ACTA ARITHMETICA
LXV.4 (1993)

A generalization of Sylvester's and Frobenius' problems on numerical semigroups

by

Zdzisław Skupień (Kraków)

1. Introduction. Our aim is to formulate and study a "modular change problem". Let $\mathcal{A}$ be a set of t natural numbers $a_1, \ldots, a_t$ (which are coin denominations or semigroup generators). Integer linear combinations of these numbers are clearly multiples of $\gcd \mathcal{A}$, their greatest common divisor. If indeterminate coefficients, say x_i's, are nonnegative, $x_i \in \mathbb{N}_0$, then those combinations form a numerical semigroup S (under addition),

$$S = S(\mathcal{A}) := \left\{ n \in \mathbb{N}_0 \;\middle|\; n = \sum_{i=1}^{t} x_i a_i,\ \text{all } x_i \in \mathbb{N}_0 \right\},$$

which includes 0 and all multiples of $\gcd \mathcal{A}$ large enough. In fact, the following is known.

Proposition 1.1. *All integer linear combinations of integers a_i in $\mathcal{A}$ coincide with all the multiples of* $\gcd \mathcal{A}$. *If the coefficients are nonnegative integers*, *the combinations include all multiples of* $\gcd \mathcal{A}$ *large enough.* ■

Let Ω $(= \Omega(\mathcal{A}) = |\mathbb{N} - S| \le \infty)$ denote the cardinality of the complement of S in $\mathbb{N}$. Hence, if the given numbers are relatively prime, that is,

$$\gcd(a_1, \ldots, a_t) = 1\,, \tag{1.1}$$

then $\Omega < \infty$ is the number of integers $n \in \mathbb{N}_0$ without any representation

$$n = \sum_{i=1}^{t} x_i a_i\,, \tag{1.2}$$

with

$$\text{all } x_i \in \mathbb{N}_0\,. \tag{1.3}$$

The largest of these omitted n's is denoted by $g(\mathcal{A})$ (or $N(\mathcal{A})$); by definition $g(\mathcal{A}) = \infty$ if $\Omega = \infty$, and $g(\mathcal{A}) = -1$ if $\Omega = 0$. The study of the functions Ω and g dates back to Sylvester [14] and Frobenius (cf. [2]), respectively. Another related function—the number of partitions (1.2)–(1.3) of n, denoted by $\nu_n(\mathcal{A})$—is older and was studied by Euler. The study of Ω, g, and/or ν_n constitutes the classical "change problem" (cf. [9], where only ν_n is considered).

Let $q \in \mathbb{N}$ and let L, $L = L_q$, be a complete system of residues modulo q (e.g., $\mathbb{Z} \supset L = \{0, 1, \ldots, q-1\}$ unless otherwise stated). For a $\kappa \in L$, we impose the additional requirement

$$\sum_{i=1}^{t} x_i \equiv \kappa \pmod{q} \tag{1.4}$$

and consider the related functions Ω_κ, N_κ and $\nu_{n\kappa}$ which represent the number of so-called κ-omitted integers n (among nonnegative ones, $n \in \mathbb{N}_0$); the largest of them, $+\infty$, or -1; and the number of κ-representations of n, respectively. Then $(\mathcal{A}, q)$ is the pair of arguments of the functions and

$$g(\mathcal{A}, q) := \max\{N_\kappa(\mathcal{A}, q) : \kappa \in L_q\}.$$

This new problem, the "modular change problem", includes the classical one (for $q = 1$) and is prompted by applications of the problem (1.2)–(1.4) in constructive graph theory [13] where the following condition is desirable.

(1.5) *A solution exists for all natural n large enough.*

Our main result yields a useful equivalent of the condition (1.5) (or finiteness of g) in case of our modular problem. Moreover, explicit formulae in case of two generators ($t = 2$) and, in general case, efficient algorithms for evaluating both all Ω_κ and all N_κ are provided.

THEOREM 1.2. *The finiteness of an $N_\kappa(\mathcal{A}, q)$ is equivalent to the conjunction of* (1.1) *and*

$$\gcd(q, a_2 - a_1, a_3 - a_2, \ldots, a_t - a_{t-1}) = 1, \tag{1.6}$$

and is equivalent to the finiteness of g (or all N_κ's).

The proof of necessity uses the general solution of a linear Diophantine equation. (It is not excluded that $t = 1$, in which case (1.1) and (1.6) mean that $a_1 = 1 = q$.)

A correct reference to Sylvester's problem (and result, proved by W. J. C. Sharp [14] using a generating function) will be provided.

2. General results. We need the following notation:

$$D_i = \gcd(a_1, \ldots, a_i), \quad D_0 := 0,$$

whence $D_1 = a_1$ and $D_i = \gcd(D_{i-1}, a_i)$, $i = 1, \ldots, t$. It is known that the general integer solution x of (1.2) is the integer vector

$$x = \widetilde{x}_0 + \sum_{j=1}^{t-1} u_j y_j \tag{2.0}$$

where $\widetilde{x}_0$ is a particular integer solution of (1.2) and y_j's are $t-1$ integer vectors which form a basis for the rational solution space of the simplified (homogeneous) equation

$$\sum_{i=1}^{t} x_i a_i = 0 \tag{2.1}$$

such that u_j can be arbitrary integers. Hence, each y_j is a t-vector which is divisor minimal, that is, its components are relatively prime. In particular, it is known that a solution y of (2.1) for $t = 2$, $y = (x_1, x_2)$, is unique up to a factor of ± 1,

$$y = \pm(a_2/D_2, -a_1/D_2)\,. \tag{2.2}$$

For $j = 1, \ldots, t$, let ξ_j be an integer column j-vector with components ξ_{ij} satisfying the auxiliary equation

$$\sum_{i=1}^{j} a_i \xi_{ij} = D_j \tag{2.3}$$

whence $\xi_1 = \xi_{11} = 1$. Assume that not only all ξ_j but also $\widetilde{x}_0$ and all y_j are column vectors, $y_j = [y_{ij}]_{t\times 1}$. Then

$$\widetilde{x}_0 = n\xi_t/D_t$$

provided that $D_t \,|\, n$. By Proposition 1.1, the equation (2.3) can be replaced by

$$D_{j-1} w_j + a_j \xi_{jj} = D_j \quad (j = 1, \ldots, t)\,. \tag{2.4}$$

Now, a solution of (2.4) determines the last component ξ_{jj} of the vector ξ_j and the remaining components can be computed recursively,

$$\xi_{ij} = \xi_{i,j-1} w_j \quad \text{for } i < j \text{ and } j \geq 2\,.$$

We are now ready to construct all vectors y_j, $j < t$. Assume that the last $t - j - 1$ components of y_j are zero, and the $(j+1)$th component $y_{j+1,j}$ is negative and has the smallest possible absolute value. Then

$$D_j z_j + a_{j+1} y_{j+1,j} = 0 \quad \text{for some } z_j \in \mathbb{N}_0\,,$$

whence, using (2.3), (2.2), and the Kronecker δ symbol, we finally have

$$y_j = \begin{bmatrix} z_j \xi_j \\ y_{j+1,j} \\ 0 \end{bmatrix} = \left(a_{j+1} \begin{bmatrix} \xi_j \\ 0 \end{bmatrix} - D_j [\delta_{i,j+1}]_{t\times 1} \right) \Big/ D_{j+1} \quad (1 \leq j < t)\,. \tag{2.5}$$

The above method which produces a "first-column-missing upper triangular" matrix $[y_{ij}]_{t\times(t-1)}$ (see also [1]) usually gives solution vectors y_j with large components y_{ij} (in absolute value) depending on the ordering of a_i's. A computationally efficient method to find D_t and a vector ξ_t together with all basis solutions y_j (with components small enough) can be found in [6, 5]. The above method, however, readily gives the general solution to each equation (2.3). Namely, if k replaces j there, then $\widetilde{x}_0 = \xi_k$ and the corresponding solution basis is formed by the columns of the leading $k\times(k-1)$ submatrix of $[y_{ij}]$.

From (2.5), using (2.3) to eliminate ξ_{jj}, we get

$$(2.6)\quad \sum_{i=1}^{t} y_{ij} = \Big(\xi_{jj}a_{j+1} - D_j + a_{j+1}\sum_{i=1}^{j-1}\xi_{ij}\Big)\Big/D_{j+1}$$
$$= \Big(D_j(a_{j+1}-a_j) + a_{j+1}\sum_{i=1}^{j-1}(a_j-a_i)\xi_{ij}\Big)\Big/a_jD_{j+1},\quad j<t\,.$$

Proof of Theorem 1.2. First, by Proposition 1.1, the existence of an integer solution of (1.2) for any n is equivalent to (1.1).

Necessity of (1.1) is thus proved. Hence, if p is a prime divisor of the left-hand side of (1.6) then $p\nmid a_k$ for all k and therefore $p\mid\sum_i y_{ij}$ in (2.6) for all j. Then by (2.0), for any $n=(kq-1+\kappa)a_1$ ($k\in\mathbb{N}$) in (1.2), (1.4) is not satisfied since $p\mid q$, a contradiction.

Sufficiency. Using (2.0) and (2.6) one can see that (1.1) and (1.6) imply the existence of a solution to (1.2) and (1.4) for any n and for any $\kappa\in L_q$. Now, let $-Y_{n,\kappa}$ and $Z_{n,\kappa}$ be the corresponding parts of the right-hand side of (1.2) with nonpositive and nonnegative coefficients, respectively. Assume that the number $+Y_{n,\kappa}$ is as small as possible. Thus $Y_{0,0}=0=Z_{0,0}$ (where $n=0$ and $\kappa=0$).

Let $-Y^0$ be a linear combination of a_i's such that, for all i, the coefficient of a_i is chosen to be the smallest of (nonpositive) coefficients of the a_i in all $-Y_{0,\kappa}$ (where $n=0$). For $n=1$ and $\kappa=0$, let $Y=Y_{1,0}$ and $Z=Z_{1,0}$ whence $1=-Y+Z$. Consider the following a_1 consecutive integers n:

$$\begin{gathered}(a_1-1)Y + \qquad Y^0\,,\\ (a_1-2)Y+Z+Y^0\,,\\ \dots\dots\dots\dots\dots\dots\\ (a_1-1)Z+Y^0\,.\end{gathered}$$

Each of them is fully representable, i.e., has representations (1.2)–(1.4) for all $\kappa\in L_q$, because any representation can be modified by adding any of the q expressions $0=-Y_{0,\kappa}+Z_{0,\kappa}$ where $n=Y^0-Y_{0,\kappa}$ has a representation (1.2) and (1.3) by the very definition of Y^0. Each larger integer also has full representations, by adding a multiple of a_1 to representations of one of the a_1 integers above. ∎

The above sufficiency proof extends that of the existence of g for $q = 1$, due to Ö. Beyer, as presented in Selmer [12] (1986).

In what follows (1.1) and (1.6) are assumed. Moreover,

$$a_1 < \ldots < a_t \,. \tag{2.7}$$

A generator which has a 1-representation (modulo q) by the remaining generators can be removed from $\mathcal{A}$ without altering the value of any N_κ. Call the set $\mathcal{A}$ of generators *q-independent* if either $q = 1 = t = a_1$ or $t > 1$ and no a_i in $\mathcal{A}$ is 1-representable modulo q by the remaining generators; otherwise $\mathcal{A}$ is called *q-dependent* (1-representable modulo 1 means representable). Hence the 1-independence of $\mathcal{A}$ ($q = 1$) is the known notion of independence of generators.

Note that

$$|\mathcal{A}| = t \le qa_1 = q \min \mathcal{A} \tag{2.8}$$

is a necessary condition for $\mathcal{A}$ to be q-independent (whence $a_t \ge \lceil t/q \rceil + t - 1$ if $\mathcal{A}$ is q-independent).

In fact, suppose $qa_1 < t$. Then $|\mathcal{A} - \{a_1\}| \ge qa_1$. Hence there is $j \ge 2$ such that $a_j \equiv a_1 \pmod{qa_1}$ or there are $i, j \ge 2$ with $a_i \equiv a_j \pmod{qa_1}$. In either case $\mathcal{A}$ is q-dependent. ∎

Recall that $g(\mathcal{A}, q)$ is the largest integer (or $+\infty$) which is not fully representable modulo q by $\mathcal{A}$. The Frobenius problem consists in finding (an upper bound for) the integer $g(\mathcal{A})$, $g(\mathcal{A}) = g(\mathcal{A}, 1) = N_0(\mathcal{A}, 1)$, i.e., if $q = 1$ and $\kappa = 0$. In this context we shall assume

$$a_t \le g(\mathcal{A} - \{a_t\}, q) \quad \text{if } t \ge 2 \,, \tag{2.9}$$

i.e., first we shall possibly eliminate excessively large (irrelevant) generators. This natural assumption, which only admits of independence of the largest generator a_t from the remaining ones, is usually omitted in the published upper bounds for $g(\mathcal{A}, 1)$ or—as in [11]—it is sometimes replaced by requiring the independence of the whole $\mathcal{A}$.

Given a positive integer $\widetilde{n}$ which has a representation (1.2)–(1.3) with $n = \widetilde{n}$ (e.g., $\widetilde{n} = a_i$, $\sum a_i$, etc., the smallest $\widetilde{n} = a_1$), let

$$m = q\widetilde{n}$$

and, for each residue r modulo m and a fixed $\kappa \in L_q$, let $n_{r\kappa}$ be the least n which is in the residue class of r modulo m and has a κ-representation. Hence, by the choice of m, if $n \equiv r \pmod{m}$, n clearly has a κ-representation if and only if $n \ge n_{r\kappa}$. Thus, the finiteness of N_κ's is equivalent to the existence of all numbers $n_{r\kappa}$; moreover,

$$N_\kappa = \max_r n_{r\kappa} - m \tag{2.10}$$

because, if N_κ is finite, there is $\varrho \in \mathbb{N}_0$ with $\varrho < m$ such that $N_\kappa \equiv \varrho \pmod{m}$, whence N_κ is clearly m smaller than $n_{\varrho\kappa}$. This extends a formula for g due to Brauer and Shockley [2, Lemma 3] ($q = 1$ and $\kappa = 0$). Thus, knowing the qm numbers $n_{r\kappa}$ [and a κ-representation of each $n_{r\kappa}$] we can determine all sets, say $\mathfrak{I}^{\mathrm{c}}_\kappa$, of κ-omitted integers [and a κ-representation of each positive n such that $n \notin \mathfrak{I}^{\mathrm{c}}_\kappa$]. Analogously, on partitioning $\mathfrak{I}^{\mathrm{c}}_\kappa$ into residue classes modulo m,

$$\begin{aligned} \varOmega_\kappa := |\mathfrak{I}^{\mathrm{c}}_\kappa| &= \sum_{r=0}^{m-1} (n_{r\kappa} - r)/m \\ &= -(m-1)/2 + \sum_r n_{r\kappa}/m \qquad \text{(cf. [11])} \\ &= \sum_r \lfloor n_{r\kappa}/m \rfloor \qquad \text{(cf. [7])}\,. \end{aligned} \tag{2.11}$$

This formula generalizes those by Selmer [11, Theorem] and Nijenhuis [7], respectively, for $\varOmega$ if $q = 1$.

3. The case of two generators, $t = 2$. Throughout this section,

$$\kappa \in \{-1, 0, \ldots, q-2\}\,. \tag{3.1}$$

Let us use standard notation:

$$a = a_1, \quad b = a_2, \quad x = x_1, \quad y = x_2 \quad (a < b)\,.$$

Since (1.1) and (1.6) are assumed to hold,

$$\gcd(a, b) = 1 = \gcd(q, b - a)\,. \tag{3.2}$$

Sylvester's contribution to the change problem is misquoted or misplaced quite often (cp. [8, 11, 12, 4] and (!) [13]). The following is what Sylvester actually presents in [14] (where in fact p and q stand for a and b, resp.): "If a and b are relative primes, prove that the number of integers inferior to ab which cannot be resolved into parts (zeros admissible), multiples respectively of a and b, is

$$\tfrac{1}{2}(a-1)(b-1)\,."$$

It is explained in [14] by means of an example that integers in question are to be positive. Notice that it belongs to the mathematical folklore now that the bound ab above [integer $ab - a - b$] is the largest integer which is not representable as a linear combination of a and b with positive [nonnegative] integer coefficients.

We refer to κ-representations, κ-omitted integers and symbols $g(\mathcal{A},q)$ and $N_\kappa(\mathcal{A},q)$ as defined in Introduction. In order to avoid trivialities, assume

$$(3.3)\qquad 1\le a<b \quad \text{but} \quad a>1 \quad \text{if } q=1\,,$$

because if $1\in\mathcal{A}$ then $S=\mathbb{N}_0$, whence $g(\{1,b\},q)=-1$ if $q=1$. Define

$$(3.4)\qquad g:=qab-a-b\,,$$

whence, by (3.2), g is odd;

$$(3.5)\qquad \begin{aligned} N_\kappa &:= qab-b-(q-1-\kappa)a, &\quad -1\le\kappa\le q-2\\ &= g-(q-2-\kappa)a, &\quad \text{by (3.4)}\,. \end{aligned}$$

Theorem 3.1. *Under the above assumptions*, *if* $t=2$ *and* $\mathcal{A}=\{a,b\}$, *the largest* κ*-omitted integer* $N_\kappa(\mathcal{A},q)=N_\kappa$ (*whence* $g(\mathcal{A},q)=N_{q-2}=g$) *and* $\Omega_\kappa=(g+1)/2$ *is the number of* κ*-omitted integers.*

Hence the interval $[0,g]$ contains as many κ-representable integers as κ-omitted ones. The proof is based on a series of auxiliary results which follow.

Proposition 3.2 (Folklore). *If* $a,b\in\mathbb{N}$ *and* $\gcd(a,b)=1$ *then*, *for each* $n\ge(a-1)(b-1)$, *there is exactly one pair of nonnegative integers* ϱ *and* σ *such that* $\sigma<a$ *and* $n=\varrho a+\sigma b$.

Notice for the proof that, for $j=0,1,\dots,a-1$, if $\gcd(a,b)=1$, all integers $n-jb$ are mutually distinct modulo a. Hence, for exactly one j, say $j=\sigma$, we have $n=\varrho a+\sigma b$, whence $\varrho\ge0$ because $\varrho a\ge -a+1$. ■

It is well known that

$$(3.6)\qquad (x,y)=(x^0+ub,y^0-ua),\qquad u\in\mathbb{Z}\,,$$

is a general solution of (1.2) in our case, which agrees with (2.0) and (2.2). Hence we have

Proposition 3.3. *For any* κ, *if* $n<qab$ (*or* $n\le g$ *in* (3.4)) *then* n *has at most one* κ*-representation.* ■

Using (3.4), let

$$\mathfrak{I}:=\mathbb{Z}\cap[0,g],\qquad \mathfrak{I}':=\mathbb{Z}\cap[0,qab)\,.$$

Let $\mathfrak{I}_\kappa^\rightarrow$ denote the set of κ-representable integers and let

$$(3.7)\qquad \mathfrak{I}_\kappa:=\mathfrak{I}_\kappa^\rightarrow\cap\mathfrak{I},\qquad \mathfrak{I}'_\kappa:=\mathfrak{I}_\kappa^\rightarrow\cap\mathfrak{I}',\qquad \mathfrak{I}_\kappa^{\mathrm{c}}:=\mathfrak{I}-\mathfrak{I}_\kappa\,.$$

Moreover, $k+A:=\{k+x\mid x\in A\}$ if $A\subseteq\mathbb{Z}$. Notice that if $q=1$ (and $\kappa=-1$), then $\mathfrak{I}_\kappa^\rightarrow=S$, whence, by Proposition 3.2 and formula (3.4), $\mathfrak{I}_\kappa^{\mathrm{c}}=\mathbb{N}_0-S$. We are going to show that in general $\mathfrak{I}_\kappa^{\mathrm{c}}$ is the set of κ-omitted integers (cf. the end of the preceding section).

Proposition 3.4. *For any* κ, $N_\kappa \in \mathfrak{I}^c_\kappa$.

Proof. By (3.3) and (3.5), $N_\kappa \ge 0$. By (3.5) and (3.6), all solutions of (1.2) for $n = N_\kappa$ are of the form

$$x = \kappa + 1 + (q-u)b - q \quad \text{and} \quad y = ua - 1, \quad u \in \mathbb{Z}.$$

Then $x, y \ge 0$ can be satisfied only if $1 \le u < q$, which is a contradiction if $q = 1$; otherwise, due to (3.2), $x+y$ $(= \kappa + (b-1)q - (b-a)u) \not\equiv \kappa \pmod q$, contrary to (1.4). ∎

The following transformation is used by Nijenhuis and Wilf [8] in order to solve Sylvester's problem (with $q = 1$ and $\kappa = -1$).

Proposition 3.5. *The transformation*

$$\varphi : \mathfrak{I}_\kappa \ni n \mapsto g - n$$

is a bijection onto $\mathfrak{I}^c_{q-2-\kappa}$ *if* $0 \le \kappa \le q-2$, *and onto* $\mathfrak{I}^c_\kappa$ *if* $\kappa = -1$.

Proof. By (3.4) and (3.5), $g = N_{q-2}$. Hence, if $n \in \mathfrak{I}_\kappa$ then $\varphi(n) \notin \mathfrak{I}_{q-2-\kappa}$ because otherwise $g = n + \varphi(n) \in \mathfrak{I}_{q-2}$, contrary to Proposition 3.4. Moreover, injectivity of φ is clear. Notice that assumptions (3.2) ensure the existence of a solution (x_1, y_1) of (1.2) such that $0 \le x_1 < qb$ and $x_1 + y_1 \equiv q - 2 - \kappa \pmod q$. Suppose $n \in \mathfrak{I}^c_{q-2-\kappa}$ if $\kappa \ge 0$, and $n \in \mathfrak{I}^c_{-1}$ if $\kappa = -1$. Then clearly $y_1 < 0$. Therefore, by (3.4), $g - n = (qb - 1 - x_1)a + (-y_1 - 1)b \in \mathfrak{I}_\kappa$, whence $\varphi(g-n) = n$, which proves surjectivity of φ. ∎

Corollary 3.6. $|\mathfrak{I}_{-1}| = |\mathfrak{I}^c_{-1}| = |\mathfrak{I}|/2 = (g+1)/2$ (cf. (3.7)). ∎

Proposition 3.7.

$$(q-2-\kappa)a = \min \begin{cases} \mathfrak{I}_{q-2-\kappa} & \text{if } \kappa \ge 0, \\ \mathfrak{I}_{-1} & \text{if } \kappa = -1. \end{cases} \quad ∎$$

Proposition 3.8. $\max(\mathbb{Z} - \mathfrak{I}^{\rightarrow}_\kappa) = N_\kappa$.

Proof. Owing to Proposition 3.4, it is enough to show that $k \in \mathfrak{I}^{\rightarrow}_\kappa$ if $k > N_\kappa$. To this end, assume $q \ge 2$ because the case $q = 1$ is covered by Proposition 3.2. Next, assume $\kappa \ne q-2$ and $N_\kappa < k \le g$. Then, by (3.5), $0 \le g - k < g - N_\kappa = (q-2-\kappa)a$, whence, due to Propositions 3.7 and 3.5, $k \in \mathfrak{I}_\kappa$ and we are done. Finally, assume that $n = k > g$ $(= N_{q-2})$. Then

$$n_k := k - (q-1)ab \ge (a-1)(b-1) \quad \text{by (3.4)},$$

whence, by Proposition 3.2, $n_k = \varrho a + \sigma b$ for exactly one pair $(\varrho, \sigma) \ge (0,0)$ and $\sigma < a$. Hence, (1.2) and $x, y \in \mathbb{N}_0$ are satisfied if

$$x = \varrho + (q-1-j)b \quad \text{and} \quad y = \sigma + ja$$

for q consecutive values of j, $j = 0, \ldots, q-1$, whence, by (3.2), the congruence (1.4) is satisfied for one of these j's. Thus $k \in \mathfrak{I}^{\rightarrow}_\kappa$. ∎

Corollary 3.9. $\mathfrak{I}^c_\kappa$ *is the set of* κ*-omitted integers.* ∎

Proof of Theorem 3.1. The first part of the Theorem follows from Proposition 3.8. As for the counting part, let

$$\mathfrak{I}_\kappa^- = \mathfrak{I}_\kappa - \{g, g-1, \ldots, g-a+1\}.$$

Then, by (3.7), Proposition 3.8 and formula (3.5), $|\mathfrak{I}_\kappa^-| = |\mathfrak{I}_\kappa| - a$ for $\kappa < q-2$. Moreover, using Proposition 3.3, one can see that, for each $\kappa \geq 0$,

$$\psi_\kappa : \mathfrak{I}_{\kappa-1}^- \ni n \mapsto n + a$$

is a bijection onto $\mathfrak{I}_\kappa - \{(kq+\kappa)b \mid k = 0, 1, \ldots, a-1\}$, a set of cardinality $|\mathfrak{I}_\kappa| - a$, by (3.7), (3.4) and (3.1). Hence, $|\mathfrak{I}_{\kappa-1}| = |\mathfrak{I}_\kappa|$ for each $\kappa \geq 0$, which, due to (3.7) and Corollaries 3.6 and 3.9, ends the proof. ∎

The following result extends Corollary 3.9 and Proposition 3.3 and reduces determining $\nu_{n\kappa}$, the number of κ-representations of n, to the membership problem for the residue (n mod qab) (cf. [9] for $q = 1$).

Corollary 3.10. (A) *The set of integers n such that $n \in \mathbb{N}_0$ and $\nu_{n\kappa} = k$, $k \in \mathbb{N}_0$, is $\mathfrak{I}_\kappa^{\mathrm{c}}$ of cardinality $(g+1)/2$ if $k = 0$, else $((k-1)qab + \mathfrak{I}'_\kappa) \cup (kqab + \mathfrak{I}_\kappa^{\mathrm{c}})$ of cardinality qab. Hence, $kqab + \mathfrak{I}_\kappa^{\rightarrow}$ is the set of integers n such that $\nu_{n\kappa} \geq k+1$, $k \geq 0$. Moreover*,

(B) *For $n \in \mathbb{N}_0$, $\nu_{n\kappa}$ is $\lfloor n/(qab) \rfloor + 1$ or $\lfloor n/(qab) \rfloor$ according as* (n mod qab) *is representable* ($\in \mathfrak{I}_\kappa^{\rightarrow}$) *or is not* ($\in \mathfrak{I}_\kappa^{\mathrm{c}}$). ∎

Theorem 3.1 is equivalent to a part of the next result. Moreover, the author's paper [13] referred to above contains a result equivalent to the non-counting parts of this result in case $q = 2$ and $\kappa = -1$.

Theorem 3.11. *Given any integers m_a, m_b and*

$$\widetilde{n} := am_a + bm_b, \qquad \widetilde{N}_\kappa := \widetilde{n} + g - (q - 1 - \widetilde{\varepsilon}_\kappa)a \qquad (= \widetilde{n} + g \text{ if } q = 1)$$

(see (3.4) for g) *where*

$$\widetilde{\varepsilon}_\kappa \equiv (\kappa + 1 - m_a - m_b) \pmod{q}, \qquad 0 \leq \widetilde{\varepsilon}_\kappa < q,$$

all integers n, $n \geq \widetilde{n}$, which cannot be represented as integer linear combinations $xa + yb$ under assumptions (3.2) *and* (3.3) *and requirements $x \geq m_a$, $y \geq m_b$ and $x + y \equiv \kappa \pmod{q}$ are in the interval $[\widetilde{n}, \widetilde{N}_\kappa]$, their number is $(g+1)/2$ (which is independent of κ) and $\widetilde{N}_\kappa$ is the largest of them. On the other hand, the uniqueness of (x, y) is implied by either of the following inequalities: $m_a \leq x < m_a + qb$, $m_b \leq y < m_b + qa$.* ∎

4. Algorithms. Let $g(\mathcal{A}, q) < \infty$ and $t > 1$. Then two algorithms for evaluating the integers N_κ and Ω_κ can be presented. One, (W): a toroidal lattice-of-lights, extends Wilf's circle-of-lights [15], and another one, (N): a minimum-path algorithm, devised after Nijenhuis' [7].

The algorithm (W) processes consecutive integers $n \in \mathbb{N}_0$ using the following simple rule. ($n =$) 0 is 0-representable; any $n \in \mathbb{N}$ is $(\kappa+1)$-representable iff $n - a_i$ is κ-representable for some $i = 1, 2, \ldots, t$ where $\kappa \in L_q$. The corresponding information (0: no (or light off) or 1: yes (light on)) on n and any κ is put at position (r, κ), $r = (n \bmod a_t)$, of the resulting doubly cyclic (toroidal) 0-1 list of size qa_t. Additionally, RP$[\kappa]$, the number of κ-representable integers, is updated and the a_1th of consecutive κ-representable integers n is recorded as $N[\kappa]$. The process stops at the first n which is the a_1th of consecutive fully representable integers. Then output is $N_\kappa = N[\kappa] - a_1$ and $\Omega_\kappa = n + 1 - \mathrm{RP}[\kappa]$. Thus, since $t \le a_t$, space complexity is $O(qa_t)$. Since $g \ge a_1 - 1$, time complexity can be shown to be $O(tqg)$ or $O((t+q)g)$ depending on the (data structure dealing with 0-1 vectors and) implementation. As a by-product the algorithm gives the following inequality which is not sharp in general but, for $q = 1$, it improves on one due to Wilf:

$$g \le (qa_t - 2)a_t - 1 \quad \text{for } t \ge 2\,. \tag{4.1}$$

P r o o f. This is true if $t = 2$ (and $q = 1$). Else, if not all lights are on, each full sweep around the lattice increases the number of lights which are on because otherwise (it would only cause the rotation of lights and) g would be infinite, contrary to Theorem 1.2. We may stop at n such that at most $z := \lceil a_t/a_1 \rceil - 1$ lights are left off. Then $g \le n + za_1$. Since 1 is at $(0,0)$ due to the initial condition, the first sweep adds at least two new 1's (if $t > 2$ or $q > 1$). Thus, $n \le (qa_t - 2 - z)a_t$, whence the result follows. ∎

The bound (4.1) on g can be improved considerably. Erdős–Graham's important upper bound for $g(\mathcal{A}, 1)$ (see [3]) (whose simple proof can be found in Rödseth [10]) can be extended to any admissible q. Adapting Rödseth's argument to formula (2.10) with $m = qa_t$ gives the result. Let $q\mathcal{A}$ be the sum of q copies of the set $\mathcal{A}$, let $\mathcal{A}_0 = q\mathcal{A} \cup \{0\} - \{qa_t\}$, and let $h = 2\lfloor a_t/(t - 1 + 1/q) \rfloor$. Then

$$\begin{aligned} N_0(\mathcal{A}, q) &\le \max \sum_{b_j \in \mathcal{A}_0} y_j b_j - qa_t \qquad \text{with max over } y_j\text{'s from } \mathbb{N}_0 \text{ such that } \textstyle\sum y_j \le h \text{ and some of } y_j\text{'s are small,} \\ &\le \max_{x_i \in \mathbb{N}_0, \Sigma x_i \le qh,\, x_t < q} \sum_{i=1}^{t} x_i a_i - qa_t \\ &\le (qh - q + 1)a_{t-1} - a_t \quad (\text{for } \kappa = 0)\,, \end{aligned}$$

and

$$N_\kappa(\mathcal{A}, q) \le N_0(\mathcal{A}, q) + \kappa a_1, \qquad \kappa = 0, 1, \ldots, q-1\,,$$

whence

$$g(\mathcal{A},q) \leq 2qa_{t-1}\lfloor a_t/(t-1+1/q)\rfloor - (q-1)(a_{t-1}-a_1) - a_t \,. \tag{4.2}$$

Therefore g is $O(qa_t^2/t)$ (and so is Ω_κ for any κ because $\Omega_\kappa \leq g+1$). It can be seen that the bound (4.2) is sharp in the sense that, for each $q \geq 1$ and each $t \geq 2$, there is an $\mathcal{A}$ with $|\mathcal{A}| = t$, a_t large enough and $g(\mathcal{A},q) = \Theta(qa_t^2/t)$, Θ indicating the exact order of magnitude.

The algorithm (N) is more efficient but is also only pseudo-polynomial (i.e., a common bound on complexities is a polynomial in t, q and some a_i). The algorithm is based on generating all q^2a_1 integers $n_{r\kappa}$ as sums of generators a_i, see formulae (2.10)–(2.11) with $m = qa_1$, the smallest possible value of m. It maintains a heap (i.e., a binary tree) of κ-heaps whose entries are available sums which are put in increasing order along paths going from the root of the κ-heap, κ-heaps being similarly ordered by their roots. The algorithm starts by taking 0 as n_{00}. Next, if $n_{r\kappa}$ is identified (as the smallest available sum) and removed from the heap, the algorithm accommodates each of the sums $s = n_{r\kappa} + a_j$ in the $(\kappa+1)$-heap, i.e., inserts s as the $(r,\kappa+1)$-entry where $r = (s \bmod m)$ provided that the entry either has not appeared yet or is larger than s. Time of labour associated with each s is $O(\log_2(q^2a_1))$. The space and time complexities of the algorithm are $O(t + q^2a_1)$ and $O(tq^2a_1\log_2(q^2a_1))$, respectively. Our complexity estimates correct some of those by Nijenhuis [7].

For the set $\mathcal{A} = \{271, 277, 281, 283\}$ (dealt with by Wilf [15] for $q = 1$), our computer programs (W) and (N) found data presented in Table 1 for $q = 5, 3, 1$ in stated seconds on PC AT 386 (20 MHz) (A) and XT (8 MHz) (X), respectively. Notice that $q = 2$ (or any even q) is not allowed.

Table 1

		$q=5$		$q=3$		$q=1$	
	κ	N	Ω	N	Ω	N	Ω
	0	63 699	32 099	38 225	19 316	13 022	6533
	1	63 970	32 098	38 496	19 316		
	2	62 886	32 097	37 954	19 316		
	3	63 157	32 098				
	4	63 428	32 099				
Time (seconds):	$\begin{pmatrix}\mathrm{WA} & \mathrm{WX}\\ \mathrm{NA} & \mathrm{NX}\end{pmatrix}$	$\begin{pmatrix}9.12 & 65.14\\ 1.27 & 9.29\end{pmatrix}$		$\begin{pmatrix}4.12 & 28.95\\ 0.44 & 3.13\end{pmatrix}$		$\begin{pmatrix}0.94 & 6.37\\ 0.01 & 0.33\end{pmatrix}$	

Programs (N) and (W) can easily be supplemented so as to generate q^2a_1 integers $n_{r\kappa}^{(1)}$ (this is the smallest κ-representable integer in the residue class of r modulo qa_1), together with an explicit representation of each of them. This can yield all sets $\mathfrak{I}_\kappa^{\mathrm{c}}$ of omitted integers [and some representations of the remaining ones].

5. Problems and concluding remarks. A natural, though not easy, problem is to study the function $\kappa \mapsto (N_\kappa, \Omega_\kappa)$ in case $t \geq 3$. Partial questions can be of interest.

(a) Formulae (3.5) in case $t = 2$ and many examples of pairs $(\mathcal{A}, q)$ with $t \geq 3$ suggest that $N_\kappa \in \{g - ja_1 \mid j = 0, 1, \ldots, q-1\}$, $g = g(\mathcal{A}, q)$. Nevertheless, this is not the case in general. Namely, if a and b are relatively prime natural numbers, $a < b$ and $b - a$ is odd then, for $\mathcal{A} = \{a, b, a+b\}$ and $q = 2$, one has $g = g(\mathcal{A}, 2) = ab - a = N_{b \bmod 2}$ and $ab/2 = \Omega_\kappa$ for both $\kappa = 0, 1$; moreover,

$$N_{a \bmod 2} = \begin{cases} g + a - b = ab - b & \text{if } b < 2a\,, \\ g - a & \text{otherwise.} \end{cases}$$

(For the proof, use representations by the set $\{a, b\}$ with $q = 1$, see Section 3. In particular, all omitted integers there and half of the set $\{ia, jb \mid i = 0, \ldots, b-1; j = 1, \ldots, a-1\}$ can coincide with our κ-omitted integers.) It is easily seen, however, that all N_κ's are in the closed interval $[g - (q-1)a_1, g]$. In fact, use (2.7) and (2.10) with $m = qa_1$ to see that all integers $n_{r\kappa} + a_1$ are $(\kappa+1)$-representable and their residues modulo qa_1 form a complete system, whence

$$N_{\kappa+1} \leq N_\kappa + a_1 \quad \text{for all pairs } \kappa, \kappa+1 \text{ in } \mathbb{Z}\,.$$

Hence, the result follows.

(b) For $q = 1$, it is known [8] that $\Omega \geq (g+1)/2$. For any q, by using the transformation $n \mapsto g - n$ as in Proposition 3.5, one can prove $\max_\kappa \Omega_\kappa \geq (g+1)/2$ or, more generally,

$$\max_\kappa \Omega_\kappa + \min_\kappa \Omega_\kappa \geq g + 1\,.$$

Characterize all (or find more interesting examples of) pairs $(\mathcal{A}, q)$ with $t \geq 3$ such that $\Omega_\kappa = \text{const}$ on L_q $(q > 1)$ where possibly const $= (g+1)/2$ $(q \geq 1)$ (cp. $t = 2$ above or supersymmetric semigroups in [4] for $q = 1$).

(c) Characterize $(\mathcal{A}, q)$ with $q > 1$ and $t = |\mathcal{A}| > 2$ such that $\Omega_\kappa > g(\mathcal{A}, q)/2$ for all $\kappa \in L_q$. Characterize $\mathcal{A}$ such that this holds for all admissible q (or—on the contrary—does not hold for almost all such q). Determine the largest admissible integer q, denote it by $\xi(\mathcal{A})$, such that

$$\Omega_\kappa > g(\mathcal{A}, q)/2 \quad \text{for all } \kappa \in L_q\,. \tag{5.1}$$

Let $\xi'(\mathcal{A})$ be the largest integer k such that (5.1) holds for all admissible $q \leq k$. Notice that $\xi' \leq \xi$ for all $t \geq 2$. If $t = 1$ then $\xi' = \infty$ and $\xi = 1$ (and $\mathcal{A} = \{1\}$). Characterize $\mathcal{A}$ with $\xi' = \xi$.

In what follows, $\mathcal{A} = \mathcal{A}_{t,a} := \{a, a+1, \ldots, a+t-1\}$ with $t \geq 2$, a set of consecutive generators (dealt with in [8]) with t elements, a being the smallest. One can see now that $\xi' = \infty = \xi$ iff $t-1$ divides a, iff $\Omega_\kappa = \text{const}$ on L_q for each q; moreover, const $= (g+1)/2$ iff $a = 1 = q$ or $q = 2$ and $t-1 \mid a-1$, or finally, $t-1 \mid a-2$ with the restriction that $q = 1$ if $t \geq 4$. On the other hand, for $t \geq 3$, we have $\xi' = t$ and $\xi = a$ if $t-1 \mid a-1$ unless $a = 1$ and then $\xi' = 2 = \xi$.

Acknowledgments. The author is indebted to his daughter Anna /Sliz of Toronto and Dr. Paul Vaderlind of Stockholm for providing him with copies of Sylvester's contribution [14(a)]. He also thanks Dr. Anna Rycerz for her calling the author's attention to Nijenhuis' paper [7]. Remarks of Prof. G. Hofmeister which resulted in improving the contents of the paper are gratefully acknowledged. Partial support of Polish KBN Grant Nr 2 P301 050 03 is acknowledged.

References

[1] J. Bond, *Calculating the general solution of a linear Diophantine equation*, Amer. Math. Monthly 74 (1967), 955–957.

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

[3] P. Erdős and R. L. Graham, *On a linear diophantine problem of Frobenius*, Acta Arith. 21 (1972), 399–408.

[4] R. Fröberg, C. Gottlieb and R. Häggkvist, *On numerical semigroups*, Semigroup Forum 35 (1987), 63–83.

[5] S. Kertzner, *The linear diophantine equation*, Amer. Math. Monthly 88 (1981), 200–203.

[6] S. Morito and H. M. Salkin, *Finding the general solution of a linear diophantine equation*, Fibonacci Quart. 17 (1979), 361–368.

[7] A. Nijenhuis, *A minimal-path algorithm for the "money changing problem"*, Amer. Math. Monthly 86 (1979), 832–834.

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

[9] G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis I*, Springer, 1925 [revised and enlarged: *Problems and Theorems in Analysis I*, Springer, 1978, pp. 174 and 180 [Problems I 9, I 26–27].

[10] Ö. J. Rödseth, *Two remarks on linear forms in non-negative integers*, Math. Scand. 51 (1982), 193–198.

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

[12] —, *The local postage stamp problem*, Part 1: General theory, Ch. II; Part 3: Supplementary volume, Supplement to Ch. II; preprints, University of Bergen, 42 (1986) and 57 (1990), resp.

[13] Z. Skupień, *Exponential constructions of some nonhamiltonian minima*, in: Proc. 4th CS Sympos. on Combinat., Graphs and Complexity (held in Prachatice 1990), J. Nešetřil and M. Fiedler (eds.), Ann. Discrete Math. 51, Elsevier, 1992, 321–328.

[14] J. J. Sylvester, [Problem] 7382 (and *Solution by W. J. Curran Sharp*), The Educational Times 37 (1884), 26; reprinted in (a): Mathematical Questions, with their Solutions, from the "Educ. Times", with Many Papers (...) 41 (1884), 21.

[15] H. S. Wilf, *A circle-of-lights algorithm for the "money-changing problem"*, Amer. Math. Monthly 85 (1978), 562–565.

INSTITUTE OF MATHEMATICS AGH
ACADEMY OF MINING AND METALLURGY
MICKIEWICZA 30
30-059 KRAKÓW, POLAND

INSTITUTE OF COMPUTER SCIENCE
JAGIELLONIAN UNIVERSITY
NAWOJKI 11
30-072 KRAKÓW, POLAND

Received on 20.11.1992
and in revised form on 25.3.1993 (2346)