Available online at www.sciencedirect.com

SCIENCE DIRECT®

Finite Fields and Their Applications 11 (2005) 622–653

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

# Recent progress in algebraic design theory

Qing Xiang[1]

*Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA*

Received 2 March 2005; revised 1 June 2005

Communicated by Gary L. Mullen

**Abstract**

We survey recent results on difference sets, *p*-ranks and Smith normal forms of certain set-inclusion matrices and subspace-inclusion matrices.

*Keywords:* Bush-type Hadamard matrix; Code; Design; Difference set; Gauss sum; Hadamard difference set; Hadamard matrix; Jacobi sum; Monomial basis; Multiplier; Nonabelian difference set; *p*-rank; Reversible difference set; Skew Hadamard difference set; Smith normal form; Symmetric design; Strongly regular graph

## 1. Introduction

In this paper, we survey some recent results in algebraic design theory. By algebraic design theory we mean the theory of studying combinatorial designs by using algebraic and number theoretic methods. A representative list of topics in algebraic design theory can be found in Lander's book [76]. Among the topics of algebraic design theory, difference sets are of central importance. Therefore we will devote a large part of this paper to difference sets. There exist several recent surveys on difference sets, for example, see [63,66,67,12, Chapter 6]. So it is natural for us to concentrate on results obtained after [12, Chapter 6] was written. Besides difference sets, we will also survey

*E-mail address:* xiang@math.udel.edu.

[1] Research supported in part by NSF Grant DMS 0400411.

1071-5797/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2005.06.003

recent results on $p$-ranks and Smith normal forms of certain incidence matrices. In particular, we describe the results on the Smith normal forms of the incidences of points and subspaces of $\mathrm{PG}(m, q)$ and $\mathrm{AG}(m, q)$ in [20]. This work involves heavy use of representations of the general linear groups and $p$-adic number theory, and has led to interesting applications to problems in finite geometry [19].

The paper is organized as follows. In Section 2, we define 2-$(v, k, \lambda)$ designs, difference sets, Smith normal forms of designs, etc., and recall some basic results. In Sections 3 through 9, we discuss recent results on difference sets. Roughly speaking, the theory of difference sets has four aspects. These are nonexistence proofs of difference sets, constructions of difference sets, inequivalence of difference sets, and connections of difference sets to other areas of combinatorics. We report recent results on all four of these aspects. The highlights are the proof of Lander's conjecture for abelian difference sets of prime power orders by Leung et al. [78] (Section 3), the construction of cyclic difference sets with classical parameters by Dillon and Dobbertin [34] (Section 5), the surprising construction of new skew Hadamard difference sets in $(\mathbb{F}_{3^m}, +)$ by Ding and Yuan [35] (Section 6), and the construction of Bush-type Hadamard matrices using reversible Hadamard difference sets by Muzychuk and Xiang [95] (Section 7). In Section 4, we collect recent results on multipliers of abelian difference sets, and in Section 8, we discuss nonabelian difference sets. Section 9 is concerned with $p$-ranks and Smith normal forms of difference sets. We show how to use Smith normal forms to prove inequivalence of difference sets when $p$-ranks are not sufficient for this purpose. In Section 10, we describe Wilson's results [113–115] on diagonal forms of certain set-inclusion matrices. In Section 11, we explain in detail the work of Chandler et al. [20] on the Smith normal forms of the incidences of points and subspaces of $\mathrm{PG}(m, q)$ and $\mathrm{AG}(m, q)$. Finally in Section 12, we describe two important recent results closely related to algebraic design theory; one is the surprisingly elementary proof of the prime power conjecture for projective planes of order $n$ with an abelian collineation group of order $n^2$ by Blokhuis et al. [13], the other is the construction of a Hadamard matrix of order 428 by Kharaghani and Tayeh-Rezaie [72].

It is impractical to mention all recent work in algebraic design theory in this paper. Some topics had to be omitted. An apparent omission is the work on Hadamard difference sets in elementary abelian 2-groups (i.e., bent functions). However, we hope that this survey will show that algebraic design theory in general, and the theory of difference sets in particular are alive and vital.

## 2. Definitions and basic results

We first give the definition of a 2-design.

**Definition 2.1.** A 2-$(v, k, \lambda)$ *design* is a pair $(\mathcal{P}, \mathcal{B})$ that satisfies the following properties:

(1) $\mathcal{P}$ is a set of $v$ elements (called *points*).

(2) $\mathcal{B}$ is a family of $b$ subsets of $\mathcal{P}$ (called *blocks*), each of size $k$.
(3) Every 2-subset of $\mathcal{P}$ is contained in exactly $\lambda$ blocks.

We will require $v > k$ to avoid triviality. Simple counting arguments show that $b = \frac{\lambda v(v-1)}{k(k-1)}$, and the number of blocks containing each point of $\mathcal{P}$ is $\frac{\lambda(v-1)}{k-1}$, which will be denoted by $r$ (called the *replication number* of the design). The *order* of the 2-design, denoted by $n$, is defined to be $r-\lambda$. A 2-$(v,k,\lambda)$ design $(\mathcal{P},\mathcal{B})$ is said to be *simple* if it does not have repeated blocks (i.e., $\mathcal{B}$ is a set). The most basic necessary condition for the existence of 2-designs is Fisher's inequality which states that $b \geqslant v$ if a 2-$(v,k,\lambda)$ design with $b$ blocks exists. A simple 2-$(v,k,\lambda)$ design $(\mathcal{P},\mathcal{B})$ with $b=v$ is called a *symmetric design*. We note that for a $(v,k,\lambda)$ symmetric design, the order is $n=k-\lambda$.

Given two 2-$(v,k,\lambda)$ designs $\mathcal{D}_1 = (\mathcal{P}_1,\mathcal{B}_1)$ and $\mathcal{D}_2 = (\mathcal{P}_2,\mathcal{B}_2)$, we say that $\mathcal{D}_1$ and $\mathcal{D}_2$ are *isomorphic* if there exists a bijection $\phi : \mathcal{P}_1 \to \mathcal{P}_2$ such that $\phi(\mathcal{B}_1) = \mathcal{B}_2$ and for all $p \in \mathcal{P}_1$ and $B \in \mathcal{B}_1$, $p \in B$ if and only if $\phi(p) \in \phi(B)$. An *automorphism* of a 2-design is an isomorphism of the design with itself. The set of all automorphisms of a 2-design forms a group, *the* (*full*) *automorphism group* of the design. An *automorphism group* of a 2-design is any subgroup of the full automorphism group.

Isomorphism of designs can also be defined by using incidence matrices of designs, which we define now. Let $\mathcal{D} = (\mathcal{P},\mathcal{B})$ be a 2-$(v,k,\lambda)$ design and label the points as $p_1, p_2, \ldots, p_v$ and the blocks as $B_1, B_2, \ldots, B_b$. An *incidence matrix* of $(\mathcal{P},\mathcal{B})$ is the matrix $A = (a_{ij})$ whose rows are indexed by the blocks $B_i$ and whose columns are indexed by the points $p_j$, where the entry $a_{ij}$ is 1 if $p_j \in B_i$, and 0 otherwise. From the definition of 2-designs, we see that the matrix $A$ satisfies

$$A^{\top}A = (r-\lambda)I + \lambda J, \quad AJ = kJ, \tag{2.1}$$

where $I$ is the identity matrix, and $J$ is the all-one matrix. Now let $\mathcal{D}_1 = (\mathcal{P}_1,\mathcal{B}_1)$ and $\mathcal{D}_2 = (\mathcal{P}_2,\mathcal{B}_2)$ be two 2-$(v,k,\lambda)$ designs, and let $A_1$ and $A_2$ be incidence matrices of $\mathcal{D}_1$ and $\mathcal{D}_2$, respectively. Then $\mathcal{D}_1$ and $\mathcal{D}_2$ are isomorphic if and only if there are permutation matrices $P$ and $Q$ such that

$$PA_1Q = A_2, \tag{2.2}$$

that is, the matrices $A_1$ and $A_2$ are permutation equivalent.

Next we define codes, $p$-ranks, and Smith normal forms of 2-designs. Let $\mathcal{D}$ be a 2-$(v,k,\lambda)$ design with incidence matrix $A$. The *p-rank* of $\mathcal{D}$ is defined as the rank of $A$ over a field $F$ of characteristic $p$, and it will be denoted by $\mathrm{rank}_p(\mathcal{D})$. The $F$-vector space spanned by the rows of $A$ is called the (*block*) *code* of $\mathcal{D}$ over $F$, which is denoted by $C_F(\mathcal{D})$. If $F = \mathbb{F}_q$, where $q$ is a power of $p$, then we denote the code of $\mathcal{D}$ over $\mathbb{F}_q$ by $C_q(\mathcal{D})$. We proceed to define the Smith normal form of $\mathcal{D}$. Let $R$ be a principal ideal domain. Viewing $A$ as a matrix with entries in $R$, we can find (see for example, [25]) two invertible matrices $U$ and $V$ over $R$ such that

$$UAV = \begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & & \\ 0 & & \ddots & & \vdots \\ \vdots & & & d_{v-1} & 0 \\ 0 & & \cdots & 0 & d_v \\ 0 & & \cdots & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix} \tag{2.3}$$

with $d_1|d_2|d_3|\cdots$. The $d_i$ are unique up to units in $R$. When $R = \mathbb{Z}$, the $d_i$ are integers, and they are called the *invariant factors of* $A$; the matrix on the right-hand side of (2.3) (now with integer entries) is called the *Smith normal form* (*SNF*) *of* $A$. If on the right-hand side of (2.3) we do not require the divisibility condition $d_1|d_2|d_3|\cdots$, then that matrix is said to be a *diagonal form* of $A$. We define the *Smith normal form of* $\mathcal{D}$ to be that of $A$. Smith normal forms and $p$-ranks of 2-designs can help distinguish nonisomorphic 2-designs with the same parameters: let $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1)$ and $\mathcal{D}_2 = (\mathcal{P}_2, \mathcal{B}_2)$ be two 2-$(v, k, \lambda)$ designs with incidence matrices $A_1$ and $A_2$ respectively. From (2.2) we see that if $\mathcal{D}_1$ and $\mathcal{D}_2$ are isomorphic, then $A_1$ and $A_2$ have the same Smith normal form over $\mathbb{Z}$; hence $\mathcal{D}_1$ and $\mathcal{D}_2$ have the same Smith normal form, in particular, $\mathrm{rank}_p(\mathcal{D}_1) = \mathrm{rank}_p(\mathcal{D}_2)$ for any prime $p$. The usefulness of Smith normal forms of designs goes well beyond isomorphism testing. For example, the Smith normal forms of symmetric designs were used by Lander [76] to construct a sequence of $p$-ary codes which were then used to give a (partial) coding theoretic proof of the Bruck–Ryser–Chowla theorem. We will see some other applications of SNF of incidence matrices in Sections 10 and 11.

We now define difference sets. Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a 2-$(v, k, \lambda)$ symmetric design with a sharply transitive automorphism group $G$. Then we can identify the elements of $\mathcal{P}$ with the elements of $G$. After this identification, each block of $\mathcal{D}$ is now a $k$-subset of $G$. Since $G$ acts sharply transitively on $\mathcal{B}$, we may choose a base block $D \subset G$. All other blocks in $\mathcal{B}$ are simply "translates" $gD = \{gx | x \in D\}$ of $D$, where $g \in G$ and $g \neq 1$. That $\mathcal{D}$ is a symmetric design implies

$$|D \cap gD| = \lambda$$

for all nonidentity elements $g \in G$. That is, every nonidentity element $g \in G$ can be written as $xy^{-1}$, $x, y \in D$, in $\lambda$ ways. This leads to the definition of difference sets.

**Definition 2.2.** Let $G$ be a finite (multiplicative) group of order $v$. A $k$-element subset $D$ of $G$ is called a $(v, k, \lambda)$ *difference set* in $G$ if the list of "differences" $xy^{-1}$, $x, y \in D$, $x \neq y$, represents each nonidentity element in $G$ exactly $\lambda$ times. If the group $G$ is cyclic (resp. abelian), then $D$ is called a cyclic (reps. abelian) difference set.

Note that any group $G$ contains *trivial* difference sets, namely, $\emptyset$, $G$, $\{g\}$, $G \setminus \{g\}$, where $g$ is an arbitrary element of $G$. We will use the term "difference set" to mean a non-trivial difference set. In the above, we see that sharply transitive symmetric designs give rise to difference sets. In the other direction, if $D$ is a $(v, k, \lambda)$-difference set in a group $G$, then we can use the elements of $G$ as points, and use the "translates" $gD$ of $D$, $g \in G$, as blocks, and we obtain a symmetric design $(G, \{gD | g \in G\})$ with a sharply transitive automorphism group $G$. (This design is usually called *the symmetric design developed from D*, and will be denoted by $\mathrm{dev}(D)$.) Hence difference sets and sharply transitive symmetric designs are the same objects.

Let $D_1$ and $D_2$ be two $(v, k, \lambda)$-difference sets in an abelian group $G$. We say that $D_1$ and $D_2$ are *equivalent* if there exists an automorphism $\sigma$ of $G$ and an element $g \in G$ such that $\sigma(D_1) = D_2 g$. Note that if $D_1$ and $D_2$ are equivalent, then $\mathrm{dev}(D_1)$ and $\mathrm{dev}(D_2)$ are isomorphic. Therefore, one way to distinguish inequivalent difference sets is to show that the symmetric designs developed from them are nonisomorphic.

We end this section by giving some classical examples of 2-designs and difference sets. Let $\mathrm{PG}(m, q)$ be the $m$-dimensional projective space over the finite field $\mathbb{F}_q$, where $q$ is a prime power, let $\mathrm{AG}(m, q)$ be the $m$-dimensional affine space over $\mathbb{F}_q$, and let $\begin{bmatrix} m \\ i \end{bmatrix}_q$ denote the number of $i$-dimensional subspaces of an $m$-dimensional vector space over $\mathbb{F}_q$. We have the following classical examples of 2-designs:

**Example 2.3.** Let $m \geqslant 2$ and $m \geqslant d \geqslant 2$ be integers. The points of $\mathrm{PG}(m, q)$ and the $(d-1)$-dimensional subspaces of $\mathrm{PG}(m, q)$ form a 2-design with parameters

$$v = \begin{bmatrix} m+1 \\ 1 \end{bmatrix}_q = (q^{m+1} - 1)/(q - 1), \quad k = \begin{bmatrix} d \\ 1 \end{bmatrix}_q = (q^d - 1)/(q - 1),$$

$$r = \begin{bmatrix} m \\ d-1 \end{bmatrix}_q, \quad \lambda = \begin{bmatrix} m-1 \\ d-2 \end{bmatrix}_q, \text{ and } b = \begin{bmatrix} m+1 \\ d \end{bmatrix}_q.$$

In particular, when $d = m$, we obtain the classical symmetric design of points and hyperplanes in $\mathrm{PG}(m, q)$ which can be developed from a (cyclic) Singer difference set.

**Example 2.4.** Let $m \geqslant 2$ and $m - 1 \geqslant d \geqslant 1$ be integers. The points of $\mathrm{AG}(m, q)$ and the $d$-flats of $\mathrm{AG}(m, q)$ form a 2-design with parameters $v = q^m$, $k = q^d$, $r = \begin{bmatrix} m \\ d \end{bmatrix}_q$, $\lambda = \begin{bmatrix} m-1 \\ d-1 \end{bmatrix}_q$, and $b = q^{m-d} \begin{bmatrix} m \\ d \end{bmatrix}_q$. Here the $d$-flats of $\mathrm{AG}(m, q)$ are the cosets of $d$-dimensional subspaces of the underlying $m$-dimensional vector space over $\mathbb{F}_q$.

**Example 2.5.** Let $q = 4n - 1$ be a prime power. Then the set $D$ of nonzero squares in $\mathbb{F}_q$ forms a $(4n - 1, 2n - 1, n - 1)$ difference set in $(\mathbb{F}_q, +)$. This will be called the Paley difference set.

## 3. Nonexistence results on difference sets

The existence theory of abelian difference sets is well developed. The theory seems naturally to bifurcate into two parts: one part deals with $(v, k, \lambda)$ abelian difference sets with $\gcd(k-\lambda, v) = 1$, and the other deals with those with $\gcd(k-\lambda, v) > 1$. For $(v, k, \lambda)$ abelian difference sets with $\gcd(k-\lambda, v) = 1$, multipliers are very useful for nonexistence proofs. In contrast for $(v, k, \lambda)$ abelian difference sets with $\gcd(k-\lambda, v) > 1$, the character theoretic approach introduced by Turyn [107] proved to be fruitful.

While most $(v, k, \lambda)$ abelian difference sets with $\gcd(k-\lambda, v) = 1$ prefer to live in high exponent abelian groups (for example, all known abelian difference sets with the same parameters as those of Singer difference sets live in cyclic groups), all $(v, k, \lambda)$ abelian difference sets with $\gcd(k-\lambda, v) > 1$ seem to prefer to live in low exponent abelian groups. The Ryser conjecture from 1963 and the Lander conjecture from 1983 convey this feeling.

**Conjecture 3.1** (*Ryser [102]*). *There does not exist a* $(v, k, \lambda)$ *difference set with* $\gcd(k-\lambda, v) > 1$ *in a cyclic group.*

**Conjecture 3.2** (*Lander [76]*). *Let G be an abelian group of order* $v$ *containing a* $(v, k, \lambda)$ *difference set. If p is a prime dividing* $\gcd(k-\lambda, v)$, *then the Sylow p-subgroup of G cannot be cyclic.*

We also mention the following important special case of Ryser's conjecture. A *Hadamard matrix* of order $v$ is a $v$ by $v$ matrix $H$ with entries ±1, such that

$$HH^{\top} = vI_v,$$

where $I_v$ is the identity matrix of order $v$. A *circulant Hadamard matrix* of order $v$ is a Hadamard matrix of the following form

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_v \\ a_v & a_1 & a_2 & \cdots & a_{v-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix}. \tag{3.1}$$

The circulant Hadamard matrix conjecture is the following:

**Conjecture 3.3.** *There does not exist any circulant Hadamard matrix of order* $v > 4$.

Since the existence of a circulant Hadamard matrix of order $v$ implies the existence of a cyclic $(4u^2, 2u^2-u, u^2-u)$ difference set where $v = 4u^2$, $u$ odd (see [12, Chapter 6]), we see that the Ryser conjecture implies the circulant Hadamard matrix conjecture.

Recently, Leung et al. [78] proved the following conclusive general result on Lander's conjecture.

**Theorem 3.4.** *Lander's conjecture and thus Ryser's conjecture is true for $(v, k, \lambda)$ abelian difference sets with $k - \lambda$ a power of a prime $> 3$.*

This is a major advance in the existence theory of abelian difference sets. Previous results on Lander's conjecture are either proved under extra conditions (such as the self-conjugacy condition), or much less conclusive than Theorem 3.4. The main idea in the proof of Theorem 3.4 is to use the character theoretic approach to show that a $(v, k, \lambda)$ abelian difference set with $k-\lambda = p^r$ a prime power, $p|v$, decomposes into two parts: a "subfield part" and a "kernel part". We remark that similar decompositions were previously used by Jia [59] to obtain some partial results on Lander's conjecture. A more general decomposition result for group ring elements is proved by Leung and Schmidt [81]. Applications of this decomposition result include the nonexistence of circulant Hadamard matrices of order $v$ with $4 < v < 548, 964, 900$ and the nonexistence of Barker sequences of length $\ell$ with $13 < \ell < 10^{22}$. For more details, we refer the reader to [81].

Next we consider nonexistence results on abelian difference sets whose parameters are from special infinite families. In this regard, the best known result is the following theorem:

**Theorem 3.5** (*Davis [29], Kraemer [75]*). *Let G be an abelian group of order $2^{2m+2}$. Then G contains a $(2^{2m+2}, 2^{2m+1} - 2^m, 2^{2m} - 2^m)$ difference set if and only if the exponent of G is $\leqslant 2^{m+2}$.*

In another case, the McFarland parameters for difference sets are

$$v = q^{m+1}\left(1 + \frac{q^{m+1}-1}{q-1}\right),\ k = \frac{q^m(q^{m+1}-1)}{q-1},\ \lambda = \frac{q^m(q^m-1)}{q-1}, \tag{3.2}$$

where $q = p^t$ is a prime power and $m$ is a positive integer. McFarland [91] constructed difference sets with parameters (3.2) in abelian groups $G = E \times K$ of order $q^{m+1}(1+\frac{q^{m+1}-1}{q-1})$, where $E$ is an elementary abelian $p$-group of order $q^{m+1}$. The problem here is to decide which abelian groups contain a difference set with McFarland parameters. We refer the reader to [66, Section 2.3] for a detailed account of results on this problem obtained before 1997. Recently, Arasu et al. [2] proved the following interesting theorem on abelian difference sets with parameters (3.2), where $q \geqslant 8$ is a power of 2 and $m = 1$.

**Theorem 3.6.** *Let G be an abelian group of order $2^{2t+1}(2^{t-1} + 1)$ with $t \geqslant 3$. Then G contains a $(2^{2t+1}(2^{t-1} + 1), 2^t(2^t + 1), 2^t)$ difference set if and only if G contains an elementary abelian subgroup of order $2^{2t}$.*

Theorem 3.6 in particular shows that there does exist a $(640, 72, 8)$ difference set in $G_1 = \mathbb{Z}_4^2 \times \mathbb{Z}_2^3 \times \mathbb{Z}_5$ or $G_2 = \mathbb{Z}_4^3 \times \mathbb{Z}_2 \times \mathbb{Z}_5$. We explain the history of this problem below. In 1995, Arasu and Sehgal [5] constructed a $(96, 20, 4)$ difference set (i.e., with

$q = 4$ and $m = 1$ in (3.2)) in the group $\mathbb{Z}_4^2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. This sparked a search for a similar difference set with larger $q$ in (3.2). The most likely candidate was generally thought at that time to be a $(640, 72, 8)$ difference set (i.e., with $q = 8$ and $m = 1$ in (3.2)) in $G_1$ or $G_2$ as given above. Indeed, the search for difference sets in these two groups led Davis and Jedwab to construct a family of difference sets with brand new parameters (see [30, p. 16]); but the existence of a $(640, 72, 8)$ difference set in $G_1$ and $G_2$ was not settled in [30]. Theorem 3.6 now settles this problem and says much more.

Finally, we mention that Baumert and Gordon [10] proved nonexistence of several cyclic difference sets with small parameters, and showed that there do not exist cyclic projective planes of nonprime power order $\leqslant 2 \cdot 10^9$. They also looked at the existence of cyclic $(v, k, \lambda)$ difference sets with $k \leqslant 300$, and cyclic $(v, \frac{v-1}{2}, \frac{v-3}{4})$ difference sets with $v \leqslant 10,000$.

## 4. Multipliers

Let $D$ be a difference set in $G$. An automorphism $\alpha$ of $G$ is called a *multiplier* of $D$ if it induces an automorphism of the symmetric design $\mathrm{dev}(D)$ developed from $D$; furthermore if $G$ is abelian and $\alpha : G \to G$ is given by $x \mapsto x^t$, $\gcd(t, |G|) = 1$, we call $\alpha$, or simply the integer $t$, a *numerical multiplier* of $D$. Multipliers were first discovered by Hall [47]. They are one of the earliest tools for constructing difference sets and proving nonexistence results on difference sets. One of the major open problems concerning multipliers of difference sets is Hall's multiplier conjecture.

**Conjecture 4.1.** *Let $D$ be a $(v, k, \lambda)$ difference set in an abelian group of order $v$, and let $p$ be any prime divisor of $n = k - \lambda$ with $\gcd(p, v) = 1$. Then $p$ is a multiplier of $D$.*

The multiplier conjecture can be proved rather easily in the case $n = p^\alpha$, where $p$ is a prime not dividing the order of the group. So it is natural to consider the cases $n = 2p^\alpha$ and $n = 3p^\alpha$. Muzychuk [94] finished completely the case $n = 2p^\alpha$, $p$ an odd prime, and obtained partial results in the case where $n = 3p^\alpha$. Recently, Qiu [101] finished the case $n = 3p^\alpha$ completely. We summarize their results in the following theorem.

**Theorem 4.2** (*Muzychuk [94], Qiu [101]*). *Let $D$ be a $(v, k, \lambda)$ difference set in an abelian group of order $v$, and let $n = k - \lambda$. If $n = 2p^\alpha$, where $p$ is an odd prime not dividing $v$, or $n = 3p^\alpha$, where $p$ is a prime not dividing $v$, then $p$ is a multiplier of $D$.*

One of the reasons that we seem not to make much headway on the multiplier conjecture is the scarcity of examples of $(v, k, \lambda)$ difference sets in abelian groups of exponent greater than 3 with the properties that $\gcd(v, k - \lambda) = 1$ and $k - \lambda$ is not a prime power. (Note that when $k - \lambda$ is a prime power, the multiplier conjecture for $(v, k, \lambda)$ difference sets is true.) It is a quite challenging problem to construct new difference sets satisfying the above constraints. Also of interest is the following problem.

**Problem 4.3.** *Does there exist a difference set with only the trivial numerical multiplier in an abelian group of exponent greater than* 3?

Note that difference sets in elementary abelian 2-groups certainly have only the trivial numerical multiplier. Also the Paley–Hadamard difference set in $(\mathbb{F}_{3^m}, +)$ has only the trivial numerical multiplier. That is the reason we require the abelian group involved in Problem 4.3 to have exponent greater than 3.

In the rest of this section, we discuss difference sets with multiplier $-1$. If $D$ is an abelian difference set with multiplier $-1$, then by a theorem of McFarland and Rice [93], we may assume that $D$ is fixed by $-1$, that is, $D^{(-1)} = D$, where $D^{(-1)} = \{d^{-1} | d \in D\}$. A difference set fixed by $-1$ is sometimes called a *reversible difference set*. The parameters of a reversible abelian difference set are severely restricted. See [63, Section 13] for a list of restrictions. In fact, McFarland made the following conjecture.

**Conjecture 4.4.** *Let D be a* $(v, k, \lambda)$ *abelian difference set with* $-1$ *multiplier* (*w.l.o.g. assume* $k < v/2$ *by complementation*). *Then either* $(v, k, \lambda) = (4000, 775, 150)$ *or* $(v, k, \lambda) = (4u^2, 2u^2 - u, u^2 - u)$ *for some positive integer u.*

Making use of sub-difference sets of reversible difference sets, Ma [87] proved that the truth of the following conjecture on the solutions of two diophantine equations would imply the truth of Conjecture 4.4.

**Conjecture 4.5.** *Let p be an odd prime,* $a \geqslant 0$ *and* $b, t, r \geqslant 1$. *Then*

(1) $Y = 2^{2a+2}p^{2t} - 2^{2a+2}p^{t+r} + 1$ *is a square if and only if* $t = r$ (*i.e.,* $Y = 1$).
(2) $Z = 2^{2b+2}p^{2t} - 2^{b+2}p^{t+r} + 1$ *is a square if and only if* $p = 5$, $b = 3$, $t = 1$, *and* $r = 2$ (*i.e.,* $Z = 2401$).

Le and Xiang [77] could verify part (1) of Conjecture 4.5. At one time, Z.F. Cao claimed that he had a proof of part (2) of Conjecture 4.5 (see [66, Section 4.1]). But this is not substantiated. Recently, Luca and Stănică [86] proved the following result concerning part (2) of Conjecture 4.5.

**Theorem 4.6.** *Let p be any fixed odd prime. Then the diophantine equation*

$$x^2 = 2^{2b+2}p^{2t} - 2^{b+2}p^{t+r} + 1$$

*in positive integer unknowns* $x, b, t, r \geqslant 1$ *has at most* $2^{30,000}$ *solutions.*

In summary, it seems that we still do not have a complete proof of Conjecture 4.5. Thus Conjecture 4.4 is not completely settled either.

Turning to nonabelian reversible difference sets, we remark that the parameters of such difference sets are not as restricted as in the abelian case. There exist examples of nonabelian reversible difference sets whose parameters are not as specified in Conjecture 4.4, see [88,14]. For example, many nonabelian $(96, 20, 4)$ reversible difference sets were constructed in [14]. Finally we comment that if $D$ is a reversible difference set in a group $G$, then the Cayley graph $\mathrm{Cay}(G, D)$ is a strongly regular graph. Therefore reversible difference sets are closely related to Schur rings, strongly regular graphs and association schemes. We will see such connections in use in Section 7.

## 5. Difference sets with classical parameters

The Singer difference sets arise from the classical designs of points and hyperplanes in projective space $\mathrm{PG}(m-1, q)$; they are cyclic difference sets with parameters

$$v = \frac{q^m - 1}{q - 1}, \ k = \frac{q^{m-1} - 1}{q - 1}, \ \lambda = \frac{q^{m-2} - 1}{q - 1}, \tag{5.1}$$

where $m \geqslant 3$ and $q$ is a prime power. The parameters in (5.1) or the complementary parameters of (5.1) are called *classical parameters*. It is known that there exist many infinite families of cyclic difference sets with classical parameters which are inequivalent to the Singer difference sets; early examples of such difference sets are the GMW difference sets constructed in 1962 (see [42]). Initiated by [90,98,97], there has been a surge of activity in this sub-area of the theory of difference sets. For a survey of results up to 1999, we refer the reader to [118]. After [118] was written, more cyclic difference sets with classical parameters were constructed; several tough conjectures in this area were proved. The most significant result is the following theorem of Dillon and Dobbertin [34].

**Theorem 5.1.** *Let* $\mathbf{L} = \mathbb{F}_{2^m}$ *and for each* $k$ *satisfying* $1 \leqslant k < m/2$ *and* $\gcd(k, m) = 1$ *let* $\Delta_k(X) = (X+1)^d + X^d + 1$, *where* $d = 4^k - 2^k + 1$. *Then* $\mathcal{B}_k := \mathbf{L} \setminus \Delta_k(\mathbf{L})$ *is a difference set with classical parameters in* $\mathbf{L}^*$. *Moreover, for each fixed* $m$, *the* $\phi(m)/2$ *difference sets* $\mathcal{B}_k$ *are pairwise inequivalent.*

The proof of Theorem 5.1 uses techniques from Fourier analysis on the additive group of $\mathbb{F}_{2^m}$ and the theory of quadratic forms in characteristic 2. Note that Theorem 5.1 states that $\mathcal{B}_k$ is a difference set in the *multiplicative* group of $\mathbb{F}_{2^m}$, but the proof uses Fourier analysis on the *additive* group of $\mathbb{F}_{2^m}$. Such ideas of using additive characters to prove that a subset in $\mathbb{F}_{2^m}$ is a difference set in $\mathbb{F}_{2^m}^*$ appeared earlier in [117,33].

The paper [34] contains proofs of all five conjectures in [98], and the complete proof of the No–Chung–Yun conjecture in [97]. Besides these, [34] also contains a wealth of information on cyclic $(2^m-1, 2^{m-1}-1, 2^{m-2}-1)$ difference sets, Dickson and Müller–Cohen–Matthews polynomials, bent functions, and quadratic forms in characteristic 2. It follows from the results in [34] that every known $(2^m-1, 2^{m-1}-1, 2^{m-2}-1)$ cyclic difference set belongs to a series given by a constructive theorem. (For references on exhaustive searches for $(2^m-1, 2^{m-1}-1, 2^{m-2}-1)$ cyclic difference sets with small $m$, we refer the reader to [118].) This naturally raises the following problem.

**Problem 5.2.** *Does there exist a* $(2^m-1, 2^{m-1}-1, 2^{m-2}-1)$ *cyclic difference set inequivalent to the known ones*?

Based on [52], it seems very likely that the difference sets $\mathcal{B}_k$ in Theorem 5.1 are related to the maximal arc $\mathcal{C}(2^k) = \{(1, x, x^{2^k}, x^{2^k+1}) | x \in \mathbb{F}_{2^m}\} \cup \{(0, 0, 0, 1)\}$, where $\gcd(k, m) = 1$, in $\mathrm{PG}(3, 2^m)$. Note that Maschietti's construction [90] is based on hyperovals, which are maximal arcs of degree 2 in $\mathrm{PG}(2, 2^m)$. It is of interest to explore the geometry behind the difference sets $\mathcal{B}_k$. To this end, we ask the following question:

**Problem 5.3.** *Is there a geometric proof of Theorem* 5.1 *using maximal arcs in* $\mathrm{PG}(3, 2^m)$?

Next we consider difference sets with parameters (5.1) satisfying $q > 2$. At the end of the survey [118], we commented that there is not much known about difference sets with classical parameters (5.1), with the additional conditions that $q > 2$ and $m$ is prime. (Note that when $m$ is prime, the GMW construction [42] does not apply.) In particular, we asked for explanations of the three $(121, 40, 13)$ non-Singer difference sets listed in the survey paper [48] by Hall. There are now several families of $((3^m-1)/2, (3^{m-1}-1)/2, (3^{m-2}-1)/2)$ cyclic difference sets inequivalent to the Singer difference sets. To describe these new difference sets, we need some notation. As usual we use $\mathbb{F}_{q^m}^*$ to denote the multiplicative group of $\mathbb{F}_{q^m}$. Also we use $\mathrm{Tr}_{q^m/q}$ to denote the trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, and $\rho : \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ to denote the natural epimorphism.

**Theorem 5.4** (*Arasu and Player [4]*). *Let* $m > 1$ *be an odd integer. Let* $\tau : \mathbb{F}_{3^m} \to \mathbb{F}_{3^m}$ *be the map defined by* $\tau(x) = x + x^6$ *for all* $x \in \mathbb{F}_{3^m}$. *Then*

$$D = \frac{1}{3}(\rho(\tau(\mathbb{F}_{3^m}) \setminus \{0\}) - G),$$

*where* $G = \mathbb{F}_{3^m}^*/\mathbb{F}_3^*$, *is a difference set in* $G$ *with classical parameters.*

**Theorem 5.5** (*Helleseth et al. [51], Chandler and Xiang [21], and No [96]*). *Let* $q{=}3^e$, $e \geqslant 1$, *let* $m = 3k$, $k$ *a positive integer,* $d = q^{2k} - q^k + 1$, *and set*

$$R = \{x \in \mathbb{F}_{q^m} | \mathrm{Tr}_{q^m/q}(x + x^d) = 1\}. \tag{5.2}$$

*Then* $\rho(R)$ *is a* $((q^m-1)/(q-1), q^{m-1}, q^{m-2}(q-1))$ *difference set in* $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$.

Theorem 5.5 was first proved by using the language of sequences with ideal 2-level autocorrelation in [51] in the case $q = 3$. See [21,96] for a complete proof of this theorem (the paper [21] also showed that $R$ is a relative difference set). For future use, we will call this difference set $\rho(R)$ the HKM difference set.

**Theorem 5.6.** *Let $m \geqslant 3$ be an odd integer, let $d = 2 \cdot 3^{(m-1)/2} + 1$, and set*

$$R = \{x \in \mathbb{F}_{3^m} | \mathrm{Tr}_{3^m/3}(x + x^d) = 1\}. \tag{5.3}$$

*Then $\rho(R)$ is a $((3^m - 1)/2, 3^{m-1}, 2 \cdot 3^{m-2})$ difference set in $\mathbb{F}_{3^m}^*/\mathbb{F}_3^*$.*

Theorem 5.6 was conjectured by Lin [84], and recently proved by Arasu et al. [1]. For future use, we will call this difference set $\rho(R)$ the Lin difference set.

There are more constructions of cyclic difference sets with parameters (5.1) and with $q$ not necessarily equal to 2. No [96] used $d$-homogeneous functions on $\mathbb{F}_{q^m}^*$ over $\mathbb{F}_q$ with difference-balanced property to construct cyclic difference sets with classical parameters. Also Arasu [1] promised to give many more constructions of such difference sets by using Stickelberger's theorem on Gauss sums.

There is no doubt that more cyclic difference sets with parameters (5.1) and with $q > 2$ will be discovered. It seems to be more interesting to construct difference sets with classical parameters with a view to Hamada's conjecture (see Section 9).

## 6. Skew Hadamard difference sets

In this section, we consider skew Hadamard difference sets. A difference set $D$ in a finite group $G$ is called *skew Hadamard* if $G$ is the disjoint union of $D$, $D^{(-1)}$, and $\{1\}$, where $D^{(-1)} = \{d^{-1} | d \in D\}$. A classical example of skew Hadamard difference sets is the Paley difference set defined in Example 2.5. Let $D$ be a $(v, k, \lambda)$ skew Hadamard difference set in an abelian group $G$. Then we have

$$1 \notin D, \; k = \frac{v-1}{2}, \text{ and } \lambda = \frac{v-3}{4}.$$

If we employ group ring notation, then in $\mathbb{Z}[G]$, we have

$$\begin{aligned} DD^{(-1)} &= \frac{v+1}{4} + \frac{v-3}{4}G, \\ D + D^{(-1)} &= G - 1. \end{aligned}$$

Applying any nonprincipal character $\chi$ of $G$ to the above two equations, one has

$$\chi(D) = \frac{-1 \pm \sqrt{-v}}{2}.$$

This is an important property of skew Hadamard abelian difference sets which places severe restrictions on these difference sets. Skew Hadamard difference sets were studied by Johnsen [60], Camion and Mann [16], Jungnickel [62], and Chen et al. [24]. The results in [60,16,24] can be summarized as follows:

**Theorem 6.1.** *Let $D$ be a $(v, k, \lambda)$ skew Hadamard difference set in an abelian group $G$. Then $v$ is equal to a prime power $p^m \equiv 3 \pmod 4$, and the quadratic residues modulo $v$ are multipliers of $D$. Moreover, if $G$ has exponent $p^s$ with $s \geqslant 2$, then $s \leqslant (m+1)/4$. In particular,* if *$v = p^3$ or $p^5$, then $G$ must be elementary abelian.*

It was conjectured that if an abelian group $G$ contains a skew Hadamard difference set, then $G$ has to be elementary abelian. This is still open in general. Theorem 6.1 contains all known results on this conjecture. It was further conjectured some time ago that the Paley difference set in Example 2.5 is the only example of skew Hadamard difference sets in abelian groups. This conjecture is now disproved by Ding and Yuan [35], who constructed new skew Hadamard difference sets in $(\mathbb{F}_{3^m}, +)$ by using certain Dickson polynomials.

Let $a \in \mathbb{F}_q$ and let $n$ be a positive integer. We define the *Dickson polynomial* $D_n(X, a)$ over $\mathbb{F}_q$ by

$$D_n(X,a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-a)^j X^{n-2j},$$

where $\lfloor n/2 \rfloor$ is the largest integer $\leqslant n/2$. It is well known that the Dickson polynomial $D_n(X, a)$, $a \in \mathbb{F}_q^*$, is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(n, q^2 - 1) = 1$ (see [82, p. 356]). Let $m$ be a positive odd integer. For any $u \in \mathbb{F}_{3^m}^*$, define

$$g_u(X) = D_5(X^2, -u) = X^{10} - uX^6 - u^2X^2.$$

Since $D_5(X, -u)$ is a permutation polynomial of $\mathbb{F}_{3^m}$, we see that the map $g_u : \mathbb{F}_{3^m} \to \mathbb{F}_{3^m}$ induced by $g_u(X)$ is two-to-one from $\mathbb{F}_{3^m}^*$ to $\mathbb{F}_{3^m}^*$. In particular,

$$|\mathrm{Im}(g_u) \setminus \{0\}| = (3^m - 1)/2.$$

The following is the main theorem in [35].

**Theorem 6.2.** *Let $m$ be a positive odd integer, and let $u \in \mathbb{F}_{3^m}^*$. Then $\mathrm{Im}(g_u) \setminus \{0\}$ is a skew Hadamard difference set in $(\mathbb{F}_{3^m}, +)$. Moreover, $\mathrm{Im}(g_u) \setminus \{0\}$ is inequivalent to the Paley difference set formed by the nonzero squares of $\mathbb{F}_{3^m}$ if $m > 3$.*

The key observation used in the proof of Theorem 6.2 is the fact that for any nonzero $u \in \mathbb{F}_{3^m}$, $g_u(X)$ induces a planar function from $\mathbb{F}_{3^m}$ to itself, where $m$ is odd. In the special case where $u = -1$, this fact was first observed by Coulter and Matthews [26]. Since the exponent of each monomial in $g_u(X)$ can be written as $3^i + 3^j$, for some $i$ and $j$, $g_u(X)$ is a so-called Dembowski–Ostrom polynomial. It is well known [32] that any Dembowski–Ostrom polynomial over $\mathbb{F}_q$ inducing a planar function from $\mathbb{F}_q$ to itself will produce a translation plane (in fact, a semifield plane). Thus the polynomials $g_u(X)$ not only give rise to skew Hadamard difference sets, but also produce semifield planes. Coulter and Henderson [27] showed that $g_{-1}(X)$ over $\mathbb{F}_{3^m}$ gives rise to new semifield planes if $m > 3$ is odd. To completely sort out the isomorphism of affine planes produced by $g_u(X)$, they showed in [28] that it suffices to consider the cases $u = 1$ and $u = -1$ only, and proved the following theorem:

**Theorem 6.3.** *Let $g_1(X) = X^{10} - X^6 - X^2$ and $m$ be odd, so that $g_1(X)$ is a planar Dembowski–Ostrom polynomial over $\mathbb{F}_{3^m}$. If $m \geqslant 4$, then the affine plane produced by $g_1(X)$ via the standard procedure in* [32] *is not isomorphic to any known affine plane.*

## 7. Bush-type Hadamard matrices

In this section, we describe the recent construction of symmetric Bush-type Hadamard matrices in [95]. A Hadamard matrix $H = (H_{ij})$ of order $4n^2$, where $H_{ij}$ are $2n \times 2n$ block matrices, is said to be of *Bush-type* if

$$H_{ii} = J_{2n}, \text{ and } H_{ij}J_{2n} = J_{2n}H_{ij} = 0 \tag{7.1}$$

for $i \neq j$, $1 \leqslant i, j \leqslant 2n$. Here $J_{2n}$ denotes the all-one matrix of order $2n$. Bush [15] proved that the existence of a projective plane of order $2n$ implies the existence of a symmetric Bush-type Hadamard matrix of order $4n^2$. So if one can prove the nonexistence of symmetric Bush-type Hadamard matrices of order $4n^2$, where $n$ is odd, then the nonexistence of a projective plane of order $2n$, $n$ odd, will follow. This was Bush's original motivation for introducing Bush-type Hadamard matrices. (We will see that this approach to proving nonexistence of projective planes of order $2n$, $n$ odd, fails almost completely.) Kharaghani and his coauthors [70,56–58,65] rekindled the interest in Bush-type Hadamard matrices by showing that these matrices are very useful for constructions of symmetric designs and strongly regular graphs. We refer the reader to the recent survey [65] by Jungnickel and Kharaghani for known results on Bush-type matrices before [95] was written. Kharaghani [70] conjectured that Bush-type Hadamard matrices of order $4n^2$ exist for all $n$. While it is relatively easy to construct Bush-type Hadamard matrices of order $4n^2$ for all even $n$ for which a Hadamard matrix of order $2n$ exists (see [69]), it is not easy to decide whether such matrices of order $4n^2$ exist if $n > 1$ is an odd integer. In [65], Jungnickel and Kharaghani wrote "Bush-type Hadamard matrices of order $4n^2$, where $n$ is odd, seem pretty hard to construct. Examples are known for $n = 3$, $n = 5$, and $n = 9$ (see [56–58], respectively); all other cases are open". Very recently the following theorem is proved in [95].

**Theorem 7.1.** *There exists a symmetric Bush-type Hadamard matrix of order $4m^4$ for every odd $m$.*

The proof of Theorem 7.1 is based on the construction of $(4p^4, 2p^4 - p^2, p^4 - p^2)$ Hadamard difference sets in [116] and Turyn's compositiontheorem in [109]. It is well known that the existence of a symmetric Bush-type Hadamard matrix of order $4n^2$ is equivalent to the existence of a strongly regular graph with parameters

$$v = 4n^2,\ k = 2n^2 - n,\ \lambda = \mu = n^2 - n$$

and with the additional property that the vertex set of the graph can be partitioned into $2n$ disjoint cocliques of size $2n$. The latter object is in turn equivalent to an amorphic three-class association scheme by a result of Haemers and Tonchev [46]. So in order to construct symmetric Bush-type matrices, we simply construct the special three-class association schemes. This was done in two steps in [95]. First, we observe that the construction in [116] (together with the necessary two-intersection sets constructed in [23]) not only produces a reversible $(4p^4, 2p^4 - p^2, p^4 - p^2)$ Hadamard difference set in $G = \mathbb{Z}_2^2 \times \mathbb{Z}_p^4$, $p$ an odd prime, but also a partition of $G$ into the disjoint union of two reversible $(4p^4, 2p^4 - p^2, p^4 - p^2)$ Hadamard difference sets and a subgroup of order $2p^2$. Hence we obtain a three-class amorphic association scheme on $4p^4$ vertices. Second, we show that Turyn's composition theorem "respects" the aforementioned partitions. Putting these together, Theorem 7.1 is proved.

Kharaghani [70,71] showed how to use Bush-type Hadamard matrices to simplify Ionin's method [54] for constructing symmetric designs. Based on his constructions in [70,71], symmetric designs with new parameters are obtained from Theorem 7.1.

**Theorem 7.2** (*Muzychuk and Xiang [95]*). *Let m be an odd integer. If $q = (2m^2 - 1)^2$ is a prime power, then there exists twin symmetric designs with parameters*

$$v = 4m^4 \frac{(q^{\ell+1} - 1)}{q - 1},\ k = q^\ell(2m^4 - m^2),\ \lambda = q^\ell(m^4 - m^2) \tag{7.2}$$

*for every positive integer $\ell$.*

**Theorem 7.3** (*Muzychuk and Xiang [95]*). *Let m be an odd integer. If $q = (2m^2 + 1)^2$ is a prime power, then there exists Siamese twin symmetric designs with parameters*

$$v = 4m^4 \frac{(q^{\ell+1} - 1)}{q - 1},\ k = q^\ell(2m^4 + m^2),\ \lambda = q^\ell(m^4 + m^2)$$

*for every positive integer $\ell$.*

Theorem 7.2 can be viewed as further evidence in support of the following conjecture of Ionin and Kharaghani [55].

**Conjecture 7.4.** *For any integers $h \neq 0$ and $\ell \geqslant 0$, if $q = (2h-1)^2$ is a prime power, then there exists a symmetric design with the following parameters*:

$$v = 4h^2 \frac{(q^{\ell+1}-1)}{q-1}, \; k = q^{\ell}(2h^2 - h), \; \lambda = q^{\ell}(h^2 - h).$$

In relation to Theorem 7.2, we also ask the following question.

**Problem 7.5.** *Does there exist a difference set with the parameters in* (7.2)?

## 8. Nonabelian difference sets

While we have a well developed theory of abelian difference sets, our knowledge of nonabelian difference sets is fragmentary. For a survey of the status of nonabelian difference sets up to 1999, we refer the reader to [83]. Most of the recent papers on nonabelian difference sets are concerned with difference sets with specific parameters or difference sets in specific groups. We collect several recent results on nonabelian difference sets in this section.

The first result concerns difference sets in dihedral groups. It is a well-known conjecture that there exists no nontrivial difference set in any dihedral group. Leung et al. [79] made considerable progress towards this conjecture. In particular, they proved that the parameters of a difference set in a dihedral group (in short, a dihedral difference set) are quite restrictive. (We note that the order of a dihedral difference set must be a square since the order of a dihedral group is even.) More recently, Leung and Schmidt [80] proved the following asymptotic nonexistence result on dihedral difference sets.

**Theorem 8.1.** *Let $p_1, p_2, \ldots, p_r$ be distinct primes. There are only finitely many u's of the form $\prod_{i=1}^{r} p_i^{\alpha_i}$ for which a dihedral difference set of order $u^2$ can exist.*

More detailed nonexistence results on dihedral difference sets can be found in [80]. For example, it is proved in [80] that with the possible exception of $u = 735$ there is no difference set of order $u^2 \leqslant 10^6$ in any dihedral group.

Next we consider nonabelian Hadamard difference sets with parameters $(4p^2, 2p^2 - p, p^2 - p)$, where $p$ is a prime. McFarland in his celebrated paper [92] proved that if a $(4p^2, 2p^2 - p, p^2 - p)$ abelian difference set exists, where $p$ is a prime, then $p = 2$ or 3. Smith [106] could construct a difference set in a nonabelian group of order 100, and he called such a difference set genuinely nonabelian since an abelian counterpart does not exist by McFarland's result. Iiam [53] studied nonabelian $(4p^2, 2p^2 - p, p^2 - p)$ difference sets systematically, and could rule out a little bit more than one half of the groups of order $4p^2$, $p \geqslant 5$ a prime, from having a $(4p^2, 2p^2 - p, p^2 - p)$ Hadamard difference set. While there are more constructions of nonabelian difference sets in groups of order 100 [41,110,61], no nonabelian $(4p^2, 2p^2 - p, p^2 - p)$ difference set with $p > 5$ a prime has been found so far.

Becker [11] recently undertook a systematic study of nonabelian difference sets with parameters $(120, 35, 10)$. Abelian difference sets with these parameters were shown not to exist by Turyn [107]. Thus if a nonabelian $(120, 35, 10)$ difference set exists, it will be genuinely nonabelian. The main result of Becker [11] is the following theorem:

**Theorem 8.2.** *If a solvable group contains a* $(120, 35, 10)$ *difference set, then it is one of the following groups*:

$$G_1 = \langle x, y, z | y^3 = x^5 = z^8 = zxz^{-1}x^{-1} = zyz^{-1}y = xyx^{-1}y^{-1} = 1 \rangle,$$

$$G_3 = \langle x, y, z | y^3 = x^5 = z^8 = zyz^{-1}y = zxz^{-1}x = yxy^{-1}x^{-1} = 1 \rangle,$$

$$G_7 = \langle x, y, z | y^3 = x^5 = z^8 = zyz^{-1}y = yxy^{-1}x^{-1} = zxz^{-1}x^{-2} = 1 \rangle.$$

The existence of a $(120, 35, 10)$ difference set in $G_1$ (respectively, in $G_3$ and $G_7$) is not settled.

We end this section by mentioning the following problem related to the material discussed in Section 6. It is well known and easy to prove that any group of order $p^2$, $p$ a prime, is abelian. Thus it is natural to ask

**Problem 8.3.** (1) *Let* $p > 3$ *be a prime. Does there exist a difference set in a nonabelian group of order* $p^3$?

(2) *Let* $p > 3$ *be a prime congruent to* 3 *modulo* 4. *Does there exist a skew Hadamard difference set in a nonabelian group of order* $p^3$?

For difference sets in nonabelian groups of order 27, we refer the reader to Kibler [74].

## 9. The *p*-ranks and SNF of difference sets with classical parameters

In the study of difference sets with classical parameters, one often faces the following question. After constructing a family of difference sets with classical parameters, how can one tell whether the difference sets constructed are equivalent to the known ones or not? This question was usually answered by comparison of $p$-ranks of the difference sets involved. For example, in [36], we computed the 2-ranks of the cyclic difference sets from hyperovals and showed that these difference sets are inequivalent to previously known cyclic difference sets with the same parameters. Indeed, testing inequivalence of difference sets provided much motivation for recent work on $p$-ranks of difference sets. But we should not forget that another motivation for studying $p$-ranks of difference sets with classical parameters comes from Hamada's conjecture.

**Conjecture 9.1** (*Hamada [49]*). *Let* $\mathcal{D}$ *be a symmetric design with the classical parameters*

$$((q^m - 1)/(q - 1), (q^{m-1} - 1)/(q - 1), (q^{m-2} - 1)/(q - 1)),$$

*where $q = p^t$, $p$ a prime. Then one has*

$$\mathrm{rank}_p \mathcal{D} \geqslant \binom{p+m-2}{m-1}^t + 1,$$

*with equality if and only if $\mathcal{D}$ is the development of a classical Singer difference set.*

Hamada's conjecture was proved to be true in the case $q = 2$ by Hamada and Ohmori [50]. There is little progress towards Conjecture 9.1 after [50]. Even though there is some doubt that Conjecture 9.1 is true for an arbitrary symmetric design $\mathcal{D}$ with classical parameters (see [63, p. 311]), it is very likely that the conjecture is true in the special case where $\mathcal{D}$ is developed from a cyclic difference set. Therefore, it is of interest to ask the following question.

**Problem 9.2.** *Is it possible to give a proof of Hamada's conjecture under the extra assumption that $\mathcal{D}$ is developed from a cyclic difference set*?

Turning to computations of $p$-ranks of difference sets from specific families, we report that the $p$-ranks of the classical GMW difference sets are computed in [3]. This solves an open problem mentioned in [100, p. 84; 12, p. 461]. However, we should mention that due to the involved product construction, the $p$-rank formulae in [3] are not very explicit. A related problem is to decide whether inequivalent classical GMW difference sets give rise to nonisomorphic symmetric designs. This problem is now settled by Kantor [68] who showed that isomorphism implies equivalence.

We mention more $p$-rank results. The 3-ranks of the difference sets in Theorem 5.4 are computed in [4], and the 3-ranks of the HKM difference sets are determined in [21,99]. The paper [99] also contains the computations of the 3-ranks of the Lin difference sets. The techniques for computing $p$-ranks in [3,21,4] are similar to that in [36]; the use of Gauss and Jacobi sums and Stickelberger's theorem on Gauss sums is becoming standard for this purpose.

From the computations of 3-ranks in [21,99], we know that in the case $q = 3$, $m = 3k$, $k > 1$, the 3-rank of the HKM difference set is $2m^2 - 2m$. The Lin difference set also has 3-rank $2m^2 - 2m$, where $m > 3$ is odd, see [99]. Therefore when $m$ is an odd multiple of 3, these two difference sets have the same 3-rank. Hence they can not be distinguished by 3-ranks. It is therefore natural to consider using the Smith normal form (SNF) of these two families of difference sets to distinguish them. The following lemma is very useful for determining the SNF of $(v, k, \lambda)$ difference sets with $\gcd(v, k - \lambda) = 1$.

**Lemma 9.3** (*Chandler and Xiang [22]*). *Let $G$ be an abelian group of order $v$, let $p$ be a prime not dividing $v$, and let $\mathfrak{P}$ be a prime ideal in $\mathbb{Z}[\xi_v]$ lying above $p$, where $\xi_v$ is a complex primitive $v$*th *root of unity. Let $D$ be a $(v, k, \lambda)$ difference set in $G$, and let $\alpha$ be a positive integer. Then the number of invariant factors of $D$ which are not divisible by $p^\alpha$ is equal to the number of complex characters $\chi$ of $G$ such that $\chi(D) \not\equiv 0 \pmod{\mathfrak{P}^\alpha}$.*

Setting $\alpha = 1$ in Lemma 9.3, we see that the $p$-rank of $D$ is equal to the number of complex characters $\chi$ such that $\chi(D) \not\equiv 0 \pmod{\mathfrak{P}}$, which was proved by MacWilliams and Mann [89]. Using Lemma 9.3, Fourier transforms, and Stickelberger's congruence on Gauss sums, we [22] computed the number of 3's in the SNF of the Lin and HKM difference sets.

**Theorem 9.4.** *Let $m > 9$. Then the number of 3's in the Smith normal form of the HKM difference sets with parameters $((3^m - 1)/2, 3^{m-1}, 2 \cdot 3^{m-2})$ is*

$$\frac{2}{3}m^4 - 4m^3 - \frac{28}{3}m^2 + 62m + \varepsilon(m) \cdot m.$$

*The number of 3's in the Smith normal form of the Lin difference sets when $m > 7$ is*

$$\frac{2}{3}m^4 - 4m^3 - \frac{14}{3}m^2 + 39m + \delta(m) \cdot m.$$

*The values of $\varepsilon(m)$ and $\delta(m)$ are 0 or 1.*

Since the two "almost" polynomial functions in Theorem 9.4 are never equal when $m > 9$, and since the Smith normal forms of the Lin and HKM difference sets are also different when $m = 9$ (by direct computations), the following conclusion is reached.

**Theorem 9.5.** *Let $m$ be an odd multiple of 3. The Lin and HKM difference sets with parameters $(\frac{3^m-1}{2}, 3^{m-1}, 2 \cdot 3^{m-2})$ are inequivalent when $m > 3$, and the associated symmetric designs are nonisomorphic when $m > 3$.*

The work in [22] motivated us to ask whether it is true that two symmetric designs with the same parameters and having the same SNF are necessarily isomorphic. The answer to this question is negative. It is known [6] that the Smith normal form of a projective plane of order $p^2$, $p$ prime, is

$$1^r p^{(p^4+p^2-2r+2)} (p^2)^{(r-2)} ((p^2+1)p^2)^1,$$

where the exponents indicate the multiplicities of the invariant factors and $r$ is the $p$-rank of the plane. That is, the $p$-rank of the plane completely determines the Smith normal form of the plane. There are four projective planes of order 9. The desarguesian one has 3-rank 37, while the other three all have 3-rank 41 (cf. [103]), so the three non-desarguesian projective planes have the same Smith normal form, yet they are nonisomorphic. However, the answer to the following more restricted question is not known.

**Problem 9.6.** *If two cyclic difference sets with classical parameters have the same Smith normal form, are the associated designs necessarily isomorphic*?

## 10. The diagonal forms of some set-inclusion matrices

Let $X$ be a finite set with $v$ elements, and let $t$ and $k$ be two integers such that $0 < t \leqslant k < v$. Let $W_{tk}$ be the $\binom{v}{t}$ by $\binom{v}{k}$ matrix with rows indexed by the $t$-subsets of $X$ and columns indexed by the $k$-subsets of $X$ and with the $(T, K)$-entry 1 if $T \subseteq K$ and 0 otherwise. These higher incidence matrices proved to be very useful in many combinatorial investigations, e.g., in the study of $t$-designs and extremal set theory (see [73,7]). (In fact, the authors of [73] used the term algebraic design theory to mean the study of these higher incidence matrices, and its applications to design theory problems. We certainly have enlarged the scope of algebraic design theory here.)

Gottlieb [43] probably was the first to study these matrices $W_{tk}$. However, it was Graver and Jurkat [45] and Wilson [112] who first used these matrices to study (signed) $t$-designs. Later, Foody and Hedayat [37], and Graham et al. [44] further developed the theory of null designs (or trades), and used it to study designs. We refer the reader to [73] for a survey of some results on these higher incidence matrices. We mention that in recent papers [17,105], Singhi and his coauthor defined tags on subsets, and used them to study the matrices $W_{tk}$ and certain general $(t, k)$ existence problems. In the following, we collect some results on $p$-ranks and diagonal forms of $W_{tk}$. These are mainly the results of Wilson in [113–115].

In [113], Wilson found the $p$-rank and a diagonal form of $W_{tk}$. We state his theorems as follows:

**Theorem 10.1.** *For $t \leqslant \min\{k, v-k\}$, the rank of $W_{tk}$ modulo a prime $p$ is*

$$\sum \binom{v}{i} - \binom{v}{i-1},$$

*where the sum is extended over those indices $i$ such that $p$ does not divide the binomial coefficient $\binom{k-i}{t-i}$.*

**Theorem 10.2.** *If $t \leqslant \min\{k, v-k\}$, then $W_{tk}$ has as a diagonal form the $\binom{v}{t} \times \binom{v}{k}$ diagonal matrix with diagonal entries $\binom{k-i}{t-i}$ with multiplicity $\binom{v}{i} - \binom{v}{i-1}$.*

Frumkin and Yakir [38] gave a different proof for Theorems 10.1, 10.2 by using representations of the symmetric group $S_v$. They also considered similar problems for the $q$-analogues of $W_{tk}$ but only obtained partial results in that case (see Section 11).

Wilson [114] considered certain integral matrices which are useful for his theory of signed hypergraph designs, and found diagonal forms for those matrices.

**Theorem 10.3** (*Wilson [114]*). *Let $X$ be a $v$-set. Let $M$ be an integral matrix whose $\binom{v}{t}$ rows are indexed by the $t$-subsets of $X$ and which has the property that the set of column vectors of $M$ is invariant under the action of the symmetric group $S_v$ acting on the $t$-subsets of $X$. Let $d_i$ be the greatest common divisor of all entries of $W_{it}M$,*

*$i = 0, 1, \ldots, t$. Then a diagonal form for $M$ is given by the diagonal entries $d_i$ with multiplicity $\binom{v}{i} - \binom{v}{i-1}$, $i = 0, 1, \ldots, t$.*

More recently, Wilson [115] considered incidence matrices of $t$-subsets and hypergraphs. He showed nice applications of these matrices to a zero-sum Ramsey-type problem modulo 2 and to inequalities concerning $t$-wise balanced designs. For details, we refer the reader to [115].

## 11. The SNF of the incidence matrices of points and subspaces in PG$(m, q)$ and AG$(m, q)$

In this section, we describe the recent work in [20] on the SNF of the incidence matrices of the 2-designs in Examples 2.3 and 2.4. Note that these incidence matrices are special cases of the $q$-analogues of the matrices $W_{tk}$ discussed in Section 10. We will concentrate on the design coming from projective geometry. The SNF of the design coming from AG$(m, q)$ follows from the results in the projective case.

Let PG$(m, q)$ be the $m$-dimensional projective space over $\mathbb{F}_q$ and let $V$ be the underlying $(m + 1)$-dimensional vector space over $\mathbb{F}_q$, where $q = p^t$, $p$ a prime. For any $d$, $1 \leqslant d \leqslant m$, we will refer to $d$-dimensional subspaces of $V$ as $d$-subspaces and denote the set of these subspaces in $V$ as $\mathcal{L}_d$. The set of projective points is then $\mathcal{L}_1$. The pair $(\mathcal{L}_1, \mathcal{L}_d)$, where $d > 1$, with incidence being set inclusion, is the 2-design in Example 2.3. Let $A$ be an incidence matrix of the 2-design $(\mathcal{L}_1, \mathcal{L}_d)$. So $A$ is a $b \times v$ $(0, 1)$-matrix, where $b = \begin{bmatrix} m+1 \\ d \end{bmatrix}_q$ and $v = \begin{bmatrix} m+1 \\ 1 \end{bmatrix}_q$. We will determine the Smith normal form of $A$. There is a somewhat long history of this problem. We refer the reader to [20] for a detailed account.

The following theorem shows that all but one invariant factor of $A$ are $p$ powers.

**Theorem 11.1.** *Let $A$ be the matrix defined as above. The invariant factors of $A$ are all $p$-powers except for the* $v$th *invariant, which is a $p$-power times $(q^d - 1)/(q - 1)$.*

This has been known at least since [104], and it essentially follows from the fact that $A$ is the incidence matrix of a 2-design. For a detailed proof, see [20]. In view of Theorem 11.1, to determine the SNF of $A$, it suffices to determine the multiplicity of $p^i$ appearing as an invariant factor of $A$. It will be convenient to view $A$ as a matrix with entries from a $p$-adic local ring $R$ (some extension ring of $\mathbb{Z}_p$, the ring of $p$-adic integers). We will define this ring $R$ and introduce two sequences of $R$-modules and two sequences of $q$-ary codes in the following subsection:

### *11.1. R-modules and q-ary codes*

Let $q = p^t$ and let $K = \mathbb{Q}_p(\xi_{q-1})$ be the unique unramified extension of degree $t$ over $\mathbb{Q}_p$, the field of $p$-adic numbers, where $\xi_{q-1}$ is a primitive $(q-1)$th root of unity in $K$. Let $R = \mathbb{Z}_p[\xi_{q-1}]$ be the ring of integers in $K$ and let $\mathfrak{p}$ be the unique maximal ideal in $R$ (in fact, $\mathfrak{p} = pR$). Then $R$ is a principal ideal domain, and the reduction of $R \pmod{\mathfrak{p}}$ is $\mathbb{F}_q$. Define $\bar{x}$ to be $x \pmod{\mathfrak{p}}$ for $x \in R$.

We now view the above matrix $A$ as a matrix with entries from $R$. Define

$$M_i = \{x \in R^{\mathcal{L}_1} | Ax^\top \in p^i R^{\mathcal{L}_d}\}, \quad i = 0, 1, \ldots \ .$$

Here we are thinking of elements of $R^{\mathcal{L}_1}$ as row vectors of length $v$. Then we have a sequence of nested $R$-modules

$$R^{\mathcal{L}_1} = M_0 \supseteq M_1 \supseteq \cdots \ .$$

Define $\overline{M}_i = \{(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_v) \in \mathbb{F}_q^{\mathcal{L}_1} | (x_1, x_2, \ldots, x_v) \in M_i\}$ for $i = 0, 1, 2, \ldots$ . For example,

$$\overline{M}_1 = \left\{ (\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_v) \in \mathbb{F}_q^{\mathcal{L}_1} | A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_v \end{pmatrix} \in pR^{\mathcal{L}_d} \right\}. \tag{11.1}$$

That is, $\overline{M}_1$ is the dual code of the $q$-ary (block) code of the 2-design $(\mathcal{L}_1, \mathcal{L}_d)$. We have a sequence of nested $q$-ary codes

$$\mathbb{F}_q^{\mathcal{L}_1} = \overline{M}_0 \supseteq \overline{M}_1 \supseteq \cdots \ .$$

This is similar to what Lander did for symmetric designs; see [76,85, p. 399]. Note that if $i > v_p(d_v)$, where $v_p$ is the $p$-adic valuation and $d_v$ is the $v$th invariant factor of $A$, then $\overline{M}_i = \{0\}$. It follows that there exists a smallest index $\ell$ such that $\overline{M}_\ell = \{0\}$. So we have a finite filtration

$$\mathbb{F}_q^{\mathcal{L}_1} = \overline{M}_0 \supseteq \overline{M}_1 \supseteq \cdots \supseteq \overline{M}_\ell = \{0\}.$$

For completeness, we also define

$$N_i = \{x \in R^{\mathcal{L}_1} | p^{i-1}x \in R\text{-span of the rows of } A\}, \quad i = 0, 1, \ldots \ .$$

For example, $N_1$ is simply the $R$-span of the rows of $A$. We have another sequence of nested $R$-modules associated with $A$:

$$\{0\} = N_0 \subseteq N_1 \subseteq \cdots \ .$$

Similarly, we have a sequence of $q$-ary codes

$$\{0\} = \overline{N}_0 \subseteq \overline{N}_1 \subseteq \cdots \subseteq \mathbb{F}_q^{\mathcal{L}_1}.$$

We have the following easy but important lemma. See [20] for its proof.

**Lemma 11.2.** *For* $0 \leqslant i \leqslant \ell - 1$, $p^i$ *is an invariant factor of* $A$ *with multiplicity* $\dim_{\mathbb{F}_q}(\overline{M}_i/\overline{M}_{i+1})$.

In what follows, we will determine $\dim_{\mathbb{F}_q}(\overline{M}_i)$, for each $i \geqslant 0$. In fact, we will construct an $\mathbb{F}_q$-basis for each $\overline{M}_i$. To this end, we construct a basis of $\mathbb{F}_q^{\mathcal{L}_1}$ first.

### 11.2. Monomial basis of $\mathbb{F}_q^{\mathcal{L}_l}$ and types of basis monomials

Let $V = \mathbb{F}_q^{m+1}$. Then every function $f : V \to \mathbb{F}_q$ can be written in the form

$$f(\mathbf{x}) = \sum_{\substack{0 \leqslant b_i \leqslant q-1 \\ 0 \leqslant i \leqslant m}} \lambda_{b_0, b_1, \ldots, b_m} \prod\nolimits_{i=0}^{m} x_i^{b_i} \tag{11.2}$$

for unique $\lambda_{b_0,b_1,\ldots,b_m} \in \mathbb{F}_q$. Since the characteristic function of $\{0\}$ in $V$ is $\prod_{i=0}^{m}(1 - x_i^{q-1})$, we obtain a basis for $\mathbb{F}_q^{V\setminus\{0\}}$ by excluding $x_0^{q-1}x_1^{q-1}\cdots x_m^{q-1}$ (some authors prefer to exclude $x_0^0 x_1^0 \cdots x_m^0$, see [39]).

The functions on $V \setminus \{0\}$ which descend to $\mathcal{L}_1$ are exactly those which are invariant under scalar multiplication by $\mathbb{F}_q^*$. Therefore, we obtain a basis $\mathcal{M}$ of $\mathbb{F}_q^{\mathcal{L}_1}$ as follows.

$$\mathcal{M} = \left\{ \prod_{i=0}^{m} x_i^{b_i} \,|\, 0 \leqslant b_i \leqslant q-1, \sum_i b_i \equiv 0 \pmod{q-1}, (b_0, b_1, \ldots, b_m) \right.$$
$$\left. \neq (q-1, q-1, \ldots, q-1) \right\}.$$

This basis $\mathcal{M}$ will be called the *monomial basis* of $\mathbb{F}_q^{\mathcal{L}_1}$, and its elements are called *basis monomials*.

Next we define the type of a nonconstant basis monomial. Let $\mathcal{H}$ denote the set of $t$-tuples $(s_0, s_1, \ldots, s_{t-1})$ of integers satisfying (for $0 \leqslant j \leqslant t-1$) the following:

$$\begin{aligned} &(1)\quad 1 \leqslant s_j \leqslant m, \\ &(2)\quad 0 \leqslant p s_{j+1} - s_j \leqslant (p-1)(m+1), \end{aligned} \tag{11.3}$$

with the subscripts read (mod $t$). The set $\mathcal{H}$ was introduced in [49], and used in [9] to describe the module structure of $\mathbb{F}_q^{\mathcal{L}_1}$ under the natural action of $\mathrm{GL}(m+1, q)$.

For a nonconstant basis monomial

$$f(x_0, x_1, \ldots, x_m) = x_0^{b_0} \cdots x_m^{b_m},$$

in $\mathcal{M}$, we expand the exponents

$$b_i = a_{i,0} + pa_{i,1} + \cdots + p^{t-1}a_{i,t-1} \quad 0 \leqslant a_{i,j} \leqslant p-1$$

and let

$$\lambda_j = a_{0,j} + \cdots + a_{m,j}. \tag{11.4}$$

Because the total degree $\sum_{i=0}^{m} b_i$ is divisible by $q-1$, there is a uniquely defined $t$-tuple $(s_0, \ldots, s_{t-1}) \in \mathcal{H}$ [9] such that

$$\lambda_j = ps_{j+1} - s_j.$$

One way of interpreting the numbers $s_j$ is that the total degree of $f^{p^i}$ is $s_{t-i}(q-1)$, when the exponent of each coordinate $x_i$ is reduced to be no more than $q-1$ by the substitution $x_i^q = x_i$. We will say that $f$ is of *type* $(s_0, s_1, \ldots, s_{t-1})$.

Let $c_i$ be the coefficient of $x^i$ in the expansion of $(\sum_{k=0}^{p-1} x^k)^{m+1}$. Explicitly,

$$c_i = \sum_{j=0}^{\lfloor i/p \rfloor} (-1)^j \binom{m+1}{j} \binom{m+i-jp}{m}.$$

**Lemma 11.3.** *Let $c_i$ and $\lambda_j$ be defined as above. The number of basis monomials in $\mathcal{M}$ of type $(s_0, s_1, \ldots, s_{t-1})$ is $\prod_{j=0}^{t-1} c_{\lambda_j}$.*

The proof of this lemma is straightforward, see [20]. For $(s_0, s_1, \ldots, s_{t-1}) \in \mathcal{H}$, we will use $c_{(s_0,s_1,\ldots,s_{t-1})}$ to denote the number of basis monomials in $\mathcal{M}$. The above lemma gives a formula for $c_{(s_0,s_1,\ldots,s_{t-1})}$.

### *11.3. Modules of the general linear group, Hamada's formula and the SNF of A*

Let $G = \mathrm{GL}(m+1, q)$. Then $G$ acts on $\mathcal{L}_1$ and $\mathcal{L}_d$, and $G$ is an automorphism group of the design $(\mathcal{L}_1, \mathcal{L}_d)$. Hence each $M_i$ is an $RG$-submodule of $R^{\mathcal{L}_1}$ and each $\overline{M}_i$ is an $\mathbb{F}_q G$-submodule of $\mathbb{F}_q^{\mathcal{L}_1}$. In [9], the submodule lattice of $\mathbb{F}_q^{\mathcal{L}_1}$ is completely determined, and it is described via a partial order on $\mathcal{H}$. We will need the following result which follows easily from the results in [9]. To simplify the statement of the theorem, we say that a basis monomial $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m}$ *appears* in a function $f \in \mathbb{F}_q^{\mathcal{L}_1}$ if when we write $f$ as the linear combination of basis monomials, the coefficient of $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m}$ is nonzero.

**Theorem 11.4.** (1) *Every $\mathbb{F}_q G$-submodule of $\mathbb{F}_q^{\mathcal{L}_1}$ has a basis consisting of all basis monomials in the submodule.*

(2) *Let $M$ be any $\mathbb{F}_q G$-submodule of $\mathbb{F}_q^{\mathcal{L}_1}$ and let $f \in \mathbb{F}_q^{\mathcal{L}_1}$. Then $f \in M$ if and only if each monomial appearing in $f$ is in $M$.*

For the proof of (1), see [20]. Part (2) follows from part (1) easily. The following is the main theorem on $\overline{M}_1$. It was proved by Delsarte [31] in 1970, and later in [39,9].

**Theorem 11.5.** *Let $\overline{M}_1$ be defined as above, i.e., $\overline{M}_1$ is the dual code of the $q$-ary* (*block*) *code of the* 2*-design* $(\mathcal{L}_1, \mathcal{L}_d)$.

(1) *For any $f \in \mathbb{F}_q^{\mathcal{L}_1}$, we have $f \in \overline{M}_1$ if and only if every basis monomial appearing in $f$ is in $\overline{M}_1$.*
(2) *Let $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m}$ be a basis monomial of type $(s_0, s_1, \ldots, s_{t-1})$. Then $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m} \in \overline{M}_1$ if and only if there exists some $j$, $0 \leqslant j \leqslant t-1$, such that $s_j < d$.*

This is what Glynn and Hirschfeld [39] called “the main theorem of geometric codes”. As a corollary, we have

**Corollary 11.6.** (1) *The dimension of $\overline{M}_1$ is*

$$\dim_{\mathbb{F}_q} \overline{M}_1 = \sum_{\substack{(s_0, s_1, \ldots, s_{t-1}) \in \mathcal{H} \\ \exists j, s_j < d}} c_{(s_0, s_1, \ldots, s_{t-1})}.$$

(2) *The $p$-rank of $A$ is*

$$\operatorname{rank}_p(A) = 1 + \sum_{\substack{(s_0, s_1, \ldots, s_{t-1}) \in \mathcal{H} \\ \forall j, s_j \geqslant d}} c_{(s_0, s_1, \ldots, s_{t-1})}.$$

The rank formula in part (2) of the above corollary is the so-called Hamada’s formula.

Generalizing Theorem 11.5, we proved the following theorem in [20]:

**Theorem 11.7.** *Let $\alpha \geqslant 1$ be an integer, and let $\overline{M}_\alpha$ be defined as above.*

(1) *For any $f \in \mathbb{F}_q^{\mathcal{L}_1}$, we have $f \in \overline{M}_\alpha$ if and only if every basis monomial appearing in $f$ is in $\overline{M}_\alpha$.*
(2) *Let $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m}$ be a basis monomial of type $(s_0, s_1, \ldots, s_{t-1})$. Then $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m} \in \overline{M}_\alpha$ if and only if $\sum_{j=0}^{t-1} \max\{0, d - s_j\} \geqslant \alpha$*

An immediate corollary is

**Corollary 11.8.** *Let $0 \leqslant \alpha \leqslant (d-1)t$, and let $h(\alpha, m, d+1)$ be the multiplicity of $p^{\alpha}$ appearing as an invariant factor of A. Then*

$$h(\alpha, m, d+1) = \delta(0, \alpha) + \sum_{\substack{(s_0, s_1, \ldots, s_{t-1}) \in \mathcal{H} \\ \sum_j \max\{0, d-s_j\} = \alpha}} c_{(s_0, s_1, \ldots, s_{t-1})},$$

*where*

$$\delta(0, \alpha) = \begin{cases} 1 & \text{if } \alpha = 0, \\ 0 & \text{otherwise}. \end{cases}$$

We give some indication on how Theorem 11.7 was proved in [20]. Of course Part (1) of Theorem 11.7 follows from the more general result in Theorem 11.4. About Part (2) of the theorem, if $\sum_{j=0}^{t-1} \max\{0, d-s_j\} \geqslant \alpha$, we need to show that there exists a lifting of the monomial $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m}$ to $R^{\mathcal{L}_1}$ that is in $M_\alpha$. It turns out that the Teichmüller lifting $T(x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m})$ of $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m}$ will suit our purpose. Indeed to show that $T(x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m}) \in M_\alpha$, we used a theorem of Wan [111] which gives a lower bound on the $p$-adic valuation of certain multiplicative character sums. The other direction of Part (2) of Theorem 11.7 is much more difficult to prove. We need to prove that if $\sum_{j=0}^{t-1} \max\{0, d-s_j\} < \alpha$, then no lifting of $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m}$ to $R^{\mathcal{L}_1}$ is in $M_\alpha$. We need to use the action of $G$ on $M_\alpha$, a special but very useful group ring element in $RG$ involving transvections in $G$, Jacobi sums, and Stickelberger's theorem on Gauss sums to achieve this. For details, we refer the reader to [20].

We also state the counterpart of Theorem 11.7 for the $q$-ary codes $\overline{N}_\alpha$.

**Theorem 11.9.** *Let $\alpha \geqslant 1$ be an integer, and let $\overline{N}_\alpha$ be defined as above.*

(1) *For any $f \in \mathbb{F}_q^{\mathcal{L}_1}$, we have $f \in \overline{N}_\alpha$ if and only if every basis monomial appearing in $f$ is in $\overline{N}_\alpha$.*
(2) *Let $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m}$ be a basis monomial of type $(s_0, s_1, \ldots, s_{t-1})$. Then $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m} \in \overline{N}_\alpha$ if and only if $\sum_{j=0}^{t-1} \max\{0, d-(m+1)+s_j\} < \alpha$*

We mention that the $p$-adic ideas here and the results in Theorem 11.7 have already found applications in problems in finite geometry, namely in controlling the intersection sizes of unitals in $\mathrm{PG}(2, q^2)$. These are contained in the recent paper of Chandler [19]

### *11.4. The SNF of the 2-design in Example 2.4*

Let $\mathrm{AG}(m, q)$ be the $m$-dimensional affine space over $\mathbb{F}_q$, where $q = p^t$, $p$ is a prime. Let $\mathcal{D}$ be the design in Example 2.4, i.e., the design of the points and $d$-flats of $\mathrm{AG}(m, q)$. Let $A'$ be an incidence matrix of $\mathcal{D}$. By viewing $\mathrm{AG}(m, q)$ as obtained from $\mathrm{PG}(m, q)$ by deleting a hyperplane, we prove the following theorem in [20].

**Theorem 11.10.** *The invariant factors of $A'$ are $p^\alpha$, $0 \leqslant \alpha \leqslant dt$, with multiplicity $h(\alpha, m, d+1) - h(\alpha, m-1, d+1)$, where $h(\alpha, \cdot, \cdot)$ is defined in Corollary* 11.8.

In closing this section, we mention the following open problem. Adopting the notation introduced at the beginning of this section, we let $A_{d,e}$ be a (0,1)-matrix with rows indexed by elements $Y$ of $\mathcal{L}_d$ and columns indexed by elements $Z$ of $\mathcal{L}_e$, and with the $(Y, Z)$ entry equal to 1 if and only if $Z \subset Y$. Note that $A_{d,1} = A$, an incidence matrix of the 2-design $(\mathcal{L}_1, \mathcal{L}_d)$. We are interested in finding the Smith normal form of $A_{d,e}$ when $e > 1$.

**Problem 11.11.** *Let $e > 1$. What is the p-rank of $A_{d,e}$? And what is the SNF of $A_{d,e}$?*

The first question in Problem 11.11 appeared in [40], and later in [8]. The $\ell$-rank of $A_{d,e}$, where $\ell$ is a prime different from $p$, is known from [38]. Furthermore, the Smith normal form of $A_{d,e}$ over the $\ell$-adic integers, $\ell$ is a prime different from $p$, is recently obtained in [18].

## 12. Miscellanea

In this final section, we collect two important recent results, which are closely related to the material in previous sections. We begin by describing the result of Blokhuis et al. [13] on projective planes with a large abelian collineation group.

The prime power conjecture for projective planes asserts that the order of a finite projective plane is a prime power. This conjecture is far from being proved. Most work on this conjecture was done under some extra assumptions on the collineation group of the projective plane. The following theorem of Blokhuis et al. [13] and Jungnickel and de Resmini [64] is one of the strongest results in recent years in this direction.

**Theorem 12.1** (*Blokhuis et al. [13], Jungnickel and de Resmini [64]*). (1). *Let $G$ be an abelian collineation group of order $n^2$ of a projective plane of order $n$. Then $n$ is a prime power, say $n = p^b$, $p$ a prime. If $p > 2$, then the p-rank of the abelian group $G$ is at least $b+1$.*

(2). *Let $G$ be an abelian collineation group of order $n(n-1)$ of a projective plane of order $n$. Then $n$ must be a power of a prime $p$ and the p-part of $G$ is elementary abelian.*

Concerning the proof of Part (1) of Theorem 12.1, we remark that if $\Pi$ is a projective plane of order $n$ with an abelian collineation group $G$ of order $n^2$, then results of André and Dembowski and Piper imply that either $\Pi$ is a translation plane or its dual (hence $n$ is a prime power), or $\Pi$ can be described by a certain relative difference set (and the plane is called type (b)). Using elementary and elegant group ring techniques, the authors of [13] proved that the order of a plane of type (b) is also a prime power. The proof of the second part is similar.

Next we mention some recent results of Kharaghani and Tayfeh-Rezaie [72] on Hadamard matrices. A well-known conjecture in combinatorics is that there exists a Hadamard matrix of order $4n$ for all positive integers $n$. This conjecture has been studied extensively. Prior to 2004, the smallest order for which no Hadamard matrix was known is 428. Then in June 2004, Kharaghani and Tayfeh-Rezaie announced the discovery of a Hadamard of order 428. Currently, the smallest order of Hadamard matrices not known to exist is 668. We remark that one of the ideas in the construction in [72] of a Hadamard matrix of order 428 goes back to a paper by Turyn [108]. (Note that Turyn's composition theorem [109] also played an important role in the construction of symmetric Bush-type Hadamard matrices. See Section 7.) In [72], Kharaghani and Tayfeh-Rezaie implemented a fast algorithm on a cluster of 16 PCs to search for Turyn-type sequences and found Turyn-type $(1, -1)$ sequences $X, Y, Z, W$ of lengths 36, 36, 36, 35. By a theorem of Turyn [108], these sequences give rise to a T-sequence of length 107, which in turn yields a Hadamard matrix of order 428. For the definition of Turyn type sequences and T-sequences, and other Hadamard matrices constructed by this method, we refer the reader to [72] for details.

## Acknowledgments

The author would like to thank David Chandler, Robert Coulter, Dieter Jungnickel, and Peter Sin for their helpful comments.

## References

[1] K.T. Arasu, private communication, July, 2001.

[2] K.T. Arasu, Y.Q. Chen, A. Pott, On abelian $(2^{2m+1}(2^{m-1}+1, 2^m(2^m+1), 2^m)$-difference sets, preprint.

[3] K.T. Arasu, H.D.L. Hollmann, K. Player, Q. Xiang, On the $p$-ranks of GMW difference sets, Codes and designs (Columbus, OH, 2000), 9-35, Ohio State University Mathematic Research Institute Publications, vol. 10, de Gruyter, Berlin, 2002.

[4] K.T. Arasu, K.J. Player, A new family of cyclic difference sets with Singer parameters in characteristic three, Des. Codes Cryptogr. 28 (2003) 75–91.

[5] K.T. Arasu, S.K. Sehgal, Some new difference sets, J. Combin. Theory Ser. A 69 (1995) 170–172.

[6] E.F. Assmus, Jr., Applications of algebraic coding theory to finite geometric problems, in: N.L. Johnson, M.J. Kallaher, C.T. Long (Eds.), Finite Geometries: Proceedings of a Conference in Honor of T.G. Ostrom, Lecture Notes in Pure and Applied Mathematics, vol. 82, 1983, 23–32.

[7] L. Babai, P. Frankl, Linear algebraic methods in combinatorics, preliminary version 2, 1992.

[8] B. Bagchi, S.P. Inamdar, Projective geometric codes, J. Combin. Theory Ser. A 99 (1) (2002) 128–142.

[9] M. Bardoe, P. Sin, The permutation modules for $\mathrm{GL}(n+1, \mathbb{F}_q)$ acting on $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{F}_q^{n+1}$, J. London Math. Soc. 61 (2000) 58–80.

[10] L.D. Baumert, D. Gordon, On the existence of cyclic difference sets with small parameters, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams,

Fields Institute Communication, vol. 41, American Mathematical Society, Providence, RI, 2004, pp. 61–68.

[11] P. Becker, Investigation of solvable $(120, 35, 10)$ difference sets, J. Combin. Designs 13 (2005) 79–107.

[12] T. Beth, D. Jungnickel, H. Lenz, Design Theory, vol. I, second ed., Encyclopedia of Mathematics and its Applications, vol. 78, Cambridge University Press, Cambridge, 1999.

[13] A. Blokhuis, D. Jungnickel, B. Schmidt, Proof of the prime power conjecture for projective planes of order $n$ with abelian collineation groups of order $n^2$, Proc. Amer. Math. Soc. 130 (2002) 1473–1476.

[14] A.E. Brouwer, J.H. Koolen, M. Klin, A root graph that is locally the line graph of the Petersen graph, The 2000 Com$^2$MaC Conference on Association Schemes, Codes and Designs (Pohang), Discrete Math. 264 (2003) 13–24.

[15] K.A. Bush, Unbalanced Hadamard matrices and finite projective planes of even order, J. Combin. Theory Ser. A 11 (1971) 38–44.

[16] P. Camion, H.B. Mann, Antisymmetric difference sets, J. Number Theory 4 (1972) 266–268.

[17] J.S. Chahal, N.M. Singhi, Tags on $k$-subsets and $t$-designs, J. Combin. Inform. System Sci. 26 (2001) 33–50.

[18] D.B. Chandler, The Smith normal forms of designs with classical parameters, Ph.D. Thesis, University of Delaware, 2004.

[19] D.B. Chandler, On the intersection sizes of Hermitian unitals with other unitals in $\mathrm{PG}(2, q^2)$ and of Hermitian varieties with certain other sets in $\mathrm{PG}(n, q^2)$, preprint.

[20] D.B. Chandler, P. Sin, Q. Xiang, The invariant factors of the incidence matrices of points and subspaces in $\mathrm{PG}(n, q)$ and $\mathrm{AG}(n, q)$, Trans. Amer. Math. Soc., to appear.

[21] D.B. Chandler, Q. Xiang, Cyclic relative difference sets and their $p$-ranks, Des. Codes Cryptogr. 30 (2003) 325–343.

[22] D.B. Chandler, Q. Xiang, The invariant factors of some cyclic difference sets, J. Combin. Theory Ser. A 101 (2003) 131–146.

[23] Y.Q. Chen, On the existence of abelian Hadamard difference sets and a new family of difference sets, Finite Fields Appl. 3 (1997) 234–256.

[24] Y.Q. Chen, Q. Xiang, S. Sehgal, An exponent bound on skew Hadamard abelian difference sets, Des. Codes Cryptogr. 4 (1994) 313–317.

[25] P.M. Cohn, Algebra, vol. 1, Wiley, Chichester, 1974.

[26] R.S. Coulter, R.W. Matthews, Planar functions and planes of Lenz–Barlotti class II, Des. Codes Cryptogr. 10 (1997) 167–184.

[27] R.S. Coulter, M. Henderson, Commutative presemifields and semifields, preprint.

[28] R.S. Coulter, M. Henderson, A new class of commutative presemifields of odd order, preprint.

[29] J.A. Davis, Difference sets in abelian 2-groups, J. Combin. Theory Ser. A 57 (1991) 262–286.

[30] J.A. Davis, J. Jedwab, A unifying construction for difference sets, J. Combin. Theory Ser. A 80 (1997) 13–78.

[31] P. Delsarte, On cyclic codes that are invariant under the general linear group, IEEE Trans. Inform. Theory IT-16 (1970) 760–769.

[32] P. Dembowski, T.G. Ostrom, Planes of order $n$ with collineation groups of order $n^2$, Math. Z 103 (1968) 239–258.

[33] J.F. Dillon, Multiplicative difference sets via additive characters, Des. Codes Cryptogr. 17 (1999) 225–235.

[34] J.F. Dillon, H. Dobbertin, New cyclic difference sets with Singer parameters, Finite Fields Appl. 10 (2004) 342–389.

[35] C. Ding, J. Yuan, A new class of skew Hadamard difference sets, J. Combin. Theory (A), to appear.

[36] R. Evans, H.D.L. Hollmann, C. Krattenthaler, Q. Xiang, Gauss sums, Jacobi sums, and $p$-ranks of cyclic difference sets, J. Combin. Theory Ser. A 87 (1999) 74–119.

[37] W. Foody, A. Hedayat, On theory and applications of BIB designs with repeated blocks, Ann. Statist. 5 (1977) 932–945.

[38] A. Frumkin, A. Yakir, Rank of inclusion matrices and modular representation theory, Israel J. Math. 71 (1990) 309–320.

[39] D.G. Glynn, J.W.P. Hirschfeld, On the classification of geometric codes by polynomial functions, Des. Codes Cryptogr. 6 (1995) 189–204.

[40] C.D. Godsil, Problems in algebraic combinatorics, Electron. J. Combin. 2 (1995) #F1.

[41] A. Golemac, T. Vučičić, New difference sets in nonabelian groups of order 100, J. Combin. Des. 9 (2001) 424–434.

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

[43] D.H. Gottlieb, A certain classes of incidence matrices, Proc. Amer. Math. Soc. 17 (1966) 1233–1237.

[44] R.L. Graham, S.-Y.R. Li, W.C.W. Li, On the structure of *t*-designs, SIAM J. Algebraic Discrete Methods 1 (1980) 8–14.

[45] J.E. Graver, W.B. Jurkat, The module structure of integral designs, J. Combin. Theory (A) 15 (1973) 75–90.

[46] W.H. Haemers, V.D. Tonchev, Spreads in strongly regular graphs, Des. Codes Cryptogr. 8 (1996) 145–157 (Special issue dedicated to Hanfried Lenz).

[47] M. Hall Jr., Cyclic projective planes, Duke Math. J. 14 (1947) 1079–1090.

[48] M. Hall Jr., A survey of difference sets, Proc. Amer. Math. Soc. 7 (1956) 975–986.

[49] N. Hamada, On the *p*-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error-correcting codes, Hiroshima Math. J. 3 (1973) 154–226.

[50] N. Hamada, H. Ohmori, On the BIB design having the minimum *p*-rank, J. Combin. Theory Ser. A 18 (1975) 131–140.

[51] T. Helleseth, P.V. Kumar, H.M. Martinsen, A new family of ternary sequences with ideal two-level autocorrelation, Designs, Codes Cryptogr. 23 (2001) 157–166.

[52] H.D.L. Hollmann, Q. Xiang, Maximal arcs in projective three-spaces and double-error-correcting cyclic codes, J. Combin. Theory Ser. A 93 (2001) 168–172.

[53] J.E. Iiam, On difference sets in groups of order $4p^2$, J. Combin. Theory Ser. A 72 (1995) 256–276.

[54] Y. Ionin, New symmetric designs from regular Hadamard matrices, Electronic J. Combin. 5 (1998) R1.

[55] Y. Ionin, H. Karaghani, A recursive construction for new symmetric designs, Des. Codes Cryptogr. 35 (2005) 303–310.

[56] Z. Janko, The existence of a Bush-type Hadamard matrix of order 36 and two new infinite classes of symmetric designs, J. Combin. Theory, Ser. A 95 (2001) 360–364.

[57] Z. Janko, H. Kharaghani, V.D. Tonchev, A Bush-type Hadamard matrix of order 100 and two new infinite classes of symmetric designs, J. Combin. Des. 9 (2001) 72–78.

[58] Z. Janko, H. Kharaghani, V.D. Tonchev, The existence of a Bush-type Hadamard matrix of order 324 and two new infinite classes of symmetric designs, Des. Codes Cryptogr. 24 (2001) 225–232.

[59] Z. Jia, New necessary conditions for the existence of difference sets without self-conjugacy, J. Combin. Theory Ser. A 98 (2002) 312–327.

[60] E.C. Johnsen, Skew-Hadamard Abelian group difference sets, J. Algebra 4 (1966) 388–402.

[61] L.K. Jørgensen, M. Klin, Switching of edges in strongly regular graphs. I. A family of partial difference sets on 100 vertices, Electron. J. Combin. 10 (2003), Research Paper 17, 31pp. (electronic).

[62] D. Jungnickel, On $\lambda$-ovals and difference sets, Contemporary Methods in Graph Theory, Bibliographisches Institute, Mannheim, 1990, pp. 429–448.

[63] D. Jungnickel, Difference sets, Contemporary Design Theory, Wiley, Discrete Mathematics and Optimation, Wiley, New York, 1992, pp. 241–324.

[64] D. Jungnickel, M.J. de Resmini, Another case of the prime power conjecture for finite projective planes, Adv. Geom. 2 (2002) 215–218.

[65] D. Jungnickel, H. Kharaghani, Balanced generalized weighing matrices and their applications, Le Mat., to appear.

[66] D. Jungnickel, B. Schmidt, Difference sets: an update, Geometry, combinatorial Designs and Related Structures (Spetses, 1996), London Mathematical Society, Lecture Note Series, vol. 245, Cambridge University Press, Cambridge, 1997, pp. 89–112.

[67] D. Jungnickel, B. Schmidt, Difference sets: a second update, Combinatorics ’98 (Mondello), Rend. Circ. Mat. Palermo 53 (2) (1998) 89–118.

[68] W.M. Kantor, Note on GMW designs, European J. Combin. 22 (2001) 63–69.

[69] H. Kharaghani, New classes of weighing matrices, Ars Combinatoria 19 (1985) 69–72.

[70] H. Kharaghani, On the twin designs with the Ionin-type parameters, Electron. J. Combin. 7 (2000) R1.

[71] H. Kharaghani, On the Siamese twin designs, in: D. Jungnickel, H. Niederreiter (Eds.), Finite Fields and Applications, Springer, Berlin, 2001, pp. 303–312.

[72] H. Kharaghani, B. Tayfeh-Rezaie, A Hadamard matrix of order 428, J. Combin. Designs, to appear.

[73] G.B. Khosrovshahi, Ch. Maysoori, On the structure of higher incidence matrices, Bull. Inst. Combin. Appl. 25 (1999) 13–22.

[74] R.E. Kibler, A summary of noncyclic difference sets, $k < 20$, J. Combin. Theory Ser. A 25 (1978) 62–67.

[75] R.G. Kraemer, Proof of a conjecture on Hadamard 2-groups, J. Combin. Theory Ser. A 63 (1993) 1–10.

[76] E.S. Lander, Symmetric Designs: An Algebraic Approach, London Math. Society Lecture Note Series, vol. 74, Cambridge University Press, Cambridge, 1983.

[77] M.H. Le, Q. Xiang, A result on Ma’s conjecture, J. Combin. Theory Ser. A 73 (1996) 181–184.

[78] K.H. Leung, S.L. Ma, B. Schmidt, Nonexistence of abelian difference sets: Lander’s conjecture for prime power orders, Trans. Amer. Math. Soc. 356 (2004) 4343–4358.

[79] K.H. Leung, S.L. Ma, Y.L. Wong, Difference sets in dihedral groups, Des. Codes Cryptogr. 1 (1991) 333–338.

[80] K.H. Leung, B. Schmidt, Asymptotic nonexistence of difference sets in dihedral groups, J. Combin. Theory Ser. A 99 (2002) 261–280.

[81] K.H. Leung, B. Schmidt, The field descent method, Des. Codes Cryptogr. 36 (2005) 171–188.

[82] R. Lidl, H. Niederreiter, Finite Fields, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[83] R.A. Liebler, Constructive representation theoretic methods and non-abelian difference sets, Difference sets, sequences and their correlation properties (Bad Windsheim, 1998), NATO Advanced Science Institute Series C of Mathematical, Physical and Science, vol. 542, Kluwer Academic Publishers, Dordrecht, 1999.

[84] H.A. Lin, From cyclic Hadamard difference sets to perfectly balanced sequences, Ph.D. Thesis, University of Southern California, 1998.

[85] J. van Lint, R.M. Wilson, A Course in Combinatorics, second ed., Cambridge University Press, Cambridge, 2001.

[86] F. Luca, P. Stănică, On a conjecture of Ma, Result. Math., to appear.

[87] S.L. Ma, McFarland’s conjecture on abelian difference sets with multiplier $-1$, Des. Codes Cryptogr. 1 (1991) 321–332.

[88] S.L. Ma, A family of difference sets having $-1$ as an invariant, European J. Combin. 10 (1989) 273–274.

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

[90] A. Maschietti, Difference sets and hyperoval, Des. Codes Cryptogr. 14 (1998) 89–98.

[91] R.L. McFarland, A family of difference sets in non-cyclic groups, J. Combin. Theory Ser. A 15 (1973) 1–10.

[92] R.L. McFarland, Difference sets in abelian groups of order $4p^2$, Mitt. Math. Sem. Giessen No. 192 (i–iv) (1989) 1–70.

[93] R.L. McFarland, B.F. Rice, Translates and multipliers of abelian difference sets, Proc. Amer. Math. Soc. 68 (3) (1978) 375–379.

[94] M. Muzychuk, Difference sets with $n = 2p^m$, J. Algebraic Combin. 7 (1998) 77–89.

[95] M. Muzychuk, Q. Xiang, Symmetric Bush-type Hadamard matrices of order $4m^4$ exist for all odd *m*, Proc. Amer. Math. Soc., to appear.

[96] J.-S. No, New cyclic difference sets with Singer parameters constructed from *d*-homogeneous functions, Des. Codes Cryptogr. 33 (2004) 199–213.

[97] J.-S. No, H. Chung, M.-S. Yun, 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) 1278–1282.

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

[99] J.-S. No, D.-J. Shin, T. Helleseth, On the *p*-ranks and characteristic polynomials of cyclic difference sets, Des. Codes Cryptogr. 33 (2004) 23–37.

[100] A. Pott, Finite Geometry and Character Theory, Lecture Notes in Mathematics, vol. 1601, Springer, Berlin, 1995.

[101] W.S. Qiu, Complete settling of the multiplier conjecture for the case of $n = 3p^r$, Sci. China Ser. A 45 (2002) 1117–1134.

[102] H.J. Ryser, Combinatorial Mathematics, Wiley, New York, 1963.

[103] H.E. Sachar, Error-correcting codes associated with finite projective planes, Ph.D. Thesis, Lehigh University, 1973.

[104] P. Sin, The elementary divisors of the incidence matrices of points and linear subspaces in $P^n(\mathbb{F}_p)$, J. Algebra 232 (2000) 76–85.

[105] N.M. Singhi, Tags on subsets, Disc. Math., to appear.

[106] K.W. Smith, Non-abelian Hadamard difference sets, J. Combin. Theory Ser. A 70 (1995) 144–156.

[107] R.J. Turyn, Character sums and difference sets, Pacific J. Math. 15 (1965) 319–346.

[108] R.J. Tury, Hadamard matrices, Baumert–Hall units, four-symbol sequences, pulse compression, and surface wave encodings, J. Combin. Theory Ser. A 16 (1974) 313–333.

[109] R.J. Turyn, A special class of Williamson matrices and difference sets, J. Combin. Theory Ser. A 36 (1984) 111–115.

[110] T. Vučičić, New symmetric designs and nonabelian difference sets with parameters $(100, 45, 20)$, J. Combin. Des. 8 (2000) 291–299.

[111] D. Wan, A Chevalley–Warning approach to *p*-adic estimates of character sums, Proc. Amer. Math. Soc. 123 (1) (1995) 45–54.

[112] R.M. Wilson, The necessary conditions for *t*-designs are sufficient for something, Util. Math. 4 (1973) 207–217.

[113] R.M. Wilson, A diagonal form for the incidence matrices of *t*-subsets vs. *k*-subsets, European J. Combin. 11 (1990) 609–615.

[114] R.M. Wilson, Signed hypergraph designs and diagonal forms for some incidence matrices, Des. Codes Cryptogr. 17 (1999) 289–297.

[115] R.M. Wilson, Some applications of incidence matrices of *t*-subsets and hypergraphs, preprint.

[116] R.M. Wilson, Q. Xiang, Constructions of Hadamard difference sets, J. Combin. Theory Ser. A 77 (1997) 148–160.

[117] Q. Xiang, On balanced binary sequences with two-level autocorrelation functions, IEEE Trans. Inform. Theory 44 (1) (1998) 3153–3156.

[118] Q. Xiang, Recent results on difference sets with classical parameters, in: A. Pott et al. (Eds.), Proceedings of the NATO ASI Difference sets, sequences and their correlation properties, Avon Books, New York, 1999, pp. 419–437.