PARAMETRIC SOLUTION OF LINEAR HOMOGENEOUS DIOPHANTINE EQUATIONS

WALLACE GIVENS

1. **Introduction.** Certain parametric expressions were recently shown by L. W. Griffiths [1][1] to yield all the integral solutions of a system of linear homogeneous equations with integer coefficients in terms of integral values of the parameters. A simpler proof of this same result is given in the next section (cf. our equations (4) with Griffiths' [1] equations (2)). Following this we prove that the denominator in the formulas may be made independent of the values assigned the parameters, a possibility not discussed by Miss Griffiths. The proof of this stronger theorem is made to depend on one of its special cases, namely a result of Hermite's which states that the n minors of order $n-1$ of an $n-1$ by n matrix can have preassigned integral values for a suitable choice of integral values of the components of the matrix.

2. **Form of the solution.** Without essential loss of generality, we may assume that the system of equations is linearly independent and contains more unknowns than equations. Let the equations be

$$\sum_{i=1}^{n} a_{\alpha i}x_i = 0, \qquad \alpha = 1, 2, \cdots, r \geqq 0, \tag{1}$$

where the $a_{\alpha i}$ are rational integers, the matrix $A = \|a_{\alpha i}\|$ is of rank r and we set $n = r+s+1$ with $s \geqq 0$. We shall suppose for convenience that the x_i have been numbered so that the determinant of $\|a_{\alpha\beta}\|$ ($\alpha, \beta = 1, \cdots, r$) is different from 0.

We now adjoin to (1) the system of equations

$$\sum_{i=1}^{n} p_{\rho i}x_i = 0, \qquad \rho = 1, 2, \cdots, s, \tag{2}$$

and let D_i equal $(-1)^{i+1}$ times the determinant obtained by omitting the ith column of the $n-1$ by n matrix

$$\left\| \begin{matrix} A \\ P \end{matrix} \right\|, \qquad \text{where } P = \|p_{\rho i}\|. \tag{3}$$

Then $x_i = D_i$ is an integral solution of (1) and (2) for any choice of

Presented to the Society, December 28, 1946; received by the editors November 22, 1946, and, in revised form, January 11, 1947.

[1] Numbers in brackets refer to the references cited at the end of the paper.

integral values of the $p_{\rho i}$. If at least one of the D_i is different from zero, a relatively prime solution of (1) and (2) is unique to within sign and hence is obtained by dividing the D_i by their greatest common divisor, d, which will depend on the matrix P as well as on A. That every relatively prime solution of (1) alone is obtained in this way by some choice of P is proved by letting ξ_i be a particular non-zero solution of (1) and taking

$$(2') \qquad P = \begin{Vmatrix} 0 & 0 \cdots 0 & \xi_n & 0 \cdots 0 & -\xi_{r+1} \\ 0 & 0 \cdots 0 & 0 & \xi_n \cdots 0 & -\xi_{r+2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 \cdots 0 & 0 & 0 \cdots \xi_n & -\xi_{n-1} \end{Vmatrix}$$

where for convenience we have supposed the last $n-r$ variables renumbered, if necessary, so that $\xi_n \neq 0$. With this choice of P, $D_i = (-1)^{n+1}(\xi_n)^{s-1}$ (determinant of $\|a_{\alpha\beta}\|)\xi_i$. Hence an arbitrary solution of (1) is of the form

$$(4) \qquad x_1 = \frac{pD_1}{d}, \quad x_2 = \frac{pD_2}{d}, \quad \cdots, \quad x_n = \frac{pD_n}{d},$$

where p is an arbitrary integer. This is Griffiths' result.

In case $r=0$, (2') is an $n-1$ by n matrix with signed minors equal to $(-1)^{n+1}(\xi_n)^{n-2}\xi_i$. Modifying (2') in this case we can obtain a matrix having the ξ_i for signed minors. For, making even permutations on the rows and adding suitable integral multiples of one row to another, we can arrange to have all zeros in the last column except perhaps for the last element in it. Moreover, the values of the minors are unchanged and the elements of the first $n-1$ columns remain divisible by ξ_n. Dividing each of the first $n-2$ rows of the reduced matrix by ξ_n and multiplying one row by $(-1)^{n+1}$, we obtain a matrix having its signed minors equal to the (arbitrary) integers ξ_i. This proves the result due to Hermite [2] and stated in section one. (Hermite's original proof is also elementary in character.)

3. **The stronger theorem.** By Laplace's expansion, the D_i are polynomials in the elements of P with coefficients which are the signed r-rowed minors of A. The greatest common divisor of these minors, say a, is therefore a divisor of each D_i for every choice of the parameters. We now show that the denominator d in (4) can be replaced by a, which is independent of the parameters, thus proving the following theorem.

If $r<n-1$, the polynomials D_i/a in the $n(n-r-1)$ parameters $p_{\rho i}$

have the two properties: (1) $x_i = D_i/a$ *is an integral solution of* (1) *for arbitrary integral values of the parameters and* (2) *every integral solution of* (1) *is obtained in this way for some integral values of the parameters. If* $r = n-1$, *the expressions* pD_i/a *in the single parameter* p *have these two properties.*

The case $r = n-1$ was proved above so we shall suppose $s = n-r-1 > 0$ in what follows. The proof then consists essentially in reducing the given system of equations to an equivalent system in canonical form (r of the variables $= 0$, the others arbitrary) and obtaining the parameter matrix of the original from that of the reduced system, the existence of the latter being guaranteed by Hermite's result.

PROOF OF THE THEOREM. Kronecker [3] proved that there exist square matrices M and N with integral elements, having determinants $+1$ or -1, of orders r and n respectively, and such that

$$B = MAN = \left\| \begin{matrix} e_1 & 0 & 0 \cdots 0 & 0 \cdots 0 \\ 0 & e_2 & 0 \cdots 0 & 0 \cdots 0 \\ \cdot & \cdot & \cdot \cdot \cdot \cdot & \cdot \cdot \cdot \cdot \\ 0 & 0 & 0 \cdots e_r & 0 \cdots 0 \end{matrix} \right\|, \tag{5}$$

where $e_\beta = (d_\beta/d_{\beta-1})$, d_β is the greatest common divisor of the β-rowed minors of A and $d_0 = 1$. It is clearly possible to choose the determinant of M to be $+1$ and we do this.

If, now, ξ_i is a particular integral solution of (1) and we set

$$\eta_i = \sum_{j=1}^{n} n_{ij}\xi_j, \tag{6}$$

where $\|n_{ij}\| = N^{-1}$ has integral elements, η_i will be an integral solution of the equations

$$\sum_{i=1}^{n} b_{\alpha i}\eta_i = 0, \qquad \alpha = 1, 2, \cdots, r. \tag{7}$$

Hence $\eta_1 = \eta_2 = \cdots = \eta_r = 0$. Adjoining to (7) the equations

$$\sum_{i=1}^{n} q_{\rho i}\eta_i = 0, \qquad \rho = 1, 2, \cdots s, \tag{8}$$

and designating the signed $(n-1)$-rowed minors of the matrix

$$\left\| \begin{matrix} B \\ Q \end{matrix} \right\|, \qquad \text{where } Q = \|q_{\rho i}\|, \tag{9}$$

by Δ_i, it turns out to be possible to find values for the elements of Q so that

$$\eta_i = \Delta_i/a, \tag{10}$$

where $a = d_r = e_1e_2 \cdots e_r$ = the greatest common divisor of the r-rowed minors of A. Indeed (10) reduces for $i \leqq r$ to $\eta_1 = \eta_2 = \cdots = \eta_r = 0$ and for $i > r$ to the equality of η_i and $(-1)^{i+1}$ times the determinant obtained by omitting the ith column of the matrix $\|q_{\rho\tau}\|$ ($\rho = 1, 2, \cdots, s$; $\tau = r+1, \cdots, n$). The existence of such integral values of the $q_{\rho\tau}$ is guaranteed by the theorem of Hermite proved in §2. The values of the parameters $q_{\rho\alpha}$ ($\rho = 1, \cdots, s$; $\alpha = 1, \cdots, r$) may be assigned arbitrarily.

We now define a parameter matrix $P = QN^{-1}$, and consider the signed $(n-1)$-rowed minors of the three matrices:

$$\left\| \begin{matrix} A \\ P \end{matrix} \right\| = \left\| \begin{matrix} M^{-1} & BN^{-1} \\ & QN^{-1} \end{matrix} \right\|, \quad \left\| \begin{matrix} B & N^{-1} \\ Q & N^{-1} \end{matrix} \right\| = \left\| \begin{matrix} B \\ Q \end{matrix} \right\| N^{-1}, \text{ and } \left\| \begin{matrix} B \\ Q \end{matrix} \right\|. \tag{11}$$

A particular minor of the first of these matrices is equal to the corresponding minor of the second, multiplied by the determinant of M^{-1}, which we chose to be $+1$. Denoting as before the common value of these signed minors by D_i we then find that they are related to the Δ_i by the formula

$$\Delta_i = \pm \sum_{j=1}^{n} n_{ij} D_j, \tag{12}$$

the plus sign being used if the determinant of N is $+1$ and the minus sign if it is -1. Using (10) and (6) we find that

$$\xi_i = \pm D_i/a, \tag{13}$$

and the sign may be absorbed into one row of the parameter matrix.

References

1. L. W. Griffiths, *A note on linear homogeneous diophantine equations*, Bull. Amer. Math. Soc. vol. 52 (1946) pp. 734–736.

2. M. Hermite. *Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres*, J. Reine Angew. Math. vol. 40 (1850) pp. 261–315, in particular p. 264.

3. L. Kronecker, *Reduktion der Systeme von n^2 ganzzahligen elementen*, J. Reine Angew. Math. vol. 107 (1891) pp. 135–136.

Illinois Institute of Technology