ACTA ARITHMETICA
LXXVI.2 (1996)

Equations in roots of unity

by

Hans Peter Schlickewei (Ulm)

1. Introduction. Suppose that $n \geq 1$ and that $a_1, \ldots, a_n$ are nonzero complex numbers. We study equations

$$a_1\xi_1 + \ldots + a_n\xi_n = 1 \tag{1.1}$$

to be solved in roots of unity ξ_i. We call a solution $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_n)$ of (1.1) *nondegenerate* if $\sum_{i\in I} a_i\xi_i \neq 0$ for each nonempty subset I of $\{1, \ldots, n\}$. Write $\nu(a_1, \ldots, a_n)$ for the number of nondegenerate solutions $\boldsymbol{\xi}$ of (1.1), whose components are roots of unity. Equations (1.1) have been first studied by H. B. Mann [2]. His result implies that for $a_1, \ldots, a_n \in \mathbb{Q}$ we have

$$\nu(a_1, \ldots, a_n) \leq e^{c_1 n^2},$$

where c_1 is a positive absolute constant. This was improved by J. H. Conway and A. J. Jones [1]. They proved that for $a_1, \ldots, a_n \in \mathbb{Q}$ we get

$$\nu(a_1, \ldots, a_n) = O_c(\exp(cn^{3/2}(\log n)^{1/2}))$$

for any $c > 1$. In the case when $a_1, \ldots, a_n$ lie in a number field K of degree d, A. Schinzel [4] has shown that

$$\nu(a_1, \ldots, a_n) \leq c_2(n, d)$$

for some function c_2, which depends only upon n and d. U. Zannier [7] has improved upon Schinzel's result and also determined c_2 explicitly.

In the current paper we address the problem to derive a bound for $\nu(a_1, \ldots, a_n)$ for arbitrary complex numbers a_i. We prove that in fact

$$\nu(a_1, \ldots, a_n) \leq c_3(n),$$

i.e., we derive a uniform bound that depends only upon n.

Write E for the group of roots of unity. Given a point $\boldsymbol{w} = (w_1, \ldots, w_n)$ in E^n and a natural number m we write $A(\boldsymbol{w}, m)$ for the set of points $\boldsymbol{v} = (v_1, \ldots, v_n) \in E^n$ with components of the shape $v_i = \eta_i w_i$, where η_i is an mth root of unity. We prove

THEOREM. *There exist points* $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t \in E^n$ *with*

$$t \leq 2^{2(n+1)!} \tag{1.2}$$

and there exist prime numbers

$$p_1 < p_2 < \ldots < p_s \leq (n+1)!$$

with the following property: *Any nondegenerate solution* $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_n)$ *of* (1.1) *in roots of unity is contained in the union*

$$\bigcup_{\tau=1}^{t} A(\boldsymbol{w}_\tau, p_1 \ldots p_s).$$

Moreover, *we have for any nonzero complex numbers* $a_1, \ldots, a_n$

$$\nu(a_1, \ldots, a_n) \leq 2^{4(n+1)!}. \tag{1.3}$$

We remark at this point that the results of [1], [2], [4] and [7] for rational or algebraic coefficients a_i respectively are constructive, i.e., in principle the proofs provide us with algorithms to determine explicitly the solutions $\boldsymbol{\xi}$ of (1.1). This is no longer the case with our Theorem. In fact, it is not clear how our method of proof could give us an effective procedure to construct the points $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_t$.

In a subsequent paper [5] we will apply our result to estimate the number of solutions of linear equations over division groups of finitely generated subgroups G of the multiplicative group $\mathbb{C}^*$. In that wider setting the current Theorem establishes the result of [5] for groups G of rank 0.

2. Rational coefficients. Suppose $m \geq 2$. Let $b_1, \ldots, b_m$ be nonzero integers and consider the relation

$$\sum_{i=1}^{m} b_i \xi_i = 0, \tag{2.1}$$

where the ξ_i are roots of unity. We say that a solution $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$ of (2.1) is *nondegenerate* if for each nonempty proper subset I of $\{1, \ldots, m\}$ we have

$$\sum_{i \in I} b_i \xi_i \neq 0. \tag{2.2}$$

LEMMA 2.1. *There exist distinct primes* $p_1, \ldots, p_u \leq m$ *such that any nondegenerate solution* $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$ *of* (2.1) *in roots of unity is of the shape*

$$\xi_i = \xi \eta_i, \tag{2.3}$$

where the η_i *are* $p_1 \ldots p_u$*-th roots of unity* (*and where* ξ *is a suitable root of unity*).

This is Theorem 1 of H. B. Mann [2].

LEMMA 2.2. *Let the hypotheses be the same as in Lemma* 2.1. *Then the primes* $p_1, \dots, p_u$ *satisfy*

$$\sum_{i=1}^{u} (p_i - 2) \le m - 2. \tag{2.4}$$

This is Theorem 5 of Conway and Jones [1].

3. Multilinear maps. Let $\mathbb{C}^N$ be the vector space of N-tuples $(x_1, \dots, x_N)$. Let $\mathfrak{S}_N$ be the group of permutations of $\{1, \dots, N\}$, so that $|\mathfrak{S}_N| = N!$. Let V be the space of vectors with components z_σ $(\sigma \in \mathfrak{S}_N)$, so that $\dim V = N!$. We introduce the map from $\mathbb{C}^N \times \dots \times \mathbb{C}^N$ (with N factors) into V given by

$$(\boldsymbol{x}_1, \dots, \boldsymbol{x}_N) \mapsto \boldsymbol{z}(\boldsymbol{x}_1, \dots, \boldsymbol{x}_N).$$

Here $\boldsymbol{z}$ has components

$$z_\sigma = (\operatorname{sign} \sigma) x_{1,\sigma(1)} \dots x_{N,\sigma(N)}, \tag{3.1}$$

where $\boldsymbol{x}_i = (x_{i1}, \dots, x_{iN})$ and $\operatorname{sign} \sigma = \pm 1$ according as σ is an even or odd permutation. It is clear that $\boldsymbol{z}$ is linear in each $\boldsymbol{x}_i$ and we have

$$\sum_{\sigma \in \mathfrak{S}_N} z_\sigma(\boldsymbol{x}_1, \dots, \boldsymbol{x}_N) = \det(\boldsymbol{x}_1, \dots, \boldsymbol{x}_N). \tag{3.2}$$

Suppose we are given a hyperplane U of $\mathbb{C}^N$ defined by the equation

$$\sum_{i=1}^{N} c_i x_i = 0. \tag{3.3}$$

Assume that the coefficients in (3.3) satisfy

$$c_1 \dots c_N \neq 0. \tag{3.4}$$

Given vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_N \in U$, we obviously get

$$\sum_{\sigma \in \mathfrak{S}_N} z_\sigma(\boldsymbol{x}_1, \dots, \boldsymbol{x}_N) = 0. \tag{3.5}$$

LEMMA 3.1. *Let* d_σ $(\sigma \in \mathfrak{S}_N)$ *be complex numbers such that*

$$\sum_{\sigma \in \mathfrak{S}_N} d_\sigma z_\sigma(\boldsymbol{x}_1, \dots, \boldsymbol{x}_N) = 0 \tag{3.6}$$

for each tuple of points $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_N)$ *with* $\boldsymbol{x}_i \in U$ $(1 \le i \le N)$. *Then* $(d_\sigma)_{\sigma \in \mathfrak{S}_N}$ *is proportional to* $(1, \dots, 1)$, *i.e.*, (3.6) *is a consequence of* (3.5).

This is Lemma 4 of [6].

Write $\mathfrak{M}$ for the set of proper nonempty subsets $\mathfrak{R}$ of $\mathfrak{S}_N$. Given $\mathfrak{R} \in \mathfrak{M}$ we define the multilinear form $F_{\mathfrak{R}}$ in vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N \in U$, by

$$F_{\mathfrak{R}}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N) = \sum_{\sigma \in \mathfrak{R}} z_\sigma(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N). \tag{3.7}$$

Lemma 3.1 implies that $F_{\mathfrak{R}}$ does not vanish identically on $U \times \ldots \times U$ (N factors). We may conclude that the set of points $\boldsymbol{y} \in U$ such that $F_{\mathfrak{R}}(\boldsymbol{y}, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_N)$ vanishes identically in $\boldsymbol{x}_2, \ldots, \boldsymbol{x}_N \in U$ is a proper subspace of U. We denote this subspace by $U_{1\mathfrak{R}}$. We may perform this procedure for every $\mathfrak{R} \in \mathfrak{M}$. Now pick an element $\boldsymbol{y}_1 \in U \setminus \bigcup_{\mathfrak{R} \in \mathfrak{M}} U_{1\mathfrak{R}}$. Consider the set of elements $\boldsymbol{y} \in U$ such that $F_{\mathfrak{R}}(\boldsymbol{y}_1; \boldsymbol{y}, \boldsymbol{x}_3, \ldots, \boldsymbol{x}_N)$ vanishes identically as $\boldsymbol{x}_3, \ldots, \boldsymbol{x}_N$ run through U. By our choice of $\boldsymbol{y}_1$, this condition defines for each $\mathfrak{R} \in \mathfrak{M}$ a proper subspace $U_{2\mathfrak{R}}$ of U. Pick $\boldsymbol{y}_2$ in $U \setminus \bigcup_{\mathfrak{R} \in \mathfrak{M}} U_{2\mathfrak{R}}$. Our set of multilinear forms $F_{\mathfrak{R}}$ ($\mathfrak{R} \in \mathfrak{M}$) is symmetric in the following sense: For each $\mathfrak{R} \in \mathfrak{M}$ and for each $\sigma \in \mathfrak{S}_N$ there exists $\mathfrak{R}' \in \mathfrak{M}$ such that

$$F_{\mathfrak{R}}(\boldsymbol{x}_{\sigma(1)}, \ldots, \boldsymbol{x}_{\sigma(N)}) = \pm F_{\mathfrak{R}'}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n).$$

It follows that we have

$$\bigcup_{\mathfrak{R} \in \mathfrak{M}} U_{2\mathfrak{R}} \supset \bigcup_{\mathfrak{R} \in \mathfrak{M}} U_{1\mathfrak{R}}.$$

We may continue our construction in an obvious way. Finally, we get points $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{N-1}$ and subspaces $U_{i\mathfrak{R}}$ for $i = 1, \ldots, N-1$ and $\mathfrak{R} \in \mathfrak{M}$. Then each equation

$$F_{\mathfrak{R}}(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{N-1}, \boldsymbol{x}) = 0 \quad \text{in } \boldsymbol{x} \in U \tag{3.8}$$

will define a proper subspace $U_{N\mathfrak{R}}$ of U and we have

$$\bigcup_{\mathfrak{R} \in \mathfrak{M}} U_{N\mathfrak{R}} \supset \bigcup_{\mathfrak{R} \in \mathfrak{M}} U_{N-1,\mathfrak{R}} \supset \ldots \supset \bigcup_{\mathfrak{R} \in \mathfrak{M}} U_{1\mathfrak{R}}.$$

Our construction now implies

Lemma 3.2. *Suppose the points $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{N-1}$ and the subspaces $U_{N\mathfrak{R}}$ ($\mathfrak{R} \in \mathfrak{M}$) are constructed as above. Then for each point $\boldsymbol{x} \in U \setminus \bigcup_{\mathfrak{R} \in \mathfrak{M}} U_{N\mathfrak{R}}$ we have*

$$\sum_{\sigma \in \mathfrak{S}_N} z_\sigma(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{N-1}, \boldsymbol{x}) = 0 \tag{3.9}$$

but no proper nonempty subsum of the left hand side of (3.9) *vanishes.*

For the proof it suffices to observe that the subsums of (3.9) are just our multilinear forms $F_{\mathfrak{R}}$. But our construction is such that for $\boldsymbol{x} \in U \setminus \bigcup_{\mathfrak{R} \in \mathfrak{M}} U_{N\mathfrak{R}}$ we have $F_{\mathfrak{R}}(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{N-1}, \boldsymbol{x}) \neq 0$ for each $\mathfrak{R} \in \mathfrak{M}$.

We finally remark that the number of subspaces $U_{N\mathfrak{R}}$ ($\mathfrak{R} \in \mathfrak{M}$) is bounded by

$$2^{N!}. \tag{3.10}$$

4. Linear subspaces. Let $N \geq 2$ and suppose that $c_1, \ldots, c_N$ are nonzero complex numbers. Consider the subspace U of $\mathbb{C}^N$ defined by

$$c_1x_1 + \ldots + c_Nx_N = 0, \tag{4.1}$$

which was already studied in Section 3. Write B for the subset of points $\boldsymbol{x} = (x_1, \ldots, x_N)$ in U whose components x_i are roots of unity. Denote by E the set of all roots of unity and by E_m the set of mth roots of unity. If $B \neq \emptyset$, we define for $\boldsymbol{u} \in B$ and for $l \in \mathbb{N}$ the set $B(\boldsymbol{u}, l)$ by

$$B(\boldsymbol{u}, l) = \{(\zeta\zeta_1u_1, \ldots, \zeta\zeta_Nu_N) \mid \zeta \in E,\ \zeta_i \in E_l\}. \tag{4.2}$$

LEMMA 4.1. *Suppose that $B \neq \emptyset$. Then there exists $\boldsymbol{u}_0 \in B$, there are primes $q_1 < \ldots < q_a$ with*

$$\sum_{i=1}^{a}(q_i - 2) \leq N! - 2$$

and there are proper linear subspaces $W_1, \ldots, W_{t_1}$ of U such that the following assertion holds true: *The set of solutions B of* (4.1) *in roots of unity is contained in the union*

$$B(\boldsymbol{u}_0, q_1 \ldots q_a) \cup W_1 \cup \ldots \cup W_{t_1}.$$

Here we have

$$t_1 \leq 2^{N!}. \tag{4.3}$$

P r o o f. Recall the definition of the multilinear forms $F_{\mathfrak{R}}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N)$ in (3.7). The subspaces $U_{1\mathfrak{R}}$ ($\mathfrak{R} \in \mathfrak{M}$) in Section 3 do not depend on any choice of points. We distinguish two cases: Either B is contained in the union $\bigcup_{\mathfrak{R}\in\mathfrak{M}} U_{1\mathfrak{R}}$. Then obviously the assertion of the lemma is satisfied with $\{W_1, \ldots, W_{t_1}\} = \{U_{1\mathfrak{R}} \mid \mathfrak{R} \in \mathfrak{M}\}$. In that case the set $B(\boldsymbol{u}_0, q_1 \ldots q_a)$ will not be needed at all. So any $\boldsymbol{u}_0 \in B$ and any primes $q_1 < \ldots < q_a$ as in the assertion will do. Otherwise we may pick $\boldsymbol{y}_1 \in B \setminus \bigcup_{\mathfrak{R}\in\mathfrak{M}} U_{1\mathfrak{R}}$ and define subspaces $U_{2\mathfrak{R}}$ ($\mathfrak{R} \in \mathfrak{M}$) with respect to $\boldsymbol{y}_1$. Then if $B \subset \bigcup_{\mathfrak{R}\in\mathfrak{M}} U_{2\mathfrak{R}}$, we may choose $\boldsymbol{u}_0 \in B$, $q_1 < q_2 < \ldots < q_a$ according to the assertion arbitrarily and again the lemma follows. Continuing in this way, there are two alternatives: either the construction ends after step j with $j \leq N-1$, B will be contained in the union $\bigcup_{\mathfrak{R}\in\mathfrak{M}} U_{j\mathfrak{R}}$ and we are done. Or we may find points $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_{N-1} \in B$ and define subspaces $U_{N\mathfrak{R}}$ ($\mathfrak{R} \in \mathfrak{M}$) with respect to these points.

Then we take $\{W_1, \dots, W_{t_1}\} = \{U_{N\mathfrak{R}} \mid \mathfrak{R} \in \mathfrak{M}\}$. We now assume that $B \setminus \bigcup_{\mathfrak{R}\in\mathfrak{M}} U_{N\mathfrak{R}} \neq \emptyset$. We may apply Lemma 3.2 and conclude that for each $\boldsymbol{x} \in B \setminus \bigcup_{\mathfrak{R}\in\mathfrak{M}} U_{N\mathfrak{R}}$

$$\sum_{\sigma\in\mathfrak{S}_N} z_\sigma(\boldsymbol{y}_1, \dots, \boldsymbol{y}_{N-1}, \boldsymbol{x}) = 0 \tag{4.4}$$

but no proper nonempty subsum of the left hand side of (4.4) vanishes. However, by definition of B, the summands $z_\sigma(\boldsymbol{y}_1, \dots, \boldsymbol{y}_{N-1}, \boldsymbol{x})$ in (4.4) are roots of unity. So (4.4) is an equation of the type considered in (2.1), and in fact we have nondegenerate solutions $(z_\sigma(\boldsymbol{y}_1, \dots, \boldsymbol{y}_{N-1}, \boldsymbol{x}))_{\sigma\in\mathfrak{S}_N}$. We may apply Lemma 2.2 with $m = N!$ and with $b_1 = \dots = b_m = 1$. Now Lemma 2.2 says the following: For any solution $\boldsymbol{x} \in B \setminus \bigcup_{\mathfrak{R}\in\mathfrak{M}} U_{N\mathfrak{R}}$ the point $(z_\sigma(\boldsymbol{y}_1, \dots, \boldsymbol{y}_{N-1}, \boldsymbol{x}))_{\sigma\in\mathfrak{S}_N}$ is of the shape $(\zeta\eta_\sigma)_{\sigma\in\mathfrak{S}_N}$, where ζ is an arbitrary root of unity and where the η_σ are $q_1 \dots q_a$-th roots of unity with

$$\sum_{i=1}^{a} (q_i - 2) \leq N! - 2.$$

We may assume without loss of generality that $2 \in \{q_1, \dots, q_a\}$. Otherwise we enlarge the set by taking $\{2, q_1, \dots, q_a\}$.

Recall that the components z_σ are the summands in the Laplace expansion of the determinant

$$\det(\boldsymbol{y}_1, \dots, \boldsymbol{y}_{N-1}, \boldsymbol{x}) = \begin{vmatrix} y_{11} & \dots & y_{1N} \\ y_{21} & \dots & y_{2N} \\ \dots & \dots & \dots \\ x_1 & \dots & x_N \end{vmatrix}.$$

We claim that for $i = 1, \dots, N$ we can find a root of unity ζ_i of order dividing $q_1 \dots q_a$ such that

$$x_i = \frac{x_1}{y_{11}} y_{1i} \zeta_i \tag{4.5}$$

holds true for $i = 1, \dots, N$.

To verify (4.5) consider in the expansion of the determinant the element we get along the main diagonal, i.e., $y_{11}y_{22} \dots y_{N-1,N-1}x_N$. Compare this element with the one where we replace the top left corner by the bottom left corner and the bottom right corner with the top right corner but otherwise we remain on the main diagonal, i.e., consider the element $x_1y_{22} \dots y_{N-1,N-1}y_{1N}$. Taking quotients we get

$$\frac{y_{11}x_N}{y_{1N}x_1} = \pm\eta_N,$$

where η_N is a root of unity of order dividing $q_1 \dots q_a$. By our assumption $2 \in \{q_1, \dots, q_a\}$ however, and therefore $-\eta_N$ is a root of unity of order dividing $q_1 \dots q_a$ as well. Thus (4.5) in the case $i = N$ is verified with $\zeta_N = \pm\eta_N$.

Interchanging columns in the determinant we get (4.5) in general. Therefore taking $\boldsymbol{u}_0 = \boldsymbol{y}_1$ we may infer that each point $\boldsymbol{x} \in B \setminus \bigcup_{\mathfrak{R}\in\mathfrak{M}} U_{N\mathfrak{R}}$ is of the shape

$$(x_1, \ldots, x_N) = (\zeta\zeta_i y_{1i}) = (\zeta\zeta_i u_{0i}) \quad \text{with } \zeta = x_1/y_{11}$$

and the lemma follows.

5. Proof of the Theorem. For $n = 1$ equation (1.1) has at most a single solution in E and the Theorem follows trivially.

Now suppose that $n > 1$ and that the assertion is proved for all $n' < n$. Put $n + 1 = N$ and write equation (1.1) in homogenized form as

$$a_1x_1 + \ldots + a_{N-1}x_{N-1} - x_N = 0, \tag{5.1}$$

to be solved in roots of unity x_i.

To prove assertion (1.2) of the Theorem it will suffice to show that there are points $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_t \in E^N$ with

$$t \le 2^{2N!}$$

such that any nondegenerate solution $\boldsymbol{x} = (x_1, \ldots, x_N)$ of (5.1) is contained in the union

$$\bigcup_{\tau=1}^{t} B(\boldsymbol{u}_\tau,\, p_1 \ldots p_s)$$

with $B(\boldsymbol{u}, l)$ as in (4.2). Then clearly the general solution $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_n)$ of (1.1) will be of the shape

$$\xi_i = \frac{x_i}{x_N} \quad (i = 1, \ldots, n).$$

Thus in the Theorem the sets $A(\boldsymbol{w}_\tau, p_1 \ldots p_s)$ $(\tau = 1, \ldots, t)$ will do, where $\boldsymbol{w}_\tau = (w_{\tau 1}, \ldots, w_{\tau n})$ is defined by

$$w_{\tau i} = \frac{u_{\tau i}}{u_{\tau N}} \quad (i = 1, \ldots, n).$$

We may apply Lemma 4.1 to (5.1). Thus, there exist proper linear subspaces $W_1, \ldots, W_{2^{N!}}$ of the $(N-1)$-dimensional space defined by (5.1) and there exists a tuple $\boldsymbol{u}_0 = (u_{01}, \ldots, u_{0N})$ of roots of unity such that any solution $\boldsymbol{x} = (x_1, \ldots, x_N)$ of (5.1) is contained in the union

$$B(\boldsymbol{u}_0, q_1 \ldots q_a) \cup W_1 \cup \ldots \cup W_{2^{N!}}.$$

Here

$$\sum_{i=1}^{a} (q_i - 2) \le N! - 2.$$

Consider a typical subspace, say W. It may be defined by an equation

$$b_1x_1 + \ldots + b_{N-1}x_{N-1} = 0, \tag{5.2}$$

where not all b_i are equal to zero.

Let I be a nonempty subset of $\{1, \ldots, N-1\}$ and let $C(I)$ be the subset of solutions of (5.2) satisfying

$$\sum_{i \in I} b_i x_i = 0, \tag{5.3}$$

but no proper subsum of the left hand side of (5.3) vanishes. We may apply the induction hypothesis to the solutions of (5.3) lying in $C(I)$.

Consequently, there exist $2^{2|I|!}$ points $\boldsymbol{v}_j$ in $|I|$-dimensional space, and with roots of unity as components, such that any nondegenerate solution of (5.3) is contained in the union

$$\bigcup B(\boldsymbol{v}_j, r_1 \ldots r_b).$$

Here $r_1, \ldots, r_b$ are suitable primes satisfying $r_1 < \ldots < r_b \leq |I|!$.

Let $\boldsymbol{v} = (v_i)_{i \in I}$ be a typical point among the $\boldsymbol{v}_j$. Then the elements in $B(\boldsymbol{v}, r_1 \ldots r_b)$ may be written as $(x_i)_{i \in I}$ with components

$$x_i = x\eta_i v_i \quad (i \in I), \tag{5.4}$$

where x is an arbitrary root of unity and η_i is a root of unity whose order divides $r_1 \ldots r_b$. We may substitute (5.4) into (5.1) and obtain, writing $a_N = -1$,

$$\Big(\sum_{i \in I} a_i \eta_i v_i\Big) x + \sum_{i \notin I} a_i x_i = 0. \tag{5.5}$$

This is an equation in the $N - |I| + 1$ variables x_i with $i \notin I$ and x. As in (5.3) we clearly have $|I| \geq 2$, we may apply the inductive hypothesis again. By the hypothesis of our Theorem, on the left hand side of (5.5) no proper subsum vanishes. Thus by induction we get $2^{2(N-|I|+1)!}$ points $\boldsymbol{y}_j \in E^{N-|I|+1}$ and primes $s_1 < \ldots < s_c \leq (N - |I| + 1)!$ such that the solutions x, x_i $(i \notin I)$ of (5.5) are contained in the union of the sets $B(\boldsymbol{y}_j, s_1 \ldots s_c)$. We now combine the results we have derived for (5.3) and (5.5).

Given a point $\boldsymbol{v}$ corresponding to (5.3) and a point $\boldsymbol{y}$ corresponding to (5.5) we construct a point $\boldsymbol{u} \in E^N$ as follows: Suppose $\boldsymbol{y}$ has the components y, y_i $(i \notin I)$. Then we put

$$u_i = \begin{cases} v_i y & \text{for } i \in I, \\ y_i & \text{for } i \notin I. \end{cases}$$

So $\boldsymbol{u} = (u_1, \ldots, u_N)$ has components which are roots of unity.

Recall that the subspace W with the set I produces $2^{2|I|!}$ points $\boldsymbol{v}$ and $2^{2(N-|I|+1)!}$ points $\boldsymbol{y}$. So the pair W, I gives rise to no more than

$$2^{2(|I|!+(N-|I|+1)!)} \quad \text{points } \boldsymbol{u}. \tag{5.6}$$

A closer look at (5.3) and (5.5) shows that for $|I| = 2$ in (5.3) a single point $\boldsymbol{v}$ and for $|I| = N-1$ in (5.5) a single point $\boldsymbol{y}$ will suffice. In both cases we obtain only $2^{2(N-1)!}$ points $\boldsymbol{u}$. Estimating the total number of points $\boldsymbol{u}$ corresponding to a single subspace W we finally obtain the bound

$$\left(\binom{N}{2} + \binom{N}{N-1}\right)2^{2(N-1)!} + \sum_{|I|=3}^{N-2}\binom{N}{|I|}2^{2(|I|!+(N-|I|+1)!)} \leq 2^{2(N-1)!}(2^N - N).$$

Consequently, each subspace W gives rise to not more than $2^{N!}-1$ points $\boldsymbol{u}$.

Allowing a factor $2^{N!}$ from Lemma 4.1 for the number of subspaces W, we finally see that altogether $2^{2N!}$ points $\boldsymbol{u}$ will suffice for the set of subspaces W. This bound also easily takes care of the extra point $\boldsymbol{u}_0$ arising from the assertion of Lemma 4.1.

We still have to discuss how the primes $r_1, \ldots, r_b$ and $s_1, \ldots, s_c$ from (5.3) and (5.5) and the primes $q_1, \ldots, q_a$ corresponding to $\boldsymbol{u}_0$ fit together. However, we had

$$\begin{aligned} &q_1 < \ldots < q_a, \quad \sum_{i=1}^{a}(q_i - 2) \leq N! - 2, \\ &r_1 < \ldots < r_b \leq |I|!, \\ &s_1 < \ldots < s_c \leq (N - |I| + 1)!. \end{aligned}$$

Therefore, we have only primes not exceeding $N!$. Thus in the assertion of the Theorem it suffices to take the set $\{p_1, \ldots, p_s\}$ as the union of the sets $\{r_1, \ldots, r_b\}$, $\{s_1, \ldots, s_c\}$, the union being taken over all points $\boldsymbol{v}$ and $\boldsymbol{y}$ in our construction together with the primes $\{q_1, \ldots, q_a\}$ coming from the extra point $\boldsymbol{u}_0$ in Lemma 4.1. Assertion (1.2) follows with $N = n + 1$.

As for assertion (1.3), we remark that by Theorem 9 of J. B. Rosser and L. Schoenfeld [3] we have for $x > 0$

$$\sum_{p \leq x} \log p \leq 1.02x. \tag{5.7}$$

In the above considerations leading to the proof of (1.2), it is clear that points $\boldsymbol{w}_\tau$ coming from a subspace W_τ involve only primes $\leq (N-1)!$. In view of (5.7) there will be not more than $\exp(1.02(N-1)!)$ possibilities for each component ξ_i of a solution $\boldsymbol{\xi}$ in the corresponding set $A(\boldsymbol{w}_\tau, p_1 \ldots p_s)$. Hence $A(\boldsymbol{w}_\tau, p_1 \ldots p_s)$ in that case contains not more than $2^{2(n+1)!}$ solutions $\boldsymbol{\xi}$.

There remains the exceptional point $\boldsymbol{u}_0$ in Lemma 4.1. The corresponding set $B(\boldsymbol{u}_0, q_1 \dots q_a)$ in view of Lemmata 2.1 and 2.2 has

$$q_1 < \dots < q_a, \qquad \sum_{i=1}^{a} (q_i - 2) \le N! - 2.$$

Estimating roughly, again we see that there are not more than $2^{2(n+1)!}$ solutions $\boldsymbol{\xi}$ in the set $A(\boldsymbol{w}_0, q_1 \dots q_a)$ derived from $B(\boldsymbol{u}_0, q_1 \dots q_a)$. Allowing the factor $2^{2(n+1)!}$ for the number of sets $A(\boldsymbol{w}_\tau, p_1 \dots p_s)$ we finally get (1.3).

References

[1] J. H. Conway and A. J. Jones, *Trigonometric diophantine equations* (*On vanishing sums of roots of unity*), Acta Arith. 30 (1976), 229–240.

[2] H. B. Mann, *On linears relations between roots of unity*, Mathematika 12 (1965), 107–117.

[3] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.

[4] A. Schinzel, *Reducibility of lacunary polynomials*, *VIII*, Acta Arith. 50 (1988), 91–106.

[5] H. P. Schlickewei, *Linear equations over groups of finite rank*, to appear.

[6] H. P. Schlickewei and W. M. Schmidt, *On polynomial-exponential equations*, Math. Ann. 296 (1993), 339–361.

[7] U. Zannier, *On the linear independence of roots of unity over finite extensions of* $\mathbb{Q}$, Acta Arith. 52 (1989), 171–182.

Abteilung Mathematik II
Universität Ulm
Helmholzstr. 18
D-89069 Ulm, Germany
E-mail: hps@mathematik.uni-ulm.de

Received on 17.5.1994 (2615)