Novák's conjecture on cyclic Steiner triple systems and its generalization

Tao Feng[a], Daniel Horsley[b] and Xiaomiao Wang[c]

[a]*Department of Mathematics, Beijing Jiaotong University, Beijing 100044, P.R. China*
[b]*School of Mathematics, Monash University, VIC 3800, Australia*
[c]*School of Mathematics and Statistics, Ningbo University, Ningbo 315211, P.R. China*

Abstract

Novák conjectured in 1974 that for any cyclic Steiner triple systems of order v with $v \equiv 1 \pmod 6$, it is always possible to choose one block from each block orbit so that the chosen blocks are pairwise disjoint. We consider the generalization of this conjecture to cyclic (v, k, λ)-designs with $1 \leqslant \lambda \leqslant k-1$. Superimposing multiple copies of a cyclic symmetric design shows that the generalization cannot hold for all v, but we conjecture that it holds whenever v is sufficiently large compared to k. We confirm that the generalization of the conjecture holds when v is prime and $\lambda = 1$ and also when $\lambda \leqslant (k-1)/2$ and v is sufficiently large compared to k. As a corollary, we show that for any $k \geqslant 3$, with the possible exception of finitely many composite orders v, every cyclic $(v, k, 1)$-design without short orbits is generated by a $(v, k, 1)$-disjoint difference family.

Keywords: Steiner triple system; Novák's conjecture; cyclic design; disjoint difference family

1 Introduction

Let V be a set of v *points*, and $\mathcal{B}$ be a collection of k-subsets of V called *blocks*. A pair $(V, \mathcal{B})$ is called a (v, k, λ)-*design* if every pair of distinct elements of V is contained in precisely λ blocks of $\mathcal{B}$. A $(v, 3, 1)$-design is called a *Steiner triple system* of order v and is written as an STS(v).

An *automorphism* of a (v, k, λ)-design $(V, \mathcal{B})$ is a permutation on V leaving $\mathcal{B}$ invariant. A (v, k, λ)-design is said to be *cyclic* if it admits an automorphism consisting of a cycle of length v. Without loss of generality we identify V with $\mathbb{Z}_v$, the additive group of integers modulo v. The blocks of a cyclic (v, k, λ)-design can be partitioned into orbits under $\mathbb{Z}_v$. We can choose any fixed block from each orbit and then call these *base blocks*. If the cardinality of an orbit is equal to v, the orbit is *full*. Otherwise, it is *short*. It follows from the orbit-stabilizer theorem that the cardinality of any orbit is a divisor of v and is at least v/k. If $\gcd(v, k) = 1$, then all orbits of a cyclic (v, k, λ)-design are full (see [15, Lemma 1]). It is known that a cyclic STS(v) exists if and only if $v \equiv 1, 3 \pmod 6$ and $v \neq 9$ (see [10, Theorem 7.3]).

[a]E-mail address: tfeng@bjtu.edu.cn; Supported by NSFC under Grant 11871095
[b]E-mail address: danhorsley@gmail.com; Supported by ARC grants DP150100506 and FT160100048
[c]E-mail address: wangxiaomiao@nbu.edu.cn; Supported by NSFC under Grant 11771227

A useful tool for generating cyclic designs is the concept of a difference family. A (v,k,λ)-*cyclic difference family* is a family $\mathcal{F}$ of k-subsets (called *base blocks*) of $\mathbb{Z}_v$ such that the multiset $\Delta\mathcal{F} := \{x-y : x,y \in F, x \neq y, F \in \mathcal{F}\}$ contains every element of $\mathbb{Z}_v \setminus \{0\}$ exactly λ times. Such a family is denoted as a (v,k,λ)-CDF. It consists of $\lambda(v-1)/(k(k-1))$ base blocks. A (v,k,λ)-CDF $\mathcal{F}$ can generate a cyclic (v,k,λ)-design with block-multiset $\mathrm{dev}\mathcal{F} := \{F+t : F \in \mathcal{F}, t \in \mathbb{Z}_v\}$ (see [18, Theorem 3.46]). Furthermore, when $\gcd(v,k)=1$, $\mathcal{F}$ is a (v,k,λ)-CDF if and only if $\mathrm{dev}\mathcal{F}$ is a cyclic (v,k,λ)-design (see [3, Proposition VII.1.5]).

A (v,k,λ)-CDF is said to be *disjoint* and written as a (v,k,λ)-DDF when its base blocks are mutually disjoint. Novák [16] conjectured in 1974 that for any cyclic STS(v) with $v \equiv 1 \pmod 6$, it is always possible to find a set of $(v-1)/6$ disjoint base blocks which come from different block orbits to form a $(v,3,1)$-DDF (see also [1, Remark 16.22] or [10, Work point 22.5.2]).

Conjecture 1. (Novák, 1974) [16] *Every cyclic STS(v) with $v \equiv 1 \pmod 6$ is generated by a $(v,3,1)$-DDF.*

Conjecture 1 is widely believed to be true but not much progress has been made on it. So far it is only known that Conjecture 1 holds for all $v \equiv 1 \pmod 6$ and $v \leqslant 61$ (see [10, Theorem 22.3]). On the other hand, Dinitz and Rodney [11] proved that a $(v,3,1)$-DDF exists for any $v \equiv 1 \pmod 6$ by taking a suitable $(v,3,1)$-CDF and then replacing each of its base blocks B_i by a suitable translate $B_i + t_i$. For more information on $(v,3,1)$-DDFs with $v \equiv 3 \pmod 6$, interested readers are referred to [6, 12].

Recently, using the Combinatorial Nullstellensatz, Karasev and Petrov [14] proved the following result.

Lemma 1. [14, Theorem 2] *Let $\mathbb{F}$ be an arbitrary field, and let m and d be positive integers such that $(md)!/(d!)^m \neq 0$ in $\mathbb{F}$. Let $X_1,\ldots,X_m$ and $T_1,\ldots,T_m$ be subsets of $\mathbb{F}$ such that*

$$\forall i<j \quad |X_i - X_j| \leqslant 2d, \qquad \forall i \quad |T_i| \geqslant (m-1)d+1,$$

where $X_i - X_j := \{x-y : x \in X_i, y \in X_j\}$. Then there exists a system of representatives $t_i \in T_i$ such that the sets $X_1+t_1,\ldots,X_m+t_m$ are pairwise disjoint.

We now apply Lemma 1 to show that Conjecture 1 is true whenever v is a prime.

Theorem 1. *Let $k \geqslant 2$ and let p be a prime. Every cyclic $(p,k,1)$-design is generated by a $(p,k,1)$-DDF.*

Proof. We may assume $p > k$ because otherwise the result is trivial. Since $\gcd(p,k)=1$, a cyclic $(p,k,1)$-design has $m = (p-1)/(k(k-1))$ full orbits and no short orbits. Let $B_1,\ldots,B_m$ be base blocks of a cyclic $(p,k,1)$-design and let $d = \lceil k^2/2 \rceil$. Then $|B_i - B_j| \leqslant 2d$ for any $1 \leqslant i < j \leqslant m$. Let $T_1 = \cdots = T_m = \mathbb{Z}_p$. Then $|T_i| = p \geqslant (m-1)d+1$ for $k \geqslant 2$. Since $md < p$ when $k \geqslant 2$, $(md)!/(d!)^m \not\equiv 0 \pmod p$. Therefore, by Lemma 1, there exists a system of representatives $t_i \in T_i$ such that $B_1+t_1,\ldots,B_m+t_m$ are pairwise disjoint. So $B_1+t_1,\ldots,B_m+t_m$ form a $(p,k,1)$-DDF. $\square$

Theorem 1 motivates us to present the following conjecture on cyclic $(v,k,1)$-designs, which also allows for designs with short orbits.

Conjecture 2. *For any cyclic $(v,k,1)$-design, it is always possible to choose one block from each block orbit so that the chosen blocks are pairwise disjoint.*

The existence of $(v,k,1)$-DDFs is in general quite a hard problem. Conjecture 2, if true, would reduce the existence of $(v,k,1)$-DDFs to the existence of $(v,k,1)$-CDFs. The following results on CDFs are known in the literature.

Lemma 2.

(1) [9] *For any prime* $p \equiv 1 \pmod{12}$, *there exists a* $(p,4,1)$*-CDF.*

(2) [9] *For any prime* $p \equiv 1 \pmod{20}$, *there exists a* $(p,5,1)$*-CDF.*

(3) [8] *For any prime* $p \equiv 1 \pmod{30}$ *and* $p \neq 61$, *there exists a* $(p,6,1)$*-CDF.*

(4) [7] *Let* $p \equiv 1 \pmod{k(k-1)}$ *be a prime. Then a* $(p,k,1)$*-CDF exists if* $p > \binom{k}{2}^{2k}$.

As a corollary of Theorem 1 together with Lemma 2, we obtain the following existence results on DDFs.

Theorem 2. *Let* $p \equiv 1 \pmod{k(k-1)}$ *be a prime.*

(1) *There exists a* $(p,k,1)$*-DDF for each* $k \in \{4,5,6\}$ *and* $(k,p) \neq (6,61)$.

(2) *There exists a* $(p,k,1)$*-DDF whenever* $p > \binom{k}{2}^{2k}$.

We remark that by using Weil's theorem on estimates of character sums, Wu, Yang and Huang [19] also established the existence of a $(p,4,1)$-DDF for any prime $p \equiv 1 \pmod{12}$. We also observe that the main result of [13] shows that, for fixed k and large v, one can find a family $\mathcal{F}$ of $(1-o(1))\frac{v-1}{k(k-1)}$ pairwise disjoint base blocks of size k such that $\Delta\mathcal{F}$ contains each difference at most once. This is accomplished by letting H be the disjoint union of $(1-o(1))\frac{v-1}{k(k-1)}$ copies of K_k and applying [13, Theorem 1.2] to find a rainbow copy of H in the complete graph on $\mathbb{Z}_v$ with edges coloured according to their differences.

In this paper, we shall provide a proof of Conjecture 2 when v is sufficiently large compared to k. In fact, we consider a more general setting. We shall examine cyclic (v,k,λ)-designs with $k \geqslant 2\lambda+1$. As the main result of this paper, we prove Theorem 3 below. In fact we prove a stronger statement which sometimes guarantees the existence of a family of mutually disjoint blocks containing many blocks from each orbit (see Theorem 4).

Theorem 3. *Let* k *and* λ *be fixed positive integers such that* $k \geqslant 2\lambda+1$. *There exists an integer* v_0 *such that, for any cyclic* (v,k,λ)*-design with* $v \geqslant v_0$, *it is always possible to choose one block from each block orbit so that the chosen blocks are pairwise disjoint.*

Combining Theorems 1 and 3 yields the following corollary.

Corollary 1. *Let* $k \geqslant 3$ *be a fixed integer. With the possible exception of finitely many composite orders* v, *every cyclic* $(v,k,1)$*-design without short orbits is generated by a* $(v,k,1)$*-DDF.*

2 Preliminaries

For any positive integer c, let $[c] := \{1,\ldots,c\}$. We will make use of the following simple lemma which shows that, for large v and fixed k and λ, a cyclic (v,k,λ)-design has few short orbits.

Lemma 3. *Let* $k \geqslant 2$ *and* $\lambda \geqslant 1$ *be fixed integers. If* $(V,\mathcal{B})$ *is a cyclic* (v,k,λ)*-design with* h *short orbits and* m *full orbits, then*

(i) $h \leqslant 2\lambda\sqrt{k}$; *and*

(ii) $\frac{\lambda(v-1)}{k(k-1)} - 2\lambda\sqrt{k} \leqslant m \leqslant \frac{\lambda(v-1)}{k(k-1)} \leqslant m+h \leqslant \frac{\lambda(v-1)}{k(k-1)} + 2\lambda\sqrt{k}$.

Proof. Let the point set of $(V,\mathcal{B})$ be $\mathbb{Z}_v$ and let $\mathcal{B}_1,\ldots,\mathcal{B}_h$ be the short orbits of $(V,\mathcal{B})$. Let $i\in[h]$. Recall that by the orbit-stabilizer theorem we have $|\mathcal{B}_i|=\ell_i$ where $\frac{v}{k}\leqslant\ell_i<v$ and $\ell_i\mid v$. Let B_i be a base block from $\mathcal{B}_i$ such that B_i contains the point 0. Since $|\mathcal{B}_i|=\ell_i$, $B_i+\ell_i=B_i$. It follows that B_i contains all multiples of ℓ_i. Write $S_i:=\{0,\ell_i,2\ell_i,\ldots,(\frac{v}{\ell_i}-1)\ell_i\}$. Then $S_i\subseteq B_i$. Furthermore, for any $a\in B_i$, $a+S_i\subseteq B_i$, and so B_i is a disjoint union of some cosets of S_i in $\mathbb{Z}_v$, which implies $|S_i|\mid|B_i|$. That is, $\frac{v}{\ell_i}\mid k$. Also, because exactly λ blocks in $\mathcal{B}$ contain the pair $\{0,\ell_i\}$, we have that at most λ of the orbits $\mathcal{B}_1,\ldots,\mathcal{B}_h$ have cardinality ℓ_i.

Thus, $h\leqslant\lambda\sigma_0(k)$ where $\sigma_0(k)$ denotes the number of divisors of k. We know that $\sigma_0(k)\leqslant 2\sqrt{k}$ for any positive integer k by using the fact that $d\mid k$ if and only if $\frac{k}{d}\mid k$, and so (i) follows. Then (ii) follows from (i) by routine calculation after observing that $mv+\sum_{i=1}^{h}\ell_i=|\mathcal{B}|=\frac{\lambda v(v-1)}{k(k-1)}$. □

An r-*uniform hypergraph* G is a pair (V,E) where V is a vertex set and E is a set of r-subsets of V called edges. The *degree* $\deg_G(x)$ of a vertex $x\in V$ is the number of edges of G containing x. For distinct vertices x and y of G, the *codegree* $\mathrm{codeg}_G(x,y)$ is the number of edges of G containing both x and y. We write $\delta_G:=\min\limits_{x\in V}\deg_G(x)$, $\Delta_G:=\max\limits_{x\in V}\deg_G(x)$ and $\Delta_G^c:=\max\limits_{x,y\in V,x\neq y}\mathrm{codeg}_G(x,y)$.

A *proper edge-colouring* of a hypergraph $G=(V,E)$ with c colours is a function $f:E\longrightarrow[c]$ such that no two edges that share a vertex get the same colour. The following powerful result of Pippenger and Spencer [17] (based on the Rödl nibble) shows that every almost regular r-uniform hypergraph G with small maximum codegree can be edge-coloured with close to Δ_G colours.

Lemma 4. [17] *Let $r\geqslant 2$ be an integer. For each real number $\eta>0$, there exists a real number $\eta^*>0$ and an integer n_0 such that if G is an r-uniform hypergraph on $n\geqslant n_0$ vertices satisfying $\delta_G\geqslant(1-\eta^*)\Delta_G$ and $\Delta_G^c\leqslant\eta^*\Delta_G$, then G has a proper edge-colouring with $(1+\eta)\Delta_G$ colours.*

3 Proof of Theorem 3

A *partial parallel class* of a (v,k,λ)-design is a set of pairwise disjoint blocks. Let $(V,\mathcal{B})$ be a cyclic (v,k,λ)-design with orbits $\mathcal{B}_1,\ldots,\mathcal{B}_t$, let $\mathcal{P}$ be a partial parallel class of $(V,\mathcal{B})$ and let $s=\lfloor\frac{k-1}{\lambda}\rfloor$. For any nonnegative integer a we define $T_a(\mathcal{P})=\{i\in[t]:|\mathcal{P}\cap\mathcal{B}_i|=a\}$ to be the set of indices of orbits of $(V,\mathcal{B})$ that contain exactly a blocks in $\mathcal{P}$, and we define $\tau_a(\mathcal{P})=|T_a(\mathcal{P})|$. Also, we say that a block $B\in\mathcal{B}$ is $\mathcal{P}$-*good* if, for each $i\in[t]$, B intersects at most one block in $\mathcal{P}\cap\mathcal{B}_i$ and, for each $i\in T_0(\mathcal{P})\cup\cdots\cup T_{s-1}(\mathcal{P})$, B intersects no block in $\mathcal{P}\cap\mathcal{B}_i$. Blocks in $\mathcal{B}$ that are not $\mathcal{P}$-good are $\mathcal{P}$-*bad*. Intuitively, a $\mathcal{P}$-good block B has the property that if we add B to $\mathcal{P}$ and remove all blocks of $\mathcal{P}$ incident with B, then each orbit that intersected $\mathcal{P}$ in at least $s-1$ blocks still intersects the resulting partial parallel class in at least $s-1$ blocks. Finally we define, if $s\geqslant 2$,

$$d(\mathcal{P})=\sum_{a=0}^{s-2}(s-1-a)\tau_a(\mathcal{P}).$$

One can think of $d(\mathcal{P})$ as a measure of how far $\mathcal{P}$ is from intersecting each orbit in at least $s-1$ blocks. The definitions of $\mathcal{P}$-good and $d(\mathcal{P})$ are implicitly dependent on the value of $s=\lfloor\frac{k-1}{\lambda}\rfloor$.

Our strategy is to first, in Lemma 5 below, apply Lemma 4 to an auxiliary hypergraph in order to obtain a partial parallel class in the design that contains s blocks from almost every orbit. For such a partial parallel class $\mathcal{P}$ we then, in Lemma 6, prove that if each orbit that intersects $\mathcal{P}$ in fewer than $s-1$ blocks contains sufficiently many $\mathcal{P}$-good blocks, then $\mathcal{P}$ can be modified to produce a new class that contains s blocks from almost every orbit and $s-1$ blocks from each remaining orbit. Finally, to prove Theorem 4, we show that Lemma 6 can successfully be applied to a partial parallel class obtained by making some modifications to a class given by Lemma 5.

Lemma 5. *Let k and λ be positive integers and let $s = \lfloor \frac{k-1}{\lambda} \rfloor$. For each real number $\epsilon^* > 0$, there exists an integer v_0^* such that, for each integer $v \geqslant v_0^*$, any cyclic (v,k,λ)-design with m full orbits has a partial parallel class $\mathcal{P}$ that contains s blocks from each of $(1-\epsilon^*)m$ full orbits and no blocks from any other orbit.*

Proof. Let $(V,\mathcal{B})$ be a cyclic (v,k,λ)-design with full orbits $\mathcal{B}_1,\ldots,\mathcal{B}_m$. Observe that, by Lemma 3(ii), $\frac{\lambda(v-1)}{k(k-1)} - 2\lambda\sqrt{k} \leqslant m \leqslant \frac{\lambda(v-1)}{k(k-1)}$. Hence, supposing v is sufficiently large, we have $\frac{\lambda(v-1)}{k^2} < m \leqslant \frac{\lambda(v-1)}{k(k-1)}$. Let $w = \lfloor \frac{v-1}{k} \rfloor$ and choose integers $s_1,\ldots,s_m \in \{s, s+1\}$ such that $s_1 + \cdots + s_m = w$. Such integers exist because $sm \leqslant \frac{v-1}{k}$ using $s \leqslant \frac{k-1}{\lambda}$ and $m \leqslant \frac{\lambda(v-1)}{k(k-1)}$, and because $(s+1)m > \frac{v-1}{k}$ using $s+1 \geqslant \frac{k}{\lambda}$ and $m > \frac{\lambda(v-1)}{k^2}$. Let $W = \{u_{i,j} : i \in [m], j \in [s_i]\}$ be a set of w vertices disjoint from V. We form a $(k+1)$-uniform hypergraph G with vertex set $V \cup W$ and edge set

$$\{B \cup \{u_{i,j}\} : B \in \mathcal{B}_i, i \in [m], j \in [s_i]\}.$$

Observe that, for each $x \in V$, we have $\deg_G(x) = ks_1 + \cdots + ks_m = kw$ because x is in k blocks in each full orbit, and hence we have $v-k \leqslant \deg_G(x) \leqslant v-1$. Also, $\deg_G(x) = v$ for each $x \in W$ because each full orbit contains v blocks. Furthermore $\mathrm{codeg}_G(x,y) \leqslant \lambda(s+1) \leqslant k+\lambda-1$ for all distinct $x,y \in V$ because $(V,\mathcal{B})$ is a design of index λ, $\mathrm{codeg}_G(x,y) = 0$ for all distinct $x,y \in W$, and $\mathrm{codeg}_G(x,y) = k$ for all $x \in V$ and $y \in W$ because k blocks from any full orbit contain a given vertex in V. So G has $v+w$ vertices, vw edges, $\delta_G \geqslant v-k$, $\Delta_G \leqslant v$, and $\Delta_G^c \leqslant k+\lambda-1$. Thus Lemma 4 implies that for any real number $\epsilon^* > 0$, supposing v is sufficiently large, G has a proper edge-colouring with $(1+\frac{\epsilon^*}{s+1})v$ colours.

Let $\mathcal{C}$ be a largest colour class of this colouring. Then $\mathcal{C}$ is a set of disjoint edges of G and, because G has vw edges, $|\mathcal{C}| \geqslant \frac{(s+1)w}{s+1+\epsilon^*} > w - \epsilon^* \frac{w}{s+1} > w - \epsilon^* m$ where the last inequality follows because $w < (s+1)m$. Let

$$M = \big\{ i \in [m] : |\{j \in [s_i] : u_{i,j} \text{ is in an edge in } \mathcal{C}\}| \geqslant s \big\}.$$

Observe that $|M| > (1-\epsilon^*)m$ because each edge of G contains exactly one vertex in W and hence there are less than $\epsilon^* m$ vertices in W that are not in an edge of $\mathcal{C}$. Let $\mathcal{C}'$ be the set of edges in $\mathcal{C}$ that contain a vertex in $\{u_{i,j} : i \in M, j \in [s_i]\}$ and let $\mathcal{P} = \{E \cap V : E \in \mathcal{C}'\}$. Then, by the definitions of G and $\mathcal{C}'$, $\mathcal{P}$ is a partial parallel class in $(V,\mathcal{B})$ that contains at least s blocks from $\mathcal{B}_i$ for each $i \in M$ and no other blocks. So, by deleting some blocks from $\mathcal{P}$ if necessary, we can obtain a partial parallel class with the desired properties. $\square$

Lemma 6. *Let k and λ be positive integers such that $k \geqslant 2\lambda+1$ and let $s = \lfloor \frac{k-1}{\lambda} \rfloor$. Let $(V,\mathcal{B})$ be a cyclic (v,k,λ)-design with orbits $\mathcal{B}_1,\ldots,\mathcal{B}_t$, and let $\mathcal{P}'$ be a partial parallel class that contains at most s blocks from each orbit. If, for each $i \in T_0(\mathcal{P}') \cup \cdots \cup T_{s-2}(\mathcal{P}')$, $\mathcal{B}_i$ contains more than $k^2(ks-k+1)(d(\mathcal{P}')-1)$ $\mathcal{P}'$-good blocks, then there is a partial parallel class $\mathcal{P}''$ of $(V,\mathcal{B})$ such that $\tau_{s-1}(\mathcal{P}'') \leqslant (k+1)d(\mathcal{P}') + \tau_{s-1}(\mathcal{P}')$ and $\tau_s(\mathcal{P}'') = t - \tau_{s-1}(\mathcal{P}'')$.*

Proof. Note that $s \geqslant 2$ by our hypotheses. We prove the result by induction on the quantity $d(\mathcal{P}')$. If $d(\mathcal{P}') = 0$ then $\tau_0(\mathcal{P}') = \cdots = \tau_{s-2}(\mathcal{P}') = 0$ and we can take $\mathcal{P}'' = \mathcal{P}'$ to complete the proof. So suppose that $d(\mathcal{P}') = \ell$ for some positive integer ℓ and that the result holds for $d(\mathcal{P}') < \ell$. Let $j \in T_0(\mathcal{P}') \cup \cdots \cup T_{s-2}(\mathcal{P}')$ and let B_j be a $\mathcal{P}'$-good block in $\mathcal{B}_j$ (such a block exists by the hypotheses of the lemma because $d(\mathcal{P}') \geqslant 1$). Let $\mathcal{Q}$ be the set of blocks in $\mathcal{P}'$ which intersect B_j and let $\mathcal{P}^* = (\mathcal{P}' \cup \{B_j\}) \setminus \mathcal{Q}$. Note that $\mathcal{P}^*$ is a partial parallel class of $(V, \mathcal{B})$ and that $|\mathcal{Q}| \leqslant |B_j| = k$. Also, because B_j was $\mathcal{P}'$-good, $\tau_1(\mathcal{Q}) = |\mathcal{Q}|$ and $T_1(\mathcal{Q}) \subseteq T_s(\mathcal{P}')$.

Observe that $|\mathcal{P}^* \cap \mathcal{B}_j| = |\mathcal{P}' \cap \mathcal{B}_j| + 1$, $|\mathcal{P}^* \cap \mathcal{B}_i| = s-1$ for each $i \in T_1(\mathcal{Q})$, and $\mathcal{P}^* \cap \mathcal{B}_i = \mathcal{P}' \cap \mathcal{B}_i$ for all $i \in [t] \setminus (T_1(\mathcal{Q}) \cup \{j\})$. Thus $d(\mathcal{P}^*) = d(\mathcal{P}') - 1$ and $\tau_{s-1}(\mathcal{P}^*) \leqslant \tau_{s-1}(\mathcal{P}') + k + 1$. Any block in $\mathcal{B}$ that was $\mathcal{P}'$-good but is $\mathcal{P}^*$-bad must intersect one of the at most $ks - k + 1$ blocks in $\{B_j\} \cup \bigcup_{i \in T_1(\mathcal{Q})} (\mathcal{P}^* \cap \mathcal{B}_i)$. For each $i \in T_0(\mathcal{P}^*) \cup \cdots \cup T_{s-2}(\mathcal{P}^*)$, at most k^2 blocks in $\mathcal{B}_i$ intersect each of these blocks and so, because more than $k^2(ks-k+1)(d(\mathcal{P}')-1)$ blocks in $\mathcal{B}_i$ were $\mathcal{P}'$-good, more than

$$k^2(ks-k+1)(d(\mathcal{P}')-1) - k^2(ks-k+1) = k^2(ks-k+1)(d(\mathcal{P}')-2) = k^2(ks-k+1)(d(\mathcal{P}^*)-1)$$

blocks in $\mathcal{B}_i$ are $\mathcal{P}^*$-good. Thus we can apply our inductive hypothesis to $\mathcal{P}^*$ to establish the existence of a partial parallel class $\mathcal{P}''$ of $(V, \mathcal{B})$ such that $\tau_{s-1}(\mathcal{P}'') \leqslant (k+1)d(\mathcal{P}^*) + \tau_{s-1}(\mathcal{P}^*)$ and $\tau_s(\mathcal{P}'') = t - \tau_{s-1}(\mathcal{P}'')$. The proof is now complete by observing that

$$\tau_{s-1}(\mathcal{P}'') \leqslant (k+1)d(\mathcal{P}^*) + \tau_{s-1}(\mathcal{P}^*) \leqslant (k+1)(d(\mathcal{P}')-1) + \tau_{s-1}(\mathcal{P}') + k + 1 = (k+1)d(\mathcal{P}') + \tau_{s-1}(\mathcal{P}').$$

$\square$

Theorem 4. *Let k and λ be fixed positive integers such that $k \geqslant 2\lambda + 1$ and let $s = \lfloor \frac{k-1}{\lambda} \rfloor$. For each real number $\epsilon > 0$, there is an integer v_0 such that, for each integer $v \geqslant v_0$, any cyclic (v, k, λ)-design with t orbits has a partial parallel class that contains $s-1$ blocks from each of at most ϵt orbits and contains s blocks from each other orbit.*

Proof. Note that $s \geqslant 2$ by our hypotheses. We may assume that $\epsilon < \frac{1}{4k^2}$. Let $\epsilon^* = \frac{\epsilon}{2(k+1)s}$. Let $(V, \mathcal{B})$ be a cyclic (v, k, λ)-design with orbits $\mathcal{B}_1, \ldots, \mathcal{B}_t$ and suppose that m of these orbits are full. Throughout this proof, we will tacitly assume v is sufficiently large whenever necessary and will use asymptotic notation with respect to this regime. Note that $t = \frac{\lambda(v-1)}{k(k-1)} + O(1)$ by Lemma 3(ii) and hence $t = \Theta(v)$. By Lemma 5 there is a partial parallel class $\mathcal{P}$ of $(V, \mathcal{B})$ such that $T_0(\mathcal{P})$ contains at most $\epsilon^* m \leqslant \epsilon^* t$ indices of full orbits and every other index of a full orbit is in $T_s(\mathcal{P})$. Let

$$R = \{i \in [t] : \mathcal{B}_i \text{ contains at least } \tfrac{1}{2}st \ \mathcal{P}\text{-bad blocks}\}.$$

A block in $\mathcal{B}$ is $\mathcal{P}$-bad if and only if it intersects at least two blocks in $\mathcal{P} \cap \mathcal{B}_i$ for some $i \in T_s(\mathcal{P})$. At most $k^2\lambda\binom{s}{2}$ blocks of $\mathcal{B}$ intersect at least two blocks in $\mathcal{P} \cap \mathcal{B}_i$ for each $i \in T_s(\mathcal{P})$, and so it follows that at most $k^2\lambda\binom{s}{2}\tau_s(\mathcal{P}) \leqslant k^2\lambda\binom{s}{2}t$ blocks in $\mathcal{B}$ are $\mathcal{P}$-bad. Thus, by the definition of R, we have $|R| \leqslant k^2 s\lambda$.

We can greedily choose a partial parallel class $\mathcal{R}$ in $(V, \mathcal{B})$ such that $|\mathcal{R} \cap \mathcal{B}_i| = s$ for each $i \in R$ and $\mathcal{R} \cap \mathcal{B}_i = \emptyset$ for each $i \in [t] \setminus R$. To see this, suppose that $x < s|R| \leqslant k^2 s^2 \lambda$ blocks of the class have already been chosen and note that, for each $i \in R$, at most k^2 of blocks in $\mathcal{B}_i$ intersect each already chosen block and

$$|\mathcal{B}_i| \geqslant \tfrac{v}{k} \gg k^4 s^2 \lambda > k^2 x.$$

Thus we can indeed choose a suitable $\mathcal{R}$ greedily.

Now let

$$Q = \{i \in [t] \setminus R : \text{some block in } \mathcal{P} \cap \mathcal{B}_i \text{ intersects some block in } \mathcal{R}\}.$$

Observe that $ks|R| \leqslant k^3 s^2 \lambda$ vertices in V are in a block in $\mathcal{R}$ and hence $|Q| \leqslant k^3 s^2 \lambda$.

Let $\mathcal{P}' = \mathcal{R} \cup \bigcup_{i \in [t] \setminus Q} (\mathcal{P} \cap \mathcal{B}_i)$ and note that $\mathcal{P}'$ is a partial parallel class in $(V, \mathcal{B})$. So $T_s(\mathcal{P}') = (T_s(\mathcal{P}) \cup R) \setminus Q$ and $T_0(\mathcal{P}') = [t] \setminus T_s(\mathcal{P}')$. Thus $\tau_1(\mathcal{P}') = \cdots = \tau_{s-1}(\mathcal{P}') = 0$ and $\tau_0(\mathcal{P}') \leqslant \tau_0(\mathcal{P}) + |Q|$. Furthermore, $T_0(\mathcal{P})$ contains at most $\epsilon^* t$ indices of full orbits and, by Lemma 3(i), at most $2\lambda\sqrt{k}$ indices of short orbits. From this it follows that

$$d(\mathcal{P}') = (s-1)\tau_0(\mathcal{P}') \leqslant (s-1)(\tau_0(\mathcal{P}) + |Q|) < \frac{\epsilon t}{2(k+1)} + O(1) \ll \frac{\epsilon t}{k+1}. \tag{1}$$

Any block in $\mathcal{B}$ that was $\mathcal{P}$-good but is $\mathcal{P}'$-bad must intersect two of the s blocks in $\mathcal{P}' \cap \mathcal{B}_i$ for some $i \in R$. For each $i \in R$, at most $k^2\lambda\binom{s}{2}$ blocks in $\mathcal{B}$ intersect two of the blocks in $\mathcal{P}' \cap \mathcal{B}_i$. So at most $k^2\lambda\binom{s}{2}|R| \leqslant k^4 s \lambda^2 \binom{s}{2}$ blocks in $\mathcal{B}$ were $\mathcal{P}$-good but are $\mathcal{P}'$-bad. Thus, for each $i \in T_0(\mathcal{P}')$, because $i \notin R$ and hence less than $\frac{1}{2}st$ blocks in $\mathcal{B}_i$ were $\mathcal{P}$-bad, the number of $\mathcal{P}'$-bad blocks in $\mathcal{B}_i$ is less than $\frac{1}{2}st + k^4 s \lambda^2 \binom{s}{2}$. Now $t \leqslant \frac{\lambda(v-1)}{k(k-1)} + 2\lambda\sqrt{k}$ by Lemma 3(ii) and hence $st \leqslant \frac{v}{k} + O(1)$. So, since $|\mathcal{B}_i| \geqslant \frac{v}{k}$, more than $\frac{v}{k} - \frac{1}{2}st - k^4 s\lambda^2\binom{s}{2} \geqslant \frac{1}{2}st - O(1)$ blocks in $\mathcal{B}_i$ are $\mathcal{P}'$-good. Thus $\mathcal{P}'$ satisfies the conditions of Lemma 6 because

$$k^2(ks - k + 1)(d(\mathcal{P}') - 1) < \epsilon k^2 st < \tfrac{1}{4}st \ll \tfrac{1}{2}st - O(1)$$

where the first inequality follows by (1) because $ks - k + 1 < s(k+1)$ and the second follows because $\epsilon < \frac{1}{4k^2}$. Thus, by applying Lemma 6 to $\mathcal{P}'$, there is a partial parallel class $\mathcal{P}''$ of $(V, \mathcal{B})$ such that $\tau_s(\mathcal{P}'') = t - \tau_{s-1}(\mathcal{P}'')$ and

$$\tau_{s-1}(\mathcal{P}'') \leqslant (k+1)d(\mathcal{P}') < \epsilon t$$

where the last inequality follows by (1). $\square$

Note that in the special case where λ divides $k-1$, the partial parallel class given by Theorem 4 uses all but at most $\epsilon k t + 1$ points of the design.

Proof of Theorem 3 This follows directly from Theorem 4, noting that $s \geqslant 2$ because $k \geqslant 2\lambda + 1$. $\square$

4 Concluding remarks

A (v, k, λ)-DDF necessarily has $1 \leqslant \lambda \leqslant k-1$ apart from the trivial case of a (k, k, k)-DDF (see [5]). Theorem 3 requires $1 \leqslant \lambda \leqslant (k-1)/2$. It is natural to ask whether it is possible to relax this condition. We make the following conjecture.

Conjecture 3. *Let k and λ be fixed positive integers such that $k \geqslant \lambda + 1$. There exists an integer v_0 such that, for any cyclic (v, k, λ)-design with $v \geqslant v_0$, it is always possible to choose one block from each block orbit so that the chosen blocks are pairwise disjoint.*

Compared with Conjecture 2, Conjecture 3 is stated for sufficiently large v. This is from the observation that the union of λ copies of a $(k(k-1)+1, k, 1)$-CDF forms a $(k(k-1)+$

$1, k, \lambda)$-CDF which yields a cyclic $(k(k-1)+1, k, \lambda)$-design without short orbits. Note that a $(k(k-1)+1, k, 1)$-CDF is often called a *cyclic difference set* (see [2]) and it generates a symmetric design, any two blocks of which must intersect in one point. Thus the resulting cyclic $(k(k-1)+1, k, \lambda)$-design cannot be generated by a DDF.

Actually Novák made a stronger conjecture on cyclic STS(v) than Conjecture 1 in 1974. A $(v, 3, 1)$-DDF for $v \equiv 1 \pmod 6$ is called *symmetric* if its base blocks can be chosen in such a way that for any nonzero x of $\mathbb{Z}_v$, at most one of x and its complement $v - x$ occurs in the base blocks and no base block contains zero.

Conjecture 4. (Novák, 1974) [16] *Every cyclic STS*(v) *with* $v \equiv 1 \pmod 6$ *is generated by a symmetric* $(v, 3, 1)$*-DDF.*

So far it is only known that Conjecture 4 holds for all $v \equiv 1 \pmod 6$ and $v \leqslant 61$ (see [10, Theorem 22.3]).

Finally we remark that in a recent paper [4] a new concept of "doubly disjoint difference family" was introduced to establish a composition construction for resolvable difference families. Roughly speaking, if we take $k = 3$ and $\lambda = 1$ in Theorem 4, then the induced cyclic difference family "almost" forms a doubly disjoint difference family.

Acknowledgments

Research for this paper was carried out while the first and third authors were visiting Monash University. They express their sincere thanks to the School of Mathematics at Monash University for its kind hospitality.

References

[1] R.J.R. Abel and M. Buratti, Difference families, in: C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs (2nd Edition), CRC Press, Boca Raton, FL, 2006, 392–410.

[2] L.D. Baumert, Cyclic Difference Sets, Springer, Berlin, 1971.

[3] T. Beth, D. Jungnickel, and H. Lenz, Design Theory, Cambridge University Press, Cambridge, UK, 1999.

[4] S. Bonvicini, M. Buratti, M. Garonzi, G. Rinaldi, and T. Traetta, The first families of highly symmetric Kirkman Triple Systems whose orders fill a congruence class, arXiv: 2012.02668.

[5] M. Buratti, On disjoint $(v, k, k-1)$ difference families, Des. Codes Cryptogr., 87 (2019), 745–755.

[6] M. Buratti and D. Ghinelli, On disjoint $(3t, 3, 1)$ cyclic difference families, J. Stat. Plann. Inference, 140 (2010), 1918–1922.

[7] M. Buratti and A. Pasotti, Combinatorial designs and the theorem of Weil on multiplicative character sums, Finite Fields Appl., 15 (2009), 332–344.

[8] K. Chen and L. Zhu, Existence of $(q, 6, 1)$ difference families with q a prime power, Des. Codes Crypt., 15 (1998), 167–174.

[9] K. Chen and L. Zhu, Existence of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, J. Combin. Des., 7 (1999), 21–30.

[10] C.J. Colbourn and A. Rosa, Triple Systems, Oxford University Press, Oxford, 1999.

[11] J.H. Dinitz and P. Rodney, Disjoint difference families with block size 3, Util. Math., 52 (1997), 153–160.

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

[13] S. Ehard, S. Glock, and F. Joos, A rainbow blow-up lemma for almost optimally bounded edge-colourings, arXiv:1907.09950 (2019).

[14] R.N. Karasev and F.V. Petrov, Partitions of nonzero elements of a finite field into pairs, Israel Journal of Mathematics, 192 (2012), 143–156.

[15] E. Köhler, k-difference-cycles and the construction of cyclic t-designs, in: Geometries and Groups, in: Lecture Notes in Math., Springer-Verlag, Berlin, 893 (1981), 195–203.

[16] J. Novák, A note on disjoint cyclic Steiner triple systems, in: Recent Advances in Graph Theory (Proc. Symp. Prague 1974), Academia, Praha, 1975, 439–440.

[17] N. Pippenger and J. Spencer, Asymptotic behavior of the chromatic index for hypergraphs, J. Combin. Theory Ser. A, 51 (1989), 24–42.

[18] D.R. Stinson, Combinatorial Designs: Constructions and Analysis, Berlin, Heidelberg, New York: Springer, 2004.

[19] D. Wu, J. Yang, and B. Huang, The existence of $(v, 4, 1)$ disjoint difference families with v a prime power, Acta Math. Sin. (Engl. Ser.), 24 (2008), 643–648.