Proc. Indian Acad. Sci. (Math. Sci.), Vol. 104, No. 3, August 1994, pp. 549–555.

Row-reduction and invariants of Diophantine equations

N J WILDBERGER
School of Mathematics, University of New South Wales, Sydney 2052 Australia

MS received 30 March 1993; revised 9 February 1994

Abstract. To any Diophantine equation with integral coefficients we associate a finitely generated abelian group. The analysis of this group by row-reduction generally leads to simpler equations which are equivalent to the original but often dramatically easier to solve. This method of studying equations is useful over finite fields as well as over **Q**. Some applications and an example are discussed.

Keywords. Diophantine equations; row-reduction.

Introduction

Let f be a polynomial in the variables $X_1,\ldots,X_n$ with integral coefficients and consider the problem of finding all rational solutions of the equation

$$f(X_1,\ldots,X_n)=0. \tag{1}$$

Historically work on this problem has focused on particular equations of low degree with a few variables. General results that apply to all polynomials or even large classes of polynomials are few and are mostly concerned with the existence of non-zero solutions, where a solution $(s_1,\ldots,s_n)$ of (1) is called non-zero if at least one of the s_i is non-zero.

For an arbitrary large non-homogeneous polynomial f, however, it would seem that this basic problem is hopelessly difficult. We hope to show in this paper that this is not so; specifically we will present a method to modify the general equation (1) which often results in a drastic simplification of the equation and sometimes to a complete determination of all solutions. It will be seen that this method can be useful when trying to solve (1) over any field, and in particular over a finite field it is surprisingly powerful considering its simplicity.

Before presenting the method in detail, we make a comment on the relevance of non-zero solutions of (1). Consider the following elementary method of obtaining such solutions. Suppose that $n \geqslant 2$. If one of the variables X_i occurs in each term of f, set $X_i=0$ and let the other variables be arbitrary with at least one of them non-zero; this is a non-zero solution. Otherwise, pick one of the variables, set it to zero and examine the resulting equation for a variable which occurs in each term. If one occurs and the number of variables still exceeds 1, then we have a non-zero solution as before, otherwise we continue. We eventually get a non-zero solution or arrive at an equation with exactly one variable. If we can find a non-zero solution to this one-variable equation, we have a non-zero solution to the original equation.

We see that if the polynomial $f(X_1,\ldots,X_n)$ has k terms with $k<n$, then (1) has a non-zero solution. The reason is as follows. If after setting a variable to zero the total number of variables has decreased by 2 or more then a non-zero solution may be obtained immediately. Otherwise at each stage of the above algorithm the number of variables exceeds the number of terms, so we can never reach a one-variable equation and must arrive instead at a non-zero solution.

These remarks show that non-zero solutions may often exist for trivial reasons. Define therefore a solution $(s_1,\ldots,s_n)$ of (1) to be non-trivial if all of the s_i are non-zero. Henceforth in this paper the term solution refers to non-trivial solution.

1. The method

Write

$$f(X_1,\ldots,X_n)=\sum_{j=1}^{k} c_j \prod_{i=1}^{n} X_i^{\alpha_{ij}} \tag{2}$$

where c_j are non-zero integers and α_{ij} are non-negative integers. Introduce a new variable X_0, multiply f by X_0, and write $f(X_0,X_1,\ldots,X_n)=X_0 f(X_1,\ldots,X_n)$. To each variable X_i associate the power vector $\alpha_i=(\alpha_{i1},\ldots,\alpha_{ik})\in\mathbf{Z}^k$. The power vector of X_0 is just $\alpha_0=(1,\ldots,1)$. Let $A_f\in M((n+1)\times k,\mathbf{Z})$ be the matrix whose rows are $\alpha_0,\alpha_1,\ldots,\alpha_n$ in that order. Call A_f the power matrix of f. Let G_f be the subgroup of the abelian group $\mathbf{Z}^k$ generated by the vectors $\alpha_0,\alpha_1,\ldots,\alpha_n$. Call G_f the power group of f. Finally let $c=(c_1,\ldots,c_k)$ and call it the coefficient vector of f.

These definitions are closely connected to the only general change of variable that leaves k unchanged. Introduce new variables $Y_0, Y_1,\ldots, Y_m$ and suppose that

$$X_j=\prod_{i=0}^{m} Y_i^{\beta_{ij}} \qquad 0\leqslant j\leqslant n \tag{3}$$

for some constants $\beta_{ij}\in\mathbf{Z}$. Let $B\in M((m+1)\times(n+1),\mathbf{Z})$ be defined by $B=[\beta_{ij}]$, $0\leqslant i\leqslant m, 0\leqslant j\leqslant n$.

Then

$$\begin{aligned} f(X_0,X_1,\ldots,X_n)&=\sum_{j=1}^{k} c_j \prod_{i=0}^{n}\left(\prod_{l=0}^{m} Y_l^{\beta_{li}}\right)^{\alpha_{ij}} \\ &=\sum_{j=1}^{k} c_j \prod_{l=0}^{m} Y_l^{\gamma_{lj}} \\ &=h(Y_0,Y_1,\ldots,Y_m). \end{aligned} \tag{4}$$

If $A_h=[\gamma_{lj}]\in M((m+1)\times k,\mathbf{Z})$ is the power matrix of h, then (4) shows that

$$A_h=BA_f. \tag{5}$$

If B has a (generalized) left inverse $B'\in M((n+1)\times(m+1),\mathbf{Z})$, then the change of variable (3) is invertible and $A_f=B'A_h$.

Note that h has exactly k terms and the same coefficient vector as f. Any solution of

$h(Y_0, Y_1, \ldots, Y_m) = 0$ immediately gives us via (3) a solution of $f(X_0, X_1, \ldots, X_n) = 0$. This suggests that we introduce a partial ordering on the set of all polynomials of k terms with coefficient vector c. If f, h are two such polynomials related as above, then we will write $h < f$. If $h < f$ and $f < h$ then we will say that f and h are equivalent and write $f \sim h$. If G_f and G_h are the power groups of f and h respectively, then $h < f$ if and only if $G_h \subset G_f$. Thus $h \sim f$ if and only if $G_h = G_f$ and so the equivalence class of a polynomial f of k terms is determined completely by its coefficient vector c and its power group G_f.

Now any non-trivial subgroup G_f of $\mathbf{Z}^k$ must be free abelian of rank $(r+1) \leqslant k$ for some non-negative integer r which we call the rank of f. If $r < n$ then some of the variables $X_i, i > 0$ are redundant in the sense that f is equivalent to a polynomial h with strictly fewer variables. This will necessarily occur, for example, if $k < n$.

To determine G_f as precisely as possible, we may row reduce the power matrix A_f. Since we are dealing with integral matrices, we are allowed to interchange rows, multiply a row by -1, or add a multiple of one row to another row. We may also permute columns, since this corresponds to relabelling the terms of f, as long as we remember that the coefficient vector c also changes thereby.

The result is to obtain a matrix in the row echelon form

$$\begin{vmatrix} 1 & 1 & \cdots & & & & 1 \\ 0 & d_1 & * & & \cdots & & * \\ \vdots & & \vdots & \vdots & & & \vdots \\ 0 & & & d_r & * & \cdots & * \\ 0 & & \cdots & & & & 0 \\ \vdots & & & & & & \vdots \\ 0 & & \cdots & & & & 0 \end{vmatrix} \tag{6}$$

such that

1) row 0 consists entirely of 1's.
2) $1 \leqslant d_1 \leqslant \cdots \leqslant dr$
3) all rows past row r are zero
4) any entry s above d_i, but not in row 0 satisfies $0 \leqslant s < d_i$
5) For any $1 \leqslant i \leqslant r$ and $j > i$, the elements of the jth column from row i to row r inclusive generate a subgroup of $\mathbf{Z}$ which is 0 or whose minimal positive generator h satisfies $d_i \leqslant h$. In particular any non-zero entry s lying to the right and possibly below d_i must have absolute value at least d_i.

Such a reduced matrix corresponds to an equation equivalent to the original but often considerably simpler. Let us now consider some conditions which ensure that the new equation is easily solvable.

Let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ denote the element of $\mathbf{Z}^k$ with exactly one 1 in the ith position. If an equation contains a variable X_j with power vector e_i, then solving the equation is easy because X_j appears linearly in only one term. Specifically let all the other variables be arbitrary and non-zero, solve for X_j and reject cases for which X_j is zero. This gives us all solutions of the equation.

More generally if an equation has a power group which contains a vector e_i, then we may make a change of variable to get an equivalent equation which contains e_i

as a power vector. The above method then gives us all solutions to the modified equation which we can transform back to get all solutions of the original equation.

A related situation occurs when we find that the power group contains a vector e consisting entirely of 0's and 1's with at least one of each. Then a change of variable as described above results in an equation of the form

$$Y_1 h_1(Y_2,\ldots,Y_m) = h_2(Y_2,\ldots,Y_m) \tag{7}$$

where both h_1 and h_2 have fewer than k terms. Let $Y_2,\ldots,Y_m$ be arbitrary and non-zero such that either both $h_1(Y_2,\ldots,Y_m)$ and $h_2(Y_2,\ldots,Y_m)$ are non-zero or both are zero. In the first case we may solve for non-zero Y_1 directly; in the second case Y_1 may be an arbitrary non-zero value. Similar remarks can be made when G_f contains a vector consisting entirely of 0's and d's where the problem reduces to identifying rationals as dth powers.

As an illustration of the above consider the special case when f is diagonal; that is of the form

$$f(X_1,\ldots,X_k) = c_1 X_1^{\alpha_{11}} + \cdots + c_k X_k^{\alpha_{kk}}. \tag{8}$$

The power matrix is

$$A_f = \begin{vmatrix} 1 & 1 & \cdots & & 1 \\ \alpha_{11} & 0 & \cdots & & 0 \\ & \alpha_{22} & 0 & \cdots & 0 \\ & & \vdots & & \vdots \\ 0 & & & & \alpha_{kk}. \end{vmatrix} \tag{9}$$

Suppose one of the α_{ii}, say α_{11}, is relatively prime to all the rest. Then by the Chinese Remainder Theorem, we may find integers $t_1,\ldots,t_k,t$ such that $\alpha_{11}t_1 + 1 = \alpha_{22}t_2 = \cdots = \alpha_{kk}t_k = t$. But then $e_1 = t\alpha_0 - t_1\alpha_1 - t_2\alpha_2 - \cdots - t_k\alpha_k$ so that $e_1 \in G_f$. Conversely if G_f contains a vector e_i then α_{ii} is relatively prime to all the other α_{jj}. The method above then shows how to obtain all rational solutions to $f(X_1,\ldots,X_k) = 0$. This is the result essentially contained in Wildberger [1]. We may extend this result by noting that G_f will contain a vector e consisting entirely of 0's and 1's with at least one of each if and only if the set $\{\alpha_{ii} | i = 1,\ldots,k\}$ can be partitioned into 2 non-empty subsets such that each element of one subset is relatively prime to all the elements of the other subset. In this case the method above shows how to obtain all rational solutions to $f(X_1,\ldots,X_k) = 0$.

In the above discussion the nature of the coefficient vector c is largely irrelevant. Equations whose power groups contain vectors like e_i are insensitive to changes of the coefficients (as long as they all remain non-zero). This motivates us to define a subgroup $G \subseteq \mathbf{Z}^k$ to be universally solvable if any equation whose power group is G has at least one solution. It seems of some interest to classify these.

2. Congruence equations

Now consider the case of a congruence equation. Let p be a prime, f a polynomial as in (2) with $c_j \not\equiv 0 \pmod p$, $j = 1,\ldots,k$, and consider the equation

$$f(X_1,\ldots,X_n) \equiv 0 \pmod p. \tag{10}$$

A solution $(s_1,\ldots,s_n)\in\mathbf{Z}_p^n$ is non-trivial if and only if $S_i\not\equiv 0(\mathrm{mod}\,p)$ for all $i=1,\ldots,n$. From Fermat's theorem it follows that we need only know the exponents α_{ij} up to a multiple of $m=p-1$. Thus the power vectors α_i are in $\mathbf{Z}_m^k$, the power matrix A_f has entries in $\mathbf{Z}_m$ and the power group G_f is a subgroup of $\mathbf{Z}_m^k$. These objects are images of the corresponding vectors, matrices and groups defined in the rational case under the obvious homomorphisms. There are then only a finite number of equivalence classes of equations since there are only a finite number of subgroups of $\mathbf{Z}_m^k$. Row reducing A_f as before we obtain the description following (6) but now in addition we may arrange that all entries s satisfy $0\leqslant s<m$ and that each d_i is a divisor of m.

Consider for example the case when $m=2q$ with q a prime, and suppose that A_f is of the form described above. The possible values for d_i are $1,2$ and q and we may immediately deduce the following concerning the entries $s_{ij}\ 0\leqslant i\leqslant n, 1\leqslant j\leqslant k$ of A_f. If $d_i=q$ then $s_{ij}=0$ for $i<j\leqslant r$ and $s_{ij}=0$ or q for $r<j$. If $d_i=2$ and $d_l=q$ and $s_{lj}=q$ then $s_{ij}=0$. If $d_i=1$ and $d_j=2$ and $d_l=q$ then one of s_{ij},s_{il} is 0. If $d_i=q$ for some i, then the corresponding equation is of the form

$$Y_i^q h_1(Y_1,\ldots,\hat{Y}_i,\ldots,Y_n)\equiv h_2(Y_1,\ldots,\hat{Y}_i,\ldots,Y_n)\qquad(\mathrm{mod}\,p)\tag{11}$$

where h_1,h_2 are polynomials with fewer than k terms. Since $Y_i^q\equiv\pm 1(\mathrm{mod}\,p)$, the original equation is then reduced to two equations with fewer terms. A similar analysis will be possible whenever m has a small number of prime factors.

3. An example

We now illustrate the general procedure with an example. Consider the congruence equation

$$13x^2y+4x^4z^3+5x^3y^5z^6+3y^7z^{16}\equiv 0\qquad(\mathrm{mod}\,71).\tag{12}$$

Introduce another variable and rewrite the equation as

$$f(X_0,X_1,X_2,X_3)=$$
$$13X_0X_1^2X_2+4X_0X_1^4X_3^3+5X_0X_1^3X_2^5X_3^6+3X_0X_2^7X_3^{16}\equiv 0\quad(\mathrm{mod}\,71).\tag{13}$$

Then the power matrix of f is

$$A_f=\begin{vmatrix}1&1&1&1\\2&4&3&0\\1&0&5&7\\0&3&6&16\end{vmatrix},\tag{14}$$

with entries in $\mathbf{Z}_{70}$. Row reducing, we find that if

$$B=\begin{vmatrix}1&0&0&0\\2&18&32&-1\\-26&43&10&-2\\5&-2&-1&1\end{vmatrix}\tag{15}$$

then $BA_f = C$ where

$$C = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 12 \\ 0 & 0 & 0 & 14 \end{vmatrix} \tag{16}$$

It may be checked that $\det B = 39$; since $(39, 70) = 1$, B is invertible. We introduce new variables $Y_0, \ldots, Y_3$ and set

$$\begin{aligned} X_0 &= Y_0\, Y_1^2\, Y_2^{-26}\, Y_3^5 \\ X_1 &= Y_1^{18}\, Y_2^{43}\, Y_3^{-2} \\ X_2 &= Y_1^{32}\, Y_2^{10}\, Y_3^{-1} \\ X_3 &= Y_1^{-1}\, Y_2^{-2}\, Y_3. \end{aligned} \tag{17}$$

Then f is transformed to

$$13Y_0 + 4Y_0\, Y_1 + 5Y_0\, Y_2 + 3Y_0\, Y_2^{12}\, Y_3^{14} \equiv 0 \qquad (\text{mod } 71) \tag{18}$$

or

$$\begin{aligned} Y_1 &\equiv -4^{-1}(13 + 5Y_2 + 3Y_2^2\, Y_3^{14}) \\ &\equiv 50 + 52Y_2 + 17Y_2^{12}\, Y_3^{14} \qquad (\text{mod } 71). \end{aligned} \tag{19}$$

Now to go back to the original problem we disregard X_0 and Y_0 and let $Y_2 = s$, $Y_3 = t$ to get the parametric solution

$$\begin{aligned} x &= (50 + 52s + 17s^{12}t^{14})^{18} s^{43} t^{-2} \\ y &= (50 + 52s + 17s^{12}t^{14})^{32} s^{10} t^{-1} \\ z &= (50 + 52s + 17s^{12}t^{14})^{-1} s^{-2} t \end{aligned} \tag{20}$$

where s and t range over all non-zero values in $\mathbf{Z}_{71}$ that do not satisfy

$$50 + 52s + 17s^{12}t^{14} \equiv 0 \qquad (\text{mod } 71). \tag{21}$$

Note that this equation has fewer terms than the original. We may rewrite this as

$$t^{14} \equiv 43s^{58} + 22s^{59} \qquad (\text{mod } 71) \tag{22}$$

which has a solution if and only if

$$(43s^{58} + 22s^{59})^5 \equiv s^{10}(43 + 22s)^5 \equiv 1 \qquad (\text{mod } 71). \tag{23}$$

An easy check shows this last equation has exactly 2 solutions, $s \equiv 25$ or $s \equiv 47$. It thus follows that the original equation has exactly $70^2 - 14 \cdot 2 = 4872$ solutions and they are all described as above.

This example is not as special as it may look. The reader is encouraged to verify this claim by choosing some equations randomly and utilizing the same procedure to simplify them.

4. Final remarks

We conclude with some general remarks on the range of applicability of the above method, which ultimately depends on row-reduction affecting the power matrix A_f non-trivially. If the power vectors α_i are numerous and haphazard, the method works well. If n is small compared to k then row-reduction will accomplish little (the extreme case here being a single variable equation with many terms.) However in this case the possibility arises of a useful preliminary linear change of variable which will decrease k. We have in this paper ignored linear changes of variable, but a complete theory ought to take into account both linear and multiplicative changes of variable together with their interactions. The method is also ineffective when the power vectors α_i do not interact with each other or with α_0. This will happen typically in the diagonal case when the exponents have a large number of common divisors. The worst case is when all exponents are identical, so the equation may be said to be of Fermat type. From our point of view then equations of Fermat type are not only historical curiosities but are the purest examples of difficult Diophantine equations.

Reference

[1] Wildberger N J, A soluble Diophantine equation, *Math-Mag.* **49** (1976) pp. 200–201