Des. Codes Cryptogr. (2017) 82:511–529
DOI 10.1007/s10623-016-0179-6

# A generalization of combinatorial designs and related codes

**Jerod Michel**[1] · **Baokun Ding**[1]

Received: 17 May 2015 / Revised: 7 January 2016 / Accepted: 7 January 2016 /
Published online: 19 January 2016

**Abstract** In this paper we study a certain generalization of combinatorial designs related to almost difference sets, namely the $t$-adesign, which was coined by Ding (Codes from difference sets, 2015). It is clear that 2-adesigns are partially balanced incomplete block designs which naturally arise in many combinatorial and statistical problems. We discuss some of their basic properties and give several constructions of 2-adesigns (some of which correspond to new almost difference sets and some to new almost difference families), as well as two constructions of 3-adesigns. We discuss basic properties of the incidence matrices and make an initial investigation into the codes which they generate. We find that many of the codes have good parameters in the sense they are optimal or have relatively high minimum distance.

**Keywords** Almost difference set · $t$-Design · Cyclotomic class · Linear code · $t$-Adesign

**Mathematics Subject Classification** 05B05 · 05B10 · 11T22 · 51E30 · 05B30 · 94C30

## 1 Introduction

Combinatorial designs have extensive applications in many fields, including finite geometry [6,17], design of experiments [3,14], cryptography [5,22], and authentication codes and secret sharing schemes [20,22]. We will assume some familiarity with combinatorial design theory. A $t$-$(v, k, \lambda)$ *design* (with $v > k > t > 0$) is an incidence structure $(V, \mathcal{B})$ where $V$ is a set of $v$ points and $\mathcal{B}$ is a collection of $k$-subsets of $V$ (called blocks), such that any $t$-subset of $V$ is contained in exactly $\lambda$ blocks [22]. When $t = 2$, a $t$-design is sometimes referred to as a balanced incomplete block design. Denoting the number of blocks by $b$ and the number of blocks containing a given point by $r$, the identities

Communicated by A. Pott.

✉ Jerod Michel
contextolibre@gmail.com

[1] School of Mathematics, Zhejiang University, Hangzhou 310027, China

$$bk = vr$$

and

$$r(k-1) = (v-1)\lambda$$

restrict the possible parameter sets. A $t$-$(v, k, \lambda)$ design in which $b = v$ and $r = k$ is called *symmetric*, and any two blocks meet in $\lambda$ points. A $t$-$(v, k, \lambda)$ design is called *quasi-symmetric* if there are exactly two intersection numbers among pairs of blocks. The *dual* $(V, \mathcal{B})^{\perp}$ of an incidence structure $(V, \mathcal{B})$ is the incidence structure $(\mathcal{B}, V)$ with the roles of points and blocks interchanged. A symmetric incidence structure is always isomorphic to its dual.

Difference sets [16] and almost difference sets [19] also have applications in many areas such as digital communications [12,26], sequence design [23,25], and CDMA and cryptography [5]. We will also assume familiarity with difference sets and almost difference sets. Let $G$ be a finite additive group with identity 0. Let $k$ and $\lambda$ be positive integers such that $2 \le k < v$. A $(v, k, \lambda)$ *difference set* in $G$ is a subset $D \subseteq G$ that satisfies the following properties:

1. $|D| = k$,
2. the multiset $\{x - y \mid x, y \in D, x \neq y\}$ contains every member of $G - \{0\}$ exactly $\lambda$ times.

Almost difference sets are a generalization of difference sets. A $(v, k, \lambda, t)$ *almost difference set* in $G$ is a subset $D \subseteq G$ that satisfies the following properties:

1. $|D| = k$,
2. the multiset $\{x - y \mid x, y \in D, x \neq y\}$ contains $t$ members of $G - \{0\}$ which appear $\lambda$ times and $v - 1 - t$ members of $G - \{0\}$ which appear $\lambda + 1$ times.

Our motivation for studying t-adesigns is in constructing linear codes. Also, due to their having extensive applications, it is worthwhile to study the combinatorial objects arising from almost difference sets. In Sect. 2 we introduce the generalizations and discuss some basic properties. In Sect. 3 we give three constructions of 2-adesigns from quadratic residues, several constructions of 2-adesigns which are almost difference families are given in Sect. 4, and some constructions of 2-adesigns from symmetric $t$-designs are given in Sect. 5. In Sect. 6 we discuss 3-adesigns and two constructions are given, and in Sect. 7 we discuss the codes of $t$-adesigns (and some related structures), and include some of the codes with good parameters in a table. Section 8 concludes the paper.

## 2 Preliminaries

Let $G$ be an additive group of order $v$. A $k$-element subset $D \subseteq G$ has *difference levels* $\mu_1 < \cdots < \mu_s$ if there exist integers $t_1, \ldots, t_s$ such that the multiset

$$M = \{g - h \mid g, h \in D\}$$

contains exactly $t_i$ members of $G - \{0\}$ each with multiplicity $\mu_i$ for all $i$, $1 \le i \le s$. We will denote the $t_i$ members of the multiset $M$ with multiplicity $\mu_i$ by $T_i$. Note that the $T_i$'s form a partition of $G - \{0\}$. It is easy to see that in the case where $s = 1$, $D$ is a difference set [16], and in the case where $s = 2$ and $\mu_2 = \mu_1 + 1$, $D$ is an almost difference set [19]. In this correspondence we are concerned only with those structures having two difference levels, and all groups are assumed to be additive. The basic equation describing a $k$-element subset $D \subseteq G$ with difference levels $\mu_1 < \mu_2$ is given by

$$\mu_1 t + \mu_2(v - 1 - t) = k(k-1). \tag{1}$$

Let $V$ be a $v$-set and $\mathcal{B}$ a collection of subsets of $V$, called blocks, each having cardinality $k$. If there are positive integers $\mu_1 < \mu_2$ such that every subset of $V$ of cardinality $t$ is incident with exactly $\mu_i$ blocks for $i = 1$ or 2, and for each $i$, $i = 1, 2$, there exists a subset of $V$ of cardinality $t$ that is incident with exactly $\mu_i$ blocks, then we say that the incidence structure $(V, \mathcal{B})$ has *$t$-levels* $\mu_1 < \mu_2$. We denote $|\mathcal{B}|$ by $b$. An incidence structure $(V, \mathcal{B})$ is called *symmetric* if $b = v$. In the case where $s = 2$, $(V, \mathcal{B})$ is a partially balanced incomplete block design, and if $\mu_2 = \mu_1 + 1$, we call $(V, \mathcal{B})$ a $t$-$(v, k, \mu_1)$ *adesign* (or simply a *$t$-adesign*), which was coined by Ding in [10]. It is easy to see that in the case where $s = 1$, $(V, \mathcal{B})$ is simply a $t$-design [22].

We call the set $\{D + g \mid g \in G\}$ of translates of $D$, denoted by $Dev(D)$, the *development* of $D$. We have the following lemmas whose proofs are omitted as they are simple counting exercises.

**Lemma 2.1** *Let $D$ be a $(v, k, \lambda)$ almost difference set in an Abelian group $G$. Then $(G, Dev(D))$ is a 2-$(v, k, \lambda)$ adesign.*

Let $(V, \mathcal{B})$ be an incidence structure with $t$-levels $\mu_1 < \mu_2$. Let $A$ be a $v$ by $b$ matrix whose rows and columns are indexed by points and blocks respectively and whose $(i, j)$-th entry is 1 if the point corresponding to the $i$th row is incident with the block corresponding to the $j$th row, and 0 otherwise. We call $A$ the *incidence matrix* of $(V, \mathcal{B})$. We will denote the $n \times n$ identity and all-one matrices by $I_n$ and $J_n$ respectively, or, when it is clear from the context, simply by $I$ and $J$.

**Lemma 2.2** *Let $D$ be a $k$-subset of an Abelian group $G$ of cardinality $v$ with the two difference levels $\mu_1 < \mu_2$. Let $A$ be the $v \times v$ incidence matrix of the symmetric incidence structure $(G, Dev(D))$. Then*

$$A^T A = AA^T = kI + \mu_1 A_1 + \mu_2(J - A - I). \tag{2}$$

Next, we give some constructions of 2-adesigns from almost difference sets.

## 3 Constructions of 2-adesigns from quadratic residues

Cyclotomic classes have proven to be a powerful tool for constructing difference sets and almost difference sets, e.g. see [12,13,19]. Let $q$ be a prime power, $\mathbb{F}_q$ a finite field, and $e$ a divisor of $q-1$. For a primitive element $\alpha$ of $\mathbb{F}_q$ let $D_0^e$ denote $\langle \alpha^e \rangle$, the multiplicative group generated by $\alpha^e$, and let

$$D_i^e = \alpha^i D_0^e, \text{ for } i = 1, 2, \ldots, e-1.$$

We call $D_i^e$ the *cyclotomic classes* of order $e$. The *cyclotomic numbers* of order $e$ are defined to be

$$(i, j)_e = \left| D_i^e \cap (D_j^e + 1) \right|.$$

It is easy to see there are at most $e^2$ different cyclotomic numbers of order $e$. When it is clear from the context, we simply denote $(i, j)_e$ by $(i, j)$. The cyclotomic numbers $(h, k)$ of order $e$ have the following properties [7]:

$$(h,k) = (e-h, k-h), \tag{3}$$

$$(h,k) = \begin{cases} (k,h), & \text{if } f \text{ even,} \\ (k+\frac{e}{2}, h+\frac{e}{2}), & \text{if } f \text{ odd.} \end{cases} \tag{4}$$

Our first three constructions make use of quadratic residues. We will need the following lemma [7].

**Lemma 3.1** *If $q \equiv 1$ (mod 4) then the cyclotomic numbers of order two are given by*

$$\begin{aligned} (0,0) &= \frac{q-5}{4}, \\ (0,1) = (1,0) = (1,1) &= \frac{q-1}{4}. \end{aligned}$$

*If $q \equiv 3$ (mod 4) then the cyclotomic numbers of order two are given by*

$$\begin{aligned} (0,1) &= \frac{q+1}{4}, \\ (0,0) = (1,0) = (1,1) &= \frac{q-3}{4}. \end{aligned}$$

We are ready to give our first construction.

**Theorem 3.2** *Let $q$ be an odd prime power and $\alpha$ a primitive member of $\mathbb{F}_q$. Define $C_i = \{z \in \mathbb{Z}_{q-1} \mid \alpha^z \in D_i^2 - 1\}$ for $i = 0, 1$. Then the incidence structure $(\mathbb{Z}_{q-1} \cup \{\infty\}, Dev^{\infty}(C_0) \cup Dev(C_1))$, where $Dev^{\infty}(C_0)$ denotes the blocks of $Dev(C_0)$ each modified by adjoining the point "$\infty$", is a 2-$(q, \frac{q-1}{2}, \frac{q-5}{2})$ adesign.*

*Proof* We will denote $\{\alpha^z \mid z \in C_i\}$ by $\alpha^{C_i}$. For $w \in \mathbb{Z}_{q-1}$ we have

$$|C_0 \cap (C_0 + w)| = \left|\alpha^{C_0} \cap \alpha^{C_0 + w}\right|$$

which, since $\alpha^z$ is nonzero and

$$|((D_0^2 - 1) - \{0\}) \cap ((D_0^2 - \alpha^w) - \{0\})| = |((D_0^2 - \{1\}) - 1) \cap ((\alpha^w D_0^2 - \{\alpha^w\}) - \alpha^w)|,$$

is

$$\begin{cases} \left|(D_0^2 - \{1\}) \cap (D_0^2 - \{\alpha^w\} + (1-\alpha^w))\right| & \text{if } w \text{ even,} \\ \left|(D_0^2 - \{1\}) \cap (D_1^2 - \{\alpha^w\} + (1-\alpha^w))\right| & \text{if } w \text{ odd.} \end{cases}$$

Since $\alpha^w(1-\alpha^w)^{-1} = (1-\alpha^w)^{-1} - 1$, this becomes

$$\begin{cases} \left|(D_0^2 - \{(1-\alpha^w)^{-1}\}) \cap (D_0^2 - \{(1-\alpha^w)^{-1} - 1\} + 1)\right| & \text{if } w \text{ even,} \\ \left|(D_0^2 - \{(1-\alpha^w)^{-1}\}) \cap (D_1^2 - \{(1-\alpha^w)^{-1} - 1\} + 1)\right| & \text{if } w \text{ odd,} \end{cases}$$

which simplifies to

$$\begin{cases} \left|D_0^2 \cap (D_0^2 + 1) - \{(1-\alpha^w)^{-1}\}\right| & \text{if } w \text{ even,} \\ \left|D_0^2 \cap (D_1^2 + 1) - \{(1-\alpha^w)^{-1}\}\right| & \text{if } w \text{ odd.} \end{cases}$$

There are four cases depending on the parity of $w$ and whether $(1-\alpha^w)^{-1} \in D_0^2$ or $D_1^2$. By Theorem 3.1 we have

$$|C_0 \cap (C_0+w)| = \begin{cases} (0,0)-1 & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_0^2, \\ (0,0) & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_1^2, \\ (0,1)-1 & \text{if } w \text{ odd and } (1-\alpha^w)^{-1} \in D_0^2, \\ (1,0)-1 & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_0^2. \end{cases}$$

Thus if $q \equiv 1 (\mathrm{mod}\ 4)$ then

$$|C_0 \cap (C_0+w)| = \begin{cases} \frac{q-9}{4} & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_0^2, \\ \frac{q-5}{4} & \text{otherwise,} \end{cases}$$

and if $q \equiv 3 (\mathrm{mod}\ 4)$ then

$$|C_0 \cap (C_0+w)| = \begin{cases} \frac{q-3}{4} & \text{if } w \text{ odd and } (1-\alpha^w)^{-1} \in D_0^2 \text{ or if } w \text{ even and } (1-\alpha^w)^{-1} \in D_1^2, \\ \frac{q-7}{4} & \text{otherwise.} \end{cases}$$

Also, we have

$$|C_1 \cap (C_1+w)| = \begin{cases} \left|D_1^2 \cap (D_1^2+1)+(1-\alpha^w)\right| & \text{if } w \text{ even,} \\ \left|D_1^2 \cap (D_1^2+1)+(1-\alpha^w)\right| & \text{if } w \text{ odd.} \end{cases}$$

Thus if $q \equiv 1 (\mathrm{mod}\ 4)$ then

$$|C_1 \cap (C_1+w)| = \begin{cases} \frac{q-5}{4} & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_1^2, \\ \frac{q-1}{4} & \text{otherwise.} \end{cases}$$

and if $q \equiv 3 (\mathrm{mod}\ 4)$ then

$$|C_1 \cap (C_1+w)| = \begin{cases} \frac{q+1}{4} & \text{if } w \text{ odd and } (1-\alpha^w)^{-1} \in D_1^2, \\ \frac{q-3}{4} & \text{otherwise.} \end{cases}$$

We need to compute the number of blocks of $(\mathbb{Z}_{q-1}, Dev(C_0) \cup Dev(C_1))$ in which an arbitrary pair of points appear. Consider the incidence structures $(\mathbb{Z}_{q-1}, Dev(C_i))$ for $i = 0, 1$. Let $C_i^\perp, (C_i+w)^\perp$ denote the points of the dual structures $(Dev(C_i), \mathbb{Z}_{q-1})$ corresponding to the blocks $C_i, C_i+w$. We have that $(\mathbb{Z}_{q-1}, Dev(C_i))$ is a self-dual incidence structure and by Lemma 2.2 the number of blocks of $(\mathbb{Z}_{q-1}, Dev(C_0) \cup Dev(C_1))$ in which the points $C_i^\perp, (C_i+w)^\perp$ appear is, if $q \equiv 1 (\mathrm{mod}\ 4)$,

$$\begin{cases} \frac{q-9}{4} + \frac{q-1}{4} = \frac{2q-10}{4} & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_0^2, \\ \frac{q-5}{4} + \frac{q-5}{4} = \frac{2q-10}{4} & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_1^2, \\ \frac{q-5}{4} + \frac{q-1}{4} = \frac{2q-6}{4} & \text{otherwise,} \end{cases}$$

and if $q \equiv 3 (\mathrm{mod}\ 4)$,

$$\begin{cases} \frac{q-3}{4} + \frac{q-3}{4} = \frac{2q-6}{4} & \text{if } w \text{ odd and } (1-\alpha^w)^{-1} \in D_0^2, \\ \frac{q-7}{4} + \frac{q+1}{4} = \frac{2q-6}{4} & \text{if } w \text{ even and } (1-\alpha^w)^{-1} \in D_1^2, \\ \frac{q-7}{4} + \frac{q-3}{4} = \frac{2q-10}{4} & \text{otherwise.} \end{cases}$$

It is easy to see that the block sizes of the incidence structures $(\mathbb{Z}_{q-1}, Dev(C_0))$ and $(\mathbb{Z}_{q-1}, Dev(C_1))$ are $\frac{q-3}{2}$ and $\frac{q-1}{2}$ respectively and that the number of blocks containing a given point in $(\mathbb{Z}_{q-1}, Dev(C_0))$ is $\frac{2q-6}{4}$. Then the incidence structure $(\mathbb{Z}_{q-1} \cup \{\infty\}, Dev^{\infty}(C_0) \cup Dev(C_1))$, where $Dev^{\infty}(C_0)$ denotes the blocks of $Dev(C_0)$ each modified by adjoining the point $\infty$, is a 2-adesign. □

Note that appending the symbol "$\infty$" to certain blocks in a combinatorial design has been done before, e.g. see [18, Chapter 8 ]. Our constructions in this section also use this symbol only, rather than extending complimentary blocks to obtain a 3-design, we first consider various other ways of obtaining a set of blocks where any two have lengths differing by at most one, and then extend the shorter blocks to obtain a 2-adesign.

*Example 3.3* With $q = 11$ and $C_i$ defined as in Theorem 3.2 we get that $(\mathbb{Z}_{10} \cup \{\infty\}, Dev^{\infty}(C_0) \cup Dev(C_1))$ is a 2-(10, 5, 3) adesign with blocks:

$$\begin{array}{ccccc}
\{0,1,3,4,8\} & \{1,3,4,6,7\} & \{2,4,5,7,8\} & \{0,2,3,7,9\} & \{3,5,6,8,9\} \\
\{0,1,5,7,8\} & \{1,2,4,5,9\} & \{0,2,3,5,6\} & \{0,4,6,7,9\} & \{1,2,6,8,9\} \\
\{2,5,6,7,\infty\} & \{0,1,6,9,\infty\} & \{3,6,7,8,\infty\} & \{1,4,5,6,\infty\} & \{0,1,2,7,\infty\} \\
\{1,2,3,8,\infty\} & \{2,3,4,9,\infty\} & \{4,7,8,9,\infty\} & \{0,5,8,9,\infty\} & \{0,3,4,5,\infty\}
\end{array}$$

The next two constructions will use the following lemmas.

**Lemma 3.4** [1] *Let $p$ be a prime. The number of pairs of consecutive quadratic residues mod $p$ is*

$$N(p) = \frac{1}{4}\left(p - 4 - (-1)^{\frac{p-1}{2}}\right)$$

*and the number of pairs of consecutive quadratic non-residues mod $p$ is*

$$N'(p) = \frac{1}{4}\left(p - 2 + (-1)^{\frac{p-1}{2}}\right).$$

In the sequel we will sometimes use the following lemma without making reference to it.

**Lemma 3.5** [2] *Let $p \equiv 1 (mod\, 4)$ be a prime. The the set of quadratic residues mod $p$ forms a $\left(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{2}\right)$ almost difference set in $\mathbb{Z}_p$.*

**Lemma 3.6** *Let $p \equiv 1 (mod\, 4)$ be a prime and $D \subseteq \mathbb{Z}_p$ be the set of quadratic residues. Two distinct points $x, y \in D$ occur together in exactly $\frac{p-5}{4}$ translates of $D$ if and only if $x - y$ is a quadratic residue. Dually, $D + x$ and $D + y$ are translates of $D$ with $x - y \in D$ if and only if $|(D + x) \cap (D + y)| = \frac{p-5}{4}$.*

*Proof* Let $x, y \in D$ be distinct. Denote $\frac{p-5}{4}$ by $\lambda$. Without loss of generality we can take $y = 1$. Let

$$D, D + \alpha_1, \ldots, D + \alpha_{\lambda-1}$$

be precisely the $\lambda$ translates of $D$ in which $x$ and 1 appear together. Then

$$x = x_1 + \alpha_1 = \cdots = x_{\lambda-1} + \alpha_{\lambda-1}$$

for some distinct quadratic residues $x_1, \ldots, x_{\lambda-1}$ and

$$1 = y_1 + \alpha_1 = \cdots = y_{\lambda-1} + \alpha_{\lambda-1}$$

for some distinct quadratic residues $y_1, \ldots, y_{\lambda-1}$. Now suppose that $x-1$ is a quadratic non-residue. Then

$$x-1 = x_1 - y_1 = \cdots = x_{\lambda-1} - y_{\lambda-1}.$$

Since $p \equiv 1 (\mathrm{mod}\ 4)$ we have $(x-1)^{-1}$ is also a quadratic nonresidue. Then we have

$$1 = (x-1)^{-1}x - (x-1)^{-1} = (x-1)^{-1}x_i - (x-1)^{-1}y_i$$

for $i = 1, \ldots, \lambda-1$. This gives precisely $\lambda$ pairs of consecutive non-residues, these being the *only* pairs of consecutive quadratic non-residues. But this contradicts Lemma 3.4, from which we have that the number of pairs of consecutive quadratic non-residues is $\lambda+1$. The condition is necessary and sufficient, and the dual argument follows from the fact that the 2-adesign $(\mathbb{Z}_p, Dev(D))$ is symmetric. □

We are now ready to construct two more families of 2-adesigns.

**Theorem 3.7** *Let $p \equiv 1(mod\ 4)$ be a prime greater than 5, and let $D \subseteq \mathbb{Z}_p$ be the set of quadratic residues. Let $\mathcal{B} = \{b \cap D \mid b \in Dev(D), b \neq D\}$, and let $\mathcal{B}_\infty$ be the set containing all members of $\mathcal{B}$ of size $\frac{p-1}{4}$, as well as all members of $\mathcal{B}$ of size $\frac{p-5}{4}$ modified by adjoining the point $\infty$. Then $(D \cup \{\infty\}, \mathcal{B}_\infty)$ is a 2-$(\frac{p+1}{2}, \frac{p-1}{4}, \frac{p-9}{4})$ adesign.*

*Proof* Let $x, y \in D$ be distinct. Denote $\frac{p-5}{4}$ by $\lambda$ and $\frac{p-1}{2}$ by $k$. If $x$ and $y$ appear together in exactly $\lambda$ translates of $D$, then $x$ and $y$ appear together in exactly $\lambda$ blocks in $\mathcal{B}_\infty$. Similarly, if $x$ and $y$ appear together in $\lambda+1$ translates of $D$ then $x$ and $y$ appear together in $\lambda+1$ blocks in $\mathcal{B}_\infty$. We want to show that $x$ and $\infty$ appear together in exactly $\lambda$ blocks in $\mathcal{B}_\infty$. Without loss of generality, we can take $x = 1$. There are $k-1$ blocks in $\mathcal{B}_\infty$ containing 1. Let

$$D, D+\alpha_1, \ldots, D+\alpha_w$$

be precisely the translates of $D$ containing 1. By Lemma 3.6, if $|D \cap (D+\alpha_i)| = \lambda$, then $\alpha_i$ is a quadratic residue. If $y + \alpha_i = 1$ then we have a pair $y, -\alpha_i$ of consecutive quadratic residues. By Lemma 3.4, the number of pairs of consecutive quadratic residues is exactly $\lambda$.

To see that there are pairs $x, y \in D$ of distinct points appearing in $\lambda-1$ blocks as well as those appearing in $\lambda$ blocks, suppose that $y_1, \ldots, y_{k-1}$ be the $k-1$ points in $D - \{1\}$. We can again, without loss of generality, take $x = 1$. Suppose that 1 and $y_i$ appear together in exactly $\lambda$ translates of $D$ for each $i$, $1 \leq i \leq k-1$. Then $y_i - 1 \in D$ for all $y_i$. By Lemma 3.4 this gives too many pairs of quadratic residues, which completes the proof. □

*Example 3.8* With $p = 13$ we apply Theorem 3.7 and get that $(D \cup \{\infty\}, \mathcal{B}_\infty)$ is a 2-(7, 3, 1) adesign and $\mathcal{B}_\infty$ contains the following blocks:

$$\begin{array}{cccc}
\{4, 10, \infty\} & \{3, 4, 10\} & \{1, 3, 12\} & \{4, 9, 12\} \\
\{4, 12, \infty\} & \{10, 12, \infty\} & \{1, 3, \infty\} & \{4, 9, \infty\} \\
\{1, 4, 9\} & \{1, 10, 12\} & \{3, 9, 10\} & \{3, 9, \infty\}
\end{array}$$

Let $\mathcal{B}$ and $\mathcal{B}_\infty$ be defined as in Theorem 3.7. The second construction is the following.

**Theorem 3.9** *Let $p \equiv 1(mod\ 4)$ be a prime greater than 5, and let $D \subseteq \mathbb{Z}_p$ be the set of quadratic residues. Let $\bar{\mathcal{B}}_\infty$ be the set of complements of members of $\mathcal{B}_\infty$ in $\mathbb{Z}_p \cup \{\infty\}$. Then $(D \cup \{\infty\}, \bar{\mathcal{B}}_\infty)$ is a 2-$\left(\frac{p+1}{2}, \frac{p+3}{4}, \frac{p-1}{4}\right)$ adesign.*

*Proof* Let $x, y \in D \cup \{\infty\}$ be distinct. Denote $\frac{p-5}{4}$ by $\lambda$ and $\frac{p-1}{2}$ by $k$. Suppose $x$ and $y$ appear together in $\lambda$ blocks in $\mathcal{B}_\infty$. Then there are $\lambda$ blocks in $\bar{\mathcal{B}}_\infty$ not containing $x$ or $y$. Also there are $k-1$ blocks in $\bar{\mathcal{B}}_\infty$ not containing $x$ and $k-1$ blocks not containing $y$. Then the number of blocks in $\bar{\mathcal{B}}_\infty$ containing $x$ and $y$ is

$$|\bar{\mathcal{B}}_\infty| - (|\{b \in \bar{\mathcal{B}}_\infty \mid x \notin b\}| + |\{b \in \bar{\mathcal{B}}_\infty \mid y \notin b\}|) + |\{b \in \bar{\mathcal{B}}_\infty \mid x, y \notin b\}|$$

which is easily seen to be $\lambda + 1$. A similar calculation shows that if $x$ and $y$ appear together in $\lambda - 1$ blocks in $\mathcal{B}_\infty$ then $x$ and $y$ appear together in $\lambda$ blocks $\bar{\mathcal{B}}_\infty$. □

*Example 3.10* With $p = 13$ we apply Theorem 3.9 and get that $(D \cup \{\infty\}, \bar{\mathcal{B}}_\infty)$ is a 2-(7, 4, 3) adesign and $\bar{\mathcal{B}}_\infty$ contains the following blocks:

$$\begin{array}{cccc}
\{1,3,9,12\} & \{4,9,10,\infty\} & \{1,3,9,10\} & \{4,9,10,12\} \\
\{3,9,10,\infty\} & \{1,4,12,\infty\} & \{1,9,12,\infty\} & \{1,3,10,\infty\} \\
\{1,3,4,9\} & \{3,4,10,12\} & \{3,4,9,\infty\} & \{1,4,10,12\}
\end{array}$$

## 4 Constructions of 2-adesigns that are almost difference families

Almost difference families were studied by Ding and Yin in [11]. Suppsoe $G$ is a finite Abelian group of order $v$ in which the identity element is denoted "0". Let $k$ and $\lambda$ be positive integers such that $2 \leq k < v$. A $(v, k, \lambda)$ *difference family* in $G$ is a collection of subsets $D_0, \ldots, D_l$ of $G$ such that

1. $|D_i| = k$ for all $i$, $0 \leq i \leq l$,
2. the multiset union $\cup_{i=1}^{l}\{x - y \mid x, y \in D_i, x \neq y\}$ contains each member of $G - \{0\}$ $\lambda$ times,

and a $(v, k, \lambda, t)$ *almost difference family* is defined similarly only the multiset union $\cup_{i=1}^{l}\{x - y \mid x, y \in D_i, x \neq y\}$ contains $t$ members of $G - \{0\}$ with multiplicity $\lambda$ and $v - t - 1$ members of $G$ with multiplicity $\lambda + 1$.

It is trivial that an almost difference family is a 2-adesign. All of the 2-adesigns in this section are also almost difference families, however, our treatment will still be in terms of 2-adesigns.

Our next two constructions make use of quadratic residues. We will need the following lemma [7].

**Lemma 4.1** *Let $q = 4f + 1 = x^2 + 4y^2$ be a prime power with $x, y \in \mathbb{Z}$ and $x \equiv 1 \pmod 4$ (here, $y$ is two-valued depending on the choice of the primitive root $\alpha$ defining the cyclotomic classes). The five distinct cyclotomic numbers of order four for odd $f$ are*

$$\begin{aligned}
(0,0) = (2,2) = (2,0) &= \frac{q - 7 + 2x}{16}, \\
(0,1) = (1,3) = (3,2) &= \frac{q + 1 + 2x - 8y}{16}, \\
(1,2) = (0,3) = (3,1) &= \frac{q + 1 + 2x + 8y}{16}, \\
(0,2) &= \frac{q + 1 - 6x}{16}, \\
\textit{all others} &= \frac{q - 3 - 2x}{16},
\end{aligned}$$

*and those for even $f$ are*

$$\begin{aligned}(0,0) &= \frac{q-11-6x}{16},\\ (0,1)=(1,0)=(3,3) &= \frac{q-3+2x+8y}{16},\\ (0,2)=(2,0)=(2,2) &= \frac{q-3+2x}{16},\\ (0,3)=(3,0)=(1,1) &= \frac{q-3+2x-8y}{16},\\ \textit{all others} &= \frac{q+1-2x}{16}.\end{aligned}$$

When computing difference levels of a subset $C$ of a group $G$, it is sometimes convenient to use the difference function which is defined as $d(w) = |C \cap (C+w)|$ where $C+w$ denotes the set $\{c+w \mid c \in C\}$. We are now ready to give our first construction of a 2-adesign that is a difference family.

**Theorem 4.2** *Let $q = 4f+1 = x^2+4y^2$ be a prime power with $f$ odd. Let $C_0 = D_0^4 \cup D_1^4$, $C_1 = D_0^4 \cup D_2^4$, and $C_2 = D_0^4 \cup D_3^4$. Then $(\mathbb{F}_q, Dev(C_0) \cup Dev(C_1) \cup Dev(C_2))$ is a 2-$(q, \frac{q-1}{2}, \frac{3q-11}{4})$ adesign.*

*Proof* Let $w^{-1} \in D_h^4$. First we let $C$ denote $D_i^4 \cup D_{i+1}^4$. Then when we expand $|C \cap (C+w)|$ we get

$$\left|D_{i+h}^2 \cap (D_{i+h}^2+1)\right| + \left|D_{i+h}^4 \cap (D_{i+h+1}^4+1)\right| + \left|D_{i+h+1}^4 \cap (D_{i+h}^4+1)\right| + \left|D_{i+h+1}^4 \cap (D_{i+h+1}^4+1)\right|$$

whence

$$\begin{aligned}|C \cap (C+w)| &= (i+h, i+h) + (i+h, i+h+1) + (i+h+1, i+h) + (i+h+1, i+h+1)\\ &= \begin{cases} \frac{q-2y-3}{4} & \text{for } i=0 \text{ and } h=0 \text{ or } 2,\\ \frac{q+2y-3}{4} & \text{for } i=0 \text{ and } h=1 \text{ or } 3,\\ \frac{q-2y-3}{4} & \text{for } i=3 \text{ and } h=0 \text{ or } 2,\\ \frac{q+2y-3}{4} & \text{for } i=3 \text{ and } h=1 \text{ or } 3.\end{cases} \quad \text{(by Lemmas 3.1 and 4.1)}\end{aligned}$$

We also have

$$|C_1 \cap (C_1+w)| = \begin{cases} \frac{q-5}{4} & \text{for } h=0 \text{ or } 2,\\ \frac{q-1}{4} & \text{for } h=1 \text{ or } 3.\end{cases}$$

Now consider the incidence structures $(\mathbb{F}_q, DevC_i)$ for $i = 0, 1, 2$. Let $C_i^{\perp}$, $(C_i+w)^{\perp}$ denote the points of the dual structures $(Dev(C_i), \mathbb{F}_q)$ corresponding to the blocks $C_i$, $C_i+w$. We have that $(\mathbb{F}_q, Dev(C_i))$ is a self-dual incidence structure and by Lemma 2.2 the number of blocks of $(\mathbb{F}_q, Dev(C_0) \cup Dev(C_1) \cup Dev(C_2))$ which the points $C_i^{\perp}$, $(C_i+w)^{\perp}$ appear in is

$$\begin{cases} \frac{3p-11}{4} & \text{if } w^{-1} \in D_0^4 \cup D_2^4,\\ \frac{3p-7}{4} & \text{if } w^{-1} \in D_1^4 \cup D_3^4.\end{cases}$$

□

Another construction is the following.

**Theorem 4.3** *Let $q = 4f + 1 = x^2 + 4y^2$ be a prime power with $f$ even and $x = 1$ or $-3$. Then $(\mathbb{F}_q, Dev(D_0^4) \cup Dev(D_2^4))$ is a 2-$\left(q, \frac{q-1}{4}, \frac{q-7-2x}{8}\right)$ adesign.*

*Proof* We have, by Lemma 4.1,

$$\begin{aligned}\left|D_i^4 \cap (D_i^4 + w)\right| &= \left|D_h^4 \cap (D_h^4 + 1)\right| \\ &= (i+h, i+h) \\ &= \begin{cases} \frac{q-11-6x}{16} & \text{if } h = 0, i = 0 \text{ or } h = 2, i = 2, \\ \frac{q-3+2x-8y}{16} & \text{if } h = 1, i = 0 \text{ or } h = 2, i = 2, \\ \frac{q-3+2x}{16} & \text{if } h = 2, i = 0 \text{ or } h = 3, i = 2, \\ \frac{q-3+2x+8y}{16} & \text{for } h = 3, i = 0 \text{ or } h = 0, i = 2. \end{cases}\end{aligned}$$

Now consider the incidence structures $(\mathbb{F}_q, Dev(D_i^4))$ for $i = 0, 2$. Let $C_i^\perp$, $(C_i + w)^\perp$ denote the points of the dual structures $(Dev(D_i^4), \mathbb{F}_q)$ corresponding to the blocks $C_i$, $C_i + w$. We have that $(\mathbb{F}_q, Dev(C_i))$ is a self-dual incidence structure and by Lemma 2.2 the number of blocks of $(\mathbb{F}_q, Dev(D_0^4) \cup Dev(D_2^4))$ which the points $C_i^\perp$, $(C_i + w)^\perp$ appear in is

$$\begin{cases} \frac{2q-14-4x}{16} & \text{if } w^{-1} \in D_0^4 \cup D_2^4, \\ \frac{2q-6+4x}{16} & \text{if } w^{-1} \in D_1^4 \cup D_3^4. \end{cases}$$

Thus, we have $(\mathbb{F}_q, Dev(D_0^4) \cup Dev(D_2^4))$ is a 2-adesign whenever $x = 1$, or $-3$. □

We close this section with yet a few more constructions. Now let $q$ be an odd prime power, and $C \subseteq \mathbb{F}_q$. According to [19], if

1. $C = D_i^4 \cup D_{i+1}^4$, $q \equiv 5 \pmod 8$ and $q = s^2 + 4$ with $s \equiv 1 \pmod 4$, or
2. $C = D_0^8 \cup D_1^8 \cup D_2^8 \cup D_5^8$, $q = l^2$ where $l$ is a prime power of form $l = t^2 + 2 \equiv 3 \pmod 8$, or
3. $C = \cup_{i \in I} D_i^{\sqrt{q}+1}$ where $I \subseteq \{0, 1, \ldots, \sqrt{q}\}$ with $|I| = \frac{\sqrt{q}+1}{2}$ and $q = l^2$ for some prime power $l$,

then $C$ is a $\left(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{2}\right)$ almost difference set in $\mathbb{F}_q$.

It is easy to show, also, that if $q$ is an odd prime power, $(\mathbb{F}_q, Dev(D_0^2) \cup Dev(D_1^2))$ is a 2-$\left(q, \frac{q-1}{2}, \frac{2q-6}{4}\right)$ design. We then have the following.

**Theorem 4.4** *Let $q$ be an odd prime power, and $C \subseteq \mathbb{F}_q$. If*

1. *$C = D_i^4 \cup D_{i+1}^4$, $q \equiv 5 (mod\ 8)$ and $q = s^2 + 4$ with $s \equiv 1 (mod\ 4)$, or*
2. *$C = D_0^8 \cup D_1^8 \cup D_2^8 \cup D_5^8$, $q = l^2$ where $l$ is a prime power of form $l = t^2 + 2 \equiv 3 (mod\ 8)$, or*
3. *$C = \cup_{i \in I} D_i^{\sqrt{q}+1}$ where $I \subseteq \{0, 1, \ldots, \sqrt{q}\}$ with $|I| = \frac{\sqrt{q}+1}{2}$, $I$ contains both even and odd numbers, and $q = l^2$ for some prime power $l$,*

*then $(\mathbb{F}_q, Dev(D_0^2) \cup Dev(D_1^2) \cup Dev(C))$ is a 2-$(q, \frac{q-1}{2}, \frac{3q-11}{4})$ adesign.*

## 5 Constructions of 2-adesigns from symmetric designs

Let $(V, \mathcal{B})$ be an incidence structure with $|\mathcal{B}| = b$. The numbers of blocks in which given single points appear (called the *replication numbers*) become the block sizes of the dual

$(V, \mathcal{B})^{\perp}$, and the intersection numbers among pairs of blocks become the numbers of blocks of $(V, \mathcal{B})^{\perp}$ in which any two points appear. Then the following is clear.

**Lemma 5.1** *Let $(V, \mathcal{B})$ be an incidence structure with $|V| = v$, and in which the replication numbers are a constant $k$ and the intersection numbers among pairs of blocks are integers $\lambda$ and $\lambda + 1$. Then $(V, \mathcal{B})^{\perp}$ is a 2-$(b, k, \lambda)$ adesign.*

*Remark 5.1* The dual of a quasi-symmetric design whose intersection numbers $x$, $y$ are such that $y - x = 1$ is always a 2-adesign.

In [2] constructions of almost difference sets from difference sets were introduced. In this section we further generalize this idea. We will use the following lemma which is actually a trivial construction in itself.

**Lemma 5.2** *Let $(V, \mathcal{B})$ be a symmetric 2-$(v, k, \lambda)$ design. Let $\mathbf{b}_1, \ldots, \mathbf{b}_k$ be any $k$ blocks in $\mathcal{B}$. Let "$\infty$" denote a point. Let $\mathcal{B}'$ denote the blocks of $\mathcal{B}$ modified by adjoining the point "$\infty$" to each of $\mathbf{b}_1, \ldots, \mathbf{b}_k$. Then $(V, \mathcal{B}')^{\perp}$ is a 2-$(v, k, \lambda)$ adesign.*

*Proof* The replication numbers in the incidence structure $(V, \mathcal{B}')$ are all $k$, and the intersection numbers among pairs of blocks in $\mathcal{B}'$ are $\lambda$ and $\lambda + 1$. The result follows from Lemma 5.1. □

Note that the number of times which Lemma 5.2 can be applied to any given symmetric 2-$(v, k, \lambda)$ design is $\lfloor \frac{v}{k} \rfloor$.

The following theorem gives another construction.

**Theorem 5.3** *Let $(V, \mathcal{B})$ be a symmetric 2-$(v, k, \lambda)$ design. Let $\mathbf{b} = \{b_1, \ldots, b_k\}$ be a block. Suppose that $\mathbf{b}_1, \ldots, \mathbf{b}_k$ are $k$ blocks not equal to $\mathbf{b}$ such that*

1. *$b_i \notin \mathbf{b}_i$ for all $i$, $1 \le i \le k$, and*
2. *$b_j \in \mathbf{b}_l$ implies $b_l \notin \mathbf{b}_j$ for all $j \ne l$, $1 \le j, l \le k$.*

*Let $\mathcal{B}'$ denote the blocks of $\mathcal{B}$ modified by adjoining the point $b_i$ to the block $\mathbf{b}_i$ for all $i$, $1 \le i \le k$, and then removing the block $\mathbf{b}$. Then $(V, \mathcal{B}')^{\perp}$ is a 2-$(v, k, \lambda)$ adesign.*

*Proof* It is easy to see that the replication numbers of $(V, \mathcal{B}')$ are all $k$. The second condition in the statement ensures that the intersection numbers among pairs of blocks of $\mathcal{B}'$ are either $\lambda$ or $\lambda + 1$. The result then follows from Lemma 5.1. □

Next, we show how to construct almost difference sets from planar difference sets. The following constructions are not optimal but, for certain dimensions, give the best known value for $d_1$. A $(v, k, \lambda)$ difference set is called planar if $\lambda = 1$. It is easy to show that, given a planar difference set $D$ in an (additive) Abelian group $G$ of order $v$, if we choose any $a_0 \in G - D$ such that $2a_0$ cannot be written as the sum of two distinct members of $D$, then $D \cup \{a_0\}$ will be an almost difference set with $\lambda = 1$. This is simply due to the fact that, because of the way we chose $a_0$, we cannot have $a_0 - a = b - a_0$ for any $a, b \in D$, thereby forcing each member of $G$ to appear as a difference of two distinct members of $D \cup \{a_0\}$ only one or two times.

Again, let $D$ be a $(v, k, 1)$ difference set in an Abelian group $G$ of order $v$. Also let $\kappa : G \to \mathbb{Z}_2 \times G$ by $x \mapsto (0, x)$. Suppose $a_0, \ldots, a_{s-1} \in G$ are such that the differences $(1, \tau)$ in $\kappa(D) \cup \{(1, a_0), \ldots, (1, a_{s-1})\}$ cover $\{1\} \times G$ each having multiplicity at most 2, that exactly one of the $a_i$s is a member of $D$, and twice any $a_i$ is not the sum of two other distinct $a_i$s. If there is at least one difference in $\kappa(D) \cup \{(1, a_0), \ldots, (1, a_{s-1})\}$ having multiplicity 1, then since the difference $(1, 0)$ occurs exactly twice (because exactly one of the $a_i$s is in $D$), we have both 1 and 2 occurring as multiplicities. No difference can occur with multiplicity greater than 2 since $G$ is planar and twice any $a_i$ is not the sum of two other distinct $a_i$s. We also have the differences in $\kappa(D) \cup \{(1, a_0), \ldots, (1, a_{s-1})\}$ covering $\mathbb{Z}_2 \times G$: the differences $(0, \tau)$ cover $\{0\} \times G$ due to $G$ being a planar difference set and we have assumed that the differences $(1, \tau)$ cover $\{1\} \times G$. This discussion is summarized in the following.

**Theorem 5.4** *Let $D$ be a $(v, k, 1)$ difference set in an (additive) Abelian group $G$. Suppose $a_0, \ldots, a_{s-1} \in G$ are such that the differences $(1, \tau)$ in $\kappa(D) \cup \{(1, a_0), \ldots, (1, a_{s-1})\}$ cover $\{1\} \times G$ each having multiplicity at most 2, that exactly one of the $a_i$s is a member of $D$, and twice any $a_i$ is not the sum of two other distinct $a_i$s. If there is at least one difference in $\kappa(D) \cup \{(1, a_0), \ldots, (1, a_{s-1})\}$ having multiplicity 1 then $\kappa(D) \cup \{(1, a_0), \ldots, (1, a_{s-1})\}$ is a $(2v, k + s, 1, t)$ almost difference set in $\mathbb{Z}_2 \times G$. The resulting symmetric 2-adesign $(\mathbb{Z}_2 \times G, Dev(\kappa(D) \cup \{(1, a_0), \ldots, (1, a_{s-1})\}))$ has parameters $(2v, k + s, 1)$.*

*Example 5.5* Consider the Singer difference set $\{1, 2, 4\}$ in $\mathbb{Z}_7$. With $a_0 = 0$ we have $2a_0$ is not the sum of two distinct members of $D$, and $\kappa(D) \cup \{(1, 0)\}$ is a $(14, 4, 0, 1)$ almost difference set in $\mathbb{Z}_{14}$. With $a_1 = 1$ we have $\kappa(D) \cup \{(1, 0), (1, 1)\}$ is a $(14, 5, 1, 6)$ almost difference set in $\mathbb{Z}_{14}$

*Example 5.6* Consider the Singer difference set $D = \{0, 1, 5, 11\}$ in $\mathbb{Z}_{13}$. With $a_0 = 10$, we have $2a_0$ is not the sum of two distinct members of $D$, and it is easily checked that $\kappa(D) \cup \{(1, 10)\}$ is a $(26, 5, 0, 5)$ almost difference set in $\mathbb{Z}_{26}$. With $a_1 = 11$ we have that $\kappa(D) \cup \{(1, a_0), (1, a_1)\}$ is a $(26, 6, 1, 11)$ almost difference set.

*Example 5.7* Now consider the Singer difference set $D = \{0, 3, 13, 15, 20\}$ in $\mathbb{Z}_{21}$. We have $\{9, 13, 16\}$ are such that the differences $(1, \tau)$ cover $\{1\} \times \mathbb{Z}_{21}$ with multiplicities no more than 2 and that 13 is the only member that is also in $D$. It is also easy to see that the difference $(1, 9)$ can only occur as the difference $(1, 9) - (0, 0)$. Thus we have $\kappa(D) \cup \{(1, 9), (1, 13), (1, 16)\}$ is a $(42, 8, 1, 16)$ almost difference set.

## 6 Constructions of 3-adesigns

In this section we will give two constructions each of which produce infinitely many 3-adesigns.

Our first constructions makes use of quadratic residues.

**Theorem 6.1** *Let $q \equiv 3(mod\ 4)$ be an odd prime power. Then $(\mathbb{F}_q, Dev(D_0^2) \cup Dev(D_1^2))$ is a 3-$(q, \frac{q-1}{2}, \frac{q-7}{4})$ adesign.*

*Proof* Denote $\frac{q-1}{2}$ by $k$ and $\frac{q-3}{4}$ by $\lambda'$. Let $x, y, z \in \mathbb{F}_q$ be arbitrary. To count the number of blocks in which $x, y, z$ appear together, we first count the number of blocks of $Dev(D_0^2) \cup Dev(D_1^2 \cup \{0\})$ in which $x, y, z$ appear together. Suppose that the three points $x, y, z$ appear in $\mu$ blocks in $Dev(D_0^2)$. Using the fact that $(\mathbb{F}_q, Dev(D_0^2))$ is a 2-$(q, k, \lambda')$ design, a simple counting argument gives that there are $q - 3k + 3\lambda' - \mu$ blocks in $Dev(\overline{D_0^2})$:=$Dev(D_1^2 \cup \{0\})$ containing $x, y, z$. Thus, there are $q - 3k + 3\lambda' = \lambda'$ blocks in $Dev(D_0^2) \cup Dev(\overline{D_0^2})$ containing $x, y, z$. Since $w \in D_1^2 \cup \{0\} + w$ for all $w \in \mathbb{F}_q$, we want to know how many of the $q - 3k + 3\lambda' - \mu$ blocks in $Dev(\overline{D_0^2})$ are also in $\{\overline{D_0^2} + x, \overline{D_0^2} + y, \overline{D_0^2} + z\}$. Without loss of generality suppose that both $\overline{D_0^2}+x$ and $\overline{D_0^2}+y$ contain the three points $x, y, z$. Then we must have $y-x, z-x \notin D_0^2$ and $x-y, z-y \notin D_0^2$. But this would imply that $x-y, y-x \in D_1^2$ where both $x-y$ and $y-x$ are nonzero. But this is impossible as the additive inverse of any member of $D_1^2$ cannot also be a member whenever $q \equiv 3 \pmod 4$. Then no more than one of the blocks $\overline{D_0^2}+x$, $\overline{D_0^2}+y$, $\overline{D_0^2}+z$ can contain all three of $x, y, z$. We now need to show that there are two different 3-levels, i.e. that $(\mathbb{F}_q, Dev(D_0^2) \cup Dev(D_1^2))$ is not a 3-design, but a 3-adesign. To show this we assume that $(\mathbb{F}_q, Dev(D_0^2) \cup Dev(D_1^2))$ is a 3-$(q, k, \lambda)$-design for some $\lambda$. Then the number of blocks must be given by $\lambda \frac{\binom{q}{3}}{\binom{k}{3}}$. The only choices for $\lambda$ are $\lambda'$ or $\lambda' - 1$. If $\lambda = \lambda'$ then we get that $q-5 = q-4$. If $\lambda = \lambda' - 1$ then we get that $(q-3)(q-5) = (q-7)(q-2)$. Either way we get a contradiction, which completes the proof. □

*Example 6.2* With $q = 11$ we apply Theorem 6.1 and get that $(\mathbb{Z}_{11}, Dev(D_0^2) \cup Dev(D_1^2))$ is a 3-$(11, 5, 1)$ adesign with blocks:

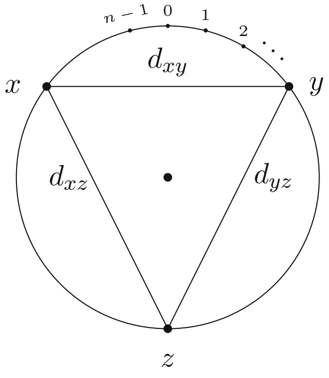
$\{1,3,4,5,9\}$ $\{2,4,5,6,10\}$ $\{0,3,5,6,7\}$ $\{1,4,6,7,8\}$ $\{2,5,7,8,9\}$ $\{0,4,5,6,8\}$
$\{3,6,8,9,10\}$ $\{0,4,7,9,10\}$ $\{0,1,5,8,10\}$ $\{0,1,2,6,9\}$ $\{1,2,3,7,10\}$ $\{1,5,6,7,9\}$
$\{0,2,3,4,8\}$ $\{2,6,7,8,10\}$ $\{0,3,7,8,9\}$ $\{1,4,8,9,10\}$ $\{0,2,5,9,10\}$
$\{0,1,3,6,10\}$ $\{0,1,2,4,7\}$ $\{1,2,3,5,8\}$ $\{2,3,4,6,9\}$ $\{3,4,5,7,10\}$

Our second construction is related to graphs, though it is simple enough to avoid graph-theoretical preliminaries.

**Theorem 6.3** *Let $n$ ($\geq 7$) be an odd integer not divisible by 3. Consider, for fixed $a \in \mathbb{Z}_n$, all pairs $\{a-i \pmod n, a+i \pmod n\}$ for $i = 1, \cdots, \frac{n-1}{2}$. The union of any two distinct pairs gives a block consisting of four points. Denote, for fixed $a \in \mathbb{Z}_n$, the set of all blocks obtained in this way by $B_a$. Then $(\mathbb{Z}_n, \cup_{a \in \mathbb{Z}_n} B_a)$ is a 3-$(n, 4, 2)$ adesign.*

*Proof* Arrange all the points in a circle as is shown in the graph below. For any three points $x, y, z \in \mathbb{Z}_n$, denote $|x-y|, |x-z|, |y-z|$ by $d_{xy}, d_{xz}, d_{yz}$ respectively.

Since $n$ is not divisible by 3, $d_{xy} = d_{xz} = d_{yz}$ cannot happen. Then suppose two of them are equal. Without loss of generality, suppose $d_{xz} = d_{yz}$. Then when $x$ and $y$ are in a pair, $z$ must be the fixed point so that there is no block containing all three of $x$, $y$ and $z$. When $x$ and $z$ are in a pair or $y$ and $z$ are in pair, we can find exactly one block containing the three points in each case. If $d_{xy}$, $d_{xz}$ and $d_{yz}$ are distinct, then we can find one block containing these three points when any two points are in pair, in which case we have three blocks containing these three points together.



□

*Example 6.4* With $n = 7$ we apply Theorem 6.3 and get that $(\mathbb{Z}_7, \cup_{a \in \mathbb{Z}_7} B_a)$ is a 3-(7, 4, 2) adesign with blocks:

$$\begin{array}{ccccccc}
\{1,7,2,6\} & \{1,7,3,5\} & \{2,6,3,5\} & \{7,6,1,5\} & \{7,6,2,4\} & \{1,5,2,4\} & \{1,4,2,3\} \\
\{1,3,7,4\} & \{1,3,6,5\} & \{7,4,6,5\} & \{7,2,6,3\} & \{7,2,5,4\} & \{6,3,5,4\} & \{1,2,7,3\} \\
\{1,6,2,5\} & \{1,6,3,4\} & \{2,5,3,4\} & \{7,5,1,4\} & \{7,5,2,3\} & \{7,3,6,4\} & \{1,2,6,4\}
\end{array}$$

Let $(V, \mathcal{B})$ be an incidence structure. Let $p \in V$, and define $\mathcal{B}_p = \{\mathcal{B} - \{p\} \mid \mathcal{B} \in \mathcal{B} \text{ and } p \in \mathcal{B}\}$. We call the incidence structure $(V - \{p\}, \mathcal{B}_p)$ the *contraction* of $(V, \mathcal{B})$ at $p$. It is clear that contracting at points of a 3-adesign will give a 2-adesign as long as not all 3-sets of points occur in the same number of blocks of the contraction.

*Example 6.5* The contraction at the point $p = 1$ of the 3-(11, 5, 1) adesign in Example 6.2 is a symmetric 2-(10, 4, 1) adesign with the ten blocks:

$$\begin{array}{ccccc}
\{3,4,5,9\} & \{4,6,7,8\} & \{0,5,8,10\} & \{0,2,6,9\} & \{2,3,7,10\} \\
\{4,8,9,10\} & \{0,3,6,10\} & \{0,2,4,7\} & \{2,3,5,8\} & \{5,6,7,9\}
\end{array}$$

*Remark 6.1* Interestingly, a contraction at any point of the incidence structure $(\mathbb{F}_q, Dev(D_0^2) \cup Dev(D_1^2))$ from Theorem 6.1 gives a symmetric 2-$\left(q-1, \frac{q-3}{2}, \frac{q-7}{4}\right)$ adesign and, since it contains punctured translates of both $D_0^2$ and $D_1^2$, cannot be the development of any almost difference set.

# 7 Related codes

A linear binary *code* $C$ of *length* $n$ and *dimension* $k$ (or simply an $[n, k]$ code), is a $k$-dimensional linear subspace of the $n$-dimensional binary vector space $\mathbb{F}_2^n$. The *dual* $C^\perp$ of an $[n, k]$ code $C$ is the $[n, n-k]$ code that is the orthogonal space of $C$ with respect to the inner product of the binary field. Any basis of $C$ is called a *generator matrix* of $C$, and any basis of $C^\perp$ is called a *parity check matrix* of $C$. The Hamming distance between two vectors $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ is the number of indices $i$ such that $x_i \neq y_i$. The Hamming *weight* of a vector is the number of its nonzero coordinates. The minimum distance $d$ of a code is smallest possible distance between pairs of distinct codewords. An $[n, k]$ code $C$ is *self-orthogonal* if $C \subseteq C^\perp$. An $[n, k]$ code $C$ is *optimal* if, given its length and dimension, has the largest possible minimum distance. The best codes for a given length and dimension can be found in the code tables in [15].

## 7.1 Cyclic codes

We assume some familiarity with cyclic codes. For more details on the subject the reader is referred to [10]. An $[n, k]$ code $C$ over $\mathbb{F}_2$ is called *cyclic* if $(c_0, c_1, \dots, c_{n-1}) \in C$ implies that the circular shift $(c_{n-1}, c_0, \dots, c_{n-2})$ is also in $C$. By identifying any vector $(c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_2^n$ with the polynomial

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_2[x]/(x^n - 1),$$

any linear code $C$ of length $n$ over $\mathbb{F}_2$ corresponds to a subset of $\mathbb{F}_2[x]/(x^n - 1)$. The code is cyclic if and only if the corresponding subset is an ideal in the ring $\mathbb{F}_2[x]/(x^n - 1)$. Note that every ideal of $\mathbb{F}_2[x]/(x^n - 1)$ is principal. Let $g(x) \in \mathbb{F}_2[x]/(x^n - 1)$ be monic and of minimum degree, and let $C = \langle g(x) \rangle$. Then $g(x)$ is called the *generator polynomial* of $C$, and $h(x) = (x^n - 1)/g(x)$ is referred to as the *parity-check* polynomial. The dimension of $C$ is given by the degree of $h(x)$.

The following theorem is easy to prove.

**Lemma 7.1** *Let $D$ be subset of $\mathbb{Z}_n$ with two difference levels. Define $D(x) = \sum_{i \in D} x^i \in \mathbb{F}_2[x]$, $g(x) = gcd(x^n - 1, D(x))$, and $h(x) = (x^n - 1)/g(x)$. Then the code $C = \langle g(x) \rangle$ is an $[n, k]$ cyclic code where $k = deg(h(x))$.*

### 7.2 Known results on cyclic codes from 2-adesigns

It is known that when $p \equiv 1 (\bmod 4)$ the code $C = \langle D_0^2(x) \rangle$ is a quadratic residue code if 2 is a square in $\mathbb{F}_p^*$, and a trivial cyclic code otherwise [10]. When $p = 9 + 4y^2 \equiv 1(\bmod 4)$ resp. $p = 49 + 4y^2 \equiv 1(\bmod 4)$ is a prime, $D_0^4$ resp. $D_0^4 \cup \{0\}$ is an almost difference set [19]. If $D$ is either of these almost difference sets, then some parameters for the code $C = \langle D(x) \rangle$ are known and can be found in [9]. When $p_1$ and $p_2$ are primes such that $p_2 - p_1 = 4$, the set $E = E_1^{(2)} \cup \{p_1, 2p_1, \ldots, (p_2 - 1)p_1\}$, where $E_1^{(2)} = \{0 \leq i \leq p_1 p_2 \mid \frac{i}{p_1 p_2} = -1\}$, is an almost difference set [19], and some of the parameters of $C = \langle E(x) \rangle$ are known and can be found in [8]. Lastly, when $q$ is a prime power and $\alpha$ a generator of $\mathbb{F}_{q^2}^*$, the set $D_q = \{0 \leq i \leq n - 1 \mid Tr(\alpha^i) = 1\}$ is a planar almost difference set (i.e. with difference levels 0 and 1), and the code $C = \langle D_q(x) \rangle$ has parameters $\left[q^2 - 1, q + 1, q - 1\right]$ [10]. There are many other constructions of almost difference sets, and the parameters of their linear codes are open in general.

### 7.3 Cyclic codes from sets with two difference levels

Sets with two difference levels that are not almost difference sets can also generate codes with good parameters. For example, when $q \equiv 1(\bmod 8)$ is a prime power with unique representation $q = x^2 + 4y^2 = a^2 + 2b^2$ where $x, a \equiv 1(\bmod 4)$, and $\alpha$ is a generator of $\mathbb{F}_q^*$, we can define $D = D_0^8 \cup D_1^8 \cup D_2^8 \cup D_5^8$ and $\Delta_j = |(D + \alpha^j \cap D|$. It was shown in [13] that

$$\Delta_0 = \Delta_2 = \Delta_4 = \Delta_6 = \frac{16q - 48 + 8x - 8a - 16y}{64} \tag{5}$$

$$\Delta_1 = \Delta_5 = \frac{16q - 80 - 16x + 16a - 32y}{64} \tag{6}$$

$$\Delta_3 = \Delta_7 = \frac{16q - 16}{64}. \tag{7}$$

Thus, if $3(a - x) - 2y = 4$, we have that $(\mathbb{F}_q, Dev(D))$ is an incidence structure with two difference levels given by $\mu_1 = \frac{16q-48+8x-8a-16y}{64}$ and $\mu_2 = \frac{16q-16}{64}$.

*Example 7.2* With $q = 73$ we have the unique representation is given by $x = -3$, $y = 4$ and $a = 1, b = 6$. Thus the two difference levels are $\mu_1 = 16$ and $\mu_2 = 18$. Since the difference levels are $\equiv 0(\bmod 2)$, the inner product over the field $\mathbb{F}_2$ of any two rows of the incidence matrix will be 0, making the code $C = \langle D(x) \rangle$ self-orthogonal. We checked using MAGMA, and $C$ is a [73, 18, 24] code. According the code tables in [15], the best binary code with length 73 and dimension 18 has minimum weight 24.

We also have computed the following example using cyclotomic classes of order ten. The cyclotomic numbers of order ten are known and can be found in [24].

*Example 7.3* Let $q = 151$, and define $D = D_4 \cup D_5 \cup D_8 \cup D_9$. Then $D$ has the two difference levels $\mu_1 = 22$ and $\mu_2 = 24$ and the code $C = \langle D(x) \rangle$ is self-orthogonal. We checked using MAGMA, and $C$ is a $[151, 30, 48]$ code. According the code tables in [15], the best binary code with length 151 and dimension 30 has minimum weight 48.

**Lemma 7.4** *Let $A$ be a $v \times v$ incidence matrix of the symmetric incidence structure $(G, \mathcal{B})$ obtained from the development of some $k$-subset $D$ in the Abelian group $G$ (where $|G| = v$) with difference levels $\mu_1 < \cdots < \mu_s$. Suppose that $k \equiv \mu_1 \equiv \cdots \equiv \mu_s (mod\ 2)$.*

1. *If $k$ is even the binary code of length $v$ with generator matrix $A$ is self-orthogonal.*
2. *If $k$ is odd the matrix*

$$\begin{bmatrix} 1 & \\ \vdots & A \\ 1 & \end{bmatrix}$$

*generates a binary self-orthogonal code of length $v + 1$.*

*Proof* By Lemma 2.2 we can see that, in both cases, the weights of the rows of the generator matrix are all even and the inner product of any two rows is even as well. □

We will refer to an incidence structure $(V, \mathcal{B})$ whose incidence matrix generates a self-orthogonal code simply as *self-orthogonal*.

We will use the following lemma.

**Lemma 7.5** *Let $(G, \mathcal{B})$ be a symmetric incidence structure coming from the development of a $k$-subset $D$ of the Abelian group $G$ (where $|G| = v$) with difference levels $\mu_1$ and $\mu_2$. Let $t$ denote the number of members of $G - \{0\}$ which appear $\mu_1$ times in the multiset $\{x - y \mid x, y \in D, x \neq y\}$. The the number of pairs of points in $G$ appearing in exactly $\mu_1$ blocks in $\mathcal{B}$ is $\frac{vt}{2}$ and the number of pairs of points of $V$ appearing in $\mu_2$ blocks is $\frac{v(v-1-t)}{2}$.*

*Proof* For each $x \in V$, there are $t$ points in $V - \{x\}$ each appearing together with $x$ in exactly $\mu_1$ blocks. Thus, there are $\frac{vt}{2}$ pairs of points of $V$ appearing in $\mu_1$ blocks. Similarly, there are $\frac{v(v-1-t)}{2}$ pairs of points of $V$ appearing in $\mu_2$ blocks. It is easily seen that $\frac{vt}{2} + \frac{v(v-1-t)}{2} = \binom{v}{2}$. □

We were able to come up with the following bound on the minimum distance of a code generated by a self-orthogonal incidence structure with two difference levels. However, as is clear from Examples 7.2 and 7.3, there is much room for improvement.

**Theorem 7.6** *Let $A$ be the incidence matrix of a self-orthogonal incidence structure $(G, \mathcal{B})$ coming from the development of a $k$-subset $D$ of the Abelian group $G$ (where $|G| = v$) with difference levels $\mu_1$ and $\mu_2$. Let $t$ denote the number of members of $G - \{0\}$ which appear $\mu_1$ times in the multiset $\{x - y \mid x, y \in D, x \neq y\}$. The dual of the binary code with generator matrix $A$ has minimum distance*

$$d \geq \frac{(\mu_2 + k) + \sqrt{(\mu_2 + k)^2 + 4\mu_2(\mu_2 - \mu_1)vt}}{2\mu_2}.$$

*Proof* Let $S$ be a minimal set of linearly dependent columns of $A$. Then every row of $A$ must intersect an even number of these columns in 1s. Let $n_i$ denote the number of rows of $A$ intersecting exactly $i$ columns of $S$ in 1s. Let $d = |S|$. Since every column of $A$ contains $k$ 1s (because the incidence structure $(G, \mathcal{B})$ is symmetric) and the scalar product (over the reals) of any two columns is either $\mu_1$ or $\mu_2$, using Lemma 7.5 we have

$$\sum 2in_{2i} = kd$$

and

$$\sum 2i(2i-1)n_{2i} = \mu_2 d(d-1) - (\mu_2 - \mu_1)vt.$$

Subtracting the first equation from the second we have

$$\sum 2i(2i-2)n_{2i} = d((d-1)\mu_2 - k) - (\mu_2 - \mu_1)vt \geq 0.$$

On one hand we get that $d((d-1)\mu_2 - k) \geq (\mu_2 - \mu_1)vt \geq 0$ and on the other hand we get that $d^2\mu_2 - d(\mu_2 + k) - (\mu_2 - \mu_1)vt \geq 0$. The result follows from solving the quadratic. □

### 7.4 Noncyclic codes from adesigns

In general, the parameters of codes generated from adesigns are open. Using MAGMA we have computed the parameters of the codes generated by the transpose of the incidence matrix of many of our constructions. We have included the parameters and construction information in the following two tables.

*Remark 7.1* The [159, 52, 36] code corresponding to the 2-(53, 26, 37) adesign in Table 1 actually improves the lower bound for the minimum weight given in [15] for the best binary code with length 53 and dimension 26.

*Remark 7.2* The code corresponding to the 3-(7, 4, 2) adesign in Table 2 is in fact an optimal, projective two-weight [21, 6, 8] code, and so is an optimal code that corresponds to a strongly regular graph [4].

*Remark 7.3* The codes corresponding to the 3-(7, 3, 0) and 3-(19, 9, 3) adesigns in Table 2 are both extremal self-dual codes [21].

**Table 1** Parameters of codes from new 2-adesigns computed by MAGMA

| 2-Adesign ref | $(v, k, \lambda)$ | No. of blocks | Code parameters | Best $d$ | Optimal |
|---|---|---|---|---|---|
| Theorem 3.2 | (11, 5, 3) | 20 | [20, 11, 4] | 5 | No |
| Theorem 3.2 | (19, 9, 7) | 36 | [36, 19, 7] | 8 | No |
| Theorem 3.7 | (9, 4, 2) | 16 | [16, 8, 5] | 5 | Yes |
| Theorem 3.7 | (21, 10, 8) | 40 | [40, 20, 9] | 9 | No |
| Theorem 3.9 | (9, 5, 4) | 16 | [16, 9, 4] | 4 | Yes |
| Theorem 3.9 | (21, 11, 10) | 40 | [40, 21, 8] | 8 | No |
| Theorem 4.2 | (13, 6, 7) | 39 | [39, 12, 12] | 14 | No |
| Theorem 4.2 | (29, 14, 19) | 87 | [87, 28, 22] | 24 | No |
| Theorem 4.2 | (53, 26, 37) | 159 | [159, 52, 36] | 35 | No |
| Theorem 4.3 | (17, 4, 1) | 34 | [34, 16, 6] | 8 | No |
| Theorem 4.3 | (73, 18, 8) | 146 | [146, 72, 20] | 22 | No |

The column “Best $d$” contains the best known minimum distances according to [15]

**Table 2** Parameters of codes from new 3-adesigns computed by MAGMA

| 3-Adesign ref | $(v, k, \lambda)$ | No. of blocks | Code parameters | Best $d$ | Optimal |
|---|---|---|---|---|---|
| Theorem 6.1 | (7, 3, 0) | 14 | [14, 7, 4] | 4 | Yes |
| Theorem 6.1 | (19, 9, 3) | 38 | [38, 19, 8] | 8 | No |
| Theorem 6.3 | (7, 4, 2) | 21 | [21, 6, 8] | 8 | Yes |
| Theorem 6.3 | (11, 4, 2) | 110 | [110, 10, 40] | 50 | No |

The column "Best $d$" contains the best minimum distances according to [15]

## 8 Concluding remarks

We have investigated some generalizations of combinatorial designs arising from almost difference sets, especially the $t$-adesigns. We have discussed some of their basic properties and have given several constructions for 2-adesigns, and two constructions for 3-adesigns. Many of the codes arising from these structures have good parameters, as was discussed in Sect. 7, and we have included some of these in the tables of the previous section. Questions concerning the parameters of the codes arising from adesigns are open in general and, as good codes are arising from many of these structures, further investigation would be worthwhile.

**Acknowledgements** We would like to thank the anonymous referees for the valuable and insightful comments which helped us to improve this paper.

## References

1. Andrews G.E.: Number Theory, pp. 128–132. W. B. Saunders, Philadelphia (1971).
2. Arasu K.T., Ding C., Helleseth T., Kumar P.V., Martinsen H.M.: Almost difference sets and their sequences with optimal autocorrelation. IEEE Trans. Inf. Theory **47**, 2934–2943 (2001).
3. Bose R.C.: A note on fisher's inequality for balanced incomplete block designs. Ann. Math. Stat. **20**(4), 619–620 (1949).
4. Calderbank R., Kantor W.M.: The geomertry of two-weight codes. Bull. Lond. Math. Soc. **18**, 97–122 (1986)
5. Cusick T.W., Ding C., Renvall A.: Stream Ciphers and Number Theory. Elsevier, North-Holland (1998).
6. Dembowski P.: Finite Geometries. Springer, New York (1968).
7. Dickson L.E.: Cyclotomy, higher congruences and Waring's problem. Am. J. Math. **57**, 391–424 (1935).
8. Ding C.: Cyclic codes from the two-prime sequences. IEEE Trans. Inf. Theory **58**(6), 3881–3891 (2012).
9. Ding C.: Cyclic codes from cyclotomic sequences of order four. Finite Fields Appl. **23**, 8–34 (2013).
10. Ding C.: Codes from Difference Sets, p. 75. World Scientific, Singapore (2015).
11. Ding C., Yin J.: Constructions of almost difference families. Discret. Math. **308**, 4941–4954 (2008).
12. Ding C., Helleseth T., Martinsen H.: New families of binary sequences with optimal three-level autocorrelation. IEEE Trans. Inf. Theory **47**(1), 428–433 (2001).
13. Ding C., Pott A., Wang Q.: Constructions of almost difference sets from finite fields. Des Codes Cryptogr. **72**, 581–592 (2014).
14. Fisher R.A.: An examination of the different possible solutions of a problem in incomplete blocks. Ann. Eugen. **10**, 52–75 (1940).
15. Grassl M.: Tables for linear codes. Online at http://www.codetables.de.
16. Hall Jr. M.: A survey of difference sets. Proc. AMS **7**, 975–986 (1956).
17. Hirschfeld J.W.P.: Projective Geometries Over Finite Fields, 2nd edn. Oxford University Press, Oxford (1988).
18. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
19. Nowak K.: A survey on almost difference sets (2014). arXiv:1409.0114v1.

20. Ogata W., Kurosawa K., Stinson D.R., Saido H.: New combinatorial designs and their applications to authentication codes and secret sharing schemes. Discret. Math. **279**, 384–405 (2004).
21. Rains E.M.: Shadow bounds for self-dual codes. IEEE Trans. Inf. Theory **44**(1), 134–139 (1998).
22. Stinson D.R.: Combinatorial Designs: Constructions and Analysis. Springer, New York (2003).
23. Tang X.H., Gong G.: New constructions of binary sequences with optimal autocorrelation magnitude/value. IEEE Trans. Inf. Theory **56**(3), 1278–1286 (2010).
24. Whiteman A.L.: The cyclotomic numbers of order ten. Acta Arith. **10**, 95–111 (1960).
25. Yu N.Y., Gong G.: New binary sequences with optimal autocorrelation. IEEE Trans. Inf. Theory **54**(10), 4771–4779 (2008).
26. Zhang Y., Lei J.G., Zhang S.P.: A new family of almost difference sets and some necessary conditions. IEEE Trans. Inf. Theory **52**(5), 2052–2061 (2006).