Nonabelian sets with distinct k-sums

Andrew M. Odlyzko

AT&T Bell Laboratories
Murray Hill, New Jersey 07974
(Email: amo@research.att.com)

Warren D. Smith

NEC
4 Independence Way
Princeton, New Jersey 08540
(Email: wds@research.nj.nec.com)

ABSTRACT

A modified Bose-Chowla construction of sets with distinct sums of k-element subsets is presented. In infinitely many cases it yields sets with a certain multiplicative symmetry. These sets are then used to construct large sets S in certain nonabelian groups with the property that all k-letter words with letters from S are distinct.

Keywords: S_k-sets, sets with distinct sums, additive basis, groups, combinatorics.

Nonabelian sets with distinct k-sums

A. M. Odlyzko

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

W. D. Smith

NEC
4 Independence Way
Princeton, New Jersey 08540

1. Introduction

Sets with distinct k-sums are (hopefully large) sets S such that all sums of k elements selected from S are distinct. (For short, we will call such sets *S_k-sets.*) In the past, interest has generally been focused on such sets inside of Z_m (that is, the *sum* is evaluated modulo m). Most of the applications still work if S and the $+$ operation live inside any abelian group. In some cases, larger sets S may be found inside such groups than exist in the cyclic group of the same order. S_k-sets have many uses in combinatorics [5, 11, 7, 3].

We first show that for each $k \geq 2$, an infinite number of values m exist so that a set S with distinct k-sums exists inside Z_m, where $|S|^k > m$, and such that these sets S enjoy a *multiplicative symmetry* modulo m. (These sets are a slight variant of a well-known construction. What is new is that our modification gives sets with multiplicative symmetries.)

Second, we extend the S_k-set notion to nonabelian groups G. We prove that for each value of $k = 2, 3, \ldots$, an infinite number of groups G exist, such that there is a set S inside G with $|G|^{1/k} = O(|S|k)$ and such that all k-letter words whose letters are in S are distinct in G. These sets arose in connection with the second author's ongoing work on maximal number of edges in graphs of small girth.

Definition 1. *Perfect difference sets* are sets S, $S \subset Z_m$, where Z_m is the additive abelian group of integers modulo m, such that every nonzero integer modulo m has a unique representation as a difference $a - b \bmod m$, $a \in S$, $b \in S$.

In 1938, James Singer ([15], [10], [16]) constructed perfect difference sets for $|S| = q$, q any prime power. So far, Singer's construction is the only construction (up to obvious isomorphisms) that has ever been found for perfect difference sets. It is not known whether perfect difference sets exist that are not of Singer's type.

Marshall Hall found that Singer's sets, as well as all known generalized difference sets (that is, in which each nonzero element of Z_m is represented in λ [a constant] number of ways as a difference of two elements in S) always possess isomorphs exhibiting *multiplicative symmetries*. That is, multiplying S by some integer t (modulo m) leaves it invariant. Indeed, Hall observes [10] that for every known generalized difference set, any prime t such that $\gcd(m, t) = 1$ and $t|(|S| - \lambda)$ gives rise to a multiplicative symmetry.

For example, with $q = 2$, $m = 7$, the set $S = \{1, 2, 4\}$ is a perfect difference set featuring the multiplicative symmetry $S = 2S$. With $q = 3$, $m = 13$, the set $S = \{0, 1, 3, 9\}$ is a perfect difference set featuring the multiplicative symmetry $S = 3S$.

This phenomenon was partially explained by Hall and Ryser's *multiplier theorem* [10, Theorem 11.4.1, p. 160 and Theorem 11.15.2, p. 166].

Perfect difference sets may be generalized in the following two ways. First, we may consider replacing Z_m by an arbitrary abelian group. (As motivation, we mention that, as was observed in [3], there is an S_2-set of size 7 inside $G = Z_2^3 \times Z_3$, $|G| = 24$. The least m so that an S_2=set of size 7 exists inside Z_m is 48 [8].) Secondly, we note that the sums of two elements in S are distinct if and only if the differences of elements in S are distinct, since $a + b = c + d$ if and only if $a - d = c - b$, which suggests the generalization of letting there be more than two elements in the sum:

Definition 2. S_k*-sets* are sets $S \subset G$, where G is any abelian finite group, such that the sum of any k elements selected (with replacement) from S is not equal to the sum of any other k elements of S.

Thus S_2-sets in $G = Z_m$, if $m = |S|^2 - |S| + 1$, are precisely the perfect difference sets. Applications of S_k-sets may be found in [5, 11, 7, 3].

How large can an S_k-set be, compared to the size of the containing group G? Obviously

$$|G| \geq \frac{|S|(|S|+1)\ldots(|S|+k-1)}{k!}, \tag{1.1}$$

since the right-hand side is the number of ways to choose (a multiset of) k elements from S, with replacement. Thus when $|G|$ is large and k is fixed, we have

$$|S| \precsim (k!|G|)^{1/k} . \tag{1.2}$$

An upper bound with better asymptotic behavior is

$$|G| \geq \frac{\prod_{i=0}^{\lfloor k/2 \rfloor} (|S| - \lceil k/2 \rceil + i) \cdot \prod_{j=0}^{\lceil k/2 \rceil} (|S| + j)}{\lfloor k/2 \rfloor ! \cdot \lceil k/2 \rceil !} . \tag{1.3}$$

This arises as follows. Choose $\lfloor k/2 \rfloor$ elements with replacement from S, and let their sum be A. From the remaining $\geq |S| - \lfloor k/2 \rfloor$ elements, choose $\lceil k/2 \rceil$ elements, and let their sum be B. Then the differences $A - B$ are distinct, and their number is bounded below by the quantity on the right hand side of (1.3). When $|G|$ is large and k is fixed, this leads to

$$|S| \lesssim (\lfloor k/2 \rfloor ! \cdot \lceil k/2 \rceil ! \cdot |G|)^{1/k} . \tag{1.4}$$

When $k = 2$, Singer's construction, known results on prime gaps, and this upper bound are sufficient to determine the asymptotics of the minimal order $\nu(n)$ of an abelian group G containing an S_2-set of cardinality n:

$$\nu(n) \sim n^2 . \tag{1.5}$$

This observation settles an open problem mentioned in [3, p. 1343].

R.C. Bose and S. Chowla [2] constructed S_k-sets of cardinality $q + 1$, where $k = 2, 3, 4, \ldots$ and q is any prime power, inside Z_m, where $m = \frac{q^{k+1}-1}{q-1}$. These specialize to Singer's sets when $k = 2$. They also constructed S_k-sets of cardinality q, where $k = 2, 3, 4, \ldots$ and q is any prime power, inside Z_m, where $m = q^k - 1$.

Observe that in the limit when $k \geq 3$ is fixed and $|G|$ is large, Bose and Chowla's S_k-sets are only a constant factor ($\approx \frac{k}{2e}$, if k is large, where $e \approx 2.71828$ is Euler's constant) smaller than the asymptotic upper bound (1.4). When $k \geq 3$, however, Bose and Chowla's sets are not necessarily *exactly* optimal.

- Example: Bose and Chowla supply a 6-element S_3-set inside Z_{156}, but there is a 8-element S_3-set in Z_{156}: $S = \{1, 5, 25, 125\} \cup \{2, 10, 50, 94\}$.

- Example: Bose and Chowla supply a 5-element S_3-set inside Z_{124}, but there is a 6-element S_3-set in Z_{124}: $S = \{1, 5, 25\} \cup \{2, 10, 50\}$.

Also note that both these examples have a multiplicative symmetry $S = 5S$.

In the present paper, we will observe that in an infinite number of cases some isomorph of Bose and Chowla's second type of set possesses a multiplicative symmetry.

Theorem 1. *For every integer $k \geq 2$ and every prime p so that $k|(p-1)$, there exists an S_k-set S of cardinality p inside Z_m, where $m = p^k - 1$, such that $S = pS$.*

Next, we will extend the S_k-set notion to nonabelian groups G.

Definition 3. A *nonabelian S_k-set* is a set $S \subset G$, where G is a (nonabelian) finite group, such that all k-letter words, whose letters are selected (with replacement) from S, are distinct in G.

Notice that any S_k-set, including a nonabelian one, is also an S_j-set for every $j = 1, 2, \ldots k$. (Proof: consider appending a $(k-j)$-letter constant suffix to the end of the j-letter words.)

We prove the following result.

Theorem 2. *For each value of $k = 2, 3, \ldots$, and any prime p with $k|(p-1)$, a nonabelian group G of order $|G| = (p^k - 1)k$ exists which contains a nonabelian S_k-set S of cardinality $(p-1)/k$.*

Analogously to (1.1), one easily sees that any nonabelian S_k-set S inside a group G must obey

$$|S| \leq |G|^{1/k}, \tag{1.6}$$

so the construction of Theorem 2 comes within a constant factor (in the asymptotic regime where k is fixed and $|G|$ is large) of this upper bound. When k is large, this constant factor is approximately k.

We can do better if $k = 2$ and if we do not require that words a^2 be distinct (or equivalently, if we remove the words *with replacement* from Definition 3):

Theorem 3. *Let q be a prime power. Then there exists a set S of cardinality $q + 2$ inside the dihedral group D_{2m} of order $2m$, where $m = (q^3 - 1)/(q - 1)$, such that the products xy with $x, y \in S$, $x \neq y$, are distinct. (In particular, $xy \neq yx$ for $x \neq y$.)*

Proof. Let D_{2m} be generated by r and f where $r^m = f^2 = (rf)^2 = 1$. Let S consist of the $q + 1$ elements of D_{2m} of form $r^z f$ where z is in Singer's perfect difference set inside Z_m, and 1. ∎

Remark: One may also construct a set S of cardinality $1 + \prod_i (q_i + 1)$ inside a group of order $2 \prod_i (q_i^3 - 1)/(q_i - 1)$ where the q_i are prime powers, such that all the words xy, $x \neq y$, are distinct.

2. S_k-sets with multiplicative symmetries

In this section we prove Theorem 1. We modify the Bose-Chowla construction [2, 9]. Let g be a primitive element of $GF(p^k)$ (i.e., an element of multiplicative order $p^k - 1$). The discrete logarithm of $y \in GF(p^k)$, $y \neq 0$, is an integer ℓ, taken as an element of Z_m, $m = p^k - 1$, such that $y = g^\ell$. We write $\ell = \log_g y$. We will often use the bijection between Z_m and $GF(p^k) \setminus \{0\}$ given by the discrete logarithm.

As in the Bose-Chowla construction, choose $x \in GF(p^k)$ so that x is of degree k over $GF(p)$, and is thus not in any proper subfield of $GF(p^k)$. For a fixed $b \in Z_m$, we let

$$S = \{\log_g(x+j) + b : \ 0 \leq j \leq p-1\} \ . \tag{2.1}$$

The standard Bose-Chowla construction has $b = 0$. The present sets remain S_k-sets since the addition of a constant to all elements does not affect the S_k-set property.

We now show that if we choose x and b properly, then S will have the multiplicative symmetry $pS = S$. This symmetry property will hold if for every $j \in GF(p)$, there is an $h \in GF(p)$ such that

$$p(\log_g(x+j) + b) = \log_g(x+h) + b \tag{2.2}$$

holds in Z_m. Exponentiating, we find this is equivalent to the equation

$$g^{bp}(x+j)^p = g^b(x+h) \tag{2.3}$$

in $GF(p^k)$, which (by the "freshman's dream" identity $(A+B)^p \equiv A^p + B^p \bmod p$) in turn is equivalent to

$$x^p = g^{-b(p-1)}x + g^{-b(p-1)}h - j \ . \tag{2.4}$$

If there are fixed g, x and b such that as j varies over $GF(p)$, the h defined by Eq. (2.4) remains in $GF(p)$, then we must have

$$\alpha = g^{-b(p-1)} \in GF(p) \ . \tag{2.5}$$

Moreover, we then must have

$$x^p = \alpha x + \alpha h - j \ . \tag{2.6}$$

If Eq. (2.6) holds for even a single pair (h, j) with $\alpha \in GF(p)$, then for every $j \in GF(p)$, there will be an $h \in GF(p)$ such that Eq. (2.6) holds, and the set S will satisfy $pS = S$.

Suppose that $k|(p-1)$. We will show that a suitable choice of x and α exists so that Eq. (2.6) holds with $h = (j+1)/\alpha$ for all j. We choose

$$\alpha = g^{(p^k-1)/k} \ . \tag{2.7}$$

We first show that α satisfies Eq. (2.5). To prove this, it suffices to show that $p-1$ divides $(p^k-1)/k$. This is equivalent to showing that k divides

$$\frac{p^k-1}{p-1} = p^{k-1} + p^{k-2} + \ldots + 1 \ .$$

However, modulo $p-1$ the sum on the right hand side above is k, and since k divides $p-1$, we are done.

We now come to the heart of the proof. Consider the equation

$$z^p - \alpha z - 1 = 0 \ . \tag{2.8}$$

When we factor this over $GF(p)$, we *claim* that it has one linear factor and $(p-1)/k$ irreducible factors, each of which is of degree k. If z is in $GF(p)$, then $z^p = z$ by Fermat's little theorem, so (2.8) shows that $z = -1/(\alpha-1)$. Further, (2.8) has no multiple roots by the derivative test, so we have established the claimed result about linear factors. Suppose now that z is a root of (2.8) but z is not in $GF(p)$. The conjugates of z are z^p, z^{p^2}, z^{p^3},.... We find that

$$z^{p^2} = (\alpha z + 1)^p = \alpha z^p + 1 = \alpha^2 z + \alpha + 1 \ . \tag{2.9}$$

An easy induction establishes the more general relation

$$z^{p^r} = \alpha^r z + \frac{\alpha^r - 1}{\alpha - 1} \ . \tag{2.10}$$

Since α is a primitive kth root of unity, we find that $z^{p^\mu} = z$ for $\mu = k$, but for no smaller positive μ. Hence z is of degree k over $GF(p)$, and our *claim* is now proved.

We have shown that for $k|(p-1)$, if we select α according to (2.7), then there will be an x satisfying (2.8) such that the set S will have the multiplicative symmetry $pS = S$. ■

We now mention some further consequences of the above proof.

1. The mapping $x \rightarrow px$ of our set S to itself consists of one fixed point and $(p-1)/k$ orbits of length k. To see this, note that for x and α, $\alpha \neq 0$, fixed,

$$\alpha h - j = x^p - \alpha x = 1$$

has exactly one solution (h, j) with $h = j$, namely $h = j = 1/(\alpha - 1)$, corresponding to the fixed point. There cannot be orbits of length r, $2 \le r < k$, since that would imply

$$h = \alpha^r h - \frac{\alpha^r - 1}{\alpha - 1}$$

so that (we are allowed to divide out the factor of $\alpha^r - 1$, since it is nonzero, since α is a primitive kth root of unity) $h = 1/(\alpha - 1)$, but that was the fixed point. ■

2. Our construction requires that $k|(p-1)$. Conversely, one can show that if Eq. (2.6) is satisfied for any h and j, and some $\alpha \in GF(p)$, with x of degree k over $GF(p)$, then $k|(p-1)$.

3. The value of the *offset* b may be deduced, from Eqs. (2.5), (2.7), and the fact that α is a primitive kth root of unity, to be

$$b = \frac{(p^k - 1)(k - 1)}{(p - 1)k}. \tag{2.11}$$

4. The symmetric S_k-sets in Z_m which arise in this construction will remain symmetric S_k-sets if any multiple of m/k is added to each element, or equivalently to b.

In practice, to construct the set S, we would select α to be any element of $GF(p) \setminus \{0\}$ of multiplicative order k, and let $f(X)$ be one of the irreducible factors of degree k of $X^p - \alpha X - 1$ over $GF(p)$. The field $GF(p^k)$ would then be represented as $GF(p)[X]/(f(X))$, with x the image of X, and g would be a $((p^k-1)/k)$-th root of α generating $GF(p^k)$.

We now give an example to illustrate the construction procedure. Let $p = 11$ and $k = 5$. Note $5|(11-1)$. The prime factorization of $m = 11^5 - 1 = 161050$ is $2 \cdot 5^2 \cdot 3221$.

We select $\alpha = 9$ since $9^5 \equiv 1 \bmod 11$.

The factorization of $x^{11} - 9x - 1$ over $GF(11)$ is

$$(7 + x)(2 + 4x + 9x^2 + 6x^3 + 2x^4 + x^5)(7 + 4x + 9x^2 + 6x^3 + 2x^4 + x^5). \tag{2.12}$$

We will therefore use $f(x) = 2 + 4x + 9x^2 + 6x^3 + 2x^4 + x^5$.

A suitable g, which is a 32210th root of 9 (modulo F and modulo 11), is $g = 2 + x^2$. The fact that this g is a generator (as opposed to just being any old 32210th root of 9) may be verified by observing that none of $g^{5\cdot5\cdot2} = 2x + 6x^2 + 4x^3 + 10x^4$, $g^{3221\cdot5\cdot2} = 9$, and $g^{3221\cdot5\cdot5} = 4$ are 1.

We find Eq. (2.11) that $b = 12884$. Then $\log_g(x + 7) = 3221$, $\log_g(x + 0) = 30542$, $\log_g(x + 6) = 70549$, and so on, as are easily verified, so that, upon adding b to these values, we arrive finally at the sought-after S_5-set modulo 161050:

$$\{16105\} \cup \{43426, 83433\} \times \{1, 11, 11^2, 11^3, 11^4\}. \tag{2.13}$$

Note that the complicated steps here were the selection of g and the discrete logarithm calculations. (Both of these computations are of course easy to verify by binary powering, but it is not immediately clear how to do them.) Selecting g is actually quite efficiently accomplished by random trial. The probability that a random nonzero element of $GF(p^k)$ is a generator is $\phi(m)/m$, where ϕ is Euler's totient function and $m = p^k - 1$, and the probability that a random generator g will obey $g^{m/k} = \alpha$ is $1/k$. The combined probability $\phi(m)/(mk)$ (which in the present case is $1288/16105 \approx 0.08$) is of order at least $1/(k^2 \log p)$.

The discrete logarithms are certainly the computational bottleneck. In small cases such as this one, exhaustive search suffices. For larger values of $m = p^k - 1$, one can use the polynomial factorization algorithms in [6] and discrete logarithm algorithms in [13, 14].

3. Large nonabelian S_k-sets

In this section we prove Theorem 2.

The group is the following group of permutations of $m = p^k - 1$ letters:

$$\begin{array}{c} x \to x + a \bmod m, \ \ a = 0..m-1, \ \ \textit{rotations} \\ x \to xp + a \bmod m, \ \ \textit{scramblings} \end{array} \tag{3.1}$$

and the permutations they generate, namely

$$x \to xp^e + a \bmod m, \ (e = 0..k-1, a = 0..m-1) \ . \tag{3.2}$$

We observe that

- The group has order km.
- The kth power of a scrambling is a rotation (since $p^k \equiv 1 \bmod m$).

Note that the composition of k scramblings with a-values a_1, a_2, a_3,... a_k is the following permutation:

$$x \to xp^k + (a_1 p^{k-1} + a_2 p^{k-2} + \ldots + a_k) \tag{3.3}$$

which is actually a rotation since $p^k = 1 \bmod m$. (It is not the identity, however, unless $a_1 = a_2 = \ldots = a_k \in \{0, p-1\}$.)

Let T be an ordinary abelian S_k-set of cardinality p, inside Z_m constructed in Theorem 1, and having the multiplicative symmetry $Tp = T$. Then divide T into $(|T| - 1)/k$ equivalence classes of size k (also called *orbits*) under this symmetry plus a singleton. Then let S be the scramblings with a's consisting of one representative from each cardinality-k equivalence class.

The reason this set S works is that $a_i p^{k-i}$ is also an element of T due to the multiplicative symmetry, so that the rotation length in (3.3) is a sum of k elements of T, so these are distinct – except for the possibility of two such sums being the same sum in a different order, which cannot happen since we have picked one representative from each equivalence class. ■

4. Open problems

1. Understand the multiplicative symmetries of S_k-sets in Z_m.

2. Here are two alternative ways to define *nonabelian S_k-sets S* inside a nonabelian group G.

   - Consider the $2k$-letter words whose letters are alternately in S and in S^{-1}, and where we only allow words such that no letter is adjacent to its inverse. We require that none of these words are the identity.

   - Consider the ℓ-letter words w whose letters lie in S or S^{-1}. Again, no letter of w is allowed to be adjacent to its inverse. We require that none of these words are the identity.

   Can large nonabelian S_k-sets of these two types be constructed? If these problems are solved, then one will have also made progress on an open problem in graph theory, the problem of finding the graphs of fixed girth $g > 2k$ and having the most edges. Specifically, Cayley graphs and bipartite doubles of Cayley graphs constructed using generators from S will have large girths.

References

[1] J. A. Bondy and U. S. R. Murty, *Graph theory with applications*, North-Holland, 1976.

[2] R. C. Bose and S. Chowla, Theorems in the additive theory of numbers, *Math. Helvet.*, 37 (1962–3) 141–147.

[3] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, A new table of constant weight codes, *IEEE Trans. Information Th.*, 36(6) (1990) 1334–1380.

[4] R. H. Bruck, Difference sets in a finite group, *Trans. Amer. Math. Soc.*, 78 (1955) 464-481.

[5] F. R. K. Chung, Diameters and eigenvalues, *J. AMS*, 2(2) (1989) 187–196.

[6] K. O. Geddes, S.R. Czapor, and G. Labahn, *Algorithms for computer algebra*, Kluwer, 1992.

[7] R. L. Graham and N. J. A. Sloane, Lower bounds for constant weight codes, *IEEE Trans. Info. Theory*, 26 (1980) 37–43.

[8] R. L. Graham and N. J. A. Sloane, On additive bases and harmonious graphs, *SIAM J. Algebraic & Discr. Methods*, 1 (1980) 382–404.

[9] H. Halberstam and K. F. Roth, *Sequences*, Oxford University Press, 1966.

[10] Marshall Hall, Jr., *Combinatorial Theory*, Wiley, 1986.

[11] Torliev Kløve, A lower bound for $A(n, 4, w)$, *IEEE Trans. Info. Theory*, 27(2) (1981) 257–258.

[12] Rudolf Lidl and Harald Niederreiter, *Finite Fields*, Addison-Wesley, 1983.

[13] K. S. McCurley, *The discrete logarithm problem*, pp. 49-74 in *Cryptology and computational number theory*, ed. C. Pomerance, AMS Proc. Sympos. Pure Math. #42, 1990.

[14] A. M. Odlyzko, *Discrete logarithms in finite fields and their cryptographic significance*, pp. 224-314 in *Advances in Cryptology, Proceedings of EUROCRYPT 84*, ed.

T. Beth, N. Cot, and I. Ingemarsson, Springer-Verlag Lecture Notes in Computer Science #209, 1985.

[15] James Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, 43 (1938) 377–385.

[16] James Singer, Perfect difference sets, *Trans. New York Acad. Sci.*, (2) 28 (1965/6) 883–888.