ON A PROBLEM RELATED TO ONE OF LITTLEWOOD AND OFFORD

R. C. VAUGHAN AND T. D. WOOLEY

1. Introduction

Let $z_1, z_2, \dots, z_n$ be complex numbers of modulus at least one. Denote by $N(\mathbf{z}) = N(z_1, \dots, z_n)$ the number of sums of the form

$$\sum_{i=1}^{n} \varepsilon_i z_i,$$

with $\varepsilon_i = 1$ or -1, lying in the interior of a given disc of unit radius.

From their investigations on "random polynomials", Littlewood and Offord were led to consider bounds for $N(\mathbf{z})$, and gave one adequate for their purposes (see Littlewood and Offord [7, Theorem 1]). Erdős [2] applied a Sperner's Theorem argument (see Bollobás [1, §§3,4]) to deduce that when the z_i are all real, we have

$$N(\mathbf{z}) \leqslant \binom{n}{\lfloor n/2 \rfloor},$$

with equality holding when $z_1 = \dots = z_n = 1$. Later, Kleitman [5, 6] and Katona [4] extended this result to the complex field, and even to an analogous result on vectors in an arbitrary archimedean normed space. More recently, Griggs [3] has elaborated on these results and arguments.

It would appear that all results thus far have been on archimedean spaces of some sort, and indeed this would appear to be essential for the Sperner's Theorem argument to succeed. We now give a result for a non-archimedean example:

Theorem 1. *Let $\alpha_1, \dots \alpha_n$ be reduced residues* (mod q)*, and let $N(q; \boldsymbol{\alpha})$ denote the number of choices of $\varepsilon_1, \dots, \varepsilon_n$, with $\varepsilon_i = 0$ or 1, such that*

$$\sum_{i=1}^{n} \varepsilon_i \alpha_i \equiv 0 \pmod{q}.$$

If $q > (n+1)/2$, then

$$N(q; \boldsymbol{\alpha}) \leqslant \binom{n}{\lfloor n/2 \rfloor},$$

where $\lfloor x \rfloor$ denotes the integer part of x. Further, putting

$$\gamma_i^{(n)} = \begin{cases} 1, & \text{for } 1 \leqslant i \leqslant \lfloor n/2 \rfloor, \\ -1, & \text{for } \lfloor n/2 \rfloor < i \leqslant n, \end{cases}$$

we have $N(q; \boldsymbol{\gamma}^{(n)}) = \binom{n}{\lfloor n/2 \rfloor}$.

Corollary 1.1. *Let $\alpha_1, \dots, \alpha_n \in \mathbb{Q}_p$ satisfy $|\alpha_i|_p = 1$ (with the p-adic valuation normalised with $|p|_p = p^{-1}$). Denote by*

$$N^{(r)}(p; \boldsymbol{\alpha}) = N^{(r)}(p; \alpha_1, \dots, \alpha_n)$$

the number of choices of $\varepsilon_1, \dots, \varepsilon_n$ with $\varepsilon_i = 0$ or 1, such that

$$\left| \sum_{i=1}^{n} \varepsilon_i \alpha_i \right|_p \leqslant p^{-r}.$$

If $p^r > (n+1)/2$, then

$$N^{(r)}(p; \boldsymbol{\alpha}) \leqslant \binom{n}{\lfloor n/2 \rfloor}.$$

The corollary is immediate from the theorem on considering congruences (mod p^r). Results less precise than the theorem have recently been used in investigations on the local solubility of simultaneous additive equations (see, for example, [8, Lemma 3.4]).

Our proof is divided into many cases. When n is even, the use of exponential sums makes the result almost immediate. However, life is rather harder when n is odd, and we must take care to exploit all available asymmetries present in the residue system, these tending to deflate $N(q; \boldsymbol{\alpha})$.

The second author wishes to thank the Science and Engineering Research Council for a research grant.

2. Proof of the theorem

Let

$$S(\beta) = 1 + e(\beta/q).$$

Then, by considering the underlying exponential sums, we have

$$N(q; \boldsymbol{\alpha}) = q^{-1} \sum_{r=1}^{q} \prod_{i=1}^{n} S(r\alpha_i). \tag{2.1}$$

We divide into cases.

(**A**) Suppose that n is even. Applying Hölder's inequality to (2.1), we have

$$N(q; \boldsymbol{\alpha}) \leqslant \prod_{i=1}^{n} \left(q^{-1} \sum_{r=1}^{q} |S(r\alpha_i)|^n \right)^{1/n} = \prod_{i=1}^{n} \left(q^{-1} \sum_{r=1}^{q} |S(r)|^n \right)^{1/n}$$

by a change of variable. Thus, since n is even and $q > (n+1)/2$, we have

$$N(q; \boldsymbol{\alpha}) \leqslant N(q; \boldsymbol{\gamma}^{(n)}) = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{\lfloor n/2 \rfloor}{j}^2 = \binom{n}{\lfloor n/2 \rfloor},$$

and the result holds in case (A).

(**B**) Suppose that n is odd. We write $n = 2k+1$ with k a positive integer (the case $n = 1$ is trivial). We divide into cases according to the value of $\eta = \alpha_1 + \ldots + \alpha_n$.

(**i**) Suppose that $(\eta, q) = 1$. For λ a given reduced residue (mod q), let $N_\lambda(q; \boldsymbol{\alpha})$ denote the number of choices of $\varepsilon_1, \dots, \varepsilon_n$ with $\varepsilon_i = 0$ or 1, such that

$$\sum_{i=1}^{n} \varepsilon_i \alpha_i \equiv \lambda \pmod{q}. \tag{2.2}$$

Then $N_\eta(q; \boldsymbol{\alpha}) = N(q; \boldsymbol{\alpha})$, since whenever (2.2) holds with $\lambda = \eta$, we have

$$\sum_{i=1}^{n} (1 - \varepsilon_i)\alpha_i \equiv 0 \pmod{q}.$$

Then we have

$$N(q; \alpha_1, \dots, \alpha_n, -\eta) = N(q; \boldsymbol{\alpha}) + N_\eta(q; \boldsymbol{\alpha}) = 2 \cdot N(q; \boldsymbol{\alpha}). \tag{2.3}$$

But by part (A), we have

$$N(q; \alpha_1, \dots, \alpha_n, -\eta) \leqslant \binom{2k+2}{k+1} = 2\binom{2k+1}{k},$$

and the result follows in case (B)(i).

(**ii**) Suppose that (η, q) is a proper divisor of q. Let $d = (\eta, q)$. By applying Hölder's inequality to (2.1), we have

$$\begin{aligned} N(q; \alpha_1, \dots, \alpha_n, -\eta) \leqslant \prod_{i=1}^{k} \left(q^{-1} \sum_{r=1}^{q} |S(r\alpha_i)|^{2k} \cdot |S(r\eta)|^2 \right)^{1/(2k)} \\ \times \prod_{i=k+1}^{n} \left(q^{-1} \sum_{r=1}^{q} |S(r\alpha_i)|^{2k+2} \right)^{1/(2k+2)} \end{aligned}$$

We now observe that

$$q^{-1} \sum_{r=1}^{q} |S(r\alpha_i)|^{2k+2} = N(q; \boldsymbol{\gamma}^{(n+1)}) = \binom{2k+2}{k+1} = 2\binom{2k+1}{k},$$

and, by a change of variable,

$$q^{-1} \sum_{r=1}^{q} |S(r\alpha_i)|^{2k} \cdot |S(r\eta)|^2 = N(q; \boldsymbol{\gamma}^{(n-1)}, \xi, -\xi),$$

for some ξ with $(\xi, q) = d$.

We establish now a lemma which is useful both here and later.

Lemma 2.1. *Suppose that $k \geqslant 1$, $q \geqslant k+2$ and $\alpha \not\equiv \pm 1, 0 \pmod{q}$. Then*

$$N(q; \boldsymbol{\gamma}^{(2k)}, \alpha, -\alpha) < \frac{2k+3}{4k+8} \binom{2k+3}{k+1} \quad \textit{for} \quad k \neq 2,$$

and

$$N(q; \boldsymbol{\gamma}^{(4)}, \alpha, -\alpha) \leqslant 16.$$

Proof. We have

$$N(q;\boldsymbol{\gamma}^{(2k)},\alpha,-\alpha)=N_0(q;\boldsymbol{\gamma}^{(2k)})+N_{\alpha-\alpha}(q;\boldsymbol{\gamma}^{(2k)})+N_{\alpha}(q;\boldsymbol{\gamma}^{(2k)})+N_{-\alpha}(q;\boldsymbol{\gamma}^{(2k)}).$$

Since $\alpha\not\equiv\pm1,0\pmod q$ we have

$$N(q;\boldsymbol{\gamma}^{(2)},\alpha,-\alpha)=2N_0(q;\boldsymbol{\gamma}^{(2)})=4<\frac{25}{6}=\frac{5}{12}\binom{5}{2},$$

and

$$N(q;\boldsymbol{\gamma}^{(4)},\alpha,-\alpha)\leqslant 2N_0(q;\boldsymbol{\gamma}^{(4)})+4=16.$$

Thus we may suppose that $k\geqslant 3$. Choose u and t so that $0\leqslant u<q$, $0\leqslant t<q$, $\alpha+u\equiv 0\pmod q$, $-\alpha+t\equiv 0\pmod q$. Then, as $\alpha\not\equiv\pm1,0\pmod q$ we have $u\geqslant 2$, $t\geqslant 2$.

When $u\leqslant k$ the congruence

$$\sum_{i=1}^{2k}\varepsilon_i\gamma_i^{(2k)}\equiv\alpha\pmod q$$

has

$$\sum_{r=0}^{k-u}\binom{k}{r}\binom{k}{r+u}=\binom{2k}{k-u}$$

solutions of the type $r\cdot 1+(r+u)(-1)\equiv\alpha\pmod q$, when $t\leqslant k$ it has $\binom{2k}{k-t}$ of the type $(r+t)\cdot 1+r(-1)\equiv\alpha\pmod q$, and it has no other solutions since $q\geqslant k+2$. There is a concomitant conclusion when α is replaced by $-\alpha$. Thus, on using part (A) to estimate $2N_0(q;\boldsymbol{\gamma}^{(2k)})$, we deduce that

$$N(q;\boldsymbol{\gamma}^{(2k)},\alpha,-\alpha)\leqslant 2\binom{2k}{k}+2\binom{2k}{k-u}+2\binom{2k}{k-t}.$$

Since $u\equiv-\alpha\equiv-t\pmod q$, we have $u+t=q$, and without loss of generality we may suppose now that $t\geqslant u$, whence $t\geqslant\frac12 q\geqslant\frac12 k+1$. Thus we may now assume that

$$N(q;\boldsymbol{\gamma}^{(2k)},\alpha,-\alpha)\leqslant 2\binom{2k}{k}+2\binom{2k}{k-2}+2\binom{2k}{k-t}$$

holds with $k\geqslant 3$ and $t\geqslant\frac12 k+1$. Hence

$$N(q;\boldsymbol{\gamma}^{(2k)},\alpha,-\alpha)\leqslant\frac{2k+3}{4k+8}\binom{2k+3}{k+1}\lambda$$

where λ is given by

$$(\lambda-1)\frac{(2k+1)(2k+3)^2}{2k+4}=1-2k+\frac{3}{2k+4}+2k(k-1)\prod_{m=3}^{t}\frac{k+1-m}{k+m}.$$

When $k=3,5,6$ the right hand side does not exceed $-\frac{27}{10}$, $-9+\frac{3}{14}+\frac{10}{3}$, $-11+\frac{3}{16}+8$ respectively, so $\lambda<1$. When $k=4$ and $t\geqslant 4$ it does not exceed $-7+\frac14+\frac67$, so again

$\lambda < 1$. When $k = 4$ and $t = 3$, we have $3 \geqslant q/2 \geqslant 3$, so $q = 6$, $u = 3$. Thus

$$N(q; \boldsymbol{\gamma}^{(8)}, \alpha, -\alpha) \leqslant 2\binom{8}{4} + 4\binom{8}{1} = 172 < \frac{11}{24}\binom{11}{5}.$$

Therefore we may suppose that $k \geqslant 7$. Now the product on the right hand side is

$$\exp\left(\sum_{m=3}^{t} \log\left(\frac{1 - \frac{2m-1}{2k+1}}{1 + \frac{2m-1}{2k+1}}\right)\right) < \exp\Big(-\sum_{m=3}^{t} \frac{4m-2}{2k+1}\Big)$$

and when $k \geqslant 7$ we have

$$\sum_{m=3}^{t} \frac{4m-2}{2k+1} = \frac{2t^2-8}{2k+1} \geqslant \frac{(k+2)^2-16}{4k+2} = \frac{k}{4} + \frac{7}{8} - \frac{55}{16k+8} > \frac{k+1}{4}$$

and $\exp((k+1)/4) > k$. The last inequality may be established by observing that $f(x) = \exp((x+1)/4) - x$ is strictly increasing for $x \geqslant 8\log 2 - 1$, and that $7 > 8\log 2 - 1$ and $e^2 > 7$, and so $f(k) \geqslant f(7) > 0$.

It now follows that

$$(\lambda - 1)\frac{(2k+1)(2k+3)^2}{2k+4} < 2 - 2k + 2(k-1) = 0,$$

whence $\lambda < 1$ once more.

This completes the proof of the lemma. □

Returning to the proof of the theorem, by the lemma,

$$\begin{aligned} 2N(q; \boldsymbol{\alpha}) = N(q; \alpha_1, \ldots, \alpha_n, -\eta) &< \left(\frac{1}{2}\left(\frac{2k+3}{k+2}\right)^2 \binom{2k+1}{k}\right)^{\frac{1}{2}} \left(2\binom{2k+1}{k}\right)^{\frac{1}{2}} \\ &< 2\binom{2k+1}{k}. \end{aligned}$$

Thus the result follows in the case (B)(ii).

(**iii**) Suppose that $q|\eta$. Then we have

$$\alpha_n \equiv -(\alpha_1 + \ldots + \alpha_{n-1}) \pmod{q},$$

and hence

$$\begin{aligned} N(q; \alpha_1, \ldots, \alpha_n) &= N(q; \alpha_1, \ldots, \alpha_{n-1}, -(\alpha_1 + \ldots + \alpha_{n-1})) \\ &= 2 \cdot N(q; \alpha_1, \ldots, \alpha_{n-1}). \end{aligned} \tag{2.4}$$

We now divide into further cases.

(**a**) Suppose that there is a β with $\alpha_i \equiv \pm\beta$ for $i = 1, \ldots, n$. Suppose that there are m values of i with $\alpha_i \equiv \beta$, and $n - m$ values of i with $\alpha_i \equiv -\beta$. Thus

$$m\beta - (n-m)\beta \equiv 0 \pmod{q}.$$

Without loss of generality we may assume that $n - m \geqslant m$. Then since $(\beta, q) = 1$ and $q > (n+1)/2$, we have either $n = 2m$ or $n = 2m + q$. The first case cannot occur, since we have supposed n to be odd. Then we must have $1 \leqslant m = (n-q)/2 < k/2$.

We therefore have

$$\begin{aligned} N(q;\boldsymbol{\alpha}) &= \sum_{r=0}^{m}\binom{n-m}{r}\binom{m}{r} + \sum_{r=0}^{m}\binom{n-m}{q+r}\binom{m}{r} \\ &= \binom{n}{m} + \binom{n}{q+m} \\ &= \binom{2k+1}{k} 2\prod_{i=1}^{k-m}\frac{m+i}{k+1+i}. \end{aligned}$$

Then on noting that $2(m+1) < k+2$, we deduce that

$$N(q;\boldsymbol{\alpha}) \leqslant \binom{2k+1}{k},$$

and the result follows once again.

(**b**) Suppose that there is no β such that for $i = 1,\dots,n$ we have $\alpha_i \equiv \pm\beta$. By a rearrangement of variables we may suppose that there is no β such that for $i = 1,\dots,n-1$ we have $\alpha_i \equiv \pm\beta$. The case $k = 1$ is trivial. Suppose then that $k > 1$, and let $S_\zeta \subseteq \{1,\dots,n-1\}$ denote the set of indices for which $\alpha_i \equiv \pm\zeta \pmod q$. There are three cases:

($\boldsymbol{\alpha}$) We may choose ζ with $1 < \operatorname{card}(S_\zeta) \leqslant 2k-2$. Choose ζ so that $s = \operatorname{card}(S_\zeta)$ is minimal amongst those ζ satisfying $1 < \operatorname{card}(S_\zeta) \leqslant 2k-2$. Then we may rearrange variables so that $S_\zeta = \{2k-s+1,\dots,2k\}$, and by Hölder's inequality, for $k > 2$ we have

$$\begin{aligned} N(q;\alpha_1,\dots,\alpha_{n-1}) \leqslant \prod_{i=1}^{2k-s}\Bigg(&\bigg(q^{-1}\sum_{r=1}^{q}|S(r\alpha_i)|^{2k-2}\cdot|S(r\zeta)|^2\bigg)^{\frac{2k-2-s}{(2k-4)(2k-s)}} \\ &\times\bigg(q^{-1}\sum_{r=1}^{q}|S(r\alpha_i)|^2\cdot|S(r\zeta)|^{2k-2}\bigg)^{\frac{s-2}{(2k-4)(2k-s)}}\Bigg). \end{aligned}$$

For $k = 2$ (and $s = 2$), by Cauchy's inequality we have

$$N(q;\alpha_1,\dots,\alpha_{n-1}) \leqslant \prod_{i=1}^{2}\bigg(q^{-1}\sum_{r=1}^{q}|S(r\alpha_i)|^2\cdot|S(r\zeta)|^2\bigg)^{\frac12}.$$

($\boldsymbol{\beta}$) For every ζ, $\operatorname{card}(S_\zeta) \leqslant 1$. Then we have

$$\begin{aligned} N(q;\alpha_1,\dots,\alpha_{n-1}) \leqslant \prod_{i=1}^{k}\Bigg(&\bigg(q^{-1}\sum_{r=1}^{q}|S(r\alpha_{2i-1})|^{2k-2}\cdot|S(r\alpha_{2i})|^2\bigg)^{\frac{1}{2k}} \\ &\times\bigg(q^{-1}\sum_{r=1}^{q}|S(r\alpha_{2i-1})|^2\cdot|S(r\alpha_{2i})|^{2k-2}\bigg)^{\frac{1}{2k}}\Bigg). \end{aligned}$$

($\boldsymbol{\gamma}$) There are reduced residues ζ and ξ with $\operatorname{card}(S_\zeta) = 1$ and $\operatorname{card}(S_\xi) = 2k-1$. We may rearrange variables so that $S_\zeta = \{2k\}$. Then by Hölder's inequality, we have

$$N(q;\alpha_1,\dots,\alpha_{n-1}) \leqslant \bigg(q^{-1}\sum_{r=1}^{q}|S(r\xi)|^{2k-2}|S(r\zeta)|^2\bigg)^{\frac12}\bigg(q^{-1}\sum_{r=1}^{q}|S(r\xi)|^{2k}\bigg)^{\frac12}.$$

We now observe that given α and β with $(\alpha\beta, q) = 1$ and $\alpha \not\equiv \pm\beta \pmod q$ there is a β' with $\beta' \not\equiv \pm 1, 0 \pmod q$ such that

$$q^{-1}\sum_{r=1}^{q} |S(r\alpha)|^{2k-2} \cdot |S(r\beta)|^2 = N(q; \boldsymbol{\gamma}^{(2k-2)}, \beta', -\beta').$$

The premiss of the lemma is satisfied with k replaced by $k-1$, since $k \geqslant 2$. Thus the above does not exceed $\dfrac{2k+1}{4k+4}\binom{2k+1}{k}$ when $k \neq 3$ and 16 when $k = 3$. Hence in cases (α) and (β) we have

$$2N(q; \alpha_1, \dots, \alpha_{n-1}) \leqslant \binom{2k+1}{k}$$

and the result follows from (2.4).

In the case (γ), when $k \neq 3$ we obtain, via part (A),

$$2N(q; \alpha_1, \dots, \alpha_{n-1}) \leqslant 2\left(\frac{2k+1}{4k+4}\binom{2k+1}{k}\binom{2k}{k}\right)^{\frac{1}{2}} = \binom{2k+1}{k}$$

and again the result follows from (2.4).

When $k = 3$ we obtain, in the same way,

$$N(q; \alpha_1, \dots, \alpha_{n-1}) \leqslant \left(16\binom{6}{3}\right)^{\frac{1}{2}} = (320)^{\frac{1}{2}} < 18.$$

Thus, by (2.4),

$$N(q; \boldsymbol{\alpha}) \leqslant 34 < 35 = \binom{7}{3}.$$

This completes the proof of the theorem.

References

[1] B. Bollobás, *Combinatorics*, Cambridge University Press, 1986.

[2] P. Erdős, *On a lemma of Littlewood and Offord*, Bull. Amer. Math. Soc. **51** (1945), 898–902.

[3] J. R. Griggs, *The Littlewood-Offord problem: tightest packing and an M-part Sperner theorem*, Europ. Jl. Combin. **1** (1980), 225–234.

[4] G. O. H. Katona, *On a conjecture of Erdős and a stronger form of Sperner's theorem*, Studia Sci. Math. Hungar. **1** (1966), 59–63.

[5] D. J. Kleitman, *On a lemma of Littlewood and Offord on the distribution of certain sums*, Math. Z. **90** (1965), 251–259.

[6] D. J. Kleitman, *On a lemma of Littlewood and Offord on the distributions of linear combinations of vectors*, Adv. Math. **5** (1970), 155–157.

[7] J. E. Littlewood and A. C. Offord, *On the number of real roots of a random algebraic equation, III*, Mat. Sbornik **12** (1943), 277–286.

[8] T. D. Wooley, *On simultaneous additive equations, III*, Mathematika **37** (1990), 85–96.

Imperial College of Science and Technology, Department of Mathematics, Huxley Building, 180 Queen's Gate, London SW7 2BZ