Polytopes, lattice points, and a problem of Frobenius

Matthias Beck

SUNY Binghamton

Sinai Robins

Temple University

www.math.binghamton.edu/matthias

"If you think it's simple, then you have misunderstood the problem"

Bjarne Strustrup
(lecture at Temple University, 11/25/97)

Frobenius problem: Given relatively prime positive integers $a_1, \ldots, a_d$, we call an integer n representable if there exist nonnegative integers $m_1, \ldots, m_d$ such that

$$n = m_1 a_1 + \cdots + m_d a_d \, .$$

Find the largest integer (the Frobenius number $g(a_1, \ldots, a_d)$) which is not representable.

Consider the partition function

$$p_{\{a_1,\ldots,a_d\}}(n) := \# \left\{ \begin{array}{l} (m_1, \ldots, m_d) \in \mathbb{Z}^d_{\geq 0} \ : \\ m_1 a_1 + \cdots + m_d a_d = n \end{array} \right\}$$

Frobenius problem: find the largest value for n such that $p_{\{a_1,\ldots,a_d\}}(n) = 0$. Geometrically, this partition function enumerates integer ("lattice") points on the n-dilate of the polytope

$$\left\{ \begin{array}{r} (x_1, \ldots, x_d) \in \mathbb{R}^d : \qquad\qquad\qquad\qquad \\ x_j \geq 0, x_1 a_1 + \cdots + x_d a_d = 1 \end{array} \right\} .$$

Some known results:

- (Sylvester, 1884)

$$g(a_1, a_2) = a_1 a_2 - a_1 - a_2$$

- (Erdös, 1940's, ...)

$$p_{\{a_1,\ldots,a_d\}}(n) = \frac{n^{d-1}}{a_1 \cdots a_d (d-1)!} + O\left(n^{d-2}\right)$$

- (Stanley, Wilf, 1970's)

$$p_{\{a_1,a_2\}}(n) = \frac{n}{a_1 a_2} + f(n)$$

where $f(n)$ is periodic in n with period $a_1 a_2$.

Theorem (Tripathi, B-R)

$$p_{\{a_1,a_2\}}(n) = \frac{n}{a_1 a_2} - \left\{\frac{a_2^{-1} n}{a_1}\right\} - \left\{\frac{a_1^{-1} n}{a_2}\right\} + 1 \, .$$

Here $\{x\} = x - \lfloor x \rfloor$ denotes the fractional part of x ,

$$a_1^{-1} a_1 \equiv 1 \pmod{a_2} \, ,$$

and

$$a_2^{-1} a_2 \equiv 1 \pmod{a_1} \, .$$

"The proof is left as an exercise."

Corollary (Sylvester) $g(a,b) = ab - a - b$

Proof.

$$p_{\{a,b\}}(ab-a-b+n) = \frac{ab-a-b+n}{ab}$$

$$-\left\{\frac{b^{-1}(ab-a-b+n)}{a}\right\} - \left\{\frac{a^{-1}(ab-a-b+n)}{b}\right\} + 1$$

$$= 2 - \frac{1}{b} - \frac{1}{a} + \frac{n}{ab} - \left\{\frac{-1+n}{a}\right\} - \left\{\frac{-1+n}{b}\right\}$$

If $n = 0$ use $\left\{\frac{-1}{a}\right\} = 1 - \frac{1}{a}$ to obtain

$$p_{\{a,b\}}(ab-a-b) =$$

$$2 - \frac{1}{b} - \frac{1}{a} - \left(1 - \frac{1}{a}\right) - \left(1 - \frac{1}{b}\right) = 0\ .$$

If $n > 0$ note that $\left\{\frac{m}{a}\right\} \le 1 - \frac{1}{a}$ and hence

$$p_{\{a,b\}}(ab-a-b+n) \ge$$

$$2 - \frac{1}{b} - \frac{1}{a} + \frac{n}{ab} - \left(1 - \frac{1}{a}\right) - \left(1 - \frac{1}{b}\right) = \frac{n}{ab} > 0\ .$$

Corollary (Sylvester) Exactly half of the integers between 1 and $(a-1)(b-1)$ are representable.

Proof. If $n \in [1, ab-1]$ is not a multiple of a or b then

$$p_{\{a,b\}}(ab-n) = \frac{ab-n}{ab} - \left\{\frac{b^{-1}(ab-n)}{a}\right\}$$

$$- \left\{\frac{a^{-1}(ab-n)}{b}\right\} + 1$$

$$= 2 - \frac{n}{ab} - \left\{\frac{-b^{-1}n}{a}\right\} - \left\{\frac{-a^{-1}n}{b}\right\}$$

$$\overset{(\star)}{=} -\frac{n}{ab} + \left\{\frac{b^{-1}n}{a}\right\} + \left\{\frac{a^{-1}n}{b}\right\}$$

$$= 1 - p_{\{a,b\}}(n) \ .$$

$(\star)$ follows from $\{-x\} = 1 - \{x\}$ if $x \notin \mathbb{Z}$. Hence for n between 1 and $ab-1$ and not divisible by a or b , exactly one of n and $ab-n$ is not representable. There are

$$ab - a - b + 1 = (a-1)(b-1)$$

such integers.

Extension: we call an integer n k-representable if $p_{\{a_1,\ldots,a_d\}}(n) = k$, that is, n can be represented in exactly k ways. Define $g_k(a_1, \ldots, a_d)$ to be the largest k-representable integer.

Theorem (B-R) $g_k(a, b) = (k+1)ab - a - b$

This follows directly from

Lemma $p_{\{a,b\}}(n + ab) = p_{\{a,b\}}(n) + 1$

Proof.

$$p_{\{a,b\}}(n + ab) = \frac{n+ab}{ab} - \left\{ \frac{b^{-1}(n+ab)}{a} \right\} - \left\{ \frac{a^{-1}(n+ab)}{b} \right\} + 1$$

$$= \frac{n}{ab} + 2 - \left\{ \frac{b^{-1}n}{a} \right\} - \left\{ \frac{a^{-1}n}{b} \right\}$$

$$= p_{\{a,b\}}(n) + 1$$

More exercises:

- Given $k \geq 2$, the smallest k-representable integer is $ab(k-1)$.
- Given $k \geq 2$, the smallest interval containing all k-representable integers is

$$[\ g_{k-2}(a,b) + a + b\ ,\ \ g_k(a,b)\ ]\ .$$

- There are $ab - 1$ uniquely representable integers. Given $k \geq 2$, there are exactly ab k-representable integers.
- Extend all of this to $d > 2$.