On the Frobenius Coin Problem

Bogdan Grechuk • 22 May 2026

This post continues my series on favorite theorems of the 21st century, choosing one theorem for each year and for each of the seven major subject categories. For an overview of the categories and of my previous selections, see this earlier post. My choice for 2002 in *Algorithms and Complexity* is the theorem of Barvinok and Woods giving an efficient algorithm, for every fixed number of coin denominations, to compute the total number of unattainable amounts in the Frobenius coin problem. The theorem was proved in 2002 and published in 2003 (Barvinok and Woods 2003).

Given positive coprime integers $a_1, a_2, \dots, a_n$, let

$$S(a_1, a_2, \dots, a_n) = \left\{ m \in \mathbb{Z}_{>0} : m \neq \sum_{i=1}^{n} m_i a_i \text{ for all } m_i \in \mathbb{Z}_{\geq 0} \right\}.$$

Thus $S(a_1, a_2, \dots, a_n)$ is the set of positive integers that cannot be paid using coins of denominations $a_1, \dots, a_n$, when any non-negative number of coins of each denomination is allowed. The assumption that the a_i are coprime is essential: it guarantees that all sufficiently large positive integers are representable, and hence that the set $S(a_1, a_2, \dots, a_n)$ is finite.

The classical *Frobenius coin problem* asks for the largest element of this finite set. For $n = 2$ there is the famous closed formula

$$\max S(a_1, a_2) = a_1 a_2 - a_1 - a_2,$$

but for larger n the problem becomes much subtler. If n is allowed to vary as part of the input, the Frobenius problem is computationally hard; in particular, it is known to be NP-hard. On the other hand, Kannan (Kannan 1992) proved in 1992 that for every fixed n the Frobenius number $\max S(a_1, a_2, \dots, a_n)$ can be computed in polynomial time. This is a typical and beautiful phenomenon in the geometry of numbers and integer programming: a problem may be intractable in variable dimension but become efficiently solvable once the dimension is fixed.

Barvinok and Woods pushed this point of view further. Instead of asking only for the largest exceptional integer, they asked for the total number of exceptional integers. In other words, they considered the size

$$\left| S(a_1, a_2, \dots, a_n) \right|.$$

This quantity is sometimes called the *genus* of the numerical semigroup generated by $a_1, \ldots, a_n$. It measures the full extent of the failure of representability, not just the final failure before all larger integers become attainable.

Theorem 1 *For every fixed n, there is an algorithm which, given positive coprime integers $a_1, a_2, \ldots, a_n$, computes*

$$\left|S(a_1, a_2, \ldots, a_n)\right|$$

in time polynomial in the input size.

The striking feature of Theorem 1 is not only that the answer can be computed efficiently, but also the method by which it is computed. The proof is based on the theory of short rational generating functions, a technique developed by Barvinok for counting lattice points in polyhedra of fixed dimension. Rather than listing the elements of a set one by one, the method encodes the set as a compact rational function.

For a finite set T of positive integers, define its generating function by

$$f(T, x) = \sum_{m \in T} x^m.$$

If we could explicitly list all elements of $S(a_1, \ldots, a_n)$, then the polynomial

$$f(S(a_1, \ldots, a_n), x) = \sum_{m \in S(a_1, \ldots, a_n)} x^m$$

would immediately give the desired number, since

$$\left|S(a_1, \ldots, a_n)\right| = f(S(a_1, \ldots, a_n), 1).$$

The difficulty is that the set $S(a_1, \ldots, a_n)$ may be very large, so writing down this polynomial term by term may be hopelessly inefficient.

The key insight of Barvinok and Woods is that, when n is fixed, one can compute a *short* expression for the relevant generating function. Such an expression is typically a sum of rational functions of the form

$$\frac{x^u}{(1 - x^{v_1})(1 - x^{v_2}) \cdots (1 - x^{v_k})},$$

where the number of summands and the size of the data appearing in them are polynomially bounded. This compact representation can encode an enormous finite or infinite set without enumerating its elements.

The representable positive integers are generated by the semigroup

$$\left\{ \sum_{i=1}^{n} m_i a_i : m_i \in \mathbb{Z}_{\geq 0} \right\}.$$

The formal generating function of this semigroup is closely related to

$$\frac{1}{(1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_n})},$$

although this expression counts representations rather than represented integers, since the same integer may have many different representations. The work of Barvinok and Woods supplies the algorithmic machinery needed to pass from such representation-counting data to a short generating function for the actual set of attainable integers, and hence also for its finite complement among the positive integers.

If $\overline{S}$ denotes the set of positive representable integers, then

$$f(S,x) + f(\overline{S},x) = \frac{x}{1-x},$$

because every positive integer is either unattainable or attainable. Thus a short rational expression for one of these two generating functions gives a short rational expression for the other. Since S is finite, its generating function is regular at $x = 1$, and the desired number is obtained by taking the limit

$$\bigl|S(a_1,\ldots,a_n)\bigr| = \lim_{x\to 1} f(S(a_1,\ldots,a_n),x).$$

Although the rational expression may have apparent poles at $x = 1$, these singularities cancel, and the limit can be evaluated efficiently.

What makes this theorem especially elegant is the way it transforms a problem about coins into a problem about the geometry and algebra of generating functions. The unattainable integers are not found by a direct search through a long interval, nor by computing the Frobenius number first and checking every smaller integer. Instead, the whole exceptional set is compressed into a symbolic object of polynomial size, and the answer is extracted from that object analytically.

References

Barvinok, Alexander, and Kevin Woods. 2003. “Short Rational Generating Functions for Lattice Point Problems.” *J. Amer. Math. Soc.* 16 (4): 957–79.

Kannan, Ravi. 1992. “Lattice Translates of a Polytope and the Frobenius Problem.” *Combinatorica* 12 (2): 161–77.