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

Tao Feng

Department of Mathematics
Beijing Jiaotong University

Joint work with Daniel Horsley and Xiaomiao Wang
Cyclic 2-designs

▶ A \((v, k, \lambda)\)-design is said to be cyclic if it admits an automorphism consisting of a cycle of length \(v\).
▶ A cyclic \((v, 3, 1)\)-design is called a cyclic Steiner triple system.
Cyclic 2-designs

- A \((v, k, \lambda)\)-design is said to be cyclic if it admits an automorphism consisting of a cycle of length \(v\).
- A cyclic \((v, 3, 1)\)-design is called a cyclic Steiner triple system.
- For example: a cyclic STS\((13)\):

<table>
<thead>
<tr>
<th>Block orbit 1</th>
<th>Block orbit 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>{0, 1, 4}, {1, 2, 5}, {2, 3, 6}, {3, 4, 7}, {4, 5, 8}, {5, 6, 9}, {6, 7, 10}, {7, 8, 11}, {8, 9, 12}, {0, 9, 10}, {1, 10, 11}, {2, 11, 12}, {0, 3, 12};</td>
<td></td>
</tr>
<tr>
<td>{0, 2, 7}, {1, 3, 8}, {2, 4, 9}, {3, 5, 10}, {4, 6, 11}, {5, 7, 12}, {0, 6, 8}, {1, 7, 9}, {2, 8, 10}, {3, 9, 11}, {4, 10, 12}, {0, 5, 11}, {1, 6, 12}.</td>
<td></td>
</tr>
</tbody>
</table>
Cyclic 2-designs

- A \((v, k, \lambda)\)-design is said to be cyclic if it admits an automorphism consisting of a cycle of length \(v\).
- A cyclic \((v, 3, 1)\)-design is called a cyclic Steiner triple system.
- For example: a cyclic STS(13):

  block orbit 1  \{0, 1, 4\}, \{1, 2, 5\}, \{2, 3, 6\}, \{3, 4, 7\}, \{4, 5, 8\}, \{5, 6, 9\},
  \{6, 7, 10\}, \{7, 8, 11\}, \{8, 9, 12\}, \{0, 9, 10\}, \{1, 10, 11\},
  \{2, 11, 12\}, \{0, 3, 12\};

  block orbit 2  \{0, 2, 7\}, \{1, 3, 8\}, \{2, 4, 9\}, \{3, 5, 10\}, \{4, 6, 11\}, \{5, 7, 12\},
  \{0, 6, 8\}, \{1, 7, 9\}, \{2, 8, 10\}, \{3, 9, 11\}, \{4, 10, 12\}, \{0, 5, 11\},
  \{1, 6, 12\}.

- The blocks of a cyclic \((v, k, \lambda)\)-design can be partitioned into orbits under \(\mathbb{Z}_v\). Choose any fixed block from each orbit and then call them base blocks.
Novák’s conjecture on cyclic Steiner triple systems

Conjecture (Novák, 1974)

For any cyclic $\text{STS}(v)$ 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.

---


Novák’s conjecture on cyclic Steiner triple systems

Conjecture (Novák, 1974)

For any cyclic STS($v$) 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.

Novák’s Conjecture is widely believed to be true but not much progress has been made on it (see also Remark 16.22 in \(^a\) or Work point 22.5.2 in \(^b\)).

---


Novák’s conjecture on cyclic Steiner triple systems

Conjecture (Novák, 1974)

For any cyclic STS$(v)$ 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.

- Novák’s Conjecture is widely believed to be true but not much progress has been made on it (see also Remark 16.22 in $^a$ or Work point 22.5.2 in $^b$).
- It is known that Novák’s Conjecture holds for all $v \equiv 1 \pmod{6}$ and $v \leq 61$.

---


Cyclic difference families

- A \((v, k, \lambda)\)-cyclic difference family (CDF) 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 \(\lambda\) times. It consists of \(\lambda(v - 1)/(k(k - 1))\) base blocks.
Cyclic difference families

- A $(v, k, \lambda)$-cyclic difference family (CDF) 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 $\lambda$ times. It consists of $\lambda(v - 1)/(k(k - 1))$ base blocks.

- A $(v, k, \lambda)$-CDF $\mathcal{F}$ $\Rightarrow$ a cyclic $(v, k, \lambda)$-design with block-multiset

$$dev\mathcal{F} := \{F + t : F \in \mathcal{F}, t \in \mathbb{Z}_v\}.$$
Cyclic difference families

▶ A $(v, k, \lambda)$-cyclic difference family (CDF) 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 $\lambda$ times. It consists of $\lambda(v - 1)/(k(k - 1))$ base blocks.

▶ A $(v, k, \lambda)$-CDF $\mathcal{F}$ $\Rightarrow$ a cyclic $(v, k, \lambda)$-design with block-multiset

$$dev \mathcal{F} := \{F + t : F \in \mathcal{F}, t \in \mathbb{Z}_v\}.$$ 

The converse is usually not true. But when $\gcd(v, k) = 1$, $\mathcal{F}$ is a $(v, k, \lambda)$-CDF $\Leftrightarrow$ $dev \mathcal{F}$ is a cyclic $(v, k, \lambda)$-design.
Disjoint difference families

- A \((v, k, \lambda)\)-CDF is said to be disjoint and written as a \((v, k, \lambda)\)-DDF when its base blocks are mutually disjoint.
Disjoint difference families

- A $(v, k, \lambda)$-CDF is said to be disjoint and written as a $(v, k, \lambda)$-DDF when its base blocks are mutually disjoint.

Conjecture (Novák, 1974)

Every cyclic $STS(v)$ with $v \equiv 1 \pmod{6}$ is generated by a $(v, 3, 1)$-DDF.
Disjoint difference families

- A \((v, k, \lambda)\)-CDF is said to be disjoint and written as a \((v, k, \lambda)\)-DDF when its base blocks are mutually disjoint.

Conjecture (Novák, 1974)

Every cyclic STS\((v)\) with \(v \equiv 1 \pmod{6}\) is generated by a \((v, 3, 1)\)-DDF.

Remark

Dinitz and Rodney \(^a\) 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 \(B_i + t_i\).

Karasev and Petrov’s Theorem

Theorem

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

1. $\forall i < j \ |X_i - X_j| \leq 2d$,  
2. $\forall i \ |T_i| \geq (m - 1)d + 1$,

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 $^a$.

---

Karasev and Petrov’s Theorem

Theorem

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

1. $\forall i < j \ |X_i - X_j| \leq 2d$,
2. $\forall i \ |T_i| \geq (m - 1)d + 1$,

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 $^a$.

---


- Apply the above theorem with $m = (p - 1)/6$ and $d = 5$, where $p \equiv 1 \pmod{6}$ is a prime.
Application of Karasev and Petrov’s Theorem

Theorem

Let $k \geq 2$ and $p$ be a prime. Every cyclic $(p, k, 1)$-design is generated by a $(p, k, 1)$-DDF \footnote{T. Feng, D. Horsley, and X. Wang, Novák’s conjecture on cyclic Steiner triple systems and its generalization, arXiv:2001.06995.}. 
Known results on cyclic $(p, k, 1)$-design with $p$ a prime

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

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

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

---

\(^c\)M. Buratti, Constructions for $(q, k, 1)$ difference families with $q$ a prime power and $k = 4, 5$, Discrete Math. 138 (1995), 169–175.


\(^f\)R.M. Wilson, Cyclotomy and difference families in elementary abelian groups, J. Number Theory, 4 (1972), 17–47.
A generalization of Novák’s conjecture

Conjecture 1

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.
A generalization of Novák’s conjecture

Conjecture 1

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 above conjecture, if true, would reduce the existence of \((v, k, 1)\)-DDFs to the existence of \((v, k, 1)\)-CDFs.
A generalization of Novák’s conjecture

Conjecture 1

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 above conjecture, if true, would reduce the existence of \((v, k, 1)\)-DDFs to the existence of \((v, k, 1)\)-CDFs.

Applications of DDFs

Frequency hopping sequences, self-synchronising codes, splitting A-codes, secret sharing schemes with cheater detection, algebraic manipulation detection codes, and high-rate quasi-cyclic codes \(^a\).

\(^a\)S. Ng, M.B. Paterson, Disjoint difference families and their applications, Des. Codes Cryptogr., 78 (2016), 103–127.
Sketch of the proof on Karasev and Petrov’s Theorem

Theorem (Karasev and Petrov)

Let \((md)!/(d!)^m \neq 0\) in \(\mathbb{F}\) and

$$\forall i < j \ |X_i - X_j| \leq 2d, \ \forall i \ |T_i| \geq (m - 1)d + 1.$$  

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.
Sketch of the proof on Karasev and Petrov’s Theorem

Theorem (Karasev and Petrov)
Let \((md)!/(d!)^m \neq 0\) in \(\mathbb{F}\) and

\[
\forall i < j \ |X_i - X_j| \leq 2d, \quad \forall i \ |T_i| \geq (m - 1)d + 1.
\]

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.

▶ For \(1 \leq i < j \leq m\), let \(x_i \in X_i\) and \(x_j \in X_j\).
Sketch of the proof on Karasev and Petrov's Theorem

Theorem (Karasev and Petrov)

Let \((md)!/(d!)^m \neq 0\) in \(\mathbb{F}\) and

\[
\forall i < j \quad |X_i - X_j| \leq 2d, \quad \forall i \quad |T_i| \geq (m - 1)d + 1.
\]

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.

- For \(1 \leq i < j \leq m\), let \(x_i \in X_i\) and \(x_j \in X_j\).
- Then \(x_i + t_i \neq x_j + t_j \Rightarrow x_i - x_j \neq t_j - t_i\).
Sketch of the proof on Karasev and Petrov’s Theorem

Theorem (Karasev and Petrov)

Let \((md)!/(d!)^m \neq 0\) in \(\mathbb{F}\) and

\[
\forall i < j \ |X_i - X_j| \leq 2d, \quad \forall i \ |T_i| \geq (m - 1)d + 1.
\]

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.

- For \(1 \leq i < j \leq m\), let \(x_i \in X_i\) and \(x_j \in X_j\).
- Then \(x_i + t_i \neq x_j + t_j \Rightarrow x_i - x_j \neq t_j - t_i\).
- Set \(X_{ij} = X_i - X_j\).
Sketch of the proof on Karasev and Petrov’s Theorem

Theorem (Karasev and Petrov)

Let \((md)!/(d!)^m \neq 0\) in \(\mathbb{F}\) and

\[
\forall i < j \ |X_i - X_j| \leq 2d, \quad \forall i \ |T_i| \geq (m - 1)d + 1.
\]

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.

- For \(1 \leq i < j \leq m\), let \(x_i \in X_i\) and \(x_j \in X_j\).
- Then \(x_i + t_i \neq x_j + t_j \Rightarrow x_i - x_j \neq t_j - t_i\).
- Set \(X_{ij} = X_i - X_j\).
- Write \(f(t_1, \ldots, t_m) = \prod_{1 \leq i < j \leq m} \prod_{x \in X_{ij}} (t_i - t_j - x)\).
Sketch of the proof on Karasev and Petrov’s Theorem

**Theorem (Karasev and Petrov)**

Let \((md)!/(d!)^m \neq 0\) in \(\mathbb{F}\) and

\[
\forall i < j \quad |X_i - X_j| \leq 2d, \quad \forall i \quad |T_i| \geq (m - 1)d + 1.
\]

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.

- For \(1 \leq i < j \leq m\), let \(x_i \in X_i\) and \(x_j \in X_j\).
- Then \(x_i + t_i \neq x_j + t_j \Rightarrow x_i - x_j \neq t_j - t_i\).
- Set \(X_{ij} = X_i - X_j\).
- Write \(f(t_1, \ldots, t_m) = \prod_{1 \leq i < j \leq m} \prod_{x \in X_{ij}} (t_i - t_j - x)\).
- If \(f\) attain a nonzero value on \(T_1 \times \cdots \times T_m\) then the proof is complete.
Combinatorial Nullstellensatz

Theorem

Assume that

1. a polynomial $f(x_1, x_2, \ldots, x_n)$ over a field $\mathbb{F}$ has degree at most $c_1 + c_2 + \cdots + c_n$, where $c_i$ are non-negative integers, and denote by $C$ the coefficient at $x_1^{c_1} \cdots x_n^{c_n}$ in $f$ (maybe, $C = 0$);

2. $A_1, A_2, \ldots, A_n$ be arbitrary subsets of $\mathbb{F}$ such that $|A_i| = c_i + 1$ for any $i$.

If $C \neq 0$, then there exists a system of representatives $\alpha_i \in A_i$ such that $f(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$. 

Further generalization of Novák’s conjecture

Conjecture 2

Let $k \geqslant \lambda + 1$. There exists an integer $v_0$ such that, for any cyclic $(v, k, \lambda)$-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.
Further generalization of Novák’s conjecture

Conjecture 2

Let \( k \geq \lambda + 1 \). There exists an integer \( v_0 \) such that, for any cyclic \((v, k, \lambda)\)-design with \( v \geq v_0 \), it is always possible to choose one block from each block orbit so that the chosen blocks are pairwise disjoint.

- Compared with Conjecture 1, Conjecture 2 is stated for sufficiently large \( v \).
Further generalization of Novák’s conjecture

Conjecture 2

Let $k \geq \lambda + 1$. There exists an integer $v_0$ such that, for any cyclic $(v, k, \lambda)$-design with $v \geq v_0$, it is always possible to choose one block from each block orbit so that the chosen blocks are pairwise disjoint.

- Compared with Conjecture 1, Conjecture 2 is stated for sufficiently large $v$.

Remark

A $(v, k, \lambda)$-DDF necessarily has $1 \leq \lambda \leq k - 1$ apart from the trivial case of a $(k, k, k)$-DDF \(^a\).

\(^{a}\)M. Buratti, On disjoint $(v, k, k - 1)$ difference families, Des. Codes Cryptogr., 87 (2019), 745–755.
Asymptotic solution

A **partial parallel class** of a \((v, k, \lambda)\)-design is a set of pairwise disjoint blocks.

**Theorem**

Let \( k \geq 2\lambda + 1 \) and let \( s = \left\lfloor \frac{k-1}{\lambda} \right\rfloor \). For each real number \( \epsilon > 0 \), there is an integer \( v_0 \) such that, for each integer \( v \geq v_0 \), any cyclic \((v, k, \lambda)\)-design with \( t \) orbits has a partial parallel class that contains \( s - 1 \) blocks from each of at most \( \epsilon t \) orbits and contains \( s \) blocks from each other orbit.
Asymptotic solution

A partial parallel class of a \((v, k, \lambda)\)-design is a set of pairwise disjoint blocks.

**Theorem**

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

- **Parameter \(s\):**

\[
\frac{(v - 1)/k}{\lambda(v - 1)/k(k - 1)} = \frac{k - 1}{\lambda}.
\]
Sketch of the proof - Preliminaries

- Let $(V, B)$ be a cyclic $(v, k, \lambda)$-design with orbits $B_1, \ldots, B_t$ and suppose that $m$ of these orbits are full.
Sketch of the proof - Preliminaries

Let \((V, \mathcal{B})\) be a cyclic \((v, k, \lambda)\)-design with orbits \(\mathcal{B}_1, \ldots, \mathcal{B}_t\) and suppose that \(m\) of these orbits are full.

Let \(\mathcal{P}\) be a partial parallel class of \((V, \mathcal{B})\). For any nonnegative integer \(a\), 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 define

\[
\tau_a(\mathcal{P}) = |T_a(\mathcal{P})|.
\]
Sketch of the proof - Preliminaries

- Let \((V, \mathcal{B})\) be a cyclic \((v, k, \lambda)\)-design with orbits \(\mathcal{B}_1, \ldots, \mathcal{B}_t\) and suppose that \(m\) of these orbits are full.

- Let \(\mathcal{P}\) be a partial parallel class of \((V, \mathcal{B})\). For any nonnegative integer \(a\), 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 define

\[
\tau_a(\mathcal{P}) = |T_a(\mathcal{P})|.
\]

- **Goal**: find a partial parallel class \(\mathcal{P}''\) of \((V, \mathcal{B})\) such that \(\tau_a(\mathcal{P}'') = 0\) for \(0 \leq a \leq s - 2\), \(\tau_{s-1}(\mathcal{P}'') < \epsilon t\) and \(\tau_s(\mathcal{P}'') = t - \tau_{s-1}(\mathcal{P}'')\).
Sketch of the proof - Two steps

- **STEP 1**: We obtain a partial parallel class $\mathcal{P}$ of $(V, B)$ such that

\[ \tau_0(\mathcal{P}) \leq \epsilon^* t \quad \text{and} \quad \tau_s(\mathcal{P}) = t - \tau_0(\mathcal{P}). \]

So $\mathcal{P}$ contains $s$ blocks from almost every block orbit.
Sketch of the proof - Two steps

► **STEP 1**: We obtain a partial parallel class $\mathcal{P}$ of $(V, B)$ such that

$$\tau_0(\mathcal{P}) \leq \epsilon^* t \quad \text{and} \quad \tau_s(\mathcal{P}) = t - \tau_0(\mathcal{P}).$$

So $\mathcal{P}$ contains $s$ blocks from almost every block orbit.

► **STEP 2**: We then prove that if each orbit of $(V, B)$ contains sufficiently many “good blocks” relative to some partial parallel class, then this class can be modified so that it contains $s$ blocks from almost every orbit and $s - 1$ blocks from each remaining orbit.
Sketch of the proof - Step 1

- Let \( W = \{u_{i,j} : i \in [m], j \in [s]\} \) be a set of vertices disjoint from \( V \).
- Form a \((k + 1)\)-uniform hypergraph \( G \) with vertex set \( V \cup W \) and edge set

\[
\{B \cup \{u_{i,j}\} : B \in \mathcal{B}_i, i \in [m], j \in [s]\}.
\]
Sketch of the proof - Step 1

- Let $W = \{u_{i,j} : i \in [m], j \in [s]\}$ be a set of vertices disjoint from $V$.
- Form a $(k + 1)$-uniform hypergraph $G$ with vertex set $V \cup W$ and edge set

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

- $\delta_G \geq v - k$, $\Delta_G \leq v$, and $\Delta^c_G \leq k + \lambda - 1$. 
Sketch of the proof - Step 1

- By Pippenger and Spencer’s theorem on edge-colouring of $r$-uniform hypergraphs, we shows that $G$ has a proper edge-colouring with $(1 + o(1))v$ colours.
  
  ▶ (Pippenger and Spencer’s Theorem) Every almost regular $r$-uniform hypergraph $G$ with small maximum codegree can be edge-coloured with close to $\Delta_G$ colours.
Sketch of the proof - Step 1

- By Pippenger and Spencer’s theorem on edge-colouring of $r$-uniform hypergraphs, we shows that $G$ has a proper edge-colouring with $(1 + o(1))v$ colours.
  ▶ (Pippenger and Spencer’s Theorem) Every almost regular $r$-uniform hypergraph $G$ with small maximum codegree can be edge-coloured with close to $\Delta_G$ colours.

- Let $C$ be a largest colour class of this colouring and let

$$M = \left\{ i \in [m] : \left| \{ j \in [s] : u_{i,j} \text{ is in an edge in } C \} \right| = s \right\}.$$  

  Then $|M| > (1 - \epsilon^*)m$. 

Sketch of the proof - Step 1

- By Pippenger and Spencer’s theorem on edge-colouring of $r$-uniform hypergraphs, we shows that $G$ has a proper edge-colouring with $(1 + o(1))v$ colours.
  
  ▶ (Pippenger and Spencer’s Theorem) Every almost regular $r$-uniform hypergraph $G$ with small maximum codegree can be edge-coloured with close to $\Delta_G$ colours.

- Let $C$ be a largest colour class of this colouring and let

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

  Then $|M| > (1 - \epsilon^*)m$.

- $C|_M$ gives rise to the required partial parallel class $\mathcal{P}$. 
Sketch of the proof - Step 2

We say that a block \( B \in \mathcal{B} \) is \( \mathcal{P} \)-good if,

1. for each \( i \in T_0(\mathcal{P}) \cup \cdots \cup T_{s-1}(\mathcal{P}) \), \( B \) intersects no block in \( \mathcal{P} \cap B_i \);
2. for each \( i \in T_s(\mathcal{P}) \), \( B \) intersects at most one block in \( \mathcal{P} \cap B_i \).

Careful counting shows that if each orbit of \( (V, \mathcal{B}) \) contains sufficiently many good blocks relative to some partial parallel class, then this class can be modified so that it contains \( s \) blocks from almost every orbit and \( s - 1 \) blocks from each remaining orbit.
Strong Novák’s conjecture on cyclic STSs

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.
Strong Novák’s conjecture on cyclic STSs

- 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 (Novák, 1974)

Every cyclic $\text{STS}(v)$ with $v \equiv 1 \pmod{6}$ is generated by a symmetric $(v, 3, 1)$-DDF.
Strong Novák’s conjecture on cyclic STSs

- 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 (Novák, 1974)

Every cyclic \(\text{STS}(v)\) with \(v \equiv 1 \pmod{6}\) is generated by a symmetric \((v, 3, 1)\)-DDF.

- For example: a cyclic \(\text{STS}(13)\) that implies a \((v, 3, 2)\)-DDF:
  - \(\{0, 1, 4\}, \{1, 2, 5\}, \{2, 3, 6\}, \{3, 4, 7\}, \{4, 5, 8\}, \{5, 6, 9\}, \{6, 7, 10\}, \{7, 8, 11\}, \{8, 9, 12\}, \{0, 9, 10\}, \{1, 10, 11\}, \{2, 11, 12\}, \{0, 3, 12\}\);
  - \(\{0, 2, 7\}, \{1, 3, 8\}, \{2, 4, 9\}, \{3, 5, 10\}, \{4, 6, 11\}, \{5, 7, 12\}, \{0, 6, 8\}, \{1, 7, 9\}, \{2, 8, 10\}, \{3, 9, 11\}, \{4, 10, 12\}, \{0, 5, 11\}, \{1, 6, 12\}\).
Extension of STSs to designs with size four

Theorem

Let \( v \equiv 1 \pmod{6} \). If there exists a symmetric \((\mathbb{Z}_v, 3, 1)\)-DDF, then there exists a \((2v, 2, 4, 1)\)-CDF.
Extension of STSs to designs with size four

Theorem

Let $v \equiv 1 \pmod{6}$. If there exists a symmetric $(\mathbb{Z}_v, 3, 1)$-DDF, then there exists a $(2v, 2, 4, 1)$-CDF.

- Let $\{a_i, b_i, c_i\}, 1 \leq i \leq (v - 1)/6$, be a symmetric $(\mathbb{Z}_v, 3, 1)$-DDF.
Extension of STSs to designs with size four

**Theorem**

Let $v \equiv 1 \pmod{6}$. If there exists a symmetric $(\mathbb{Z}_v, 3, 1)$-DDF, then there exists a $(2v, 2, 4, 1)$-CDF.

- Let $\{a_i, b_i, c_i\}, 1 \leq i \leq (v-1)/6$, be a symmetric $(\mathbb{Z}_v, 3, 1)$-DDF.
- Then

$$\mathcal{F} = \{((0,0), (1,a_i), (1,b_i), (1,c_i)) : 1 \leq i \leq (v-1)/6\}$$

forms a $(2v, 2, 4, 1)$-CDF over $\mathbb{Z}_2 \times \mathbb{Z}_v \cong \mathbb{Z}_{2v}$. 
Conclusion

Conjecture 1

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.

Conjecture 2

Let $k \geq \lambda + 1$. There exists an integer $v_0$ such that, for any cyclic $(v, k, \lambda)$-design with $v \geq v_0$, it is always possible to choose one block from each block orbit so that the chosen blocks are pairwise disjoint.

Conjecture (Novák, 1974)

Every cyclic STS($v$) with $v \equiv 1 \pmod{6}$ is generated by a symmetric $(v, 3, 1)$-DDF.
Thanks for your attention!