Second Proof: Every Positive Integer is a Frobenius Number of Three Generators

Firuz Kamalov
Mathematics Department
Canadian University of Dubai
Dubai, UAE

Ho-Hon Leung
Mathematics Department
Canadian University of Dubai
Dubai, UAE

Copyright © 2015 Firuz Kamalov and Ho-Hon Leung. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract
Let \( n \) be any positive integer. We give a simple proof to the theorem that there always exist positive integers \( a, b \) and \( c \) such that the Frobenius number generated by \( a, b, c \) is equal to \( n \).

Mathematics Subject Classification: 13A99, 22A20, 41A63

Keywords: Frobenius number

1 Introduction
Let \( n_1, n_2, ..., n_k \) be positive integers such that \( \gcd(n_1, n_2, ..., n_k) = 1 \). Let \( S := S(n_1, n_2, ..., n_k) \) be the following set of integers:

\[
S(n_1, n_2, ..., n_k) = \{ n \mid n = x_1n_1 + x_2n_2 + ... + x_kn_k, x_1, x_2, ..., x_k \in \mathbb{Z}_{\geq 0} \}.
\]
It is well-known that the set \( \mathbb{Z}_\geq 0 - S \) is finite. The Frobenius number, \( F(n_1, n_2, \ldots, n_k) \), is defined as the largest integer in \( \mathbb{Z}_\geq 0 - S \). The Conductor, \( N(n_1, n_2, \ldots, n_k) \), is the smallest integer in \( S \) such that all integers greater than it belong to \( S \).

It is clear that 
\[
N(n_1, \ldots, n_k) = F(n_1, \ldots, n_k) + 1.
\]

For \( k = 2 \), Sylvester proved in [6] that 
\[
F(n_1, n_2) = n_1 n_2 - n_1 - n_2.
\]

Equivalently, \( N(n_1, n_2) = (n_1 - 1)(n_2 - 1) \). For \( k = 3 \), Curtis showed in [3] that there is no closed formula for \( F(n_1, n_2, n_3) \). Nevertheless, it would be interesting to determine properties of the Frobenius number of three generators. In particular, the authors proved in [5] that \( F(n_1, n_2, n_3) \) is surjective, i.e. there exist positive integers \( a, b, c \) such that \( F(a, b, c) = n \) for every nonnegative integer \( n \).

In [2], Arnold provided a geometrical method to find the Conductors of three generators. The same method can be easily extended to find the Conductors of more than three generators, see [1]. In this paper, we give a simple geometric proof (in the sense of Arnold) that every positive integer greater than 1 can be represented as the Conductor \( N(a, b, c) \) for some positive integers \( a, b, c \). This result can be taken as an alternative proof that the Frobenius number \( F(a, b, c) \) is a surjection onto the set of nonnegative integers since \( N(a, b, c) \) is always one greater than \( F(a, b, c) \).

### 2 Main Results

#### 2.1 Arnold’s domain \( D_a(b, c) \)

Let \( a, b, c \) be positive integers such that \( \gcd(a, b, c) = 1 \). In the first quadrant \( \{y \geq 0, z \geq 0\} \), for each \( \alpha = 0, 1, \ldots, a - 1 \), define the valuation function 
\[
l_a(y, z) := yb + zc
\]
and define \( I_\alpha \) be the set of points 
\[
I_\alpha := \{(y, z) \mid l_a(y, z) = \alpha \mod a\}.
\]

Let \( M_\alpha \subset I_\alpha \) be the set of points such that \( l_a(y, z) \) is minimal. The Arnold’s domain \( D_a := D_a(b, c) \) is the union of the sets \( M_\alpha \) over all \( \alpha = 0, 1, \ldots, a - 1 \). \( D_b \) and \( D_c \) can be defined similarly.

Let \( L_a := L_a(b, c) = \max \{l_a(y, z) \mid (y, z) \in D_a(b, c)\} \). In [2], it is shown that the Conductor \( N(a, b, c) \) can be computed as follows:
\[
N(a, b, c) = L_a - a + 1.
\]

It is also shown that the domains \( D_a, D_b \) and \( D_c \) have the form of Young diagrams: The boundary of \( D_a \) in the \( yz \)-plane consists of a base segment along the \( y \)-axis, a vertical segment along the \( z \)-axis and a staircase line.
Example 2.1 For the domain $D_5(19,22)$, it is shown in the following Fig.1 as the region bounded by the bold line. The bold number in the position $(1,1)$ in the $(y,z)$-plane corresponds to $L_5(19,22) = (1)(19) + (1)(22) = 41$. Hence, by (1), $N(5,19,22) = 41 - 5 + 1 = 37$.

2.2 Main proofs

In Lemma 2.2, Lemma 2.3 and Lemma 2.4, we deal with the cases for $n$ modulo 2, 3 and 4 respectively.

Lemma 2.2 If $n$ is an even number, then there exist $a,b,c$ such that $N(a,b,c) = n$.

Proof. If $a = b$, then $N(a,a,c) = N(a,c) = (a - 1)(c - 1)$ by Sylvester’s formula in [6]. Let $n = 2k$ where $k$ is any positive integer. Set $a = b = 2$ and $c = 2k + 1$, then we get $N(2,2,2k+1) = n$ by (1).

Lemma 2.3 If $n > 1$ and $n \not\equiv 1 \mod 3$, then there exist $a,b,c$ such that $N(a,b,c) = n$.

Proof. If $n = 2$, then it is done by Lemma 2.2. If $n = 3k + 2$ where $k$ is any positive integer, then set $a = 3$, $b = 3k + 2$ and $c = 3k + 4$. The domain $D_3(3k + 2,3k + 4)$ is shown in Fig. 2. $L_3(3k + 2,3k + 4) = c = 3k + 4$ and hence by (1), $N(3,3k + 2,3k + 4) = (3k + 4) - 3 + 1 = n$. 
If \( n = 3k \) where \( k \) is any positive integer, then set \( a = 3, b = 3k + 1 \) and \( c = 3k + 2 \). The domain \( D_3(3k+1, 3k+2) \) is shown in Fig. 3. \( L_3(3k+1, 3k+2) = c = 3k + 2 \) and hence by (1), \( N(3, 3k+1, 3k+2) = (3k+2) - 3 + 1 = n \). Hence the result.

**Figure 2:** The domain \( D_3(3k+2, 3k+4) \).

\[
\begin{array}{cccc}
0 & 2 & 1 & 0 \\
2 & 1 & 0 & 2 \\
1 & 0 & 2 & 1 \\
0 & 2 & 1 & 0 \\
\end{array}
\]

**Figure 3:** The domain \( D_3(3k+1, 3k+2) \).

\[
\begin{array}{cccc}
0 & 1 & 2 & 0 \\
1 & 2 & 0 & 1 \\
2 & 0 & 1 & 2 \\
0 & 1 & 2 & 0 \\
\end{array}
\]

**Lemma 2.4** If \( n > 1 \) and \( n \neq 1 \mod 4 \), then there exist \( a, b, c \) such that \( N(a, b, c) = n \).

**Proof.** The cases when \( n = 0 \) or \( 2 \mod 4 \) are done by Lemma 2.2.

Let \( n = 4k + 3 \) where \( k \) is any positive integer. Set \( a = 4 \) and \( b = 2k + 3 \). Let \( c \) be an integer such that \( b + c = 0 \mod 4 \) and \( 2b > c > b \). The domain \( D_4(b, c) \) is shown in Fig. 4 for the case \( b = 1 \mod 4 \) and \( c = 3 \mod 4 \). (The domain for the case \( b = 3 \mod 4 \) and \( c = 1 \mod 4 \) is very similar.) Since \( 2b > c \), \( L_4(b, c) = 2b = 2(2k + 3) = 4k + 6 \). By (1), \( N(4, b, c) = (4k + 6) - 4 + 1 = 4k + 3 = n \). Hence the result.

A combination of Lemma 2.2, Lemma 2.3 and Lemma 2.4 gives us the following corollary:
Every positive integer is a Frobenius number ...

Corollary 2.5 If \( n > 1 \) and \( n \neq 1 \mod 12 \), then there exist \( a, b, c \) such that \( N(a, b, c) = n \).

The following lemma will be used inductively in the proof of Theorem 2.8.

Lemma 2.6 Let \( p \) be a prime. If \( n > p(p-1)(p-2) \) and \( n \neq 1 \mod p \), then there exist \( b, c \) such that \( N(p, b, c) = n \).

Proof. For such \( n \), set \( c = n + (p - 1) \). It immediately implies that \( c > (p - 1)^3 \) and \( c \neq 0 \mod p \).

We need to choose \( b \) such that \( b + c = 0 \mod p \) and \( (p - 2)b < c < (p - 1)b \). There always exist \( b \) satisfying these two conditions if the following inequality holds:

\[
\frac{c}{p - 2} - \frac{c}{p - 1} > p.
\]

It is equivalent to \( c > p(p - 1)(p - 2) \). It must hold as we fix \( c \) such that \( c > (p - 1)^3 \).

For such a pair of \( b, c \), the domain \( D_p(b, c) \) has a L-shaped diagram which covers the positions \((0, 0), (0, 1), (1, 0), (2, 0),..., (p - 2, 0)\) in the \( y, z \)-plane and \( L_p(b, c) = c \). (For example, see Fig.5 for the case \( D_p(13, 171, 2000) \).) Now, by (1), \( N(p, b, c) = c - p + 1 = n \). Hence the result.

The following lemma describes certain arithmetic properties of prime numbers. It will be used in the inductive argument of Theorem 2.8.

Lemma 2.7 Let \( p_i \) be the \( i \)th prime number. For \( n \geq 1 \), let \( R(n) \) and \( Q(n) \) be the following statements:

\[
R(n) = 1 + 2p_1p_2...p_n
\]
\[
Q(n) = p_{n+1}(p_{n+1} - 1)(p_{n+1} - 2).
\]

Then \( R(n) > Q(n) \) for all \( n \geq 5 \).
Proof. For \( n \geq 1 \), define \( R'(n) \) and \( Q'(n) \) by the following statements:

\[
R'(n) = p_1p_2...p_n \\
Q'(n) = p_{n+1}^3.
\]

It is clear that \( R(n) > R'(n) \) and \( Q'(n) > Q(n) \) for all \( n \geq 1 \). So we only need to prove that \( R'(n) > Q'(n) \) for \( n \geq 5 \).

It is obvious that \( R'(n) > Q'(n) \) for \( n = 5, 6, 7, 8 \) since \( R'(5) = 2310, R'(6) = 30030, R'(7) = 510510, R'(8) = 9699690 \) and \( Q'(5) = 2197, Q'(6) = 4913, Q'(7) = 6859, Q'(8) = 12167 \) respectively.

In [4], Nagura showed that \( 1 < \frac{p_{n+1}}{p_n} < 1.2 \), for \( n > 9 \).

Hence, for \( n \geq 9 \), the following inequalities are true:

\[
\frac{R'(n+1)}{R'(n)} = p_{n+1} > 2 > 1.728 = (1.2)^3 > \left(\frac{p_{n+2}}{p_{n+1}}\right)^3 = \frac{Q'(n+1)}{Q'(n)}.
\]

Since \( R'(9) = 223092870 > 24389 = Q'(9) \), we have \( R'(n) > Q'(n) \) for all \( n \geq 9 \) by (2). Hence the result.

Finally, we will prove the main theorem of this article:

**Theorem 2.8** For any positive integer \( n \) greater than 1, there always exist \( a, b, c \) such that \( N(a, b, c) = n \).

**Proof.** A straightforward check shows that \( N(5, 8, 9) = 13, N(5, 11, 18) = 25, N(5, 22, 19) = 37 \) (shown in Example 2.1 and Fig.1) and \( N(5, 22, 31) = 49 \). Hence, by Corollary 2.5 and an application of Lemma 2.6 to the case \( p = 5 \), it remains to show that there always exist \( a, b, c \) such that \( N(a, b, c) = n \) where \( n > 1 \) and \( n = 1 \mod 60 \).
Every positive integer is a Frobenius number ...

It can be shown that \( N(7, 17, 33) = 61 \), \( N(7, 38, 51) = 121 \) and \( N(7, 58, 71) = 181 \). By an application of Lemma 2.6 to the case \( p = 7 \), it remains to check the cases when \( n > 1 \) and \( n = 1 \mod 420 \).

It can be shown that \( N(11, 92, 113) = 421 \) and \( N(11, 206, 215) = 841 \). By an application of 2.6 to the case \( p = 11 \), it remains to check the cases when \( n > 1 \) and \( n = 1 \mod 4620 \). By the notations of Lemma 2.7, these \( n \)'s are greater than or equal to \( R(5) \) and hence greater than \( Q(5) = (13)(12)(11) \). But by Lemma 2.6 when \( p_6 = 13 \), it remains to check the cases when \( n \) is greater than or equal to \( R(6) \) and \( n = 1 \mod 2p_1p_2p_3p_4p_5p_6 \). But then these \( n \)'s are all greater than \( Q(6) \) by Lemma 2.7 and we can apply Lemma 2.6 again for \( p_7 = 17 \) to reduce the proof to checking the cases when \( n \) is greater than or equal to \( R(7) \) and \( n = 1 \mod 2p_1p_2p_3p_4p_5p_6p_7 \). As these are all greater than \( Q(7) \) by Lemma 2.7 and the same argument based on using Lemma 2.6 for the next prime numbers just as before can be applied inductively. The proof is complete for all positive integers \( n \) greater than 1.

References


Received: March 2, 2015; Published: April 4, 2015