BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 28, Number 2, April 1993

ON THE DISTRIBUTION OF SUMS OF RESIDUES

JERROLD R. GRIGGS

ABSTRACT. We generalize and solve the mod q analogue of a problem of Littlewood and Offord, raised by Vaughan and Wooley, concerning the distribution of the 2^n sums of the form $\sum_{i=1}^n \varepsilon_i a_i$, where each ε_i is 0 or 1. For all q, n, k we determine the maximum, over all reduced residues a_i and all sets P consisting of k arbitrary residues, of the number of these sums that belong to P.

1. INTRODUCTION

Vaughan and Wooley [15] raised the problem of determining the maximum number of the 2^n sums of the form $\sum_{i=1}^n \varepsilon_i a_i$, where each ε_i is 0 or 1, that are congruent to 0 mod q. The maximum is over all residues $a_1, \ldots, a_n$ that are *reduced*, which means that $(a_i, q) = 1$ for all i. Results about this problem have been applied to study the solutions of simultaneous additive equations.

By using analytical tools, including exponential sums and classical inequalities, and by treating many cases, Vaughan and Wooley show that the maximum is $\binom{n}{\lfloor n/2 \rfloor}$ provided that $q > \lceil n/2 \rceil$. This bound is sharp, since it is attained by letting a_i be 1 for $i \leq \lceil n/2 \rceil$ and -1 for $i > \lceil n/2 \rceil$. (To see this, observe that for this choice of a_i's, we have $\sum_{i=1}^n \varepsilon_i a_i \equiv 0$ precisely when an equal number of ε_i's are 1 for $i \leq \lceil n/2 \rceil$ and -1 for $i > \lceil n/2 \rceil$. This happens if and only if the number of indices i with $i \leq \lceil n/2 \rceil$ and $\varepsilon_i = 1$ plus the number with $i > \lceil n/2 \rceil$ and $\varepsilon_i = 0$ is $\lfloor n/2 \rfloor$, so that the choices correspond to the subsets of $\{1, \ldots, n\}$ of size $\lfloor n/2 \rfloor$.)

When $\lceil n/2 \rceil \geq q$, wraparound effects mod q come into play. For example, with the a_i's chosen as above, the sum $\sum_{i=1}^q a_i$ is also congruent to 0, so the answer exceeds $\binom{n}{\lfloor n/2 \rfloor}$.

We solve the problem for arbitrary n and q, using an inductive argument that is inspired by the study of the extremal properties of the Boolean lattice B_n on the collection $2^{[n]}$ of all subsets of the n-set $[n] = \{1, \ldots, n\}$, ordered by inclusion. Let us adopt the notation

$$\binom{n}{s}_q := |\{A \subseteq [n]: |A| \equiv s\}| = \sum_{j \equiv s} \binom{j}{s},$$

for the mod q binomial coefficients in n. We shall see that for general n and q, the maximum number of sums congruent to 0 is the middle mod q binomial coefficient $\binom{n}{\lfloor n/2 \rfloor}_q$. The maximum is attained as before by dividing

Received by the editors September 2, 1992.
1991 *Mathematics Subject Classification.* Primary 11P83; Secondary 11A07, 05A05, 06A07.
Research supported in part by NSA/MSP Grant MDA90-H-4028 and by a Visiting Professorship at Simon Fraser University.

0273-0979/93 $1.00 + $.25 per page

the a_i's as evenly as possible between 1 and -1. In general, the maximum number of sums congruent to any single residue is $\binom{n}{\lfloor n/2 \rfloor}_q$. Throughout the paper we maintain the condition that the residues a_i be reduced. Without this restriction, one would select a_i's with common factors, in order to increase the number of sums congruent to 0.

This problem we are considering is the analogue for residues of a famous problem about the clustering of partial sums of a collection of complex numbers. In connection with their study of roots of random polynomials, Littlewood and Offord [13] were led to consider the following question. For $a_1, \ldots, a_n \in \mathbf{C}$ with $\|a_i\| \geq 1$ for all i and for an open ball $S \subset \mathbf{C}$ of unit diameter, how many of the 2^n sums of the form $\sum_{i=1}^n \varepsilon_i a_i$, where each ε_i is 0 or 1, can belong to S? They sought the maximum over all choices of a_i's and S. In particular, if one selects a_i to be 1 for all i and centers S at $\lfloor n/2 \rfloor$, one can pack $\binom{n}{\lfloor n/2 \rfloor}$ sums into S, and this was believed to be optimal. While Erdös [3] soon proved this for the real a_i case, it was twenty years before the original complex case was solved, by Katona [8] and Kleitman [10] independently, from an appropriate extension of the theorem of Sperner [14] about the maximum size of an antichain in the Boolean lattice.

Although the usual Sperner method does not extend to higher dimensions, Kleitman [11, also in 5] found a remarkable proof that the answer is still $\binom{n}{\lfloor n/2 \rfloor}$ in any dimension m (or indeed, in Hilbert space): For any vectors $a_1, \ldots, a_n \in \mathbf{R}^m$ of length at least one, there is a partition of $2^{[n]}$ into just $\binom{n}{\lfloor n/2 \rfloor}$ blocks, such that for any sets I, J in the same block, the sums $\sum_{i \in I} a_i$ and $\sum_{j \in J} a_j$ are far apart (distance at least one). Hence any open ball S of unit diameter contains at most $\binom{n}{\lfloor n/2 \rfloor}$ sums. The idea behind this construction is that for every n, the sizes of the blocks partitioning $2^{[n]}$ exactly match the sizes of the chains in the famous inductive symmetric chain decomposition of B_n discovered by de Bruijn et al. [2].

Erdös [3] considered the more general problem of maximizing the number of sums of vectors inside an open ball in $\mathbf{R}^m$ of diameter $d \geq 1$. He solved this problem for the real case $(m = 1)$ using Sperner theory, and he found that the value attained when all $a_i = 1$ is optimal for all d. This value is the sum of the $\lceil d \rceil$ middle binomial coefficients, $\sum_{(n-\lceil d \rceil)/2 \leq j < (n+\lceil d \rceil)/2} \binom{n}{j}$. However, the problem is more complicated when $m \geq 2$ and completely solved only in some special cases. Using a variety of tools from extremal set theory, probability, and geometry, many authors have attacked this more general question, including Kleitman [12], Griggs [6], and Frankl and Füredi [4]. Also see the survey by Anderson [1].

In marked contrast to previous results of the Littlewood-Offord type, the setting for the work of Vaughan and Wooley is the additive group $\mathbf{Z}_q$ of integers mod q. Nonetheless, as with the unit diameter problem above, we shall see that their theorem can be obtained by an inductive partition construction inspired by a particular chain partition of the Boolean lattice. The method yields the solution to the extension of their problem to general n and q.

More generally, we determine the maximum number of the 2^n sums $\sum_{i=1}^n \varepsilon_i a_i$ congruent mod q to any of k arbitrary residues ρ_j, for $1 \leq j \leq k$,

over all choices of the residues ρ_j and the reduced residues a_i. The answer is the sum of the k middle mod q binomial coefficients in n. This bound is attained by selecting all a_i to be 1 and selecting the k middle values for the residues ρ_j. Switching some a_i in this solution to -1 has the effect of shifting the collection of all 2^n sums down by 1. Thus the bound is also attained by selecting a_i to be 1 for $i \le \lceil n/2 \rceil$ and -1 for $i > \lceil n/2 \rceil$ and by choosing the k initial values in the sequence $0, 1, -1, 2, -2, \ldots$ for the residues ρ_j.

2. The main result

We fix the integer $q > 0$ and work in $\mathbf{Z}_q$.

Theorem 1. *Let $a_1, \ldots, a_n$ be reduced residues in $\mathbf{Z}_q$. Let $P \subseteq \mathbf{Z}_q$, where $|P| = k$. Then the number of the 2^n sums $\sum_{i=1}^n \varepsilon_i a_i$ in P, where each ε_i is 0 or 1, is at most the sum of the k middle mod q binomial coefficients $\sum_{(n-k)/2 \le j < (n+k)/2} \binom{n}{j}_q$, and this bound is best possible.*

Proof. For $S \subseteq \mathbf{Z}_q$ and $a \in \mathbf{Z}_q$, let $S + a := \{s + a : s \in S\} \subseteq \mathbf{Z}_q$. For $\mathscr{A} \subseteq 2^{[n]}$, define the *sum set*

$$S(\mathscr{A}) = \left\{ \sum_{i \in I} a_i \pmod q : I \subset \mathscr{A} \right\}.$$

We say that $\mathscr{A} \subseteq 2^{[n]}$ is a *structure* for $a_1, \ldots, a_n$ provided that the sums in $S(\mathscr{A})$ are distinct.

We shall partition $2^{[n]}$ into $\binom{n}{\lfloor n/2 \rfloor}_q$ structures in such a way that the bound in the theorem will follow for all k. The construction is carried out by induction on n for a given sequence of reduced residues $a_1, a_2, \ldots$. It starts at $n = 0$ with the single structure $\{\varnothing\}$. For the induction step, suppose we are given a partition of $2^{[n-1]}$ into structures $\mathscr{A}_j$ for $a_1, \ldots, a_{n-1}$. Then the structures $\mathscr{A}_j$ and $\mathscr{A}_j' := \{I \cup \{n\} : I \in \mathscr{A}_j\}$ for $a_1, \ldots, a_n$ partition $2^{[n]}$, but they are not quite the ones we want. Notice that $S(\mathscr{A}_j') = S(\mathscr{A}_j) + a_n$. We require an easy fact.

Lemma. *Let $\varnothing \ne S \subseteq \mathbf{Z}_q$ and $a \in \mathbf{Z}_q$ with $(a, q) = 1$. Then $S + a = S$ if and only if $S = \mathbf{Z}_q$.*

If $S(\mathscr{A}_j)$ is $\mathbf{Z}_q$, then so is $S(\mathscr{A}_j')$, and we leave both structures alone. However, if $S(\mathscr{A}_j) \ne \mathbf{Z}_q$, then by the lemma there exists at least one element $t \in S(\mathscr{A}_j') \backslash S(\mathscr{A}_j)$, say $t = \sum_{i \in I} a_i$ where $I \in \mathscr{A}_j'$, so that we may replace $\mathscr{A}_j$ and $\mathscr{A}_j'$ by the structures $\mathscr{B}_j = \mathscr{A}_j \cup \{I\}$ and $\mathscr{B}_j' = \mathscr{A}_j' \backslash \{I\}$. We have $|\mathscr{B}_j| = |\mathscr{A}_j| + 1$ and $|\mathscr{B}_j'| = |\mathscr{A}_j| - 1$. In the case where $|\mathscr{A}_j| = 1$, we discard $\mathscr{B}_j'$.

Now denote the structures in this partition of $2^{[n]}$ by $\mathscr{A}_j$ for $j = 1, 2, \ldots$. Since sets in a structure have distinct sums, it follows that

$$\left| \left\{ I \subseteq [n] : \sum_{i \in I} a_i \in P \right\} \right| \le \sum_j \min(k, |\mathscr{A}_j|). \tag{1}$$

It suffices to show that the sum on the right-hand side of inequality (1) is at most the sum of the k middle mod q binomial coefficients in n.

Since the collection of structure sizes $|\mathscr{A}_j|$ depends in no way on the actual values of the a_i's, it is enough to consider the case where all $a_i = 1$. One can verify by induction on n that the sum set $S(\mathscr{A}_j)$ for each structure consists of all q residues or else consists of values congruent to an interval $x, x+1, \ldots, y \in \mathbf{Z}$ centered about $n/2$, which means $x + y = n$. The number of structures in the partition is $\binom{n}{\lfloor n/2 \rfloor}_q$, because every structure contains a set with sum (i.e., cardinality) $\equiv \lfloor n/2 \rfloor$. For general k, we see that the sum on the right-hand side of (1) is the number of subsets of cardinality congruent to any of the k middle values around $n/2$. □

When $q > \lceil n/2 \rceil$, we have that $\binom{n}{\lfloor n/2 \rfloor}_q = \binom{n}{\lfloor n/2 \rfloor}$, which implies the original result of Vaughan and Wooley [15]:

Corollary 1. *Let $a_1, \ldots, a_n$ be reduced residues in $\mathbf{Z}_q$, where $q > \lceil n/2 \rceil$. Then the number of the 2^n sums $\sum_{i=1}^n \varepsilon_i a_i$ congruent to 0, where each ε_i is 0 or 1, is at most $\binom{n}{\lfloor n/2 \rfloor}$, and this bound is best possible.*

3. Related remarks

The inspiration for the proof of the theorem is the inductive partition of the Boolean lattice B_n into saturated chains of size at most q, that is, into collections of at most q totally ordered subsets of consecutive sizes. Katona [9] used this construction to determine the maximum number of subsets of $\{1, \ldots, n\}$ containing no sets $A \subset B$ with $0 < |B \backslash A| < q$. The author [7] later independently devised the same construction to obtain a maximum-sized collection of disjoint saturated chains of size q in B_n. The collection of structure sizes $|\mathscr{A}_j|$ in our construction exactly corresponds to the collection of chain sizes in Katona's partition.

By applying the theorem with $k = q - 1$, it is also possible to determine the minimum number of sums in any residue class.

Corollary 2. *Let $a_1, \ldots, a_n$ be reduced residues in $\mathbf{Z}_q$, where $n \geq q - 1$. Let $\rho \in \mathbf{Z}_q$. Then the number of the 2^n sums $\sum_{i=1}^n \varepsilon_i a_i$ congruent to ρ, where each ε_i is 0 or 1, is at least $\binom{n}{\lceil (n-q)/2 \rceil}_q$, and this bound is best possible.*

The bound in Corollary 2 is attained by taking all $a_i = 1$ and $\rho \equiv \lceil (n-q)/2 \rceil$. For $n < q - 1$, no sums are congruent to -1 when all a_i equal 1. The asymptotic growth of the mod q binomial coefficients, studied in connection with saturated chain partitions [7], implies that the lower bound in Corollary 2 approaches $2^n/q$ as $n \to \infty$ with fixed q. (This remains true even if q grows with n, provided that $q = o(n^{1/2})$.) Hence, for any sequence $\{a_1, a_2, \ldots\}$ of reduced residues mod q, the distribution of the mod q sums of the first n residues is asymptotically uniform as $n \to \infty$.

The Littlewood-Offord problem has an equivalent formulation that considers the concentration of sums of the form $\sum_{i=1}^n \delta_i a_i$ with each $\delta_i = 1$ or -1, where as before $\|a_i\| \geq 1$ for all i. The analogous problem in $\mathbf{Z}_q$ can be solved by a reduction to the original problem of Theorem 1.

Corollary 3. *Let* $a_1, \ldots, a_n$ *be reduced residues in* $\mathbf{Z}_q$. *Let* $P \subseteq \mathbf{Z}_q$, *where* $|P| = k$. *Then the number of the* 2^n *sums* $\sum_{i=1}^{n} \delta_i a_i$ *in* P, *where each* δ_i *is* 1 *or* -1, *is at most the sum of the* k *middle* $\bmod r$ *binomial coefficients in* n, *where* r *is* q *when* q *is odd and* $q/2$ *when* q *is even, and this bound is best possible.*

Acknowledgment

The author is grateful to Oren Patashnik and Ted Sweetser for many suggestions that greatly improved the presentation of this paper.

References

1. I. Anderson, *Combinatorics of finite sets*, Clarendon Press, Oxford, 1987.
2. N. G. de Bruijn, C. A. van Ebbenhorst Tengbergen, and D. R. Kruyswijk, *On the set of divisors of a number*, Nieuw Arch. Wisk. (2) **23** (1952), 191–193.
3. P. Erdös, *On a lemma of Littlewood and Offord*, Bull. Amer. Math. Soc. **51** (1945), 898–902.
4. P. Frankl and Z. Füredi, *The Littlewood-Offord problem in higher dimensions*, Ann. of Math. (2) **128** (1988), 259–270.
5. C. Greene and D. J. Kleitman, *Proof techniques in the theory of finite sets*, Studies in Combinatorics (G.-C. Rota, ed.), Math. Assn. America, Philadelphia, PA, 1978, pp. 22–79.
6. J. R. Griggs, *The Littlewood-Offord problem: Tightest packing and an M-part Sperner theorem*, European J. Combin. **1** (1980), 225–234.
7. ———, *Saturated chains of subsets and a random walk*, J. Combin. Theory Ser. A **47** (1988), 262–283.
8. G. O. H. Katona, *On a conjecture of Erdös and a stronger form of Sperner's theorem*, Studia Sci. Math. Hungar. **1** (1966), 59–63.
9. ———, *Families of subsets having no subset containing another with small difference*, Nieuw Arch. Wisk. (3) **20** (1972), 54–67.
10. D. J. Kleitman, *On a lemma of Littlewood and Offord on the distribution of certain sums*, Math. Z. **90** (1965), 251–259.
11. ———, *On a lemma of Littlewood and Offord on the distributions of linear combinations of vectors*, Adv. in Math. **5** (1970), 1–3.
12. ———, *Some new results on the Littlewood-Offord problem*, J. Combin. Theory Ser. A **20** (1976), 89–113.
13. J. E. Littlewood and A. C. Offord, *On the number of real roots of a random algebraic equation*, Mat. Sb. **12** (1943), 277–286.
14. E. Sperner, *Ein Satz über Untermengen einer endlichen Menge*, Math. Z. **27** (1929), 544–548.
15. R. C. Vaughan and T. D. Wooley, *On a problem related to one of Littlewood and Offord*, Quart. J. Math. Oxford (2) **42** (1991), 379–386.

Department of Mathematics, University of South Carolina, Columbia, South Carolina 29208

E-mail address: griggs@math.scarolina.edu