J. Austral. Math. Soc. **70** (2001), 401–423

FRACTIONAL PARTS OF LINEAR POLYNOMIALS AND AN APPLICATION TO HYPERGEOMETRIC FUNCTIONS

ROBERTO DVORNICICH and UMBERTO ZANNIER

(Received 12 March 1998; revised 8 November 2000)

Communicated by W. W. L. Chen

Abstract

Using a result on arithmetic progressions, we describe a method for finding the rational h-tuples $\boldsymbol{\rho} = (\rho_1, \ldots, \rho_h)$ such that all the multiples $m\boldsymbol{\rho}$ (for m coprime to a denominator of $\boldsymbol{\rho}$) lie in a linear variety modulo $\mathbb{Z}$. We give an application to hypergeometric functions.

2000 *Mathematics subject classification*: primary 11J54, C35.

1. Introduction

We consider a class of relations of the type

$$c_0 + \sum_j c_j ((L_j(\mathbf{y}))) = 0, \tag{1}$$

where $((x)) = \{x\} - 1/2$, $x \in \mathbb{R}$. The L_js are linear polynomials in $\mathbb{Q}[\mathbf{y}]$, $\mathbf{y} = (y_1, \ldots, y_h)$, and the c_js are rational numbers. We are interested in the rational h-tuples $\boldsymbol{\rho} = (\rho_1, \ldots, \rho_h)$ with the following property. Let m be a common denominator for $\rho_1, \ldots, \rho_h$. For all n coprime with m (this is a technical condition), we require that $\mathbf{y} = n\boldsymbol{\rho}$ be a solution of (1). We expect that these multiples $n\boldsymbol{\rho}$ will in general be well-distributed modulo $\mathbb{Z}^h$. On the other hand, if they all satisfy the relation (1), then they have special properties which we try to analyse. We show that they in fact form a 'quasi-linear' set, being roughly described by finitely many linear equalities mod $\mathbb{Z}^h$ (see Section 2-II and Theorem 1 in Section 2-III). Moreover, these sets can be effectively computed.

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

In the fundamental cases (which will be called *indecomposable*) such quasi-linear sets will turn out to be translations by $\mathbb{Z}^h$ of finitely many lines plus or minus finitely many points. We shall give practical methods for computing the linear conditions which describe completely the above quasi-linear set.

The problem we study was motivated by the work of Schwarz [15], who in 1873 classified the hypergeometric differential equations

$$(2) \qquad D(\alpha, \beta, \gamma)y = x(1-x)\frac{d^2y}{dx^2} + [\gamma - (1+\alpha+\beta)x]\frac{dy}{dx} - \alpha\beta = 0$$

having a full system of algebraic solutions. We briefly recall Schwarz's work and restrict our considerations to the operators which are irreducible over $\mathbb{C}(x)$.

Set $\lambda = 1-\gamma$, $\mu = \gamma - \alpha - \beta$, $\nu = \alpha - \beta$. Looking at the singularities and at the reducibility of (2), it can be proved that for such operators $\alpha, \beta, \gamma \in \mathbb{Q}$, while none of the numbers $\lambda, \mu, \nu, \alpha, \beta, \gamma - \alpha, \gamma - \beta$ belongs to $\mathbb{Z}$. Further, if $D(\alpha, \beta, \gamma)y = 0$ has only algebraic solutions, one sees that the same is true for $D(\alpha+l, \beta+m, \gamma+n)y = 0$ for any $l, m, n \in \mathbb{Z}$. Hence we may assume that $0 < \lambda < 1, 0 < \mu < 1, 0 < |\nu| < 1$.

Schwarz also found a group of 24 transformations on (λ, μ, ν) isomorphic to $\mathcal{S}_4$ and preserving the algebraicity of solutions; this allows the further restriction $\lambda \geq \mu \geq \nu$. Under these conditions Schwarz proved that, apart from an explicitly given finite number of sporadic cases (see also [13]), algebraic solutions occur if and only if

$$(\lambda, \mu, \nu) = (1/2, 1/2, \nu)$$

or, equivalently,

$$(\alpha, \beta, \gamma) = (\alpha, 1-\alpha, 1/2)\,.$$

In this case the monodromy group is dihedral of order $2n$, where n is the denominator of ν. Moreover, Schwarz produced the full list of solutions.

In 1904 and 1911 Landau ([11, 12]), applying Eisenstein's criterion to power series solutions of (2), obtained the following arithmetic condition for algebraic solutions in terms of the rational parameters

$$\alpha = \frac{a}{m}, \quad \beta = \frac{b}{m}, \quad \gamma = \frac{c}{m} \qquad ((a, b, c, m) = 1).$$

For every integer n such that $(n, m) = 1$ we have

$$(3) \qquad \text{either } na < nc < nb \pmod m \qquad \text{or } nb < nc < na \pmod m,$$

where the inequalities are referred to the minimal non-negative residue.

In 1943 Errera [5] used Landau's condition to obtain Schwarz's list by an elementary arithmetic argument (an account of which is also given in [13]).

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

The arithmetic condition (3) appears also when one assumes that (2) satisfies the hypotheses for the Grothendieck conjecture: this roughly states that, if a linear differential equation with polynomial coefficients has a full system of solutions modulo all large primes, then it has a full system of algebraic solutions. In fact, this connection between (3) and the reduction of (2) mod p has been observed by Katz, who verified in [9] the Grothendieck conjecture for Picard-Fuchs differential equations, so in particular for (2) (see [9, Section 6.4]). This part of Katz's paper is however independent of the rest and essentially self-contained. One may then combine this with the Landau-Errera Theorems and Schwarz's list to verify in a different and more elementary way the Grothendieck conjecture for equations (2).

To connect with the problem described at the beginning, we shall interpret the two alternative inequalities appearing in (3) in the form of just one equality of type (1) with $\mathbf{y} = n\boldsymbol{\rho}$, $\boldsymbol{\rho} = (\alpha, \beta, \gamma)$, namely

$$(4)\quad 2((n\gamma)) = ((n\alpha)) + ((n\beta)) + ((n(\gamma-\alpha))) + ((n(\gamma-\beta))) \quad \text{for } (n,m)=1,$$

where $((x)) = \{x\} - 1/2$, assuming that $\gamma, \alpha, \beta, \gamma-\alpha, \gamma-\beta \notin \mathbb{Z}$. To our knowledge, this formulation of (3) seems to be new.

We give and explicit computation of the linear equations which describe completely the above quasi-linear set in the case (4) (see Theorem 2 and Section 2). In this procedure we shall use a result on arithmetic progressions, proved in [4], which we recall as Lemma 10. It is quite possible that these methods can be applied to more general hypergeometric equations.

In Section 2 we study general relations of type (1), while Section 3 will be devoted to the attainment of Schwarz's list (apart from sporadic cases).

2. Fractional parts of linear polynomials

I. Uniform distribution Let $f : \mathbb{R}^h \to \mathbb{R}$ be a function periodic mod $\mathbb{Z}^h$, and define

$$(5)\qquad S = S_f = \{\mathbf{x} \in \mathbb{R}^h \mid f(\mathbf{x}) = 0\}.$$

Observe that S_f is invariant under translations by $\mathbb{Z}^h$.

Later on f will be a linear combination of functions of the form $((a_1x_1 + \cdots + a_hx_h + \beta))$, where $a_i \in \mathbb{Z}$, $\beta \in \mathbb{R}$, and $((x)) = \{x\} - \frac{1}{2}$.

We shall be interested in characterizing the set $X_f \subset \mathbb{Q}^h$ defined by

$$(6)\quad X_f = \{\boldsymbol{\rho} \in \mathbb{Q}^h \mid n\boldsymbol{\rho} \in S_f \quad \forall n \in (\mathbb{Z}/R\mathbb{Z})^*, \text{ where } R \in \mathbb{N} \text{ and } R\boldsymbol{\rho} \in \mathbb{Z}^h\}.$$

REMARK 1. We observe that the definition of X_f does not depend on R, provided that $R\boldsymbol{\rho} \in \mathbb{Z}^h$. In fact, a simple argument based on the Chinese Remainder Theorem proves that whenever $R \mid R'$ every class in $(\mathbb{Z}/R\mathbb{Z})^*$ has a representative in $(\mathbb{Z}/R'\mathbb{Z})^*$.

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

For technical reasons, which will appear later, it will be convenient to work with a set more general than X_f. To be precise, for a congruence class a mod q where $(a, q) = 1$, define

$$X_f(a, q) = \{\rho \in \mathbb{Q}^h \mid n\rho \in S_f \ \forall n \equiv a \pmod q,\ (n, R) = 1\}, \tag{7}$$

where R is any natural number such that $R\rho \in \mathbb{Z}^h$. We contend that the definition of $X_f(a, q)$ is independent of the choice of R with the given property. To see this, it is enough to show that in (7) we can replace R with any of its multiples, or, equivalently, that if $R|R'$ and n is such that $(n, R) = 1$, $n \equiv a \pmod q$, then there exists $n' \equiv a \pmod q$, $(n', R') = 1$, $n' \equiv n \pmod R$. Now, the reduction $(\mathbb{Z}/[q, R'])^* \to (\mathbb{Z}/[q, R])^*$ is surjective. But the class of n mod $[q, R]$ is coprime with $[q, R]$ since $(a, q) = 1$; hence it lies in the image of the reduction, which proves our contention.

This important remark will be used repeatedly in the sequel: for instance we shall assume, replacing possibly R by qR, that q divides R. More generally, we may assume that R is divisible by any given integer.

The technique below was introduced by Davenport and Schinzel [3], who dealt with a problem concerning roots of unity. Another approach can be found in [7] and [8].

REMARK 2. The condition $(n, R) = 1$ seems rather artificial. In fact, it may be replaced by restricting n to any subset $\mathscr{M}$ of $(\mathbb{Z}/R\mathbb{Z})$ such that the exponential sums $\sum_{n\in\mathscr{M}} \mathbf{e}(nc/R)$ can be estimated somewhat non trivially. A motivation for choosing this condition is provided, for instance, by the example coming from the hypergeometric equations and discussed in the next section.

For $q \mid R$, $(a, q) = 1$, we set $R = qR^*$ and, for integral c, we put

$$S(c, a, q, R) = \sum_{\substack{(m,R)=1 \\ m\equiv a \pmod q}} \mathbf{e}(cm/R).$$

LEMMA 1. *Setting $d = (c, R^*)$ we have*

$$|S(c, a, q, R)| \le \frac{\phi(R)}{\phi(R^*/d)}$$

where ϕ is Euler's function.

PROOF.

$$S(c, a, q, R) = \sum_{(m,R)=1} \mathbf{e}\left(\frac{cm}{R}\right) \frac{1}{q} \sum_{t=1}^{q} \mathbf{e}\left(\frac{t(m-a)}{q}\right)$$

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

$$= \sum_{t=1}^{q} \frac{1}{q} \mathbf{e}\left(\frac{-at}{q}\right) \sum_{(m,R)=1} \mathbf{e}\left(\frac{cm}{R} + \frac{tm}{q}\right)$$
$$= \frac{1}{q} \sum_{t=1}^{q} \mathbf{e}\left(\frac{-at}{q}\right) \sum_{(m,R)=1} \mathbf{e}\left((c + tR^*)\frac{m}{R}\right)$$
$$= \frac{1}{q} \sum_{t=1}^{q} \mathbf{e}\left(\frac{-at}{q}\right) S(c + tR^*, R),$$

where $S(c, R)$ is the Ramanujan sum $S(c, 0, 1, R)$. This sum may be easily evaluated. We have (see [6, Theorem 272, page 238])

$$S(c, R) = \mu\left(R/d'\right) \frac{\phi(R)}{\phi(R/d')},$$

where $d' = (c, R)$. Plugging this value in the formula above and setting $d_t = (R, c + tR^*)$ we get

$$S(c, a, q, R) = \frac{\phi(R)}{q} \sum_{t=1}^{q} \mathbf{e}(-at/q)\, \mu(R/d_t)\, \frac{1}{\phi(R/d_t)}$$

whence

$$|S(c, a, q, R)| \leq \phi(R) \max_{1 \leq t \leq q} \frac{1}{\phi(R/d_t)} \leq \frac{\phi(R)}{\phi(R^*/d)}.$$

In fact, $(c + tR^*, R^*) = d$ for all t and $(R^*/d) \mid (R/d_t)$. □

We shall need the following lemma on Fourier series, stated without proof.

LEMMA 2. *Let $0 < \delta < 1/2$. Let $F_\delta : \mathbb{R} \to \mathbb{R}$ be periodic mod $\mathbb{Z}$ and defined in $[-1/2, 1/2]$ as follows:*

$$F_\delta(x) = \begin{cases} \delta - |x| & \text{for } |x| \leq \delta; \\ 0 & \text{for } \delta \leq |x| \leq 1/2. \end{cases}$$

Then, for all $x \in \mathbb{R}$, $F(x) = \sum_{n=-\infty}^{\infty} a_n \mathbf{e}(nx)$, where $a_0 = \delta^2$ while, for $n \neq 0$, $a_n = \sin^2 \pi n\delta / \pi^2 n^2$.

PROPOSITION 1. *Let $\rho \in X_f(a, q)$, $0 < \delta < 1/2$ and assume that there is a cube of side 2δ disjoint from S. Then there exist integers $m_1, \ldots, m_h$ not all zero such that*

(i) $q \mid m_i$;
(ii) $m_1\rho_1 + \cdots + m_h\rho_h \in \mathbb{Z}$;
(iii) $|m_i| \leq c_1$,

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

where $c_1 = c_1(\delta, h, q)$ is effectively computable (one may take $c_1 = 6q^3 h\delta^{-(1+3h)}$).

PROOF. Let $(y_1, \dots, y_h)$ be the center of a cube of side 2δ disjoint from S. Let also

$$G(x_1, \dots, x_h) = \prod_{i=1}^{h} F_\delta(x_i - y_i).$$

Clearly, $G(\mathbf{x}) = 0$ for $\mathbf{x} \in S$, whence, if $\boldsymbol{\rho} \in X_f(a, q)$ and $R = qR^*$ is a denominator for $\boldsymbol{\rho}$ divisible by q,

$$\sum_{\substack{m \in (\mathbb{Z}/R\mathbb{Z})^* \\ m \equiv a \pmod q}} G(m\rho_1, \dots, m\rho_h) = 0.$$

Using the Fourier series for F_δ, multiplying out and changing the order of summation we get

$$0 = \sum_{\mathbf{n} \in \mathbb{Z}^h} a_{n_1} \cdots a_{n_h} \mathbf{e}(-\mathbf{n} \cdot \mathbf{y}) \sum_{\substack{m \in (\mathbb{Z}/R\mathbb{Z})^* \\ m \equiv a \pmod q}} \mathbf{e}((\mathbf{n} \cdot \boldsymbol{\rho})m).$$

If $\rho_i = r_i/R$ this formula becomes

$$\sum_{\mathbf{n} \in \mathbb{Z}^h \setminus \{\mathbf{0}\}} a_{n_1} \cdots a_{n_h} \mathbf{e}(-\mathbf{n} \cdot \mathbf{y}) S((\mathbf{n} \cdot \mathbf{r}), a, q, R) = -a_0^h S(0, a, q, R).$$

Let $B > 0$ and split the sum according to whether $\max |n_i| > B$ or not.

$$\begin{aligned}
\frac{\phi(R)}{\phi(q)}\delta^{2h} &\le \sum_{|n_i| \le B} |a_{n_1}| \cdots |a_{n_h}| S((\mathbf{n} \cdot \mathbf{r}), a, q, R) \\
&\quad + 2h \frac{\phi(R)}{\phi(q)} \sum_{n > B} |a_n| \left(\sum_{n_1, \dots, n_{h-1}} |a_{n_1}| \cdots |a_{n_{h-1}}| \right) \\
&\le \frac{\phi(R)}{\min_{|n_i| \le B} \phi(R^*/d_{\mathbf{n}})} (F(0))^h + \frac{2h}{\pi^2(B-1)} \frac{\phi(R)}{\phi(q)} (F(0))^{h-1} \\
&\le \frac{\phi(R)}{\min_{|n_i| \le B} \phi(R^*/d_{\mathbf{n}})} \delta^h + \frac{2h}{\pi^2(B-1)} \frac{\phi(R)}{\phi(q)} \delta^{h-1},
\end{aligned}$$

where $d_{\mathbf{n}} = (R^*, (\mathbf{n} \cdot \mathbf{r}))$. Let $B = 4h\delta^{-(1+h)}/\pi^2 + 1$; we get

$$\min_{|n_i| \le B} \phi(R^*/d_{\mathbf{n}}) \le \frac{2}{\delta^h} \phi(q).$$

Using, for simplicity, the crude inequality $\phi(x) \ge \sqrt{x/2}$ we derive the existence of integers $n_1^*, \dots, n_h^*$ not all zero, such that

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

(i) $|n_i^*| \le B$;
(ii) $R^*\delta^{2h}/8 \le (R^*, (\mathbf{n}^*\mathbf{r}))\phi^2(q)$.

Setting $n_1^* r_1 + \cdots + n_h^* r_h = N = d_{\mathbf{n}^*} s$ and $R^* = d_{\mathbf{n}^*} R'$ we easily find

$$(qR'n_1^*)\rho_1 + \cdots + (qR'n_h^*)\rho_h \in \mathbb{Z}$$

and the conclusion follows with $m_i = qR'n_i^*$. □

In case S_f is not dense, we shall use the foregoing proposition to decrease the dimension h in the problem of describing the set $X_f(a, q)$.

To be precise, suppose S is not dense. Then S is disjoint from a suitable cube and we may apply Proposition 1 with $\boldsymbol{\rho} = (\rho_1, \ldots, \rho_h) \in X_f(a, q)$. We obtain the existence of a non-trivial relation

$$m_1\rho_1 + \cdots + m_h\rho_h = m \in \mathbb{Z}, \quad |m_i| \le c_1, \quad q \mid m_i \quad \text{for every } i. \tag{8}$$

Suppose, for example, that $m_h \neq 0$ and set, for $b \in \mathbb{Z}$,

$$g_b(x_1, \ldots, x_{h-1}) = f\left(m_h x_1, \ldots, m_h x_{h-1}, \frac{b}{m_h} - \sum_{i=1}^{h-1} m_i x_i\right). \tag{9}$$

Note that g_b is the restriction of f to a certain linear subspace. Since f is periodic mod $\mathbb{Z}^h$, any such g_b is periodic mod $\mathbb{Z}^{h-1}$.

Moreover, in view of the periodicity of f, we get in this way only finitely many functions; in fact g_b depends only on the class of b mod m_h.

We abbreviate

$$\boldsymbol{\rho}^* = \frac{\boldsymbol{\rho}'}{m_h} = \left(\frac{\rho_1}{m_h}, \ldots, \frac{\rho_{h-1}}{m_h}\right).$$

Since $\boldsymbol{\rho} \in X_f(a, q)$, we have $f(t\boldsymbol{\rho}) = 0$ for $(t, R) = 1$ and $t \equiv a \pmod q$, where R is a denominator for $\boldsymbol{\rho}$ which we may assume is divisible by m_h, as already observed.

In particular, letting t_0 be any congruence class mod m_h such that $t_0 \equiv a \pmod q$, $(t_0, m_h) = 1$, we have $f(t\boldsymbol{\rho}) = 0$ for $t \equiv t_0 \pmod{m_h}$, $(t, R) = 1$, that is, $\boldsymbol{\rho} \in X_f(t_0, m_h)$. But then, for such values of t, relation (8) yields

$$\begin{aligned} 0 = f(t\rho_1, \ldots, t\rho_{h-1}, t\rho_h) &= f\left(t\rho_1, \ldots, t\rho_{h-1}, t\frac{m}{m_h} - \sum_{i=1}^{h-1} \frac{tm_i}{m_h}\rho_i\right) \\ &= f\left(t\rho_1, \ldots, t\rho_{h-1}, \frac{t_0 m}{m_h} - \sum_{i=1}^{h-1} \frac{tm_i}{m_h}\rho_i\right) = g_{t_0 m}(t\boldsymbol{\rho}^*). \end{aligned}$$

Therefore we can conclude that $\boldsymbol{\rho}^* \in X_{g_{t_0 m}}(t_0, m_h)$.

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

We may clearly reverse the steps of the argument and show that, if $\rho^* \in X_{g_{t_0 m}}(t_0, m_h)$ and ρ satisfies (8), then $\rho \in X_f(t_0, m_h)$.

Note that, as t_0 varies mod m_h, we obtain all classes $t \equiv a \pmod q$.

We may rephrase the preceding discussion as the following lemma.

LEMMA 3. *Assume that S_f is not dense. If ρ satisfies* (8), *then*

$$\rho \in X_f(a, q) \Leftrightarrow \rho^* \in \bigcap_{\substack{t_0 \equiv a \\ (\mathrm{mod}\ m_h)}} X_{g_{t_0 m}}(t_0, m_h).$$

The usefulness of this lemma comes from the lowering of the dimension from h to $h - 1$. In fact, the function $f(x_1 \ldots, x_h)$ is replaced by several of its restrictions to suitable subspaces of dimension $h - 1$. This will be the main tool for proving Theorem 1.

Whenever possible, we apply this procedure again to the functions $g_{t_0 m}$ obtained in this way, and so on. The functions which arise in this procedure have the following form:

$$g(t_1, \ldots, t_\nu) = f(L_1(\mathbf{t}) + \tau_1, \ldots, L_h(\mathbf{t}) + \tau_h), \tag{10}$$

where $L_1, \ldots, L_h$ are linear forms in $t_1, \ldots, t_\nu$ ($\nu \leq h$) with integer coefficients, while the τ_i's are rationals.

The bounds for the coefficients of the L_i's as well as for the heights of the τ_i's can be determined inductively depending on the size of a cube contained in the support of any of the functions to which Proposition 1 is applied. Moreover, the whole procedure is effective, provided we can give an effective lower bound for the size of such cubes.

The procedure of reducing the dimension terminates when either the dimension has gone down to zero, or the relevant function g has a dense zero set S_g. In the first case we obtain a finite number of solutions mod $\mathbb{Z}^h$.

It remains to determine the structure of $X_f(a, q)$ for any function f with a dense zero set. Hence from now on we restrict f to be of the following type

$$f(\mathbf{x}) = \sum_{i=1}^{k} c_i((l_i(x_1, \ldots, x_h) + \xi_i)), \tag{11}$$

where l_i are linear forms with integer coefficients of maximal rank and $c_i, \xi_i \in \mathbb{Q}$. Observe that the functions defined by (10) have the same form as f.

II. Quasi-linear sets Before stating our main results, we describe the general structure of S_f for f of type (11) (see Proposition 2). We choose the affine description; of course one might as well work directly on the torus $\mathbb{R}^h/\mathbb{Z}^h$, since S_f is invariant under

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

translations by integral vectors. We define an affine rational linear subspace $\mathscr{L} \subset \mathbb{R}^h$ as the set of solutions of a linear system

$$f_j(\mathbf{x}) = a_j, \quad j = 1, \ldots, r$$

with rational coefficients. A rational linear strip $\mathscr{U}$ will be the set of solutions of a system

$$g_j(\mathbf{x}) \in I_j, \quad j = 1, \ldots, r,$$

where g_j are rational linear forms and I_j are intervals (closed, open or half-open) with rational endpoints. For any set $X \subset \mathbb{R}^h$, write $X^* = X + \mathbb{Z}^h$ for the saturated set of X under integral translations.

DEFINITION 1. A quasi-linear set is a finite union of sets of the form $X^* \setminus \bigcup_{i=1}^{s} Y_i^*$, where $X, Y_1, \ldots, Y_s$ are rational linear subspaces.

DEFINITION 2. A semi-linear set is a finite union of sets of the form $X^* \setminus \bigcup_{i=1}^{s} Y_i^*$, where $X, Y_1, \ldots, Y_s$ are rational linear strips.

It is easy to see that quasi-linear (respectively semi-linear) sets are closed under finite union, intersection and complementation. In fact, they are the minimal family with this property containing the starred linear subspaces (respectively linear strips). By abuse of language, we shall use sometimes quasi-linear to mean the set of rational points of a quasi-linear set; this will cause no problem since everything will be defined over $\mathbb{Q}$.

LEMMA 4. *Let $l(\mathbf{x}) = a_1 x_1 + \cdots + a_h x_h$ $(a_1 \neq 0)$ be a rational linear form and let $\xi \in \mathbb{Q}$. Then the set*

$$V = \{\mathbf{x} \in \mathbb{R}^h \mid l(\mathbf{x}) + \xi \in \mathbb{Z}^h\} \tag{12}$$

is a quasi-linear set.

PROOF. For $0 \leq r < |a_1|$, let $\mathscr{H}_r$ be the affine hyperplane

$$l(\mathbf{x}) + \xi = r.$$

We claim that

$$V = \bigcup_{0 \leq r < |a_1|} \mathscr{H}_r^*.$$

In fact, $\mathscr{H}_r^* \subset V$ is obvious; let $\mathbf{x} \in V$ and set $l(\mathbf{x}) + \xi = b \in \mathbb{Z}$. Then $b = qa_1 + r$, $0 \leq r < |a_1|$ and $\mathbf{x} - (q, 0, \ldots, 0) \in \mathscr{H}_r$. □

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

Observe that, conversely, if $\mathscr{H}$ is a rational hyperplane, then $\mathscr{H}^*$ is of type (12). In fact, let

$$\mathscr{H} = \{\mathbf{x} \mid l(\mathbf{x}) + \xi = 0\}.$$

We may assume that l is an integral primitive form (that is, with coprime coefficients); then

$$\begin{aligned}\mathscr{H}^* &= \{\mathbf{x} \mid l(\mathbf{x}) + \xi \in l(\mathbb{Z}^h)\} \\ &= \{\mathbf{x} \mid l(\mathbf{x}) + \xi \in \mathbb{Z}\}.\end{aligned}$$

PROPOSITION 2. *For f of type (11) S_f is a semi-linear set and it may be effectively determined. In particular, either S_f is dense and $[0, 1]^h \setminus S_f$ is contained in a finite union of hyperplanes or we may compute the side 2δ of some cube outside S_f.*

PROOF. For any subset $\gamma \subset \{1, \dots, k\}$ let

$$V_\gamma = \{\mathbf{x} \in \mathbb{R}^h \mid l_i(\mathbf{x}) + \xi \in \mathbb{Z} \Leftrightarrow i \in \gamma\}.$$

By Lemma 4 and the preceding remark it follows that V_γ is a quasi-linear set. Clearly $S_f = \bigcup_\gamma (S_f \cap V_\gamma)$ and we show that each term of the union is of the desired type. Now $S_f \cap V_\gamma$ is the set of points of V_γ which satisfy

$$\sum_{i \notin \gamma} c_i \{l_i(\mathbf{x}) + \xi\} = \frac{1}{2} \sum_{i=1}^{k} c_i. \tag{13}$$

Observe also that for all $\mathbf{x} \in \mathbb{R}^h$ we have

$$\{l(\mathbf{x}) + \xi\} = l(\{x\}) + \{\xi\} + n \tag{14}$$

for some integer n depending on $\mathbf{x}$ but uniformly bounded (in fact, $|n| < |a_1| + \cdots + |a_h| + 1$ if $l(\mathbf{x}) = a_1 x_1 + \cdots + a_h x_h$). Now $S_f \cap V_\gamma$ is the set of points of V_γ which satisfy one of the following finitely many systems

$$\begin{cases} \{l_i(\mathbf{x}) + \xi_i\} = l_i(\{\mathbf{x}\}) + \{\xi_i\} + n_i & \text{for all } i \notin \gamma \\ \displaystyle\sum_{i \notin \gamma} (c_i l_i(\{\mathbf{x}\}) + c_i\{\xi\} + c_i n_i) = \frac{1}{2} \sum_{i=1}^{k} c_i. \end{cases} \tag{15}$$

It suffices to show that each equation in these systems defines a semi-linear set. Let us first consider an equation of type (14). This is equivalent to an equation

$$[l(\mathbf{x}) + \xi] = a_1[x_1] + \cdots + a_h[x_h] + [\xi] - n. \tag{16}$$

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

Now the set

$$\mathscr{B} = \{\mathbf{x} \mid [x_1] = \cdots = [x_h] = 0, [l(\mathbf{x}) + \xi] = [\xi] - n\}$$

is an intersection of stripes, whence $\mathscr{B}^*$ is semi-linear; but $\mathscr{B}^*$ is precisely the set of solutions of (16). In fact, (16) may be written in the form

$$[l(\mathbf{x}) + \xi] = l([\mathbf{x}]) + [\xi] - n$$

which is equivalent to

$$[l(\{\mathbf{x}\}) + \xi] = [\xi] - n.$$

Finally, the last equation in system (15) is of the type

$$l(\{\mathbf{x}\}) = \tau, \tag{17}$$

where again l is an integral form and $\tau \in \mathbb{Q}$. Let $\mathscr{B}$ be the set of solutions of the system

$$\begin{cases} l(\mathbf{x}) = \tau \\ [x_1] = \cdots = [x_h] = 0. \end{cases}$$

Clearly, $\mathscr{B}^*$ is semi-linear and coincides with the set of solutions of (17).

The statement about effectivity is a consequence of the proof. □

Concerning quasi-linear sets, we shall also need the following lemma.

LEMMA 5. *Let $\pi : \mathbb{R}^n \to \mathbb{R}^m$ be a linear map defined over $\mathbb{Q}$. If $V \subset \mathbb{R}^m$ is quasi-linear, then $\pi^{-1}(V)$ is quasi-linear.*

PROOF. We may assume without loss of generality that V is a starred hyperplane, that is,

$$V = \{\mathbf{x} \mid l(\mathbf{x}) + \xi \in \mathbb{Z}\}$$

for some integral linear form l and some $\xi \in \mathbb{Q}$. Then

$$\pi^{-1}(V) = \{\mathbf{y} \mid (l \circ \pi)(\mathbf{y}) + \xi \in \mathbb{Z}\}$$

and Lemma 4 applies. □

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

III. Structure of X_f We are ready to state our main results.

THEOREM 1. *Let f be as in* (11). *Then $X_f(a, q)$ is quasi-linear and effectively computable.*

By 'effectively computable' we mean that we may compute equations for the rational linear subspaces which, according to Definition 1, describe the quasi-linear set in question.

In the practical computation, however, we need a better way of finding the equations of the linear subspaces involved. We shall now describe a method which enables one to determine more quickly the positive dimensional pieces of X_f.

By Theorem 1, we may express X_f as a finite union of sets of the form $X^* \setminus \bigcup_{i=1}^{s} Y_i^*$, where X and the Y_i are affine rational linear spaces with $\dim Y_i < \dim X$. Observe that, by definition, $f = 0$ on X_f, hence f must vanish on X^*, except possibly for a lower dimensional set. We express this fact by the following definition.

DEFINITION 3. Let X be an affine rational subspace of $\mathbb{Q}^h$. We say that $f = 0$ on X^* *a.e.* (almost everywhere) if $f(x) = 0$ holds for all $x \in X^*$, except possibly for a lower dimensional linear set. We shall simply write $f = 0$ *a.e.* if $X = X^* = \mathbb{Q}^h$.

Recall that f is of type

$$f(\mathbf{x}) = \sum_{i=1}^{k} c_i((l_i(x_1, \ldots, x_h) + \xi_i)). \tag{18}$$

We shall say that a relation $f = 0$ on X^* *a.e.* is *indecomposable* if no proper subsum in (18) has the same property. Clearly any relation $f = 0$ on X^* *a.e.* can be split into indecomposable ones. Parametrizing X by means of linear substitutions, we may reduce to the case when $X = \mathbb{Q}^{h'}$ for some $h' \leq h$; in terms of the new parameters, we may assume that $f = 0$ *a.e.* on the whole space.

The next result will be useful to determine the indecomposable relations $f = 0$ *a.e.* of given length k.

THEOREM 2. *Let f be as in* (11) *and assume that $f = 0$ a.e. is an indecomposable relation. Then* rank $L_i \leq 1$. *If* rank $L_i = 1$, *after a linear substitution, we may write*

$$l_i(x) = m_i x, \quad \textit{where} \quad \gcd\{m_i\} = 1.$$

Then $m_i \neq 0$ for all i and, setting $M = \operatorname{lcm}\{m_i\} = \prod p^{\alpha_p}$, we have

(i) $\sum \alpha_p (p-1) \leq k-2$;

(ii) $M\left(\xi_i/m_i - \xi_j/m_j\right) \in \mathbb{Z}$ *for every* i, j .

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

We observe that condition (ii) enables one to assume $\xi_i \in (1/M)\mathbb{Z}$ after a suitable translation.

PROOF OF THEOREM 1. After a suitable substitution we may assume that rank $(l_1, \ldots, l_k) = h$. (This does not affect statement of the theorem. In fact, if $h >$ rank $(l_1, \ldots, l_k)$ we may write $l_1, \ldots, l_k$ as linear combinations with integral coefficients of suitable integral forms $m_1, \ldots, m_r$ of maximal rank, which will be taken as new variables. Then we may apply Lemma 5 and obtain that the inverse image of a quasi-linear set by this substitution is quasi-linear). We argue by induction on h. Let first $h = 1$. We distinguish two cases:

Case 1: $f = 0$ a.e.

Now $S_f = \mathbb{R} \setminus \mathscr{F}^*$, where $\mathscr{F} = \{c_1, \ldots, c_r\}$ is a finite set contained in $\mathbb{Q}$. If $\rho \notin X_f(a, q)$, then there exist $c \in \mathscr{F}$, $t \in \mathbb{Z}$ such that $m\rho = c + t$ for a suitable m coprime with den (ρ). In particular, den (ρ) divides a fixed integer, proving that

$$X_f = \mathbb{Q} \setminus \mathscr{H}^*,$$

where $\mathscr{H}$ is finite.

Case 2: $f \neq 0$ holds in an open set.

We apply Proposition 1 and obtain that if $\rho \in X_f(a, q)$ then $m_1\rho \in \mathbb{Z}$ for some bounded $m_1 \neq 0$. It is easy to conclude that $X_f = \mathscr{H}^*$ for some finite $\mathscr{H}$.

Now assume $h > 1$ and distinguish again two cases:

Case 1A: $f = 0$ a.e.

There are finitely many rational hyperplanes $\mathscr{P}_1, \ldots, \mathscr{P}_r$ such that $f(\mathbf{x}) = 0$ if $\mathbf{x} \notin \mathscr{P}_1^* \cup \cdots \cup \mathscr{P}_r^*$. Assume $\boldsymbol{\rho} \notin X_f(a, q)$; then, for some $m \equiv a \pmod q$, $(m, R) = 1$ and for some i we have $m\boldsymbol{\rho} \in \mathscr{P}_i^*$, whence $m\boldsymbol{\rho}$ satisfies $(m\boldsymbol{\rho} \cdot \mathbf{v}_i) \in \mathbb{Z}$, where we may assume $\mathbf{v}_i \in q\mathbb{Z}^h \setminus \{\mathbf{0}\}$. From this relation we see that den $(\boldsymbol{\rho} \cdot \mathbf{v}_i)$ divides den $(\boldsymbol{\rho})$ as well as m. Since $(m, R) = 1$ we get den $(\boldsymbol{\rho} \cdot \mathbf{v}_i) = 1$, that is, $(\boldsymbol{\rho} \cdot \mathbf{v}_i) \in \mathbb{Z}$.

Let $\gamma_i = \{\boldsymbol{\rho} \in \mathbb{Q}^h \mid (\boldsymbol{\rho} \cdot \mathbf{v}_i) \in \mathbb{Z}\}$. We have proved that

$$X_f(a, q) = \left(\mathbb{Q}^h \setminus \bigcup_{i=1}^{r} \gamma_i\right) \cup (X_f(a, q) \cap \gamma_1) \cup \cdots \cup (X_f(a, q) \cap \gamma_r).$$

Clearly, by Lemma 4, γ_i is quasi-linear. The proof will be complete if we show that, if $\gamma = \{\boldsymbol{\rho} \in \mathbb{Q}^h \mid m_1\rho_1 + \cdots + m_h\rho_h \in \mathbb{Z}\}$, where the m_i's are integers not all zero and divisible by q, then $\gamma \cap X_f(a, q)$ is quasi-linear.

Assume for instance $m_h \neq 0$ and set $m_1\rho_1 + \cdots + m_h\rho_h = m \in \mathbb{Z}$. We have seen in Lemma 3 that, if such assumption is satisfied, then the assertions $\boldsymbol{\rho} \in X_f(a, q)$ and $\boldsymbol{\rho}^* \in \bigcap_{t_0 \equiv a \pmod q} X_{g_{t_0 m}}(t_0, m_h)$ are equivalent, where $\boldsymbol{\rho}^* = (\rho_1/m_h, \ldots, \rho_{h-1}/m_h)$ and

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

the $g_{t_0 m}$ are given by (9). By the inductive assumption,

$$\bigcap_{t_0 \equiv a \pmod q} X_{g_{t_0 m}}(t_0, m_h) = \mathscr{H}_m,$$

where $\mathscr{H}_m$ is a quasi-linear set in $\mathbb{Q}^{h-1}$, depending only on the class of m mod m_h. Let $\bar{c}$ be a class mod m_h and set

$$\mathscr{R}_{\bar{c}} = \{\boldsymbol{\rho} \in \mathbb{Q}^h \mid m_1\rho_1 + \cdots + m_h\rho_h = m \in \mathbb{Z} \text{ for some } m \equiv \bar{c} \pmod{m_h}\}.$$

Clearly, $\mathscr{R}_{\bar{c}}$ is quasi-linear. If $\pi : \mathbb{Q}^h \to \mathbb{Q}^{h-1}$ is given by

$$\pi(x_1, \ldots, x_h) = \left(\frac{x_1}{m_h}, \ldots, \frac{x_{h-1}}{m_h}\right),$$

then we have shown that

$$\mathscr{R}_{\bar{c}} \cap X_f(a, q) = \mathscr{R}_{\bar{c}} \cap \pi^{-1}(\mathscr{H}_{\bar{c}}).$$

But $\pi^{-1}(\mathscr{H}_{\bar{c}})$ is quasi-linear by Lemma 5, so $\mathscr{R}_{\bar{c}} \cap X_f(a, q)$ is quasi-linear. Also

$$\gamma \cap X_f(a, q) = \bigcup_{c=1}^{m_h} \{\mathscr{R}_{\bar{c}} \cap X_f(a, q)\}$$

is quasi-linear. Finally,

$$X_f(a, q) = \left(\mathbb{Q}^h \setminus \bigcup_{j=1}^{r} \gamma_j\right) \cup (\gamma_1^* \cap X_f(a, q)) \cup \cdots \cup (\gamma_r^* \cap X_f(a, q))$$

is quasi-linear, as wanted.

Case 2A: $f \neq 0$ holds in an open set.

We may effectively determine a positive number $\delta < \frac{1}{2}$ and a cube of side 2δ such that $f(\mathbf{x}) \neq 0$ for all $\mathbf{x}$ inside that cube. By Proposition 1 we see that if $\boldsymbol{\rho} \in X_f(a, q)$, then $\boldsymbol{\rho}$ must satisfy at least one of finitely many relations $m_1\rho_1 + \cdots + m_h\rho_h \in \mathbb{Z}$ and now the proof proceeds exactly as before.

Finally, the proof is completely constructive and the statement about effectivity follows. □

For the proof of Theorem 2 we need a number of lemmas.

LEMMA 6. *We have the following identities*:

(i) $((-x)) = -((x))$ *for* $x \notin \mathbb{Z}$;

(ii) $((mx)) = \sum_{h \in (\mathbb{Z}/m\mathbb{Z})} ((x + h/m))$ *for* $m > 0$.

We omit the simple proof of this well-known fact (see for instance [14]).

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

LEMMA 7. *Let* $\alpha_1, \ldots, \alpha_T$ *be distinct* mod 1, $c_0, \ldots, c_T \in \mathbb{R}$ *and assume*

$$c_0 + \sum_{i=1}^{T} c_i((x + \alpha_i)) = 0 \quad a.e.$$

Then $c_i = 0$ *for every* i.

PROOF. Let $g(x) = c_0 + \sum_{i=1}^{T} c_i((x + \alpha_i))$. We have

$$c_i((x + \alpha_i)) = -c_0 - \sum_{j \neq i} c_j((x + \alpha_j)) \quad \text{a.e.}$$

In a suitable neighbourhood I of $-\alpha_i$ the right-hand side is equal to a linear function $l(x)$. For $x \in I$ we have

$$c_i((x + \alpha_i)) = \begin{cases} c_i(x - \alpha_i - 1/2) & \text{if } x > -\alpha_i; \\ c_i(x + \alpha_i + 1/2) & \text{if } x < -\alpha_i. \end{cases}$$

So, setting $h(x) = l(x) - c_i(x + \alpha_i)$, we have for $x \in I$

$$h(x) = \begin{cases} -c_i/2 & \text{for } x > -\alpha_i \text{ a.e.;} \\ c_i/2 & \text{for } x < -\alpha_i \text{ a.e.} \end{cases}$$

By continuity $c_i = 0$. □

Let

$$f(x) = c_0 + \sum_{i=1}^{k} c_i((m_i x + \beta_i)) = 0 \quad \text{a.e.} \tag{19}$$

be an indecomposable relation, where $m_i \neq 0$ are integers for every $i \geq 1$, and $c_i, \beta_i \in \mathbb{R}$. In view of Lemma 6 (i) we may assume $m_i > 0$. Let $M = \operatorname{lcm}\{m_i\}$.

LEMMA 8. *The following hold*

(i) $c_0 = 0$;

(ii) *there exists* β *such that* $\beta_i = m_i\beta + m_i b_i/M$, *where* $b_i \in \mathbb{Z}$. *In other words, after a suitable translation, all* β_i*s become rational with denominator* M;

(iii) *letting* χ_i *be the characteristic function of the arithmetic progression* $b_i + (M/m_i)\mathbb{Z}$, *we have*

$$\sum_{i=1}^{k} c_i \chi_i(n) = 0, \quad \textit{for } n \in \mathbb{Z}. \tag{20}$$

Moreover (20) *is indecomposable and primitive.*

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

Strictly speaking, statement (i) implies that the relation is decomposable. What we really mean is that no constant term appears in the definition of f given by (19).

PROOF. (i) The statement follows from the fact that $\int_0^1((mx+\beta))\,dx = 0$ for $m \neq 0$.

(ii) From Lemma 6 we have $0 = \sum_{i=1}^{k} c_i \sum_{h=0}^{m_i-1}((x+(h+\beta_i)/m_i))$. Denote by $\alpha_1, \ldots, \alpha_T$ the distinct classes mod 1 of the numbers $(h+\beta_i)/m_i$ as h and i vary. Grouping together the terms congruent mod 1 and applying Lemma 7 we get

$$c_j^* = \sum_{(h+\beta_i)/m_i \equiv \alpha_j} c_i = 0 \quad \text{for all } j. \tag{21}$$

Observation: if $(h_1+\beta_r)/m_r \equiv (h_2+\beta_s)/m_s$, then $\beta_r/m_r - \beta_s/m_s \in (1/[m_r, m_s])\mathbb{Z} \subset (1/M)\mathbb{Z}$.

Define an equivalence relation on $\{1, 2, \ldots, k\}$ by

$$r \sim s \iff \beta_r/m_r - \beta_s/m_s \in (1/M)\mathbb{Z}.$$

Let γ be any equivalence class. Observe that

$$\sum_{\substack{(h+\beta_i)/m_i \equiv \alpha_j \\ i \in \gamma}} c_i = 0.$$

In fact, either the sum is empty or it must contain all the terms occurring in (21) which, in view of the observation, must be equivalent. Working backwards, it follows that

$$\sum_{i \in \gamma} c_i((m_i x + \beta_i)) = 0 \quad \text{a.e.}$$

hence $\gamma = \{1, \ldots, k\}$. We thus may put $\beta_s/m_s = \beta + b_s/M$, where β is any of the β_r/m_r, proving (ii).

(iii) Let χ_i be the characteristic function of $b_i + (M/m_i)\mathbb{Z}$.

$$\sum c_i \chi_i(n) = \sum_{\substack{i,\ 0 \le h \le m_i - 1 \\ b_i + hM/m_i \equiv n \pmod M}} c_i = \sum_{b_i/M + h/m_i \equiv n/M \pmod 1} c_i$$

$$= \sum_{\substack{i,h \\ (h+\beta_i)/m_i \equiv n/M + \beta}} c_i = 0 \quad \text{(by (21))}.$$

Moreover, $\gcd(M/m_i) = 1$ since $\operatorname{lcm}\{m_i\} = M$. □

We finally remark that if (19) is not indecomposable, then (ii) may not be true, whence a corresponding relation (20) may not exist. On the contrary, starting from (20), we are led to (19) and this will be indecomposable if and only if (20) is such.

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

LEMMA 9. *Let $L_1, \dots, L_k$ be linear forms in $x_1, \dots, x_h$ with rational coefficients, $\beta_1, \dots, \beta_k$ be reals and assume we have an indecomposable relation*

$$\sum_{i=1}^{k} c_i((L_i(x_1, \dots, x_h) + \beta_i)) = 0 \quad a.e. \tag{22}$$

Then rank $(L_1, \dots, L_k) \leq 1$.

PROOF. After a rational linear change of variables we may assume that the rank of $L_1, \dots, L_k$ is equal to h and $L_1 = x_1, \dots, L_h = x_h$. Consider another term and write it in as $((\lambda + \gamma))$ where $\gamma \in \mathbb{R}$ and $\lambda = \lambda(x_1 \dots, x_h) = mx_1 + l(x_2, \dots, x_h)$. Assume now that $m \in \mathbb{Q} \setminus \{0\}$ and l is a non-zero linear form with rational coefficients. Specialize now $x_2, \dots, x_h$ to $x_2^*, \dots, x_h^* \in \mathbb{R}$ such that

$$\sum_{i=1}^{k} c_i((L_i(x_1, x_2^*, \dots, x_h^*) + \beta_i)) = 0 \quad \text{a.e.} \tag{23}$$

as a relation in x_1. This holds for almost all specializations, say those belonging to a set $Y_1 \subset \mathbb{R}^{h-1}$. Now (23) in general could be decomposable. We claim however that, for almost all specializations in Y_1, the term in question will lie in an indecomposable subsum *different* from that of $((L_1 + \beta_1))$. In fact, let Y_2 be the set for which the two terms belong to the same indecomposable subsum. This subsum can be written in the form (19) after a substitution $x_1 = qx$, where q is a suitable non-zero integer. In particular, $qm = m'$ is a non-zero integer. Observe that q does not depend on the particular specialization for $x_2, \dots, x_h$; hence the same holds for the integers m_i occurring in the expression of the subsum in the form (19).

By Lemma 8 (ii), applied to both terms in question, we easily get

$$\beta_1 - \frac{\lambda + l(x_2^*, \dots, x_h^*)}{m} \in \frac{1}{M'}\mathbb{Z}$$

for a certain integer M' independent of the chosen specialization in Y_2. This however can hold only for $(x_2^*, \dots, \mathbf{x}_h^*)$ lying in a subset of $\mathbb{R}^{h-1}$ of measure zero, since $l \neq 0$. This proves our claim.

We may rephrase our conclusion by saying that, for almost all specializations of the last $h - 1$ variables, the indecomposable subsum of L_1 in (23) will contain either terms originally depending only on x_1 or constant terms, originally depending only on $x_2, \dots, x_h$. In particular, take one such specialization and consider the indecomposable subsum containing $((L_1 + \beta_1))$ in (23). There exists $i_1 < i_2 < \cdots < i_t$ such that

$$\sum_{\mu=1}^{t} c_{i_\mu}((L_{i_\mu}(x_1, x_2^*, \dots, x_h^*) + \beta_{i_\mu})) = 0 \quad \text{a.e.}$$

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

is indecomposable as a relation in x_1. By Lemma 8 (i), we may neglect the terms independent of x_1. By the above argument, the remaining terms were originally dependent only on x_1, whence

$$\sum_{\mu=1}^{t} c_{i_\mu}((L_{i_\mu}(x_1, x_2, \ldots, x_h) + \beta_{i_\mu})) = 0 \quad \text{a.e.}$$

is a vanishing subsum of (22), which is proper if $h > 1$. □

Before proving Theorem 2 we quote one more lemma, proved in [4] as Theorem 2. Let

$$\chi_i(n) = \begin{cases} 1 & \text{if } n \equiv a_i \pmod{q_i}; \\ 0 & \text{otherwise} \end{cases} \tag{24}$$

be the characteristic function of the arithmetic progression $a_i + q_i\mathbb{Z}$. Assume that we have an indecomposable relation

$$\sum_{i=1}^{k} c_i \chi_i(n) = 0 \qquad \forall n \in \mathbb{N} \tag{25}$$

holding over a field K, where $c_i \in K$. Let also $Q = \operatorname{lcm}\{q_1, \ldots, q_k\}$ and assume that $(q_1 \ldots, q_k) = 1$. Then

LEMMA 10. *The number of terms k in* (25) *is at least*

$$2 + \sum_{\nu=1}^{r} h_\nu(p_\nu - 1). \tag{26}$$

PROOF OF THEOREM 2. That rank $L_i \leq 1$ is the content of Lemma 9.

Assume $h = 1$ and $l_i(x) = m_i x$, $\gcd\{m_i\} = 1$. As in Lemma 8 we may assume $m_i \geq 0$ for all i: namely we use (i) of Lemma 6 in the form

$$((m_i x + \xi_i)) = -(((-m_i)x - \xi_i)) \quad \text{a.e.}$$

whenever $m_i < 0$. Such substitution does not affect (i) and (ii) of Theorem 2 and moreover the new relation $f = 0$ a.e. is still indecomposable if $k > 2$ (if $k = 2$ then the same is true unless f is of type $f = \lambda((x + \xi)) + \lambda((-x - \xi))$, in which case the theorem holds).

Now, the fact $m_i \neq 0$ for every i is Lemma 8 (i). With the notation of that lemma we obtain the indecomposable relation

$$\sum_{i=1}^{k} c_i \chi_i(n) = 0 \quad \forall n \in \mathbb{Z}$$

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

among the characteristic functions χ_i of the arithmetic progressions $b_i + (M/m_i)\mathbb{Z}$. Then Lemma 10 implies (i). Finally Lemma 8 (ii) implies immediately (ii). □

In the next section we give an example how Theorem 2 may be useful in the practical computation of the linear set in the statement of Theorem 1.

3. Attainment of the parametric families in Schwarz's list

The argument we are going to present is perhaps rather lengthy, but we remark that in principle the computations involved are a computer job and may be implemented in every analogous situation.

First of all we show that the set of triples of reals (x, y, z) such that either $\{x\} \le \{z\} < \{y\}$ or $\{y\} \le \{z\} < \{x\}$ coincides with the set of solutions of

$$f(x, y, z) = 2((z)) - ((x)) - ((y)) - ((z - x)) - ((z - y)) = 0. \tag{27}$$

In fact, observe that, for reals α, β

$$\delta(\alpha, \beta) = ((\beta)) - ((\alpha)) - ((\beta - \alpha)) = \begin{cases} 1/2 & \text{if } \{\alpha\} \le \{\beta\}; \\ -1/2 & \text{if } \{\alpha\} > \{\beta\}. \end{cases}$$

Our assertion follows, since

$$f(x, y, z) = \delta(x, z) + \delta(y, z).$$

By Landau's (or Katz's) criterion, the set Ω of relevant triples of rationals $(a/m, b/m, c/m)$ consists of those such that, for every n coprime to m,

$$\text{either} \quad \left\{\frac{na}{m}\right\} < \left\{\frac{nc}{m}\right\} < \left\{\frac{nb}{m}\right\} \quad \text{or} \quad \left\{\frac{nb}{m}\right\} < \left\{\frac{nc}{m}\right\} < \left\{\frac{na}{m}\right\}.$$

In particular, $\Omega \subset X_f$. If $(a/m, b/m, c/m) \in X_f \setminus \Omega$ then, for some n coprime to m either $na \equiv nc \pmod M$ or $nb \equiv nc \pmod M$ whence $a \equiv c$ or $b \equiv c \pmod M$. By symmetry, we may thus assume that $(a/m, b/m, a/m) \in X_f$. This is however impossible unless $a \equiv 0 \pmod M$, since otherwise $\{na/m\}$ would be less than $\{nb/m\}$ for all n coprime to m. But

$$\left\{\frac{na}{m}\right\} < \left\{\frac{nb}{m}\right\} \implies \left\{\frac{-na}{m}\right\} > \left\{\frac{-nb}{m}\right\}$$

hence we get a contradiction. We have proved that

$$X_f \setminus \Omega = \{(\mathbb{Q} \setminus \mathbb{Z}) \times \mathbb{Z} \times \mathbb{Z}\} \cup \{\mathbb{Z} \times (\mathbb{Q} \setminus \mathbb{Z}) \times \mathbb{Z}\}. \tag{28}$$

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

From Theorem 1 we conclude at once that Ω is a quasi-linear set.

We now show how the preceding methods can be used to determine X_f, apart from a set $\mathscr{F}^*$ where $\mathscr{F}$ is finite.

We begin by showing that X_f does not contain two-parameter families. Assume the contrary; by Lemma 9 the relation resulting from (27) after the parametrization of the family must be reducible. Let us consider the partition λ corresponding to the indecomposable subsums. It cannot be of type $(4, 1)$: in fact, consider the corresponding indecomposable relation with four terms: any four of the linear forms $z, x, y, z-x, z-y$ occurring in formula (27) have rank 3, so x, y, z can be written as linear combinations of those four terms. But, by Lemma 9, after the parametrization all four terms depend on one parameter only, so the same should be true for x, y, z.

The same argument works if λ is of type $(3, 2)$ except for the case when the indecomposable subsums are

$$2((z)) - ((x)) - ((z-x)) \quad \text{and} \quad ((y)) + ((z-y))$$

or, symmetrically,

$$2((z)) - ((y)) - ((z-y)) \quad \text{and} \quad ((x)) + ((z-x)).$$

Take the first case. Letting $x = \tilde{x}(t, u) + \lambda$, $y = \tilde{y}(t, u) + \mu$, $z = \tilde{z}(t, u) + \nu$ where $\tilde{x}, \tilde{y}, \tilde{z}$ are linear homogeneous, Lemma 9 implies that

$$\operatorname{rank}(\tilde{y}, \tilde{z} - \tilde{y}) \leq 1, \quad \operatorname{rank}(\tilde{z}, \tilde{x}, \tilde{z} - \tilde{x}) \leq 1.$$

Since, however, we are assuming $\operatorname{rank}(\tilde{x}, \tilde{y}, \tilde{z}) = 2$, the only possibility is $\tilde{z} = 0$. Finally the relation

$$((y)) + ((z-y)) = 0 \quad \text{a.e.}$$

would imply $z = 0$, whence $2((0)) - ((x)) - ((-x)) = -1$ a.e. unless $\tilde{x} = 0$, which gives a one-parameter family (actually in this way we find the components of $X_f \setminus \Omega$).

It is even more straightforward to check that a partition in more than two subsets gives rise to two independent relations among $\tilde{x}, \tilde{y}, \tilde{z}$.

We are left with the case $\operatorname{rank}(\tilde{x}, \tilde{y}, \tilde{z}) = 1$. Assume first that the resulting relation is indecomposable. By Theorem 2 we may write

$$\begin{aligned} &\tilde{z} = m_1 t, \quad \tilde{x} = m_2 t, \quad \tilde{y} = m_3 t, \quad m_1 \neq m_2, \quad m_1 \neq m_3, \\ &M = \operatorname{lcm}(m_1, m_2, m_3, m_1 - m_2, m_1 - m_3) = \prod p^{\alpha_p}, \\ &1 = \gcd(m_1, m_2, m_3, m_1 - m_2, m_1 - m_3). \end{aligned}$$

Moreover, $\sum \alpha_p (p-1) \leq 3$, whence $M = 1, 2, 3, 4, 6, 8$. But M is clearly even, and so we are left with the cases $M = 2, 4, 6, 8$. Changing if necessary t with $-t$ we may

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

assume $m_1 > 0$. Also, in view of the symmetries among x and $z - x$, y and $z - y$, x and y, we may reduce to $m_3 \geq m_2 \geq m_1/2 > 0$.

It is now practical to work with the arithmetic progressions associated to the functions $((mt + \xi))$ according to Lemma 8. Denoting by $\chi(q, b)$ the characteristic function of the arithmetic progression $b + q\mathbb{Z}$ we get

$$2\chi\left(\frac{M}{m_1}, b_1\right) = \chi\left(\frac{M}{m_2}, b_2\right) + \chi\left(\frac{M}{m_3}, b_3\right) \pm \chi\left(\frac{M}{|m_1 - m_2|}, b_4\right) \pm \chi\left(\frac{M}{|m_1 - m_3|}, b_5\right),$$

where the signs equal $\operatorname{sign}(m_1 - m_2)$ or $\operatorname{sign}(m_1 - m_3)$ respectively. Reduce the relation mod 2, getting

$$\chi\left(\frac{M}{m_2}, b_2\right) + \chi\left(\frac{M}{m_3}, b_3\right) + \chi\left(\frac{M}{|m_1 - m_2|}, b_4\right) + \chi\left(\frac{M}{|m_1 - m_3|}, b_5\right) \equiv 0.$$

If $M \geq 6$, this relation must be decomposable in $\mathbf{F}_2$ by Lemma 10. The splitting will be necessarily $(2, 2)$, that is, we must have two pairs of equal progressions, say χ_2, χ_3. But then

$$2\chi\,(M/m_1, b_1) = 2\chi_2 \pm 2\chi_3$$

is a relation of three terms, which implies $M \leq 2$. Hence $M \leq 4$. We have the following list of possibilities:

	M	m_1	m_2	m_3	$m_1 - m_2$	$m_1 - m_3$
I	2	1	2	2	−1	−1
II	2	2	1	1	1	1
III	4	2	1	4	1	−2

According to Lemma 8, we may have the following possibilities:

(I) $2\chi(2, b_1) = \chi(1, 0) + \chi(1, 0) - \chi(2, b_1) - \chi(2, b_1)$ *false*;

(II) $2\chi(1, 0) = \chi(2, b_2) + \chi(2, b_3) + \chi(2, -b_2) + \chi(2, -b_3)$ *true* when $b_2 \not\equiv b_3 \pmod 2$;

(III) $2\chi(2, b_1) = \chi(4, b_3) + \chi(1, 0) + \chi(4, 2b_1 - b_3) - \chi(2, b_1)$ *false*.

The true relation (II), say with $b_2 = 0$, $b_3 = 1$, corresponds to the family

$$z = 2t, \quad x = t, \quad y = t + 1/2.$$

Now we deal with decomposable relations. Start with partitions containing a singleton. By symmetry such singleton may be assumed to be either $2((z))$ or $((x))$. In the first case $z = 1/2$, and the remaining terms give rise to

$$((x)) + ((1/2 - x)) + ((y)) + ((1/2 - y)) = 0.$$

https://doi.org/10.1017/S144678870000241X Published online by Cambridge University Press

Assume this to be decomposable, $x = m_1 t + \xi_1$, $y = m_2 t + \xi_2$, $(m_1, m_2) = 1$. We may assume $M = \operatorname{lcm}(m_1, m_2) \leq 4$, hence, by symmetry, $m_1 = 1$, $|m_2| = M$. By Theorem 2 (ii)

$$\frac{\xi}{m_2} - \frac{\xi_2 - 1/2}{m_2} \in \frac{1}{M}\mathbb{Z},$$

a contradiction. Hence such relation becomes decomposable. If the corresponding partition λ is of type (3, 1) we again get a contradiction with (i) of Lemma 8. If λ is of type (2, 2) or (2, 1, 1), necessarily $((x)) + ((y))$ or $((x)) + ((-y + 1/2))$ is a vanishing subsum. We get thus two solutions (which become however equivalent under the action of the Schwarz's group)

$$z = 1/2, \quad y = -x$$

or

$$z = 1/2, \quad y = x + 1/2.$$

If the singleton is $((x))$ the remaining terms give rise to

$$2((z)) - ((y)) - ((z - y)) - ((z - 1/2)) = 0.$$

By direct checking one sees that this must be decomposable. Let $\tilde{z} = m_1 t$, $\tilde{y} = m_2 t$, $(m_1, m_2) = 1$, $M = \operatorname{lcm}(m_1, m_2, m_2 - m_1)$. Since $M \leq 4$, by Theorem 2 we get $M = 1, 2$ and, M being even, $M = 2$.

Arguing as before we only consider the case $m_1 = 1$, $m_2 = 2$, giving

$$2((t)) - ((2t + \xi)) + ((t + \xi)) - ((t - 1/2)) = 0 \quad \text{a.e.}$$

By Theorem 2 (ii), $\xi/2 \in (1/2)\mathbb{Z}$; this implies that ξ may be assumed to be 0, giving a false identity.

Finally, we consider a partition of type (3, 2). But the indecomposable relations of length 2 and 3 are, up to a translation, multiples of

$$((t)) + ((-t)) = 0 \quad \text{a.e.} \qquad ((2t)) - ((t)) - ((t + 1/2)) = 0 \quad \text{a.e.}$$

and this excludes immediately this last possibility.

Acknowledgement

The authors thank the School of Mathematics of the Institute for Advanced Study for the support and hospitality when the final version of this paper was prepared. They

also wish to thank the James D. Wolfensohn Foundation for the financial support during their stay at the Institute.

References

[1] F. Baldassarri and B. Dwork, 'On second order linear differential equations with algebraic solutions', *Amer. J. Math.* **101** (1979), 42–76.
[2] F. Beukers and G. Heckman, 'Monodromy for the hypergeometric function ${}_nF_{n-1}$', *Invent. Math.* **95** (1989), 325–354.
[3] H. Davenport and A. Schinzel, 'Diophantine approximation and sums of roots of unity', *Math. Ann.* **169** (1967), 118–135.
[4] R. Dvornicich and U. Zannier, 'On sums of roots of unity', *Monatsh. Math.* **129** (2000), 97–108.
[5] A. Errera, 'Zahlentheoretische Lösung einer functionentheoretischen Frage', *Rend. Circ. Mat. Palermo* **35** (1913), 107–144.
[6] G. H. Hardy and E. M. Wright, *Introduction to the theory of numbers* (Oxford at Clarendon Press, 1979).
[7] A. J. Jones, 'Cyclic overlattices (I)', *Acta Arith.* **XVII** (1970), 303–314.
[8] ———, 'Cyclic overlattices (II)', *Acta Arith.* **XVIII** (1971), 93–103.
[9] N. M. Katz, 'Algebraic solutions of differential equations (p-curvature and the Hodge filtration)', *Invent. Math.* **18** (1972), 1–118.
[10] ———, 'A conjecture in the arithmetic theory of differential equations', *Bull. Soc. Math. France* **110** (1982), 203–239.
[11] E. Landau, 'Eine Anwendung des Eisensteinschen Satzes auf die Theorie der Gaussschen Differentialgleichung', *J. Reine Angew. Math.* **127** (1904), 92–102.
[12] ———, 'Über einen zahlentheoretischen Satz und seine Anwendung auf die hypergeometrische Reihe', *S.-B. Heidelberger Akad. Wiss.* **18** (1911), 3–38.
[13] M. Matsuda, *Lectures on algebraic solutions of hypergeometric differential equations* (Dept. of Mathematics, Kyoto Univ., Kinokuniya Co., Ltd., 1985).
[14] J. Milnor, 'On polylogarithms, Hurwitz zeta-functions, and the Kubert identities', *Enseign. Math.* **29** (1983), 281–322.
[15] H. A. Schwarz, 'Über diejenigen Fälle, in welchen die gaussische hypergeometrische Reihe eine algebraische Function ihres vierten Elementes darstellt', *J. Reine Angew. Math.* **75** (1873), 292–335.

Dipartimento di Matematica
via Buonarroti, 2
56127 Pisa
Italy
e-mail: dvornic@dm.unipi.it

Istituto Universitario di Architettura D.C.A.
S. Croce, 191 (Tolentini)
30135 Venezia
Italy
e-mail: zannier@brezza.iuav.unive.it