EXHAUSTIVE DETERMINATION OF (511, 255, 127)-CYCLIC DIFFERENCE SETS

ROLAND B. DREIER AND KENNETH W. SMITH

1. Introduction

In this paper we describe an exhaustive search for all cyclic difference sets with parameters $(v, k, \lambda) = (511, 255, 127)$, and discuss the implications of this search for Golomb's conjecture on the relationship between the autocorrelation property and the de Bruijn property for binary sequences.

Recall the definition of a difference set. If G is a group of order v (with group operation written multiplicatively), we say a subset D of G is a (v, k, λ) *difference set* if:

1. D has k elements.
2. For each element $g \in G$, $g \neq 1$, there are precisely λ pairs (x, y) of elements of G such that $xy^{-1} = g$.

If D is a difference set, then any translation gD is also a difference set. Similarly, if σ is an automorphism of G, then $\sigma(D)$ is again a difference set. If two difference sets D and D' can be transformed into one another by a combination of translations and automorphisms, we will call them *equivalent* (one easily verifies that this is indeed an equivalence relation).

Following [Hal74], we will also regard a difference set D as giving rise to an element of the group ring $\mathbf{Z}[G]$ (i.e. the set of formal sums of elements of G with coefficients in $\mathbf{Z}$, endowed with a ring structure via componentwise addition and multiplication). If D is a difference set, then define the element of the group ring $\theta(D) = \sum_{g \in D} g$.

For $d = \sum a_g g \in \mathbf{Z}[G]$, define $d^{-1} = \sum a_g g^{-1}$. Note that d^{-1} is not the multiplicative inverse of d in $\mathbf{Z}[G]$; indeed, not every element of the group ring is invertible. But this will not be relevant for us.

Now let $\theta(D) = \sum a_g g$ for D a difference set. From the defining properties of difference sets, one immediately sees:

1. Every coefficient a_g is either 0 or 1, and exactly k of the a_g are non-zero.
2. $\theta(D)\theta(D)^{-1} = (k - \lambda)1 + \sum_{g \in G} \lambda g$ (1 is the identity element of G)

Conversely, suppose we have $d = \sum a_g g \in \mathbf{Z}[G]$ satisfying the properties above. It is easy to check that $D = \{g \in G : a_g \neq 0\}$ is a difference set.

In this paper we will only be concerned with *cyclic* difference sets, that is difference sets with the group $G = \mathbf{C}_v$, the cyclic group with v elements. We will often wish to regard $\mathbf{C}_v$ as the additive group of integer residues modulo v; however, for convenience in dealing with the group ring, we will write $\mathbf{C}_v$ with multiplicative notation. To fix notation, we will regard $\mathbf{C}_v$ as the abelian group generated by g_v with the relation $g_v^v = 1$. Henceforth, when we refer to a difference set, we will mean a cyclic difference set.

If $(t, v) = 1$, then $g \mapsto g^t$ defines an automorphism of the group $\mathbf{C}_v$, which we will write as f_t. If D is a difference set, then if $f_t(D) = gD$ for some $g \in \mathbf{C}_v$, we will say t is a *multiplier* of D. This terminology makes sense if $\mathbf{C}_v$ is viewed additively; for then f_t is multiplication by t. In fact, these f_t are all of the automorphisms of $\mathbf{C}_v$.

2. The Search

Cyclic difference sets with parameters $(2^d - 1, 2^{d-1} - 1, 2^{d-2} - 1)$, which we will call Hadamard difference sets, are intimately connected with almost-balanced, autocorrelated binary sequences of length $2^d - 1$. For if D is a difference set, then the definition of a difference set implies that the binary sequence $\{s_n\}$ given by $s_n = 0$ if and only if $c_v^n \in D$ is almost-balanced and autocorrelated.

In [Che83], an exhaustive search for all cyclic difference sets with $d = 8$ (and hence $(v, k, \lambda) = (255, 127, 63)$) is described.

We will describe our search for the case when $d = 9$. In what follows, when we refer to a difference set, we will mean a Hadamard difference set, usually with $d = 9$ (and hence parameters $(511, 255, 127)$). At the most naive level, searching for all such difference sets means hunting for subsets of size 255 of size 511. Clearly, we cannot check $\binom{511}{255}$ putative difference sets.

However, we need not search this entire space to be sure of determining all difference sets. If we can find a representative of each equivalence class, then it is a simple matter to enumerate all difference sets in the class. [Bau71] contains several theorems that allow us to reduce our work by searching only for equivalence classes.

First, 2 is always a multiplier of a Hadamard difference set ([Bau71, Theorem 3.1]). Second, if D is a difference set with multiplier t, then there is some $D' = gD$, a translate of D, with the property $f_t(D') = D'$ ([Bau71, Lemma 3.7]). Combining these two facts, we see that if we find all difference sets fixed by the action of f_2, we can be sure we have a representative of every equivalence class.

The action of f_2 partitions $\mathbf{C}_v$ into orbits which we will call *cyclotomic cosets* (modulo 2). Clearly, if $D \subset \mathbf{C}_v$ is such that $f_2(D) = D$, then D is a union of cyclotomic cosets.

However, there are still 59 cyclotomic cosets in $\mathbf{C}_{511}$. Of the 59 cyclotomic cosets, there is one of size 1, two of size 3 and 56 of size 9. $255 = 3 + 28 \times 9$, so any difference set must contain exactly one of the size 3 cosets and 28 of the size 9 cosets. However, this collection of putative difference sets has $2 \times \binom{56}{28} \approx 1.5 \times 10^{16}$ members, which is still too many to search exhaustively, so we need to look further for reductions in our work.

In general, if w divides v, then there is a natural homomorphism (which corresponds to reducing modulo w if we were working in an additive group)

$$\begin{aligned} m_w : \mathbf{C}_v &\longrightarrow \mathbf{C}_w \\ g_v^n &\longmapsto g_w^{n \bmod w} \end{aligned}$$

Any homomorphism of groups naturally extends to a homomorphism of group rings. So if D is a difference set, by applying the homomorphism m_w to both sides of our equation in the group ring, we obtain

$$m_w(\theta(D)\theta(D)^{-1}) = m_w(\theta(D))m_w(\theta(D))^{-1} = (k-\lambda)1 + \frac{v}{w}\sum_{g\in\mathbf{C}_w} \lambda g$$

This means that the images of a difference set under these homomorphism m_w will satisfy a relation analogous to the difference set property. So our strategy for reducing the work will be to find all possible homomorphic images of difference sets into smaller cyclic groups. Once we have done this, only the set of preimages of these possible homomorphic images need be searched.

Note that these homomorphisms m_w necessarily map cyclotomic cosets to cyclotomic cosets, and so we can still use cyclotomic cosets in $\mathbf{C}_w$ to reduce our search for homomorphic images.

We can also use automorphisms of $\mathbf{C}_v$ other than f_2 to further reduce our search. We have already used f_2 to show that every equivalence class of difference sets contains a representative that is the union of cyclotomic cosets modulo 2. In the case of $\mathbf{C}_{511}$, we will also be able to use several other automorphisms to further reduce the number of sets we must check. Note that we do not assume that these other automorphisms necessarily come from multipliers for our difference set; in fact, they probably will not.

We know $\mathbf{C}_{511}$ is the direct product of $\mathbf{C}_7$ and $\mathbf{C}_{73}$. $\mathbf{C}_7$ has only three cyclotomic cosets. The three cyclotomic cosets in $\mathbf{C}_7$ are $\{g_7^0\} = \{1\}$, $\{g_7^1, g_7^2, g_7^4\}$, and $\{g_7^3, g_7^5, g_7^6\}$. These three cosets give rise to three elements of the group ring $\mathbf{Z}[\mathbf{C}_7]$, $c_0 = e$, $c_1 = g_7^1 + g_7^2 + g_7^4$ and $c_3 = g_7^3 + g_7^5 + g_7^6$. By our argument above, any homomorphic image into $\mathbf{Z}[\mathbf{C}_7]$ of $\theta(D)$ (where D is a difference set) must be a sum of $a_0c_0 + a_1c_1 + a_3c_3$, with the relation:

$$(a_0c_0 + a_1c_1 + a_3c_3)(a_0c_0^{-1} + a_1c_1^{-1} + a_3c_3^{-1}) = 128 \cdot 1 + 73 \sum_{g \in \mathbf{C}_7} 127g$$

This equation holds in the group ring $\mathbf{Z}[\mathbf{C}_7]$. However, it can be turned into several simultaneous diophantine equations in the integers a_0, a_1 and a_3 by expanding out the products and noting that for the equation to hold, it must hold for the coefficients of each group element individually.

Note that the automorphism f_3 permutes the nonzero cyclotomic cosets modulo 7, so we can assume without loss of generality that $a_1 \geq a_3$. We then easily obtain the two solutions

$$(a_0, a_1, a_3) = (45, 37, 33) \text{ or } (27, 37, 39)$$

$\mathbf{C}_{73}$ is slightly harder. It has nine cyclotomic cosets, generated by g_{73} to the powers 0, 1, 3, 5, 11, $73 - 11 = 62$, $73 - 5 = 68$, $73 - 3 = 70$, and $73 - 1 = 72$. One obtains equations for the nine coefficients b_0, b_1, b_3, b_5, b_{11}, b_{-11}, b_{-5}, b_{-3} and b_{-1}. Also, one notes that f_{15} cycles the nonzero cyclotomic cosets modulo 73, so again we can assume that b_1 has the largest value. Also f_{15} leaves the cyclotomic cosets modulo 7 fixed, so this assumption does not interfere with our previous assumption on the order of solutions from $\mathbf{C}_7$. In any event, our equations can be exhaustively solved to give the four solutions

$$(b_0, b_1, b_3, b_5, b_{11}, b_{-11}, b_{-5}, b_{-3}, b_{-1}) = \begin{cases} (3, 5, 1, 3, 3, 5, 3, 3, 5) \\ (3, 5, 1, 3, 4, 4, 5, 4, 2) \\ (3, 6, 3, 4, 2, 2, 3, 5, 3) \\ (3, 7, 3, 3, 3, 3, 3, 3, 3) \end{cases}$$

With all possible homomorphic images of difference sets in $\mathbf{C}_{511}$ into both $\mathbf{C}_7$ and $\mathbf{C}_{73}$, we are in a position to complete our exhaustive search.

Our putative difference sets will be subsets of $\mathbf{C}_{511}$ whose homomorphic images in $\mathbf{C}_7$ and $\mathbf{C}_{73}$ fall into one of the cases we have listed above. This can be conveniently imagined as filling in a 7×73 array with 0s and 1s such that we match given row and column sums, with the additional condition that the entry in position (x, y) must equal the entry in position $(2x, 2y)$.

This was done in two stages. First we note that the 3 cyclotomic cosets in $\mathbf{C}_7$ and 9 cosets in $\mathbf{C}_{73}$ divide the full group $\mathbf{C}_{511}$ into 27 classes. Each of these classes contains either one or three cyclotomic cosets of $\mathbf{C}_{511}$. From the standpoint of homomorphic images into $\mathbf{C}_7$ and $\mathbf{C}_{73}$, any two cyclotomic cosets of $\mathbf{C}_{511}$ that lie in the same class are indistinguishable. So we can first fill in a collapsed 3×9 array with column and row sums constrained, with the entries now corresponding to the number (either 0 or 1, or in the range 0-3) of cosets of $\mathbf{C}_{511}$ we are choosing from that class. There are roughly 254,000 permissable ways to do this.

For each permissable way of filling in the 3×9 array, we must check whether each way of actually picking the given numbers of cyclotomic cosets of $\mathbf{C}_{511}$ gives a difference set. This final expansion gives rise to roughly 36 billion cases, which were divided up among roughly 20 Sun workstations and exhaustively checked over the course of about a week.

3. Results

It is a trivial fact that there is a one-to-one correspondence between cyclic difference sets and almost-balanced binary sequences with the autocorrelation property. Therefore, constructing all cyclic difference sets with parameters $(511, 255, 127)$ is equivalent to finding all almost-balanced binary sequences with the autocorrelation property. We say a binary sequence of length $2^d - 1$ has the de Bruijn property if all d-long subsequences other than d zeros appear somewhere in the sequence. In [Gol80], Golomb makes his "conjecture I", that $S \cap C = PN$. In the language we are using, this is the conjecture that any almost-balanced binary sequence with the de Bruijn and autocorrelation properties must be primitive (a sequence of length $2^d - 1$ is primitive if its minimal polynomial has degree precisely d).

The exhaustive search we outlined above produced five inequivalent difference sets, which are listed in the appendix below along with the minimal polynomial for the corresponding binary sequence and its factorization. For each of these difference sets, the binary sequence that they give rise to along with every decimation of the sequence was checked for the de Bruijn property. We check every decimation because it is not clear that a decimation of a non-primitive, autocorrelated, de Bruijn binary sequence must necessarily also be de Bruijn. Only the primitive sequences, which correspond to the Singer-type difference sets, had the de Bruijn property, which verifies Golomb's conjecture for degree $d = 9$.

Appendix A. Difference Sets

We give a representative for each of the five equivalence classes of $(511, 255, 127)$ cyclic difference sets. Rather than list all 255 elements of each difference set, we simply list generators for each of the 29 cyclotomic cosets that form the difference set. The full difference set can be obtained from these 29 elements by multiplying all of the 29 elements by all powers of 2.

A.1. **Singer Type:**

$$\left\{\begin{array}{rrrrrrrrrr} 1, & 7, & 13, & 17, & 21, & 23, & 31, & 35, & 37, & 39, \\ 51, & 53, & 55, & 59, & 61, & 75, & 77, & 79, & 83, & 85, \\ 91, & 95, & 103, & 109, & 123, & 183, & 187, & 219, & 223 & \end{array}\right\}$$

Minimal polynomial (primitive): $x^9 + x^7 + x^6 + x^3 + x^2 + x + 1$

A.2. **Miscellaneous Types:**

$$\left\{\begin{array}{rrrrrrrrrr} 1, & 3, & 5, & 7, & 13, & 15, & 19, & 21, & 23, & 25, \\ 27, & 37, & 39, & 45, & 55, & 57, & 59, & 63, & 77, & 83, \\ 91, & 107, & 117, & 123, & 183, & 191, & 219, & 239, & 255 & \end{array}\right\}$$

Minimal polynomial:

$$\begin{array}{l} (x^9 + x^8 + x^7 + x^6 + x^3 + x + 1) \cdot (x^9 + x^5 + 1) \cdot (x^9 + x^8 + x^7 + x^2 + 1) \cdot \\ (x^9 + x^8 + x^7 + x^5 + x^4 + x^3 + 1) \cdot (x^9 + x^7 + x^5 + x^2 + 1) \cdot \\ (x^9 + x^7 + x^5 + x^4 + x^2 + x + 1) \cdot (x^9 + x^8 + x^7 + x^6 + x^4 + x^2 + 1) \end{array}$$

$$\left\{\begin{array}{rrrrrrrrrr} 1, & 5, & 23, & 27, & 29, & 31, & 37, & 39, & 41, & 47, \\ 55, & 59, & 63, & 75, & 77, & 79, & 85, & 87, & 95, & 109, \\ 117, & 123, & 171, & 175, & 183, & 191, & 219, & 223, & 255 & \end{array}\right\}$$

Minimal polynomial:

$$\begin{array}{l} (x^9 + x^4 + x^3 + x + 1) \cdot (x^9 + x^8 + x^4 + x^3 + x^2 + x + 1) \cdot \\ (x^9 + x^8 + x^7 + x^5 + x^4 + x^2 + 1) \end{array}$$

$$\left\{\begin{array}{rrrrrrrrrr} 1, & 3, & 5, & 7, & 9, & 11, & 17, & 29, & 31, & 43, \\ 53, & 55, & 57, & 61, & 63, & 75, & 77, & 91, & 95, & 109, \\ 117, & 123, & 125, & 171, & 175, & 183, & 219, & 239, & 255 & \end{array}\right\}$$

Minimal polynomial:

$$\begin{array}{l} (x^9 + x^5 + x^4 + x + 1) \cdot (x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1) \cdot \\ (x^9 + x^8 + x^7 + x^6 + x^4 + x^2 + 1) \end{array}$$

$$\left\{\begin{array}{rrrrrrrrrr} 1, & 3, & 5, & 7, & 9, & 13, & 15, & 23, & 27, & 35, \\ 37, & 53, & 55, & 57, & 61, & 75, & 77, & 87, & 107, & 117, \\ 119, & 127, & 171, & 175, & 183, & 191, & 219, & 239, & 255 & \end{array}\right\}$$

Minimal polynomial:

$$\begin{array}{l} (x^9+x^4+1)\cdot(x^9+x^6+x^5+x^3+x^2+x+1)\cdot \\ (x^9+x^7+x^4+x^3+1)\cdot(x^9+x^8+x^4+x+1)\cdot \\ (x^9+x^8+x^5+x^4+1)\cdot(x^9+x^8+x^6+x^3+1)\cdot \\ (x^9+x^8+x^6+x^3+x^2+x+1)\cdot(x^9+x^8+x^7+x^2+1)\cdot \\ (x^9+x^8+x^7+x^6+x^5+x+1) \end{array}$$

References

[Bau71] L. D. Baumert, *Cyclic difference sets*, Lecture Notes in Mathematics 182, Springer-Verlag, New York, 1971.

[Che83] U. Cheng, *Exhaustive construction of* $(255, 127, 63)$*-cyclic difference sets*, Journal of Combinatorial Theory, Series A **35** (1983), no. 2, 115–125.

[Gol80] S. W. Golomb, *On the classification of balanced binary sequences of period* $2^n - 1$, IEEE Transactions on Information Theory **IT-26** (1980), no. 6, 730–732.

[Hal74] M. Hall, *Difference sets*, Mathematical Centre Tracts 57, Mathematical Centre, September 1974, pp. 1–25.

(R. Dreier) Department of Mathematics, Oklahoma State University, Stillwater, OK 74078

E-mail address, R. Dreier: droland@math.okstate.edu

(K. Smith) Department of Mathematics, Central Michigan University, Mt. Pleasant MI 48859

E-mail address, K. Smith: smith_k@mth15.mth.cmich.edu