Journal of Integer Sequences, Vol. 9 (2006),
Article 06.4.6

On a Generalization of the Coin Exchange Problem for Three Variables

Amitabha Tripathi
Department of Mathematics
Indian Institute of Technology
Hauz Khas
New Delhi - 110016
India
atripath@maths.iitd.ac.in

Sujith Vijay[1]
Department of Mathematics
Rutgers University – New Brunswick
Piscataway, NJ 08854
USA
sujith@math.rutgers.edu

Abstract

Given relatively prime and positive integers $a_1, a_2, \ldots, a_k$, let Γ denote the set of nonnegative integers representable by the form $a_1x_1 + a_2x_2 + \cdots + a_kx_k$, and let $\Gamma^\star$ denote the positive integers in Γ. Let $\mathcal{S}^\star(a_1, a_2, \ldots, a_k)$ denote the set of all positive integers n not in Γ for which $n + \Gamma^\star$ is contained in $\Gamma^\star$. The purpose of this article is to determine an algorithm which can be used to obtain the set $\mathcal{S}^\star$ in the three variable case. In particular, we show that the set $\mathcal{S}^\star(a_1, a_2, a_3)$ has at most two elements. We also obtain a formula for $g(a_1, a_2, a_3)$, the largest integer not representable by the form $a_1x_1 + a_2x_2 + a_3x_3$ with the x_i's nonnegative integers.

[1]This work was done while the second author was at the Department of Mathematics, Indian Institute of Technology, Delhi.

1 Introduction

Given relatively prime and positive integers $a_1, a_2, \ldots, a_k$ and a positive integer N, consider the equation

$$a_1x_1 + a_2x_2 + \ldots + a_kx_k = N \tag{1}$$

If each x_i is a nonnegative integer, it is well known and easy to show that (1) has a solution for all sufficiently large N. Hence, if we denote by Γ the set $\{a_1x_1+a_2x_2+\cdots+a_kx_k : x_j \geq 0\}$, then $\Gamma^c := \mathbb{N} \setminus \Gamma$ is a finite set. A natural problem that then arises is finding the largest N such that (1) has no solution in nonnegative integers, or in other words, of the largest element in Γ^c. This problem was first posed by Frobenius, who is believed to have been the first person to show that $a_1a_2 - a_1 - a_2$ is the largest element in Γ^c in the two variable case. Frobenius was also responsible in introducing the notation $g(a_1, a_2, \ldots, a_k)$ to denote the *largest* number in Γ^c. It is for this reason that the problem is also known as the linear Diophantine problem of Frobenius. The coin exchange problem derives its name from the obvious interpretation of this problem in terms of exchanging coins of arbitrary denomination with an infinite supply of coins of certain fixed denominations. The number of elements in Γ^c, denoted by $n(a_1, a_2, \ldots, a_k)$, was later introduced by Sylvester [25], and it was shown that $n(a_1, a_2) = \frac{1}{2}(a_1-1)(a_2-1)$. Another related function is $s(a_1, a_2, \ldots, a_k)$, which stands for the sum of elements in Γ^c, introduced by Brown and Shiue [6], wherein it was shown that $s(a_1, a_2) = \frac{1}{12}(a_1 - 1)(a_2 - 1)(2a_1a_2 - a_1 - a_2 - 1)$.

An explicit solution for the functions g and n in more than two variables has met with little success over the years except in special cases. There is a simple formula for each of these functions when the a_j's are in *arithmetic progression* [2, 9, 19, 27], but results obtained in other cases usually give upper bounds, deal with a special case or give an algorithmic solution [3, 4, 5, 11, 12, 13, 15, 20, 21, 22, 23, 24]. We refer to the book [18] where a complete account of the Frobenius problem can be found.

A variation of the coin exchange problem which also leads to its generalization was introduced by Tripathi [28]. We employ the notation used in [28], and denote by $\mathcal{S}^\star(a_1, a_2, \ldots, a_k)$ the set of all $n \in \Gamma^c$ such that

$$n + \Gamma^\star \subseteq \Gamma^\star,$$

where $\Gamma^\star = \Gamma\backslash\{0\}$. Let $g^\star(a_1, a_2, \ldots, a_k)$ (respectively, $n^\star(a_1, a_2, \ldots, a_k)$ and $s^\star(a_1, a_2, \ldots, a_k)$) denote the *least* (respectively, the *number* and *sum* of) elements in $\mathcal{S}^\star$. It is apparent that $g(a_1, a_2, \ldots, a_k)$ is the *largest* element in $\mathcal{S}^\star$, so that

$$g^\star(a_1, a_2, \ldots, a_k) \leq g(a_1, a_2, \ldots, a_k),$$

and $n^\star(a_1, a_2, \ldots, a_k) \geq 1$, with equality if and only if $g^\star = g$. It is interesting to note that this problem also arises from looking at the generators for the derivation modules of certain monomial curves [16, 17] and also in comparing numerical semigroups [8], and has been extensively studied in a more algebraic setting.

For each j, $1 \leq j \leq a_1 - 1$, let m_j denote the *least* number in Γ congruent to j mod a_1. Then $m_j - a_1$ is the largest number in Γ^c congruent to j mod a_1, and no number less than this in this residue class can be in $\mathcal{S}^\star$, for they would differ by a multiple of a_1, an element in $\Gamma^\star$. Therefore

$$\mathcal{S}^\star(a_1, a_2, \ldots, a_k) \subseteq \{m_j - a_1 : 1 \leq j \leq a_1 - 1\}, \tag{2}$$

$$g^\star(a_1, a_2, \dots, a_k) \le \left(\max_{1\le j\le a_1-1} m_j \right) - a_1 = g(a_1, a_2, \dots, a_k), \tag{3}$$

$$n^\star(a_1, a_2, \dots, a_k) \le a_1 - 1, \tag{4}$$

and

$$s^\star(a_1, a_2, \dots, a_k) \le \sum_{j=1}^{a_1-1} m_j - a_1(a_1 - 1). \tag{5}$$

More precisely,

$$m_j - a_1 \in \mathcal{S}^\star(a_1, a_2, \dots, a_k) \Longleftrightarrow (m_j - a_1) + m_i \ge m_{j+i} \tag{6}$$

for $1 \le i \le a_1 - 1$. The expression for $g(a_1, a_2, \dots, a_k)$ in (3) is due to Brauer & Shockley [5]. It is known [1] that if the semigroup Γ is *symmetric* then $\mathcal{S}^\star = \{g(a_1, a_2, \dots, a_k)\}$.

The purpose of this article is to determine the set $\mathcal{S}^\star$ together with the related functions in the three variable case. We shall use the variables a, b, c, and assume that a, b, c are coprime.

Given a, b, c, we define the matrix $\mathcal{M}$ by

$$\mathcal{M} := \begin{pmatrix} x_a & y_a & z_a \\ x_b & y_b & z_b \\ x_c & y_c & z_c \end{pmatrix},$$

where the entries are nonnegative integers. Let x_a, y_b, z_c be the *least* positive integers such that

$$ax_a = by_a + cz_a \;\text{ for some integers }\; y_a \ge 0, z_a \ge 0; \tag{7}$$

$$by_b = ax_b + cz_b \;\text{ for some integers }\; x_b \ge 1, z_b \ge 0; \tag{8}$$

$$cz_c = ax_c + by_c \;\text{ for some integers }\; x_c \ge 1, y_c \ge 0. \tag{9}$$

The matrix $\mathcal{M}$, with the entries at x_b and x_c allowed to be 0, was used in [7, 10] in order to give an expression for $g(a, b, c)$; see also [Proposition 4.7.1, [18]]. For the sake of completeness, we state the proposition below.

Proposition 1. *Let x_a, y_b, z_c be the least positive integers such that there exist integers $x_b, x_c, y_a, y_c, z_a, z_b \ge 0$ with*

$$ax_a = by_a + cz_a, \quad by_b = ax_b + cz_b, \quad cz_c = ax_c + by_c.$$

(a) *If $x_b, x_c, y_a, y_c, z_a, z_b$ are all greater than 0, then*

$$x_a = x_b + x_c, \quad y_b = y_a + y_c, \quad z_c = z_a + z_b.$$

(b) (i) *If* $x_b = 0$ *or* $x_c = 0$*, then* $by_b = cz_c$ *and* $ax_a = by_a + cz_a$ *with* $y_a, z_a > 0$.

(ii) *If* $y_a = 0$ *or* $y_c = 0$*, then* $ax_a = cz_c$ *and* $by_b = ax_b + cz_b$ *with* $x_b, z_b > 0$.

(iii) *If* $z_a = 0$ *or* $z_c = 0$*, then* $ax_a = by_b$ *and* $cz_c = ax_c + by_c$ *with* $x_c, y_c > 0$.

We now state and prove our main result where we determine the set $\mathcal{S}^\star(a,b,c)$ in terms of the entries of the matrix $\mathcal{M}$.

Theorem 1. *Let* $a < b < c$ *with* $\gcd(a,b,c) = 1$*. With the entries of the matrix* $\mathcal{M}$ *as defined in* (7)*,* (8)*,* (9)*,*

$$\mathcal{S}^\star(a,b,c) = \begin{cases} \Big\{b(y_b-1)+c(z_a-1)-a,\, b(y_a-1)+c(z_c-1)-a\Big\}, \\ \text{if } y_a, z_a \geq 1; \\ \Big\{b(y_b-1)+c(z_a-1)-a\Big\}, \quad \text{if } y_a = 0; \\ \Big\{b(y_a-1)+c(z_c-1)-a\Big\}, \quad \text{if } z_a = 0. \end{cases}$$

Proof. For any integer j, with $1 \leq j \leq a-1$, let $m_j = by + cz$, where y, z are nonnegative integers. Recall that m_j is the smallest integer in Γ congruent to j mod a. Now $y \leq y_b - 1$, since otherwise $b(y - y_b) + c(z + z_b) \equiv j \bmod a$ and, by equation (8), it is less than m_j. Similarly, by using equation (9), we have $z \leq z_c - 1$.

If $y_a > y_b$, then $a(x_a - x_b) = b(y_a - y_b) + c(z_a + z_b) > 0$, contradicting the minimality of x_a. Thus, $y_a \leq y_b$, and similarly $z_a \leq z_c$. Note that these inequalities follow immediately from the above Proposition, and that the former inequality is strict if $z_a > 0$ and the latter if $y_a > 0$.

If $y \geq y_a$ and $z \geq z_a$, then $m_j - (by_a + cz_a)$ would be a positive integer less than m_j and congruent to j mod a. Therefore, *at least* one of

$$0 \leq y \leq y_a - 1 \quad \text{and} \quad 0 \leq z \leq z_c - 1 \tag{10}$$

or

$$0 \leq y \leq y_b - 1 \quad \text{and} \quad 0 \leq z \leq z_a - 1 \tag{11}$$

holds.

Case I: $(y_a, z_a \geq 1)$ We claim that $m_i^\star := b(y_a - 1) + c(z_c - 1) = m_i$ and $m_j^\star := b(y_b - 1) + c(z_a - 1) = m_j$, with $y_a < y_b$ and $z_a < z_c$. If $m_i^\star > m_i = by + cz$, then $b(y_a - y - 1) + c(z_c - z - 1) = \big(b(y_a - 1) + c(z_c - 1)\big) - (by + cz) \in a\mathbb{N}$. Since $0 \leq z \leq z_c - 1$, we have $0 \leq z_c - z - 1 < z_c$, so that from the definition of z_c we conclude $y_a - y - 1 \geq 1$. Hence, $b(y_a - y - 1) + c(z_c - z - 1) = (by_a + cz_a) + ma$ for some $m \in \mathbb{N}$. But then $ma + b(y+1) = c(z_c - z_a - z - 1)$, which contradicts the minimality of z_c. This contradiction proves that $m_i^\star = m_i$, and we have $y_a < y_b$ since $z_a > 0$ by an earlier argument in this proof. A similar argument shows that $m_j^\star = m_j$, with $z_a < z_c$.

We now claim that if $m_k = by + cz \neq b(y_a - 1) + c(z_c - 1),\ b(y_b - 1) + c(z_a - 1)$, then $m_k - a \notin \mathcal{S}^\star$. To prove this, we exhibit $m'_k \in \Gamma^\star$ such that $(m_k - a) + m'_k \notin \Gamma^\star$. If $0 \leq y \leq y_a - 1$ and $0 \leq z \leq z_c - 1$, set $m'_k := b(y_a - y - 1) + c(z_c - z - 1)$; and if $0 \leq y \leq y_b - 1$ and $0 \leq z \leq z_a - 1$, set $m'_k := b(y_b - y - 1) + c(z_a - z - 1)$. In the first case, $(m_k - a) + m'_k$

equals $m_i^\star - a$, and in the second case, it equals $m_j^\star - a$. So, in both cases, $(m_k - a) + m_k' \notin \Gamma^\star$. This proves that $\mathcal{S}^\star \subseteq \big\{b(y_a-1)+c(z_c-1)-a, b(y_b-1)+c(z_a-1)-a\big\}$.

To complete the first case of our proof, it remains to show that each of the two numbers $m_i^\star - a$, $m_j^\star - a$ belong to $\mathcal{S}^\star$. We show this for $m_i^\star - a$; a similar argument shows that $m_j^\star - a \in \mathcal{S}^\star$. Consider $N = \big(b(y_a-1)+c(z_c-1)-a\big) + n$, where $n = ax_0 + by_0 + cz_0$ with x_0, y_0, z_0 nonnegative, not all zero. Observe that $y_a - 1 \geq 0$ by assumption, and that $z_c - 1 \geq 0$ by definition. If $x_0 \geq 1$, then it is clear that $N \in \Gamma^\star$. If $y_0 \geq 1$, then $N = a(x_a - 1 + x_0) + b(y_0 - 1) + c(z_c - z_a - 1 + z_0) \in \Gamma^\star$. If $z_0 \geq 1$, then $N = a(x_c - 1 + x_0) + b(y_a + y_c - 1 + y_0) + c(z_0 - 1) \in \Gamma^\star$. This proves $m_i^\star - a \in \mathcal{S}^\star$, and completes Case I.
Case II: ($y_a = 0$ or $z_a = 0$) If $z_a = 0$, equation (10) must hold. We show that $m_i^\star - a = b(y_a-1)+c(z_c-1)-a$ is the only element in $\mathcal{S}^\star$ in this case. Indeed, the argument in Case I shows that $m_i^\star = m_i$, that $m_i^\star - a \in \mathcal{S}^\star$, and that $\mathcal{S}^\star$ has *at most* two elements. Thus, it only remains to show that $m_j^\star - a = b(y_b-1)-c-a \notin \mathcal{S}^\star$. In fact, $m_j^\star = b(y_b-1)-c = by+cz = m_j$ implies $b(y_b - y - 1) = am + c(z+1)$ for some $m \in \mathbb{N}$. Since this contradicts the minimality of y_b, $m_j^\star > m_j$ and so $m_j^\star - a = b(y_b-1)-c-a \notin \mathcal{S}^\star$. In case $y_a = 0$, equation (11) must hold, and a similar argument will show that $b(y_b-1)+c(z_a-1)-a$ is the only element in $\mathcal{S}^\star$ in this case. This completes the proof of our theorem. $\square$

Corollary 1. *Let $a < b < c$ with $\gcd(a,b,c) = 1$. With the notation of Theorem 1,*

$$g(a,b,c) = \begin{cases} \max\big\{b(y_b-1)+c(z_a-1)-a, b(y_a-1)+c(z_c-1)-a\big\}, \\ \text{if } y_a, z_a \geq 1; \\ b(y_b-1)+c(z_a-1)-a, \quad \text{if } y_a = 0; \\ b(y_a-1)+c(z_c-1)-a, \quad \text{if } z_a = 0. \end{cases}$$

Remark 1. A variation of Corollary 1 is due to Johnson [12]. In [12], the variables a, b, c are assumed to be *pairwise coprime*, so that x_b, y_b, z_b and x_c, y_c, z_c are dlyefined analogously to x_a, y_a, z_a, and therefore taken as nonnegative. In the case of Theorem 1 we only assume that a, b, c are coprime, and need the positivity of x_b, y_b, z_b and x_c, y_c, z_c. If we assume that a, b, c are pairwise coprime, $y_a > 0$ and $z_a > 0$, so that only the first case in Theorem 1 holds; see also [Theorem 2.2.3, [18]]:

Let $a < b < c$ with a, b, c pairwise coprime. With the notation of Theorem 1,

$$g(a,b,c) = \max\big\{b(y_b-1)+c(z_a-1)-a, b(y_a-1)+c(z_c-1)-a\big\}$$

Corollary 2. *Let $a < b < c$ be such that $\gcd(a,b,c) = 1$ and $a|(b+c)$. Then*

$$\mathcal{S}^\star(a,b,c) = \left\{ b\left\lfloor \frac{ac}{b+c} \right\rfloor - a, c\left\lfloor \frac{ab}{b+c} \right\rfloor - a \right\}.$$

Proof. Observe that $a|(bx-cy)$ if and only if $a|(x+y)$ since $a|(b+c)$ and $\gcd(a,b,c) = 1$ forces $\gcd(a,b) = 1 = \gcd(a,c)$. If we write $y = ma - x$, then $bx > cy$ reduces to $x > \frac{mac}{b+c}$. The least such x is clearly $y_b = \lceil \frac{ac}{b+c} \rceil$. Similarly, $z_c = \lceil \frac{ab}{b+c} \rceil$, and it is easy to see that $(y_a, z_a) = (1,1)$. Observe that $b+c$ cannot divide either ab or ac since $\gcd(b,c) = 1$. Therefore, $y_b - 1 = \lfloor \frac{ac}{b+c} \rfloor$ and $z_c - 1 = \lfloor \frac{ab}{b+c} \rfloor$, and the result now follows from Theorem 1. $\square$

Remark 2. Corollary 2 implies that

$$g(a,b,c) = \max\left\{ b\left\lfloor \frac{ac}{b+c} \right\rfloor - a, c\left\lfloor \frac{ab}{b+c} \right\rfloor - a \right\}$$

when $a|(b+c)$. This result is well-known and due to Brauer & Shockley; see [5, 26].

Corollary 3. *If* $\gcd(a,d) = 1$, *then*

$$\mathcal{S}^\star(a, a+d, a+2d) = \begin{cases} \left\{\frac{1}{2}a(a-2) + d(a-1)\right\}, & \textit{if } a \textit{ is even;} \\ \left\{\frac{1}{2}a(a-3) + d(a-1), \frac{1}{2}a(a-3) + d(a-2)\right\}, & \\ \textit{if } a \textit{ is odd.} & \end{cases}$$

Proof. Observe that $a|\{(a+d)x+(a+2d)y\}$ if and only if $a|(x+2y)$. Therefore, (y_a, z_a) equals $(0, \frac{1}{2}a)$ if a is *even* and $(1, \frac{1}{2}(a-1))$ if a is *odd*. If a is *even*, it is easy to see that $y_b = 2$, and the only element in the set is $(a+d) + \frac{1}{2}(a+2d)(a-2) - a = d(a-1) + \frac{1}{2}a(a-2)$. If a is *odd*, the required conditions to determine z_c reduce to minimizing y such that $(a+2d)y > (a+d)x$ and $2y \equiv x \bmod a$. This gives $z_c = \frac{1}{2}(a+1)$ and the set thus consists of the two elements $(a+d)+\frac{1}{2}(a+2d)(a-3)-a = d(a-2)+\frac{1}{2}a(a-3)$ and $\frac{1}{2}(a+2d)(a-1)-a = d(a-1)+\frac{1}{2}a(a-3)$. This completes the proof. □

Remark 3. Corollary 3 is the three variable version of the main result of [28]. Determination of $g(a, a+d, a+2d)$ is an immediate consequence of Corollary 3 and is also a special case of a more general result when there is no restriction on the number of variables in arithmetic progression, and is due to Roberts; see [2, 19, 27]. Corollary 3 implies

$$g(a, a+d, a+2d) = a\left\lfloor \frac{a-2}{2} \right\rfloor + d(a-1).$$

A description of the set $\mathcal{S}^\star(a,b,c)$, and hence of the several related functions, including $g(a,b,c)$ and $g^\star(a,b,c)$, involves at least a partial knowledge of the matrix $\mathcal{M}$. The description of $\mathcal{M}$ is a known result due to Morales [14], and is described in [Claim 8.4.3, [18]].

2 Acknowledgement

The authors wish to thank the referee for several suggestions and references that have helped improve an earlier version of their paper.

References

[1] V. Barucci, D. E. Dobbs and M. Fontana, Maximality properties of one-dimensional analytically irreducible local domains, *Memoires Amer. Math. Soc.*, **125/598**, 1997.

[2] P. T. Bateman, Remark on a recent note on linear forms, *Amer. Math. Monthly*, **65** (1958), 517–518.

[3] A. Brauer, On a problem of partitions – I, *Amer. J. Math.*, **64** (1942), 299–312.

[4] A. Brauer and B. M. Seelbinder, On a problem of partitions – II, *Amer. J. Math.*, **76** (1954), 343–346.

[5] A. Brauer and J. E. Shockley, On a problem of Frobenius, *J. reine Angew. Math.*, **211** (1962), 215–220.

[6] T. C. Brown and P. J. Shiue, A remark related to the Frobenius problem, *Fibonacci Quart.*, **31** (1993), 31–36.

[7] G. Denham, Short generating functions for some semigroup algebras, *The Electronic Journal of Combinatorics*, **10**, Research paper 36 (2003), 7 pages.

[8] D. E. Dobbs and G. L. Matthews, On comparing two chains of numerical semigroups and detecting Arf semigroups, *Semigroup Forum*, **63**, #2 (2001), 237–246.

[9] D. D. Grant, On linear forms whose coefficients are in arithmetic progression, *Israel J. Math.*, **15** (1973), 204–209.

[10] J. Herzog, Generators and relations of abelian semigroups and semigroup rings, *Manuscripta Math.*, **3** (1970), 175–193.

[11] G. R. Hofmeister, Zu einem Problem von Frobenius, *Norske Videnskabers Selskabs Skrifter*, **5** (1966), 1–37.

[12] S. M. Johnson, A linear diophantine problem, *Canad. J. Math.* **12** (1960), 390–398.

[13] R. J. Levit, A minimum solution for a diophantine equation, *Amer. Math. Monthly*, **63** (1956), 646–651.

[14] M. Morales, Syzygies of monomial curves and a linear diophantine problem of Frobenius, *Internal Report, Max Planck Institut für Mathematik, Bonn*, 1987.

[15] A. Nijenhuis and H. S. Wilf, Representations of integers by linear forms in non negative integers, *J. Number Theory*, **4** (1972), 98–106.

[16] D. P. Patil and Balwant Singh, Generators for the derivation modules and the relation ideals of certain curves, *Manuscripta Math.*, **68** (1990), 327–335.

[17] D. P. Patil and I. Sengupta, Minimal set of generators for the derivation modules of certain monomial curves, *Comm. Algebra*, **27** (1999), 5619–5631.

[18] J. L. Ramírez Alfonsín, The Diophantine Frobenius Problem, *Oxford Lecture Series in Mathematics and its Applications*, **30**, Oxford Univerity Press, 2005.

[19] J. B. Roberts, Note on linear forms, *Proc. Amer. Math. Soc.*, **7** (1956), 465–469.

[20] J. B. Roberts, On a diophantine problem, *Canad. J. Math.*, **9** (1957), 219–222.

[21] Ö. J. Rödseth, On a linear diophantine problem of Frobenius, *J. reine Angew. Math.*, **301** (1978), 171–178.

[22] Ö. J. Rödseth, On a linear diophantine problem of Frobenius II, *J. reine Angew. Math.*, **307/308** (1979), 431–440.

[23] E. S. Selmer and Ö. Beyer, On the linear diophantine problem of Frobenius in three variables, *J. reine Angew. Math.*, **301** (1978), 161–170.

[24] E. S. Selmer, On the linear diophantine problem of Frobenius, *J. reine Angew. Math.*, **293/294** (1977), 1–17.

[25] J. J. Sylvester, Mathematical questions with their solutions, *The Educational Times*, **41** (1884), 21.

[26] A. Tripathi, Topics in Number Theory, Ph. D. Thesis, Department of Mathematics, State University of New York, Buffalo, 1989.

[27] A. Tripathi, The coin exchange problem for arithmetic progressions, *Amer. Math. Monthly*, **101**, (1994), 779–781.

[28] A. Tripathi, On a variation of the coin exchange problem for arithmetic progressions, *Integers*, **3**, #A01 (2003), 1–5.

2000 *Mathematics Subject Classification*: Primary 11D04.
Keywords: coin exchange problem, linear diophantine problem of Frobenius.

Received December 20 2005; revised version received September 12 2006. Published in *Journal of Integer Sequences*, September 12 2006.

Return to Journal of Integer Sequences home page.