Strong External Difference Families

Maura Paterson

Birkbeck
UNIVERSITY OF LONDON

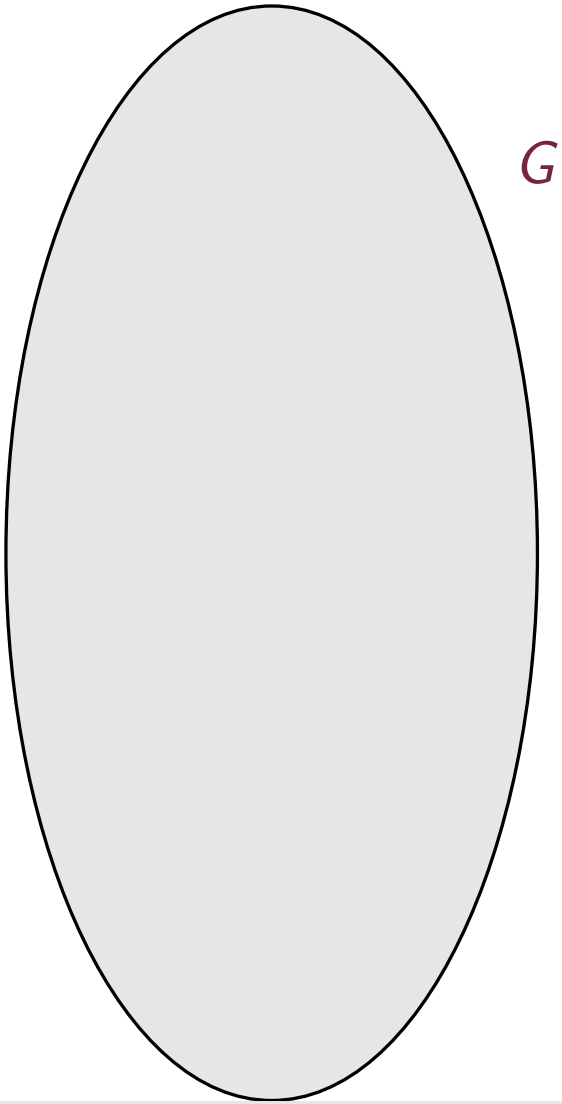
Pythagorean Conference

June 2025

(n, m, k, λ)-Strong External Difference Family

[P., Stinson '16]

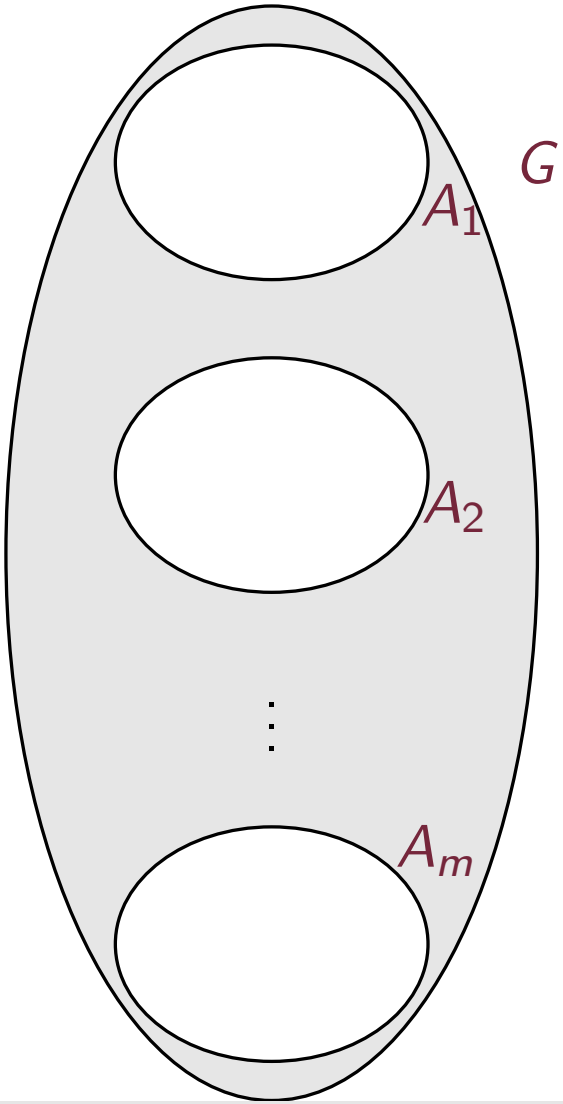
- G abelian group with $|G| = n$



(n, m, k, λ)-Strong External Difference Family

[P., Stinson '16]

- G abelian group with $|G| = n$
- $A_1, A_2, \ldots, A_m$ disjoint k-subsets of G

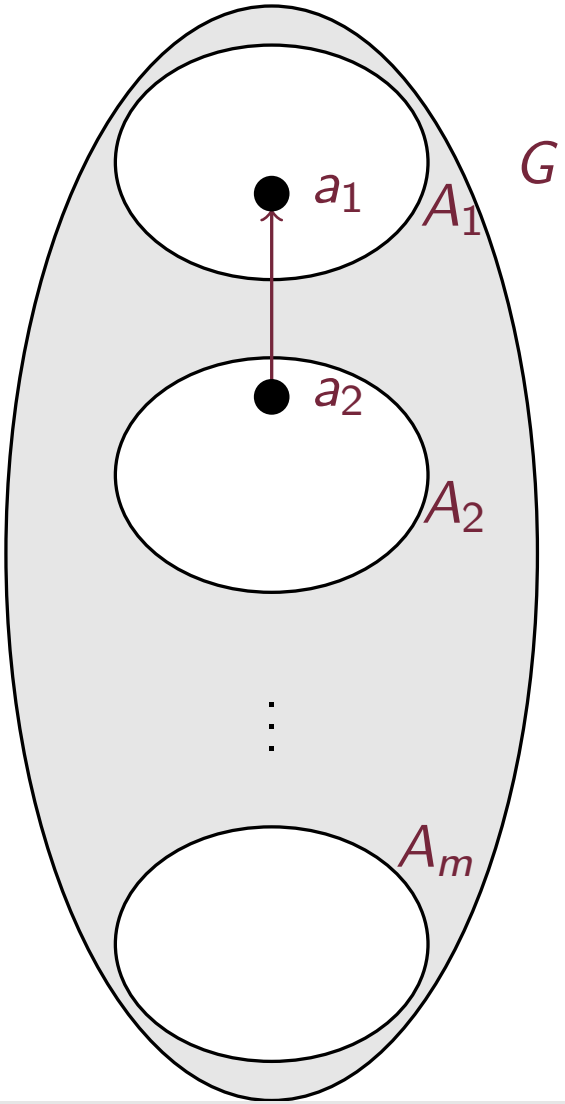


(n, m, k, λ)-Strong External Difference Family

[P., Stinson '16]

- G abelian group with $|G| = n$
- $A_1, A_2, \ldots, A_m$ disjoint k-subsets of G
- require

$$\{a_1 - a_i | a_1 \in A_1, a_i \in A_i \text{ with } i \neq 1\} = \lambda(G \setminus \{0\})$$



(n, m, k, λ)-Strong External Difference Family

[P., Stinson '16]

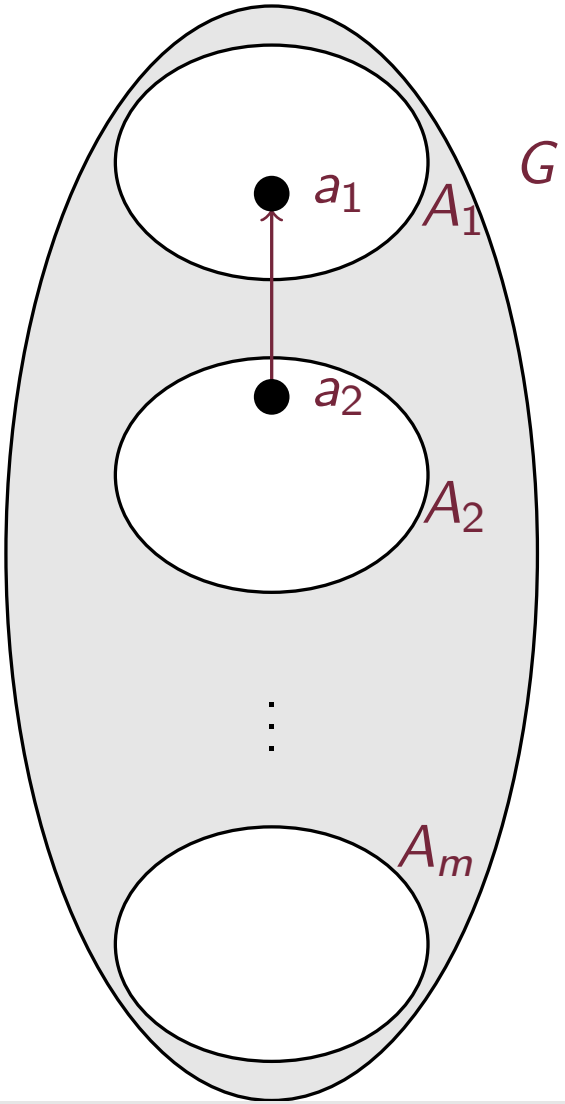
- G abelian group with $|G| = n$
- $A_1, A_2, \ldots, A_m$ disjoint k-subsets of G
- require

$$\{a_1 - a_i | a_1 \in A_1, a_i \in A_i \text{ with } i \neq 1\} = \lambda(G \setminus \{0\})$$

- similarly require

$$\{a_j - a_i | a_j \in A_j, a_i \in A_i \text{ with } i \neq j\} = \lambda(G \setminus \{0\})$$

for $j = 2, 3, \ldots, m$.

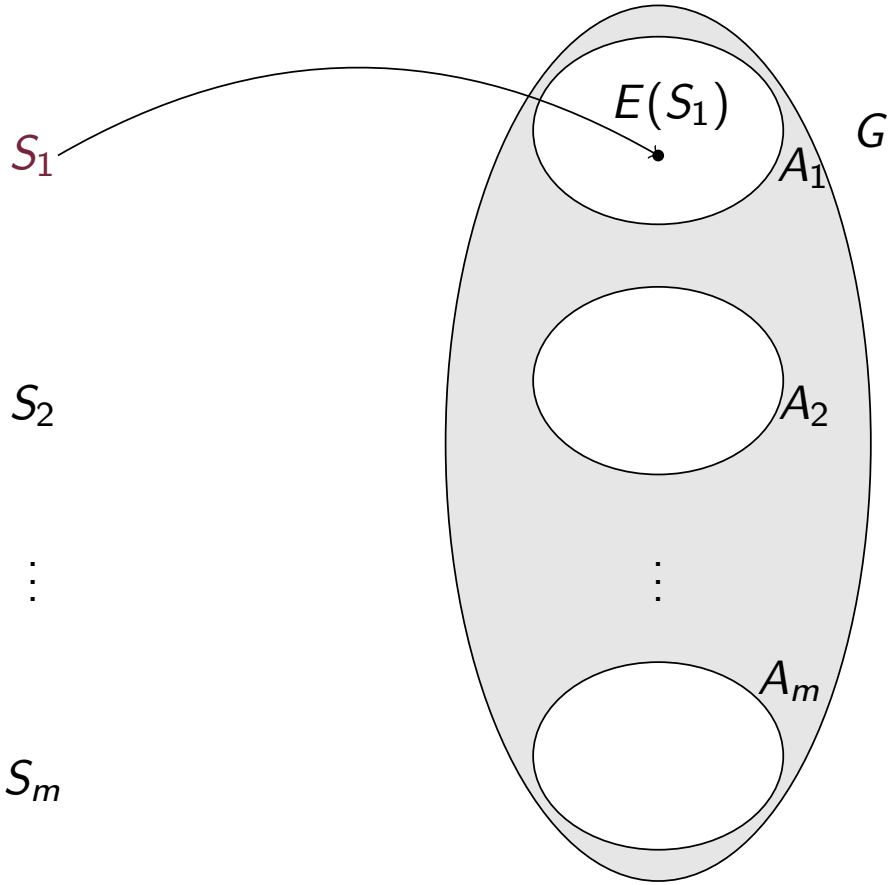


Example: $(10, 2, 3, 1)$-SEDF

- $G = \mathbb{Z}_{10}$
- $A_1 = \{0, 1, 2\}$, $A_2 = \{3, 6, 9\}$

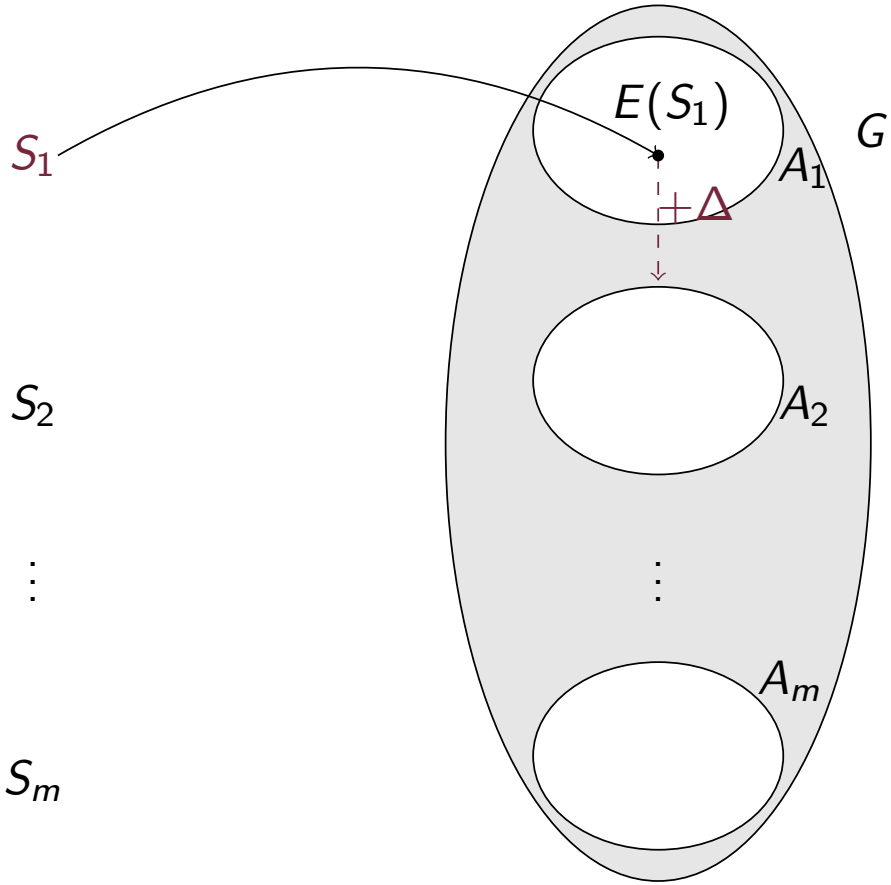
Motivation: strong algebraic manipulation detection code

[Cramer, Dodis, Fehr, Padró, Wichs '08]



Motivation: strong algebraic manipulation detection code

[Cramer, Dodis, Fehr, Padró, Wichs '08]



Limitations when $\lambda = 1$

Theorem ([P., Stinson '16])

A $(n, m, k, 1)$-SEDF exists if and only if $m = 2$ and $n = k^2 + 1$ or $k = 1$ and $m = n$.

Question: Does there exist a strong (n, m, k, λ) external difference family with $k > 1$ and $m > 2$ for some $\lambda > 1$?

Parameters where constructions of $(n, 2, k, \lambda)$-SEDFs are known

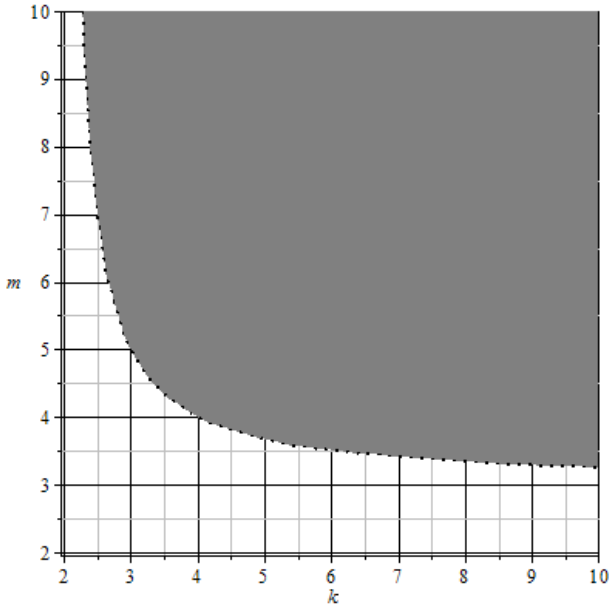
- $(n, m, k, \lambda) = (k^2 + 1, 2, k, 1)$ and $G = \mathbb{Z}_{k^2+1}$
- $(n, m, k, \lambda) = (n, 2, \frac{n-1}{2}, \frac{n-1}{4})$, $n \equiv 1 \pmod 4$ is a prime power
  [Bao, Ji, Wei, Zhang '18]
- $(n, m, k, \lambda) = (q, 2, \frac{q-1}{4}, \frac{q-1}{16})$, where $q = 16t^2 + 1$ is a prime power and $t \in \mathbb{Z}$
- $(n, m, k, \lambda) = (p, 2, \frac{p-1}{6}, \frac{p-1}{36})$, where $p = 108t^2 + 1$ is a prime and $t \in \mathbb{Z}$

Nonexistence when $\lambda > 1$

Theorem ([Huczynska, P. '18])

Let $\lambda \geq 2$. Suppose there exists an (n, m, k, λ)-SEDF with $m \geq 3$ and $k \geq \lambda + 1$. Then the following inequality must hold:

$$\frac{\lambda(k-1)(m-2)}{(\lambda-1)k(m-1)} \leq 1.$$



Character theoretic restrictions

[Martin, Stinson '17]

- $m \neq 3, 4$
- No SEDF exists with n is prime, $m > 2$, $k > 2$.

Character theoretic restrictions

[Martin, Stinson '17]

- $m \neq 3, 4$
- No SEDF exists with n is prime, $m > 2$, $k > 2$.

Question: Does there exist a strong (n, m, k, λ) external difference family with $k > 1$ and $m \geq 5$ for some $\lambda > 1$?

Yes!

[Jedwab, Li '19] [Wen, Yang, Feng '16]

Theorem

There exists a $(243, 11, 22, 20)$*-SEDF in* $\mathbb{Z}_3^5$.

Yes!

[Jedwab, Li '19] [Wen, Yang, Feng '16]

Theorem

There exists a $(243, 11, 22, 20)$*-SEDF in* $\mathbb{Z}_3^5$.

Only known example with $m > 2$!

Remaining parameters with $m > 2$ and $n \leq 10^4$

[Leung, Li, Prabowo '21]

Table 3
Plausible parameter sets for (v, m, k, λ)-SEDFs with $m > 2$ and $v \leq 10^4$.

v	m	k	λ
540	12	42	36
1701	35	40	32
2058	86	22	20
2401	7	280	196
2401	9	240	192
2500	18	105	75
2601	53	40	32
2646	16	138	108
3888	24	156	144
3888	47	78	72
3969	32	112	98
4375	7	540	400
4375	9	405	300
4375	16	270	250
4375	37	108	96
5376	44	100	80
5832	18	294	252
8625	23	280	200
8960	32	238	196
9801	26	308	242

SEDFs in non-abelian groups

Definition (modified)

We require

$$\{a_j a_i^{-1} | a_j \in A_j, a_i \in A_i \text{ with } i \neq j\}$$
$$= \lambda(G \setminus \{e\})$$

for $j = 1, 2, 3, \ldots, m$.

SEDFs in non-abelian groups

Definition (modified)

We require

$$\{a_j a_i^{-1} | a_j \in A_j, a_i \in A_i \text{ with } i \neq j\} = \lambda(G \setminus \{e\})$$

for $j = 1, 2, 3, \ldots, m$.

[Huczynska, Jefferson, Nepšinská '21]

Theorem

For k odd there is a $(k^2 + 1, 2, k, 1)$-SEDF in the dihedral group of order $k^2 + 1$.

Comment on the $m = 2$ case

If

$$\{a_1 {a_2}^{-1} | a_1 \in A_1, a_2 \in A_2\} = \lambda(G \setminus \{e\}),$$

then

$$\{a_2 {a_1}^{-1} | a_1 \in A_1, a_2 \in A_2\} = \lambda(G \setminus \{e\}).$$

Comment on the $m = 2$ case

If

$$\{a_1 {a_2}^{-1} | a_1 \in A_1, a_2 \in A_2\} = \lambda(G \setminus \{e\}),$$

then

$$\{a_2 {a_1}^{-1} | a_1 \in A_1, a_2 \in A_2\} = \lambda(G \setminus \{e\}).$$

Conclusion: when $m = 2$ we only need to check one set of conditions.

Relation to Near-Factorizations

Definition (Near-Factorization)

- G finite group
- $A_1, A_2 \subset G$

(A_1, A_2) is a (k, k)-*near-factorization* of G if

- $|A_1| = |A_2| = k$, $|G| = k^2 + 1$
- $G \setminus \{e\} = A_1 A_2$.

Relation to Near-Factorizations

Definition (Near-Factorization)

- G finite group
- $A_1, A_2 \subset G$

(A_1, A_2) is a (k, k)-*near-factorization* of G if

- $|A_1| = |A_2| = k$, $|G| = k^2 + 1$
- $G \setminus \{e\} = A_1 A_2$.

Observation: A_1, A_2 form a $(k^2 + 1, 2, k, 1)$-SEDF in G if and only if $(A_1, {A_2}^{-1})$ is a (k, k)-near-factorization of G.

A useful property

Definition

- A subset S of a group is *symmetric* if $S = S^{-1}$.
- A near-factorization (A, B) is symmetric if A and B are symmetric.
- An SEDF A_1, A_2 is symmetric if A_1 and A_2 are symmetric.

Proof by pretty picture...

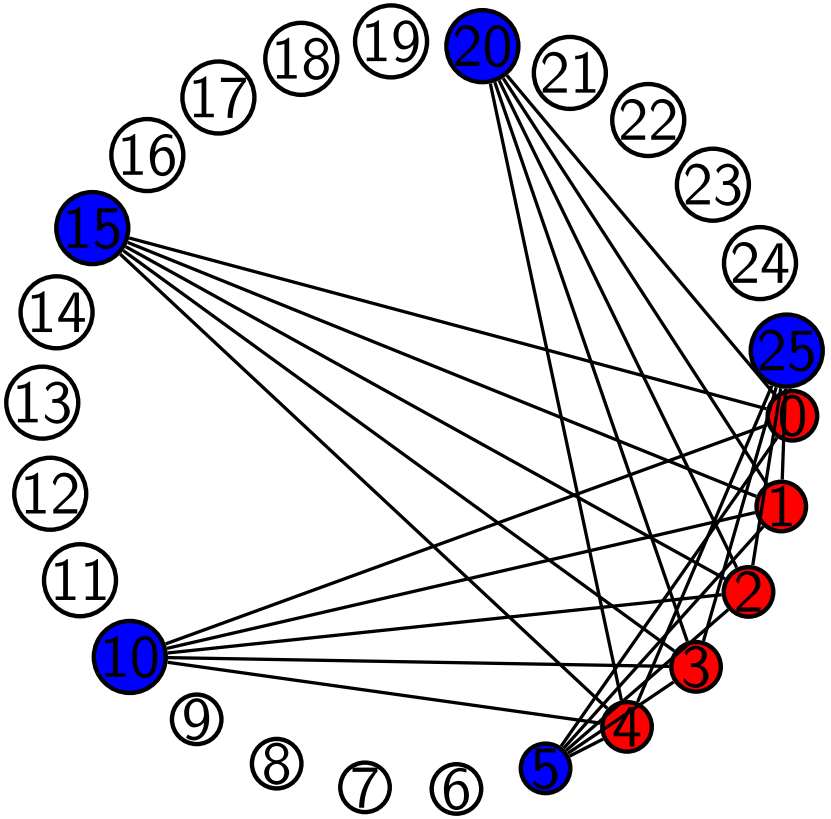
Theorem

If A_1, A_2 is an $(n, m, k, 1) - SEDF$ in an abelian group G, then there exists $g \in G$ for which $g + A_1, g + A_2$ is a symmetric $(n, m, k, 1) - SEDF$.

Proof by pretty picture...

Theorem

If A_1, A_2 is an $(n, m, k, 1) - SEDF$ in an abelian group G, then there exists $g \in G$ for which $g + A_1, g + A_2$ is a symmetric $(n, m, k, 1) - SEDF$.



SEDFs in cyclic groups give SEDFs in dihedral groups

[Pêcher '04] [Kreher, P. Stinson '24]

- For k odd there is a correspondence between symmetric $(k^2 + 1, 2, k, 1)$-SEDFs in $\mathbb{Z}_{k^2+1}$ and those in the dihedral group

$$D_{(k^2+1)/2} = \langle a, b : a^2 = b^{(k^2+1)/2} = abab = e \rangle.$$

$$x \in \mathbb{Z}_{k^2+1} \mapsto a^{(x \mod 2)} b^{(x \mod (k^2+1)/2)}.$$

SEDFs in cyclic groups give SEDFs in dihedral groups

[Pêcher '04] [Kreher, P. Stinson '24]

- For k odd there is a correspondence between symmetric $(k^2 + 1, 2, k, 1)$-SEDFs in $\mathbb{Z}_{k^2+1}$ and those in the dihedral group

$$D_{(k^2+1)/2} = \langle a, b : a^2 = b^{(k^2+1)/2} = abab = e \rangle.$$

$$x \in \mathbb{Z}_{k^2+1} \mapsto a^{(x \mod 2)} b^{(x \mod (k^2+1)/2)}.$$

- The SEDFs in $\mathbb{Z}_{k^2+1}$ are *equivalent* iff the corresponding SEDFs in D_{k^2+1} are equivalent.

Other nonabelian groups

- There are two nonequivalent $(50, 2, 7, 1)$-SEDFs in $D_5 \times C_5$.
- There are two nonequivalent $(50, 2, 7, 1)$-SEDFs in $C_5^2 \rtimes_2 C_2$.

α-valuations

Definition (Graceful labelling)

Let $\mathcal{G}$ be a graph with e edges. A labelling of the vertices with elements of the set $\{0, 1, \ldots, e\}$ is graceful if the set of absolute values of the differences between the labels on the vertices adjacent to each edge is precisely $\{1, 2, \ldots, e\}$.

α-valuations

Definition (Graceful labelling)

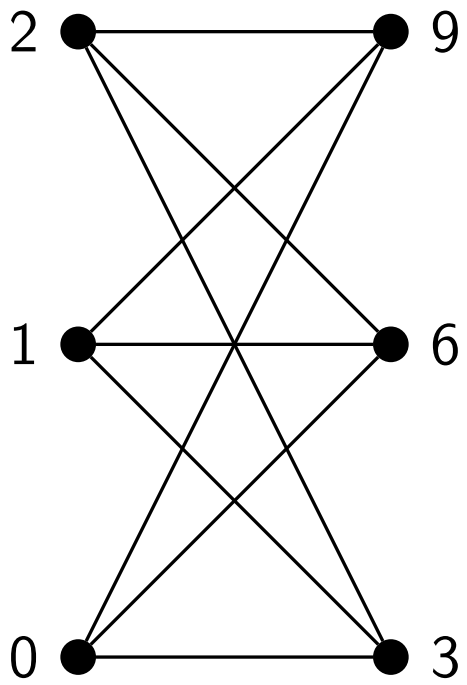
Let $\mathcal{G}$ be a graph with e edges. A labelling of the vertices with elements of the set $\{0, 1, \ldots, e\}$ is graceful if the set of absolute values of the differences between the labels on the vertices adjacent to each edge is precisely $\{1, 2, \ldots, e\}$.

[Rosa '67]

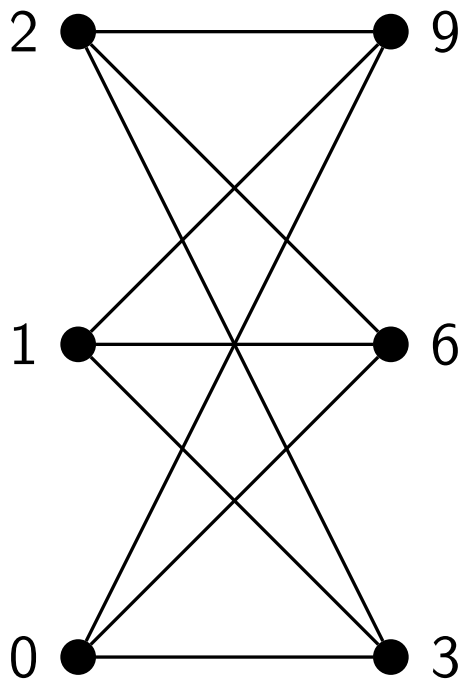
Definition (α-valuation)

A graceful labelling of a graph $\mathcal{G}$ be a graph with e edges is an α-valuation if there exists x with $0 < x < e$ such that each edge is incident with one vertex of label at most x, and one vertex of label greater than x.

Example



Example



Theorem ([P., Stinson '24])

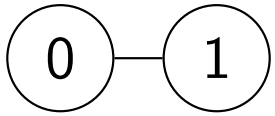
An α-valuation of the complete bipartite graph $K_{k,k}$ implies the existence of a $(k^2+1, 2, k, 1)$-SEDF in $\mathbb{Z}_{k^2+1}$.

α-valuations via blowups

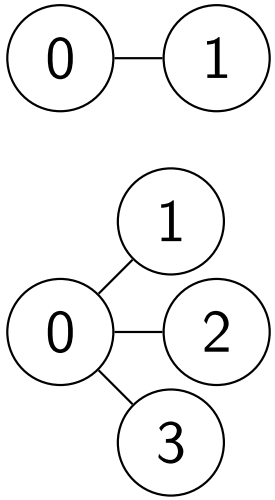
- Start with an α-valuation of a bipartite graph with vertex sets V^{small} and V^{large}.
- Multiply each label by ℓ.
- Replace each vertex of V^{small} with label ℓi by an independent set of size ℓ whose vertices are adjacent to the neighbours of original vertex and have labels $\ell i, \ell i + 1, \ldots, \ell i + (\ell - 1)$.

(Similar process can be applied to blow up the vertices of V^{large}.)
This process yields an α-valuation of the resulting graph.

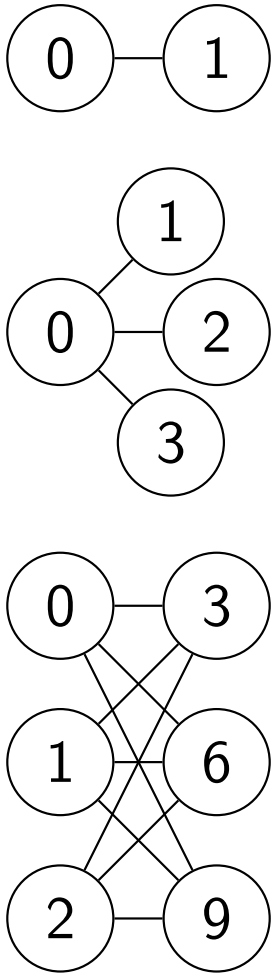
example



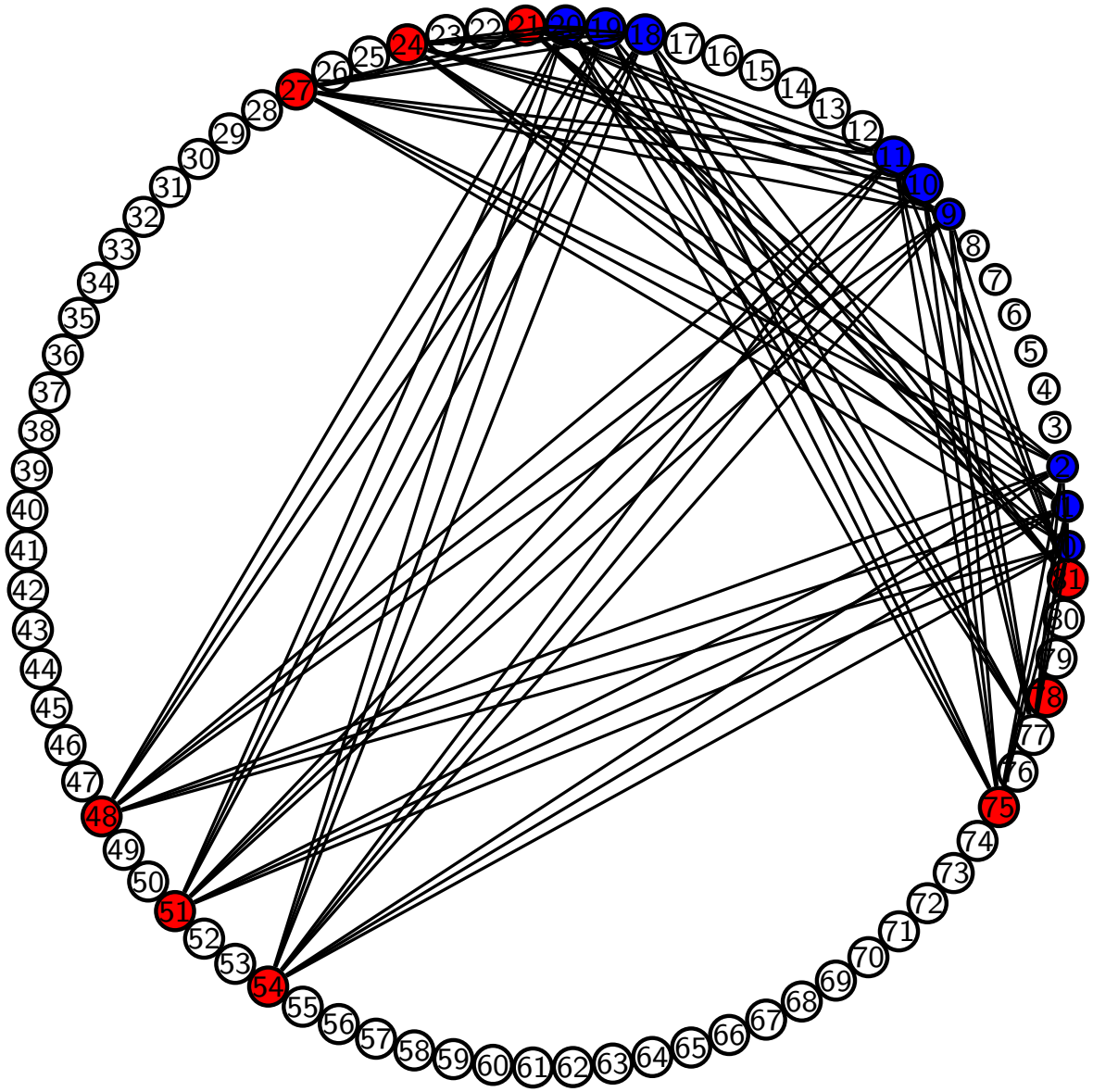
example



example



example


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81

Classification of α-valuations of complete bipartite graphs

Theorem ([Kreher, P., Stinson '25])

Every α-valuation of a complete bipartite graph can be obtained by starting with $K_{1,1}$ with labels 0 and 1, then applying a sequence of blow-up operations.

Classification of α-valuations of complete bipartite graphs

Theorem ([Kreher, P., Stinson '25])

Every α-valuation of a complete bipartite graph can be obtained by starting with $K_{1,1}$ with labels 0 and 1, then applying a sequence of blow-up operations.

[de Bruijn '56]

Classifying SEDFs with $m = 2$, $\lambda = 1$ in cyclic groups.

- Does every SEDF with $m = 2$ and $\lambda = 1$ arise from an α-valuation of a complete bipartite graph?

Classifying SEDFs with $m = 2$, $\lambda = 1$ in cyclic groups.

- Does every SEDF with $m = 2$ and $\lambda = 1$ arise from an α-valuation of a complete bipartite graph?
- No! $\{1, 4, 13, 16\}, \{2, 8, 9, 15\}$
  [Huczynska, Jefferson, Nepšinská '21]

Classifying SEDFs with $m = 2$, $\lambda = 1$ in cyclic groups.

- Does every SEDF with $m = 2$ and $\lambda = 1$ arise from an α-valuation of a complete bipartite graph?
- No! $\{1, 4, 13, 16\}, \{2, 8, 9, 15\}$
  [Huczynska, Jefferson, Nepšinská '21]
- Is every SEDF with $m = 2$ and $\lambda = 1$ equivalent to one that arises from an α-valuation of a complete bipartite graph?

Classifying SEDFs with $m = 2$, $\lambda = 1$ in cyclic groups.

- Does every SEDF with $m = 2$ and $\lambda = 1$ arise from an α-valuation of a complete bipartite graph?
- No! $\{1, 4, 13, 16\}, \{2, 8, 9, 15\}$
  [Huczynska, Jefferson, Nepšinská '21]
- Is every SEDF with $m = 2$ and $\lambda = 1$ equivalent to one that arises from an α-valuation of a complete bipartite graph?
- True for $k \leq 14$.

Thanks for listening!


Maura B. Paterson and Douglas R. Stinson. Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families. *Discrete Mathematics*, 339(12):2891-2906, 2016.


Cramer, Dodis, Fehr, Padró, Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. Eurocrypt 2008.


J. Bao, L. Ji, R. Wei, Y. Zhang. New existence and nonexistence results for strong external difference families. *Discrete Mathematics* 341 (6) 1798–1805 (2018).


S. Huczynska and M.B. Paterson. Existence and non-existence results for strong external difference families. *Discrete Mathematics*, 341(1):87-95, 2018.


W.J. Martin, D.R. Stinson. Some nonexistence results for strong external difference families using character theory. *Bulletin of the ICA*, 80:79–92, (2017).


J. Jedwab, S. Li. Construction and nonexistence of strong external difference families. *J. Algebraic Combin.* 49(1) 21–48 (2019)


J. Wen, M. Yang, K. Feng. The (n, m, k, λ) strong external difference family with $m \geq 5$ exists. https://arxiv.org/abs/1612.09495 (2016)


K.H. Leung, S. Li, T.F. Prabowo. Nonexistence of strong external difference families in abelian groups of order being product of at most three primes. *JCT A*, (178) 105338, (2021)


S. Huczynska, C. Jefferson and S. Nepšinská. Strong external difference families in abelian and non-abelian groups. *Cryptography and Communications* 13, 331–341 (2021).


A. Pêcher. Cayley partitionable graphs and near-factorizations of finite groups. *Discrete Mathematics* 276, 95–311 (2004).


Donald L. Kreher, Maura B. Paterson, Douglas R. Stinson. Near-factorizations of dihedral groups. `https://arxiv.org/abs/2411.15884` (2024).


A. Rosa. On certain valuations of the vertices of a graph. P. Rosenstiehl (Ed.), Theory of Graphs, International Symposium, Rome, 1966, 349–355 (1967)


M.B. Paterson and D.R. Stinson. Circular external difference families, graceful labellings and cyclotomy. *Discrete Mathematics*, 347(10), 2024.


D.L. Kreher, M.B. Paterson and D.R. Stinson. Strong External Difference Families and Classification of α-valuations. *Journal of Combinatorial Designs* (to appear).


N.G. de Bruijn. On number systems. *Nieuw Archief voor Wiskunde* 3, 15–17. (1956)