Available online at www.sciencedirect.com

ScienceDirect

Discrete Mathematics 308 (2008) 2854–2861

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Two applications of relative difference sets: Difference triangles and negaperiodic autocorrelation functions

Alexander Pott

Fakultät für Mathematik, 39016 Magdeburg, Germany

Received 26 May 2003; received in revised form 23 December 2003; accepted 21 June 2006
Available online 6 June 2007

Abstract

The well-known difference sets have various connections with sequences and their correlation properties. It is the purpose of this note to give two more applications of the (not so well known) relative difference sets: we use them to construct difference triangles (based on an idea of A. Ling) and we show that a certain nonexistence result for semiregular relative difference sets implies the nonexistence of negaperiodic autocorrelation sequences (answering a question of Parker [Even length binary sequence families with low negaperiodic autocorrelation, in: Applied Algebra, Algebraic Algorithms and Error-correcting Codes, Melbourne, 2001, Lecture Notes in Computer Science, vol. 2227, Springer, Berlin, 2001, pp. 200–209.]).

Keywords: Difference set; Difference triangle; Autocorrelation function

1. Introduction

A k-subset D of a group $(G, \cdot)$ of order v is called a (v, k, λ)-*difference set* if the list of "differences" $d \cdot (d')^{(-1)}$, $d, d' \in D$, covers every group element $g \neq e_G$ (e_G is the identity element in G) precisely λ times. Note that we write G multiplicatively. However, in some examples G is written additively, for instance if we take G to be the set of residues modulo some integer v, hence if G is cyclic. In this case, we call the difference set *cyclic*.

We may identify D with the group ring element

$$D = \sum_{d \in D} d \quad \text{in } \mathbb{Z}[G],$$

where

$$\mathbb{Z}[G] = \left\{ \sum_{g \in G} a_g \cdot g : a_g \in \mathbb{Z} \right\}$$

denotes the set of all formal sums with elements from G. The set $\mathbb{Z}[G]$ becomes a ring with componentwise addition

$$\left(\sum a_g g\right) + \left(\sum b_g g\right) = \sum (a_g + b_g) g$$

E-mail address: alexander.pott@ovgu.de.

0012-365X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2006.06.048

and convolution

$$\left(\sum a_g g\right) \cdot \left(\sum b_g g\right) = \sum a_g b_h \, (g \cdot h)$$

as multiplication. This ring is called the *group ring*. We note that the group ring over the cyclic group $\mathbb{Z}_v$ has the following nice interpretation:

$$\mathbb{Z}[\mathbb{Z}_v] \cong \mathbb{Z}[x]/(x^v - 1).$$

If $A = \sum a_g \cdot g$, we define

$$A^{(d)} = \sum a_g \cdot g^d.$$

It is easy to see that a k-subset D of a group G of order v is a (v, k, λ)-difference set if and only if

$$D \cdot D^{(-1)} = k \cdot e_G + \lambda \cdot (G - e_G) = (k - \lambda) \cdot e_G + \lambda \cdot G$$

(here $G = \sum_{g \in G} g$). Instead of $a \cdot e_G$, we simply write a. Using $k - \lambda =: n_D$, we obtain

$$D \cdot D^{(-1)} = n_D + \lambda \cdot G. \tag{1}$$

An easy example of a difference set is the set $\{0, 1, 3\}$ in the cyclic group $(\mathbb{Z}_7, +)$: this is a $(7, 3, 1)$-difference set. There are many more examples and infinite series of difference sets; we refer the reader to [1]. Here we just mention the following infinite series of difference sets with $\lambda = 1$ (called *Singer difference sets*):

Theorem 1 (*Singer [15]*). *Cyclic $(q^2 + q + 1, q + 1, 1)$-difference sets exist for all prime powers q.*

Difference sets and symmetric designs are intimately related; in particular, difference sets (and the generalizations considered in this note) with $\lambda = 1$ are related to projective planes. The reader is referred to [1].

Using (1), we can easily describe relative difference sets, a generalization of difference sets. Given a group G of order mn containing a subgroup N of order n, we call a k-subset R of G an (m, n, k, λ)-*relative difference set* if

$$R \cdot R^{(-1)} = k + \lambda \cdot (G - N), \tag{2}$$

i.e. the elements in $G \backslash N$ have λ representations as a "difference" $r \cdot (r')^{-1}$, $r, r' \in R$, and no element in $N \backslash \{e_G\}$ has such a representation. Therefore, we call N the "forbidden subgroup". Note that $(m, 1, k, \lambda)$-relative difference sets are the same objects as (m, k, λ)-difference sets. An example of a $(4, 2, 3, 1)$-relative difference set is the set $\{0, 1, 3\} \subset (\mathbb{Z}_8, +)$ in the cyclic group of order 8. As before, relative difference sets in cyclic groups are called *cyclic*.

An infinite series is the following:

Theorem 2 (*Bose [2]*). *Cyclic $(q + 1, q - 1, q, 1)$-relative difference sets exist for all prime powers q.*

These relative difference sets are called *Bose difference sets*.

We may extend the notion of relative difference sets relative to one subgroup N to difference sets relative to several (disjoint) subgroups:

$$R \cdot R^{(-1)} = k + \lambda \cdot (G - e_G - N_1^* - N_2^* - \cdots - N_s^*),$$

where $N_i^* = N_i \backslash \{e_G\}$, and the N_i's are subgroups with $N_i \cap N_j = \{e_G\}$ for all $i \neq j$.

In my opinion, this notion in its full generality seems to be uninteresting; for interesting special cases related to projective planes, we refer to [5]. In this paper, we only need the following example, see also [12, Example 5.3.2].

Theorem 3 (*Ganley [4]*). *Let q be a prime power, and let $\mathbb{F}_q$ be the finite field with q elements. We denote the multiplicative group of $\mathbb{F}_q$ by $\mathbb{F}_q^*$, the additive group by $\mathbb{F}_q^+$. Then the set*

$$R = \{(x, x) \in \mathbb{F}_q^* \times \mathbb{F}_q^+ : x \in \mathbb{F}_q^*\}$$

satisfies

$$R \cdot R^{(-1)} = q - 1 + (G - N_1^* - N_2^* - (1,0)) = q + G - N_1 - N_2,$$

where

$$N_1 = \{(x,0) : x \in \mathbb{F}_q^*\},$$

$$N_2 = \{(1,x) : x \in \mathbb{F}_q^+\}$$

and

$$G = \mathbb{F}_q^* \times \mathbb{F}_q^+.$$

The set R in this theorem is the subset of a cyclic group if and only if q is a prime.

Example 1. Consider the set $\{0, 1, 3, 14\}$ in the cyclic group $\mathbb{Z}_{20}$. Here we have $q = 5$ and

$$R \cdot R^{(-1)} = 5 + \mathbb{Z}_{20} - \mathbb{Z}_5 - \mathbb{Z}_4,$$

where $\mathbb{Z}_5$ and $\mathbb{Z}_4$ denote, by abuse of notation, the unique subgroups of orders 5 and 4 in $\mathbb{Z}_{20}$.

Later in this note we will consider epimorphic images of difference sets. To this end, we may extend an epimorphism

$$\psi : G \to G/U \ (=: \overline{G})$$

via linearity to an epimorphism

$$\psi : \mathbb{Z}[G] \to \mathbb{Z}[\overline{G}].$$

In particular, if D is a (v, k, λ)-difference set, then the image $\overline{D}$ satisfies

$$\overline{D} \cdot \overline{D}^{(-1)} = n + \lambda \cdot |U| \cdot \overline{G}.$$

Note that (in general) $\overline{D}$ does not correspond to a subset any more, since the coefficients are not just 0 and 1.

The situation in the case of relative difference sets R is slightly more involved since the image of the right-hand side of (2) depends on the intersection of U and N.

If $U \subseteq N$, then $\overline{R}$ has coefficients just 0 and 1 since R contains from each coset of N in G at most one element.

2. Difference triangle sets

A collection $D_1, D_2, \ldots, D_t$ of k-subsets of $(\mathbb{Z}, +)$ is called a (t, k)-*difference triangle set* if all the nonzero differences $d - d'$ with $d, d' \in D_i$, $i = 1, \ldots, t$, are different. We may assume that the minimum element in each of the D_i's is 0. The goal is to find difference triangle sets where $\max_{i=1,\ldots,t}(\max(D_i))$ is small. The smallest possible number is denoted by $m(t, k)$. The precise value of $m(t, k)$ is known for only a small number of values, see [3].

Difference triangle sets have been introduced in the late 1980s (see [8]) in connection with self-orthogonal convolutional codes. The case $t = 1$ has been considered earlier: these are the well-known Golomb rulers (see [6], for instance, a reference which also describes applications of these objects). A brief summary about difference triangle sets is [3].

Obviously, a cyclic relative difference set (in $\mathbb{Z}_v$) with $\lambda = 1$ gives rise to a difference triangle set: we just interpret the differences not modulo v but in $\mathbb{Z}$. If differences of integers are distinct modulo v, they are of course also different in $\mathbb{Z}$.

The well-known Singer difference sets and the Bose difference sets have been used to construct difference triangle sets with $t = 1$. Note that equivalent difference sets give rise to different difference triangle sets: here we call two difference sets D_1 and D_2 in a group $(G, \cdot)$ *equivalent* if there is an integer d with $\gcd(d, v) = 1$ such that $D_2 = D_1^{(d)} \cdot a$ (here we temporarily switch to multiplicative notation).

In [9], the Bose difference sets have been used in a clever way to improve the results that have been obtained by just looking at the Bose difference sets as described above, i.e. interpreting the Bose difference set in $\mathbb{Z}$. We briefly recall the construction. If R is a cyclic $(n + 1, n - 1, n, 1)$-difference set in $(G, \cdot)$ relative to N, then every coset of N contains at most one element from R.

Let $H < G$ be a subgroup of G containing N, and $G/H = \{h_1H, h_2H, \ldots, h_tH\}$. We define

$$R_i = (R \cdot (h_i)^{-1}) \cap H.$$

Note that R_i is a subset of H that contains from each coset of N at most one element. Moreover, the list of "differences" with elements from R_i are all different (and in H), and the set of "differences" $\{r \cdot (r')^{-1} : r, r' \in R_i\}$ is disjoint from the set $\{r \cdot (r')^{-1} : r, r' \in R_j\}$ if $i \neq j$. Note $|R_i| = |R \cap (Hh_i)|$. Since R contains from each coset of N at most one element (there are $n+1$ such cosets) and since $|R| = n$, there is precisely one coset of N which contains no element from R; we denote this coset by Nx. The group H contains N, hence if we look at the intersection sizes $r_i = |R \cap (Hh_i)|$, we obtain

$$r_i = \begin{cases} \dfrac{n+1}{t} & \text{if } x \notin Hh_i, \\ \dfrac{n+1}{t} - 1 & \text{if } x \in Hh_i. \end{cases}$$

Therefore, we have

$$\sum_{i=0}^{k-1} R_i R_i^{(-1)} = \sum_i r_i^2 + H - N \quad \text{in } \mathbb{Z}[H]. \tag{3}$$

We remove one element from each of the R_i's with $|R_i| = (n+1)/t$ in order to obtain difference triangle sets with $k = (n+1)/t - 1$. We may replace each of the R_i's by a suitable shift of it (i.e. we may replace R_i by $R_i \cdot g_i$) in order to make the largest element in the R_i's small. As mentioned earlier, equivalent difference sets give rise to different R_i's, hence different difference triangle sets.

Note that we may add a difference triangle set T of size $(n+1)/t - 1$ whose largest element is $\leqslant n-1$: Eq. (3) shows that no nonzero element in N is covered as a difference, therefore the difference triangle set T may be viewed as a subset of N and can be added to the R_i's.

Another variation (already contained in [9]): we may remove more than just one element from the sets R_i.

The main point in this note regarding difference triangles is to suggest looking at other "difference set type" objects. Unfortunately, the only known cyclic examples I am aware of which have not been used so far are the examples in Theorem 3 where q is a prime (denoted by p), i.e. we have a $p-1$-subset R of $\mathbb{Z}_{p(p-1)}$ which satisfies

$$RR^{(-1)} = p + \mathbb{Z}_{p(p-1)} - \mathbb{Z}_p - \mathbb{Z}_{p-1}.$$

Let H be a subgroup of $\mathbb{Z}_{p(p-1)}$ containing $\mathbb{Z}_p$. As before, we define

$$R_i = (R - h_i) \cap H,$$

where $h_1 + H, \ldots, h_t + H = \mathbb{Z}_{p(p-1)}/H$. In this situation, R contains from each coset of $\mathbb{Z}_p$ precisely one element. Since H contains $\mathbb{Z}_p$, all the R_i's have the same size $(p-1)/t$, hence we obtain difference triangle sets with $k = (p-1)/t$. More precisely,

$$\sum_{i=1}^{t} R_i R_i^{(-1)} = \frac{(p-1)^2}{t} + H - \mathbb{Z}_p - (H \cap \mathbb{Z}_{p-1}).$$

Again, we may shift the R_i and/or replace R by an equivalent difference set.

Example 2. We take $p = 11$. The "difference set" R (constructed using Theorem 3) in $\mathbb{Z}_{110}$ is

$$\{3, 8, 10, 31, 37, 45, 46, 49, 62, 94\}.$$

We take $H = \mathbb{Z}_{55}$ and get

$$R_1 = \{4, 5, 23, 31, 47\},$$

$$R_2 = \{1, 15, 18, 22, 24\}.$$

Shifting the first set by -23 and the second set by -1, we obtain the $(2, 5)$-difference triangle set

$$R_1' = \{0, 8, 24, 36, 37\},$$

$$R_2' = \{0, 14, 17, 21, 23\}$$

which gives a maximum of 37. Using inequivalent difference sets, it is not possible to decrease this value. It is known that $m(2, 5) = 22$, hence our construction is pretty bad in this case. Note that the differences formed by elements in R_1' and R_2' cover no element which is a multiple of 5 and no element which is a multiple of 11 since no nonzero elements in $\mathbb{Z}_{10} \cap H$ and in $\mathbb{Z}_{11}$ are covered by differences. Hence it would be possible to add a $(1, 5)$-difference triangle if $m(1, 5) \leqslant 10$. Unfortunately, $m(1, 5) = 11$.

Loosely speaking, the "packing" using Theorem 3 is less dense than the packing in [9] using Theorem 2, since in the first case there are more elements *not* covered by differences $r - r'$, $r, r' \in R$.

I did a computer search in the same range as [9]. There is precisely one value where my construction using Theorem 3 beats [9]: there is a $(6, 16)$-difference triangle set whose maximum element is 1257 (Ling obtained "only" 1261). The construction uses $p = 97$ in Theorem 3. This improvement shows that not only Singer and Bose difference sets are useful to construct difference triangle sets but also some of the possible generalizations.

3. Negaperiodic autocorrelation

In this section I will show another application of relative difference sets to a problem that appeared in the applicable algebra literature. In [10], Parker investigated sequences of period n with low negaperiodic autocorrelation. He conjectured that for even n, no $\{0, 1\}$-sequences with perfect negaperiodic autocorrelation function can exist. Here I will show that this conjecture is true and that it follows from a nonexistence result on relative difference sets.

Let $s(i)$ denote a binary (i.e. $\{0, 1\}$) sequence of period n (i.e. $s(n + i) = s(i)$ for all $i \in \mathbb{N}$). We define the so-called *negaperiodic autocorrelation function* Q_s of s:

$$Q_s(t) = \sum_{i=0}^{n-1} (-1)^{s(i+t)+s(i)+\lfloor (i+t)/n \rfloor}, \quad 0 \leqslant t < n. \tag{4}$$

We remind the reader that the *periodic autocorrelation function* is

$$P_s(t) = \sum_{i=0}^{n-1} (-1)^{s(i+t)+s(i)}.$$

Example 3. Let (0 1 1 0 0) be the first five entries of a binary sequence of period 5. We obtain

$$P_s(0) = 5, \quad P_s(1) = 1, \quad P_s(2) = -3, \quad P_s(3) = -3, \quad P_s(4) = 1$$

and

$$Q_s(0) = 5, \quad Q_s(1) = -1, \quad Q_s(2) = -3, \quad Q_s(3) = 3, \quad Q_s(4) = 1.$$

If a sequence s satisfies $Q_s(t) = 0$ (resp. $P_s(t) = 0$) for all $0 < t < n$, we say that s has a *perfect negaperiodic* (*resp. periodic*) *autocorrelation function*. There is a lot of evidence that the sequence (1 0 0 0) is (up to equivalence) the only binary sequence of period $n \geqslant 4$ with a perfect periodic autocorrelation function: the existence of such sequences is equivalent to the existence of circulant Hadamard matrices of size n. It is conjectured that there are no circulant Hadamard matrices of size $n > 4$; see [14] for recent progress towards this (apparently difficult) conjecture.

Note that a sequence with perfect negaperiodic autocorrelation function necessarily has even period n: the number $Q_s(t)$ is the sum of n values ± 1 which can be 0 only if the number of summands is even.

We are now going to show that there are no sequences of period $n > 2$ with perfect negaperiodic autocorrelation function.

The following theorem is also implicitly contained in [10]:

Theorem 4. *The existence of a binary sequence of period n with perfect negaperiodic autocorrelation function is equivalent to the existence of a cyclic*

$$\left(n, 2, n, \frac{n}{2}\right)\text{-relative difference set.} \tag{5}$$

Proof. Let R denote a cyclic relative difference set with parameters (5). We define for $i = 0, \ldots, n-1$

$$s(i) := \begin{cases} 1 & \text{if } i \in R, \\ 0 & \text{if } i \notin R \end{cases}$$

and for $i = 0, \ldots, 2n-1$

$$u(i) := \begin{cases} 1 & \text{if } i \in R, \\ 0 & \text{if } i \notin R. \end{cases}$$

The sequence $(s(i))$ has period n, the sequence $(u(i))$ period $2n$. Obviously, we have $s(i) = u(i)$ for $i = 0, \ldots, n-1$. We are now going to show the connection between $s(i)$ and $u(i)$ for $i = n, \ldots, 2n-1$.

Note that

$$i \in R \;\Rightarrow\; i + n \notin R$$

since otherwise $n \in \mathbb{Z}_{2n}$ had a difference representation with elements from R, but n is an element in the "forbidden subgroup" $\{0, n\} \cong \mathbb{Z}_2$.

We also have

$$i \notin R \;\Rightarrow\; i + n \in R$$

since each coset of $N = \{0, n\} < \mathbb{Z}_{2n}$ contains precisely one element from R (since $|R| = n = |\mathbb{Z}_{2n}/N|$). This shows

$$u(i+n) \Leftrightarrow s(i) + 1 \pmod 2 \quad \text{for } i = 0, \ldots, n-1. \tag{6}$$

We are now going to show that

$$Q_s(t) = \sum_{i=0}^{n-1} (-1)^{s(i+t)+s(i)+\lfloor (i+t)/n \rfloor} = 0$$

for $0 < t < n$:

$$\begin{aligned} Q_s(t) &= \sum_{i=0}^{n-1-t} (-1)^{s(i)+s(i+t)} + \sum_{i=n-t}^{n-1} (-1)^{s(i)+s(i+t)+1} \\ &= \sum_{i=0}^{n-1-t} (-1)^{s(i)+s(i+t)} + \sum_{i=n-t}^{n-1} (-1)^{s(i)+s(i+t-n)} \\ &= \frac{1}{2}\left(\sum_{i=0}^{n-1-t} (-1)^{u(i)+u(i+t)} + \sum_{i=n}^{2n-1-t} (-1)^{u(i)+u(i+t)} \right. \\ &\quad \left. + \sum_{i=n-t}^{n-1} (-1)^{u(i)+u(i+t-n)} + \sum_{i=2n-t}^{2n-1} (-1)^{u(i)+u(i+t-n)} \right). \end{aligned}$$

These equalities hold in view of (6).

The final sum above is 0: to prove this, we define

$$A := \{0 \leqslant i \leqslant 2n-1 | u(i) = 0\},$$

$$B := \{0 \leqslant i \leqslant 2n-1 | u(i) = 1\},$$

$$C := \{0 \leqslant i \leqslant 2n-1 | u(i) = u(i+t) = 1\},$$

$$D := \{0 \leqslant i \leqslant 2n-1 | u(i) = u(i+t) = 0\}.$$

Obviously, we have $|A| = |B| = n$; moreover, $|C| = n/2$ (since the element t has precisely $n/2$ representations as a difference with elements from R). This implies $|D| = n/2$, too (since $2|B| - |C| = |D|$) and therefore

$$Q_s(t) = \tfrac{1}{2}(|C| + |D| - (2n - (|C| + |D|))) = 0.$$

We leave it to the reader to reverse the proof in order to show that perfect negaperiodic autocorrelation of s implies that

$$\{i | 0 \leqslant i \leqslant n-1 \text{ and } s(i) = 1\} \cup \{i | n \leqslant i \leqslant 2n-1 \text{ and } s(i-n) = 0\}$$

is a relative difference set with parameters (5). □

The answer to Parker's question follows immediately from the following result due to the author:

Theorem 5 (*Pott [11]*). *Let R be an abelian relative difference set in G with parameters*

$$(n\lambda, n, n\lambda, \lambda).$$

Let g be an element in G. Then the order of g divides $n\lambda$, or we have $n = 2$, $\lambda = 1$ and $G \cong \mathbb{Z}_4$.

The case $n = 2$ and $\lambda = 1$ corresponds to a relative difference set $\{0, 1\}$ which gives rise to a perfect autocorrelation sequence (11) of period 2. The result shows that no cyclic example can exist if $\lambda > 1$:

Corollary 6. *There is no cyclic relative difference set with parameters* (5) *and $n > 2$; equivalently, there are no binary sequences of period $n > 2$ whose negaperiodic autocorrelation function is perfect.*

We note that this corollary is in some contrast to the apparently difficult problem to show that there are no binary sequences with a perfect periodic autocorrelation function which is, as mentioned above, the circulant Hadamard matrix conjecture.

It should be noted that, using slightly different language, the connection between relative difference sets and negaperiodic perfect sequences is already contained in [7].

References

[1] T. Beth, D. Jungnickel, H. Lenz, Design Theory, 2nd ed., Cambridge University Press, Cambridge, 1999.
[2] R.C. Bose, An affine analogue of Singer's theorem, J. Indian Math. Soc. (N.S.) 6 (1942) 1–15.
[3] C.J. Colbourn, Difference triangle sets, in: C.J. Colbourn, J.H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, 1996, pp. 312–317.
[4] M.J. Ganley, Direct product difference sets, J. Combin. Theory Ser. A 23 (1977) 321–332.
[5] D. Ghinelli, D. Jungnickel, Finite projective planes with a large abelian group, in: Surveys in Combinatorics, Bangor, London Mathematical Society Lecture Note Series, vol. 307, Cambridge University Press, Cambridge, 2003, pp. 175–237.
[6] S. Golomb, Construction of signals with favorable correlation properties, in: A. Pott, P.V. Kumar, T. Helleseth, D. Jungnickel (Eds.), Difference Sets, Sequences and their Correlation Properties, NATO Science Series, vol. 542, Kluwer Academic Publishers, Dordrecht, 1999, pp. 159–194.
[7] J. Jedwab, Generalized perfect arrays and Menon difference sets, Design Codes Cryptogr. 2 (1992) 19–68.
[8] T. Kløve, Bounds and construction for difference triangle sets, IEEE Trans. Inform. Theory 35 (1989) 879–886.
[9] A.C.H. Ling, Difference triangle sets from affine planes, IEEE Trans. Inform. Theory 48 (2002) 2399–2401.
[10] M.G. Parker, Even length binary sequence families with low negaperiodic autocorrelation, Applied Algebra Algebraic Algorithms and Error-correcting Codes, Melbourne 2001, Lecture Notes in Computer Science, vol. 2227, Springer, Berlin, 2001, pp. 200–209.

[11] A. Pott, On the structure of abelian groups admitting divisible difference sets, J. Combin. Theory Ser. A 65 (1994) 202–213.
[12] A. Pott, Finite Geometry and Character Theory, Lecture Notes in Mathematics, vol. 1601, Springer, Berlin, Heidelberg, 1995.
[14] B. Schmidt, Characters and Cyclotomic Fields in Finite Geometry, Lecture Notes in Mathematics, vol. 1797, Springer, Berlin, 2002.
[15] J. Singer, A theorem in finite projective geometry and some applications to number theory, Trans. Amer. Math. Soc. 43 (1938) 377–385.