The Frobenius Coin Problem
Upper Bounds on The Frobenius Number

Jean Gallier

April 14, 2014

1 The Frobenius Coin Problem

In its simplest form, the coin problem is this: what is the largest positive amount of money that cannot be obtained using two coins of specified distinct denominations? For example, using coins of 2 units and 3 units, it is easy so see that every amount greater than or equal to 2 can be obtained, but 1 cannot be obtained. Using coins of 2 units and 5 units, every amount greater than or equal to 4 units can be obtained, but 1 or 3 units cannot, so the largest unobtainable amount is 3. What about using coins of 7 and 10 units? We need to figure out which positive integers n are of the form

$$n = 7h + 10k, \quad \text{with} \quad h, k \in \mathbb{N}.$$

It turns out that every amount greater than or equal to 54 can be obtained, and 53 is the largest amount that cannot be achieved.

In general, we have $k \geq 2$ coins $p_1, \ldots, p_k$ such that $2 \leq p_1 < p_2 < \cdots < p_k$ and $\gcd(p_1, \ldots, p_k) = 1$. The problem is to figure out which natural numbers n can be expressed as linear combinations of $p_1, \ldots, p_k$ with nonnegative integer coefficients, that is,

$$n = i_1 p_1 + \cdots + i_k p_k,$$

with $i_1, \ldots, i_k \in \mathbb{N}$. Note that if we allow the i_j to be negative integers, then by Bézout, *every* integer $n \in \mathbb{Z}$ is representable in the above form. The restriction to nonnegative coefficients i_j makes the problem a lot more challenging.

In the case of two coins p, q (with $2 \leq p < q$ and $\gcd(p, q) = 1$), it can be shown that every integer $n \geq (p-1)(q-1)$ is representable with nonnegative coefficients, and that $pq - p - q = (p-1)(q-1) - 1$ is the largest integer that can't be represented with nonnegative coefficients.

The number $pq - p - q$, usually denoted by $g(p, q)$, is known as the *Frobenius number* of the set $\{p, q\}$, after Ferdinand Frobenius (1849–1917) who first investigated this problem,

Figure 1: Ferdinand Georg Frobenius, 1849–1917

and the fact that $pq - p - q$ is the largest integer that is not representable was proved by James Sylvester in 1884.

If $k \geq 3$, it is still true that there is some positive integer N such that every integer $n \geq N$ is representable as a linear combination of $p_1, \ldots, p_k$ with nonnegative coefficients, and thus, there is a largest positive integer $g(p_1, \ldots, p_k)$ which is not representable. This number is also called the *Frobenius number* of $\{p_1, \ldots, p_k\}$. However, for $k \geq 3$ coins, no explicit formula for $g(p_1, \ldots, p_k)$ is known! Various upper bounds (and lower bounds) for $g(p_1, \ldots, p_k)$ are known, and we will present a bound due to I. Schur in the next section.

It is remarkable that such a seemingly mundane problem has caught the attention of famous mathematicians, such as Sylvester, Schur, Erdös, Graham, just to name a few. There is even an entire book devoted to the problem: *The Diophantine Frobenius Problem*, by Jorge L. Ramirez Alfonsin, Oxford University Press, 2005.

As amusing version of the problem is the *McNuggets number* problem. McDonald's sells boxes of chicken McNuggets in boxes of $6, 9$ and 20 nuggets. What is the largest number of chicken McNuggets that can't be purchased? It turns out to be 43 nuggets!

2 Upper Bounds on the Frobenius Coin Problem

We begin with the following proposition that provides an upper bound for the Frobenius number. This bound can be improved when $k \geq 3$, but it has the advantage that the proof that it works is easy.

Proposition 2.1. *Let* $p_1, \ldots, p_k$ *be* $k \geq 2$ *integers such that* $2 \leq p_1 < p_2 < \cdots < p_k$, *with* $\gcd(p_1, \ldots, p_k) = 1$. *Then, for all* $n \geq (p_1 - 1)(p_2 + \cdots + p_k - 1)$, *there exist* $i_1, \ldots, i_k \in \mathbb{N}$ *such that*

$$n = i_1 p_1 + \cdots + i_k p_k.$$

Proof. Since $\gcd(p_1, \ldots, p_k) = 1$, by Bézout, for any integer $n \in \mathbb{Z}$, there are some integers $h_1, \ldots, h_k \in \mathbb{Z}$ such that

$$n = h_1 p_1 + \cdots + h_k p_k. \tag{$*$}$$

If we divide h_j by p_1 for $j = 2, \ldots, k$, we obtain

$$h_j = p_1 a_j + r_j, \quad 0 \leq r_j \leq p_1 - 1 \text{ for } j = 2, \ldots, k,$$

so by substituting into $(*)$, we can write

$$n = (h_1 + a_2 h_2 + \cdots + a_k h_k) p_1 + r_2 p_2 + \cdots + r_k p_k, \quad 0 \leq r_j \leq p_1 - 1 \text{ for } j = 2, \ldots, k.$$

Thus, we proved that every $n \in \mathbb{Z}$ can be written as

$$n = i_1 p_1 + i_2 p_2 + \cdots + i_k p_k,$$

for some $i_1 \in \mathbb{Z}$ and some $i_2, \ldots, i_k$ such that $0 \leq i_j \leq p_1 - 1$ for $j = 2, \ldots, k$. Let S be the set given by

$$S = \{n \in \mathbb{Z} \mid n = i_1 p_1 + i_2 p_2 + \cdots + i_k p_k,\ i_1 < 0,\ 0 \leq i_j \leq p_1 - 1 \text{ for } j = 2, \ldots, k\}.$$

Observe that this set S is bounded from above, and in fact its maximum element is

$$-p_1 + (p_1 - 1)(p_2 + \cdots + p_k).$$

Since every integer n is representable, it follows that all natural numbers in $\mathbb{Z} - S$ are representable with $i_1 \geq 0$, and since the smallest number in $\mathbb{Z} - S$ is

$$-p_1 + (p_1 - 1)(p_2 + \cdots + p_k) + 1 = (p_1 - 1)(p_2 + \cdots + p_k - 1),$$

we have proved that every natural number $n \geq (p_1 - 1)(p_2 + \cdots + p_k - 1)$ is representable with all i_j nonnegative, as desired. □

When $k = 2$, the lower bound is $(p_1 - 1)(p_2 - 1)$, and it is sharp since when $k = 2$, every integer n has a *unique* representation as

$$n = x p_1 + y p_2, \quad 0 \leq x \leq p_2 - 1.$$

This is because if

$$n = x_1 p_1 + y_1 p_2 = x_2 p_1 + y_2 p_2$$

with $0 \leq x_1, x_2 \leq p_2 - 1$, assuming $x_1 \leq x_2$ (the case $x_2 \leq x_1$ being similar), we have

$$(y_1 - y_2) p_2 = (x_2 - x_1) p_1,$$

so p_2 divides $(x_2 - x_1) p_1$, and since $\gcd(p_1, p_2) = 1$, p_2 must divide $x_2 - x_1$, which implies $x_1 = x_2$, since $0 \leq x_2 - x_1 < p_2$. Therefore, when $k = 2$, the largest natural number not expressible as a linear combination with nonnegative coefficients is

$$p_1 p_2 - p_1 - p_2 = (p_1 - 1)(p_2 - 1) - 1.$$

This was proved by James Sylvester in 1884. Sylvester also proved that the number of representable integers and the number of nonrepresentable integers is the same and equal to

$$\frac{(p_1-1)(p_2-1)}{2}.$$

This is easy to prove using the unique repesentability of numbers $n \geq (p_1-1)(p_2-1)$ in the form

$$n = xp_1 + yp_2, \quad 0 \leq x \leq p_2 - 1.$$

Indeed, if n is expressed as above, consider

$$\begin{aligned} n' &= (p_1-1)(p_2-1) - 1 - n \\ &= p_1p_2 - p_1 - p_2 - xp_1 - yp_2 \\ &= (p_2 - 1 - x)p_1 + (-1-y)p_2. \end{aligned}$$

Since $0 \leq x \leq p_2 - 1$, we have $0 \leq p_2 - 1 - x \leq p_2 - 1$. It follows that if $y \geq 0$, then n is representable and n' is not, while if $y < 0$, then n is not representable but n' is. Therefore, exactly half of the numbers $0, 1, \ldots, (p_1p_2 - p_1 - p_2)/2$ are not representable.

In contrast to the case $k = 2$, if $k \geq 3$ the number $(p_1-1)(p_2 + \cdots + p_k - 1)$ is not optimal. I. Schur proved that every integer $n \geq (p_1-1)(p_k-1)$ is expressible as a linear combination of the p_js with nonegative integer coefficients, but the number $(p_1-1)(p_k-1)$ is not the smallest one that works.

We now prove that Proposition 2.1 also holds with $(p_1-1)(p_k-1)$ instead of $(p_1-1)(p_2 + \cdots + p_k - 1)$. This result was proved by I. Schur in 1935, but not published until 1942 by Alfred Brauer. We present a minor adaptation of Brauer's proof.

Assume $k \geq 3$. The proof proceeds by induction. The key observation is that if n is expressible as a linear combination

$$n = i_1p_1 + i_2p_2 + \cdots + i_kp_k,$$

and if we let $d = \gcd(p_1, p_3, \ldots, p_k)$ (omitting p_2), then

$$n - i_2p_2 = i_1p_1 + i_3p_3 + \cdots + i_kp_k$$

is divisible by d. If we can make a suitable guess for i_2, then we are reduced to the following problem involving $k-1$ integers: find natural numbers $i_1, i_3, \ldots, i_k$ such that

$$\frac{n - i_2p_2}{d} = i_1\frac{p_1}{d} + i_3\frac{p_3}{d} + \cdots + i_k\frac{p_k}{d},$$

with

$$\gcd\left(\frac{p_1}{d}, \frac{p_3}{d}, \ldots, \frac{p_k}{d}\right) = 1.$$

We may assume that $d > 1$, since otherwise we set $i_2 = 0$ and the problem is immediately solved by induction.

Since $\gcd(p_1, p_2, p_3, \ldots, p_k) = 1$ and $\gcd(p_1, p_3, \ldots, p_k) = d$, we have $\gcd(p_2, d) = 1$, so the congruence

$$p_2 x \equiv n \pmod{d}$$

is solvable in x, and we may assume that $0 \leq x \leq d - 1$. Then, we proceed by induction, which involves checking that the bound works out.

Proposition 2.2. *Let $p_1, \ldots, p_k$ be $k \geq 2$ integers such that $2 \leq p_1 \leq p_2 \leq \cdots \leq p_k$, with $\gcd(p_1, \ldots, p_k) = 1$. Then, for all $n \geq (p_1 - 1)(p_k - 1)$, there exist $i_1, \ldots, i_k \in \mathbb{N}$ such that*

$$n = i_1 p_1 + \cdots + i_k p_k.$$

Proof. We proceed by induction on k. For $k = 2$, since $\gcd(p_1, p_2) = 1$ and $p_1 \geq 2$, we must have $p_2 > p_1$, and this case has been shown in Proposition 2.1. If $k \geq 3$, let $d = \gcd(p_1, p_3, \ldots, p_k)$ (omitting p_2). We may assume that $d > 1$, since otherwise we set $i_2 = 0$ and the problem is immediately solved by induction. Since $\gcd(p_1, p_2, p_3, \ldots, p_k) = 1$ and $\gcd(p_1, p_3, \ldots, p_k) = d$, we have $\gcd(p_2, d) = 1$, so the congruence

$$p_2 x \equiv n \pmod{d}$$

is solvable in x, and we may assume that we pick the solution i_2 so that $0 \leq i_2 \leq d - 1$. Since $n - i_2 p_2$ is divisible by d and since $d = \gcd(p_1, p_3, \ldots, p_k)$, we obtain the equation

$$\frac{n - i_2 p_2}{d} = i_1 \frac{p_1}{d} + i_3 \frac{p_3}{d} + \cdots + i_k \frac{p_k}{d},$$

and we attempt to solve it in natural numbers $i_1, i_3, \ldots, i_k$. Since

$$\gcd\left(\frac{p_1}{d}, \frac{p_3}{d}, \ldots, \frac{p_k}{d}\right) = 1,$$

by the induction hypothesis, if

$$\frac{n - i_2 p_2}{d} \geq \left(\frac{p_1}{d} - 1\right)\left(\frac{p_k}{d} - 1\right),$$

or equivalently if

$$n \geq i_2 p_2 + \left(\frac{p_1}{d} - 1\right)(p_k - d), \quad 0 \leq i_2 \leq d - 1,$$

our equation is indeed solvable. To complete the proof, it remains to prove that

$$(p_1 - 1)(p_k - 1) \geq i_2 p_2 + \left(\frac{p_1}{d} - 1\right)(p_k - d),$$

with $0 \leq i_2 \leq d - 1$. If we can prove that

$$(p_1 - 1)(p_k - 1) \geq (d - 1) p_2 + \left(\frac{p_1}{d} - 1\right)(p_k - d),$$

we are done. This amounts to proving that

$$p_1p_k - p_1 - p_k + 1 \geq (d-1)p_2 + \frac{p_1p_k}{d} - p_1 - p_k + d,$$

that is,

$$\left(1 - \frac{1}{d}\right) p_1p_k \geq (d-1)(p_2+1),$$

which is equivalent to

$$p_1p_k \geq d(p_2+1),$$

since $d \geq 2$. Now, since $p_1 \leq p_2 \leq \cdots \leq p_k$, we must have $p_k \geq p_2 + 1$, because otherwise $p_k = p_2$, but then $p_2 = p_3 = \cdots = p_k$, so $d = \gcd(p_1, p_3, \ldots, p_k) = \gcd(p_1, p_2)$, and since $\gcd(p_2, d) = 1$, we must have $d = 1$, contrary to our hypothesis. Since d divides p_1,

$$p_1p_k \geq d(p_2+1)$$

holds, as desired. □

The number $(p_1 - 1)(p_k - 1)$ is generally far from optimal, For example, for $p_1 = 6, p_2 = 10, p_3 = 15$, we have $(p_1 - 1)(p_2 - 1) = 70$, but it can be checked that every integer $n \geq 30$ is representable with nonnegative integers.

We close this section by stating some bounds that generally improve upon Schur's bound. Erdös and Graham (1972) prove that

$$g(p_1, \ldots, p_k) \leq 2p_{k-1} \left\lfloor \frac{p_k}{k} \right\rfloor - p_k,$$

and Selmer (1977) proves that

$$g(p_1, \ldots, p_k) \leq 2p_k \left\lfloor \frac{p_1}{k} \right\rfloor - p_1.$$

M. Lewin (1972) proves that for $k \geq 3$,

$$g(p_1, \ldots, p_k) \leq \left\lfloor \frac{(p_k - 2)^2}{2} \right\rfloor - 1.$$

Lewin also proves that for $k = 3$, this is the best possible bound, because equality can be attained for some triples (p_1, p_2, p_3).

In our example, $p_1 = 6, p_2 = 10, p_3 = 15$, Selmer's bound is equal to 54, which is better than Schur's bound (69), Erdös and Graham's bound is 85, which is worse, and Lewin's bound is 83 (also worse than Selmer's bound).