A)]$. NO

Also for $B = \left\{ \binom{6}{2}, \binom{1}{1}, \binom{-2}{3} \right\}$.
$\overline{B} = \{4, 22, 5\}$ so $GCD(A) = 1$ and $Span(B) = \mathbb{Z}^2$. YES

Final Thoughts

Are all $\binom{n}{d}$ determinants necessary?

See "The Multi-Dimensional Frobenius Problem",
http://www-rohan.sdsu.edu/~vadim/research.html

Final Thoughts

Are all $\binom{n}{d}$ determinants necessary?

See “The Multi-Dimensional Frobenius Problem”,
http://www-rohan.sdsu.edu/∼vadim/research.html