Sequences and arrays with desirable correlation properties[1]

K. T. ARASU

Department of Mathematics and Statistics, Wright State University,
Dayton, OH 45435, U.S.A.

Abstract: Binary perfect sequences and their variations have applications in various areas such as signal processing, synchronizing and distance measuring radars. This survey discusses their *p*-ary analogs, other variations and related matters. Many new results are also presented.

Introduction:

In recent years there have been many publications on time-discrete one and two-dimensional sequences and arrays with perfect autocorrelation functions. Such sequences find applications in signal processing and as aperture functions for electromagnetic and acoustic imaging. Applications of two-dimensional perfect binary arrays are found in 2-D synchronization (Hershey & Yarlagadda (1983)) and time-frequency coding (Golomb & Taylor (1982)). In his invited address at the 1991 British Combinatorial Conference, Golomb gave an excellent exposition on why "small correlations" of sequences and arrays are desirable in dealing with radar problems (Golomb (1991)). Some fundamental results on sequences with small correlations can be found in the excellent survey of Turyn (1968). As observed by Lüke, Bömer and Antweiler (1989), higher dimensional arrays are used in channel coding and in cryptographic coding. Because of their applications to wide-band digital communications and to optical signal processing, perfect binary arrays and their related mathematical objects deserve further study. Sequences with ideal autocorrelation property have many applications in spread spectrum communication systems such as a code division multiple access (CDMA) system, which has been adopted as a standard for multiple access method in the mobile radio communication systems. Signal designs for CDMA systems have become interesting research topics in their application area. Other applications where sequence design is a more pressing issue include: radar and audio coding. (see Golomb and Gong (2005))

This paper surveys several related areas that pertain to sequences and arrays with good correlation properties. We confine our discussion only to the "periodic" case and the "autocorrelation" discussions. The "aperiodic" discussion will take us too far and we refer the reader to Jedwab (2008) and references therein for further study on that very useful topic. For the cross correlation issues, any search engine would yield dozens of resources – we give only two references (Hertel (2006) and Gologlu and Pott (2008)). Another intriguing related topic pertains to the study of the so-called "Balanced generalized weighing matrices", for which we refer the reader to the excellent survey by Jungnickel and Kharaghani (2004).

[1] Research supported in part by grants from AFOSR and NSF.

In this survey, we shall discuss perfect sequences and perfect arrays (binary, ternary, quaternary, *p*-ary for any prime *p*) and certain variations of them. Excellent surveys and fundamental discussions on related topics can be found in Jungnickel and Pott (1999a, 1999b), Cai and Ding (2009), Xiang (1992), Xiang (2005), Jedwab (1992,2008), and Davis and Jedwab (1997); all of which also provide a wealth of references.

In section 1, we discuss binary sequences with 2-level optimal autocorrelation values (all of whose out-of-phase values being the same). Section 2 will be devoted to the 3-level case for optimal binary sequences. Generalization to the multi-dimensional case will be the focus of study in section 3, where we also investigate the inclusion of zero to the binary alphabet set $\{1,-1\}$, terming the resulting arrays as "ternary". These latter entities turn out to be equivalent to group weighing matrices. Section 4 will be devoted the "quaternary" case, primarily the 1- and 2- dimensional cases will be discussed. These will be equivalent to "complex Hadamard matrices" with a group action, which in turn give rise to a class of relative difference sets. Section 5 is a synopsis of the systematic study undertaken by Ma and Ng (2009) for the *p*-ary sequences (p any odd prime). Their terminology may slightly differ from what we shall use in section 6, wherein we study the 2-level *p*-ary case, primarily on the construction arena. Results of section 6 will serve as a preview of a rather long paper of Arasu, Dillon and Player (2010) which is nearing its completion.

In the remainder of this section, we provide some basic definitions of some combinatorial objects that arise naturally from the sequences that we shall discuss in later sections.

Let G be a multiplicatively written abelian group of order v. Let $C\ [G]$ denote the group ring of G over the field of complex numbers C. A subset S of G is identified with the group ring element which is a formal sum of the elements of S (i.e. with coefficients 0 and 1) and for an element A of CG and integer t, $A^{(t)}$ denotes the image of A under the group homomorphism x to x^t, extended linearly to all of CG; A* would denote $A^{(-1)}$ in which we also replace each coefficient of A by its complex conjugate.

Difference sets, perfect sequences and related objects are often studied using character theory. Let G^* be the group of characters of G (A homomorphism from a group G to the field of complex numbers C is called a character of G). The principal character of G is defined as the homomorphism that maps each element g of G to 1. We shall denote the principal character by χ_0. The character homomorphism can be extended linearly to the group ring. We let the induced homomorphism from CG to C also be denoted by χ.

<u>Definition</u> : (Difference Set, abbr. DS) Let D be an element of $Z[G]$ whose coefficients are from $\{0,1\}$. D is a (v, k, λ) difference set in G if

$$DD^{(-1)} = k - \lambda + \lambda G \ in \ ZG \tag{1}$$

or equivalently if

$$(\forall\chi) \mid \chi(D) \mid^2 = \begin{cases} k-\lambda & if\ \chi \neq \chi_0 \\ k^2 & if\ \chi = \chi_0 \end{cases} \tag{2}$$

where x is a multiplicative character of G.

A purely combinatorial definition of a difference set is given below:

Definition: Let G be an (additively written) abelian group of order v. A k-subset D of G is said to be a (v,k,λ) difference set in G if every non-identity element t of G has exactly λ representations as $t = d - e$ for d and e in D.)

A difference set D is called cyclic or abelian, if G has the respective property.

For any prime power q, we let F_q denote the finite field of order q and F_q* the multiplicative group of all the non-zero elements of F_q.

Example: (Singer difference set) Let $G = F^*{}_p d/F^*{}_p$ for some prime p and d some positive integer > 2.

Then

$$L = \sum \delta_{Tr(\lambda),O}\,\lambda \tag{3}$$

is a difference set with Singer parameters. (Here δ is the Kronecker delta function and Tr is the absolute trace function of F_{p^d})

Definition: (Relative Difference Set, abbr. RDS) Let R be an element of $Z[G]$ whose coefficients are from {0,1}. R is a (m,n,k,λ) relative difference set in G if

$$RR^{(-1)} = k + \lambda(G - N)\ in\ ZG \tag{4}$$

or equivalently if

$$(\forall\chi)\mid\chi(R)\mid^2 = \begin{cases} k - \lambda n & if\ \chi\mid N = \chi_0 \\ k & if\ \chi\mid N \neq \chi_0 \\ k^2 & if\ \chi = \chi_0 \end{cases} \tag{5}$$

Here N is a subgroup of G of order n and index m in G.

For the interplay of characters and difference sets, we refer the reader to Mann (1965) and Turyn (1965). A good account of difference sets is found in Lander (1983) and Beth, Jungnickel, and Lenz (1999). For a recent survey, see Jungnickel and Pott (1999b). Pott(1995) would serve as a nice reference for relative difference sets and related objects discussed in the remainder of this survey.

1. Binary sequences with optimal autocorrelations (2-level case)

Let a be a binary sequence (a_i) of period n for $i \geq 0$, so $a_i \in \{\pm 1\}$ and $a_{i+n} = a_i$ for each i. The autocorrelation of the binary sequence (a_i) for shift t is defined as the following sum:

$$C_t(a) = \sum_{i-0}^{n-1} a_i a_{i+t} \tag{6}$$

where the subscripts are modulo n.

A sequence a with a constant value of $C_t(a)$ for all possible shifts , i.e. $0 < t \leq n - 1$, is said to have constant autocorrelation. We shall say that such sequences have 2-level autocorrelation values, one value for the trivial shift and the second constant value for the remaining non-trivial shifts. The following is well known: (e.g. see Turyn (1968) or Jungnickel and Pott (1999a)).

Proposition 1.1: $C_t(a) \equiv n$ mod 4

It is important to find such sequences that are perfect (i.e. having optimal autocorrelation). A perfect sequence a is defined to have the smallest possible max $|C_t|$ for $0 < t < n$.

Thus, we wish to have sequences with the following autocorrelations for every $t \not\equiv 0$ (mod n):

$$C_t(a) = 0, \; if \;\; n \equiv 0 \; (mod \; 4) \tag{7}$$

$$C_t(a) = 1, \; if \;\; n \equiv 1 \; (\mathrm{mod}\; 4) \tag{8}$$

$$C_t(a) = \pm 2, \; if \;\; n \equiv 2 \; (mod \; 4) \tag{9}$$

$$C_t(a) = -1, \; if \;\; n \equiv 3 \; (\mathrm{mod}\; 4) \tag{10}$$

Obviously, $C_t(a) = n$ when $t \equiv 0$ (mod n) for any ±1 binary sequence.

Let $a = (a_i)$ be a binary sequence of period n. Define $D = \{0 \leq i \leq n - 1 : a_i = 1\}$ and $d_D(t) = |(t + D) \cap D|$, which is called the difference function of $D \subseteq Z_n$. Then $C_t(a) = n - 4(k - d_D(t))$ where $k = |D|$. This would serve as a bridge between binary sequences and combinatorial designs. The set D defined above would work as the required cyclic difference set in the following result which is easy to prove:

Proposition 1.2: A periodic binary sequence with period v; k entries $+1$ per period and 2-level autocorrelation function (with all nontrivial autocorrelation coefficients equal to r) is equivalent to a cyclic (v, k, λ)-difference set; where $r = v - 4(k - \lambda)$.

Detailed analysis of the 5 optimal cases of Proposition 1.2, when $r = 0, 1, 2, -2, -1$ are nicely discussed in Jungnickel and Pott (1999a). We give a very brief summary here.

Case 1: $r = 0$

The case $r = 0$ corresponds to circulant Hadamard matrices of order v, where $v = 4u^2$, which are equivalent to cyclic $(4u^2,\ 2u^2 - u, u^2 - u)$-difference sets. The only known such example is when $v = 4$ and is conjectured that there are no others. Mossinghoff (2009) has verified this for v upto $4 \cdot 10^{26}$, with fewer than 1600 exceptions. Penetrating work of Schmidt (1999, 2002) which is based on deep algebraic number theory provides valuable tools to study these and other related and similar objects. We give one such sample result of Schmidt:

Theorem 1.3: (Schmidt (1999)): Let Q be any finite set of primes. Then there are only finitely many cyclic Hadamard difference sets of order u^2; where all prime divisors of u are in Q.

Case 2: $r = 1$

The case $r = 1$ gives rise to $(2u^2 + 2u + 1; u^2; u(u-1)/2)$ cyclic difference sets. While these do exist for $u = 1$ and $u = 2$, it is believed that none exists for all other higher values of u. In fact Eliahou and Kervaire (1992) and Broughton (1995) have shown:

Result 1.4: No abelian difference sets with parameters $(2u^2 + 2u + 1; u^2; u(u - 1)/2)$ exist for u between 3 and 100; consequently perfect sequences of the type corresponding to the constant value 1 for all the non-trivial autocorrelations and period v do not exist for v between 14 and 20201.

Case 3: $r = 2$

The only systematic investigation of the case when $r = 2$ is due to Jungnickel and Pott (1999a) who show:

Result 1.5: Perfect sequences of period v for the case $r = 2$ do not exist for v between 7 and 12545; In fact, these do not exist for all periods $v < 10^9$ except possibly perhaps for the following four unresolved lengths in this range: 12 546, 174 726, 2 433 602 and 33 895 686.

We remark that the methods used to obtain the above result are standard ones from the theory of difference sets and with the advancement of technology, it should be possible to improve the bound on this result. New non-existence results in the area of difference sets would also help to strengthen this result.

Case 4: $r = -2$

It is easy to see that the only difference set corresponding to a perfect sequence with autocorrelation value -2 is the trivial $(2; 1; 0)$-difference set.

Case 5: $r = -1$

Thus the only remaining case we need to discuss pertains to the case $r = -1$, which would take us to a very fertile terrain where the examples are bountiful. In view of Proposition 1.2, these perfect binary sequences with $r = -1$ are equivalent to cyclic difference sets with parameters $(v, (v-1)/2, (v-3)/4)$, which are commonly referred to as Paley-Hadamard difference sets. We refer the reader to Beth, Jungnickel and Lenz (1999), Jungnickel and Pott (1999 b), Xiang (1992),Xiang (2005), Cai and Ding (2009) for further readings on these. We shall list below the known families of these interesting combinatorial objects:

(1) Cyclotomic cyclic difference sets and their sequences (Storer (1967), Beth, Jungnickel and Lenz (1999))

(2) Hall difference sets (Hall (1956))

(3) Paley difference sets (Paley (1933)

(4) The twin-prime construction (Stanton and Sprott (1958))

(5) Singer difference sets (Singer (1938))

(6) Hyperoval difference sets (Maschietti(1998))

(7) No-Chung-Yun difference sets (No et al (1998))

(8) Dillon-Dobbertin difference sets (Dillon-Dobbertin (2004))

(9) Gordon-Mills-Welch difference sets (Gordon et al (1962))

2. Binary sequences with optimal autocorrelations (3-level case)

We now turn our attention to discuss the cases where we allow two possible values for $C_t(a)$ for all t satisfying $0 < t \leq n-1$, referring to the underlying sequences as "almost perfect". We warn the reader that the term "almost perfect" has been used with different meanings in Jungnickel and Pott (1999a) and Ma and Ng (2009). Jungnickel and Pott (1999a) variation is also of interest, and this has been investigated by Arasu, Ma and Voss (1997) and Leung et al (1998). The optimal criteria in the situations we discuss here will correspond to having autocorrelations for every $t \not\equiv 0 \pmod{n}$:

$$C_t(a) \epsilon \{0\,,4\,\} \text{ or } \{0\,,-4\} \text{ if } \mathrm{n} \equiv 0 \text{ (mod 4)} \tag{11}$$

$$C_t(a) \epsilon \{1\,,-3\} \text{ if } \mathrm{n} \equiv 1 \ (mod\ 4) \tag{12}$$

$$C_t(a) \epsilon \{2,-2\} \text{ if } \mathrm{n} \equiv 2 \text{ (mod 4)} \tag{13}$$

$$C_t(a) \epsilon \{-1\,,3\} \text{ if } \mathrm{n} \equiv 3 \text{ (mod 4)} \tag{14}$$

Definition 2.1: Let G be an (additively written) abelian group of order v. A k-subset D of G is said to be a (v,k,λ,s)-almost difference set (ADS) of G if $d_D(t)$ takes the value λ altogether s times and the value $\lambda+1$ altogether $v-1-s$ times, as t runs over all the non-identity elements of G.

Equivalently, $A(v,k,\lambda,s)$-almost difference set D is a subset of a group G of order v with $|D| = k$ such that the 'difference list' $(d - d' | d, d' \in D \ and\ d \neq d')$ contains s elements of G exactly λ times and the remaining $v-s-1$ elements of G exactly $\lambda+1$ times.

Detailed analysis of the 3-level optimal binary sequences and their ADS counterparts can be found in the nice survey by Cai and Ding (2009). Here we mainly extract the highlights given there and also provide some new results.

Theorem 2.2: (Arasu, Ding et al (2001)) Let $(a\ (t))$ be a binary sequence of period N, and let $D = \{0 \leq i \leq N-1 : a(i) = 1\}$ be its support.

(1) Let $N \equiv 3 \pmod 4$. Then $C_t(a) = -1$ for all $t \not\equiv 0 (\mathrm{mod}\, N)$iff D is an $\left(N, \frac{(N+1)}{2}, \frac{(N+1)}{4}\right)$ or $\left(N, \frac{(N-1)}{2}, \frac{(N-3)}{4}\right) DS$ in Z_N.

(2) Let $N \equiv 1 \pmod 4$. Then $C_t(a) \in \{1, -3\}$ for all $t \not\equiv 0 \pmod N$ iff D is an $\left(N, k, k - \frac{(N+3)}{4}, Nk - k^2 - \frac{1}{4}(N-1)^2\right)$ ADS in Z_N.

(3) Let $N \equiv 2 \pmod 4$. Then $C_t(a) \in \{2, -2\}$ for all $t \not\equiv 0 \pmod N$ iff D is an $(N, k, k - (N+2)/4, Nk - k^2 - \frac{1}{4}(N-1)(N-2))$ADS in Z_N.

(4) Let $N \equiv 0 \pmod 4$. Then $C_t(a) \in \{0, -4\}$ for all $t \not\equiv 0 \pmod N$ iff D is an $(N, k, k - (N+4)/4, Nk - k^2 - \frac{1}{4}(N-1)N) ADS\ in\ Z_N$.

We now discuss each of the 4 cases mentioned in Theorem 2.2:

Case 1: $N \equiv 3 \pmod 4$

The resulting difference sets are Paley-Hadamard difference sets, which are already discussed in section 1. The extension of this case requiring the 3-level autocorrelations (allowing both -1 and 3 as autocorrelation values for all non-trivial shifts) has not been explored yet. The only such theorem that is known to us is given in:

Theorem 2.3: (Cai and Ding (2009)): Let R_2 be any $\left(2^{m/2} - 1, 2^{(m-2)/2} - 1, 2^{(m-4)2} - 1\right)$ difference set in $GF\left(2^{m/2}\right)^*$. Define

$$R_1 = \left\{x \in GF(2^m) : Tr_{2^m/2^{m/2}}(x) = 1\right\}, R = \{r_1 r_2 : r_1 \in R_1, r_2 \in R_2\} \qquad (15)$$

Then R is a $(2^m - 1, 2^{m-1} - 2^{\frac{m}{2}}, 2^{m-2} - 2^{\frac{m}{2}}, 2^{\frac{m}{2}} - 2)$ almost difference set in $GF(2^m)^*$. Furthermore, the characteristic sequence of the set $log_{\alpha} R$ has only the out-of-phase autocorrelation values $\{-1,3\}$, where α is any generator of $GF(2^m)$.

Case 2: $N \equiv 1 \pmod 4$

We summarize below the known constructions of binary sequences of period $N \equiv 1\ (mod\ 4)$ with optimal out-of-phase autocorrelation values $\{1, -3\}$:

(1) The Legendre sequences: (Legendre (1798)) Let $p \equiv 1\ (mod\ 4)$ be a prime. The set of quadratic residues modulo p form an almost difference set in Z_p. Its characteristic sequence is the Legendre sequence with optimal out-of-phase autocorrelation values $\{1, -3\}$.

(2) Ding-Helleseth-Lam sequences (Ding et al (1999)): These are equivalent to almost difference sets in Z_p , where p is a prime of the form $p = x^2 + 4$ and $x \equiv 1\ (mod\ 4)$ and are constructed using suitable cyclotomic classes of order 4. (See Ding et all (1999) for details).

(3) Ding sequences using generalized cyclotomy (Ding (1998)): Using the notion of generalized cyclotomy due to Whiteman (1962), Ding constructed a class of almost difference sets in $Z_{p(p+4)}$ where p and $p + 4$ are primes, the characteristic sequences of which would serve as optimal sequences with out-of-phase autocorrelation values $\{1, -3\}$.

Remarks:

(1) The resulting sequences from the above three constructions can be shown to be inequivalent. (Ding (2010))

(2) There is a small history behind the 3rd family discussed above, we draw it from http://www.cse.ust.hk/faculty/cding/200year.html.

Stanton and Sprott (1958) discovered the so-called two-prime difference sets and thus the twin-prime sequences with optimal autocorrelation value -1. Whiteman (1962) obtained a generalization of the theorem of Stanton and Sprott. In 1991, the two-prime sequences, which are a generalization of the twin-prime sequences, were described in Jensen, Jensen and Hoholdt (1991). However, the autocorrelation values of the two-prime sequences were not known until 1998. Ding (1998) determined the autocorrelation values under the condition that $gcd(p-1, q-1) = 2$. Mertens and Bessenrodt (1998) independently obtained the autocorrelation values of the two-prime sequences. Thus exactly two centuries after the Legendre sequences had been reported, it was discovered that the two-prime sequences have optimal autocorrelation values -3 and 1 when $q-p=4$.

It seems to be the case that balanced optimal binary sequences of period N when $N \equiv 1 \ (\mathrm{mod}\ 4)$ always exist; we do not have a proof of this of course. Computer experiments seem to suggest it. We give the following computer generated examples of such sequences:

Length	5	:	++---
Length	9	:	+++-+----
Length	13	:	+++-++-+-----
Length	17	:	++-+++-+-++------
Length	21	:	++++--++-++-+-+------
Length	25	:	+++-+-++-++--+++-+-------
Length	29	:	+++-+-+++-++-+--+++--+-------
Length	33	:	+++-+--++-+++--+++-+-++-+--------
Length	37	:	+++-+-+-++--++++--+-++-+++--+--------
Length	41	:	+++-+-+-++--++--+-++++-+--++++--+--------
Length	45	:	++++-+--+++--++--+-++-+++--+-+++-+-+---------

Case 3: $N \equiv 0 \ (mod\ 4)$

We summarize below the known constructions of binary sequences of period $N \equiv 0 \ (mod\ 4)$ with optimal out-of-phase autocorrelation values $\{0, -4\}$:

(1) Sidelnikov-Lempel-Cohn-Eastman sequences (See Sidelnikov (1969) and Lempel, Cohn and Eastman (1977)): Let q be a prime power, $q \equiv 1 \ (\mathrm{mod}\ 4)$. Let g be a primitive element of the finite field $GF(q)$. The set $D = \{a \text{ in } Z_{q-1} | g^a + 1 \text{ is a non} - \text{square in } GF(q)\}$ is an almost difference set with parameters $(q-1, ½(q-1), ¼(\mathrm{q}-5), ¼\ (q-1))$ in Z_{q-1} whose characteristic sequence is optimal having autocorrelation values $\{0, -4\}$.

(2) Arasu-Ding-Helleseth-Kumar-Martinsen sequences (See Arasu, Ding et al (2001)): There are two such sequences, both of which use cyclic difference sets with Paley parameters $(m, ½(m-1), ¼(\mathrm{m}-3))$ and certain Kronecker type composition with Z_4, thereby yielding an almost difference set in $Z_4\ X\ Z_m$ with parameters $(4m, 2m\text{–}1, m-2, m\text{–}1)$; the characteristic

sequence is optimal having autocorrelation values $\{0, -4\}$.

Remarks:

(1) The Arasu-et al family (2) above is very fertile, in view of our results from the previous section on 2-level perfect sequences with $r = -1$, all of which yielding difference sets with Paley parameters which can be used in the aforementioned construction.

(2) Use of complementary "Paley" difference sets with parameters $(m, ½(m + 1), ¼(m + 3))$ in the constructions of Arasu et al (2001) yield almost difference sets in $Z_4\, X\, Z_m$ with parameters $(4m, 2m + 1, m\,, m - 1)$; the characteristic sequence is optimal having autocorrelation values $\{0, -4\}$.

Case 4: $N \equiv 2 \text{ (mod 4)}$

We now summarize the known constructions of binary sequences of period $N \equiv 2(\text{mod } 4)$ with optimal out-of-phase autocorrelation values $\{2, -2\}$:

(1) Sidelnikov-Lempel-Cohn-Eastman sequences (See Sidelnikov (1969) and Lempel, Cohn and Eastman (1977)): Let q be a prime power, $q \equiv 3 \text{ (mod 4)}$. Let g be a primitive element of the finite field $GF(q)$. The set $D = \{a \text{ } in \text{ } Z_{q-1} | g^a + 1 \text{ is a non} - \text{square in } GF(q)\}$ is an almost difference set with parameters $(q - 1, ½(\text{q} - 1), ¼(\text{q} - 3), ¼(3\text{q} - 5))$ in Z_{q-1}, whose characteristic sequence is optimal having autocorrelation values $\{2, -2\}$.

(2) Ding-Helleseth-Martinsen sequences (See Ding,Helleseth,Martinsen (2001)): Since we believe that some clever insight into the ingenious construction of Ding,Helleseth,Martinsen (2001) might result in the use of higher order cyclotomic classes to obtain further classes of such sequences, we now outline this construction in detail.

Let F_p be a finite field of prime order p and let $d \in Z$ be a divisor of $p - 1$. Let α be a primitive element of F_p , and define $D_0^{(d,p)}$ to be the multiplicative group generated by α^d. Then, $D^{(d,p)} = \alpha^i D_0^{(d,p)}$ for integer i, where $0 < i \leq d - 1$.

We now let $p \equiv 5 \text{ (mod 8)}$, and it is known that $p = s^2 + 4t^2$ for some s and t with $s \equiv \pm 1 \text{ (mod 4)}$. Then,

$$C = \left[\{0\} \times \left(D_i^{4,p} \cup D_j^{4,p}\right)\right] \cup \left[\{1\} \times \left(D_I^{4,p} \cup D_j^{4,p}\right)\right] \cup \{(0)\} \tag{16}$$

is an (n, n/2, (n − 2)/4, (3n − 2)/4) - almost difference set in $\text{Z}_2 \times \text{Z}_\text{p}$, if

$$t = 1 \text{ and } (i, j, l) \in \{(0,1,3), (0,2,3), (1,2,0), (1,3,0)\} \tag{17}$$

or

$$s = 1 \text{ and } (i, j, l) \in \{(0,1,2), (0,3,2), (1,0,3), (1,2,3)\}. \tag{18}$$

The above constructions correspond to balanced perfect sequences of period $n \equiv 2 \text{ (mod 4)}$. The following constructions give almost balanced perfect sequences:

Let $p \equiv 5 \text{ (mod 8)}$, and $p = s^2 + 4t^2$ for some s and t with $s \equiv \pm 1\ (mod\ 4)$. Then,

$$C = \left[\{0\} \times \left(D_i^{4,p} \cup D_j^{4,p}\right)\right] \cup \left[\{1\} \times \left(D_l^{4,p} \cup D_j^{4,p}\right)\right] \tag{19}$$

is an $(n, n/2, (n-6)/4, (3n-6)/4) -$ almost difference set in $Z_2 \times Z_p$, if

$$t = 1\ and\ (i, j, l) = (0,1,3)\ or\ (0,2,1) \tag{20}$$

or

$$s = 1\ and\ (i, j, l) = (1,0,3)\ or\ (0,1,2). \tag{21}$$

The aforementioned almost difference sets readily give the optimal binary sequences having autocorrelation values $\{2, -2\}$.

We close this section by giving the following two new examples due to Arasu and Little (2010) based on computer searches:

(1) $\mathrm{D} = \{0,1,4,5,6,7,10,12,13,20,22,24,25,26,28,31,33,34,35\}$ is a $(38,19,9,28)$ -almost difference set in Z_{38}.

(2) $\mathrm{D} = \{0,1,2,4,5,8,9,10,12,15,16,17,18,19,22,24,26,28,29,31,34,35,37,,39, 40\}$ is a $(50,25,12,37)$–almost difference set in Z_{50}.

We give the corresponding balanced optimal binary sequences below:

Length 38: ++--++++--+-++------+-+-+++-+--+-+++--
Length 50: +++-++--+++-+--+++++--+-+-+-++-+--++-+-++---------

Helleseth (2002) provides the following two balanced binary optimal sequences of length 34:

+-------+-++--+-+++--+-+++--+++-++
+-------+-++-+-+-+++++---+++--++-+

The above three examples are balanced – in the sense, the number of 1's and -1's in the sequence is the same; the term "almost balanced" would mean that the number of 1's and number of -1's nearly equal. (differ by 1 or 2 depending on the length of the sequence is odd or even). Although an almost balanced optimal binary sequence of length 14 exists, a balanced one cannot (for a proof see Arasu and Pott (2009)).

We close this section by asking:

Questions: Are there other families of perfect binary sequences of period $n \equiv 2\ (mod\ 4)$ that can be constructed, balanced or otherwise? Do balanced perfect sequences of periods $n = 54,62,86,90,94, or\ 98$ exist?

Remark: The periods listed above are the only open cases for $n < 100$, when $n \equiv 2\ (mod\ 4)$.

3. Perfect arrays

An r-dimensional matrix $A = a[J_1, \dots, J_r]$ with $0 \leq J_i < S_i (1 \leq i \leq r)$ is called an $S_1 \times \dots \times S_r$ array. The array is called perfect if the periodic autocorrelation coefficients

$$R_A(u_1, \dots, u_r) = \sum_{J_1=0}^{S_1-1} \dots \sum_{J_r=0}^{S_2-1} a[J_1, \dots, J_r] a[(J_1 + u_1) \text{mod } S_1, \dots, (J_r + u_r) \text{ mod } S_r] \tag{22}$$

are zero for all $(u_1, \dots, u_r) \neq (0, \dots, 0), 0 \leq u_i < S_i$. The array is binary if each matrix entry is ± 1. The array is ternary if the entries lie in $\{0,1,-1\}$. The invertible mapping from the binary array A to $U(A) = \{(J_1, \dots, J_r) | a[J_1, \dots, J_r] = -1\}$ gives rise to an equivalence between an $S_1 \times \dots \times S_r$ perfect binary array and a Hadamard difference set (also called Menon difference set) in $Zs_1 \times \dots \times Zs_r$ (See Jedwab (1992) and Davis and Jedwab (1997)).

There is a vast literature in the area of Hadamard difference sets – we refer the reader to Beth, Jungnickel and Lenz (1999) and the Bibliography provided there for the study of this very important combinatorial structure. We just summarize below as a theorem which contains the current state of the art of the abelian groups that contain a Hadamard difference set.

Theorem 3.1: Let $G = K \times Z_{m_1}^2 \times \dots \times Z_{m_r}^2 \times Z_{p_1}^4 \dots Z_{p_r}^4$ where K is an abelian group of order 2^{2d+2} and exponent at most $2^{d+2}, d, \mathrm{m}_1 \dots \mathrm{m}_\mathrm{r}$ are non-negative integers such that $m_i = 3^{j_i}$ for some non-negative integer j_i and $p_1 \dots p_s$ are odd primes. Then G contains a Hadamard difference set.

The "smallest" open cases are : $Z_{20} \times Z_{20}$ *and* $Z_{10} \times Z_{40}$.

A study of perfect binary arrays (and Hadamard difference sets) would be incomplete without mentioning the names of some very important players and contributors in the field: W.K. Chan, Y.Q. Chen, J. Davis, J.F. Dillon, J. Iiams, W.M. Kantor, R.G. Kraemer, R. Liebler ,S.L. Ma, R.L. McFarland, D.B. Meisner, P.K. Menon, C. Mitchell, F.C. Piper, D. K. Ray-Chaudhuri, B. Schmidt, S.K. Sehgal, M.K. Siu, K. Smith, V. Tonchev, R.J. Turyn, P.R. Wild, X. Wu, R.M. Wilson, M.Y. Xia,Q. Xiang, M. Yamada, and K.Yamamoto.

A recent exposition of Hadamard difference sets containing some beautiful examples is Dillon (2010). Dillon (2010) gives several perfect multidimensional arrays and synchronization patterns with colorful pictures.

In the remainder of this section, we shall discuss perfect ternary arrays (See Arasu and Dillon (1999) for a survey on this topic). We begin by introducing "group invariant matrices" (which are also referred to as "group developed matrices").

Let H be a group of order n (H need not be abelian, but we write H additively). An $n \times n$ matrix $A = (a_{gh})$ indexed by the elements of the group H (so g and h belong to H) is said to be H-invariant (or H-developed) if it satisfies the condition

$$a_{gh} = a_{g+k,h+k} \text{ for } all\ g, h, k\ in\ H. \tag{23}$$

A is said to be circulant if the underlying group H is cyclic. Thus the matrix A is completely determined by its first row.

Let RG denote the group ring of a given group G over a ring R. Then the set of G-invariant matrices with entries from R is isomorphic to the group ring RG.

A weighing matrix $W(v, k)$ is a square matrix of size v all of whose entries lies in $\{0,1,-1\}$ satisfying

$$WW^t = kI_v \tag{24}$$

where I is the $v\times v$ identity matrix.

Note that W must have exactly k entries which are nonzero. k is called the weight of W. If $W = (|w_{ij}|)$ is the incidence matrix of a symmetric (v, k, λ)design, then the weighing matrix W is said to be balanced. Examples of balanced weighing matrices include Hadamard matrices $W(m, m)$ and conference matrices $W(m, m-1)$. We let CW(n,k) stand for a circulant weighing matrix of order n with weight k.

Each class of group invariant matrices can be described as a group ring equation. This group ring formulation of the problem is generally used to obtain existence and nonexistence of these objects. Hence the study of these group invariant matrices uses character theory and algebraic number theory.

We now turn our attention to perfect ternary arrays, drawing freely from the survey of Arasu and Dillon (1999).

Antweiler, Bomer and Luke(1990) first introduced the term perfect ternary array but 1-dimensional examples were known in the literature earlier under name of perfect ternary sequences or circulant weighing matrices, (see Chang (1997), Dillon (1979), Eades and Hain (1976), Games (1986), Geramita and Seberry (1979), Høholdt and Justensen (1983), Ipatov, Platonov and Samilov(1983), Mullin (1975), Mullin and Stanton (1975,1976), Vincent (1989) and Whiteman (1975).) Moreover, Jedwab's (1992) results on generalized perfect arrays apply to the ternary case as well.

Let A be an $s_1 \times s_2 \times \ldots s_r$ PTA. The number of nonzero entries in A is called energy of A and is denoted by $e(A)$. The ratio $e(A)/(s_1s_2 \ldots s_r)$ is called its energy efficiency.

The following is easy to prove; it gives the connection between perfect ternary arrays and group invariant/developed matrices.

Proposition 3.2: The existence of an $S_1 \times S_2 \times \ldots \times S_r$ PTA with energy k is equivalent to the existence of two disjoint subsets P and N of $G = Z_{s_1} \times Z_{s_2} \times \ldots Z_{s_r}$ satisfying $(P-N)(P-N)^{(-1)} = k$, and hence equivalent to existence of a G-developed matrix $W(\,|G|, k)$.

The next result is well known and easy to prove (see Mullin (1975), e.g.)

Proposition 3.3: Assume the existence of a G-developed weighing matrix $W(|G|, k)$. Then

(1) $k = s^2$ for some integer s;

(2) $\{|P|, |N|\} = \{(s^2 - s)/2, (s^2 + s)/2\}$

The following is an easy "composition" and "imbedding" theorem.

Theorem 3.4:

(1) If there exists a G-developed matrix $W(|G|, k)$, then there exists an H-developed matrix $W(|H|, k)$ for all groups H containing a subgroup isomorphic to G.

(2) If there exists a $CW(n, s^2)$, then there exists a $CW(mn, s^2)$ for all positive integers m.

(3) Suppose that $gcd(s_1, s_2) = 1$. Then there exists a $(Z_{s_1} \times Z_{s_2})$-developed matrix $W(n, k)$ if there exists a $CW(s_1 s_2, k)$.

(4) If there exists G_i-developed matrix $W(n_i, k_i), i = 1,2$, then there exists a $(G_1 \times G_2)$-developed matrix $W(n_1\, n_2, k_1 k_2)$.

Our next theorem uses the well known idea of "orthogonal pieces"; an explicit proof is in Arasu and Dillon (1999).

Theorem 3.5: if there exists a $CW(v, k)$ with 'v' odd, then there exists a $CW(2vm, 4k)$ for all odd $m > 1$.

An extension of theorem 3.5 to the abelian case is given below:

Theorem 3.6: Let H be an abelian group and let $D_i \in ZH$ for $i = 0,1,2 \ldots, (n-1)$.

Assume that following three conditions are satisfied:

(1) The coefficients of each of the D_i's are $0,1$ and -1

(2) $\sum_{i=0}^{n-1} D_i D_i^{(-1)} = n\,|H|$

(3) $D_i D_j^{(-1)} = 0$ for all $i \neq j$

Moreover, let G be an abelian group containing H as a subgroup of index $l > n$. Then there exists a G-developed matrix $W\big(|G|, n|H|\big)$.

Our next result contains essentially the only infinite family of *CW*s (the minimal one's).

Theorem 3.7: For each prime power q and positive integer , there exists a $CW[(q^{2d+1} - 1)/(q-1)\,, q^{2d})$.

The result of Theorem 3.7 has an interesting history. Using the so-called "affine difference sets'' of Bose (1942) and Elliot and Butson (1956), the *CW*s of the Theorem 2.9 for odd q can be easily obtained by taking a suitable homomorphic image of the underlying relative difference set. The reader may consult Arasu, Dillon, Jungnickel and Pott (1995), Elliot and Butson (1956) and Pott (1995) for more details. The q odd case was independently obtained by Eades (1977,1980). The case q odd and $d = 3$ is also contained in Wallis and Whiteman (1975). Using shift register sequences, Ipatov (1979, 1980) obtained CWs in the odd q case using the PTS language.

The case q even was first reported by Dillon (1979); Games (1986) and Høholdt and Justesen (1983) are the first published results for the q even case (using PTS language). Details of Dillon's (1979) constructions appeared in Arasu, Dillon, Jungnickel and Pott (1995).

The other known sporadic examples of $CW(n, k)$ have (n, k) equal to $(33,25)$, $(71,25)$, $(87,49)$ and $(24,9)$.

A $CW(33,25)$ was first found by Antweiler, Bömer and Lüke (1990) using a computer; a theoretical explanation of this example is due to Arasu and Torban (1997). A $CW(24,9)$ is contained in Strassler (1997) and Ang et al (2008). This was first discovered by Vincent (1989) via computer search. Strassler (1998) found examples of $CW(71,25)$ and $CW(87,49)$. These two can be easily obtained using the well known notion of "multipliers".

Jedwab and Mitchell (1988) and Wild (1988) obtain larger PBAs from smaller ones by combining them with the so called "quasiperfect binary arrays". These ideas were extended to the ternary case by Vincent (1989) and Antweiler, Bomer and Luke (1990). The most general m-ary case is dealt with by Jedwab (1992). The importance of these composition theorems can be seen in the work of Vincent (1989), where she constructs a new $CW(96,36)$ using a $CW(24,9)$ and what she calls as a quasiperfect ternary sequence of length 24 and weight 9. Modifying the "orthogonal pieces" ideas of Arasu & Dillon (1999), Arasu, Koukivinos et al (2010) have found a new perfect ternary sequence of length 142 and weight 100, which gives new examples of circulant weighing matrices, answering previously unknown cases affirmatively.

There are several non-existence results for *CW*s (see Arasu and Ma (2001), Arasu and Seberry (1996)). We begin with a "reduction theorem":

Theorem 3.8: (Arasu (1998)) Suppose that a $CW(p^a m, p^2 b u^2)$ exists where p is a prime, a, b, m and u are positive integers satisfying $gcd(p, m) = gcd(p, u) = 1$. Assume $p^f \equiv -1 \pmod{m}$ for an integer f. Then $p = 2$ and $b = 1$ and there exists a $CW(2^{a-1} m, u^2)$.

A *G*-developed weighing matrix *W* is called proper if there is no proper subgroup *H* of *G* such that *W* is *H*-developed.

The next three theorems are due to Arasu and Ma (2001).

Theorem 3.9: (Arasu and Ma (2001)) Let $G = \langle \alpha \rangle \times p^s$, $exp(H) = e, (p(p-1), e) = 1$ and p is a prime greater than 3. Then, a proper *G*-developed $W(|G|, p^{2r})$ for all $r \geq 1$ does not exist.

Theorem 3.10: (Arasu and Ma (2001)) Let $G = \langle \alpha \rangle \times H$ where $o(\alpha) = p$, $exp(H) = e, (p, e) = 1$ and p is a prime greater than 7. If e is odd or e is strictly divisible by 2 or $e \leq (p^2 + 1)/2$, then a proper *G*-developed $W(|G|, p^2)$ does not exist.

Theorem 3.11: (Arasu and Ma (2001)) Let $G = \langle \alpha \rangle \times H$ where $o(\alpha) = p^s, p$ is an odd prime, $exp(H) = e, s > 1$, and $(p, e) = 1$. Then, a proper G-developed $W(|G|, p^2)$ does not exist.

The next theorem is an extension to the abelian case of the cyclic version of a theorem due to Arasu and Seberry (1996):

Theorem 3.12: (Arasu and Hollon (2010)) Suppose that a G-developed $W(|G|, k)$ exists for an abelian group G of order n. Let p be a prime such that $p^{2t}|k$ for some $t \in N$. Further let H be a subgroup of G, of order $|H| =$ n/m. Write $G/H = J \times P$, where P is the cyclic Sylow p-subgroup of G/H and $gcd(p, |J|) = 1$. Assume also that there exists an $f \in Z$ such that $p^f \equiv -1(\text{mod } exp(J))$. Then,

(1) If p divides m, then $2n/m \geq pt$

(2) If p does not divide m, then $n/m \geq pt$

Lengths of perfect ternary sequences (equivalently circulant weighing matrices) of small weights have been classified:

(1) Eades and Hain (1976) Perfect ternary sequence of length n with weight 4 (n ≥ 4) exists if and only if n is divisible by 2 or 7.

(2) Ang, Arasu, Ma & Strassler (2008), Strassler (1997) Perfect ternary sequence of length n with weight 9 exists if and only if n is divisible by 13 or 24.

(3) (Arasu, Leung et al (2006)) Perfect ternary sequence of length n with weight 16 exists if and only if n is divisible by 21 or 31 or 14. (Here n ≥ 21).

Strassler (1997) has a table of parameters (n, k) for $k \leq 100$ and discusses the existence status of the corresponding $CW(n, k)$. Arasu and Gutman (2010) fill over 50 missing entries of Strassler's table. Group weighing matrices have been systematically studied by Ang (2003). Arasu and Hollon (2010) investigate group weighing matrices in the abelian case and provide a table, when weights and group size do not exceed 100.

For some interesting results and conjectures on circulant weighing matrices with large weights, we refer the reader to section 5 of Arasu and Dillon (1999).

We next extract some very interesting recent results of Leung and Schmidt (2010) regarding "finiteness". We need some definitions first:

Let C_v denote the cyclic group of order v. For a divisor w of v, we identify the subgroup of order w of C_v as C_w.

Definition 3.13: Let v be a positive integer, let w be a divisor of v, and let g be a generator of C_v. Every $X \in Z[C_v]$ can be uniquely written in the form:

$$X = \sum_{i=0}^{\frac{v}{w}-1} X_i g^i \text{ with } X_i \in Z[C_w]. \qquad (25)$$

If $X_i X_j = 0$ for all $i \neq j$, then we say that X is orthogonal over C_w. We say that a subset of S of $Z[C_v]$ is orthogonal over C_w if every element of S is orthogonal over C_w.

Definition 3.14: Let v be a positive integer and let $B = \{A_1 \ldots A_k\}$ be a finite set of elements of $Z[C_V]$ with $A_i \neq 0$ for all i. We call B an orthogonal family over C_v if $A_i A_j = 0$ for all $i \neq j$. We call B reducible if there is a proper divisor w of v such that B is orthogonal over C_w and irreducible otherwise. If $\sum_{i=1}^{k} A_i A_i^{(-1)} = n$ when n is an integer, we say that B has weight n.

Definition 3.14: Let v be a positive integer, let w be divisor of v and let $B = \{A_1 \ldots A_k\}$ be an orthogonal family over C_w. We say that $X \epsilon Z[C_v]$ is a coset combination of B if X has the form:

$$X = \sum_{i=1}^{k} A_i g_i \tag{26}$$

where $g_1, \ldots, g_k$ are representatives of distinct cosets of C_w in C_v.

The following is the main result of Leung and Schmidt (2010). It shows that for fixed n, all circulant weighing matrices of weight n can be determined by a finite algorithm.

Theorem 3.15: Let n be a positive integer.

(1) Every circulant weighing matrix of weigh n is a coset combination of an irreducible orthogonal family of weight n.

(2) The number of irreducible orthogonal families of weight n is finite and they can be enumerated by a finite algorithm.

In the case where the weight is an odd prime, they go much further. To formulate their result n this case we need some more terminology.

Definition 3.16: Let $B = \{A_1 \ldots A_k\}$ be an orthogonal family over C_v (recall that this requires $A_i \neq 0$ for all i). We call B nontrivial if $k \geq 2$. We say that B has coefficients $-1,0,1$ if all A_i have coefficients $-1,0,1$ only.

Theorem 3.17: There is no nontrivial orthogonal family with coefficients $-1,0,1$ of an odd prime weight.

Corollary 3.18: Let n be an odd prime power, then there are at most finitely many proper circulant weighing matrices of order n.

We close this section by providing an application of perfect ternary sequences to self dual codes. It is easy to show that perfect ternary arrays are equivalent to weighing matrices that admit a regular group action. If W is a suitable weighing matrix of order n, then it can be shown that $[I_n|W]$ generates a ternary self-dual code of length $2n$. Perfect ternary arrays yield an interesting class of self-dual codes, as in Arasu & Gulliver (2001). Arasu (2004) and Arasu, Chen, Gulliver and Song (2006), who discovered a new ternary self dual code $[96,48,24]$ whose minimum distance 24 beats all the previously known such codes. The best previously known ternary $[96,48]$ code has a minimum distance 19. Their new code has the generator matrix $[I_n|W]$, where $n = 48$ and W is the negacyclic matrix whose first row is

122221211111112112212211012211122111212121111212

The aforementioned initial row is theoretically obtained using Theorem 3 of Arasu, Chen, Gulliver and Song (2006) and the symbol “2” in the first row denotes -1. It turns out that the codes of Arasu, Chen, Gulliver and Song (2006) are equivalent to the Pless symmetry codes (Pless (1972)). A proof of this equivalence is in Arasu, Chen, Gulliver and Song (2006). Computing its minimum distance as 24 took 53 days of computing time.

4. Perfect quaternary arrays

Arasu & de Launey (2001) and Arasu, de Launey and Ma (2002) investigate complex Hadamard matrices and perfect quaternary arrays.

A perfect quaternary array (PQA) is a $t_1 \times t_2 \times \dots t_n$ array of fourth roots of unity $\left(a_{i_1 i_2 \dots i_n}\right)$ with perfect periodic autocorrelation properties, i.e.

$$\sum a_{i_1 i_2 \dots i_n} \, a_{i_1+c_1, i_2+c_2, \dots i_n+c_n} = 0 \qquad (27)$$

whenever the offset $c = (c_1, c_2, \dots, c_n)$ is non-zero.

Examples:

(1) $(1, \mathrm{i})$ is a 1×2 is a perfect quaternary array.

(2) $(1, \mathrm{i}, -1, \mathrm{i})$ is a 1×4 is a perfect quaternary array.

(3) $(1, 1, \mathrm{i}, 1, 1, -1\,, \mathrm{i}, -1)$ is a 1×8 perfect quaternary array.

The known 2-dimensional examples of perfect binary arrays have their dimensions restricted to $2^a 3^b \times 2^{a+c} 3^b$, where $c = 0 \text{ or } 2$, $a \geq 0, b \geq 0$, and $b = 0$ unless $2a + c \geq 2$. But the answer to the existence for perfect quaternary arrays appears to be very different.

Arasu & de Launey (2001) show: perfect quaternary arrays are equivalent to relative difference sets in $Z_4 \times Z_{t_1} \times Z_{t_2} \times \dots \times Z_{t_n}$, relative to the subgroup $\langle X^2 \rangle$ which is contained in $\langle X \rangle = Z_4$. Using this nice connection and algebraic techniques, several new families of perfect quaternary arrays have been constructed.

A few examples have already been discovered. Some of the new arrays obtained have dimensions: 3×6, 3× 24, 6×12, 6×48, 12×24, 12×96, 24×48, 48×96, 51× 102, 14×14, 7×28, 14×28, 28×28, 7×56, 14×56, 28×56, 21×84, 42×42, 42×84, 84×84, 18×9, 72×9 and 54×27.

Examples of Two dimensional Perfect Quaternary Arrays

Example 4.1 (Arasu & de Launey [2001]): A PQA(2,2) is shown below:

$$\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix} \qquad (28)$$

Example 4.2 (Arasu & de Launey [2001]): A PQA(3,6) is displayed below:

$$\begin{bmatrix} -1 & i & -1 & 1 & 1 & 1 \\ -1 & -i & -i & -1 & 1 & -1 \\ -i & 1 & -i & 1 & i & i \end{bmatrix} \tag{29}$$

Example 4.3: A PQA(14,14) is given in Arasu & de Launey [2001].

It should be possible to obtain several new classes of quaternary arrays , surely for dimensions higher than 2, using the techniques of Arasu and (2001), as their investigation focused only on the 2-dimensional case and routine generalization must yield results for higher dimensions.

PQA's are very closely connected to complex Hadamard matrices. We now describe how any PQA (s,t) leads to a complex Hadamard matrix with the bicyclic group $Z_s \times Z_t$ acting regularly. The concept of regular action of a group on a combinatorial object is important in combinatorial mathematics, but here it is of peripheral interest. A complex Hadamard matrix of order n is an $n \times n$ matrix C, say, whose entries are fourth roots of unity and which satisfies the equation

$$CC^* = nI_n \tag{30}$$

Here C^* is the Hermitian adjoint of C. It is obtained by forming the transpose of C and replacing each entry by its complex conjugate.

For each pair of integers u and v, where $0 \le u, v < st$, define the integers u_1, u_2, v_1 and v_2 by the relations $u = u_1 + su_2$ and $v = v_1 + sv_2$, where $0 \le u_1, v_1 < s$ and $0 \le u_2, v_2 < t$, and set $c\,(u,v) = a\,(u_1 - v_1, u_2 - v_2)$ where the arithmetic in the indices of a is done modulo s and t respectively.

Now suppose the $s \times t$ array $A = \big(a(i,j)\big)$ is a PQA (s,t). Define the $st \times st$ matrix C to be the matrix whose (u,v)-th entry is $c(u,v)$. Then the (u,w)-th entry of CC^* is

$$\textstyle\sum_{v=0}^{st-1} c(u,v)\,\overline{c(w,v)}$$

$$= \textstyle\sum_{v_1=0}^{s-1} \sum_{v_2=0}^{t-1} a(u_1 - v_1, u_2 - v_2)\,\overline{a(w_1 - v_1, w_2 - v_2)} \tag{31}$$

Putting $l_1 = u_1 - v_1$ and $l_2 = u_2 - v_2$, the right hand side becomes

$$\textstyle\sum_{l_2=1}^{s-1} \sum_{l_1=0}^{t-1} a(l_1, vl_1)\overline{a(w_1 - u_1 + l_1, w_1 - uv_2 + l_2)} =$$

$$\begin{cases} st \text{ if } w_1 = u_1 \text{ and } w_2 = u_2 \\ 0 \qquad\quad \text{otherwise} \end{cases} \tag{32}$$

Hence, $CC^* = st\, I_{st}$, and C is indeed a complex Hadamard matrix of order st. The additional property that $c(i,j)$ depends only on the values of $u_1 - v_1$ (mod s) and $u_2 - v_2$ (mod t) confers on C the aforementioned $Z_s \times Z_t$ regular action.

Complex Hadamard matrices were first discussed in Turyn (1970). The matrix $c = \big(C_{i,j}\big)$ is said to be circulant if, for all $i, j = 0,1,\ldots,n$–$1, c_{i,j} = c_{0,j-i}$. Here the difference j–i is computed modulo n.

Example 4.4: The circulant matrices with first rows

$(1, \mathrm{i})$

$(1, -\mathrm{i}, 1, \mathrm{i})$

$(1,1, \mathrm{i}, 1,1, -1, \mathrm{i}, -1)$

$(1,1, \mathrm{i}, -\mathrm{i}, \mathrm{i}, 1,1, \mathrm{i}, -1,1, -\mathrm{i}, -\mathrm{i}, -\mathrm{i}, 1, -1, \mathrm{i})$

are complex Hadamard matrices of the respective orders $n = 2,4,8$ and 16.

The following are well known:

Theorem 4.5: If there is a circulant complex Hadamard matrix of order n, then n is the sum of two squares.

Theorem 4.6: (Turyn (1970)) There are no circulant complex Hadamard matrices of order 2^t for $t > 4$ or $2p^n$ where p is an odd prime.

Using Turyn type arguments (Turyn (1965)) and techniques of (Ma (1985)), Arasu, and Ma (2002) prove several nonexistence theorems. We only state a few of them here.

Theorem 4.7: (Arasu, and Ma (2002)) Suppose $p \equiv 1 \ (\mathrm{mod}\ 4)$ is a prime. Let $\alpha \varepsilon \left[0, \frac{p-1}{2}\right]$ be an integer such that $\alpha^2 \equiv -1 \ (\mathrm{mod}\ p)$. Let t be an odd integer, $(t, p) = 1$. If there exists a circulant complex Hadamard matrix of order $2tp$, then $t \geq \frac{p}{\alpha+1}$.

Lemma 4.8: (Arasu, and Ma (2002)) Let $v = uw$ with $(u, w) = 1, q$ an integer relatively prime to v and H an abelian group of order v which contains an element h of order w. If $y \in Z[\zeta_q][H]$ satisfies $\chi(y) \in f(\zeta_w) Z(\zeta_{qv})$, for all characters χ of H with $\chi(h) = \zeta_w$, where $f(X)$ is a polynomial in $Z[\zeta_q][H]$ such that $f(\zeta_w) Z[\zeta_{qv}]$ and $uZ[\zeta_{qv}]$ are relatively prime, then

$$y = f(h) x_0 + \sum_{i=1}^{r} \left(h^{w/p^i}\right) x_i \tag{33}$$

where $x_0, x_1, \ldots x_r \in Z[\zeta_q][H]$ and $p_1, p_2, \ldots., p_r$ are all prime divisors of w.

Lemma 4.9: (Arasu, and Ma (2002) Let $G = \langle \alpha \rangle$ be a cyclic group of order $v = 4w$. Let p be an odd prime such that $p \equiv 1 \ (mod\ 4)$, $p^t || v$ and $\phi\left(\frac{v}{p^t}\right) = \left(2ord_{\frac{v}{p^t}}\right)$. If $y \in Z[G]$ satisfies $\chi(y)\chi(y) \equiv 0 \bmod p^f$ for a character χ of G of order v, and if one of the following is true:

(1) $\mathrm{f} \geq 2$

(2) $\mathrm{t} = 0$

(3) $\chi_1(\mathrm{y}) \overline{\chi_1(\mathrm{y})} \neq 0 \bmod \mathrm{p}^2$ for a character χ_1 of G of order $\mathrm{v}/\mathrm{p}^\mathrm{t}$, then

$$y = \left(a + b\alpha^{v/4}\right)x_0 + \sum_{i=1}^{r} \langle \alpha^{v/q_i} \rangle x_i \tag{34}$$

where $x_0, x_1, \ldots x_r \in Z[G], q_1, q_2, \ldots, q_r$ are all prime divisors of v and a, b are integers relatively prime to p such that $a^2 + b^2 = p^e$ with $e = [f/2]$ if $f \geq 2e = 1$ if $f = 1$. (Note that $\{a, b\}$ are unique up to ±signs and permutations.)

Lemma 4.10: (Arasu, and Ma (2002)) Let $G = \langle \alpha \rangle \times H$ be an abelian group where $o(\alpha) = 2^s, s \geq 2$ and $|H|$ is odd. Suppose 2 is self-conjugate modulo exp (H). If $y \in Z[G]$ satisfies $\chi(y)\overline{\chi(y)} \equiv 0 \; mod \; 2^r$ mod 2^r for all characters χ which are nonprincipal on $\langle \alpha \rangle$, then

$$y = 2^{r_1}\left(1 + \alpha^{s^{s-2}}\right)^{r-2r_1} x_0 + \langle \alpha^{2s-1} \rangle x_1 \tag{35}$$

where $x_0, x_1 \in Z[G]$ and $r_1 = [r/2]$.

(Here 2 is self conjugate modulo $\exp(H)$ means $2^l \equiv -1$ (mod exp (H)) for some integer l).

For non-existence results, we have only stated the above sample lemmas (further extensions of the lemmas are likely and would yield stronger results). (See Arasu, de Launey and Ma (2002) and Arasu and Ma (2001) for more such results).

Using Schmidt's results (Schmidt (1999, 2002)), we obtain the following:

Theorem 4.11: (Arasu, and Ma (2002)). Let P be a finite set of primes, and let $N(P)$ be the set of integers whose prime divisors all lie in P. Then there are finitely many circulant complex Hadamard matrices with orders in $N(P)$.

We conclude this section by making the following remark:

Remark: The following eleven orders of circulant complex Hadamard matrix up to 1000 have yet to be excluded: 260, 340, 442, 468, 520, 580, 680, 754, 820, 884, 890. In view of the conjecture that there is no circulant Hadamard matrix of order greater than 4, it is tempting to conjecture that there is no circulant complex Hadamard matrix of order greater than 16.

5. *p*-ary sequences

Ma and Ng (2009) follow the approach of Turyn (1968) and study the complex p-ary sequences, where p is an odd prime.

Definition 5.1: Let $a = (a_0, a_1, \ldots)$ be a complex sequence. The sequence a is called a complex m-ary sequence if $a_i = {\zeta_m}^{b_i}$ where ζ_m is a primitive m-th root of unity in $\mathbb{C}$ and $b_i \in \{0,1,\ldots,m-1\}$. Also a is said to be periodic with period n, if $a_i = a_{(i+n)}$ for all $i \geq 0$. Suppose a is a periodic complex m-ary sequence of period n. The autocorrelation function C of a is defined by

$$\mathrm{C(t)} = \sum_{j=0}^{n-1} a_j \overline{a_{j+t}}, \text{ for } \mathrm{t} = 0,1,\ldots,(\mathrm{n}-1). \tag{36}$$

All autocorrelation coefficients $C(t)$ with $t \not\equiv 0 \pmod{n}$ are called out-of-phase autocorrelation coefficients. A periodic sequence a is said to have a two-level autocorrelation function if all the out-of-phase autocorrelation coefficients are equal to a constant γ. In particular, the sequence a is called a perfect sequence if $\gamma = 0$ and a nearly perfect sequence if $|\gamma| = 1$.

The binary perfect and nearly perfect sequences, i.e., $m = 2$, were discussed in Sections 1 and 2. The case $m = 4$ has been studied by Turyn (1970) and Arasu, and Ma (2002). (See Section 4 of this survey). In this section, we shall discuss the case when $m = p$ where p is an odd prime, basically summarizing the results of Ma and Ng (2009).

Theorem 5.2: (Ma and Ng (2009)) Let p be a prime and let $a = (a_0, a_1, \ldots)$ be a periodic sequence for period n where $a_i = \zeta_p^{b_i}$ and $b_i \in \{0,1,\ldots,p-1\}$. Let $G = H \times P$ be an abelian group where $H = \langle h \rangle$, $P = \langle g \rangle$, $o(h) = n$, and $o(g) = p$. Then a is a perfect sequence if and only if $\{D = g^{bi}h^i | i = 0,1,\ldots,n-1\}$ is an $(n,p,n,n/p)$-relative difference set in G relative to P, i.e.,

$$DD^{(-1)} = n + n/p(G - P) \tag{37}$$

In view of Theorem 5.2, to study complex p-ary perfect sequences is equivalent to study the $(n,p,n,n/p)$-relative difference set. We list below some examples found from the literature. We are only interested in the case where p is an odd prime.

Example 5.3: (Ma and Schmidt, 1995, Theorem 2.2.9) Let $\boldsymbol{G} = \mathbb{Z}_{\boldsymbol{p}} \times \mathbb{Z}_{\boldsymbol{p}}$ and

$$\mathrm{D} = \{(\mathrm{x}, \mathrm{x}^2) | \mathrm{x} = 0,1,\ldots,\mathrm{p}-1\} \tag{38}$$

Then D is a $(p,p,p,1)$-relative difference set in G relative to $P =< (0,1) >$. So we have a complex p-ary perfect sequence of period p^2:

$$(1, \zeta_\mathrm{p}, \zeta_\mathrm{p}^{2^2}, \ldots, \zeta_\mathrm{p}^{(\mathrm{p}-1)^2}, \ldots) \tag{39}$$

Example 5.4: (Ma and Schmidt, 1995, Theorem 2.3) Let $\boldsymbol{G} = \mathbb{Z}_{\boldsymbol{p}} \times \mathbb{Z}_{\boldsymbol{p}}$ and

$$\mathrm{D} = \cup_{\mathrm{x}=0}^{\mathrm{p}-1} \cup_{\mathrm{y}=0}^{\mathrm{p}-1} (\mathrm{x} + \mathrm{py}, \mathrm{xy}) \tag{40}$$

Then D is a (p^2, p, p^2, p)-relative difference set in G relative to $P =< (0,1) >$. So, we have a complex p-ary perfect sequence of period p^2.

$$\left(\zeta_\mathrm{p}^{\mathrm{b}_0}, \zeta_\mathrm{p}^{\mathrm{b}_1}, \ldots, \zeta_\mathrm{p}^{\mathrm{b}_{(\mathrm{p}^2-1)}}\right) \text{where } \mathrm{b_i} = xy \text{ for } \mathrm{i} = \mathrm{x} + \mathrm{py}, 0 \le \mathrm{x}, \mathrm{y} \le \mathrm{p} - 1 \tag{41}$$

Definition 5.5: Let a be a periodic complex m-ary sequence.

(1) If the out-of-phase autocorrelation coefficients of a are all equal to -1, we say that a is a type I nearly perfect sequence.

(2) If the out-of-phase autocorrelation coefficients of a are all equal to 1, we say that a is a type II nearly perfect sequence.

Theorem 5.6: (Ma and Ng (2009)) Let p be a prime and let $a = (a_0, a_1, \ldots)$ be a periodic sequence of period of n where $a_i = \zeta_p^{b_i}$ and $b_i \epsilon \{0,1,\ldots,p-1\}$. Let $G = H \times P$ be an abelian group where $H =< h >$, $P =< g >$, $o(h) = n$, and $o(g) = p$. Define $D = \{g^{b_i} h^i \mid i = 0,1,\ldots,n-1\}$. Then

(1) a is type I nearly perfect sequence if and only if D is an $(n, p, k, \frac{n+1}{p} - 1, 0, \frac{n+1}{p})$- direct product difference set in G relative to H and P, i.e.,

$$\mathrm{DD}^{(-1)} = (\mathrm{n}+1) - \mathrm{H} + \frac{\mathrm{n}+1}{\mathrm{p}}(\mathrm{G}-\mathrm{P}) \qquad (42)$$

and

(2) a is a type II nearly perfect sequence if and only if D is an $(n, p, k, \frac{n-1}{p} + 1, 0, \frac{n-1}{p})$-direct product difference set in G relative to H and P, i.e.,

$$DD^{(-1)} = (n-1) + H + \frac{n-1}{p}(G-P) \qquad (43)$$

Example 5.7: (see Helleseth and Kumar, (1998), Section 3.1) Let p be a prime and q be a power of p. Let F_q be the finite field of order q and F_p be the subfield of F_q of order p. Then

$$D = \{(x, tr(x)) | x \in F_q^x\} \qquad (44)$$

is a $(q-1, p, q-1, \frac{q}{p} - 1, 0, \frac{q}{p})$ -direct product difference set $\mathrm{F}_q^x \times \mathrm{F}_p$ relative to $\mathrm{F}_q^x \times \{0\}$ and $\{0\} \times \mathrm{F}_p$ where F_q^x is the group of the units of F_q. So we have a complex p-ary type I nearly perfect sequence of period $q-1$:

$$(\zeta_{\mathrm{p}}^{\mathrm{tr}(1)}, \zeta_{\mathrm{p}}^{\mathrm{tr}(\mathrm{z})}, \ldots, \zeta_{\mathrm{p}}^{\mathrm{tr}(\mathrm{z}^{\mathrm{q}-2})}, \ldots) \qquad (45)$$

where z is a primitive element of F_q.

6. p-ary sequences via Gauss sums

In this section, we discuss a few important results on some new constructions of p-ary perfect sequences due to Arasu, Dillon and Player (2010). Detailed proofs of their results on new constructions of p-ary sequences using Gauss sums and Stickelberger combinatorics are provided in Arasu, Dillon and Player (2010). Here we provide only some of the main ideas of their construction methods.

We begin by reformulating an earlier definition for "complex" valued sequences.

For a sequence $S = (a_i), i = 0,1,2,\ldots,(n-1)$, of length n, where each a_i is a complex number, its periodic autocorrelation coefficients are defined by:

$$R_s(t) = \sum_{j=0}^{n-1} a_j \overline{a_{j+t}}, \ \ for \ \ t = 0,1,\ldots,(n-1) \qquad (46)$$

where the subscripts are taken modulo n. We shall investigate p-ary sequences (p any prime), whose entries are p-th roots of unity satisfying

$$R_s(t) = \begin{cases} -1 & if\ t \not\equiv 0 \pmod{n} \\ n & \text{otherwise} \end{cases} \tag{47}$$

We alert the reader that p-ary sequences that satisfy (47) are referred to as almost perfect p-ary sequences of type I as we saw in section 5. But we shall call these "perfect" sequences in this section.

Let $q = p^r$ for some prime p. Throughout this section, we will assume that the group G is either $F_{q^m}{}^*$ or $F_{q^m}{}^*/F_q{}^*$, which is a cyclic group.

We now define the well-known notion of a perfect sequence using group rings. Note that this definition implies that all the out-of-phase autocorrelations are minus one.

Definition 6.1: (Perfect Sequence, abbr. PS) Define R to be an arbitrary subring of C generated by some set S. S is usually taken to be the set of n-th roots of unity for some positive integer n. Let P be an element of $R[G]$ whose coefficients are from S. Then P is called a perfect sequence in G if

$$P\ P^* = (|G| + 1) - G \tag{48}$$

or equivalently if

$$\forall\chi, |\chi(P)|^2 = \begin{cases} |G| + 1 & if\ \chi \neq \chi_0 \\ 1 & if\ \chi = \chi_0 \end{cases} \tag{49}$$

Here C denotes the field of complex numbers.

Example: (m-sequence) Let $G = F^*{}_p d$ for some prime p and d a positive integer. Then $M = \sum_{\lambda \in G} \zeta_p{}^{Tr(\lambda)}\, \lambda$ is perfect.

Throughout this paper, F_m denotes a finite field with m elements.

It can be easily seen that the above definition of perfect sequences is equivalent to the standard one.

Definition 6.2: (Generalized Weighing Matrix, abbr.. GWM) Let R be an arbitrary subring of C generated by some set S where S is taken to be the set of n-th roots of unity for some positive integer n together with $\{0\}$. Let A be an element of $R[G]$ whose coefficients are from S. Let k be some positive integer. A is called a generalized weighing matrix of weight k in G if

$$A\ A^* = k \tag{50}$$

or equivalently if

$$(\forall\chi)|\chi(A)|^2 = k \tag{51}$$

It is well-known that binary perfect sequences are equivalent to difference sets with Singer parameters. But the p-ary case (for an odd prime p) behaves very differently; we are able to show that perfect p-ary sequences are equivalent to a class of generalized weighing matrices, as defined above, which in turn give rise to a class of relative difference sets which are extensions of Singer parameters (i.e. the images of these relative difference sets under the canonical homomorphim when mod out by the "forbidden" subgroup is a difference set with Singer parameters (up to complementation)). This was the reason why we have introduced the above definitions using the group ring notation.

There has been much research activity in the binary case area during the last decade. All of the known binary perfect sequences (equivalently cyclic difference sets with Singer parameters), except for the GMW-sequences, the ones that arise from cyclotomy, and the Hall sets, are contained in the following two theorems:

Theorem 6.3: (Dillon, Dobbertin (2004)): Let k be any integer in the range $l \leq k \leq m/2$ which is coprime to m. Let $d = 2^{2k} - 2^k + 1$ and let $\Delta_k(x) = (x+1)^d + x^d + 1$ for all $x \in L$. Then the punctured image $B_k = \{\Delta_k(x) | x \in F_{2^m}\} \backslash \{0\}$ of Δ_k corresponds to a perfect binary sequence of length $2^m - 1$. Moreover, these perfect sequences are pairwise inequivalent.

Theorem 6.4: (Dillon, Dobbertin (2004)) Let m be an integer which is not divisible by 3, and let k be a natural number such that $3k \equiv 1 \text{ or} - 1 \ (mod\ m)$. Let $d = 2^{2k} - 2^k + 1$ and let $\Delta_k(x) = (x+1)^d + x^d$ for all $x \in L$. Let

$$N = \begin{cases} \{(x+1)^d + x^d : x \in F_{2^m}\} & \text{if } m \text{ is even.} \\ F_{2^m} \backslash \{(x+1)^d + x^d : x \in F_{2^m}\} & \text{if } m \text{ is odd.} \end{cases} \tag{52}$$

Then $N^* = \mathrm{N} \backslash \{0\}$ corresponds to perfect binary sequences.

Researchers have become interested in the p-ary case, where p is an odd prime. M-sequences and the GMW sequences are two well understood families of perfect p-ary sequences of length $p^d - 1$ which have been known for several decades. Aside from these, there are perfect sequences due to the work of Dillon (2002), Helleseth, Kumar and Martinsen (2001), Helleseth and Gong (2002), and Lin (1998), as stated below:

Theorem 6.5: (Dillon (2002)) Let p be any odd prime and let $L = GF(p^m), m > 1\ odd$. For every even integer k, $0 \leq k \leq m - 1$, let $g_k : GF(p^m) \rightarrow GF(p)$ be the quadratic form given by $g_k\left(x + x^{p^{2k}}\right) = Tr\left(x^{p^k+1}\right)$ and let h_k be the related function given by $h_k(x) = x^f g_k(x)$, where f is the odd part of $p^m - 1$. Then $\{a_t\} = \{h_k(\omega^t)\}$ is perfect.

Theorem 6.6: (Helleseth, Gong (2002)) Let α be a primitive element of F_{p^n}. Let $n = (2m+1)k$ and let $s, 1 \leq s \leq 2m$ be an integer such that $gcd(s, 2m+1) = 1$. Define

$$f(x) = \textstyle\sum_{i=0}^{m} u_i\, x^{(2t+1)/2} \tag{53}$$

and let $b_0 = 2u_0, u_i = b_{2i} = b_{2m+1-2i}$ for $i = 1,2,\ldots,m$. Suppose $b_0 = \pm 1$ and $b_{is} = (-1)^t$ for $i = 1,2,\ldots,m$, then the sequence over F_p defined by

$$s(t) = Tr_n\big(f(\alpha^t)\big) \tag{54}$$

is perfect, where indices of b_{is} are taken mod $2m + 1$.

Theorem 6.7: (Helleseth, Gong (2002)) Let α be a primitive element of F_pn. Let $n = (2m + 1)k$ and let $1 \leq s \leq 2m$ be an integer such that $gcd(s, 2m + 1) = 1$. Define

$$f(x) = \sum_{i=o}^{m} u_2\, x^{(q^{2i+1}+1)/(q+1)} \tag{55}$$

and let $b_0 = 2u_0, u_i = b_{2i} = b_{2m+1-2i}$ for $i = 1,2, \dots, m$. Suppose $b_0 = \pm 1$ and $b_{is} = (-1)^i$ for $i = 1,2, \dots, m$, then the sequence over F_p defined by

$$s(t) = Tr_n\big(f(\alpha^t)\big) \tag{56}$$

is perfect, where indices of b_{is} are taken mod $2m + 1$.

Theorem 6.8: (Helleseth, Kumar, Martinsen (2001)) Let $d = 3^{2k} - 3^k + 1$, and let a be a primitive element of $F_{3^{3k}}$. Then the sequence $\{Tr(a^t + a^{dt})\}_{t=1,2,\dots,3^{3k}-1}$ is perfect.

Finally, Lin has made the following conjecture: (see Lin 1998)

Conjecture 6.9: (Lin (1998)) Let $d = 2 \times 3^m + 1$, and let a be a primitive element of $F_{3^{2m+1}}$. Then the sequence $\{Tr(a^t + a^{dt})\}_{t=1,2,\dots,3^{2m+1}-1}$ is perfect.

These recent results and Lin's conjecture, having as they do rather tantalizing similarities, have stimulated a lot of interest. The proofs of the known results are elegant but *ad hoc*. So far these direct methods have not yielded a proof of Lin's conjecture. Recently, Arasu, Dillon and Player (2010) have proved Lin's conjecture. The method of proof is very different from the standard methods. The new approach is described in what follows.

For convenience, we define the Gauss and Jacobi sums now: (here x and ϕ are multiplicative characters of the finite field in question. By convention, $x(0) = \phi(0) = 0$).

Definition 6.10: (Gauss Sum) The Gauss Sum on χ over F_pd denoted $G(\chi)$ is defined to be

$$G(\chi) \coloneqq \sum_{x \,\in\, F_p d} \chi(x)\, \varsigma^{Tr(x)} \tag{57}$$

(Here ς is a primitive p-th root of unity and χ is a multiplicative character of F_pd with $\chi(0) = 0$.

Definition 6.11: (Jacobi Sum) The Jacobi Sum on χ and ϕ denoted $J(\chi, \phi)$ is defined to be:

$$J(\chi, \phi) \coloneqq \sum_{x \,\in\, F_{p^d}} \chi(x)\, \phi(1 - x) \tag{58}$$

(Here χ and ϕ are multiplicative characters of F_{p^d}, with $\chi(0) = \phi(0) = 0$)

Our basic tool is the following well-known result in algebraic number theory (see Berndt et al (1998) or Lidl et al (1997), for instance):

<u>Theorem 6.12</u>: (Stickelberger`s congruence) Let $F = GF(p^d)$. Then, for any integer a not divisible by $p^d - 1, v(\,G(\omega^{-a})) = s(a)$, where G denotes the Gauss sum, ω denotes the Teichmueller character and $s(a)$ denotes the p-adic weight of the integer a after it is reduced modulo $p^d - 1$. Here v denotes the valuation function at a prime ideal P lying above p in the number field that contains the underlying Gauss sum.

For more details regarding the above theorem, please refer to Berndt, et al (1998), Evans et al (1999) or Arasu and Player (2003) .

Our next task is to explain a perfect sequence existence condition.

In the study of group developed designs, one may start with an object and try to prove that the group developed design has the required auto-correlation properties. We take the opposite approach in this paper. Start with an object in Fourier space which has the correct auto-correlation properties and try to show that its Fourier inverse has coefficients in the required subset.

Let p be a prime, d a positive integer and let $G = \mathbb{F}^*{}_{p^d}$. Define $P = P_{[a,b,c]}$ by

$$\chi\left(P_{[a,b,c]}\right) = \frac{G(\chi^a)G(\chi^c)}{G(\chi^b)} \tag{59}$$

Let $l = (b, p^d - 1)$ and let L be the unique index l subgroup of G. Then

$$\begin{aligned}&\chi^{(lL)} = \chi\left(G^{(l)}\right) = \chi^{l(G)}\\ &= \begin{cases} p^d - 1 & if \quad \chi^l = \chi_0 \\ \;\;0 & if \quad \chi^l \neq \chi_0 \end{cases}\end{aligned} \tag{60}$$

Applying (60), $\chi(\,M^{(t)}) = G(\chi^t), \chi(M^*) = \overline{G(\chi)}$ and Fourier inversion we find

$$P_{[a,b,c]} = \frac{(1+lL)(M^{(a)}M^{*(b)}M^{(c)})}{p^d} \tag{61}$$

Set $N = p^d P_{[a,b,c]}$. We can clearly remark that

<u>Remark 6.13</u>: $N \in \mathbb{Z}[\zeta_p]G \; and \; P \in \mathbb{Q}[\zeta_p]G$

Our primary tool in the new constructions of p-ary perfect sequences is given in the next theorem:

<u>Theorem 6.14</u>: The following are equivalent:

(1) $P_{[a,b,c]}$ is a perfect sequence.

(2) The coefficients of $P_{[a,b,c]}$ are p-th roots of unity.

(3) For all primes $\mathfrak{B}_i$above p in $\mathbb{Z}[\zeta_p, \zeta_{p^d-1}]$ and non-principal characters χ of G, $v_{\mathfrak{B}_i}(\chi(P)) > 0$.

(4) For all non-principal characters $\chi \ of \ G, v_{\mathfrak{B}}(\chi(P)) > 0$.

(5) For all $x, 0 < x < p^d - 1, s(ax) - s(bx) + s(cx) > 0$.

Judicious choices of a, b and c as given in the next three theorems now yield new classes of p-ary perfect sequences. The first family works for $p = 2$, the second for any odd prime p, whereas the last one requires the said prime to be 3.

Theorem 6.15: Let $p = 2$ and $d > 2$ be an integer. Also let r be any integer with $(r, d) = 1$. Assume that d and r of opposite parity. Then $P[1, -3, (2^r + 1)]$ is a perfect sequence over $GF(2^d)\setminus\{0\}$.

Remark 6.16: When $p = 2$ and $(r, d) = 1$, $P_{[1,-3,2^r+1]}$ can be shown to be the binary Dillon and Dobbertin (2004) sequences. Kashyap (2005) has proved Theorem 6.15 independently using similar methods via Stickelberger combinatorics.

Theorem 6.17: Let p be an odd prime. Let d be an integer, $d > 2$. Let r be an integer with $(p^r + 1, p^d - 1) = 2$, or equivalently $d/(r, d)$ is odd. Then $P[1, -2, p^r + 1]$ is a perfect sequence over $GF(\mathrm{p^d})\setminus\{0\}$.

Remark 6.18: It can be shown that odd prime p-ary perfect sequences of Dillon (2002), Helleseth and Gong (2002), Helleseth, Kumar and Martinsen (2001) arise as $P_{[1,-2,p^r+1]}$ of theorem 6.17 for each r with $d/(r, d)$ odd.

Theorem 6.19: Let $p = 3$ and $d > 2$ be an integer. Also let r be any integer with $(r, d) = 1$. Then

$$P[1, -2, ½(3^r + 1\ )] \text{ is a perfect sequence over } GF(3^d)\setminus\{0\} \qquad (62)$$

If, furthermore, d is odd, $P[1 + (3^d - 1)/2, -2, ½(3^r + 1) + (3^d \ - 1)/2]$ is a perfect sequence over $GF(3^d)\setminus\{0\}$

Remarks 6.20:

(1) The two ternary perfect sequences $P_{[1,-2,\frac{3^r+1}{2}]}$ and $P_{[1+\frac{3^d-1}{2},-2\,,\frac{3^r+1}{2}+\frac{3^d-1}{2}]}$ of Theorem 6.19 project to the same difference set.

(2) Arasu, Dillon and Player (2010) have shown that these families prove the conjectures of Ludkovski and Gong (2001).

(3) By focusing attention on the trace expansion of the perfect sequence in the last family with $r = (d - 1)/2$, Arasu, Dillon and Player (2010) show that it is equivalent to the Lin sequence (i.e. $P \sim \left(w^{\left(Tr(x+x^d)\right)}\right)$, where $d = 2 * 3^r + 1$). Thus we obtain:

Corollary 6.21: The Lin Conjecture (1998) is true.

Remarks 6.22:

(1) Arasu, Dillon, Player (2010)) provide the first proof of this very important result.

(2) Arasu, Dillon, Player (2010) do a lot more than what is stated in the above theorems. They also prove the inequivalence and compute the ranks in certain cases.

We end this paper with the following:

Question: Is there a more direct proof of the Lin Conjecture?

Acknowledgement

The author wishes to thank John F. Dillon, Cunsheng Ding, Tor Helleseth, Dieter Jungnickel, Siu Lun Ma, Alexander Pott, and Bernhard Schmidt for their valuable suggestions.

References:

[1] Ang, M.H., Group weighing matrices, Ph.D. Thesis, National University of Singapore, Singapore (2003).

[2] Ang, M.H, Arasu, K. T., Ma, S.L., and Strassler, Y., *Study of proper circulant weighing matrices with weight 9*, Discrete Math. 308, no. 13 (2008) pp. 2802-2809.

[3] Antweiler, M., Bömer, L., and Lüke, H. D., *Perfect ternary arrays*, *IEEE* Trans. Inf. Theory 36 (*1990*) pp. 696-705.

[4] Arasu and Pott, *Perfect binary sequences of even period*, Journal of Statistics and Applications, Vol. 4 No. 2-3, Pages 169-178, (2009).

[5] Arasu, K. T. and Gulliver, T.A., *Self-dual codes over Fp and weighing matrices*, IEEE Trans. Inform. Theory 47 (2001) pp. 2051-2055

[6] Arasu, K.T. Abstract of talk, XXVIIth Ohio State-Denison Mathematics Conference, June 11–13, 2004, The Ohio State University, Columbus, Ohio, (2004).

[7] Arasu, K. T. Leung, Ka Hin, Ma, Siu Lun, Nabavi, Ali, Ray-Chaudhuri, D. K., *Circulant weighing matrices of weight* 2^{2t}. Des. Codes Cryptogr. 41, no. 1, (2006) pp. 111-123.

[8] Arasu, K. T., and Ma, Siu Lun, *Some new results on circulant weighing matrices*, J. Algebraic Combin. 14, no. 2 (2001) pp. 91-101.

[9] Arasu, K. T., and Seberry, Jennifer, *Circulant weighing designs*, in J. Combin. Des. 4, no. 6 (1996) pp. 439-447

[10] Arasu, K. T., , Warwick; Ma, S. L. *On circulant complex Hadamard matrices*. Des. Codes Cryptogr. 25, no. 2, (2002) pp. 123-142

[11] Arasu, K. T., Dillon, J. F., *Perfect ternary arrays. Difference sets, sequences and their correlation properties* (Bad Windsheim, 1998), pp. 1-15, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 542, Kluwer Acad. Publ., Dordrecht, (1999).

[12] Arasu, K. T., Ma, S. L., and Voss, N. J., *On a class of almost perfect sequences*, J. Algebra 192, no. 2, (1997) pp. 641-650.

[13] Arasu, K. T.; Leung, Ka Hin; Ma, Siu Lun, and Nabavi, Ali; Ray-Chaudhuri, D. K., *Determination of all possible orders of weight 16 circulant weighing matrices*. Finite Fields Appl. 12, no. 4, (2006) pp. 498-538.

[14] Arasu, K.T. and Gutman, A.J.: Circulant Weighing Matrices, Cryptogr. Commun., (in press), 2010.

[15] Arasu, K.T. and Hollon, J.R., Group weighing matrices (2010), Preprint.

[16] Arasu, K.T. and Little, D., Balanced perfect sequences of period 38 and 50, (2010), Preprint.

[17] Arasu, K.T. and Pott, A., *Perfect binary sequences of even period*, Journal of Statistics and Applications, 4 (2009) pp. 169-178.

[18] Arasu, K.T. and Pott, A., *Theory of difference sets*, In: Encyclopedia for Electrical and Electronics Engineering, Ed. J. Webster, Willey, New York, Vol. 21, (1999), pp. 682-694.

[19] Arasu, K.T. and Xiang, Q., *On the existence of periodic complementary binary sequences*, Designs, Codes & Cryptography, 2 (1992) pp. 257-266.

[20] Arasu, K.T., Chen, Y.Q., Song W., and Gulliver, T.A., *Self-Dual Codes over F_3 and Negacirculant Conference Matrices*, Proc. IEEE Int. Symp. Inform. Theory, (July 2006) pp. 1301-1304.

[21] Arasu, K.T., Chen, Yu Qing, Dillon, J.F., Liu, Xiaoyu, and Player, Kevin J., *Abelian difference sets of order n dividing λ*, Des. Codes Cryptography, 44 (2007), no. 1-3, 307-319

[22] Arasu, K.T., Davis, J., Jedwab, J. & Sehgal, S.K., *New constructions of Menon difference sets*, J. Comb. Th. (A), vol 64, (1993), pp. 329-336.

[23] Arasu, K.T., , W, *Two-dimensional perfect quaternary arrays*, IEEE Trans Info Th, Vol 47, (2001), pp. 1482-1493.

[24] Arasu, K.T., Dillon, J.F., Jungnickel, D. & Pott, A., *The solution of the waterloo problem*. J. Comb. Th. (A), 71 (1995). pp. 316-331.

[25] Arasu, K.T., Dillon, J.F., *Perfect ternary arrays*, In: NATO volume on difference sets, sequences and their correlation properties., Ed. (A.Pott *et al*), Kluwer, (1999) pp. 1-15.

[26] Arasu, K.T., Dillon, J.F., Player, K.J., Character Sum Factorizations Yield Perfect Sequences (2010), Preprint.

[27] Arasu, K.T., Hollman, D.L., Player, K., Xiang, Q., *On the p-ranks of GMW difference sets*, (Columbus, OH, 2000), 9-35, Ohio State Univ. Math. Res. Inst. Publ., 10, de Gruyter, Berlin, (2002).

[28] Arasu, K.T., Player, K, *New families of Singer difference sets in characteristic three using Jacobi sums*, Designs, Codes and Cryptography, 28, (2003) no. 1, pp. 75-91.

[29] Arasu, Koukivinos, Kotsereas and Seberry, *On Circulant and Two-Circulant Weighing Matrices,* Australasian Journal of Combinatorics, (2010), Preprint.

[30] Arasu.K.T., Ding, C., Helleseth,T., Kumar. P.V., Martinsen. H., *Almost difference sets and their sequences with optimal autoacceleration*, IEEE Trans. Inform. Theory 47 (2001) pp. 2834 -2843.

[31] Arasu K.T., and Torban, D (1999), New weighing matrices of weight 25, J. Comb. Designs 7, 11-15.

[32] Arasu K.T. (1998), A reduction theorem for circulant weighing matrices, Australasian J. Combinatorics 18, 111-114.

[33] Baumert, L. D., *Cyclic difference sets*, Lecture Notes in Mathematics 182, Springer, New York (1972).

[34] Berndt, B.C., Evans, R.J., and Williams, K.S., Gauss and Jacobi Sums, Wiley-Interscience New York (1998).

[35] Beth.T., Jungnickel,D., and Lenz.H., Design Theory, 2nd Edition, Cambridge University Press, Cambridge (1999).

[36] Bose, R.C.(1942) An affine analogue of singer's theorem, J. Indian Math. Soc. 6, 1-15.

[37] Broughton, W.J., *A note on Table 1 of Barker sequences and difference set*", L'Enseignement Math. 50 (1995) pp. 105-107.

[38] Cai,Y. and Ding, C., Binary sequences with optimal autocorrelation, Theoretical Computer Science, Volume 410, Issues 24-25, pp. 2316-2322.

[39] Chang, J.A., *Ternary sequence with zero correlation*, Proceedings of the IEEE*,* vol. 55, no. 7 *(*1967) pp. 1211-1213

[40] Chang, S.W. Golomb, G. Gong and P.V. Kumar, *On ideal autocorrelation sequences arising from hyperovals*, Proceedings of the International Conference on Sequences and their Applications, Dec. 14-17, (1998), Singapore.

[41] Chang, T. Helleseth, P.V. Kumar, *Further results on a conjectured 2-level autocorrelation sequence*, In: Conference on Communication, Control and Computing, Sep. 23-25, (1998), pp. 598-599.

[42] Davis, J. A., Jedwab.J., *A unifying construction for difference sets*, J. Combin. Theory Ser. A 80 (1997) pp. 13-78.

[43] Dillon,J.F., Some REALLY Beautiful Hadamard Matrices, Cryptogr. Commun., (in press) (2010).

[44] Dillon, J.F., Elementary Hadamard difference sets, Ph.D. thesis, University of Maryland, (1974).

[45] Dillon, J.F., *The Waterloo Problem*, In F.Hoffman(ed.), Proceedings of the Tenth Southeastern Conference on combinatorics, Graph Theory and Computing, Congressus Numerantium XXIV, Utilitas Math. Publishing Co., Winnipeg, (1979) p.924.

[46] Dillon, J. F. Dobbertin, H., New cyclic difference sets with Singer parameters. Finite Fields Appl. 10, no. 3, (2004) pp. 342-389.

[47] Dillon, J. F. Geometry, codes and difference sets: exceptional connections. Codes and designs (Columbus, OH, 2000), 73-85, Ohio State Univ. Math. Res. Inst. Publ., 10, de Gruyter, Berlin, (2002).

[48] Dillon, J. F., *Multiplicative Difference sets via additive characters, Designs, Codes*, Cryptography 17 (1999), pp. 225-235.

[49] Dillon,J.F., *New p-ary perfect sequences and difference sets with Singer parameters. Sequences and their applications* (Bergen, 2001), pp. 23-33, Discrete Math. Theor. Comput. Sci. (Lond.), Springer, London, (2002).

[50] Ding.C., *Autocorrelation values of the generalized cyclotomic sequences of order 2*, IEEE Trans. Inform. Theory 44 (1998), pp. 1698-1702.

[51] Ding, C., Personal communication, (2010).

[52] Ding.C., Helleseth.T., Lam.K.Y., *Several classes of sequences with three-level autocorrelation*, IEEE Trans. Inform. Theory 45 (1999) pp. 2606-2612.

[53] Ding.C., Helleseth.T., Martinsen.H.M, *New families of binary sequences with optimal three-level autocorrelation*, IEEE Trans. Inform. Theory, 47, (2001) pp. 428-433.

[54] Dobbertin, H., *Kasami power functions, permutation polynomials and cyclic difference sets*, Proceedings of the NATO – A.S.I. Workshop "Difference sets, sequences and their correlation properties", Bad Windsheim, August 3-14, 1998, Klumer, Dordrecht, (1999) pp. 133-158.

[55] Eades, P. On the existence of orthogonal designs, Ph.D. Thesis, Australian National University, Canberra (1977).

[56] Eades, P. *Circulant (v,k,λ)-designs*, in R.W. Robinson et. Al. (eds) Combinatorial Mathematics VII, Lecture Notes in Mathematics 829, Springer, Berlin-Heidelberg, (1980) pp. 83-93.

[57] Eades, P. and Hain, R.M. *Circulant weighing matrices*, Ars Combinatoria 2, (1976) pp. 265--284.

[58] Eliahou,S., Kervaire, M., *Barker sequences and difference sets*, L'Enseignement Math. 38, (1992) pp. 345--382.

[59] Elliot, J.E.H. and Butson, A.T., *Relative Difference Sets*, Ill. J. Math 10, (1966) pp. 517-531.

[60] Evans, R., Hollman, H., Krattenthaler, C., and Xiang, Q., *Gauss Sums, Jacobi Sums and p-ranks of cyclic difference sets*, J. Comb. Th (A), 87, (1999) pp. 74-119.

[61] Games, Richard A., *The geometry of quadrics and correlations of sequences*. IEEE Trans. Inform. Theory 32 (1986), no. 3, 423-426.

[62] Geramita, Anthony V., and Seberry, Jennifer, *Orthogonal designs. Quadratic forms and Hadamard matrices*. Lecture Notes in Pure and Applied Mathematics, 45. Marcel Dekker, Inc., New York, (1979).

[63] Gologlu, Faruk and Pott, Alexander, *Results on crosscorrelation and autocorrelation of sequence*, In: Sequences and Their Applications - SETA 2008, Lecture Notes in Computer Science, (2008), Vol 5203, 95--105, Springer Berlin/Heidelberg. (Editors: Solomon W. Golomb and Matthew G. Parker and Alexander Pott and Arne Winterhof) (2008).

[64] Golomb, S. & Taylor, H., *Two dimensional synchronization patterns with minimum ambiguity*, IEEE Trans. Inform. Th. Vol IT-28, (1982) pp. 600--604.

[65] Golomb, S., *Construction of signals with favorable correlation properties*, In: Surveys in combinatorics, ed. A.D. Keedwell, London Math Society Lecture Note Series, 166, (1991) pp 1-39.

[66] Golomb, S. W. Construction of signals with favorable correlation properties. *Difference sets, sequences and their correlation properties (Bad Windsheim, 1998),* 159-194, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 542, *Kluwer Acad. Publ., Dordrech,* (1999).

[67] Golomb, Solomon W. and Gong, Guang, Signal design for good correlation. For wireless communication, cryptography, and radar. Cambridge University Press, Cambridge (2005).

[68] Gong, G., Gaal, P., and Golomb, S.W., A suspected new infinite class of $(2^n-1, 2^{n-1}-1, 2^{n-2}-1)$ *cyclic difference sets*, ITW 1997, Longyear-byen, Norway, July 6-12, (1997).

[69] Gordon.B., Mills. W.H., Welch. L.R., *Some new difference sets*, Canad. J. Math. 14 (1962) pp. 614-625.

[70] Hall Jr.,Marshall, *A survey of difference sets*, Proc. Amer. Math. Soc. 7 (1956) pp. 975-986.

[71] Helleseth, T, Gong, Guang., *New nonbinary sequences with ideal two-level autocorrelation*, IEEE Trans. Inform. Theory 48, no. 11, (2002), pp. 2868-2872.

[72] Helleseth, T., Kumar P.V., and Martinsen H., *A new family of ternary sequences ideal autocorrelation function*, Des. Codes Cryptogr. 23, no. 2, (2001) pp. 157-166.

[73] Helleseth, T., personal communication, (2002).

[74] Helleseth, Tor and Kumar, P. Vijay, *Sequences with low correlation*, Handbook of coding theory, Vol. I, II, North-Holland, Amsterdam (1998) pp. 1765-1853.

[75] Hershey, J. & Yarlagadda, R., *Two dimensional synchronization*, Electron Lett., Vol 19, (1983) pp. 801-803.

[76] Hertel, Doreen, Sequences with good correlation properties, Ph.D. Thesis, Otto-von-Guericke-University, Magdeburg (2006).

[77] Høholdt,T., and Justesen, J., *Ternary sequences with perfect periodic autocorrelation*, IEEE Transactions on Information Theory 29(4): (1983) pp. 597--600.

[78] Ipatov, V. P., Platonov, V. D., and Samoĭlov, I. M., *A new class of triple sequences with ideal periodic autocorrelation properties*. (Russian) Izv. Vyssh. Uchebn. Zaved. Mat.**,** no. 3 (1983) pp. 47-50.

[79] Ipatov, V.P., *Ternary sequences with ideal periodic autocorrelation properties*, Radio Engineering and Electronic physics 24, (1979) pp. 75-79.

[80] Ipatov, V.P., *Contribution to the theory of sequences with perfect auto correlation properties*, Radio Engineering and Electronic physics 25, (1980) pp. 31-34.

[81] Jedwab, J., Mitchell, C., *Constructing new perfect binary arrays*, Electronic letters 24, (1988) pp. 650-652.

[82] Jedwab, Jonathan, *Generalized perfect arrays and Menon difference sets*. Des. Codes Cryptogr. 2, no. 1, (1992) pp. 19-68.

[83] Jedwab, Jonathan, *What can be used instead of a Barker sequence? Finite fields and applications,* Contemp. Math., 461, Amer. Math. Soc., Providence, RI, (2008) pp. 153-178.

[84] Jensen, J.M., Jensen, H.E., Høholdt,T., *The merit factor of binary sequences related to difference sets*, IEEE Trans. IT 37(3) (1991) pp. 617-626.

[85] Jungnickel, D. and Pott, A., *Perfect and almost perfect sequences*, Discrete Appl. Math. 95 (1999a) pp. 331-359.

[86] Jungnickel, D., and Pott, A., *Recent results on difference sets with classical parameters*, Proceedings of the NATO ASI "Difference Sets: An introduction", A. Pott et al. (eds.), (1999b), pp. 259-295.

[87] Jungnickel, Dieter and Kharaghani, H., *Balanced generalized weighing matrices and their applications*, in: Matematiche 59, (2004) pp. 225-261

[88] Kashyap,N., Jacobi-like sums and cyclic difference sets, Master's Thesis, University of Maryland Baltimore County, 2005.

[89] Lander.E.S., Symmetric Designs, An Algebraic Approach, Cambridge University Press, Cambridge, (1983).

[90] Legendre, A.M., Essai sur la theorie des nombres Paris (1798), p 186.

[91] Lempel.A., Cohn. M., Eastman.W.L, *A class of binary sequences with optimal autocorrelation properties*, IEEE Trans. Inform. Theory 23 (1977) pp. 38-42.

[92] Leung, Ka Hin, Ling, San, Ma, Siu Lun, and Tay, Kian Boon, *Almost perfect sequences with θ=2*, Arch. Math. (Basel) 70 , no. 2, (1998) pp. 128-131.

[93] Leung, Ka Hin, Schmidt, B, Finiteness of Circulant Weighing Matrices of Fixed Weight (2010) Preprint.

[94] Lidl, R. and Niederreiter, H., Finite Fields, 2nd Ed., Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, Cambridge, (1997).

[95] Lin, H.A., From Hadamard difference sets to perfectly balanced sequences, Ph.D. Thesis, University of Southern California, Los Angeles, USA, (1998).

[96] Ludkovski, M. and Gong, G., *New families of ideal 2-level autocorrelation ternary sequences from second order DHT*, International Workshop on Coding and Cryptography (Paris, 2001), 10 pp. (electronic), Electon. Notes Discrete Math., 6, Elsevier, Amsterdam, (2001).

[97] Luke, H.D., Bömer, C. & Antweiler, M., *Perfect binary arrays*, Signal processing, 17 (1989), pp. 69-80.

[98] Ma, S.L., Polynomial addition sets, Ph.D. thesis (1985), University of Hong Kong.

[99] Ma, S.L. and Ng, W.S. *On non-existence of perfect and nearly perfect sequences*, Int. J. Information and Coding Theory, Vol. 1, No. 1, (2009) pp.15-38.

[100] MacWilliams, J., and Mann, H. B., *On the p-rank of the design matrix of a difference set*, Inform. Control 12 (1968) pp. 474-488.

[101] Mann, H.B., Addition Theorems, Wiley, New York (1965).

[102] Maschietti, A., *Difference sets and hyperovals*, Des. Codes Cryptgr. 14 (1998) pp. 89-98.

[103] Mertens, S., and Bessenrodt, C, *On the ground states of the Bernasconi model*, J. Phys. A: Math. Gen. 31 (1998), 3731-749.

[104] Mossinghoff, M.J., *Wieferich prime pairs, Barker sequences, and circulant Hadamard matrices*, http://www.cecm.sfu.ca/_mjm/ WieferichBarker, (2009).

[105] Mossinghoff, Michael J., *Wieferich pairs and Barker sequences*, Des. Codes Cryptogr. 53, no. 3, (2009) pp. 149-163.

[106] Mullin, R. C. and Stanton, R. G., *Group matrices and balanced weighing designs*. Utilitas Math. 8, (1975) pp. 277-301.

[107] Mullin, R. C., *A note on balanced weighing matrices*. Combinatorial mathematics, III (Proc. Third Australian Conf., Univ. Queensland, St. Lucia, 1974), pp. 28-41. Lecture Notes in Math., Vol. 452, Springer, Berlin, (1975).

[108] No, J. S., Golomb, S.W., Gong, G., Lee H.K., and Gaal, P., *Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation*, IEEE Trans. Inf. Theory 44, (1998) pp. 814-817.

[109] No, J.S., Chung, H., Yun, M.S., *Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$*, IEEE Trans. Inform. Theory 44 (1998) pp. 1278-1282.

[110] No., J., *p-ary unified sequences: p-ary extended d-form sequences with the ideal autocorrelation property*. IEEE Trans. Inform. Theory 48, no. 9 (2002) pp. 2540-2546.

[111] Paley, R.E.A.C., *On orthogonal matrices*, J. Math. Phys. MIT 12 (1933) pp. 311-320.

[112] Pless, V., *Symmetry codes over GF*(3) *and new five-designs*, J.Combin. Theory Ser. A, 12 (1972) pp. 119-142.

[113] Pott, A., Finite geometry and character theory, Springer Lecture Notes 1601, New York (1995).

[114] Schmidt, B., *Characters and cyclotomic fields in finite geometry*. Lecture Notes in Mathematics, 1797 (2002).

[115] Schmidt, B., *Cyclotomic integers and finite geometry*, J. Am. Math. Soc. 12 (1999) pp. 929-952.

[116] Sidelnikov, V.M., *Some k-valued pseudo-random sequences and nearly equidistant codes*, Probl. Inf. Transm. 5 (1969) pp. 12-16.

[117] Simon, M.K., Omura. J.K., Scholtz, R.A., and Levit, B.K., Spread Spectrum Communications, Volume I Computer Science Press, Rockville Maryland, (1985).

[118] Singer, J.F., *A theorem in finite projective geometry and some applications to number theory*, Trans. AMS 43 (1938) pp. 377-385.

[119] Stanton, R. G. and Sprott, D. A., *A family of difference sets*, in Canad. J. Math. 10 (1958), pp. 73-77.

[120] *Storer*, T., Cyclotomy and Difference Sets, Markham, Chicago (1967).

[121] Strassler, Y., The classification of circulant weighing matrices of weight 9, Ph.D. Thesis, Bar-Ilan University, Israel (1997).

[122] Strassler, Y., *New circulant weighing matrices of prime order in CW(31,16), CW(71,25), CW(127,64)*, J.Stat. Planning and Inference 73, (1998) pp. 317-330.

[123] Turyn, R. *Sequences with small correlation*. (1968) Error Correcting Codes (Proc. Sympos. Math. Res. Center, Madison, Wis.,) John Wiley, New York (1968) pp. 195-228.

[124] Turyn. R.J., *Character sums and difference sets*, Pacific J. Math., Vol. 15 (1965) pp. 319-346.

[125] Turyn. R.J., Complex Hadamard matrices, Combinatorial Structures and their Applications, Gordon and Breach, London (1970) pp. 435-437.

[126] Vincent, A., Applications of Combinatorial Designs to the Theory of Communications, PhD thesis, RHBNC, University of London (1989).

[127] Wallis, Jennifer Seberry, and Whiteman, *Albert Leon, Some results on weighing matrices*, Bull. Austral. Math. Soc. 12, no. 3 (1975) pp. 433-447.

[128] Whiteman, A.L., *A family of difference sets*, Illinois J. Math. 6 (1962) pp. 107-121.

[129] Wild, P., *Infinite families of perfect binary arrays*, Electronic letters 24, (1988) pp. 845-847.

[130] Xiang, Q., *Recent progress in algebraic design theory*, Finite Fields and Their Applications 11 (2005) pp. 622-653.

[131] Xiang, Q., *Recent results on difference sets with classical parameters*, In: J. Dinitz, D.R. Stinson (Eds.), Contemporary Design Theory, A Collection of surveys, Wiley-Interscience Series in Discrete Mathematics and Optimization, Wiley, New York (1992) pp. 419--437.

[132] Yamamoto, K, *On congruences arising from relative Gauss sums*, In: Number Theory and Combinatorics, World Scientific Publ. Japan (1985).