2-designs from strong difference families

Xiaomiao Wang

Ningbo University

Joint work with Yanxun Chang, Simone Costa and Tao Feng

Strong difference families

Definition

Let $F = [F_1, F_2, \ldots, F_t]$ with $F_i = [f_{i,0}, f_{i,1}, \ldots, f_{i,k-1}]$ for $1 \leq i \leq t$, be a family of t multisets of size k defined on a group $(G, +)$ of order g. F is a (G, k, μ) strong difference family, or a (g, k, μ)-SDF over G, if the list

$$\Delta F = \bigcup_{i=1}^{t} [f_{i,a} - f_{i,b} : 0 \leq a, b \leq k-1; a \neq b] = \underline{\mu} G.$$

- The members of F are also called base blocks.
- If a (G, k, μ)-SDF has exactly one base block, then this block is referred to as a (G, k, μ) difference multiset (or difference cover).
- Note that μ is necessarily even.
- A $(3, 3, 2)$-SDF over $\mathbb{Z}_3$: $[0, 0, 1]$.

Relative difference families

Definition

Let $(G,+)$ be an abelian group of order g with a subgroup N of order n. A (G,N,k,λ) relative difference family, or (g,n,k,λ)-DF over G relative to N, is a family $\mathfrak{B}=[B_1,B_2,\ldots,B_r]$ of k-subsets of G such that the list

$$\Delta\mathfrak{B} := \bigcup_{i=1}^{r}[x-y : x,y \in B_i, x \neq y] = \underline{\lambda}(G \setminus N).$$

- The members of $\mathfrak{B}$ are called base blocks.
- When $N=\{0\}$, a relative difference family is simply called a difference family.
- When a (relative) difference family only contains one base block, it is often called a (relative) difference set.

References on strong difference families

M. Buratti in 1999 introduced the concept of strong difference families to establish systematic constructions for relative difference families.

- K.T. Arasu, A.K. Bhandari, S.L. Ma, and S. Sehgal, *Regular difference covers*, Kyungpook Math. J., 45 (2005), 137–152.
- M. Buratti, *Old and new designs via difference multisets and strong difference families*, J. Combin. Des., 7 (1999), 406–425.
- M. Buratti and L. Gionfriddo, *Strong difference families over arbitrary graphs*, J. Combin. Des., 16 (2008), 443–461.
- K. Momihara, *Strong difference families, difference covers, and their applications for relative difference families*, Des. Codes Cryptogr., 51 (2009), 253–273.

Paley strong difference families

Theorem [Buratti, JCD, 1999]

(1) Let p be an odd prime power. Then $\{0\} \cup \underline{2}\mathbb{F}_p^{\square}$ is an $(\mathbb{F}_p, p, p-1)$-SDF (called Paley difference multiset of the first type).

(2) Let $p \equiv 3 \pmod 4$ be a prime power. Then $\underline{2}(\{0\} \cup \mathbb{F}_p^{\square})$ is an $(\mathbb{F}_p, p+1, p+1)$-SDF (called Paley difference multiset of the second type).

(3) Let p be an odd prime power. Set $X_1 = \underline{2}(\{0\} \cup \mathbb{F}_p^{\square})$ and $X_2 = \underline{2}(\{0\} \cup \mathbb{F}_p^{\boxslash})$. Then $[X_1, X_2]$ is an $(\mathbb{F}_p, p+1, 2p+2)$-SDF (called Paley strong difference family of the third type).

Twin prime power and Singer difference multisets

Theorem [Buratti, JCD, 1999]

(4) Given twin prime powers $p > 2$ and $p+2$, the set $(\mathbb{F}_p^{\square} \times \mathbb{F}_{p+2}^{\square}) \cup (\mathbb{F}_p^{\not\square} \times \mathbb{F}_{p+2}^{\not\square}) \cup (\mathbb{F}_p \times \{0\})$ is a $(p(p+2), \frac{p(p+2)-1}{2}, \frac{p(p+2)-3}{4})$ difference set over $\mathbb{F}_p \times \mathbb{F}_{p+2}$. Let D be its complement. Then $\underline{2}D$ is a $(p(p+2), p(p+2)+1, p(p+2)+1)$ difference multiset (called twin prime power difference multiset).

(5) Given any prime power p and any integer $m \geq 3$, there is a $(\frac{p^m-1}{p-1}, \frac{p^{m-1}-1}{p-1}, \frac{p^{m-2}-1}{p-1})$ difference set over $\mathbb{Z}_{\frac{p^m-1}{p-1}}$. Let D be its complement. Then $\underline{p}D$ is a $(\frac{p^m-1}{p-1}, p^m, p^m(p-1))$ difference multiset (called Singer difference multiset).

Momihara's strong difference families of order 2

Theorem [Momihara, DCC, 2009]

There exists a cyclic $(2, k, k(k-1)n/2)$-SDF if and only if $k = p_1^{e_1} p_2^{e_2} \cdots p_r^{e^r}$ with p_i's distinct primes satisfies

- $(n = 1)$ k is a square;
- $(n = 2)$ e_i is even for every $p_i \equiv 3 \pmod 4$;
- $(n = 3)$ $k \not\equiv 2, 3 \pmod 4$ and $k \neq 4^a(8b+5)$ for any positive integers $a, b \geq 0$;
- $(n \geq 4)$ k is arbitrary when $n \equiv 0 \pmod 4$; $k \not\equiv 3 \pmod 4$ when $n \equiv 2 \pmod 4$; $k \equiv 0, 1, 4 \pmod 8$ when $n \equiv 1 \pmod 2$.

Momihara's asymptotic result

For given positive integers d and m, write

$$Q(d,m)=\frac{1}{4}(U+\sqrt{U^2+4d^{m-1}m})^2, \text{ where } U=\sum_{h=1}^{m}\binom{m}{h}(d-1)^h(h-1).$$

Theorem [Momihara, DCC, 2009]

If there exists a (G,k,μ)-SDF with $\mu=\lambda d$, then there exists a $(G\times\mathbb{F}_q, G\times\{0\}, k, \lambda)$-DF

- for any even λ and any prime power $q\equiv 1 \pmod d$ with $q>Q(d,k-1)$;
- for any odd λ and any prime power $q\equiv d+1 \pmod{2d}$ with $q>Q(d,k-1)$.

2-designs

Definition

A 2-(v, k, λ) design (also called (v, k, λ)-BIBD or balanced incomplete block design) is a pair $(V, \mathcal{B})$ where V is a set of v *points* and $\mathcal{B}$ is a collection of k-subsets of V (called *blocks*) such that every 2-subset of V is contained in exactly λ blocks of $\mathcal{B}$.

- A 2-(v, k, λ) design contains $\lambda\binom{v}{2}/\binom{k}{2}$ blocks.

Automorphisms

Definition

An automorphism α of a 2-design $(V, \mathcal{B})$ is a permutation on V leaving $\mathcal{B}$ invariant, i.e.,

$$\{\{\alpha(x) : x \in B\} : B \in \mathcal{B}\} = \mathcal{B}.$$

- A $(7, 3, 1)$-BIBD over Z_7: $\{0, 1, 3\} + i, 0 \leq i \leq 6$.

Definition

A design on v points is said to be cyclic or 1-rotational if it admits an automorphism consisting of a cycle of length v or $v - 1$, respectively.

2-designs from relative difference families

Proposition

- If there exist a (G, N, k, λ)-DF and a (cyclic) 2-$(|N|, k, \lambda)$ design, then there exists a (cyclic) 2-$(|G|, k, \lambda)$ design.
- If there exist a (G, N, k, λ)-DF and a (1-rotational) 2-$(|N|+1, k, \lambda)$ design, then there exists a (1-rotational) 2-$(|G|+1, k, \lambda)$ design.

- Relative difference families was implicitly used in many papers (for example, [S. Bagchi and B. Bagchi, JCTA, 1989]).
- The concept of relative difference families was initially put forward by M. Buratti [JCD, 1998].
- When G is cyclic, we say that the (g, n, k, λ)-DF is cyclic.

Basic Lemma [Costa, Feng, Wang, FFA, 2018]

Let $F = [F_1, F_2, \ldots, F_t]$ be a (G, k, μ)-SDF and let $\Phi = (\Phi_1, \Phi_2, \ldots, \Phi_t)$ be an ordered multiset of ordered k-subsets of $\mathbb{F}_q$ with $F_i = [f_{i,0}, f_{i,1}, \ldots, f_{i,k-1}]$ and $\Phi_i = (\phi_{i,0}, \phi_{i,1}, \ldots, \phi_{i,k-1})$ for $1 \leq i \leq t$. For each $h \in G$, the list

$$L_h = \bigcup_{i=1}^{t} [\phi_{i,a} - \phi_{i,b} : f_{i,a} - f_{i,b} = h; (a, b) \in I_k \times I_k; a \neq b]$$

has size μ. In the hypothesis that $q = en + 1$, $\mu = \lambda dn$ with d a divisor of e and $L_h = C_0^{e,q} \cdot D_h$ with D_h a λ-transversal of the cosets of $C_0^{d,q}$ in $\mathbb{F}_q^*$ for each $h \in G$, then there exists a $(G \times \mathbb{F}_q, G \times \{0\}, k, \lambda)$-DF.

Proof Let S be a 1-transversal for the cosets of $C_0^{e,q}$ in $C_0^{d,q}$, the required DF is $[\{(f_{i,0}, \phi_{i,0}s), (f_{i,1}, \phi_{i,1}s), \ldots, (f_{i,k-1}, \phi_{i,k-1}s)\} : 1 \leq i \leq t; s \in S]$.

A 2-$(694, 7, 2)$ design

Take $e = q - 1$. Then $C_0^{e,q} = \{1\}$ and $S = C_0^{d,q}$.

1. A $(\mathbb{Z}_{63}, 7, 2)$-SDF: $F_1 = [0, 4, 15, 23, 37, 58, 58]$, $F_2 = [0, 1, 3, 7, 13, 25, 39]$, $F_3 = [0, 1, 3, 11, 18, 34, 47]$.
2. A $(\mathbb{Z}_{63} \times \mathbb{F}_{11}, \mathbb{Z}_{63} \times \{0\}, 7, 1)$-DF:

$$B_1 = \{(0,0), (4,3), (15,5), (23,6), (37,8), (58,1), (58,10)\},$$
$$B_2 = \{(0,0), (1,2), (3,4), (7,6), (13,1), (25,10), (39,8)\},$$
$$B_3 = \{(0,0), (1,4), (3,7), (11,9), (18,2), (34,3), (47,5)\}.$$

Then

$$[B_i \cdot (1, s) : 1 \leq i \leq 3, s \in C_0^{2,11}]$$

forms a $(\mathbb{Z}_{63} \times \mathbb{F}_{11}, \mathbb{Z}_{63} \times \{0\}, 7, 1)$-DF.

- Input a 2-$(64, 7, 2)$ design which exists by Abel [JCD, 2000].

Other six new 2-designs

- Take $e = q - 1$. Then $C_0^{e,q} = \{1\}$ and $S = C_0^{d,q}$.

  $(\mathbb{Z}_{27}, 9, 8)$-SDF $\Longrightarrow$ a 2-$(459, 9, 4)$ design and a 2-$(783, 9, 4)$ design.

- Take $e = (q-1)/2$. Then $C_0^{e,q} = \{1, -1\}$.

  $(\mathbb{Z}_{45}, 9, 8)$-SDF $\Longrightarrow$ a 2-$(765, 9, 2)$ design and a 2-$(1845, 9, 2)$ design.

- Take $e = (q-1)/4$. Then $C_0^{e,q} = \{1, -1, \xi, -\xi\}$, where ξ is a primitive 4th root of unity in $\mathbb{F}_q$.

  $(\mathbb{Z}_{63}, 8, 8)$-SDF $\Longrightarrow$ a 2-$(1576, 8, 1)$ design;
  $(\mathbb{Z}_{81}, 9, 8)$-SDF $\Longrightarrow$ a 2-$(2025, 9, 1)$ design.

A 2-$(2025, 9, 1)$ design

1. A $(\mathbb{Z}_{81}, 9, 8)$-SDF: $F_1 = [0, 4, 4, -4, -4, 37, 37, -37, -37]$,
   $F_2 = F_3 = F_4 = F_5 = [0, 1, 4, 6, 17, 18, 38, 63, 72]$,
   $F_6 = F_7 = F_8 = F_9 = [0, 2, 7, 27, 30, 38, 53, 59, 69]$.
2. A $(\mathbb{Z}_{81} \times \mathbb{F}_{25}, \mathbb{Z}_{81} \times \{0\}, 9, 1)$-DF (let $\xi = \omega^6$):

$$
\begin{aligned}
B_1 &= \{(0,0), (4,1), (4,-1), (-4,\xi), (-4,-\xi), (37,\omega), (37,-\omega), (-37,\omega\xi), (-37,-\omega\xi)\},\\
B_2 &= \{(0,0), (1,1), (4,\omega), (6,\omega^2), (17,\omega^3), (18,\omega^4), (38,\omega^5), (63,\omega^7), (72,\omega^8)\},\\
B_6 &= \{(0,0), (2,1), (7,\omega^4), (27,\omega^{17}), (30,\omega^2), (38,\omega^{18}), (53,\omega^8), (59,\omega^{10}), (69,\omega^{14})\},\\
B_3 &= B_2 \cdot (1,-1), \qquad B_4 = B_2 \cdot (1,\xi), \qquad B_5 = B_2 \cdot (1,-\xi),\\
B_7 &= B_6 \cdot (1,-1), \qquad B_8 = B_6 \cdot (1,\xi), \qquad B_9 = B_6 \cdot (1,-\xi).
\end{aligned}
$$

Then $[B_i \cdot (1, s) : 1 \le i \le 9, s \in S]$ is a $(\mathbb{Z}_{81} \times \mathbb{F}_{25}, \mathbb{Z}_{81} \times \{0\}, k, 1)$-DF, where S is a representative system for the cosets of $C_0^{6,25} = \{1, -1, \xi, -\xi\}$ in $C_0^{2,25}$.

- Input a 2-$(81, 9, 1)$ design (affine plane of order 9).

Basic Lemma with Paley difference multisets

Let $p = 4m + 1$ be a prime power with $m = \lambda d$ and let q be a prime power satisfying $\lambda(q-1) \equiv 0 \pmod{p-1}$. Let δ be a generator of $C_0^{2,p}$ and ξ be a primitive 4th root of unity in $\mathbb{F}_q$.

- Apply Basic Lemma using the first type Paley $(\mathbb{F}_p, p, p-1)$-SDF whose only base block is $(f_0, f_1, \ldots, f_{p-1}) =$

$$(0, \delta^0, \delta^0, -\delta^0, -\delta^0, \ldots, \delta^{m-1}, \delta^{m-1}, -\delta^{m-1}, -\delta^{m-1})$$

  and a multiset $(\phi_0, \phi_1, \ldots, \phi_{p-1})$ on $\mathbb{F}_q$ of the form

$$(0, y_0, -y_0, \xi y_0, -\xi y_0, \ldots, y_{m-1}, -y_{m-1}, \xi y_{m-1}, -\xi y_{m-1}).$$

- Then there exists a $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p, \lambda)$-DF provided that each D_h, $h \in \mathbb{F}_p$, is a λ-transversal for the cosets of $C_0^{d,q}$ in $\mathbb{F}_q^*$.

Improved asymptotic results - I

Theorem 1

Let p and q be prime powers with $p = 4\lambda d + 1$ and $\lambda(q-1) \equiv 0 \pmod{p-1}$.

(1) There exists an $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p, \lambda)$-DF provided that $p \equiv 1, 5 \pmod{12}$ and $q > Q(d, p-4)$.

(2) There exists an $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p, \lambda)$-DF provided that p is a power of 9, $q > Q(d, p-4)$, and either $\lambda > 1$ or $1 - \xi \notin C_0^{d,q}$, where ξ is a primitive 4th root of unity in $\mathbb{F}_q$.

Corollary [Greig, JCMCC, 1998]

There exists a $(5q, 5, 5, 1)$-DF for any prime power $q \equiv 1 \pmod{4}$.

Improved asymptotic results - I

Theorem 1

Let p and q be prime powers with $p = 4\lambda d + 1$ and $\lambda(q-1) \equiv 0 \pmod{p-1}$.

(1) There exists an $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p, \lambda)$-DF provided that $p \equiv 1, 5 \pmod{12}$ and $q > Q(d, p-4)$.

(2) There exists an $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p, \lambda)$-DF provided that p is a power of 9, $q > Q(d, p-4)$, and either $\lambda > 1$ or $1 - \xi \notin C_0^{d,q}$, where ξ is a primitive 4th root of unity in $\mathbb{F}_q$.

Corollary

There exists an $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p, (p-1)/4)$-DF for any prime powers p and q with $p \equiv q \equiv 1 \pmod 4$ and $q \geq p$.

- The above corollary generalizes a result from Buratti [JCD, 1999], in which $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod{p-1}$.

Improved asymptotic results - I

Theorem 1

Let p and q be prime powers with $p = 4\lambda d + 1$ and $\lambda(q-1) \equiv 0 \pmod{p-1}$.

(1) There exists an $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p, \lambda)$-DF provided that $p \equiv 1, 5 \pmod{12}$ and $q > Q(d, p-4)$.

(2) There exists an $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p, \lambda)$-DF provided that p is a power of 9, $q > Q(d, p-4)$, and either $\lambda > 1$ or $1 - \xi \notin C_0^{d,q}$, where ξ is a primitive 4th root of unity in $\mathbb{F}_q$.

- By Momihara's Theorem with the first type Paley SDF, there is an $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p, 1)$-DF for any odd prime powers p and q with $q \equiv p \pmod{2(p-1)}$ and $q > Q(p-1, p-1)$. This means that for $p = 13$, we must have $q > Q(12, 12) = 7.94968 \times 10^{27}$.
- The above theorem shows that $q > Q(3, 9) = 9.68583 \times 10^{9}$.

New 2-designs with block size 13 or 17

Theorem 2

(1) There exists a 2-$(13q, 13, 1)$ design for all primes $q \equiv 1 \pmod{12}$ with 19 possible exceptions.

(2) There exists a 2-$(13q, 13, 3)$ design for all primes $q \equiv 1 \pmod{4}$ and $q > 9$.

(3) There exists a 2-$(17q, 17, 1)$ design for all primes $q \equiv 1 \pmod{16}$ and $q > Q(4, 13) = 3.44807 \times 10^{17}$.

(4) There exists a 2-$(17q, 17, 2)$ design for all primes $q \equiv 1 \pmod{8}$.

(5) There exists a 2-$(17q, 17, 4)$ design for all primes $q \equiv 1 \pmod{4}$ and $q > 13$.

- Remark: [Buratti, 1997, FFA]; [Buratti, 1999, DCC].

Improved asymptotic results - II

Theorem 3

Let $p = 2\lambda d + 1$ be a prime power. There exists an $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p, \lambda)$-DF for any prime power q with $\lambda(q-1) \equiv 0 \pmod{p-1}$ and $q > Q(d, p-2)$.

Theorem 4

Let $p = 2\lambda d - 1$ be a prime power and $p \equiv 3 \pmod 4$. There exists an $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p+1, \lambda)$-DF for any prime power q with $\lambda(q-1) \equiv 0 \pmod{p+1}$ and $q > Q(d, p)$.

Resolvable 2-designs

Definition

A 2-(v, k, λ) design $(V, \mathcal{B})$ is said to be resolvable if there exists a partition $\mathcal{R}$ of $\mathcal{B}$ (called a resolution) into parallel classes, each of which is a partition of V.

- Example: A resolvable 2-$(v, 2, 1)$ design is equivalent to a 1-factorization of the complete graph K_v.

Frame difference families

Definition

Let $\mathfrak{F}$ be a (g, n, k, λ)-DF over G relative to N. $\mathfrak{F}$ is a frame difference family if it can be partitioned into $\lambda n/(k-1)$ subfamilies $\mathfrak{F}_1, \mathfrak{F}_2, \ldots, \mathfrak{F}_{\lambda n/(k-1)}$ such that each $\mathfrak{F}_i$ has size of $(g-n)/(nk)$, and the union of base blocks in each $\mathfrak{F}_i$ is a system of representatives for the nontrivial cosets of N in G.

Proposition

If there exist a (G, N, k, λ)-FDF and a resolvable 2-$(|N|+1, k, \lambda)$ design, then there exists a resolvable 2-$(|G|+1, k, \lambda)$ design.

- When $\lambda n = k-1$, a (g, n, k, λ)-FDF is said to be elementary.

Partitioned difference families

Definition

Let $(G,+)$ be an abelian group of order g with a subgroup N of order n. A (G,N,K,λ) partitioned relative difference family $(PRDF)$ is a family $\mathfrak{B}=[B_1,B_2,\ldots,B_r]$ of G such that the elements of $\mathfrak{B}$ form a partition of $G\setminus N$, and the list

$$\Delta\mathfrak{B} := \bigcup_{i=1}^{r}[x-y : x,y\in B_i, x\neq y] = \underline{\lambda}(G\setminus N),$$

where K is the multiset $\{|B_i| : 1\leq i\leq r\}$.

- When $N=\{0\}$, a $(G,\{0\},K,\lambda)$-PRDF is called a partitioned difference family and simply written as a (G,K,λ)-PDF.
- A $(G,N,[k_1^{u_1}k_2^{u_2}\cdots k_l^{u_l}],\lambda)$-PRDF is a PRDF in which there are u_j base blocks of size k_j, $1\leq j\leq l$.

Applications

Proposition

If there exists an elementary $(G, N, k, 1)$-FDF with $|N| = k - 1$, then there exists a $(G, [(k-1)^1 k^s], k-1)$-PDF, where $s = (|G| - k + 1)/k$.

Proof Let $\mathfrak{F}$ be an elementary $(G, N, k, 1)$-FDF with $|N| = k - 1$. Then $\mathfrak{F}$ satisfies $\bigcup_{F \in \mathfrak{F}, h \in N} (F + h) = G \setminus N$. Set

$$\mathfrak{B} = \{F + h : F \in \mathfrak{F}, h \in N\} \cup \{N\}.$$

Then $\mathfrak{B}$ forms a $(G, [(k-1)^1 k^s], k-1)$-PDF, where $s = (|G| - k + 1)/k$.

Applications

Proposition [Costa, Feng, Wang, DCC, 2018]

If there exists an elementary $(g, k-1, k, 1)$-FDF, then there is an optimal $(g, g, g-k+1, [(k-1)^1 k^{q-1}])_q$-constant composition code, where $q = (g+1)/k$.

Proposition [Bao, Ji, IEEE IT, 2015]

Let k and v be positive integers satisfying $k+1|v-1$. Then there exists a strictly optimal frequency hopping sequences of length kv over an alphabet of size $(kv+1)/(k+1)$ if and only if there exists an elementary $(kv, k, k+1, 1)$-FDF over $\mathbb{Z}_{kv}$.

Basic Lemma for frame difference families

Let $q \equiv 1 \pmod{e}$ be a prime power and $d|e$. Let S be a representative system for the cosets of $C_0^{e,q}$ in $C_0^{d,q}$. Let $d(q-1) \equiv 0 \pmod{ek}$ and $t = d(q-1)/ek$. Suppose that there exists a $(G, k, kt\lambda)$-SDF $\mathfrak{S} = [F_1, F_2, \ldots, F_n]$, where $\lambda|G| \equiv 0 \pmod{k-1}$ and $F_i = (f_{i,0}, f_{i,1}, \ldots, f_{i,k-1})$, $1 \le i \le n$. If there exists a partition $\mathcal{P}$ of base blocks of $\mathfrak{S}$ into $\lambda|G|/(k-1)$ multisets, each of size t, such that one can choose appropriate multiset $[\Phi_1, \Phi_2, \ldots, \Phi_n]$ of ordered k-subsets of $\mathbb{F}_q^*$ with $\Phi_i = (\phi_{i,0}, \phi_{i,1}, \ldots, \phi_{i,k-1})$, $1 \le i \le n$, satisfying

(1) $\bigcup_{i=1}^{n}[\phi_{i,a} - \phi_{i,b} : f_{i,a} - f_{i,b} = h, (a,b) \in I_k \times I_k, a \neq b] = C_0^{e,q} \cdot D_h$ for each $h \in G$, where D_h is a λ-transversal for the cosets of $C_0^{d,q}$ in $\mathbb{F}_q^*$,

(2) $\bigcup_{i:F_i \in P}[\phi_{i,a} : a \in I_k] = C_0^{e,q} \cdot E_P$ for each $P \in \mathcal{P}$, where E_P is a representative system for the cosets of $C_0^{d,q}$ in $\mathbb{F}_q^*$,

then $\mathfrak{F} = [B_i \cdot \{(1,s)\} : 1 \le i \le n, s \in S]$ is a $(G \times \mathbb{F}_q, G \times \{0\}, k, \lambda)$-FDF, where $B_i = \{(f_{i,0}, \phi_{i,0}), (f_{i,1}, \phi_{i,1}), \ldots, (f_{i,k-1}, \phi_{i,k-1})\}$.

Eight new resolvable 2-designs

Theorem 5

There exists a resolvable 2-$(v, 8, 1)$ design for $v \in \{624, 1576, 2976, 5720, 5776, 10200, 14176, 24480\}$.

[Theorem, Handbook, Table 7.41]

Values of $v \equiv 8 \pmod{56}$ for which no resolvable 2-$(v, 8, 1)$ design is known.

176	624	736	1128	1240	1296	1408	1464	1520	1576
1744	2136	2416	2640	2920	2976	3256	3312	3424	3760
3872	4264	4432	5216	5720	5776	6224	6280	6448	6896
6952	7008	7456	7512	7792	7848	8016	9752	10200	10704
10760	10928	11040	11152	11376	11656	11712	11824	11936	12216
12328	12496	12552	12720	12832	12888	13000	13280	13616	13840
13896	14008	14176	14232	21904	24480				

A resolvable 2-$(624, 8, 1)$ design

Take $e = q - 1$. Then $C_0^{e,q} = \{1\}$ and $S = C_0^{d,q}$.

1. A $(\mathbb{Z}_7, 8, 8)$-SDF: $[0, 0, 1, 1, 2, 2, 4, 4]$.
2. An elementary $(\mathbb{Z}_7 \times \mathbb{F}_{89}, \mathbb{Z}_7 \times \{0\}, 8, 1)$-FDF:

$$B = \{(0, 1), (0, 20), (1, 14), (1, 58), (2, 18), (2, 61), (4, 26), (4, 73)\}.$$

Then

$$\mathfrak{F} = [B \cdot (1, s) : s \in C_0^{8,89}]$$

forms an elementary $(\mathbb{Z}_7 \times \mathbb{F}_{89}, \mathbb{Z}_7 \times \{0\}, 8, 1)$-FDF.

- Input a trivial resolvable 2-$(8, 8, 1)$ design.

New resolvable 2-designs

Theorem 6

If there exists a $(G, k, kt\lambda)$-SDF with $\lambda|G| \equiv 0 \pmod{k-1}$, then there exists a $(G \times \mathbb{F}_q, G \times \{0\}, k, \lambda)$-FDF

- for any even λ and any prime power $q \equiv 1 \pmod{kt}$ with $q > Q(kt, k)$;
- for any odd λ and any prime power $q \equiv krt + 1 \pmod{2krt}$ with $q > Q(krt, k)$, where r is any positive integer.

New resolvable 2-designs

Theorem 7

Let $p \equiv 3 \pmod 4$ be a prime power. Then there exists an elementary $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p+1, 1)$-FDF for any prime power $q \equiv 1 \pmod{p+1}$ and $q > Q((p+1)/2, p)$.

Theorem 8

Let p and $p+2$ be twin prime powers satisfying $p > 2$. Then there exists an elementary $(\mathbb{F}_p \times \mathbb{F}_{p+2} \times \mathbb{F}_q, \mathbb{F}_p \times \mathbb{F}_{p+2} \times \{0\}, p(p+2)+1, 1)$-FDF for any prime power $q \equiv 1 \pmod{p(p+2)+1}$ and $q > Q((p(p+2)+1)/2, p(p+2))$.

Theorem 9

Let $m \geq 3$ be an integer. Then there exists an elementary $(\mathbb{Z}_{2^m-1} \times \mathbb{F}_q, \mathbb{Z}_{2^m-1} \times \{0\}, 2^m, 1)$-FDF for any prime power $q \equiv 1 \pmod{2^m}$ and $q > Q(2^{m-1}, 2^m - 1)$.

New resolvable 2-designs

Theorem 10

Let $p \equiv 1 \pmod 4$ be a prime power. Then there exists an elementary $(\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p+1, 1)$-FDF for any prime power $q \equiv 1 \pmod{2p+2}$ and $q > Q(p+1, p)$.

Theorem [Buratti, Finizio, BICA, 2007]

There exists a $(\mathbb{Z}_p \times \mathbb{Z}_q, \mathbb{Z}_p \times \{0\}, p+1, 1)$-FDF for $p \in \{5, 7\}$ and any prime q.

Outline

[Chang, Costa, Feng, Wang, DM, 2019, submitted]

- Strong differences families with special patterns:
  1. A SDF has a pattern of length two.
  2. A SDF has a pattern of length four.
- Applications to GDDs and OOCs.

A SDF has a pattern of length two

Definition

Let $(G,+)$ be an abelian group. A (G,k,μ)-SDF has a pattern of length two if it is the union of three families Σ_1, Σ_2 and Σ_3, each of which could be empty, where

1) if $k \equiv 0 \pmod 2$, then for any $A \in \Sigma_1$, A is of the form

$$[x_1, \delta + x_1, x_2, \delta + x_2, \ldots, x_{\lfloor k/2 \rfloor}, \delta + x_{\lfloor k/2 \rfloor}]$$

(resp. with a 0 at the beginning if $k \equiv 1 \pmod 2$), where δ is either an involution of G or zero, and $\Delta[x_1, x_2, \ldots, x_{\lfloor k/2 \rfloor}]$ does not contain involutions and zeros;

2) for any $A \in \Sigma_2$, each element of $\Delta(A)$ is either an involution or zero;

3) for any $A \in \Sigma_3$, the multiplicity of A in Σ_3 is even and $\Delta(A)$ does not contain involutions and zeros.

Strong differences families

Example 1

The $(\mathbb{Z}_{10}, 5, 12)$-SDF given below has a pattern of length two:

Σ_1	Σ_2	Σ_3
$[[0,3,3,7,7]]$	$[[0,0,0,5,5]]$	$[[0,9,6,7,8],\ [0,9,6,7,8],$ $[0,8,4,6,7],\ [0,8,4,6,7]]$

Lemma [Paley SDFs]

(1) Let p be an odd prime power. Then the $(p, p, p-1)$-SDF over $\mathbb{F}_p$ given by the single block $\{0\} \cup \underline{2}C_0^{2,p}$, has a pattern of length two.

(2) Let $p \equiv 3 \pmod 4$ be a prime power. Then the $(p, p+1, p+1)$-SDF over $\mathbb{F}_p$ given by the single block $\underline{2}(\{0\} \cup C_0^{2,p})$, has a pattern of length two.

$(\mathbb{Z}_{10} \times \mathbb{F}_q, \mathbb{Z}_{10} \times \{0\}, 5, 1)$-DF

Example 2

Given any prime power $q \equiv 1 \pmod{12}$ and $q > Q(6, 4)$, there exists a $(\mathbb{Z}_{10} \times \mathbb{F}_q, \mathbb{Z}_{10} \times \{0\}, 5, 1)$-DF.

Proof Take the $(\mathbb{Z}_{10}, 5, 12)$-SDF, $\Sigma = [A_1, A_2, \ldots, A_6]$, where $A_1 = [0, 3, 3, 7, 7]$, $A_2 = [0, 0, 0, 5, 5]$, $A_3 = A_4 = [0, 9, 6, 7, 8]$ and $A_5 = A_6 = [0, 8, 4, 6, 7]$. Now, consider the family $\mathcal{B} = [B_1, B_2, \ldots, B_6]$ of base blocks whose first components come from Σ, where

$$B_1 = \{(0,0), (3, y_{1,1}), (3, -y_{1,1}), (7, y_{1,2}), (7, -y_{1,2})\};$$
$$B_2 = \{(0, y_{2,1}), (0, y_{2,2}), (0, y_{2,3}), (5, y_{2,4}), (5, y_{2,5})\};$$
$$B_3 = \{(0, y_{3,1}), (9, y_{3,2}), (6, y_{3,3}), (7, y_{3,4}), (8, y_{3,5})\}; \quad B_4 = (1, -1) \cdot B_3;$$
$$B_5 = \{(0, y_{4,1}), (8, y_{4,2}), (4, y_{4,3}), (6, y_{4,4}), (7, y_{4,5})\}; \quad B_6 = (1, -1) \cdot B_5.$$

$(\mathbb{Z}_{10} \times \mathbb{F}_q, \mathbb{Z}_{10} \times \{0\}, 5, 1)$-DF (Cont.)

One can check that

$$\Delta[B_1, B_2, \ldots, B_6] = \bigcup_{g \in \mathbb{Z}_{10}} \{g\} \times D_g,$$

where $D_g = \{1, -1\} \cdot L_g$, $L_g = L_{-g}$ and

$$\begin{aligned}
L_0 &= \{2y_{1,1}, 2y_{1,2}, y_{2,1} - y_{2,2}, y_{2,1} - y_{2,3}, y_{2,3} - y_{2,2}, y_{2,4} - y_{2,5}\};\\
L_1 &= \{y_{3,2} - y_{3,1}, y_{3,2} - y_{3,5}, y_{3,5} - y_{3,4}, y_{3,4} - y_{3,3}, y_{4,2} - y_{4,5}, y_{4,5} - y_{4,4}\};\\
L_2 &= \{y_{3,1} - y_{3,5}, y_{3,5} - y_{3,3}, y_{3,2} - y_{3,4}, y_{4,1} - y_{4,2}, y_{4,2} - y_{4,4}, y_{4,4} - y_{4,3}\};\\
L_3 &= \{y_{1,1}, y_{1,2}, y_{3,4} - y_{3,1}, y_{3,2} - y_{3,3}, y_{4,1} - y_{4,5}, y_{4,5} - y_{4,3}\};\\
L_4 &= \{y_{1,2} - y_{1,1}, y_{1,2} + y_{1,1}, y_{4,4} - y_{4,1}, y_{4,1} - y_{4,3}, y_{4,3} - y_{4,2}, y_{3,3} - y_{3,1}\};\\
L_5 &= \{y_{2,4} - y_{2,1}, y_{2,4} - y_{2,2}, y_{2,4} - y_{2,3}, y_{2,5} - y_{2,1}, y_{2,5} - y_{2,2}, y_{2,5} - y_{2,3}\}.
\end{aligned}$$

For any prime power $q \equiv 1 \pmod{12}$ and $q > Q(6, 4)$, we can always require that every L_g is a system of representatives for $C_0^{6,q}$ in $\mathbb{F}_q^*$.

Therefore, given a transversal S for $\{1, -1\}$ in $C_0^{6,q}$, the family $[B \cdot (1, s) \mid s \in S,\ B \in \mathcal{B}]$ is a $(\mathbb{Z}_{10} \times \mathbb{F}_q, \mathbb{Z}_{10} \times \{0\}, 5, 1)$-DF.

Asymptotic results - III

Theorem 11

If there exists a (G, k, μ)-SDF with a pattern of length two, then there exists a $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-DF for any prime power $q \equiv 1 \pmod{\mu}$ and $q > Q(\mu/2, k-1)$.

- Let k be odd and Σ be a (G, k, μ)-SDF with a pattern of length two. If Σ consists only of base blocks belonging to Σ_1, then the lower bound on q can be improved. That is to say, there exists a $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-DF for any prime power $q \equiv 1 \pmod{\mu}$ and $q > Q(\mu/2, k-2)$.

SDFs with a pattern of length two

$(\mathbb{Z}_2, 5, 20)$-SDF	$\Sigma_2 = [[0,0,0,1,1],[0,0,0,0,1]]$
$(\mathbb{Z}_{12}, 5, 20)$-SDF	$\Sigma_2 = [[0,0,0,6,6],[0,0,0,0,6]]$ $\Sigma_3 = \underline{2}\ [[0,1,2,3,4],[0,1,2,4,5],[0,1,3,5,8],[0,1,4,5,8],[0,2,4,7,9]]$
$(\mathbb{Z}_{25}, 6, 6)$-SDF	$\Sigma_1 = [[0,0,5,5,14,14]]$ $\Sigma_3 = \underline{2}\ [[0,1,2,3,6,18],[0,2,8,12,15,19]]$
$(\mathbb{Z}_{30}, 6, 6)$-SDF	$\Sigma_1 = [[0,0,6,6,16,16],[0,15,3,18,7,22]]$ $\Sigma_3 = \underline{2}\ [[0,1,2,3,8,21],[0,2,5,9,13,18]]$
$(\mathbb{Z}_{35}, 6, 6)$-SDF	$\Sigma_1 = [[0,0,8,8,18,18]]$ $\Sigma_3 = \underline{2}\ [[0,1,2,3,5,15],[0,3,7,14,23,29],[0,4,9,17,23,28]]$
$(\mathbb{Z}_{45}, 6, 6)$-SDF	$\Sigma_1 = [[0,0,10,10,26,26]]$ $\Sigma_3 = \underline{2}\ [[0,1,3,11,17,31],[0,4,9,22,30,37],$ $[0,1,3,7,12,25],[0,1,3,7,12,25]]$
$(\mathbb{Z}_5, 6, 12)$-SDF	$\Sigma_1 = [[0,0,1,1,2,2],[0,0,2,2,4,4]]$
$(\mathbb{Z}_{15}, 6, 12)$-SDF	$\Sigma_1 = [[0,0,3,3,8,8],[0,0,4,4,9,9]]$ $\Sigma_3 = \underline{2}\ [[0,1,2,3,4,7],[0,1,2,4,8,10]]$
$(\mathbb{Z}_{35}, 7, 6)$-SDF	$\Sigma_1 = [[0,7,7,17,17,30,30]]$ $\Sigma_3 = \underline{2}\ [[0,1,2,3,5,21,29],[0,3,9,13,17,24,29]]$
$(\mathbb{Z}_{49}, 7, 6)$-SDF	$\Sigma_1 = [[0,4,4,16,16,36,36]]$ $\Sigma_3 = \underline{2}\ [0,1,3,20,28,38,43],[0,1,3,27,31,36,42],[0,1,3,27,31,36,42]]$
$(\mathbb{Z}_{21}, 7, 12)$-SDF	$\Sigma_1 = [[0,5,5,10,10,17,17],[0,3,3,9,9,17,17]]$ $\Sigma_3 = \underline{2}\ [[0,1,2,3,4,5,11],(0,1,3,7,11,13,16]]$

New relative difference families

Theorem 12

Let q be a prime. Then there exists a $(\mathbb{Z}_h \times \mathbb{F}_q, \mathbb{Z}_h \times \{0\}, k, 1)$-DF in the following cases:

(hq, h, k, λ)	possible exceptions / definite ones
$(2q, 2, 5, 1)$: $q \equiv 1 \pmod{20}$	
$(10q, 10, 5, 1)$: $q \equiv 1 \pmod{12}$	
$(12q, 12, 5, 1)$: $q \equiv 1 \pmod{20}$	
$(hq, h, 6, 1)$: $h \in \{25, 30, 35, 45\}$, $q \equiv 1 \pmod{6}$	$(25 \times 7, 25, 6, 1)$
$(hq, h, 6, 1)$: $h \in \{5, 15\}$, $q \equiv 1 \pmod{12}$	$(5 \times 13, 5, 6, 1)$
$(hq, h, 7, 1)$: $h \in \{35, 49\}$, $q \equiv 1 \pmod{6}$	$(35 \times 7, 35, 7, 1)$, $(49 \times 7, 49, 7, 1)$
$(21q, 21, 7, 1)$: $q \equiv 1 \pmod{12}$	

A SDF has a pattern of length four

Definition

Let $(G,+)$ be an abelian group of odd order. A (G,k,μ)-SDF has a pattern of length four if $k \equiv 0,1 \pmod 4$ and it is the union of two families Σ_1 and Σ_2 (Σ_2 could be empty), where

1) if $k \equiv 0 \pmod 4$, then Σ_1 consists of only one base block of the form

$$[x_1, x_1, -x_1, -x_1, \ldots, x_{\lfloor k/4 \rfloor}, x_{\lfloor k/4 \rfloor}, -x_{\lfloor k/4 \rfloor}, -x_{\lfloor k/4 \rfloor}]$$

(resp. with a 0 at the beginning if $k \equiv 1 \pmod 4$) and $\Delta[x_1, -x_1, x_2, -x_2, \ldots, x_{\lfloor k/4 \rfloor}, -x_{\lfloor k/4 \rfloor}]$ does not contain zeros;

2) for any $A \in \Sigma_2$, the multiplicity of A in Σ_2 is doubly even and $\Delta(A)$ does not contain zeros.

- For a (G,k,μ)-SDF, Σ, with a pattern of length four, the zero element of G must appear $\lfloor k/4 \rfloor \times 4$ times in $\Delta\Sigma$, so $\mu = 4\lfloor k/4 \rfloor$.

Strong differences families

Example 3

The $(\mathbb{Z}_{45}, 5, 4)$-SDF given below has a pattern of length four:

Σ_1	Σ_2
$[[0, 1, 1, -1, -1]]$	$[[0, 3, 7, 13, 30], [0, 3, 7, 13, 30], [0, 3, 7, 13, 30], [0, 3, 7, 13, 30], [0, 5, 14, 26, 34], [0, 5, 14, 26, 34], [0, 5, 14, 26, 34], [0, 5, 14, 26, 34]]$

Lemma [Paley SDFs]

Let $p \equiv 1 \pmod 4$ be an odd prime power. Then the $(p, p, p-1)$-SDF over $\mathbb{F}_p$ given by the single block $\{0\} \cup \underline{2}C_0^{2,p}$, has a pattern of length four.

$(\mathbb{Z}_{45} \times \mathbb{F}_q, \mathbb{Z}_{45} \times \{0\}, 5, 1)$-DF

Example 4

Given any prime power $q \equiv 1 \pmod 4$, there exists a $(\mathbb{Z}_{45} \times \mathbb{F}_q, \mathbb{Z}_{45} \times \{0\}, 5, 1)$-DF.

Proof Take the $(\mathbb{Z}_{45}, 5, 4)$-SDF, $\Sigma = [A_1, A_2, \ldots, A_9]$, where $A_1 = [0, 1, 1, -1, -1]$, $A_2 = A_3 = A_4 = A_5 = [0, 3, 7, 13, 30]$ and $A_6 = A_7 = A_8 = A_9 = [0, 5, 14, 26, 34]$. Let ξ be a primitive 4th root of unity in $\mathbb{F}_q^*$. Now, consider the family $\mathcal{B} = [B_1, B_2, \ldots, B_9]$ of base blocks whose first components come from Σ, where

$$
\begin{aligned}
&B_1 = \{(0,0), (1, y_{1,1}), (1, -y_{1,1}), (-1, y_{1,1}\xi), (-1, -y_{1,1}\xi)\};\\
&B_2 = \{(0, y_{2,1}), (3, y_{2,2}), (7, y_{2,3}), (13, y_{2,4}), (30, y_{2,5})\};\\
&B_3 = (1, \xi) \cdot B_2; \qquad B_4 = (1, -1) \cdot B_2; \qquad B_5 = (1, -\xi) \cdot B_2;\\
&B_6 = \{(0, y_{6,1}), (5, y_{6,2}), (14, y_{6,3}), (26, y_{6,4}), (34, y_{6,5})\};\\
&B_7 = (1, \xi) \cdot B_6; \qquad B_8 = (1, -1) \cdot B_6; \qquad B_9 = (1, -\xi) \cdot B_6.
\end{aligned}
$$

$(\mathbb{Z}_{45} \times \mathbb{F}_q, \mathbb{Z}_{45} \times \{0\}, 5, 1)$-DF (cont.)

One can check that

$$\Delta[B_1, B_2, \ldots, B_9] = \bigcup_{g \in \mathbb{Z}_{45}} \{g\} \times D_g,$$

where $D_g = \{1, -1, \xi, -\xi\} \cdot L_g$ and $|L_g| = 1$ for any $g \in \mathbb{Z}_{45}$. For any prime power $q \equiv 1 \pmod 4$, we can always require that each L_g does not contain zero. Therefore, given a transversal S for $\{1, -1, \xi, -\xi\}$ in F_q^*, the family $[B \cdot (1, s) \mid s \in S,\ B \in \mathcal{B}]$ is a $(\mathbb{Z}_{45} \times \mathbb{F}_q, \mathbb{Z}_{45} \times \{0\}, 5, 1)$-DF.

Asymptotic results - IV

Theorem 13

If there exists a (G, k, μ)-SDF with a pattern of length four, whose distinguished base block is denoted by A, then for any prime power $q \equiv 1 \pmod{\mu}$ and $q > Q(\mu/4, k-1)$, there exists a $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-DF in the following cases

1) $k \equiv 0 \pmod 4$;
2) $k = 5$;
3) $k \in \{9, 13, 17\}$ and $x_1 \neq \pm 2x_2$ for any nonzero $x_1, x_2 \in A$ (x_1 could be x_2);
4) $k \equiv 1 \pmod 4$, $k \geq 21$ and $3x \neq 0$ for any nonzero $x \in A$.

- Let Σ be a (G, k, μ)-SDF with a pattern of length four. If $\Sigma = \Sigma_1$, then the lower bound on q can be improved, that is to say, $q > Q(\mu/4, k-3)$ when $k \equiv 0 \pmod 4$ and $q > Q(\mu/4, k-4)$ when $k \equiv 1 \pmod 4$).

New relative difference families

SDFs with a pattern of length four

$(\mathbb{Z}_{63}, 8, 8)$-SDF	$\Sigma_1 = [[20, 20, -20, -20, 29, 29, -29, -29]]$ $\Sigma_2 = \underline{4}\ [[0, 1, 3, 7, 19, 34, 42, 53], [0, 1, 4, 6, 26, 36, 43, 51]]$
$(\mathbb{Z}_{81}, 9, 8)$-SDF	$\Sigma_1 = [[0, 4, 4, -4, -4, 37, 37, -37, -37]]$ $\Sigma_2 = \underline{4}\ [[0, 1, 4, 6, 17, 18, 38, 63, 72], [0, 2, 7, 27, 30, 38, 53, 59, 69]]$

Theorem 14

Let q be a prime. Then there exists a $(\mathbb{Z}_h \times \mathbb{F}_q, \mathbb{Z}_h \times \{0\}, k, \lambda)$-DF in the following cases:

(hq, h, k, λ)	possible exceptions
$(45q, 45, 5, 1)$-DF: $q \equiv 1 \pmod 4$	
$(63q, 63, 8, 1)$-DF: $q \equiv 1 \pmod 8$	$(63 \times 17, 63, 8, 1)$
$(81q, 81, 9, 1)$-DF: $q \equiv 1 \pmod 8$	$(81 \times 17, 81, 9, 1)$, $(81 \times 41, 81, 9, 1)$

Group divisible designs

Definition

Group divisible designs are closely related to difference families. Let K be a set of positive integers. A group divisible design (GDD) K-GDD is a triple $(X, \mathcal{G}, \mathcal{A})$ satisfying the following properties: (1) $\mathcal{G}$ is a partition of a finite set X into subsets (called groups); (2) $\mathcal{A}$ is a set of subsets of X (called blocks), whose cardinalities are from K, such that every 2-subset of X is either contained in exactly one block or in exactly one group, but not in both.

- If $\mathcal{G}$ contains u_i groups of size g_i for $1 \leq i \leq r$, then $g_1^{u_1} g_2^{u_2} \cdots g_r^{u_r}$ is called the type of the GDD.
- The notation k-GDD is used when $K = \{k\}$.

New group divisible designs

[Theorem 12]

A $(\mathbb{Z}_{30} \times \mathbb{F}_q, \mathbb{Z}_{30} \times \{0\}, 6, 1)$-DF for any prime $q \equiv 1 \pmod 6$.

Lemma [Handbook, Table 3.18]

It is reported that when $u < 100$, a 6-GDD of type 30^u exists for $u \in \{6, 16, 21, 26, 31, 36, 41, 51, 61, 66, 71, 76, 78, 81, 86, 90, 91, 96\}$.

Theorem 15

There exists a 6-GDD of type 30^u for $u \in \{6, 16, 21, 25, 26, 36, 41, 42, 48, 49, 51, 66, 71, 76, 78, 81, 84, 85, 86, 90, 91, 96\} \cup \{q : q \equiv 1 \pmod 6 \text{ is a prime}\}$.

Optical orthogonal codes

- A $(v, k, 1)$-optical orthogonal code (OOC) is defined as a set of k-subsets (called codewords) of $\mathbb{Z}_v$ whose list of differences does not contain repeated elements.
- It is optimal if the size of the set of missing differences is less than or equal to $k(k-1)$.
- A cyclic $(gv, g, k, 1)$-DF can be seen as a $(gv, k, 1)$-OOC whose set of missing differences is $\{0, v, 2v, \ldots, (g-1)v\}$.
- Furthermore, one can construct a $(g, k, 1)$-OOC on the set of missing differences to produce a new $(gv, k, 1)$-OOC.

New optimal optical orthogonal codes

Theorem 16

(1) There exist an optimal $(2q, 5, 1)$-OOC and an optimal $(12q, 5, 1)$-OOC for any prime $q \equiv 1 \pmod{20}$.

(2) There exists an optimal $(gq, k, 1)$-OOC where $(g, k) \in \{(10, 5), (5, 6), (15, 6), (21, 7)\}$ for any prime $q \equiv 1 \pmod{12}$ except for $(g, q, k) = (5, 13, 6)$.

(3) There exists an optimal $(gq, k, 1)$-OOC where $(g, k) \in \{(25, 6), (30, 6), (35, 6), (45, 6), (35, 7), (49, 7)\}$ for any prime $q \equiv 1 \pmod{6}$ except for $(g, q, k) \in \{(25, 7, 6), (35, 7, 7), (49, 7, 7)\}$.

(4) There exists an optimal $(45q, 5, 1)$-OOC for any prime $q \equiv 1 \pmod{4}$ and $q > 5$.

(5) There exists an optimal $(63q, 8, 1)$-OOC for any prime $q \equiv 1 \pmod{8}$ and $q > 17$.

Open problems [Buratti, 1999, JCD]

Problem A

Given a positive integer k, determine the numbers

$$t_k = \min\{t | \text{ there exists a } (k, k, \mu)\text{-SDF with } t \text{ base blocks for some integer } \mu\}.$$

$$t'_k = \min\{t | \text{ there exists a } (k-1, k, \mu)\text{-SDF with } t \text{ base blocks for some integer } \mu\}.$$

- $\surd$ The existence of $(k, k, k(k-1))$-SDF $\Longrightarrow t_k \leq k$.
- $\surd$ The existence of $(k-1, k, k(k+1))$-SDF $\Longrightarrow t'_k \leq k+1$.

Open problem [Buratti, 1999, JCD]

Problem B

Determine the sets:

$$S = \{k \in N | \text{there exists a } (k, k, k-1)\text{-SDF}\}.$$

$$S' = \{k \in N | \text{there exists a } (k-1, k, k)\text{-SDF}\}.$$

- S contains the set of odd prime powers.
- S' contains the set $\{q+1 | q \text{ prime power} \equiv 3 \pmod 4\}$, the set $\{pq+1 | p \text{ and } q \text{ twin prime powers}\}$ and the powers of 2.

Thank you!