The Higher-dimensional Frobenius Problem

Trinity REU 2005

Jeff Amos, Iuliana Pascu, Enrique Treviño, Yan Zhang
under the direction of
Professor Vadim Ponomarenko

August 12, 2005

Original Problem

- If we have 6- and 10-unit coins, for what amount can we make change?

- What about 7- and 10- instead?

Quantity	# Decomposition
54	2 * 7 + 4 * 10
55	5 * 7 + 2 * 10
56	7 * 8
57	7 + 5 * 10
⋮	⋮

Given positive integers $a_1, a_2, \ldots, a_k$ with gcd 1, find the largest integer n such that n cannot be expressed in the form $c_1 a_1 + c_2 a_2 + \ldots + c_k a_k$, where c_i are nonnegative integers.

The number n is called the *Frobenius number* $frob(a_1, a_2, \ldots, a_k)$.

1. Example: $frob(4, 5) = 11$.

2. $gcd = 1$ is necessary: $frob(6, 8)$ does not exist.

Classical result:

Theorem 1 (Classical)**.** *Given positive integers* a_1 *and* a_2 *with gcd* 1*, we can express any integer* $n > g(a_1, a_2) = a_1 a_2 - a_1 - a_2$ *as* $c_1 a_1 + c_2 a_2$*, where* c_i *are nonnegative integers.*

$k = 3$ should be easy right?

Theorem 2 (Fel 04)**.** *Fix* $k = 3$*. Set* $w = c_1 a_1 + c_2 a_2 + c_3 a_3$*. Then* $g(a_1, a_2, a_3)$ *equals*

$$\frac{1}{2}(w + \sqrt{w^2 + 4a_1 a_2 a_3 - 4(c_3 c_2 a_3 a_2 + c_3 c_1 a_3 a_1 + c_2 c_1 a_2 a_1)}).$$

Theorem 3 (Curtis 90). *There is no finite set of polynomials with complex coefficients for k variables, such that for each choice of a_1, a_2, a_3, there is some polynomial in this list which evaluates $frob(a_1, a_2, a_3)$.*

Theorem 4. *Finding $frob(S)$ is NP-hard for variable k.*

Over a hundred papers have been written and still are being written for this problem.

Extension

We explore the vector analogue of the classical Frobenius problem.

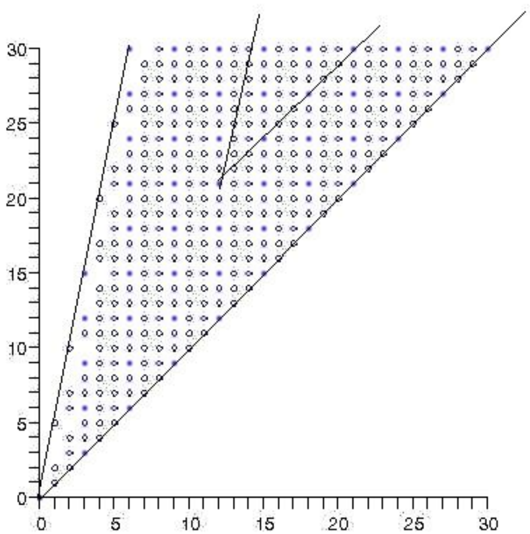
Given a set of vectors $V = \{\mathbf{v_1}, \ldots, \mathbf{v_k}\} \subset \mathbf{Z}^r$, consider $S(\mathbf{v_1}, \ldots, \mathbf{v_k})$ to be the set $\{c_1\mathbf{v_1} + \cdots + c_k\mathbf{v_k} | c_1, \ldots, c_k \in \mathbf{N}_0\}$.

Problems with Getting Started

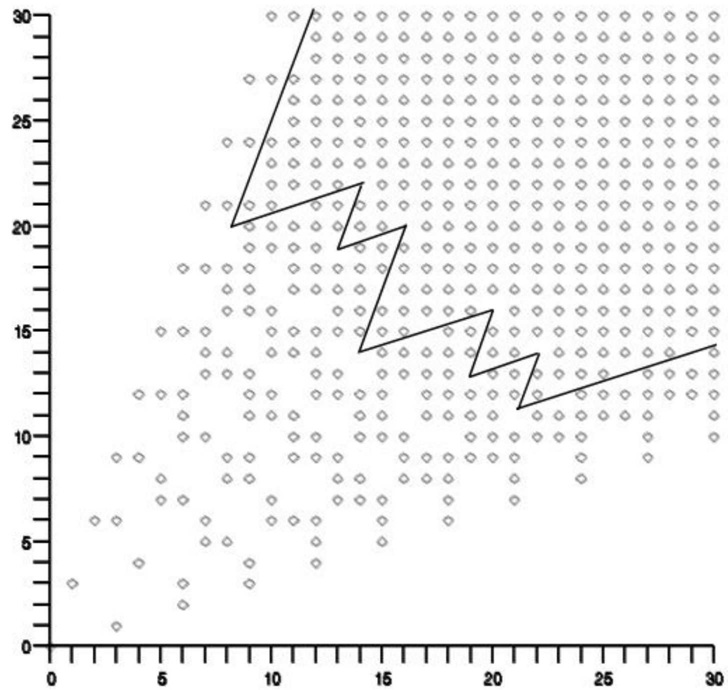
- How do we find a “maximal” vector?
- Do we have uniqueness for the “Frobenius vector”?
- Does one even exist?
- What about an analogue of gcd condition?

Cones and g-vectors

- What is a cone?
- Order by *inclusion*
- Complete points
- g-vectors



0
5
10
15
20
25
30

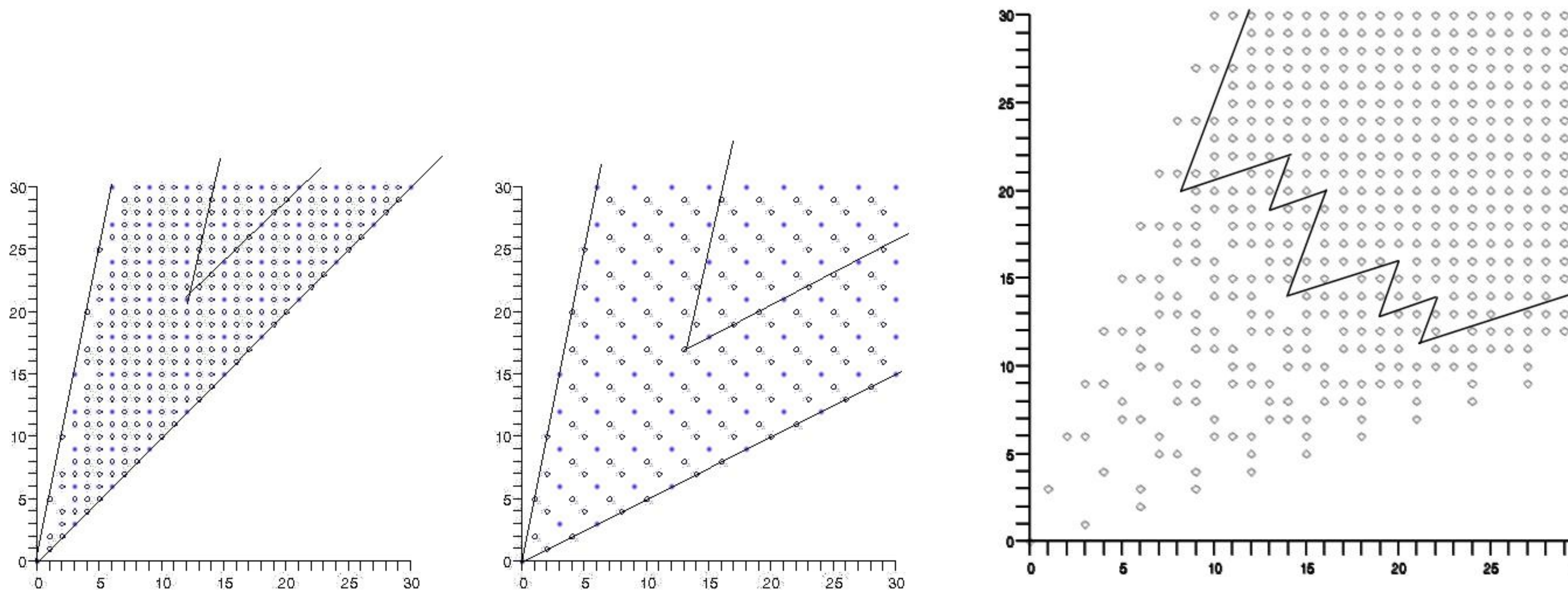


0
5
10
15
20
25
30

Density and Volume

- Density: we have "closely packed" points.

- Volume: the cone is k-dimensional



Density/volume condition

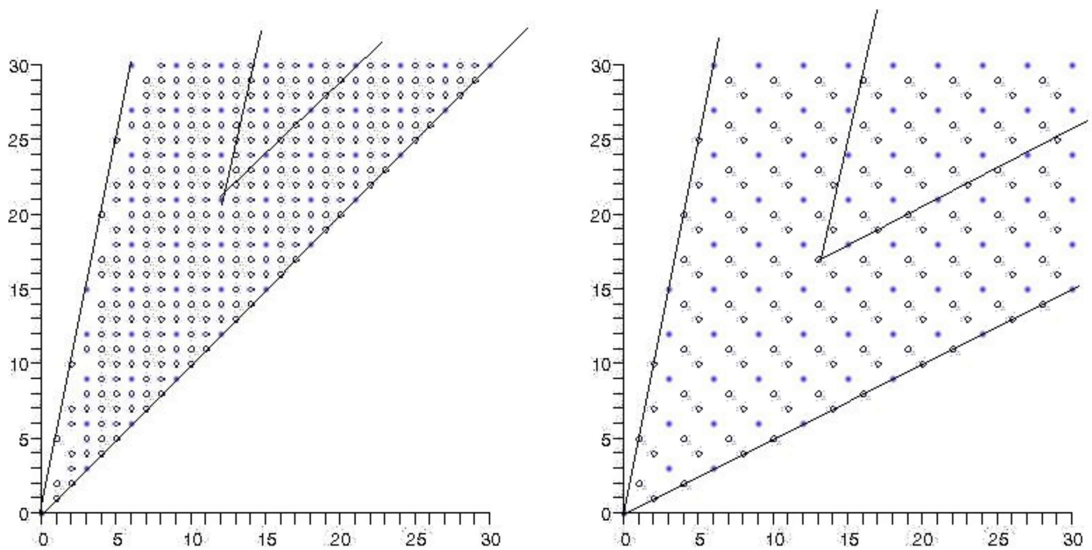
Theorem 5. *S is dense iff $gcd(\mathbf{v_1}, \ldots, \mathbf{v_k}) = 1$. $S = S_{\mathbf{N}_0}(V)$ is volume if and only if* $\text{gcd}(V) \neq \infty$.

GCD of vectors

$$
\begin{aligned}
& \gcd((1,5),(1,2),(2,1)) && (1)\\
= \; & \gcd(\det\begin{pmatrix}1 & 1\\ 5 & 2\end{pmatrix}, \det\begin{pmatrix}1 & 2\\ 5 & 1\end{pmatrix}, \det\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}) && (2)\\
= \; & \gcd(-3,-9,-3) && (3)\\
= \; & 3. && (4)
\end{aligned}
$$

GCD of vectors (Part II)

Examples: $\gcd\{(1,5),(1,2),(1,1)\} = 1$ and $\gcd\{(1,5),(1,2),(2,1)\} = 3$:



$k = r + 1$ **case**

In one dimension we have the following:

Old Theorem 1 (Classical)**.** *Given positive integers* a_1 *and* a_2 *with gcd* 1*, we can express any integer* $n > g(a_1, a_2) = a_1a_2 - a_1 - a_2$ *as* $c_1a_1 + c_2a_2$*, where* c_i *are nonnegative integers.*

With $r + 1$ vectors in r dimensions we have:

Theorem 6 (REU 05)**.** *Suppose* S *is dense, and* $S_{\mathbf{R}}$ *is a simple cone generated by* $\mathbf{v_1}, \ldots, \mathbf{v_r}$*. Let* A *be the* $r \times r$ *matrix with columns* $\mathbf{v_1}, \ldots, \mathbf{v_r}$*. Then* $g(v_1, \ldots, v_{r+1}) = \{|A|\mathbf{v_{r+1}} - \mathbf{v_1} - \ldots - \mathbf{v_{r+1}}\}$

More Generalizations

In one dimension we have the following:

Old Theorem 2 (Roberts 56). *Suppose that gcd*($m, m+w, m+2w, \ldots, m+(k-1)w$) $= 1$. *Then* $g(m, m+w, m+2w, \ldots, m+(k-1)w) = m\lfloor \frac{m-2}{k-1} \rfloor + (m-1)w$.

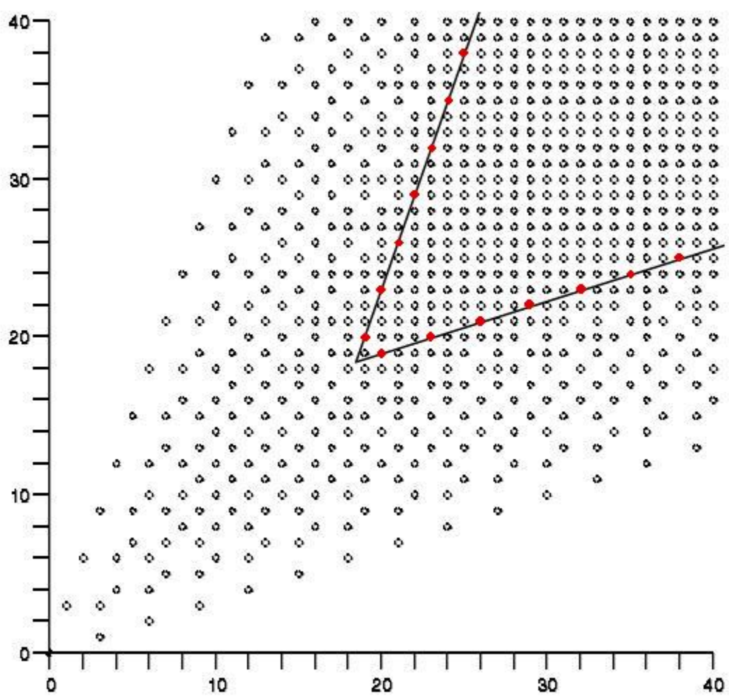
In r dimensions we have the following:

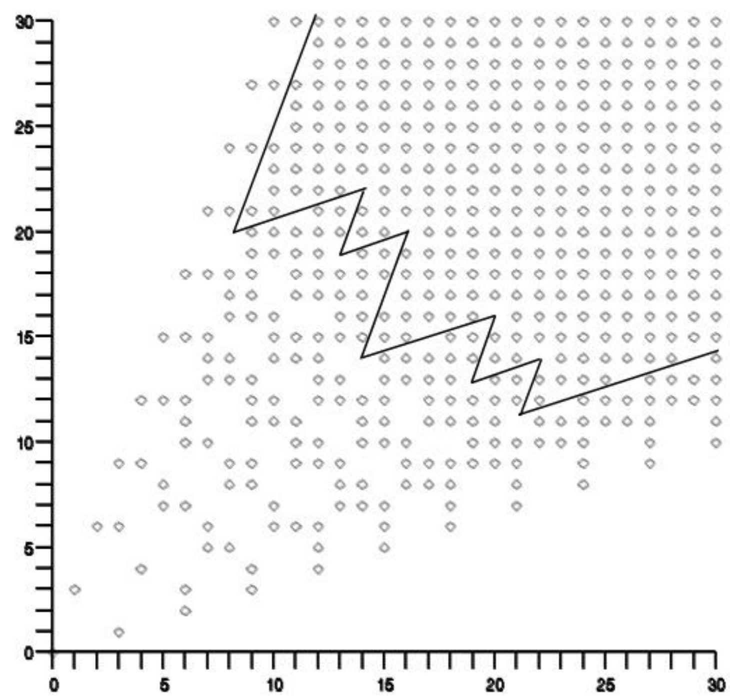
Theorem 7 (REU 05). *Let* $V = \{\mathbf{v_i} + j\mathbf{w} \mid 0 \leq r,\ 0 \leq j \leq k-1\}$. *Suppose* S *is dense, and* $S_{\mathbf{R}}$ *is a simple cone generated by* $v_1, \ldots, v_r$. *Let* A *be the* $r \times r$ *matrix with columns* $\mathbf{v_1}, \ldots, \mathbf{v_r}$. *Let* $G = \{(c_1-1)\mathbf{v_1} + \ldots + (c_r-1)\mathbf{v_r} + (|A|-1)\mathbf{w} \mid c_1, \ldots, c_r \in \mathbf{N}_0$ $c_1 + \ldots + c_r = \left\lfloor \frac{|A|-2}{k-1} \right\rfloor + 1\}$. *Now* $g(V) = G$, *and we get a meat grinder.*

Characterizing Unique g-vectors

Theorem 8 (REU 05)**.** *Let* $\mathbf{g}$ *be a g-vector. Then* $\mathbf{g}$ *is the unique g-vector iff for all* $i \in [1, r]$ *there exists* $\mathbf{w_i} = \sum_{j=1}^{r} \alpha_j \mathbf{v_j} \in \mathbf{Z}^r$ *with* $\alpha_1, \ldots, \alpha_r \in (0, 1]$ *and* $\alpha_i = 0$ *such that for all* $k \in \mathbf{Z}_{\geq 0}$*,* $\mathbf{g} + k(\mathbf{v_A} - \mathbf{v_i}) + \mathbf{w_i} \notin S$*.*

Huh?


0
10
20
30
40
0
10
20
30
40


0
5
10
15
20
25
30
0
5
10
15
20
25
30

New Stuff

Theorem 9 (Johnson 60)**.** *Let* $A = \{a_1, \ldots, a_k\}$ *and* $B = \{a_1, da_2, \ldots, da_k\}$*. Then* $dg(A) + (d-1)a_1 = g(B)$.

Theorem 10. *Let* $V = \{\mathbf{v_1}, \ldots, \mathbf{v_k}\}$ *and* $W = \{\mathbf{v_1}, \ldots, \mathbf{v_r}, d\mathbf{v_{r+1}}, \ldots, d\mathbf{v_k}\}$ *where* $d \in \mathbb{N}$*. Then* $dg(V) + (d-1)\mathbf{V_A} = g(W)$*.*

Simplified Stuff I

For D, a finite subset of $\mathbf{R}^r$, we define $lub(D)$ as a minimal vector greater than or equal to all vectors in D.

Lemma 1. *Let* $D = \{\mathbf{d_1}, ..., \mathbf{d_m}\}$ *where* $\mathbf{d_i} \in \mathbf{Z}^r$*, and let* $\mathbf{g} \in \mathbf{Z}^r$*. Then* $lub(D)$ *is unique, and can be computed as follows:*

$$lub(D) = \sum_{i=1}^{r} \max_{j \in [1,m]} \Big(P_i(\mathbf{d_j}) \Big) \mathbf{v_i}$$

Simplified Stuff II

Theorem 11. *If* $\mathbf{g} \in g(V)$ *then there exist* $\omega_{\mathbf{1}}, \ldots, \omega_{|\mathbf{A}|} \in m(V)$*, a complete set of co-set representatives, such that* $\mathbf{g} + \mathbf{V_A} = lub(\omega_{\mathbf{1}}, \ldots, \omega_{|\mathbf{A}|})$*.*

Schur Generalized

In one dimension we have the following:

Old Theorem 3 (Schur 35). *If* $a_1 \leq a_2 \leq \ldots \leq a_k$ *then* $g(S) \leq a_1 a_k - a_1 - a_k$.

In r dimensions we have the following:

Theorem 12 (REU 05). *If* $\mathbf{g} \in g(V)$ *then* $\mathbf{g} \leq lub((|A|-1)\mathbf{v_1}, \ldots, (|A|-1)\mathbf{v_r}) - \mathbf{V_A}$.

Another Special Case

Theorem 13. *Let* $V = \{\mathbf{v_1}, \ldots, \mathbf{v_r}, c_1\mathbf{w}, \ldots, c_n\mathbf{w}\}$ *where* $c_1, \ldots, c_n \in \mathrm{N}$ *with* $c_1, \ldots, c_n, |A|$ *relatively prime. Now we have* $g(V) = \{g(c_1, \ldots, c_n, |A|)\mathbf{w} + |A|\mathbf{w} - \mathbf{V_A}\}$ *where* g *is the Frobenius function.*

Notice that when $n = 1$ we have

$$\begin{aligned} g(V) &= g(c_1, \ldots, c_n, |A|)\mathbf{w} + |A|\mathbf{w} - \mathbf{V_A} \\ &= (c_1|A| - c_1 - |A|)\mathbf{w} + |A|\mathbf{w} - \mathbf{V_A} \\ &= (|A| - 1)c_n\mathbf{w} - \mathbf{V_A}. \end{aligned}$$

This is the formula we have for the case with $r + 1$ vectors in r dimensions.

Constructing a Given g-set

The reverse problem: can we make a set of numbers the Frobenius vectors? If so, with how many vectors?

In $1 - D$,

1. With 2 numbers we can get $ab - a - b$, which must be odd.

2. With 3 numbers we can get any number.

General Case

Lemma 2. *Given a legal simple cone* C *and a set of* h *vectors* $G = \{\mathbf{g_1}, \ldots, \mathbf{g_h}\} \subset RH$*, there exists some set of vectors* V *with cone* C *such that* $G \subset g(V)$ *if:*

1. *Knowing that* g_i *has* RH*-coordinates* $< g_{i1}, \ldots, g_{ir} >$*, we have* $g_{ij} \geq -1$ *for all* (i, j)*;*

2. *for all* i *and a bounding hyperplane* H *of* g_i*,*

$$(0, \ldots, 0) \cup (\bigcup_{j \neq i} intcone(\mathbf{g_j})) \not\supset (S_L \cap H \cap cone(g_i);$$

Unique g-vectors in the Positive Orthant

Theorem 14. *Let* $\mathbf{a} = (a_1, \ldots, a_r) \in \mathbf{Z}^r$*. There exists a vector set* V *of* $r+1$ *vectors with a simple cone and* $g(V) = \{\mathbf{a}\}$ *if and only if* $a_i \equiv 1 \pmod 2$ *for some* i*.*

When $r + 2$ do not suffice

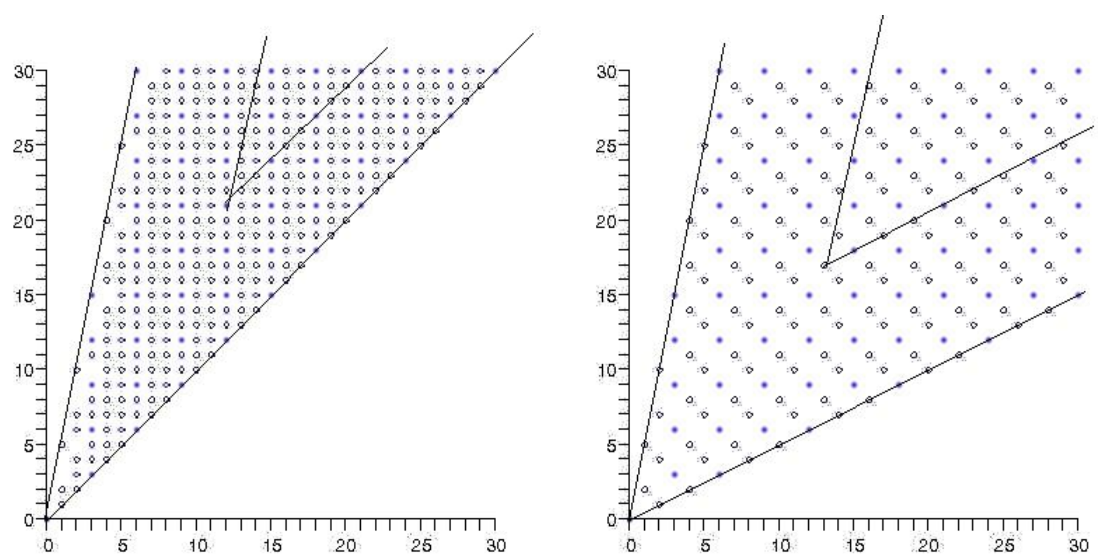
We have two weird theorems:

Theorem 15. *Let* $g = (g_1, \ldots, g_r)$*,* $g_i \in \mathbf{Z}$*. If* k *does not divide some* g_i*, then there exists* $r + k$ *vectors forming* V *such that* $g(V) = \{g\}$*.*

Theorem 16. *Let* $g = (g_1, \ldots, g_r)$*,* $g_i \in \mathbf{Z}$*. There exists at most* 3r *vectors forming* V *such that* $g(V) = \{g\}$*.*

When gcd **is not** 1

As a natural generalization of our problem, it makes sense to consider the cases when gcd(V) $\neq$ 1.



We define $G(V)$, the *generalized g-set* as

$$\{\text{min}(a \in gcd(V)RH | (intcone(a) \cap S_{\mathbf{Z}}(V)) \subset S(V))\},$$

whatever.

$$\{\text{min}(a \in RH | (intcone(a) \cap S_L) \subset S(V)\},$$

seems similar.

Furthermore, it is clear that when $gcd(V) = 1$, $g(V) = G(V)$.
Theorem 17. *Suppose that $V = DV'$, where $|D| = gcd(V)$. Then $G(V) = Dg(V')$.*

Corollary 1. *Suppose* $r = 1$, $V = \{a_1, \ldots, a_n\}$, *and* $\gcd(V) = k$. *Then* $G(V) = \{k \times frob(V')\}$, *where* $V' = \{a_1/k, \ldots, a_n/k\}$.

For example, when $V = \{10, 14\}$, $S_{\mathbf{Z}}(V) = \{2a, a \in \mathbf{Z}\}$. $frob(V) = 26$.

Future Directions

- bounding size of $g(V)$
- bounding cardinality of $g(V)$
- making a vector the unique g-vector with as few vectors as possible
- $gcd \neq 1$ case
- use general machinery to attack 1-dimensional case

Acknowledgments

- Professor Vadim Ponomarenko, our mentor
- Professor Scott Chapman, for leading the Trinity REU program
- NSF, for giving us money