NON-NEGATIVE INTEGER LINEAR CONGRUENCES

JOHN C. HARRIS AND DAVID L. WEHLAU

Abstract. We consider the problem of describing all non-negative integer solutions to a linear congruence in many variables. This question may be reduced to solving the congruence $x_1+2x_2+3x_3+\ldots+(n-1)x_{n-1} \equiv 0 \pmod{n}$ where $x_i \in \mathbb{N} = \{0,1,2,\ldots\}$. We consider the monoid of solutions of this equation and prove equivalent two conjectures of Elashvili concerning the structure of these solutions. This yields a simple algorithm for generating most (conjecturally all) of the high degree indecomposable solutions of the equation.

1. Introduction

Let $\mathbb{N} := \{0,1,2,\ldots\}$ denote the non-negative integers and let n be a positive integer. We consider the problem of finding all non-negative integer solutions to a linear congruence

$$w_1x_1 + w_2x_2 + \ldots + w_rx_r \equiv 0 \pmod{n}$$

where the coefficients $w_1, w_2, \ldots, w_n$ are all integers. By a non-negative integer solution, we of course mean an r-tuple $A = (a_1, a_2, \ldots, a_r) \in \mathbb{N}^r$ such that $w_1a_1+w_2a_2+\ldots+w_ra_r \equiv 0 \pmod{n}$.

As one would expect from such a basic question, this problem has a rich history. The earliest published discussion of this problem known to the authors was by Carl W. Strom in 1931 ([St1]). A number of mathematicians have considered this problem. Notably Paul Erdös, Jacques Dixmier, Jean-Paul Nicolas ([DEN]), Victor Kac, Richard Stanley ([K]) and Alexander Elashvili ([E]).

V. Tsiskaridze ([T]) performed a series of computer computations for all values of $n < 65$. Partially inspired by these computer calculations Elashvili made a number of fascinating conjectures concerning the structure of the monoid of solutions. Here we prove two of these conjectures are equivalent. This allows us to construct most (conjecturally all) of the "large" indecomposable solutions by a very simple algorithm.

Also of interest are the papers [EJ1], [EJ2] by Elashvili and Jibladze and [EJP] by Elashvili, Jibladze and Pataraia where the "Hermite reciprocity" exhibited by the monoid of solutions is examined.

2. Preliminaries

We take $\mathbb{N} = \{0,1,2,\ldots\}$ and let n be a positive integer. Consider the linear congruence

$$w_1x_1 + w_2x_2 + \ldots + w_rx_r \equiv 0 \pmod{n} \tag{2.0.1}$$

2000 *Mathematics Subject Classification.* Primary 11D79.

Research partially supported by NSERC and ARP.

March 2, 2005.

where $w_1, w_2, \ldots, w_r \in \mathbb{Z}$ and $x_1, x_2, \ldots, x_n$ are unknowns. We want to describe all solutions $A = (a_1, a_2, \ldots, a_{n-1}) \in \mathbb{N}^r$ to this congruence.

Clearly all that matters here is the residue class of the w_i modulo n and thus we may assume that $0 \le w_i < n$ for all i. Also if one of the w_i is divisible by n then the equation imposes no restriction whatsoever on x_i and thus we will assume that $1 \le w_i < n$ for all i.

If $w_1 = w_2$ then we may replace the single equation (2.0.1) by the pair of equations

$$w_1 y_1 + w_3 x_3 + \ldots + w_r x_r \equiv 0 \pmod{n} \qquad \text{and} \qquad x_1 + x_2 = y_1.$$

Thus we may assume that the w_i are distinct and so we have reduced to the case where $\{w_1, \ldots, w_r\}$ is a subset of $\{1, 2, ..., n-1\}$. Now we consider

$$x_1 + 2x_2 + 3x_3 + \ldots + (n-1)x_{n-1} \equiv 0 \pmod{n} \tag{2.0.2}$$

The solutions to (2.0.1) are the solutions to (2.0.2) with $x_i = 0$ for all $i \notin \{w_1, \ldots, w_r\}$. Hence to solve our original problem it suffices to find all solutions to Equation (2.0.2).

3. Monoid of Solutions

We let M denote the set of all solutions to Equation (2.0.2),

$$M := \{\vec{x} \in \mathbb{N}^{n-1} \mid x_1 + 2x_2 + \ldots + (n-1)x_{n-1} \equiv 0 \pmod{n}\} .$$

Clearly M forms a monoid under componentwise addition, i.e., M is closed under this addition and contains an additive identity, the *trivial solution* $\mathbf{0} = (0, 0, \ldots, 0)$.

In order to describe all solutions of (2.0.2) explicitly we want to find the set of minimal generators of the monoid M. We denote this set of generators by IM. We say that a non-trivial solution $A \in M$ is *decomposable* if A can be written as non-trivial sum of two other solutions: $A = B + C$ where $B, C \neq \mathbf{0}$. Otherwise we say that A is *indecomposable* (also called *non-shortenable* in the literature). Thus IM is the set of indecomposable solutions.

We define the *degree* (also called the *height* in the literature) of a solution $A = (a_1, a_2, \ldots, a_{n-1}) \in M$ by $\deg(A) = a_1 + a_2 + \ldots + a_{n-1}$ and we denote the set of solutions of degree k by $M(k) := \{A \in M \mid \deg(A) = k\}$. Similarly, we let $IM(k)$ denote the set of indecomposable solutions of degree k: $IM(k) = IM \cap M(k)$.

Gordan's Lemma [G] states that there are only finitely many indecomposable solutions, i.e., that IM is finite. This is also easy to see directly as follows. The extremal solutions $E_1 := (n, 0, \ldots, 0)$, $E_2 := (0, n, 0, \ldots, 0)$, $\ldots$, $E_{n-1} := (0, 0, \ldots, 0, n)$ show that any indecomposable solution, $(a_1, a_2, \ldots, a_n)$ must satisfy $a_i \le n$ for all i.

In fact, Emmy Noether [N] showed that if A is indecomposable then $\deg(A) \le n$. Furthermore A is indecomposable with $\deg(A) = n$ if and only if A is an extremal solution E_i with $\gcd(i, n) = 1$. For a simple proof of these results see [S].

We define the *multiplicity* of a solution A, denoted $m(A)$ by

$$m(A) := \frac{a_1 + 2a_2 + \ldots + (n-1)a_{n-1}}{n} .$$

Example 3.1. Consider $n = 4$. Here $IM = \{A_1 = (4, 0, 0), A_2 = (0, 2, 0), A_3 = (0, 0, 4), A_4 = (1, 0, 1), A_5 = (2, 1, 0), A_6 = (0, 1, 2)\}$. The degrees of these solutions are $4, 2, 4, 2, 3, 3$ respectively and the multiplicities are $1, 1, 3, 1, 1, 2$ respectively.

Let $F(n)$ denote the number of indecomposable solutions to Equation (2.0.2), $F(n) := \#IM$. Victor Kac [K] showed that the number of minimal generators for the ring of invariants of $SL(2, \mathbb{C})$ acting on the space of binary forms of degree d exceeds $F(d-2)$ if d is odd. Kac credits Richard Stanley for observing that if A is a solution of multiplicity 1 then A is indecomposable. This follows from the fact that the multiplicity function m is a homomorphism of monoids from M to $\mathbb{N}$ and 1 is indecomposable in $\mathbb{N}$. Kac also observed that the extremal solutions E_i (defined in Section 3 above) with $\gcd(i,n) = 1$ are also indecomposable. This gave Kac the lower bound $F(n) \geq p(n) + \phi(n) - 1$ where $p(n)$ denotes the number of partitions of n.

Much of the interest has centred on studying the asymptotics of the function $F(n)$.

Dixmier, Erdös and Nicholas studied the function $F(n)$ and significantly improved Kac's lower bound ([DEN]). They were able to prove that

$$\lim_{n\to\infty} \inf F(n) \cdot \left[\frac{n^{1/2}}{\log n \cdot \log\log n} p(n)\right]^{-1} > 0 \ .$$

Dixmier and Dixmier and Nicholas have also published a sequence of papers ([D1, D2, D3, D4, D5, D6, DN1, DN2, DN3]) which give more information about the asymptotics of $F(n)$. The lower bound quoted above from [DEN] is established by considering only solutions of level one (the level of a solution is defined in the next section). Tsiskaridze ([T]) performed a number of computer calculations which determined the values of $F(n)$ for $n < 65$. These computations show that the solutions of level one constitute an increasingly smaller proportion of all solutions as n increases. This suggests that the asymptotics of $F(n)$ may be qualitatively bigger than this lower bound.

4. The Automorphism Group

Let $G := Aut(\mathbb{Z}/n\mathbb{Z})$. The order of G is given by $\phi(n)$ where ϕ is the Euler phi function, also called the totient function. The elements of G may be represented by the $\phi(n)$ positive integers less than n and relatively prime to n. Each such integer g induces a permutation, $\sigma = \sigma_g$, of $\{1, 2, \ldots, n-1\}$ given by $\sigma(i) \equiv gi \pmod{n}$. Let $A = (a_1, a_2, \ldots, a_{n-1}) \in M$, i.e., $a_1 + 2a_2 + \ldots + (n-1)a_{n-1} \equiv 0 \pmod{n}$. Multiplying this equation by g gives $(g)a_1 + (2g)a_2 + (3g)a_3 + \ldots + (gn - g)a_{n-1} \equiv 0 \pmod{n}$. Reducing these new coefficients modulo n and reordering this becomes $a_{\sigma^{-1}(1)} + 2a_{\sigma^{-1}(2)} + \ldots + (n-1)a_{\sigma^{-1}(n-1)} \equiv 0 \pmod{n}$. Thus if $A = (a_1, a_2, \ldots, a_{n-1}) \in M$ then $g \cdot A := (a_{\sigma^{-1}(1)}, a_{\sigma^{-1}(2)}, \ldots, a_{\sigma^{-1}(n-1)}) \in M$. If $g \in G$ and $A = B + C$ is a decomposable solution, then $g \cdot A = g \cdot B + g \cdot C$ and therefore G preserves IM and each $IM(k)$.

The action of G was used by Dixmier, Erdös and Nicolas in [DEN]. Furthermore, Elashvili and Jibladze proved in [EJ1] that this group is the *full* automorphism group of M.

Let $g \in G$. Since $g \cdot A$ is a permutation of A, the action of G on M preserves degree, and thus G also acts on each $M(k)$ for $k \in \mathbb{N}$. Note however that the action does not preserve multiplicities in general.

Example 4.1. Consider $n = 9$. Here G is represented $\{1, 2, 4, 5, 7, 8\}$ and the corresponding six permutations of $\mathbb{Z}/9\mathbb{Z}$ are given by $\sigma_1 = e$, $\sigma_2 = (1,2,4,8,7,5)(3,6)$, $\sigma_4 = \sigma_2^2 = (1,4,7)(2,8,5)(3)(6)$, $\sigma_5 = \sigma_2^5 = (1,5,7,8,4,2)(3,6)$, $\sigma_7 = \sigma_2^4 = (1,7,4)(2,5,8)(3)(6)$

and $\sigma_8 = \sigma_2^3 = (1,8)(2,7)(3,6),(4,5)$. Thus, for example, $2\cdot(a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8) = (a_5,a_1,a_6,a_2,a_7,a_3,a_8,a_4)$ and $4\cdot(a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8) = (a_7,a_5,a_3,a_1,a_8,a_6,a_4,a_2)$.

Note that G always contains the element $n-1$ which is of order 2 and which we also denote by -1. This element induces the permutation σ_{-1} which acts via $-1\cdot(a_1,a_2,\ldots,a_{n-1}) = (a_{n-1},a_{n-2},\ldots,a_3,a_2,a_1)$.

It is tempting to think that the G-orbits of the multiplicity 1 solutions would comprise all elements of IM. This is not true however. Consider $n=6$. Then G is a group of order 2, $G=\{1,-1\}$. The solutions $A_1=(1,0,1,2,0)$ and $A_2=-1\cdot A_1=(0,2,1,0,1)$ are both indecomposable and both have multiplicity 2.

We define the *level* of a solution A, denoted $\ell(A)$, by $\ell(A)=\min\{m(g(A)) \mid g\in G\}$.

Note that $m(A)+m(-1\cdot A)=\deg(A)$. This implies $2\sum_{B\in G\cdot A} m(B) = \deg(A)\#(G\cdot A)$, i.e., that the average multiplicity of the elements in the G-orbit of A is half the degree of A.

5. Elashvili's conjectures

Elashvili ([E]) made a number of interesting and deep conjectures concerning the structure of the solutions to Equation (2.0.2). Here we will consider two of his conjectures. In order to state these conjectures we will denote by $p(t)$ the number of partitions of the integer t. We also use $\lfloor n/2\rfloor$ to denote the greatest integer less than or equal to $n/2$ and define $\lceil n/2\rceil := n-\lfloor n/2\rfloor$.

Conjecture 1: If $A\in IM(k)$ where $k\geq \lfloor n/2\rfloor+2$ then $\ell(A)=1$.

Conjecture 2: If $k\geq\lfloor n/2\rfloor+2$ then $IM(k)$ contains exactly $\phi(n)p(n-k)$ elements.

Here we prove these two conjectures are equivalent. Furthermore we will show that if $k\geq\lceil n/2\rceil+1$ then every orbit of level 1 contains exactly one multiplicity 1 element and has size $\phi(n)$. Thus if $k\geq\lceil n/2\rceil+1$ then $IM(k)$ contains exactly $\phi(n)p(n-k)$ level 1 solutions.

This gives a very simple and fast algorithm to generate all the level 1 solutions whose degree, k, is at least $\lceil n/2\rceil+1$ as follows. For each partition, $n-k=b_1+b_2+\cdots+b_s$, of $n-k$ put $b_{s+1}=\cdots=b_k=0$ and define $c_i:=b_i+1$ for $1\leq i\leq k$. Then define A via $a_i:=\#\{j : c_j=i\}$. This constructs all multiplicity 1 solutions if $k\geq\lceil n/2\rceil+1$. Now use the action of G to generate the $\phi(n)$ solutions in the orbit of each such multiplicity 1 solution.

If the above conjectures are true then this algorithm rapidly produces all elements of $IM(k)$ for $k\geq\lfloor n/2\rfloor+2$. This is surprising, since without relying on the conjectures, the computations required to generate the elements of $IM(k)$ become increasingly hard as k increases.

6. Proof of Equivalence of the Conjectures

Before proceeding further we want to make a change of variables. Suppose then that $A\in M(k)$. We interpret the solution A as a partition of the integer $m(A)n$ into k parts. This partition consists of a_1 1's, a_2 2's,…, and a_{n-1} (n-1)'s. We write this partition as an *unordered* sequence (or multi-set) of k numbers:

$$[y_1,y_2,\ldots,y_k] = [\underbrace{1,1,\ldots,1}_{a_1},\underbrace{2,2,\ldots,2}_{a_2},\ \ldots\ ,\underbrace{(n-1),(n-1),\ldots,(n-1)}_{a_{n-1}}]$$

The integers $y_1, y_2, \ldots, y_k$ with $1 \leq y_i \leq n-1$ for $1 \leq i \leq k$ are our new variables for describing A. Given $[y_1, y_2, \ldots, y_k]$ we may easily recover A since $a_i := \#\{j \mid y_j = i\}$.

We have $y_1 + y_2 + \ldots + y_k = m(A)n$.

Notice that the sequence $y_1 - 1, y_2 - 1, \ldots, y_k - 1$ is a partition of $m(A)n - k$. Furthermore, every partition of $m(A)n - k$ arises from a partition of $m(A)n$ into k parts in this manner.

The principal advantage of this new description for elements of M is that it makes the action of G on M more tractable. To see this let $g \in G$ be a positive integer less than n and relatively prime to n. Then $g \cdot [y_1, y_2, \ldots, y_k] = [gy_1 \pmod{n}, gy_2 \pmod{n}, \ldots, gy_k \pmod{n}]$.

Now we proceed to give our proof of the equivalence of Elashvili's conjectures.

Proposition 6.1. *Let $A \in M(k)$ and let $1 \leq g \leq n-1$ where g is relatively prime to n represent an element of G. Write $B = g \cdot A$, and $u = m(A)$ and $v = m(B)$. If $k \geq gu - v$ then $ug^2 - (k+u+v)g + v(n+1) \geq 0$.*

Proof. Write $A = [y_1, y_2, \ldots, y_k]$ where $y_1 \geq y_2 \geq \ldots \geq y_k$. For each i with $1 \leq i \leq k$ we use the division algorithm to write $gy_i = q_i n + r_i$ where $q_i \in \mathbb{N}$ and $0 \leq r_i < n$. Then $B = [r_1, r_2, \ldots, r_k]$. Note that the r_i may fail to be in decreasing order and also that no r_i can equal 0.

Now $gun = g(y_1 + y_2 + \ldots + y_k) = (q_1 n + r_1) + (q_2 n + r_2) + \ldots + (q_k n + r_k) = (q_1 + q_2 + \ldots + q_k)n + (r_1 + r_2 + \ldots + r_k)$ where $r_1 + r_2 + \ldots + r_k = vn$.

Therefore, $gu = (q_1 + q_2 + \ldots + q_k) + v$.

Since $y_1 \geq y_2 \geq \ldots \geq y_k$, we have $q_1 \geq q_2 \geq \ldots \geq q_k$. Therefore from $gu - v = \sum_{i=1}^{k} q_i$ we conclude that $q_i = 0$ for all $i > gu - v$. Therefore

$$\begin{aligned}
\sum_{i=1}^{gu-v} gy_i &= g\sum_{i=1}^{gu-v} [(y_i - 1) + 1] \\
&= g\sum_{i=1}^{ug-v} (y_i - 1) + g(gu - v) \\
&\leq g\sum_{i=1}^{k} (y_i - 1) + g(gu - v) \\
&= g(un - k) + g^2 u - gv
\end{aligned}$$

Also

$$\begin{aligned}
\sum_{i=1}^{gu-v} gy_i &= \sum_{i=1}^{gu-v} (q_i n + r_i) \\
&= (gu - v)n + \sum_{i=1}^{gu-v} r_i \\
&\geq gun - vn + gu - v
\end{aligned}$$

Combining these formulae we obtain the desired quadratic condition $ug^2 - (k + u + v)g + v(n+1) \geq 0$. □

Now we specialize to the case $u = v = 1$. Thus we are considering a pair of solutions A and $B = g \cdot A$ both of degree k and both of multiplicity 1.

Lemma 6.2. *Let $A \in M(k)$ be a solution of multiplicity 1. Write $A = [y_1, y_2, \dots, y_k]$ where $y_1 \geq y_2 \geq \cdots \geq y_k$. If $k \geq \lfloor n/2 \rfloor + 2$ then $y_{k-2} = y_{k-1} = y_k = 1$. If $k \geq \lceil n/2 \rceil + 1$ then $y_{k-1} = y_k = 1$.*

Proof. First suppose that $k \geq \lfloor n/2 \rfloor + 2$ and assume, by way of contradiction, that $y_{k-2} \geq 2$. Then $n = (y_1+y_2+\ldots+y_{k-2})+y_{k-1}+y_k \geq 2(k-2)+1+1 \geq 2\lfloor n/2 \rfloor+2 \geq n+1$.

Similarly if $k \geq \lceil n/2 \rceil + 1$ we assume, by way of contradiction, that $y_{k-1} \geq 2$. Then $n = (y_1 + y_2 + \ldots + y_{k-1}) + y_k \geq 2(k-1) + 1 \geq 2(\lceil n/2 \rceil) + 1 \geq n + 1$. □

Proposition 6.3. *Let $A \in M(k)$ be a solution of multiplicity 1 where $k \geq \lceil n/2 \rceil + 1$. Then the G-orbit of A contains no other element of multiplicity 1. Furthermore, G acts faithfully on the orbit of A and thus this orbit contains exactly $\phi(n)$ elements.*

Proof. Let $B = g \cdot A$ where $1 \leq g \leq n - 1$ and g represents an element of G. Further suppose B has multiplicity 1. Lemma 6.2 implies that $B = g \cdot A = [r_1, r_2, \dots, r_{k-2}, g, g]$. Since B has multiplicity 1, we have $n = r_1 + r_2 + \ldots + r_{k-2} + g + g \geq 2g + k - 2$ and thus $g \leq (n - k + 2)/2 \leq k/2$. From this we see that the hypothesis $k \geq gu - v$ is satisfied. Therefore by Proposition 6.1, g and k must satisfy the quadratic condition

$$g^2 - (k + 2)g + (n + 1) \geq 0 \ \ .$$

Let f denote the real valued function $f(g) = g^2 - (k + 2)g + (n + 1)$. Then $f(1) = n - k \geq 0$ and $f(2) = n + 1 - 2k < 0$ and thus f has a root in the interval [1,2). Since the sum of the two roots of f is $k + 2$ we see that the other root of f lies in the interval $(k, k + 1]$. Thus our quadratic condition implies that either $g \leq 1$ or else $g \geq k + 1$. But we have already seen that $g \leq k/2$ and thus we must have $g = 1$ and so $A = B$.

This shows that the G-orbit of A contains no other element of multiplicity 1. Furthermore, G acts faithfully on this orbit and thus it contains exactly $\phi(n)$ elements. □

Remark 6.4. Of course the quadratic condition $ug^2 - (k + u + v)g + v(n + 1) \geq 0$ can be applied to cases other than $u = v = 1$. For example, taking $u = v = 2$ one can show that a solution of degree k (and level 2) with $k \geq (2n + 8)/3$ must have an orbit of size $\phi(n)$ or $\phi(n)/2$.

References

[D1] Jacques Dixmier, *Sur le nombre d'invariants fondamentaux des formes binaires. (French) [On the number of fundamental invariants of binary forms]*, C. R. Acad. Sci. Paris Sr. I Math. **305** (1987), no. 8, 319–322.

[D2] Jacques Dixmier, *Sur les sous-sommes d'une partition. (French) [On the subsums of a partition]*, Mém. Soc. Math. France (N.S.) No. 35, (1988), 70 pp. (1989).

[D3] Jacques Dixmier, *Sur les sous-sommes d'une partition, II (French) [On the subsums of a partition, II]*, Portugal. Math. 46 (1989), no. 2, 137–154.

[D4] Jacques Dixmier, *Sur les sous-sommes d'une partition, III (French) [On the subsums of a partition, III]*, Bull. Sci. Math. (2) 113 (1989), no. 2, 125–149.

[D5] Jacques Dixmier, *Errata: Sur les sous-sommes d'une partition, III (French) [Errata: On the subsums of a partition, III]* Bull. Sci. Math. 113 (1989), no. 4, 505.

[D6] Jacques Dixmier, *Partitions avec sous-sommes interdites (French) [Partitions with forbidden subsums]*, Algebra, groups and geometry. Bull. Soc. Math. Belg. Sr. A 42 (1990), no. 3, 477–500.

[DEN] Jacques Dixmier, Paul Erdös and Jean-Louis Nicolas, *Sur le nombre d'invariants fondamentaux des formes binaires. (French) [On the number of fundamental invariants of binary forms]*, C. R. Acad. Sci. Paris Sr. I Math. **305** (1987), no. 8, 319–322.

[DN1] Jacques Dixmier and Jean-Louis Nicolas, *Partitions without small parts*, Number theory, Vol. I (Budapest, 1987), 9–33, Colloq. Math. Soc. Jnos Bolyai, 51, North-Holland, Amsterdam, 1990.

[DN2] Jacques Dixmier and Jean-Louis Nicolas, *Partitions sans petits sommants. (French) [Partitions with no small summands]* A tribute to Paul Erds, 121–152, Cambridge Univ. Press, Cambridge, 1990.

[DN3] Jacques Dixmier and Jean-Louis Nicolas, *Parit de certains nombres de partitions. (French) [Parity of certain numbers of partitions]*, Travaux mathmatiques. Fasc. XIII, 93–153, Trav. Math., XIII, Centre Univ. Luxembourg, Luxembourg, 2002.

[E] A. Elashvili, *Private Communication*, 1994.

[EJ1] A. Elashvili and M. Jibladze, *Hermite reciprocity for the regular representations of cyclic groups*, Indag. Math. (N.S.) **9** (1998), no. 2, 233–238.

[EJ2] A. Elashvili and M. Jibladze, *"Hermite reciprocity" for semi-invariants in the regular representations of cyclic groups*, Proc. A. Razmadze Math. Inst. **119** (1999), 21–24.

[EJP] A. Elashvili, M. Jibladze and D. Pataraia, *Combinatorics of necklaces and "Hermite reciprocity"*, J. Algebraic Combin. **10** (1999), no. 2, 173–188.

[G] P. Gordan, *Über die Auflösung linearer Gleichungen mit reellen Coefficienten*, Math. Ann. **6** (1873), 23–28.

[K] Victor G. Kac, *Root systems, representations of quivers and invariant theory*, Invariant theory (Montecatini, 1982), 74–108, Lecture Notes in Math., **996**, Springer, Berlin, 1983.

[N] E. Noether *Der endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1916) 89–92.

[S] B. Schmid, *Finite Groups and Invariant Theory*, Topics in Invariant Theory (M.-P. Malliavin Editor), 35–66, Lecture Notes in Math., **1478**, Springer-Verlag, Berlin Heidelberg New York, 1991.

[St1] Carl W. Strom, *On complete systems under certain finite groups*, Bull. Amer. Math. Soc. **37** (1931) 570–574.

[St2] Carl W. Strom, *Complete systems of invariants of the cyclic groups of equal order and degree*, Proc. Iowa Acad. Sci. **55**, (1948) 287–290.

[T] V. Tsiskaridze, *Unpublished.*

30 Marlow Avenue, Toronto, Ontario, Canada M4J 3T9
E-mail address: harrisj@pathcom.com

Department of Mathematics and Computer Science, Royal Military College
PO Box 17000 STN Forces, Kingston, Ontario, Canada K7K 7B4
E-mail address: wehlau@rmc.ca