Tiling groups with difference sets

Ante Ćustić
Department of Mathematics
Simon Fraser University
250-13450 102nd Avenue
Surrey, British Columbia, Canada V3T 0A3
acustic@sfu.ca

Vedran Krčadinac[*]
Department of Mathematics
Faculty of Science
University of Zagreb
Bijenička 30, HR-10000 Zagreb, Croatia
vedran.krcadinac@math.hr

Yue Zhou[†]
Faculty of Mathematics
Otto-von-Guericke University
Universitaetsplatz 2, D-39106 Magdeburg, Germany
and
College of Science
National University of Defense Technology
Changsha 410073, China
yue.zhou.ovgu@gmail.com

Submitted: Apr 2, 2015; Accepted: Jun 2, 2015; Published: 22 Jun, 2015
Mathematics Subject Classifications: 05B10

Abstract

We study tilings of groups with mutually disjoint difference sets. Some necessary existence conditions are proved and shown not to be sufficient. In the case of tilings with two difference sets we show the equivalence to skew Hadamard difference sets, and prove that they must be normalized if the group is abelian. Furthermore, we present some constructions of tilings based on cyclotomy and investigate tilings consisting of Singer difference sets.

Keywords: difference set; tiling

1 Introduction

Let G be an additively written group of order v. A (v, k, λ) *difference set* in G is a k-subset $D \subseteq G$ such that every nonzero element of G can be expressed as a difference $x - y$

[*] Partially supported by the Croatian Science Foundation under project 1637 and by the European Science Foundation under COST Action IC1104.

[†] Partially supported by the National Natural Science Foundation of China (No. 11401579).

with $x, y \in D$ in exactly λ ways. Multiplicative notation is sometimes used, in which case the "differences" are written as xy^{-1}. For basic results on difference sets, see [2, 17, 22]. More recent surveys on difference sets are [14] and [26].

It is not possible to partition the whole group G into disjoint (v, k, λ) difference sets. This follows from the necessary existence condition $\lambda(v-1) = k(k-1)$ when $v > k > \lambda \geqslant 1$, which is assumed throughout the paper. However, if k divides $v - 1$, it may be possible to partition $G \setminus \{0\}$ into difference sets. We introduce the following concept.

Definition 1. Let G be a finite group of order v with identity element 0. A (v, k, λ) *tiling* of G is a collection $\{D_1, \dots, D_t\}$ of mutually disjoint (v, k, λ) difference sets such that $D_1 \cup \dots \cup D_t = G \setminus \{0\}$.

Example 2. The following five difference sets are a $(31, 6, 1)$ tiling of the cyclic group $\mathbb{Z}_{31}$:

$$\begin{aligned} D_1 &= \{1, 5, 11, 24, 25, 27\}, \\ D_2 &= \{2, 10, 17, 19, 22, 23\}, \\ D_3 &= \{3, 4, 7, 13, 15, 20\}, \\ D_4 &= \{6, 8, 9, 14, 26, 30\}, \\ D_5 &= \{12, 16, 18, 21, 28, 29\}. \end{aligned}$$

Tilings of cyclic groups have a nice combinatorial interpretation. We can visualize the group $\mathbb{Z}_v$ as a necklace of v beads, with the identity element coloured in black. A (v, k, λ) tiling corresponds to a colouring of the remaining beads with t colours, such that there are k beads of every colour. Furthermore, there are exactly λ pairs of equally coloured beads at each possible distance, and for every colour. Here, a pair of beads is thought to have two distances, counted clockwise and counterclockwise. The $(31, 6, 1)$ tiling of Example 2 can be represented as the necklace in Figure 1.

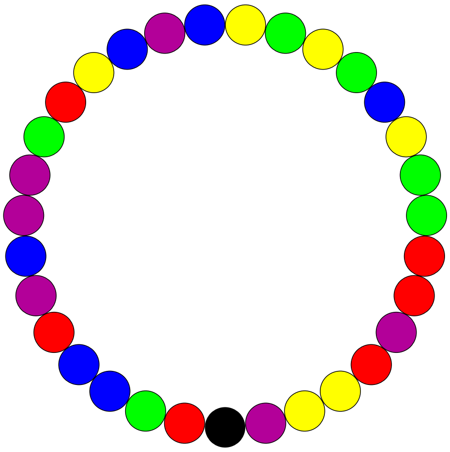

Figure 1: A $(31, 6, 1)$ tiling of $\mathbb{Z}_{31}$.

Mutually disjoint difference sets have been used to design hopping sequences for multichannel wireless networks [13]. Multiple users are assumed to communicate over a number of channels, without synchronization or a common control channel. Every user utilizes the same channel selection strategy, i.e. hopping sequence. Sequences based on difference sets ensure a high rendezvous probability. The difference sets correspond to different channels; they need to be disjoint to ensure that each time slot is assigned a single channel. A (v, k, λ) tiling of G is the extremal case, maximizing the number of channels for a given sequence length v. See also [25] for this application.

A similar concept studied earlier are *partitioned difference families* (PDFs); see [3, 27]. A (v, k, λ) tiling with t difference sets can be seen as a $(v, [k^t, 1^1], k-1)$-PDF. A more general concept are *disjoint difference families*; see [7, 10, 24]. Quite recently, Gnilke, Greferath and Pavčević [11] defined structures called *mosaics of combinatorial designs*. The simultaneous development of the t difference sets forming a (v, k, λ) tiling of G is a $(t+1)$-mosaic of symmetric designs with parameters

$$\underbrace{2\text{-}(v,k,\lambda) \oplus \cdots \oplus 2\text{-}(v,k,\lambda)}_{t \text{ times}} \oplus 2\text{-}(v,1,0).$$

The layout of our paper is as follows. In Section 2, we prove necessary conditions for the existence of (v, k, λ) tilings and consider small examples. Nonexistence of tilings for some parameter triples satisfying the necessary conditions is proved. In Section 3, tilings consisting of two difference sets are shown to be equivalent to the so-called skew Hadamard difference sets. Constructions of general tilings based on cyclotomy are considered in Section 4, and based on Singer difference sets in Section 5.

2 Necessary existence conditions and small examples

As already mentioned in the introduction, a necessary condition for the existence of (v, k, λ) difference sets in a group G of order v is $\lambda(v-1) = k(k-1)$. From this, the number t of difference sets in a (v, k, λ) tiling of G can be expressed as $t = (v-1)/k = (k-1)/\lambda$ and we have the following existence condition for tilings.

Proposition 3. *If a (v, k, λ) tiling of a group G exists, then k divides $v-1$ and λ divides $k-1$.*

An immediate consequence is that v and k are relatively prime (since v and $v-1 = t \cdot k$ are relatively prime).

The condition $\lambda(v-1) = k(k-1)$ is not sufficient for the existence of difference sets; many non-trivial nonexistence results are known. In this paper the existence of (v, k, λ) difference sets is taken for granted, in the sense that only parameter triples satisfying Proposition 3 for which there is at least one difference set are considered admissible for (v, k, λ) tilings. We shall soon see that these two conditions are not sufficient for the existence of (v, k, λ) tilings.

If D is a (v,k,λ) difference set in G, the translates of D (i.e. the sets $D+x$, $x \in G$) are also difference sets. The set of all translates of D forms a symmetric (v,k,λ) block design with the point set G. Since every two blocks of a symmetric design intersect in λ points, the difference sets forming a (v,k,λ) tiling of G cannot be translates of each other. Using this observation we can prove nonexistence of tilings for some admissible parameters.

Proposition 4. *A* $(21,5,1)$ *tiling of the cyclic group of order* 21 *does not exist.*

Proof. From the multiplier theorem [2, Theorem VI.2.11] and [2, Lemma VI.2.5] it follows that there are only two $(21,5,1)$ difference sets up to translation: $\{3,6,7,12,14\}$ and $\{7,9,14,15,18\}$. According to the observation above, a $(21,5,1)$ tiling of $\mathbb{Z}_{21}$ would require four difference sets not being translates of each other. □

Now consider $(57,8,1)$ tilings of the group $\mathbb{Z}_{57}$. As before, one can see that there are 12 cyclic $(57,8,1)$ difference sets up to translation. Seven disjoint difference sets are required for a $(57,8,1)$ tiling, so nonexistence of tilings does not follow immediately. We set up a computer search using backtracking and found that there can be at most 5 mutually disjoint cyclic $(57,8,1)$ difference sets, thus proving the following result.

Proposition 5. *A* $(57,8,1)$ *tiling of the cyclic group of order* 57 *does not exist.*

Surprisingly, the non-abelian group of order 57 can be tiled with difference sets. The next example was also found by computer search.

Example 6. Let $G = \langle a,b \mid a^3 = b^{19} = 1,\ ab^7 = ba\rangle$ be the non-abelian group of order 57. The following seven difference sets are a $(57,8,1)$ tiling of G:

$$\begin{aligned}
D_1 &= \{a, b, a^2, b^2, ab^4, ab^{10}, b^{13}, b^{18}\},\\
D_2 &= \{ab, ab^5, a^2b^6, a^2b^{13}, b^{15}, a^2b^{14}, ab^{15}, ab^{18}\},\\
D_3 &= \{a^2b, a^2b^7, a^2b^8, ab^9, ab^{12}, b^{14}, ab^{14}, a^2b^{16}\},\\
D_4 &= \{ab^2, b^4, a^2b^3, b^9, a^2b^9, b^{11}, b^{12}, a^2b^{18}\},\\
D_5 &= \{b^3, a^2b^2, b^5, b^8, a^2b^{10}, a^2b^{11}, ab^{17}, a^2b^{17}\},\\
D_6 &= \{ab^3, b^6, ab^6, ab^8, b^{10}, b^{16}, a^2b^{15}, b^{17}\},\\
D_7 &= \{a^2b^4, a^2b^5, b^7, ab^7, ab^{11}, a^2b^{12}, ab^{13}, ab^{16}\}.
\end{aligned}$$

Using our backtracking program we examined all admissible groups of order $v \leqslant 50$. Tilings exist in 11 of the 18 cases, and in 7 cases there are no tilings. The results are summarized in Table 1. Please note that the table contains only parameters (v,k,λ) satisfying Proposition 3 and only groups G with at least one (v,k,λ) difference set. For example, the parameters $(49,16,5)$ and the groups $\mathbb{Z}_{49}$ and $\mathbb{Z}_7 \times \mathbb{Z}_7$ are not included because by [17, Theorem 4.38 and Corollary 4.42] there are no $(49,16,5)$ difference sets.

A difference set in an abelian group is said to be *normalized* provided the sum of its elements is 0. The $(31,6,1)$ tiling of Example 2 is composed of normalized difference sets, and so are all tilings of abelian groups we found. Therefore we make the following conjecture.

(v,k,λ)	Group	Tiling
$(7,3,1)$	$\mathbb{Z}_7$	Paley
$(11,5,2)$	$\mathbb{Z}_{11}$	Paley
$(13,4,1)$	$\mathbb{Z}_{13}$	No
$(15,7,3)$	$\mathbb{Z}_{15}$	No
$(19,9,4)$	$\mathbb{Z}_{19}$	Paley
$(21,5,1)$	$\mathbb{Z}_{21}$	No
$(21,5,1)$	$\langle a,b \mid a^7=b^3=1, a^2b=ba\rangle$	No
$(23,11,5)$	$\mathbb{Z}_{23}$	Paley
$(27,13,6)$	$\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_3$	Paley
$(27,13,6)$	$\langle a,b \mid a^3=b^9=1,\ ab^7=ba\rangle$	Example 11
$(31,6,1)$	$\mathbb{Z}_{31}$	Example 2
$(31,15,7)$	$\mathbb{Z}_{31}$	Paley
$(35,17,8)$	$\mathbb{Z}_{35}$	No
$(37,9,2)$	$\mathbb{Z}_{37}$	Thm 12, $\mathbb{F}_{37}^*/\mathbb{F}_{37}^{(4)}$
$(40,13,4)$	$\mathbb{Z}_{40}$	No
$(40,13,4)$	$\langle a,b \mid a^5=b^8=1, a^4b=ba\rangle$	No
$(43,21,10)$	$\mathbb{Z}_{43}$	Paley
$(47,23,11)$	$\mathbb{Z}_{47}$	Paley

Table 1: Tilings of admissible groups of order $v \leqslant 50$.

Conjecture 7. The difference sets in a tiling of an abelian group are necessarily normalized.

In general we have no proof of this conjecture, but in the next section we shall prove it for tilings with two difference sets ($t=2$). Proposition 5 follows directly from the conjecture: there is a unique normalized translate of every cyclic $(57,8,1)$ difference set and it contains the elements 19 and 38. Hence, normalized $(57,8,1)$ difference sets cannot be disjoint.

3 Tiling with two difference sets

Suppose that a group G can be tiled with two difference sets $\{D_1, D_2\}$. Then the parameters (v,k,λ) are of the form $(4n-1, 2n-1, n-1)$ for some $n \geqslant 2$, i.e. D_1 and D_2 are Paley-type difference sets. The canonical example are the Paley difference sets, i.e. the nonzero squares $\mathbb{F}_q^{(2)} = \{x^2 \mid x \in \mathbb{F}_q^*\}$ in the additive group of the field $\mathbb{F}_q$ of order $q \equiv 3 \pmod 4$. The nonsquares $\mathbb{F}_q^* \setminus \mathbb{F}_q^{(2)}$ are also a difference set, and therefore $\{\mathbb{F}_q^{(2)}, \mathbb{F}_q^* \setminus \mathbb{F}_q^{(2)}\}$

is a $(q,(q-1)/2,(q-3)/4)$ tiling of the elementary abelian group of order q.

A special class of Paley-type difference sets are the *skew Hadamard* or *antisymmetric* difference sets. A difference set D in a group G is skew Hadamard provided $D \cup (-D) = G \setminus \{0\}$ holds. Since $-D = \{-x \mid x \in D\}$ is clearly also a difference set, $\{D, -D\}$ is a tiling of G with two difference sets. For a long time it was conjectured that the Paley difference sets were the only examples of skew Hadamard difference sets in abelian groups. Two new series of skew Hadamard difference set in elementary abelian groups of order 3^m, m odd, were constructed in [5, 6]. Since then there have been other constructions, see [9] and [20].

It is natural to ask whether any tiling of a group G with two difference sets $\{D_1, D_2\}$ necessarily comes from a skew Hadamard difference set, i.e. whether $D_2 = -D_1$ must hold. We shall prove this by using the group ring $\mathbb{Z}[G]$. Now we switch to multiplicative notation, and write $D^{(-1)}$ instead of $-D$. Also, we identify a subset $S \subseteq G$ with the corresponding group ring element $\sum_{g \in S} g$.

Theorem 8. *If $\{D_1, D_2\}$ is a tiling of a group G with two (v,k,λ) difference sets, then $D_2 = D_1^{(-1)}$ holds, i.e. the two difference sets are skew Hadamard.*

Proof. Since D_1 and D_2 are difference sets, the following relations in the group ring $\mathbb{Z}[G]$ hold:

$$D_1 \cdot D_1^{(-1)} = (k-\lambda) + \lambda G, \tag{1}$$

$$D_2 \cdot D_2^{(-1)} = (k-\lambda) + \lambda G. \tag{2}$$

By the definition of a tiling, we have $D_1 + D_2 + 1 = G$. Multiplying this by $D_1^{(-1)}$ from the right and using (1), we get

$$(k-\lambda) + \lambda G + D_2 \cdot D_1^{(-1)} + D_1^{(-1)} = G \cdot D_1^{(-1)} = kG. \tag{3}$$

Similarly, multiplying $D_1^{(-1)} + D_2^{(-1)} + 1 = G$ by D_2 from the left and using (2), we get

$$D_2 \cdot D_1^{(-1)} + (k-\lambda) + \lambda G + D_2 = D_2 \cdot G = kG. \tag{4}$$

Now $D_2 = D_1^{(-1)}$ follows by subtracting (3) and (4). □

By this theorem, all known restrictions for skew Hadamard difference sets also apply to tilings of groups with two difference sets. For example, it is known that the Paley difference sets are indeed the only examples in cyclic groups [15]. See the survey [26] for other known restrictions in the abelian case. One known result about skew Hadamard difference sets in elementary abelian groups is that they must be normalized; see [23, Lemma 4.3]. We are going to improve this result by proving it without the 'elementary abelian' assumption.

Theorem 9. *Every skew Hadamard difference set in an abelian group of order $|G| > 3$ is normalized.*

Proof. Let D be a skew Hadamard difference set in an abelian group G and let $h = \prod_{d\in D} d$. By [4], the order $v = |G| = p^m$ is a prime power and the quadratic residues modulo v are multipliers fixing D. If $p > 3$, we can find a quadratic residue $t > 1$ such that $t - 1$ is coprime to p, and then $g^t \neq g$ for all $g \in G \setminus \{1\}$. Now from $D^{(t)} = D$ we have

$$h^t = \prod_{d\in D} d^t = \prod_{d\in D^{(t)}} d = h$$

and thus $h = 1$.

Next we look at the case $p = 3$. According to the fundamental theorem of finitely generated abelian groups, $G \cong \mathbb{Z}_{3^{N_0}} \times \mathbb{Z}_{3^{N_1}} \times \cdots \times \mathbb{Z}_{3^{N_l}}$, where $N_0 \leqslant N_1 \leqslant \ldots \leqslant N_l$. For every $g \in G$, we write $g = (g_0, g_1, \ldots, g_l)$, where $g_i \in \mathbb{Z}_{3^{N_i}}$. Here the identity element is $(0, \ldots, 0)$ and we use additive notation on the coordinates. If $N_i > 1$, we can again find a quadratic residue $t > 1$ such that $(t - 1, 3^{N_i}) = 1$ and conclude that $h_i = 0$. Now only the case $N_i = 1$ remains.

Without loss of generality, we assume that $N_0 = 1$. Let $n_i = |\{d \in D \mid d_0 = i\}|$, for $i = 0, 1, 2$; clearly $n_0 + n_1 + n_2 = k$. Noting that $k = \frac{v-1}{2} \equiv 1 \pmod 3$ and $\lambda = \frac{v-3}{4} \equiv 0 \pmod 3$, we have

$$n_0 + n_1 + n_2 \equiv 1 \pmod 3. \tag{5}$$

Since D is a difference set, $D \cdot D^{(-1)} = (k - \lambda) + \lambda G$. Counting elements with $g_0 = 0$ on the left-hand and right-hand side yields

$$n_0^2 + n_1^2 + n_2^2 = (k - \lambda) + \lambda 3^{m-1},$$

and taking this modulo 3

$$n_0^2 + n_1^2 + n_2^2 \equiv 1 \pmod 3. \tag{6}$$

On the other hand, since D is a skew Hadamard difference set

$$D \cdot D = D(G - 1 - D^{(-1)}) = (k - \lambda)G - D - (k - \lambda).$$

Again, by counting elements with $g_0 = 0$ we have

$$n_0^2 + 2n_1n_2 = (k - \lambda)3^{m-1} - n_0 - (k - \lambda),$$

and since $m > 1$, modulo 3 we get

$$n_0^2 + 2n_1n_2 + n_0 \equiv 2 \pmod 3. \tag{7}$$

It is routine to verify that from (5), (6), (7) follows $n_0 \equiv 1 \pmod 3$ and $n_1 \equiv n_2 \equiv 0 \pmod 3$. From this we have $h_0 \equiv n_1 + 2n_2 \equiv 0 \pmod 3$. Now we see that all components of h are equal to 0, and h is the identity element. Hence, D is normalized. □

For $p > 3$, our proof is essentially the same as in [23], and for $p = 3$ our proof is simpler and more general. From Theorem 8 and Theorem 9 we have the following result.

Corollary 10. *Conjecture 7 is true for tilings of abelian groups with two difference sets.*

Skew Hadamard difference sets are known to exist in non-abelian groups; see [8] for an infinite family. The smallest example occurs in a non-abelian group of order 27.

Example 11. Let G be the group $\langle a, b \,|\, a^3 = b^9 = 1,\ ab^7 = ba\rangle$ of order 27. The following two difference sets are a $(27, 13, 6)$ tiling of G:

$$\begin{aligned} D_1 &= \{a, b^2, ab^2, a^2b^2, b^3, ab^3, b^4, a^2b^4, ab^5, a^2b^5, ab^6, ab^7, b^8\}, \\ D_2 &= \{a^2, b, ab, a^2b, a^2b^3, ab^4, b^5, b^6, a^2b^6, b^7, a^2b^7, ab^8, a^2b^8\}. \end{aligned}$$

The difference set D_1 is equivalent to one of the two non-abelian $(27, 13, 6)$ difference sets found by Kibler [16].

4 Tilings based on cyclotomy

We can use the quotient group to construct tilings with $t > 2$. Let D be a difference set in the additive group of a finite field $\mathbb{F}_q$. If D is also a subgroup of the multiplicative group $\mathbb{F}_q^*$, then $\mathbb{F}_q^*/D$ is a tiling of the additive group. The quotient group consists of disjoint cosets $\{a_1D, \ldots, a_tD\}$ for $a_i \in \mathbb{F}_q^*$. Multiplication by a nonzero element is an automorphism of the additive group, and therefore preserves the difference set property. Thus, we have proved the following theorem.

Theorem 12. *Let $\mathbb{F}_q$ be a finite field of order q. If there exists a difference set D in $(\mathbb{F}_q, +)$ such that D is a subgroup of $(\mathbb{F}_q^*, \cdot)$, then the quotient group $\mathbb{F}_q^*/D$ is a tiling of $(\mathbb{F}_q, +)$.*

The nonzero squares form a subgroup of $\mathbb{F}_q^*$, and the Paley tilings are a special case of Theorem 12. The theorem also applies to the fourth and eighth powers, i.e. to the following cyclotomic difference sets (see [1] and [14]):

- $\mathbb{F}_q^{(4)} = \{x^4 \mid x \in \mathbb{F}_q^*\}$, $q = 4t^2 + 1$, t odd;
- $\mathbb{F}_q^{(8)} = \{x^8 \mid x \in \mathbb{F}_q^*\}$, $q = 8t^2 + 1 = 64u^2 + 9$, t, u odd.

The corresponding tilings $\mathbb{F}_q^*/\mathbb{F}_q^{(4)}$ and $\mathbb{F}_q^*/\mathbb{F}_q^{(8)}$ with parameters $(q, (q-1)/4, (q-5)/16)$ and $(q, (q-1)/8, (q-9)/64)$ consist of four and of eight difference sets, respectively. The first few examples for $\mathbb{F}_q^{(4)}$ are $(37, 9, 2)$, $(101, 25, 6)$, $(197, 49, 12)$, $(677, 169, 12)$, and for $\mathbb{F}_q^{(8)}$ $(73, 9, 1)$ with the next one already being very large.

The tiling of Example 2 cannot be obtained from Theorem 12 because $D_1 = \{1, 5, 11, 24, 25, 27\}$ is not a multiplicative subgroup of $\mathbb{F}_{31}^*$. However, D_1 is a union of the subgroup $\langle 5\rangle = \{1, 5, 25\}$ and one of its cosets, while the other difference sets are multiples of D_1:

$$\begin{aligned} D_1 &= \{1, 5, 11, 24, 25, 27\} = \omega^0\langle 5\rangle \cup \omega^3\langle 5\rangle, \\ D_2 &= \{2, 10, 17, 19, 22, 23\} = \omega^4 D_1, \end{aligned}$$

$$\begin{aligned} D_3 &= \{3,4,7,13,15,20\} = \omega^8 D_1,\\ D_4 &= \{6,8,9,14,26,30\} = \omega^2 D_1,\\ D_5 &= \{12,16,18,21,28,29\} = \omega^6 D_1. \end{aligned}$$

Here $\omega = 3$ is a primitive element of $\mathbb{F}_{31}$. In general, assume we have a (q,k,λ) difference set in $\mathbb{F}_q$ fixed by the multiplier m, such that the order $|\langle m\rangle| = r$ divides k. Then D can be written as a union of cosets

$$D = \omega^{c_1}\langle m\rangle \cup \omega^{c_2}\langle m\rangle \cup \cdots \cup \omega^{c_{k/r}}\langle m\rangle.$$

The problem of tiling $\mathbb{F}_q$ by multiples of D is equivalent to tiling the set of integers $\{0,1,\ldots,n-1\}$ by cyclic shifts of $\{c_1,c_2,\ldots,c_{k/r}\}$ modulo $n=(q-1)/r$. This can be expressed as the following theorem.

Theorem 13. *Let ω be a primitive element and $\langle m\rangle$ a multiplicative subgroup of order r of the finite field $\mathbb{F}_q$. Suppose we have a (q,k,λ) difference set in $(\mathbb{F}_q,+)$ which is a union of cosets*

$$D = \omega^{c_1}\langle m\rangle \cup \omega^{c_2}\langle m\rangle \cup \cdots \cup \omega^{c_{k/r}}\langle m\rangle,$$

for $c_1,c_2,\ldots,c_{k/r} \in \{0,1,\ldots,n-1\}$, $n=(q-1)/r$. Then there exists a (q,k,λ) tiling of $(\mathbb{F}_q,+)$ by multiples of D if and only if there exist integers $b_1,b_2,\ldots,b_{(k-1)/\lambda} \in \{0,1,\ldots,n-1\}$ such that

$$b_i - b_j \not\equiv c_u - c_v \pmod{n}$$

for all $i,j \in \{1,2,\ldots,(k-1)/\lambda\}$, $i\neq j$, and $u,v\in\{1,2,\ldots,k/r\}$, $u\neq v$.

Proof. Let $C=\{c_1,c_2,\ldots,c_{k/r}\}$. From the observations above we see that the tiling can be constructed if and only if there exist integers $b_1,b_2,\ldots,b_{(k-1)/\lambda}$ such that

$$(b_1+C)\cup(b_2+C)\cup\cdots\cup(b_{(k-1)/\lambda}+C) = \{0,1,\ldots,n-1\}$$

holds modulo n. This is equivalent to sets of the form $b_i + C$ being mutually disjoint, i.e. $b_i + c_u \not\equiv b_j + c_v \pmod{n}$ for all different $i,j\in\{1,2,\ldots,(k-1)/\lambda\}$ and $u,v\in\{1,2,\ldots,k/r\}$. Finally, the condition can be expressed as $b_i - b_j \not\equiv c_u - c_v \pmod{n}$. □

If we take the $(31,6,1)$ difference set $D=\omega^0\langle 5\rangle\cup\omega^3\langle 5\rangle$, then $r=3$, $n=10$, $C=\{0,3\}$ and the problem of finding the b_i's has two solutions: $0,2,4,6,8$ and $1,3,5,7,9$. The first one gives the tiling of Example 2, and the second one a $(31,6,1)$ tiling that corresponds to the mirror image of the necklace in Figure 1.

As another application of Theorem 13, we show that $\mathbb{F}_{307}$ cannot be tiled by multiples of a $(307,18,1)$ difference set fixed by the multiplier 17. We take the primitive element $\omega=5$ and note that the multiplicative group $\langle 17\rangle=\{1,17,289\}$ is of order $r=3$. By [14, Remark 18.74], all $(307,18,1)$ difference sets are equivalent to

$$D=\omega^0\langle 17\rangle\cup\omega^{10}\langle 17\rangle\cup\omega^{30}\langle 17\rangle\cup\omega^{35}\langle 17\rangle\cup\omega^{37}\langle 17\rangle\cup\omega^{59}\langle 17\rangle.$$

Tiling $\mathbb{F}_{307}$ by multiples of D is equivalent to tiling $\{0, \ldots, 101\}$ by translates of the set $C = \{0, 10, 30, 35, 37, 59\}$ modulo $n = 102$. We set up a graph with vertices $\{0, \ldots, 101\}$, i and j being adjacent if $i - j \not\equiv u - v \pmod{102}$ for all $u, v \in C$, $u \neq v$. A tiling corresponds to a clique of size 17 in this graph. Using the program *Cliquer* [21] we found that the maximum clique size is 14. Therefore, a tiling does not exist. However, we got 14 mutually disjoint $(307, 18, 1)$ difference sets corresponding to the following numbers b_i as in Theorem 13: 0, 3, 6, 9, 12, 15, 48, 51, 54, 57, 60, 63, 66, 69.

5 Tilings using Singer difference sets

Let q be the power of a prime, $n \geqslant 3$ an integer, and G the cyclic group of order $\frac{q^n-1}{q-1}$. Singer difference sets are difference sets in G with parameters $(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1})$. The classical construction comes from projective geometry $PG(n-1, q)$. Let ω be a primitive element of $\mathbb{F}_{q^n}$ and $\mathrm{Tr}(x) = x + x^q + \cdots + x^{q^{n-1}}$ the trace mapping from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. Let β be a nonzero element in $\mathbb{F}_{q^n}$ and r an integer coprime to $\frac{q^n-1}{q-1}$. Then the set of integers

$$\{i \mid 0 \leqslant i < \frac{q^n-1}{q-1}, \mathrm{Tr}(\beta\omega^{ri}) = 0\} \tag{8}$$

forms a Singer difference set with addition modulo $\frac{q^n-1}{q-1}$. There are also other constructions of cyclic difference sets with these parameters, see [12, 19]. We are going to consider using classical Singer difference sets to tile the group G; such tilings will be called *classical Singer tilings*. Several small examples fall into this category.

Example 14. Take $q = 2$, $n = 3$ and the irreducible polynomial $f(x) = x^3 + x^2 + 1$ over $\mathbb{F}_2$ to construct the field $\mathbb{F}_{2^3}$. Take the primitive element $\omega = x$ and $\beta = 1$. Then by substituting $r = 3$ in (8) we get the squares in $\mathbb{F}_7^*$, and from $r = 1$ the non-squares. Hence, the Paley tiling of $\mathbb{F}_7$ is a classical Singer tiling.

Example 15. Take $q = 5$, $n = 3$ and the irreducible polynomial $f(x) = x^3 + 3x + 2$ over $\mathbb{F}_5$ to construct the field $\mathbb{F}_{5^3}$. Take the primitive element $\omega = x$ and $\beta = 1$. Then by substituting $r = 17, 11, 21, 37, 3$ in (8) we get the difference sets $D_1, \ldots, D_5$ of Example 2. This $(31, 6, 1)$ tiling is also a classical Singer tiling.

Example 16. Take $q = 8$, $n = 3$ and first construct the field $\mathbb{F}_8$ as in Example 14. Now take the irreducible polynomial $g(y) = y^3 + y + (x^2 + 1)$ over $\mathbb{F}_8$ to construct the field $\mathbb{F}_{8^3}$ with primitive element $\omega = y$. By substituting $\beta = 1$, $r = 1$ in (8) we get the eighth powers in $\mathbb{F}_{73}$, and from $r = 25, 11, 9, 5, 17, 13, 3$ the other cosets forming a $(73, 9, 1)$ tiling. Hence, the tiling obtained from Theorem 12 by using the eighth powers $\mathbb{F}_{73}^{(8)}$ is a classical Singer tiling as well.

To prove our main result in this section, we need the following lemma which can be found in [18, Chapter 7].

Lemma 17. *If $\varphi : \mathbb{F}_q \to \mathbb{F}_q$ is an arbitrary function, then there exists a unique polynomial $g \in \mathbb{F}_q[x]$ with $\deg(g) < q$ representing φ, in the sense that $g(c) = \varphi(c)$ for all $c \in \mathbb{F}_q$. To be precise,*

$$g(x) = \sum_{c \in \mathbb{F}_q} \varphi(c)(1-(x-c)^{q-1}).$$

Furthermore, for $f, g \in \mathbb{F}_q[x]$ we have $f(c) = g(c)$ for all $c \in \mathbb{F}_q$ if and only if $f(x) \equiv g(x) \pmod{x^q - x}$.

Theorem 18. *When $\frac{q^n-1}{q-1} > q \cdot \binom{n+q-2}{n-1} + 1$, there are no classical Singer tilings of the cyclic group of order $\frac{q^n-1}{q-1}$.*

Proof. Assume that there are β_i and r_i where $i = 1, 2, \ldots, q$, such that the classical Singer difference sets determined by (β_j, r_j) form a tiling. That means $\mathrm{Tr}(\beta_i) \neq 0$ for each i and there is a unique i such that $\mathrm{Tr}(\beta_i a^{r_i}) = 0$ for each $a \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. Hence

$$\tau(a) := \sum_{i=1}^{q} \mathrm{Tr}(\beta_i a^{r_i})^{q-1} = \begin{cases} 0, & a \in \mathbb{F}_q; \\ q-1, & \text{otherwise.} \end{cases}$$

By Lemma 17, we can write τ as a polynomial over $\mathbb{F}_{q^n}$ as follows:

$$\begin{aligned} 1 + \tau(x) &= \sum_{a \in \mathbb{F}_q} (1 - (x-a)^{q^n-1}) \\ &= -\sum_{a \in \mathbb{F}_q} \sum_{i=0}^{q^n-1} \binom{q^n-1}{i} x^{q^n-1-i}(-a)^i \\ &= \sum_{i=0}^{q^n-1} (-1)^{i+1} \binom{q^n-1}{i} \left(\sum_{a \in \mathbb{F}_q} a^i \right) x^{q^n-1-i} \\ &= \sum_{j=1}^{\frac{q^n-1}{q-1}} (-1)^{(q-1)j} \binom{q^n-1}{(q-1)j} x^{q^n-1-(q-1)j}. \end{aligned}$$

The last equality follows from the fact that

$$\sum_{a \in \mathbb{F}_q} a^i = \begin{cases} -1, & i \equiv 0 \pmod{q-1} \text{ and } i \neq 0; \\ 0, & \text{otherwise.} \end{cases}$$

Finally, using $\binom{q^n-1}{(q-1)j} \equiv 1$ modulo the characteristic of $\mathbb{F}_q$, we can write

$$\tau(x) = \sum_{j=1}^{\frac{q^n-1}{q-1}-1} (-1)^{(q-1)j} x^{q^n-1-(q-1)j}.$$

Hence, the polynomial $\tau(x)$ has $\frac{q^n-1}{q-1} - 1$ terms.

On the other hand, as the polynomial $\mathrm{Tr}(\beta_i x^{r_i})^{q-1}$ has at most $\binom{n+q-2}{n-1}$ terms, $\tau(x)$ has at most $q \cdot \binom{n+q-2}{n-1}$ terms. Note that reducing modulo $x^{q^n} - x$ cannot increase the number of terms of the polynomial. By Lemma 17, we have a contradiction when $\frac{q^n-1}{q-1} > q \cdot \binom{n+q-2}{n-1} + 1$. □

According to Theorem 18, for each given q there is an integer n_q such that, when $n \geqslant n_q$ there are no classical Singer tilings. We list several q's and the corresponding n_q's in the following table.

q	$2,3,4$	$5,\ldots,17$	$19,\ldots,109$	$113,\ldots,701$	$709,\ldots,5011$
n_q	4	5	6	7	8

Table 2: Nonexistence of classical Singer tilings.

References

[1] L. D. Baumert, *Cyclic difference sets*, Lecture Notes in Mathematics **182**, Springer, 1971.

[2] T. Beth, D. Jungnickel, and H. Lenz, *Design theory, second edition*, Cambridge University Press, 1999.

[3] M. Buratti, J. Yan, and C. Wang, *From a 1-rotational RBIBD to a partitioned difference family*, Electron. J. Combin. **17** (2010), no. 1, Research Paper #R139, 23 pp.

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

[5] C. Ding and J. Yuan, *A family of skew Hadamard difference sets*, J. Combin. Theory Ser. A **113** (2006), 1526–1535.

[6] C. Ding, Z. Wang, and Q. Xiang, *Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in $PG(3, 3^{2h+1})$*, J. Combin. Theory Ser. A **114** (2007), 867–887.

[7] J. H. Dinitz and N. Shalaby, *Block disjoint difference families for Steiner triple systems: $v \equiv 3 \pmod 6$*, J. Statist. Plann. Inference **106** (2002), 77–86.

[8] T. Feng, *Non-abelian skew Hadamard difference sets fixed by a prescribed automorphism*, J. Combin. Theory Ser. A **118** (2011), 27–36.

[9] T. Feng and Q. Xiang, *Cyclotomic constructions of skew Hadamard difference sets*, J. Combin. Theory Ser. A **119** (2012), 245–256.

[10] R. Fuji-Hara, Y. Miao, and S. Shinohara, *Complete sets of disjoint difference families and their applications*, J. Statist. Plann. Inference **106** (2002), 87–103.

[11] O. W. Gnilke, M. Greferath, and M. O. Pavčević, *Mosaics of combinatorial designs*, arXiv:1503.01643 (Mar 2015).

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

[13] F. Hou, L. X. Cai, X. Shen, and J. Huang, *Asynchronous multichannel MAC design with difference-set-based hopping sequences*, IEEE Transactions on Vehicular Technology, **60** (2011), no. 4, 1728–1739.

[14] D. Jungnickel, A. Pott, and K. W. Smith, *Difference sets*, in: Handbook of Combinatorial Designs, Second Edition (eds. C.J. Colbourn and J.H. Dinitz), Champan & Hall/CRC, 2007., pp. 419–435.

[15] J. Kelly, *A characteristic property of quadratic residues*, Proc. Amer. Math. Soc. **5** (1954), 38–46.

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

[17] E. S. Lander, *Symmetric designs: an algebraic approach*, Cambridge University Press, 1983.

[18] R. Lidl and H. Niederreiter, *Finite fields, second edition*, Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, 1997.

[19] A. Maschietti, *Difference sets and hyperovals*, Des. Codes Cryptogr. **14** (1998), 89–98.

[20] M. Muzychuk, *On skew Hadamard difference sets*, arXiv:1012.2089 (Dec 2010).

[21] S. Niskanen and P. R. J. Östergård, *Cliquer user's guide, version 1.0*, Communications Laboratory, Helsinki University of Technology, Espoo, Finland, Tech. Rep. T48, 2003.

[22] A. Pott, *Finite geometry and character theory*, Lecture Notes in Mathematics, 1601. Springer-Verlag, Berlin, 1995.

[23] G. Weng and L. Hu, *Some results on skew Hadamard difference sets*, Des. Codes Cryptogr. **50** (2009), 93–105.

[24] D. Wu, J. Yang, S. Chen, and D. Li, *The existence of $(v, 4, \lambda)$ disjoint difference families*, Australas. J. Combin. **44** (2009), 225–234.

[25] K. Wu, F. Han, F. Han, and D. Kong, *Rendezvous sequence construction in cognitive radio ad-hoc networks based on difference sets*, 2013 IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications, IEEE 2013, pp. 1840–1845.

[26] Q. Xiang, *Recent progress in algebraic design theory*, Finite Fields Appl. **11** (2005), 622–653.

[27] J. Yin, X. Shan, and Z. Tian, *Constructions of partitioned difference families*, European J. Combin. **29** (2008), no. 6, 1507–1519.