THEORY OF DIFFERENCE SETS

The construction of periodic sequences with good correlation properties is very important in signal processing. Many applications require knowledge of sequences and their correlation functions. In the binary case, sequences with period v can be equivalently described as subsets D of the cyclic group of order v. The distribution of the differences that can be formed with the elements from this subset D can be computed from the correlation function of the corresponding sequence. Therefore, we obtain the following meta-statement: Instead of looking for sequences with good correlation functions, we can equivalently search for subsets of cyclic groups with a good distribution of differences. A difference set is a subset of a group such that the list of differences contains every nonidentity group element equally often. If the group is cyclic, these difference sets correspond to sequences whose correlation function has just two values. Small variations of this uniform difference property correspond to small variations of the two-value property of the sequence. This indicates that the study of difference sets is also important in connection with the design of sequences with good correlation properties.

The investigation of difference sets and their generalizations is of central interest in discrete mathematics. For instance, one of the most popular conjectures, the circulant Hadamard matrix conjecture, is actually a question about difference sets. Difference sets have a long tradition: In 1938, Singer (1) pointed out that the symmetric point-hyperplane design of a finite projective space $PG(n, q)$ contains a cyclic group acting regularly (or sharply transitively) on the points. Geometers call this group the Singer cycle of $PG(n, q)$. After the pioneering work of Singer, more symmetric designs admitting sharply transitive groups (equivalently, more difference sets) have been constructed.

In this article, we describe the parameters of all currently known series of Abelian difference sets and provide constructions for most of them. We also discuss slight generalizations of difference sets (relative difference sets).

Many symmetric designs exist that cannot be constructed via a difference set. Therefore, the question about nonexistence of difference sets has also been investigated. Classical nonexistence results include multiplier arguments and the so-called Mann test (2). This test is based on the prime ideal decomposition of the order of the difference set in an appropriate cyclotomic field. However, this test requires an unfortunate assumption (self-conjugacy). Recently, several authors have tried to overcome this self-conjugacy assumption (3–7). We will survey both the classical nonexistence results as well as this new development.

Difference sets are important in combinatorial design theory and in designing sequences with good correlation properties. In this article, we try to give a flavor of various topics in this general area by including many results-new and old-but there are many results that are not included here. For recent surveys on these topics, we refer the reader to Jungnickel (8,9), Davis and Jedwab (10), Jungnickel and Pott (11). Beth et al. (12), Hall (13), Lander (14), Baumert (15), and Pott (16) serve as good reference books on related topics. In particular, the second edition of the classic book *Design Theory* (12) provides constructions of all known Abelian difference sets. The book also contains the most recent nonexistence results on difference sets without the self-conjugacy assumption.

In this section, we define difference sets, introduce group rings and their characters, and mention some fundamental results that can be used to study difference sets. In the following section, we summarize all the known families of Abelian difference sets. The next section deals with multipliers, a very useful tool in the investigation of existence tests. The section thereafter will be devoted to an important concept known as *self-conjugacy,* a notion introduced by Turyn (17). Relative difference sets are then be discussed. The last two sections deal with sequences having good autocorrelation properties, which can be constructed from difference sets and their generalizations.

Let G be a multiplicatively written group of order v. A subset D of G of size k is said to be a (v, k, λ) difference set in G if each nonidentity element can be expressed in exactly λ ways as $d\,(d')^{-1}$, where $d, d' \in D$. A (v, k, λ) difference set is said to be cyclic (Abelian) if the underlying group G is cyclic (Abelian). We confine ourselves to Abelian groups throughout this article. In this case the group is usually written additively, thus explaining the term *difference set.*

An easy counting shows

$$k(k-1) = \lambda(v-1) \tag{1}$$

for any (v, k, λ) difference set.

There are always trivial examples of difference sets with parameters $(v, 1, 0)$, $(v, 0, 0)$, (v, v, v) and $(v, v-1, v-2)$ in any group of order v. Moreover, difference sets always appear in pairs: If D is a (v, k, λ) difference set in G, then the complement $G \backslash D$ is again a difference set with parameters $(v, v-k, v-2k+\lambda)$. Therefore, we may assume $k \le v/2$ (actually, it is easy to see that $k = v/2$ cannot occur).

The existence of a (v, k, λ) difference set is equivalent to the existence of a symmetric (v, k, λ) design admitting a sharply transitive automorphism group. We refer the reader to Beth et al. (12) for further details.

The investigation of non-Abelian difference sets is a rapidly growing field in discrete mathematics. However, the non-Abelian case seems to be less important for constructing good sequences. Therefore, we restrict ourselves to the case of Abelian difference sets.

An important parameter for a difference set is its order n, which is defined as $n = k - \lambda$. Sometimes, we include the order in the parameter description of a difference set and speak about $(v, k, \lambda; n)$ difference sets.

We now introduce group rings. Let G be a multiplicatively written group of order v, and let R be a commutative ring with unity 1. Then the group ring RG is the free R module with basis G equipped with the following multiplication:

$$\left(\sum_g a_g g\right)\left(\sum_h b_h h\right) = \sum_k \left(\sum_{\substack{g,h \\ gh=k}} a_g b_h\right) k$$

We shall identify the unities of R, G, and RG and denote them by 1. We will use the obvious embedding of R into RG. For any subset S of G, we let S also denote the corresponding group ring element

$$S = \sum_{g \in S} g$$

For $A = \sum_{g \in G} a_g g \in RG$ and any integer t, we define

$$A^{(t)} = \sum_{g \in G} a_g g^t$$

We get the following result.

Lemma 1. Let D be a k-subset of a group G of order v, and let R be a commutative ring with 1. Assume that D is a $(v, k, \lambda; n)$ difference set in G; then the following identity holds in RG (where $n = k - \lambda$):

$$DD^{(-1)} = n + \lambda G$$

The converse also holds provided that R has characteristic 0.

We mostly deal with the case $R = \mathbb{Z}$, the ring of integers, and the group G being Abelian. For each positive integer l, we let ξ_l denote a primitive lth root of unity. A character χ of an Abelian group G is a homomophism from G to $\mathbb{C}^*$, the nonzero complex numbers. If G has exponent e, then χ maps G to the group of vth roots of unity. Each character χ of G can be extended linearly to $\mathbb{Z}G$. This extension χ is a ring homomophism from $\mathbb{Z}G$ to $\mathbb{Z}[\xi_e]$, the ring of algebraic integers in the eth cyclotomic field $Q(\xi_e)$. Let G^* denote the set of all characters of G; then G^* is a group under pointwise multiplication.

We have the following well-known result.

Lemma 2. Inversion formula: Let $A = \sum_{g \in G} a_g g \in \mathbb{Z}G$. Then

$$a_g = \frac{1}{|G|} \sum_{\chi \in G^*} \chi(A)\chi(g^{-1})$$

Hence, if $A, B \in \mathbb{Z}G$ satisfy $\chi(A) = \chi(B)$ for all characters χ of G, then $A = B$.

A symmetric design is an incidence structure consisting of v points and v blocks (which are subsets of points) with the following properties: Any two distinct points lie in exactly λ different blocks and the block size is k. The construction of such a design out of a difference set is easy: The points are the group elements, the blocks are the so-called translates $D + g = \{d + g : d \in D\}$ of D.

Finally we quote a well-known result of Bruck, Ryser, and Chowla (18–20). Their result is more general; it is applicable to any symmetric design. We state it only for (v, k, λ) difference sets.

Theorem 1. (19,20). Let D be a (v, k, λ) difference set in a group G.

1. If v is even, then $n = k - \lambda$ is a square.

2. If v is odd, then there exist integers x, y, and z, not all zero, such that $x^2 = (k - \lambda)y^2 + (-1)^{v-1/2} \lambda z^2$.

Part 1 of Theorem is actually due to Schutzenberger (21)

KNOWN FAMILIES OF DIFFERENCE SETS

In this section we summarize the known series of Abelian difference sets. In some cases, we describe a construction, but in others we give only the parameters. The reader is referred to the chapter on Abelian difference sets in Refs. 12 and 22.

Let us begin with the most classical family, the so-called Singer difference sets.

Family I: Singer Difference Sets. Let α be a generator of the multiplicative group of $\mathbb{F}_{q^{d+1}}$. Then the set of integers $\{i\colon 0 \le i < q^{d+1}_{-1}/q - 1,\ \mathrm{tr}_{(d+1)/i}(\alpha^i) = 0\} \bmod (q^{d+1} - 1)/(q - 1)$ form a (cyclic) difference set with parameters

$$\left(\frac{q^{d+1}-1}{q-1}, \frac{q^{d}-1}{q-1}, \frac{q^{d-1}-1}{q-1}; q^{d-1}\right)$$

Here the trace denotes the usual trace function $\mathrm{tr}_{(d+1/1)}(\beta) = \sum_{i=0}^{d} \beta^{q^i}$ from $\mathbb{F}_{q^{d+1}}$ onto $\mathbb{F}_q$.

In the case $d = 1$, the designs corresponding to these difference sets are the classical Desarguesian planes. The parameters can be rewritten as $(n^2 + n + 1, n + 1, 1; n)$, where n is, in the classical case, a prime power. Difference sets with these parameters are called planar difference sets. Many non-Desarguesian planes are known; however, not a single example of a plane whose order is not a prime power is known. Moreover, not a single example of a planar difference set corresponding to a non-Desarguesian plane is known. Therefore, the following two questions are of central interest in connection with planar difference sets:

Do planar difference sets of nonprime power order exist?

Do planar difference sets exist corresponding to a non-Desarguesian plane?

There are more examples of difference sets with these Singer parameters if $d > 1$. However, only one infinite family is known.

Family II: Gordon–Mills–Welch Difference Sets. Ref. (23). If s divides $d + 1$ and r is relatively prime to $q^s - 1$, then the set of integers $\{i\colon 0 \le i < (q^{d+1} - 1)/q - 1,\ \mathrm{tr}_{s/1}(\alpha^i)^r = 0\}$ is a cyclic difference set with the same parameters as the ones in Family I.

No examples of difference sets with Singer parameters are known when q is not a prime power.

We refer the reader to Pott (16) for more difference sets with the Singer parameters, which are equivalent to neither Singer nor Gordon–Mills–Welch difference sets. (Two difference sets D' and D are called equivalent if a translate $D' + g$ is the image of D under some automorphism of the underlying group.)

The Singer difference sets and the Gordon–Mills–Welch difference sets are basically subsets of the cyclic multiplicative group of a finite field. However, the definition of the sets use the additive structure of the fields. It is also possible to use the multiplicative group of a finite field to define subsets of the additive group which are difference sets. These are the so-called cyclotomic difference sets. The most popular examples are the Paley difference sets [squares in $GF(q)$, $q \equiv 3 \bmod 4$].

The next family comprises difference sets obtained using cyclotomic classes in $\mathbb{F}_q$.

Family III: Cyclotomic Difference Sets. The following subsets of $\mathbb{F}_q$ are difference sets in the additive subgroup of $\mathbb{F}_q$:

- $\mathbb{F}_q^{(2)} = \{x^2\colon x \in \mathbb{F}_q \backslash \{0,\}\}$ $q \equiv 3(\mathrm{mod}\ 4)$ (quadratic residues, Paley difference sets)
- $\mathbb{F}_q^{(4)} = \{x^4\colon x \in \mathbb{F}_q \backslash \{0,\}\}$ $q = 4t^2 + 1$, t odd
- $\mathbb{F}_q^{(4)} \cup \{0\}$, $q = 4t^2 + 9$, t odd
- $\mathbb{F}_q^{(8)} = \{x^8\colon x \in \mathbb{F}_q \backslash \{0\}\}$, $q = 8t^2 + 1 = 64u^2 + 9$, t, u odd
- $\mathbb{F}_q^{(8)} \cup \{0\}$, $q = 8t^2 + 49 = 64u^2 + 441$, t odd, u even
- $H(q) = \{x^i\colon x \in \mathbb{F}_q \backslash \{0\},\ i \equiv 0, 1 \text{ or } 3(\mathrm{mod}\ 6)\}$, $q = 4t^2 + 27$, $q \equiv 1(\mathrm{mod}\ 6)$ (Hall difference sets)

These are cyclotomic difference sets.

The next family is due to Stanton and Sprott (24).

Family IV: Twin Prime Power Difference Sets. Let q and $q + 2$ be prime powers. Then the set $D = \{(x, y)\colon x, y$ are both nonzero squares or both nonsquares or $y = 0\}$ is a twin prime power difference set with parameters

$$\left(q^2 + 2q, \frac{q^2+2q-1}{2}, \frac{q^2+2q-3}{4}; \frac{q^2+2q+1}{4}\right)$$

in the group $(\mathbb{F}_q, +) \oplus (\mathbb{F}_{q+2}, +)$.

We note that the Paley difference sets, the twin prime power difference sets and the Singer difference sets with $q = 2$ have parameters $(4n - 1, 2n - 1, n - 1; n)$. Difference sets with these parameters are sometimes called Paley–Hadamard difference sets.

The next construction is due to McFarland (25). The recent new constructions (Families VIII and IX) of difference sets can be viewed as far-reaching generalizations of McFarland's original work; see, in particular, Davis and Jedwab (29).

Family V: McFarland Difference Set. Let q be a prime power and d a positive integer. Let G be an Abelian group of order $v = q^{d+1}(q^d + \cdots + q^2 + q + 2)$, which contains an elementary Abelian subgroup E of order q^{d+1}. Identify E as the additive group of $\mathbb{F}_q^{d+1}$. Let $r = (q^{d+1} - 1)/(q - 1)$ and $H_1, H_2, \ldots, H_r$ be the hyperplanes of order q^d of E. If $g_0, g_1, \ldots, g_r$ are distinct coset representatives of E in G, then

$$D = (g_1 + H_1) \cup (g_2 + H_2) \cup \cdots \cup (g_r + H_r)$$

is a McFarland difference set with parameters

$$\left(q^{d+1}\left(1 + \frac{q^{d+1}-1}{q-1}\right), q^d\left(\frac{q^{d+1}-1}{q-1}\right), q^d\left(\frac{q^{d}-1}{q-1}\right); q^{2d}\right)$$

Modifying McFarland's construction, Spence (27) obtained the following.

Family VI: Spence Difference Sets. Let E be the elementary Abelian group of order 3^{d+1} and G a group of order $v = 3^{d+1}[(3^{d+1} - 1)/2]$ containing E. Let $m = (3^{d+1} - 1/2$ and $H_1, H_2, \ldots, H_m$ denote the subgroups of E of order 3^d. If $g_1, \ldots, g_m$ are distinct coset representatives of E in G, then

$$D = (g_1 + (E \setminus H_1) \cup (g_2 + H_2) \cup (g_3 + H_3) \cup \cdots \cup (g_m + H_m))$$

is a Spence difference set with parameters

$$\left(3^{d+1}\left(\frac{3^{d+1}-1}{2}\right), 3^d\left(\frac{3^{d+1}+1}{2}\right), 3^d\left(\frac{3^d+1}{2}\right); 3^{2d}\right)$$

We now describe Menon–Hadamard difference sets and their generalizations. Difference sets are called Menon–Hadamard if their parameters can be written in the form $(4u^2, 2u^2 - u, u^2 - u; u^2)$.

Family VII: Menon–Hadamard Difference Set. A difference set with parameters

$$(4u^2, 2u^2 - u, u^2 - u; u^2)$$

is called a Menon–Hadamard difference set.

The following theorem summarizes the known Abelian groups that contain Menon–Hadamard difference sets.

Theorem 2. Let $G \cong H \times EA(w^2)$ be an Abelian group of order $4u^2$ with $u = 2^a 3^b w^2$ where w is the product of not necessarily distinct odd primes p and $EA(w^2)$ denotes the group of order w^2, which is the direct product of groups of prime order. If H is of type $(2^{a_1})\,(2^{a_2}) \cdots (2^{a_s})\,(3^{b_1})^2 \cdots (3^{b_r})^2$ with $\sum a_i = 2a + 2$ $(a \geq 0, a_i \leq a + 2)$, $\sum b_i = 2b$ $(b \geq 0)$, then G contains a Menon–Hadamard difference set of order u^2.

We provide one construction for Family VII; several others are known.

Theorem 3. Let $H = \langle a, b: a^{s+1} = b^{s+1} = 1\rangle$ be an Abelian group of type $(2^{s+1})\,(2^{s+1})$. Let f be a mapping $\mathbb{Z}_{2^{s+1}} \to \{\pm 1\}$ satisfying $f(i + 2^s) = -f(i)$. Define a mapping μ: $\mathbb{Z}_{2^{s+1}} \to \mathbb{Z}_{2^{s+1}}$ by $\mu(2^r i) = 2^r i^*$, where i is odd and $ii^* \equiv 1$ [mod (2^{s+1})]. Then the set $D = \{a^i b^j: f(\mu(i)j) = -1\}$ is a Menon–Hadamard difference set with $u = 2^s$. Let $G = \langle a^2, c: c^2 = b\rangle$ be an Abelian group of type $(2^s)\,(2^{s+2})$. If $A = D \cap \langle a^2\rangle\,\langle b\rangle$ and $B = a^{-1}(D \backslash A)$, then $A \cup cB$ is a Menon–Hadamard difference set with $u = 2^s$ in G.

Theorem 3 is due to Dillon (28). Our next family is contained in the very important "unifying" work of Davis and Jedwab (29).

Family VIII: Davis–Jedwab Difference Sets. A difference set with parameters

$$\left(2^{2d+4}\left(\frac{2^{2d+2}-1}{3}\right), 2^{2d+1}\left(\frac{2^{2d+3}+1}{3}\right) 2^{2d+1}\left(\frac{2^{2d+1}+1}{3}\right); 2^{4d+2}\right)$$

is called a Davis–Jedwab difference set. (Here d is any nonnegative integer).

These difference sets exist in all Abelian groups of order $2^{2d+4}\,[(2^{2d+2} - 1)/3]$ that have a Sylow 2-subgroup S_2 of exponent at most 4, with the single exception $d = 1$ and $S_2 \cong \mathbb{Z}_4^3$.

The most recent family due to Chen (30) is as follows.

Family IX: Chen Difference Sets. A difference set with parameters

$$\left(4q^{2d+2}\left(\frac{q^{2d+2}-1}{q^2-1}\right), q^{2d+1}\left(\frac{2(q^{2d+2}-1)}{q+1}+1\right) q^{2d+1}(q-1)\left(\frac{q^{2d+1}+1}{q+1}\right); q^{4d+2}\right)$$

is called a Chen difference set. (Here d is a nonnegative integer and q a prime power.) The Chen family with $d = 0$ corresponds to the Menon–Hadamard family; the Chen family with $q = 2$ corresponds to the Davis–Jedwab family; and the Chen family with $q = 3$ corresponds to the Spence family. We distinguish these series for historical reasons.

Looking at the families mentioned previously we have two major questions. The first question is about nonexistence. What happens, for instance, if we replace the prime power q or the values of u in the Menon–Hadamard series by some other integer? Can we prove that for these different parameters no difference set can exist? More specifically, the following two questions have attracted a lot of attention:

Prime-Power Conjecture (PPC). Determine the parameters n for which an $(n^2 + n + 1, n + 1, 1; n)$ difference set can exist. The Singer examples with $d = 2$ show that examples exist whenever n is a prime power.

Menon–Hadamard Conjecture (MHC). Determine the possible values for u such that a Menon–Hadamard difference set of order u^2 exists. Is it true that u must be of the form in Theorem 2?

Similar questions can be asked about the Davis–Jedwab–Chen difference sets.

Another question addresses the groups that might carry difference sets. Although we know that difference sets with the parameters mentioned previously in the series do exist, it is not at all clear which Abelian groups contain these sets. In the description of our families, we have always described the groups for which it is known that they contain difference sets. In general, it is not at all clear whether other groups are also possible. Several partial nonexistence results in this direction are known for all the series mentioned previously. One of the most satisfying theorems in this direction is the following.

Theorem 4 (31). Let G be an Abelian group of order 2^{2d+2}. Then G contains a Menon–Hadamard difference set if and only if G satisfies Turyn's exponent bound $\exp(G) \leq 2^{d+2}$.

Finally, it would be interesting to obtain classification results saying that the only difference sets with certain parameters are the known ones. For instance, the only known planar difference sets correspond to the classical Desarguesian planes. A classification result would say that this must be the case.

MULTIPLIERS

Let D be a (v, k, λ) difference set in a group G. An automorphism α of G is said to be a multiplier of D if $\alpha(D) = Dg$ for some $g \in G$. If G is Abelian and if α is given by multiplication by an integer t relatively prime to the order of G, we say that t is a numerical multiplier, or simply, multiplier of D. The parameters of a hypothetical Abelian difference set D would sometimes imply the existence of numerical multipliers, which could then be used to investigate the existence of D. These ideas are due to Hall (32), who considered these for the case $\lambda = 1$. An easy extension of Hall's result obtained by Chowla and Ryser (20) is given in the following.

Theorem 5 (First Multiplier Theorem). Let D be an Abelian (v, k, λ) difference set. Let p be a prime dividing $n = k - \lambda$, but not v. If $p > \lambda$, then p is a multiplier of D.

To use the multipliers, we also need a result of McFarland and Rice (33).

Theorem 6. Let D be an Abelian (v, k, λ) difference set in G. Then there exists a translate of D that is fixed by every numerical multiplier of D.

Example 2. Consider a (21, 5, 1) difference set in $\mathbb{Z}_{21}$. Here 2 is a multiplier by Theorem 5. We may assume D consists of orbits of $\mathbb{Z}_{21}$ under $x \to 2x$, by Theorem 6. Since $k = 5$, D must be formed from the orbits {0}, {7, 14}, {3, 6, 12}, {9, 18, 15}. D_1 = {7, 14, 3, 6, 12} and D_2 = {7, 14, 9, 18, 15} both work.

Similarly, we can obtain {0, 1, 3, 9} as a (13, 4, 1) difference set in $\mathbb{Z}_{13}$, and {1, 2, 4, 8, 16, 32, 64, 5, 37} as a (73, 9, 1) difference set in $\mathbb{Z}_{73}$.

Example 2. Consider a hypothetical (31, 10, 3) difference set D in $\mathbb{Z}_{31}$. 7 is a multiplier of D by Theorem 5. But the orbits of $\mathbb{Z}_{31}$ under $x \to 7x$ have sizes 1, 15, 15. Hence D cannot exist.

The Multiplier Conjecture. Theorem 4 holds without the assumption that $p > \lambda$. All known multiplier theorems may be viewed as an attempt to eliminate conditions such as $p > \lambda$.

Theorem 7 (Second Multiplier Theorem) (34). Let D be an Abelian (v, k, λ)-difference set in G, and let $m > \lambda$ be a divisor of n that is co-prime with v. Moreover, let t be an integer co-prime with v satisfying the following condition: For every prime p dividing m there exists a nonnegative integer f with $t \equiv p^f \pmod{v^*}$, where v^* denotes the exponent of G. Then t is a numerical multiplier for D.

We next state another multiplier theorem due to McFarland (35). We first define a function M as follows:

$$M(2) = 2 \times 7, \quad M(3) = 2 \times 3 \times 11 \times 13$$
$$M(4) = 2 \times 3 \times 7 \times 31$$

recursively, $M(z)$ for $z \geq 5$ is defined as the product of the distinct prime factors of the numbers

$$z, M\left(\frac{z^2}{p^{2e}}\right), p-1, p^2-1, \ldots, p^{u(z)}-1$$

where p is a prime dividing m with $p^e \parallel m$ and where $u(z) = (z^2 - z)/2$. (The notation $p^a \parallel m$ means that $p^a \mid m$ but $p^{a+1} \nmid m$; we then say that p^a strictly divides m.)

Theorem 8. Theorem 7 remains true if the assumption $m > \lambda$ is replaced by $M(n/m)$ and v are co-prime.

NONEXISTENCE RESULTS VIA SELF-CONJUGACY

Multipliers provide nonexistence results, as we saw earlier. But most of the multiplier theorems for $(v, k, \lambda; n)$ difference sets have been proved when $(v, n) = 1$. An extension of known multiplier theorems to cover a few cases with $(v, n) > 1$ can be found in Arasu and Xiang (36), but these results are difficult to apply. Almost all results on difference sets with $(v, n) > 1$ pertain to exponent bounds and rely on character theoretic ideas introduced by Turyn (17) in his seminal paper. The notion of self-conjugacy is introduced by Turyn. A prime p is said to be self-conjugate modulo a positive integer m, if there exists an integer j, such that

$$p^j \equiv -1 \pmod{m'}$$

where m' is the p-free part of m. In the study of Abelian difference sets, we say that the self-conjugacy assumption is satisfied if every prime divisor of $n = k - \lambda$ is self-conjugate modulo $\exp(G)$.

The self-conjugacy assumption can be better understood via Abelian characters. For a $(v, k, \lambda; n)$ difference set D, viewing D as an element of the group ring $\mathbb{Z}G$ we obtain

$$\chi(D)\overline{\chi(D)} = n \tag{2}$$

for all nonprincipal characters χ of G. We note that $\chi(D)$ is an algebraic integer in a suitable cyclotomic field.

This idea of studying difference sets using character sums is due to Turyn (17). If n is self-conjugate modulo $\exp(G)$, then it can be shown: Equation (2) implies that n is a square, say $n = u^2$, and $\chi(D) = u\xi$, where ξ is a root of unity. Such solutions are called trivial solutions. Thus $\chi(D)$ is determined completely from Eq. (2) under the self-conjugacy assumption. This would then impose necessary conditions on the existence of D.

In the absence of self-conjugacy $\chi(D)$ cannot be easily determined from Eq. (2). This difficulty is the primary reason why McFarland's investigation (37) of Abelian Hadamard difference sets in groups of order $4p^2$, p a prime, was rather tedious and quite involved in the $p \equiv 1 \pmod 4$ case (where self-conjugacy is absent), whereas the case $p \equiv 3 \pmod 4$ in which self-conjugacy was present was easily disposed of (38).

Chan (39) introduced a new approach to deal with the situation without self-conjugacy. In some special situations, Chan showed that Eq. (2) has only the trivial solutions, even when there was no self-conjugacy. Using that, he was able to obtain further restrictions on Abelian groups of the form $\mathbb{Z}_{2pq} \times \mathbb{Z}_{2pq}$, where p, q are distinct primes, that contain Hadamard difference sets. In particular, he showed that Abelian Hadamard difference set in $\mathbb{Z}_{6p} \times \mathbb{Z}_{6p}$ can exist only if $p = 3$ or $p = 13$. Several useful theorems for studying difference sets without self-conjugacy can be found in Ma's work (40) on relative $(n, n, n, 1)$ difference sets.

We have seen that the existence of a difference set D yields the existence of an algebraic integer of a certain absolute value. This gives number theoretic conditions that are the basis for most nonexistence results on difference sets. In this section, we cannot survey even the most important nonexistence results, but we hope that the reader gets an impression how algebraic number theory can be used to obtain necessary conditions for the existence of difference sets.

To start with, let us look at the condition

$$\chi(D)\overline{\chi(D)} = n$$

more closely. If χ is a character of order ω, then this equation holds in $Z[\zeta_\omega]$, the ring of algebraic integers in $Q(\zeta_\omega)$; here $\zeta_\omega = e^{2\pi i/\omega}$ is a primitive ωth root of unity. The ring $Z[\zeta_\omega]$ is a Dedekind domain, that is, we can decompose the ideals $\chi(D)$, $\overline{(\chi(D))}$, and (n) uniquely into prime ideals and obtain

$$\chi(D)\overline{\chi(D)} = \prod_{i=1}^{m} P_i^{e_i}$$

where the P_is are distinct prime ideals. The prime ideal decomposition of n in $Z[\zeta_\omega]$ as well as the action of Galois automorphisms of $Q(\zeta_\omega)$ on these ideals is known:

Result 1. Let p be a prime and ζ_ω a primitive complex ωth root of unity; write $\omega = p^e w'$ where ω' is an integer relatively prime to p. The multiplicative order of p modulo ω' is denoted by f. Let $\Phi(x)$ be the number of positive integers $< x$ that are relatively prime to x. Then the following identity for ideals holds in $Z[\zeta_\omega]$:

$$(p) = (P_1 \cdots P_g)^{\Phi(p^e)}$$

where the P_i's are distinct prime ideals and $g = \Phi(\omega')/f$. If t is an integer relatively prime to p such that $t \equiv p^s \bmod \omega'$, then the Galois automorphism $\zeta_\omega \mapsto \zeta_\omega^t$ fixes the ideals P_i. If $\omega' = 1$ then $g = 1$ and $P_1 = (1 - \zeta_\omega)$.

Result 1 shows that the self-conjugacy of a prime p modulo w implies that all prime ideal divisors of p in $\mathbb{Z}[\zeta_\omega]$ are fixed by complex conjugation. This is basically the content of the so called Mann-test.

Corollary 1. Let p be self-conjugate modulo w, and let D be a difference set of order n in a group G whose exponent is divisible by w. Then p cannot divide the square-free part of n, that is, p^{2a} is the exact p power dividing n. In particular, for each character χ of order w, we have $\chi(D) \equiv \bmod p^a$.

As an example, there are no Abelian (25, 9, 3; 6) difference sets: We take $w = 5$ and $p = 3$, then $p^2 \equiv -1 \bmod w$ and hence the Galois automorphism $\zeta_5 \mapsto \zeta_5^9 = \overline{\zeta_5}$ fixes the ideal divisors of (3) in $Z[\zeta_5]$.

Note that the proof of this corollary just uses the prime ideal factorization of (p) in $Z[\zeta_\omega]$. To obtain stronger results, we must exploit the condition $\chi(D) \equiv 0 \bmod p^a$ more carefully. In this context, the following lemma is useful (41).

Lemma 3. Let p be a prime and let G be an Abelian group with a cyclic Sylow p-subgroup of order p^s. If $Y \in Z[G]$ is an element such that $\chi(Y) \equiv 0 \bmod p^a$ for all characters, then we can write

$$Y = p^a X_0 + p^{a-1} P_1 X_1 + \cdots + p^{a-r} P_r X_r$$

$r = \min(a, s)$, where P_i denotes the unique subgroup of order p^i. Moreover, if the coefficients of Y are nonnegative, the coefficients of the X_i can be chosen to be nonnegative, too.

Here is an application: Let D be an Abelian $(4u^2, 2u^2 - u, u^2 - u)$ difference set. Let $u = 2^a$ and assume that G contains a cyclic subgroup of order 2^b. Projection onto this subgroup yields a group ring element Y with $\chi(Y) \equiv 0 \bmod 2^a$ for all characters. The lemma shows that the coefficients of Y are constant modulo 2^a on cosets of subgroup P_1 of order 2. On the other hand, the coefficients are bounded by 2^{2a+2-b}. Since Y cannot be constant on cosets of N, we get $2a + 2 - b \geq a$. This bound is part of Turyn's famous exponent bound for Hadamard difference sets (17).

Another illustration is that there are no Abelian Hadamard difference sets of order p^2 in groups of order $4p^2$ if $p \equiv 3 \bmod 4$ or if the Sylow 2-subgroup is elementary abelian. Note that p is self-conjugate modulo the exponent of G; hence $\chi(D) \equiv 0 \bmod p$ for a putative difference set D. Projection onto the homomorphic image of order $4p$ yields a contradiction similar to the argument above. This (easy) proof is in remarkable contrast to the case $p \equiv 1 \bmod 4$: The nonexistence for those difference sets have been ruled out by McFarland (37) in a long, detailed paper as mentioned earlier. It is one of the first nonexistence results without using self-conjugacy.

Many more nonexistence results are variations of the approach that we have just described: Project the difference sets D in $Z[G]$ onto a group ring $Z[H]$ where H contains a cyclic Sylow p-subgroup and where p is self-conjugate modulo the exponent of H. However, in many situations (such as, for instance, for McFarland difference sets), this approach is only of limited use. The point is that elements in $Z[H]$ with the "correct" character values and "correct" coefficient sizes do exist. In other words, there are elements that "look like" images of difference sets (although the difference set might not exist). But, in general, there are many different subgroups N such that $G/N \cong H$, and the approach described earlier yields information about the image of a putative difference sets under all these projections. Several authors, notably Ma and Schmidt (3), developed some combinatorial group-theoretic tools in order to exploit the information about these different images simultaneously. This method has been applied successfully both to relative and McFarland difference sets.

Recently, two new approaches to prove nonexistence results without any self-conjugacy assumptions have been devised. Schmidt focused his attention on cyclic Hadamard difference sets and Eq. (2). He proved the following.

Result 2. Let Q be a finite set of primes. Then there are (at most) finitely many elements $(a_q)_{q\in Q} \in N^{|Q|}$ such that a cyclic Hadamard difference set of order $\prod_{q\in Q} q^{2a_q}$ exists.

A slightly different idea to overcome the self-conjugacy assumption is given by Ma (40). His idea is to get as much information as possible about elements D satisfying Eq. (2). He applies his technique to relative difference sets; in particular he obtains the following strong result on planar functions (we discuss relative difference sets and planar functions later):

Result 3. Given two primes p and q, there are no planar functions on cyclic groups of order pq.

The special case that p is self-conjugate modulo q is comparatively easy.

Arasu and Ma (42) used similar methods to investigate McFarland difference sets without the self-conjugacy assumption.

Schmidt (43) introduces further techniques to deal with difference sets without self-conjugacy. He uses properties of the decomposition group of the prime ideal divisors of the order of the difference set, coupled with ideas similar to those of McFarland (37, Sec. 4), to find restrictions on the solutions of Eq. (2). An example of such a result is given in the following special case.

Theorem 9. Let $d = p^a m$, where p is an odd prime and $d > 0$ is an odd integer relatively prime to p. If $X \in \mathbb{Z}[\zeta_d]$ satisfies

$$X\overline{X} = p$$

then with suitable j either $\zeta_d^j X \in \mathbb{Z}[\zeta_m]$ or $X = \pm\zeta_d^j Y$, where Y is a generalized Gauss sum (44).

With the aid of Theorem 9 it is often possible to find all the solutions of Eq. (2). These solutions can then be further examined to obtain necessary conditions on the existence of an Abelian difference set.

RELATIVE DIFFERENCE SETS

Relative difference sets are a generalization of difference sets. Relative difference sets provide constructions of Hadamard matrices and generalized Hadamard matrices that are of interest in various branches of mathematics. It turns out that group-invariant Hadamard matrices (equivalently Hadamard difference sets) are basically the same objects as certain relative difference sets. Similar to ordinary difference sets, relative differences sets yield sequences with interesting autocorrelation properties (45). Certain types of relative difference sets give rise to perfect ternary sequences (46).

Relative difference sets were introduced by Bose (47), although he did not use the term *relative difference sets.* The term *relative difference sets* was coined by Butson (48). Systematic investigations of these are due to Elliott and Butson (49) and Lam (50). A recent survey of these objects can be found in Pott (51). The interplay of relative difference sets, finite geometry, and character theory is the subject matter of the monograph by Pott (16).

A relative (m, n, k, λ) difference set R in a group of G of order mn relative to a normal subgroup N of order n is a k-subset of G with the following properties: the list of quotients $r(r')^{-1}$ with distinct elements $r, r' \in R$ contains each element of $G \backslash N$ exactly λ times. Moreover, no element in N has such a representation. N will be referred to as the forbidden subgroup. Note that each coset of N contains at most one element from R. (The more general divisible difference sets are subsets of G where the number of representations of elements in N is not necessarily 0, but another constant μ.) Easy counting yields

$$k(k-1) = \lambda n(m-1)$$

The obvious inequality $k \leq m$ follows, for otherwise at least one coset of N would contain more than just one element from R.

If $n = 1$, the relative difference sets become ordinary difference sets. A relative difference set is called Abelian, cyclic, etc., if the underlying group G has the respective property. All our results and examples would concern Abelian relative difference sets. A relative difference set R is said to be splitting if $G \cong H \times N$ for some subgroup H (i.e., the forbidden subgroup N must be a direct factor of G).

Example 3. The set of $\{0, 1, 3\}$ is a $(4, 2, 3, 1)$ relative difference set in $\mathbb{Z}_8$ relative to $N = \{0, 4\}$.

Example 4. The set $\{(0, 0), (1, 1), (2, 1)\}$ is a $(3, 3, 3, 1)$ relative set in $\mathbb{Z}_3 \times \mathbb{Z}_3$ relative to $N = \{0\} \times \mathbb{Z}_3$.

A relative difference set is said to be semiregular if $k = n\lambda$; otherwise it is called regular.

The following result on the parameters m, n, k, and λ of relative difference sets follows from the work of Bose and Connor (52). The symbol $(a, b)_p$ is the Hilbert symbol, which takes values $+1$ or -1 according to whether the congruence $ax^2 + by^2 \equiv 1 \pmod{p^r}$ has or has not for every value of r, rational solutions x_r and y_r.

Result 4. Let D be a regular (m, n, k, λ) relative difference set. Then the following holds:

1. If m is even, then $k - n\lambda$ is a square. If moreover $m \equiv 2 \pmod 4$ and n is even, then k is the sum of two squares.
2. If m is odd and n is even, then k is a square and

$$(k - n\lambda, (-1)^{(m-1)/2} n\lambda)_p = 1$$

for all odd primes p.

3. If both m and n are odd, then

$$(k, (-1)^{(n-1)/2} n)_p (k - n\lambda, (-1)^{(m-1/2} n\lambda)_p = 1$$

for all odd primes p.

Using the group ring notation we introduced earlier, the definition of relative (m, n, k, λ) difference sets R can be translated into a group ring equation in $\mathbb{Z}_G$:

$$RR^{(-1)} = n + \lambda(G - N) \tag{3}$$

If U is a normal subgroup of G contained in N, we consider the canonical epimorphism from G into G/U. Extending this epimorphism by linearity from $\mathbb{Z}G$ to $\mathbb{Z}[G/U]$ and applying to Eq. (3), we obtain the following.

Lemma 4. Let R be a relative (m, n, k, λ) difference set in G. If U is a normal subgroup of G contained in N, then there exists an $(m, n/u, k, \lambda_u)$ difference set in G/U relative to N/U. In particular, G/N contains an $(m, k, \lambda n)$ difference set.

KNOWN FAMILIES OF RELATIVE DIFFERENCE SETS

Extension of (*m*, *m*, *m*) Difference Sets

There exists a $(p^a, p^a, p^a, 1)$ relative difference set in $(\mathbb{Z}_p)^{2a}$ if p is an odd prime; in $(\mathbb{Z}_4)^a$ relative to $(\mathbb{Z}_2)^a$ if $p = 2$. This gives the following series of relative difference sets which are extensions of (m, m, m) difference sets.

Family I. Relative (p^a, p^b, p^a, p^{a-b}) relative difference sets exist whenever p is a prime.

Splitting relative difference sets with parameters $(n, n, n, 1)$ in $H \times N$ are equivalent to the so-called planar functions $f: H \to N$; see Dembowski and Ostrom (53). The existence of a planar function implies the existence of a projective plane with a certain automorphism group (semiregular automorphism group). In contrast to the case of planar difference sets, planar functions describing non-Desarguesian planes are known. However, in all known cases H and N are elementary Abelian (provided n is odd). It is one of the open problems concerning planar functions, whether this has to be the case. Finally, we mention that the case of even n has been settled completely (at least in the Abelian case): In this case, n has to be a power of 2 and the group has to be as mentioned before.

Menon–Hadamard difference sets of order u^2 give rise to the following two series of relative difference sets.

Family II. Relative $(4u^2, 2, 4u^2, 2u^2)$ difference sets exist whenever difference sets with parameters $(4u^2, 2u^2 \pm u, u^2 \pm u)$ exist. These are known to exist if $u = 2^a3^bm^2$, where m is any odd integer (see Theorem 2).

Family III. Relative $(8u^2, 2, 8u^2, 4u^2)$ difference sets exist whenever difference sets with parameters $(4u^2, 2u^2 \pm u, u^2 \pm u)$ exist.

Note: Family III contains only nonsplitting examples, because otherwise a group of order $8u^2$ would contain a Hadamard difference set, which is impossible. New examples of semiregular relative difference sets in groups whose order can contain more than two distinct prime factors are explored by Davis, Jedwab, and Mowbray (54) and Arasu and deLauney (55).

Extensions of $(m, m-1, m-2)$ Difference Sets

Any Desarguesian projective plane of order q gives rise to a cyclic relative $(q + 1, q - 1, q, 1)$ difference set. Thus we get:

Family IV. For any prime power q and any divisor d of $q - 1$, relative $(q + 1, (q - 1)/d, q, d)$ difference sets exist.

Note: Relative difference sets of Family IV will be considered later.

Extension of $((q^{d+1} - 1)/(q - 1), q^d, q^d - q^{d-1})$ Difference Sets

Complements of the Singer difference sets are difference sets with parameters

$$\left(\frac{q^{d+1}-1}{q-1}, q^d, q^d - q^{d-1}\right)$$

As observed by Bose (47), the above difference sets lift to cyclic relative difference sets, given in the following.

Family V. If q is a prime power, relative difference sets with parameters

$$\left(\frac{q^{d+1}-1}{q-1}, \frac{q-1}{t}, q^d, q^{d-1}t\right)$$

exist for each divisor t of $q - 1$.

Note: The case $d = 2$ reduces to Family IV. We have decided to separate these since geometers usually distinguish the planar case (dimension 2) and the general case. If q is even, Family V does not include relative difference sets if the forbidden subgroup has order 2. Arasu et al. (56) later obtained in the following:

Family VI. If q is a power of 2, and d is even, relative difference sets with parameters

$$\left(\frac{q^{d+1}-1}{q-1}, 2, q^d, \frac{q^d - q^{d-1}}{2}\right)$$

exist.

Arasu, Leung, and Ma (57) obtain the following.

Family VII. If q is a power of 2, relative difference sets with parameters

$$\left(q^2 + q + 1, 2(q-1)q^2, \frac{q}{2}\right)$$

exist. A few further sporadic examples obtained using a computer search led Arasu, Leung, and Ma (57) to the following.

Conjecture. Cyclic $((q^{d+1} - 1)/q - 1, 2(q - 1), q^d, (q^d - q^{d-1})/2(q - 1))$ relative difference sets exist if q is a power of 2 and d is a positive odd integer.

Remark. In a forthcoming paper (in preparation), Arasu, Dillon, Leung, and Ma have proved this conjecture.

DIFFERENCE SETS AND PERFECT SEQUENCES

We summarize a few results that relate difference sets and their generalization such as relative/divisible difference sets to perfect and almost perfect sequences. For recent results on this topic, we refer the reader to Jungnickel and Pott (58).

A sequence $(a_i)_{i=0,1,2,...}$ is said to be periodic with period v if $a_i = a_{i+v}$ for all i. A sequence all of whose entries are either $+1$ or -1 is called binary. The (periodic) autocorrelation function C of $(a_i)_{i=0,1,2,...}$ is defined by

$$C(t) = \sum_{i=0}^{v-1} a_i a_{i+t}$$

Since $(C(t))_{t=0,1,2,...}$ is also periodic (if (a_i) is periodic), it suffices to consider the autocorrelation coefficients $C(t)$ for $t = 0, 1, \ldots, (v - 1)$. The autocorrelation function measures how much the original sequence differs from its translates. In the binary case, $C(t)$ is the number of agreements of $(a_i)_{i=0,1,...}$ with its translate by a shift of t minus the number of disagreements. Obviously $C(0) = v$. The other autocorrelation coefficients $C(t)$, with $t \neq 0$, are called nontrivial or the off-peak autocorrelation coefficients. We let k denote the number of $+1$ entries in one period of a periodic binary sequence under consideration.

Periodic sequences with good autocorrelation properties are applicable in engineering. The following is easy to prove.

Lemma 5. A periodic binary sequence with period v, k entries $+1$ per period, and a two level autocorrelation function (with all nontrivial autocorrelation coefficients equal to γ) is equivalent to a cyclic $(v, k, \lambda; n)$ difference set, where $\gamma = v - 4(k - \lambda) = v - 4n$. A ±1-sequence (a_i) of period v is said to be perfect if it has a two-level autocorrelation function, where the off-peak autocorrelation coefficients α are as small in magnitude as possible.

By Lemma 5, sequences with two-level autocorrelation functions correspond to cyclic difference sets. As shown by Jungnickel and Pott (58), the cases $\gamma = 0, \pm 1, \pm 2$ give rise to the following classes of cyclic (v, k, λ) difference sets of order $n = k - \lambda$:

Class I. $(v, v - \sqrt{v}/2, v - 2\sqrt{v}/4)$ of order $v/4$ corresponding to $\gamma = 0$

Class II. $(v, (v - 2\sqrt{v-1})2, (v + 1 - 2\sqrt{2v-1})4)$ of order $(v - 1/4)$ corresponding to $\gamma = 1$

Class III(a). $(v, (v - \sqrt{2-v})2, (v - 2 - 2\sqrt{2-v})4)$ of order $(v + 2)4$ corresponding to $\gamma = -2$

Class III(b). $(v, (v - \sqrt{3v-2})2, (v + 2 - 2\sqrt{3v-2})4)$ of order $(v - 2)4)$ corresponding to $\gamma = -2$

Class IV. $(v, (v - 1)2, (v - 3)4)$ of order $(v + 1)/4$ corresponding to $\gamma = -1$

Lemma 5 shows that the autocorrelation coefficients are always congruent 4 modulo v. Therefore, in order to determine in absolute value the smallest coefficients, we have to distinguish v modulo 4. This yields the four series I–IV: However, in the case v congruent 2 modulo 4, it is possible that the off-peak autocorrelation coefficient is 2 or -2 [which explains the two classes III(a) and III(b)]. Class III(a) provides only the trivial (2, 1, 0) difference set, corresponding to $\gamma = 2$.

Difference sets in Class I are Hadamard difference sets (Family VII) with parameters $(4u^2, 2u^2 - u, u^2 - u)$. The only known cyclic example of such a difference set is the trivial (4, 1, 0) difference set. It is conjectured that there cannot be any others. Turyn (17) ruled out the existence of cyclic Hadamard difference sets of size $4u^2$, for $1 < u < 55$. Schmidt's recent work (5), establishes the following results:

Theorem 10. Assume the existence of a cyclic Hadamard difference set of order $u^2 = \prod_{i=1}^{s} q_i^{\alpha_i}$ where the q_is are distinct odd primes (note that u must be odd). Let

$$b_j = \min\{b : q_i^{\omega_i} \not\equiv \bmod q_j^b \text{ for all } i \neq j\}$$

where ω_i is the multiplicative order of q_i modulo $\prod_{j \neq i} q_j$. For $j = 1, \ldots, s$, define $c_j = \min\{2a_j, b_j - 1\}$. Moreover, let $u' = \prod_{j=1}^{s} q_j^{c_j}$. Then

$$u \leq \sqrt{2}[\sin(\pi/2u')]^{-1}$$

Corollary 2. Let Q be any finite set of odd primes. Then there are only finitely many cyclic Hadamard difference sets of order u^2, where all prime divisors of u are in Q.

Remark: Corollary 2 is already contained in Result 2.

Corollary 3. Cyclic Hadamard difference sets of order $1 < u \leq 2000$ with $u \notin \{165, 231, 1155\}$ do not exist.

The only known Abelian example of difference as in Series II is the (13, 4, 1) difference set. Parameters in series II can be rewritten as $(2u^2 + 2u + 1, u^2, u(u - 1)/2)$. Results by Broughton (59) and Eliahou and Kervaire (60) imply the following.

Result 5. For $3 \leq u \leq 100$, no Abelian difference sets with parameters

$$(2u^2 + 2u + 1, u^2, u(u-1)/2)$$

exist. Hence perfect sequences of Class II and period v do not exist for $13 < v \leq 20201$.

Difference sets with parameters in Class III(b) require $3v - 2$ and $v - 2$ both to be squares. This series contains the trivial (6, 1, 0) difference set. The next two candidates (66, 26, 10) and (902, 425, 200) are both ruled by Theorem 4.18 of Lander (14). The next permissible value of v is 12546. Thus we obtain the following.

Theorem 11. Perfect sequences of Class III(b) and period v do not exist for $6 < v \leq 12545$.

Difference sets of Class IV are called Paley–Hadamard difference sets. Known examples (parametrically) are given by Singer difference sets (Family I, with $q = 2$), the Paley difference sets of Family V, and the examples given in Family VI.

Song and Golomb (61) and Golomb and Song (62) systematically investigate cyclic Paley–Hadamard difference sets. It is conjectured that every such difference set has parameters as in one of the three series earlier above. Golomb and Song (62) prove the following.

Result 6. Assume the existence of a Paley–Hadamard difference set D in a cyclic group of order v, where $v < 10{,}000$. Then v is either of the form $2^m - 1$, or a prime $\equiv 3 \bmod 4$, or the product of two twin primes, with the possible exceptions of $v = 1295, 1599, 1935, 3135, 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423$.

Corollary 4. A perfect sequence of Class IV and period $v < 10{,}000$ exists if and only if v is either of the form $2^m - 1$ or a prime $\equiv 3 \bmod 4$, or the product of two twin primes, with the possible exceptions given in Result 6.

A concrete application of the perfect sequences corresponding to the twin-prime power difference sets to applied optics is explained in Jungnickel and Pott (58).

ALMOST PERFECT SEQUENCES AND DIVISIBLE DIFFERENCE SETS

As we saw in earlier, perfect ± 1-sequences with off-peak autocorrelation value 0 are quite rare. To remedy this situation, one studies the so-called almost perfect sequences (a concept due to Wolfmann (63) in an attempt to obtain further classes of sequences with good correlation properties.

An almost perfect sequence is a ± 1-sequence in which all the off-peak autocorrelation coefficients are as small as possible—with exactly one exception, say $C(g)$. Since $C(g)$ is the only exceptional autocorrelation coefficient, it follows that $g = -g$, forcing the period v to be even and $g = v/2$. The subset of $\mathbb{Z}_v$ that corresponds to an almost perfect sequence is a divisible difference set.

A k-element subset D of a group G of order v relative to a subgroup N of G of order u is called *a* $(v/u, u, k, \lambda_1, \lambda_2)$ divisible difference set if the list of all differences

$$(d_1 - d_2 : d_1, d_2 \in D, d_1 \neq d_2)$$

contains every element of $N\backslash\{0\}$ exactly λ_1 times and every element of $G\backslash N$ exactly λ_2 times. If $\lambda_1 = 0$, these reduce to relative difference sets of presented earlier.

Using group ring notations, D is a $(v/u, u, k, \lambda_1, \lambda_2)$ divisible difference set in G relative to N if and only if

$$DD^{(-1)} = (k - \lambda_1) + \lambda_1 N + \lambda_2(G - N) \text{ in } \mathbb{Z}G$$

Bradley and Pott (64) show: almost perfect sequences are equivalent to cyclic divisible difference sets with $u = 2$, of certain types. Let f be the exceptional correlation coefficient $C(v/2)$. Since v is even, we obtain three possible series of almost perfect sequences corresponding to the Classes I, III(a), and III(b) described earlier. Class I:

$$\text{Class I: } v \equiv 0 \bmod 4 : \left(\frac{v}{2}, 2, \frac{v}{2} - \theta, \frac{f+v}{4} - \theta, \frac{v}{4} - \theta\right)$$
$$\text{where } \theta = \sqrt{v+f}/2$$

Class III:

$$v \equiv 2 \bmod 4$$

Class III(a), off-peak autocorrelation 2:

$$\left(\frac{v}{2}, 2, \frac{v}{2} - \theta, \frac{f+v}{4} - \theta, \frac{v-2}{4} - \theta\right), \text{ where } \theta = \tfrac{1}{2}\sqrt{-v+f+4}$$

Class III(b); off-peak autocorrelation -2:

$$\left(\frac{v}{2}, 2, \frac{v}{2} - \theta, \frac{f+v}{4} - \theta, \frac{v+2}{4} - \theta\right), \text{ where } \theta = \tfrac{1}{2}\sqrt{3v+f-4}$$

Let us first consider the Class I. Only the cases $\theta = 0$, 1, and 2 have been investigated systematically so far. For the case $\theta = 0$, we use the following result of Jungnickel (65).

Result 7. If there exists a cyclic $(v/2, 2, v/2, 0, v/4)$ difference set, then $v = 4$.

Hence, we obtain

Theorem 12. If there exists an almost perfect sequence of type I and $\theta = 0$, then $v = 4$.

In case $\theta = 1$ of type I, an infinite family of almost perfect sequences exists: Let D consist of these elements d in the multiplicative group G of $GF(q^2)$, satisfying $\mathrm{tr}(d + d^q) = 1$. Then D is a cyclic relative difference set in G with parameters $(q + 1, q - 1, q, 1)$. Such relative difference are called affine difference sets (9). Projection yields a cyclic relative difference set with parameters

$$\left(q+1, 2, q, \frac{q-1}{2}\right)$$

if q is odd.

Hence we obtain the following.

Theorem 13. If $v = 2(q + 1)$, where q is a power of an odd prime, then almost perfect sequences of class I with period v and $\theta = 1$ exist.

It is widely conjectured that $(m + 1, 2, m, (m - 1)/2)$ relative difference sets exist only if m is a prime power. This has been verified for m up to 425 by Reuschling (66). Tools required to establish their nonexistence are listed in the following:

Result 8 (16,36). The following integers are multipliers of any cyclic relative difference sets with parameters $(m + 1, 2, m, (m - 1)/2)$:

- m
- If $m = p^k$ is a power of prime p, then p is a multiplier
- If $m = p^i q^j$ is the product of powers of two distinct primes p and q, then p^i and q^j are multipliers

Result 9 (67). Let G be an Abelian group of order $2(m + 1)$. Let t be a multiplier of a putative $(m + 1, 2, m, (m - 1)/2)$ difference set relative to N. If $G\backslash N$ contains elements x and y with $x^t = x$ and $y^q = (m + 1)y$, then G cannot contain a difference set with these parameters.

Result 10 (Mann Test). Let D be a divisible $(v/u, u, k, \lambda_1, \lambda_2)$ difference set in the Abelian group G relative to N. Moreover, let t be a multiplier of D, and let U be a subgroup of G such that G/U has exponent w $(U \neq G)$. Let p be a prime not dividing w such that $tp^f \equiv -1 \bmod w$. Then the following holds:

- If N is not contained in U, then p does not divide the square-free part of $k - \lambda_1$
- If N is contained in U, then p does not divide the square-free part of $k^2 - mn\lambda_2$

Using these tests for $m \leq 1000$ (m odd), nonexistence of cyclic $(m + 1, 2, m, (m - 1)/2)$ relative difference sets has been established for composite m (58), except for the following values of $m = 425$, 531, 545, 549, 629, 867, 909.

The case $m = 425$ has been recently settled by Arasu and Voss (68), using multipliers and intersection numbers.

Almost perfect sequences of Class I with $\theta = 2$ correspond to cyclic divisible difference sets with parameters

$$\left(\frac{v}{2}, 2, \frac{v-4}{2} 2, \frac{v-8}{4}\right)$$

Examples are known for $v = 8$, 12 and 28. Leung et al. (69) show the following.

Result 11. Almost perfect sequences of Class I with $\theta = 2$ and period v exist if and only if $v = 8$, 12, or 28.

Next we consider Class III(a). Here two possibilities arise: $\theta = 0$ when $f = v - 4$ and $\theta = 1$ when $f = v$ [note that it can be shown that $f \equiv v \pmod 4$]. The following parameters series are obtained:

$$\theta = 0 \Rightarrow \left(\frac{v}{2}, 2, \frac{v}{2}, \frac{v-2}{2}, \frac{v-2}{4}\right)$$
$$\theta = 1 \Rightarrow \left(\frac{v}{2}, 2, \frac{v-2}{2}, \frac{v-2}{2}, \frac{v-6}{4}\right)$$

If $\theta = 0$, $k - \lambda_1 = 1$. Arasu et al. (70) studied divisible difference sets with these parameters. The cyclic case has been settled completely in their work, which gives the following.

Result 12. Let D be a cyclic divisible difference set in $\mathbb{Z}_v$ with parameters

$$\left(\frac{v}{2}, 2, \frac{v}{2}, \frac{v-2}{2}, \frac{v-2}{4}\right)$$

Then $v/2$ must be an odd prime p, i.e. $\mathbb{Z}_v \cong \mathbb{Z}_p \times \mathbb{Z}_2$. The set D is, up to complementation and equivalence,

$$D = \{(x, y): x \text{ is a nonzero square in } \mathbb{Z}_p\} \cup \{(0, 0)\}$$

Corollary 5. Almost perfect sequences of Class III(a) and period v with $\theta = 0$ exist if and only if $v/2$ is an odd prime.

When $\theta = 1$, we have $k = \lambda_1$; using the classification by Bose and Connor (52) of these "divisible designs" and projection arguments, Jungnickel and Pott (58) show the following.

Theorem 14. A divisible difference set D with parameters

$$\left(\frac{v}{2}, 2, \frac{v-2}{2}, \frac{v-2}{2}, \frac{v-6}{4}\right)$$

exists in a group G relative to a normal subgroup N if and only if G/N contains a Paley–Hadamard difference set D'. If ϕ denotes the projection epimorphism $G \rightarrow G/N$, then the preimage of D' under ϕ is the desired divisible difference set.

Corollary 6. An almost perfect sequence of Class III(a) and period v with $\theta = 1$ exists if and only if a perfect sequence of period $v/2$ with $v \equiv 6 \bmod 8$ exists.

Finally we consider Class III(b). The parameter series looks quite messy; for instance, it contains divisible difference sets with $k - \lambda_1 = 0$, $k - \lambda_1 = 1$, or $\lambda_1 = \lambda_2$. The first two series have been investigated by Bose and Connor (52) and Arasu et al. (70), respectively. The last case corresponds to ordinary difference sets. This series also contains affine difference sets of Bose (47). Further parameters sets are also covered by Class III(b), which apparently do not fall into an infinite class, although they all correspond to almost perfect sequences.

BIBLIOGRAPHY

1. J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.,* **43**: 377–385, 1938.
2. H. B. Mann, *Addition Theorems,* New York: Wiley, 1965.
3. S. L. Ma and B. Schmidt, A sharp exponent bound for McFarland difference sets with $p = 2$, *J. Combinatorial Theory A,* **80**: 347–352, 1997.
4. S. L. Ma and B. Schmidt, Difference sets corresponding to a class of symmetric designs. *Des., Codes Cryptogr.,* **10**: 223–236, 1997.
5. B. Schmidt, Circulant Hadamard matrices: Overcoming non-self-conjugacy (submitted for publication).
6. B. Schmidt, Cyclotomic integers of prescribed absolute value and the class group (submitted for publication).
7. B. Schmidt, Non-existence results on Chen and Davis-Jedwab difference sets (submitted for publication).
8. D. Jungnickel, Difference sets, in J. H. Dinitz and D. R. Stinson (eds.), *Contemporary Design Theory: A Collection of Surveys,* New York: Wiley, 1992, pp. 241–324.
9. D. Jungnickel, On affine difference sets, *Sankhya A,* **54**: 219–240, 1992.
10. J. A. Davis and J. Jedwab, A survey of Hadamard difference sets, in K. T. Arasu et al. (eds.), *Groups, Difference Sets, and the Monster,* Berlin and New York: de Gruyter, 1996, pp. 145–156.
11. D. Jungnickel and A. Pott, Difference sets: Abelian, in C. J. Colbourn and J. Dinitz (eds.), *The CRC Handbook of Combinatorial Designs,* Boca Raton, FL: CRC Press, 1996, pp. 297–307.
12. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory,* 2nd ed. Cambridge, UK: Cambridge Univ. Press, 1998.
13. M. Hall, Jr., *Combinatorial Theory,* 2nd ed. New York: Wiley, 1986.
14. E. S. Lander, *Symmetric Designs: An Algebraic Approach,* Cambridge, UK: Cambridge Univ. Press, 1983.
15. L. D. Baumert, *Cyclic Difference Sets,* Vol. 182, Lect. Notes Math., New York: Springer, 1971.
16. A. Pott, *Finite Geometry and Character Theory,* Vol. 1601, Lect. Notes Math., Berlin: Springer-Verlag, 1995.
17. R. J. Turyn, Character sums and difference sets, *Pac. J. Math.,* **15**: 319–346, 1965.
18. R. H. Bruck, Difference sets in a finite group, *Trans. Amer. Math. Soc.,* **78**: 464–481, 1955.
19. R. H. Bruck and H. J. Ryser, The non-existence of certain finite projective planes, *Can. J. Math.,* **1**: 88–93, 1949.
20. S. Chowla and H. J. Ryser, Combinatorial problems, *Can. J. Math.,* **2**: 93–99, 1950.
21. M. P. Schutzenberger, A non-existence theorem for an infinite family of symmetrical block designs, *Ann. Eugen.,* **14**: 286–287, 1949.
22. C. J. Colbourn and J. H. Dinitz (eds.), *The CRC Handbook of Combinatorial Designs,* Boca Raton, FL: CRC Press, 1996.
23. B. Gordon, W. H. Mills, and L. R. Welsch, Some new difference sets, *Can. J. Math.,* **14**: 614–625, 1962.
24. R. G. Stanton and D. A. Sprott, A family of difference sets, *Can. J. Math.,* **11**: 73–77, 1958.
25. R. L. McFarland, A family of difference sets in non-cyclic abelian groups, *J. Combinatorial Theory A,* **15**: 1–10, 1973.
26. J. A. Davis and J. Jedwab, Nested Hadamard difference sets, *J. Stat. Plann. Inference,* **62**: 13–20, 1997.
27. T. Spence, A family of difference sets in non-cyclic groups, *J. Combinatorial Theory A,* **22**: 103–106, 1977.

28. J. F. Dillon, Difference sets in 2-groups, in R. L. Ward (ed.), *NSA Mathematical Sciences Meeting,* Ft. George Meade, MD, 1987, pp. 165–172.
29. J. A. Davis and J. Jedwab, A unifying construction of difference sets, *J. Combinatorial Theory, A,* **80**: 13–78, 1997.
30. Y. Q. Chen, On the existence of abelian Hadamard difference sets and a new family of difference sets, *Finite Fields Appl.,* **3**: 234–256, 1997.
31. R. G. Kraemer, Proof of a conjecture on Hadamard 2-groups, *J. Combinatorial Theory A,* **63**: 1–10, 1993.
32. M. Hall, Jr., Cyclic projective planes, *Duke J. Math.,* **14**: 1079–1090, 1947.
33. R. L. McFarland and B. F. Rice, Translates and multipliers of abelian difference sets, *Proc. Amer. Math. Soc.,* **68**: 375–379, 1978.
34. P. K. Menon, Difference sets in abelian groups, *Proc. Amer. Math. Soc.,* **11**: 368–376, 1960.
35. R. L. McFarland, On multipliers of abelian difference sets, Ph.D. thesis, Ohio State Univ., Columbus, 1970.
36. K. T. Arasu and Q. Xiang, Multiplier theorems, *J. Comb. Des.,* **3**: 257–267, 1995.
37. R. L. McFarland, Difference sets in abelian groups of order $4p^2$, *Mitt. Math. Sem. Giessen,* **192**: 1–70, 1989.
38. H. B. Mann and R. L. McFarland, On Hadamard difference sets, in J. N. Srivastava et al. (eds.), *A Survey of Combinatorial Theory,* Amsterdam: North-Holland, 1973, pp. 333–334.
39. W. K. Chan, Necessary conditions for Menon difference sets, *Des., Codes Cryptogr.,* **3**: 147–154, 1993.
40. S. L. Ma, Planar functions, relative difference sets and character theory, *J. Algebra,* **185**: 342–356, 1996.
41. K. T. Arasu et al., Exponent bounds for a family of abelian difference sets, in K. T.Arasu et al. (eds.), *Groups, Difference Sets, and the Monster,* Berlin and New York: de Gruyter, 1996, pp. 129–143.
42. K. T. Arasu and S. L. Ma, Abelian difference sets without self-conjugacy, *Des., Codes Cryptogr.* (to be published).
43. B. Schmidt, On (p^a, p^b, p^a, p^{a-b})-relative difference sets, *J. Algebraic Comb.,* **6**: 279–297, 1997.
44. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory,* New York: Springer, 1982.
45. P. V. Kumar, On the existence of square dot-matrix patterns having a specified three-valued periodic correlation function, *IEEE Trans. Inf. Theory,* **34**: 271–277, 1988.
46. K. T. Arasu et al., Relative difference sets with $n = 2$, *Discrete Math.,* **147** (1–3): 1–17, 1995.
47. R. C. Bose, An affine analogue of Singer's theorem, *J. Indian Math. Soc.,* **6**: 1–15, 1942.
48. A. T. Butson, Relations among generalized Hadamard matrices, *Can. J. Math.,* **15**: 42–48, 1963.
49. J. E. H. Elliott and A. T. Butson, Relative difference sets, *Ill. J. Math.,* **10**: 517–531, 1966.
50. C. W. H. Lam, On relative difference sets, *Proc. 7th Manitoba Conf. Numer. Math. Comput.,* 1977, pp. 445–474.
51. A. Pott, A survey on relative difference sets, in K. T. Arasu et al. (eds.), *Groups, Difference Sets and the Monster,* Berlin and New York: de Gruyter, 1996, pp. 195–232.
52. R. C. Bose and W. S. Connor, Combinatorial properties of group divisible incomplete block designs, *Ann. Math. Stat.,* **23**: 367–383, 1952.
53. P. Dembowski and T. G. Ostrom, Planes of order n with collineation groups of order n^2, *Math. Z.,* **103**: 239–258, 1968.
54. J. A. Davis, J. Jedwab, and M. Mowbray, New families of semiregular relative difference sets, *Des., Codes Cryptogr.,* **13**: 131–146, 1993.
55. K. T. Arasu and W. deLauney, Two dimensional perfect quaternary arrays, manuscript, 1998.
56. K. T. Arasu et al., The solution of the Waterloo problem, *J. Combinatorial Theory A,* **17**: 316–331, 1995.
57. K. T. Arasu, K. H. Leung, and S. L. Ma, Cyclic relative difference sets with classical parameters, manuscript, 1998.
58. D. Jungnickel and A. Pott, Perfect and almost perfect sequences, *Discrete Appl. Math.,* 1998 (to be published).
59. W. J. Broughton, A note on table 1 of "Barker sequences and difference sets," *L'Ens. Math.,* **50**: 105–107, 1994.
60. S. Eliahou and M. Kervaire, Barker sequences and difference sets, *L'Ens. Math.,* **38**: 345–382, 1992.
61. H Y. Song and S. W. Golomb, On the existence of cyclic Hadamard difference sets, *IEEE Trans. Inf. Theory,* **40**: 1266–1268, 1994.
62. S. W. Golomb and H. Y. Song, A conjecture on the existence of cyclic Hadamard difference sets, *J. Stat. Plann. Inference,* **62**: 39–42, 1997.
63. J. Wolfmann, Almost perfect autocorrelation sequences, *IEEE Trans. Inf. Theory,* **38**: 1412–1418, 1992.
64. S. P. Bradley and A. Pott, Existence and non-existence of almost-perfect autocorrelation sequences, *IEEE Trans. Inf. Theory,* **41**: 301–304, 1995.
65. D. Jungnickel, On a theorem of Ganley, *Graphs Comb.,* **3** (2): 141–143, 1987.
66. D. Reuschling, Zur Existenz von ω-zirkulanten Konferenz-Matrizen, Diplomarbeit, Universität Augsburg, 1994.
67. P. Langevin, Almost perfect binary functions. *Applicable Algebra, Algorithms and Error-Correcting Codes,* **4** (2): 95–102, 1993.
68. K. T. Arasu and N. J. Voss, Answering a question of Pott on almost perfect sequences, submitted, 1998.
69. K. H. Leung et al., Almost perfect sequences with $\theta = 2$, *Arch. Math.,* **70** (2): 128–131, 1998.
70. K. T. Arasu, D. Jungnickel, and A. Pott, Symmetric divisible designs with $k - \lambda_1 = 1$, *Discrete Math.,* **97** (1–3): 25–38, 1991.

Reading List

K. T. Arasu, S. L. Ma, and N. J. Voss, On a class of almost perfect sequences, *J. Algebra,* **192**: 641–650, 1997.

J. A. Davis and J. Jedwab, Some recent developments in difference sets, in K. Quinn et al. (eds.), *Combinatorical Designs and Applications,* London: Addison-Wesley (to be published).

J. F. Dillon, Difference sets in 2-groups. *Contemp. Math.,* **111**: 65–72, 1990.

S. Eliahou, M. Kervaire, and B. Saffari, A new restriction on the lengths of Golay complementary sequences, *J. Combinatorial Theory A,* **55**: 49–59, 1990.

J. Jedwab, Generalized perfect arrays and Menon difference sets, *Des., Codes Cryptogr.,* **2**: 19–68, 1992.

J. Jedwab et al., Perfect binary arrays and difference sets, *Discrete Math.,* **125** (1–3): 241–254, 1994.

D. Jungnickel, On automorphism groups of divisible designs, *Can. J. Math.,* **24**: 257–297, 1982.

D. Jungnickel and B. Schmidt, Difference sets: An update, *London Math. Soc. Lect. Notes,* **245**: 89–112, 1997.

R. E. Kibler, A summary of non-cyclic difference sets, $k \leq 20$, *J. Combinatorial Theory A,* **25**: 62–67, 1978.

L. E. Kopilovich, Difference sets in non-cyclic abelian groups, *Kibernetika,* **2**: 20–23, 1989.

P. K. Menon, On difference sets whose parameters satisfy a certain relation, *Proc. Amer. Math. Soc.,* **13**: 739–745, 1962.

K. W. Smith, A table no non-abelian difference sets, in C. J. Colbourn and J. H. Dinitz (eds.), *CRC Handbook of Combinatorial Designs,* Boca Raton, FL: CRC Press, 1996, pp. 308–312.

J. Storer, *Cyclotomy and Difference Sets,* Chicago: Markham, 1967.

R. Wilson and Q. Xiang, Constructions of Hadamard difference sets, *J. Combinatorial Theory A,* **77**: 148–160, 1997.

M. Y. Xia, Some infinite classes of special Williamson matrices and difference sets, *J. Combinatorial Theory A,* **61**: 230–242, 1992.

K. Yamamoto, Decomposition fields of difference sets, *Pac. J. Math.,* **13**: 337–352, 1963.

K. T. Arasu
Wright State University

Alexander Pott
University of Augsburg

THEORY OF FILTERING. See Filtering theory.

THEORY OF NUMBERS. See Number theory.

THEORY OF PROGRAMMING. See Programming theory.

THEORY OF RELIABILITY. See Reliability theory.

THERAPY, ABLATION. See Hypothermia therapy.

THERAPY, HYPOTHERMIA. See Hypothermia therapy.