Near factorization of finite groups

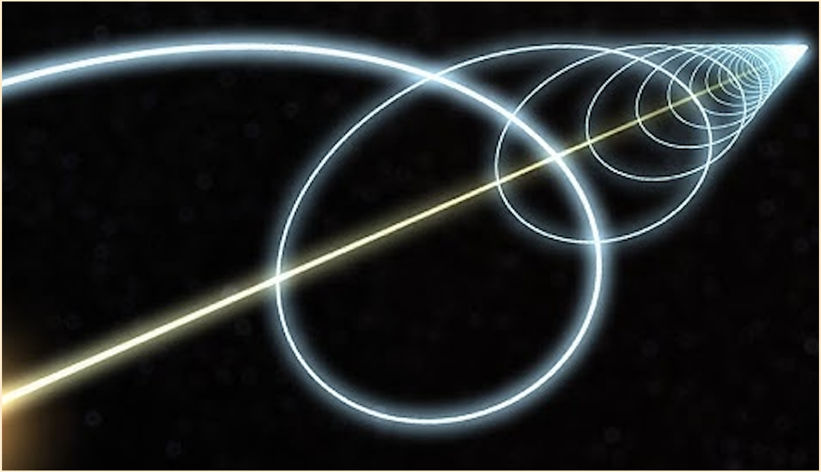
Donald L. Kreher

Department of Mathematical Sciences
Michigan Technological University

Collaborators

Shuxing Li, Bill Martin,
Maura Paterson, Doug Stinson

The 5th Pythagorean conference,
Kalamata, Greece, June 1-6, 2025



Definition

- Let $(G, \cdot)$ be a finite multiplicative group with identity e.
- For $S, T \subseteq G$, define $ST = \{gh : g \in A, h \in B\}$.
- We say that (S, T) is a near-factorization of G if

$$|S| \times |T| = |G| - 1 \quad \text{and} \quad G \setminus \{e\} = ST.$$

- In the case where we have an additive group $(G, +)$ with identity 0, the second condition becomes $G - 0 = S + T$.
- Further, (S, T) is a (s, t)-near-factorization of G if $|S| = s$ and $|T| = t$, which requires $st = |G| - 1$.
- There is always a trivial $(1, |G| - 1)$-near-factorization of G given by

$$S = \{e\}, \qquad T = G - e.$$

- A near-factorization with $|S| > 1$ and $|T| > 1$ is nontrivial.

Example 1: $\mathbb{Z}_{16}$

A $(3,5)$-near-factorization of $(\mathbb{Z}_{16},+)$ is given by

$$S = \{1,2,3\} \quad \text{and} \quad T = \{0,3,6,9,12\}.$$

We have

$$\begin{aligned} 1 + T &= \{1,4,7,10,13\} \\ 2 + T &= \{2,5,8,11,14\} \\ 3 + T &= \{3,6,9,12,15\} \end{aligned}$$

The union of these three sets is $\mathbb{Z}_{16} \setminus \{0\}$.

Example 2: $\mathbb{Z}_{1+rs}$

An (s,t)-near-factorization of $(\mathbb{Z}_{1+st}, +)$ is given by

$$S = \{1, 2, \ldots, s\} \quad \text{and} \quad T = \{0, s, 2s, \ldots, (t-1)s\}.$$

We have

$$\begin{aligned}
1 + T &= \{1, 1+s, 1+2s, \ldots, 1+(t-1)s\} \\
2 + T &= \{2, 2+s, 2+2s, \ldots, 2+(t-1)s\} \\
3 + T &= \{3, 3+s, 3+2s, \ldots, 3+(t-1)s\} \\
&\vdots \\
(s-1) + T &= \{(s-1), (s-1)+s, (s-1)+2s, \ldots, (s-1)+(t-1)s\} \\
s + T &= \{s, 2s, 3s, \ldots, st\}
\end{aligned}$$

The union of these s sets is $\mathbb{Z}_{1+st} \setminus \{0\}$.

Example 3 D_8

The dihedral group D_n of order $2n$, $n > 2$ has the presentation

$$D_n = \left\langle a, b : a^2 = b^n = abab = e \right\rangle,$$

where e is the identity element.

$$S = \{e, b, a\} \quad \text{and} \quad T = \{b^2, b^5, ab, ab^4, ab^7\}$$

form a $(3,5)$-near-factorization of the dihedral group D_8. We have

$$\begin{aligned} eT &= \{b^2, b^5, ab, ab^4, ab^7\} \\ bT &= \{b^3, b^6, a, ab^3, ab^6\} \\ aT &= \{ab^2, ab^5, b, b^4, b^7\}. \end{aligned}$$

The union of these three sets is $D_8 \setminus \{e\}$.

Example 4. D_n

We illustrate a general construction with $n = 13$.

- D_{13} can be depicted by the following diagram:

$i =$	0	1	2	3	4	5	6	7	8	9	10	11	12
b^i													
ab^i													

- Remove the identity and enter the sequence $1, 2, 3, 4, 5$ five times, as shown.

$i =$	0	1	2	3	4	5	6	7	8	9	10	11	12
b^i		1	2	3	4	5	1	2	3	4	5	1	2
ab^i	5	4	3	2	1	5	4	3	2	1	5	4	3

Example 4. continued

- Partition the cells into tiles of the same shape that each contain exactly one cell of each type.

$i =$	0	1	2	3	4	5	6	7	8	9	10	11	12
b^i		1	2	3	4	5	1	2	3	4	5	1	2
ab^i	5	4	3	2	1	5	4	3	2	1	5	4	3

- Let S be the group elements in the leftmost tile:

$$S = \{b, b^2, ab^2, ab, a\}.$$

Each tile has a "notch." Let T be the group elements corresponding to these notches:

$$T = \{e, ab^5, b^5, ab^{10}, b^{10}\}.$$

- Then $ST = D_{13} \setminus \{e\}$ and hence it is a $(5, 5)$-near-factorization.
- The same method of construction will produce a near-factorization of D_n into factors S and T, whenever $|S| \times |T| = 2n - 1$.

(0,1)-factorization of $J - I$

Example (S, T) a (2,2)-near-factorization of $\mathbb{Z}_5$,

Let $G = C_5$ with generator g. Take $S = \{g, g^2\}$ and $T = \{e, g^2\}$. Then

$$ST = \{g, g^2, g^3, g^4\} = C_5 - e.$$

Set $M_S[x, y] = \begin{cases} 1 & \text{if } x^{-1}y \in S \\ 0 & \text{otherwise;} \end{cases}$ $\quad M_T[x, y] = \begin{cases} 1 & \text{if } x^{-1}y \in T \\ 0 & \text{otherwise;} \end{cases}$

$$\underset{M_S}{\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}} \underset{M_T}{\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}} = \underset{J_5 - I_5}{\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}}$$

If (S, T) is a (k, ℓ) near-factorization of G, then $M_S M_T = J - I$

Partitionable graphs

- A graph H on $n = uv + 1$ vertices is (u, v)-partitionable if for every vertex x
  1. $H - x$ has a partition into u cliques of size v, and
  2. $H - x$ has a partition into v independent sets of size u.
- The construction uses Cayley graphs. Suppose G is a multiplicative group with identity e,
  - $S \subseteq G \setminus \{e\}$ is symmetric if $g^{-1} \in S$ whenever $g \in S$.
  - The Cayley graph with connection set S, denoted $\mathrm{Cay}(G, S)$, has vertex set G, and $\{x, y\}$ is an edge iff $x^{-1}y \in S$.

Note:

- Because S is symmetric, $x^{-1}y \in S$ iff $y^{-1}x \in S$.
- Because $e \notin S$, $x^{-1}x \notin S$, i.e. there are no loops.
- Hence because S is symmetric, $\mathrm{Cay}(G, S)$ is a graph (rather than a digraph).

Partitionable graphs Pêcher (2003)

- Suppose (S, T) is a near-factorization of G.
- Let $A = S^{-1}S \setminus \{e\} = \{x^{-1}y : x, y \in S, x \neq y\}$
- Then $\textsc{Cay}(G, A)$ has the following properties:
  1. $\textsc{Cay}(G, A)$ is vertex transitive:
     For each $g \in G$, $x \mapsto xg$ is an automorphism.
  2. $\textsc{Cay}(G, A)$ is normalized:
     for every edge xy, there is a max. clique containing $\{x, y\}$.
  3. $\textsc{Cay}(G, A)$ is partitionable:
     for every vertex $g \in G$, the induced subgraph that is obtained by deleting g, i.e., $\textsc{Cay}(G, A)[G \setminus \{g\}]$, has the partition

$$\{gbS : b \in T\} \text{ of } |T| \text{ cliques of size } |S|$$

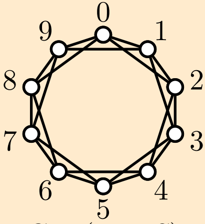
$$\{g(Ta)^{-1} : a \in S\} \text{ of } |S| \text{ independent sets of size } |T|$$

Example

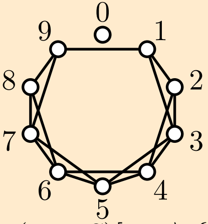
- Consider the near-factorization of $\mathbb{Z}_{10}$ given by $S = \{0, 1, 9\}$ and $T = \{2, 5, 8\}$. We have
$$-S + S = \{0, 1, 2, 8, 9\},$$
so $A = \{1, 2, 8, 9\}$.
- $\textsc{Cay}(\mathbb{Z}_{10}, A)$ is a graph whose vertices are $\mathbb{Z}_{10}$. So pairs of vertices that are distance 1 or 2 from each other are joined by edges.
- It is easy to see that $\textsc{Cay}(\mathbb{Z}_{10}, A)[\mathbb{Z}_{10} \setminus \{0\}]$ can be partitioned into three cliques of size three, namely
$$2 + S = \{1, 2, 3\},\ 5 + S = \{4, 5, 6\} \text{ and } 8 + S = \{7, 8, 9\}.$$
- It is also possible to partition $\textsc{Cay}(\mathbb{Z}_{10}, A)[\mathbb{Z}_{10} \setminus \{0\}]$ into three independent sets of size three, namely,
$$-(T + 0) = \{2, 5, 8\},\ -(T + 1) = \{1, 4, 7\},\ -(T + 9) = \{3, 6, 9\}.$$

Example

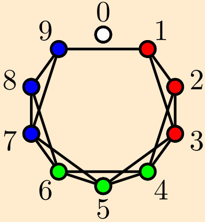
- Let $S = \{0, 1, 9\}$ and $T = \{2, 5, 8\}$. Then $S + T = \mathbb{Z}_{10} \setminus \{0\}$
- $S = (-S + S) \setminus \{0\} = \{1, 2, 8, 9\}$.



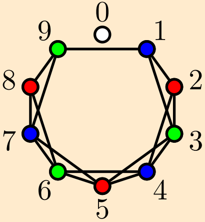
$\textsc{Cay}(\mathbb{Z}_{10}, S)$



$\textsc{Cay}(\mathbb{Z}_{10}, S)[\mathbb{Z}_{10} \setminus \{0\}]$



three cliques of size 3



three independent sets of size 3

Equivalence

Suppose (S,T) is a near-factorization of G. If $\alpha \in \textsc{Aut}(G)$ and $g \in G$, then

$$\begin{aligned}\big(\alpha(S)g\big)\big(g^{-1}\alpha(T)\big) &= \alpha(S)gg^{-1}\alpha(T) = \alpha(S)\alpha(T) = \alpha(ST)\\ &= \alpha(G \setminus \{e\}) = \alpha(G) \setminus \{\alpha(e)\}\\ &= G \setminus \{e\}\end{aligned}$$

Thus $(\alpha(S)g, g^{-1}\alpha(T))$ is an equivalent near-factorization of G.

A near-factorization (S,T) of an additive group G is symmetric if S and T are both symmetric.

Theorem 1 (de Caen et al, 1993).
If (S,T) is a near-factorization of additive abelian group G, then there exists $g \in G$ such that $(S+g, -g+T)$ is a symmetric near-factorization of G.

Every near-factorization of an abelian group is equivalent to a symmetric near-factorization.

Example

The $(3, 5)$-near-factorization of $\mathbb{Z}_{16}$ given by

$$S = \{0, 1, 15\} \quad \text{and} \quad T = \{2, 5, 8, 11, 14\}$$

is equivalent to the near-factorization

$$S' = 7S + 2 = \{2, 9, 11\} \quad \text{and} \quad T' = -2 + 7T = \{0, 1, 6, 11, 12\}$$

Theorem 1 guarantees that there is an element $g \in \mathbb{Z}_{16}$ such that $(S' + g, -g + T')$ is symmetric. The value $g = 14$ works, yielding

$$S' + 14 = \{0, 7, 9\} \quad \text{and} \quad -14 + T' = \{2, 3, 8, 13, 14\}.$$

Mates

- If S is a subset of the order n finite group G and T is such that (S, T) is a (r, s)-near-factorization of G, then we say T is a mate to S.
- If T is a mate to S, then $ST = G \setminus \{e\}$.
- Then $M_S M_T = J - I$, where $M_S[x, y] = \begin{cases} 1 & \text{if } x^{-1}y \in S; \\ 0 & \text{if not.} \end{cases}$
- Consequently $\det(J - I) = (-1)^{n-1}(n-1) \neq 0$.
- Thus $\det(M_S) \neq 0$
- Therefore

$$M_T = (M_S)^{-1}(J - I) = \frac{1}{r}J - (M_S)^{-1}$$

Theorem 2 (Kreher-Martin-Stinson 2025).
If $S \subseteq G$ has a mate T, then T is unique.

Computation

- Consider M_T

  $$M_T[x,y]=1 \Leftrightarrow x^{-1}y \in T \Leftrightarrow (yx^{-1})^{-1}e \in T \Leftrightarrow M_T[(yx^{-1}),e]=1$$

  The matrix M_T is completely determined by its "first" column.

- To determine if $S \subseteq G$ has a mate T we solve

  $$M_S X = [0,1,1,...,1]^T \quad (\text{ The first column of } J-I)$$

- If X exists and is a (0,1)-valued vector, then S has the mate T, where

  $$T=\{b^{-1} : X[b]=1\}$$

  (X is the first column of M_T.)

This is very efficient. However the number of possible subsets S to examine can be large.

reducing the search space

- The search space is the set of s element subsets $S \subseteq G \setminus \{e\}$ for which we compute a possible mate.
- If G is abelian we can assume the possible near-factorization are symmetric and only consider S, where $S = -S$.
- If we know $\textsc{Aut}(G)$ we need only consider S that are lexicographically minimal with respect to equivalence.

Computational results

- Near-factorizations of cyclic groups exist for all possible parameters. If $(n-1) = st$, then

$$\mathbb{Z}_n \setminus \{0\} = \{1, 2, \ldots, s\} + \{0, s, 2s, \ldots, (t-1)s\}$$

  See [3] for recent further results on this topic.

- For noncyclic abelian groups, it was previously known (mainly due to theoretical results in de Caen et al [1]) that there are no non-trivial examples in noncyclic abelian groups of order ≤ 100.

- We have now proven nonexistence in all noncyclic abelian groups G of order ≤ 200; there were roughly 100 parameter sets (G, r, s) to consider.
  - Most possibilities were ruled out by theoretical criteria, but several parameter sets required exhaustive searches.
  - "Difficult groups" requiring computer search: $\mathbb{Z}_{29} \times (\mathbb{Z}_2)^2$, $\mathbb{Z}_{17} \times (\mathbb{Z}_2)^3$, $\mathbb{Z}_{17} \times \mathbb{Z}_4\mathbb{Z}_2$, $\mathbb{Z}_{37} \times (\mathbb{Z}_2)^2$, $\mathbb{Z}_{17} \times (\mathbb{Z}_3)^2$, $\mathbb{Z}_{39} \times (\mathbb{Z}_2)^2$, $\mathbb{Z}_{19} \times (\mathbb{Z}_3)^2$, $\mathbb{Z}_{43} \times (\mathbb{Z}_2)^2$, $\mathbb{Z}_7 \times (\mathbb{Z}_5)^2$, $\mathbb{Z}_{11} \times \mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_{49} \times (\mathbb{Z}_2)^2$, and $\mathbb{Z}_{49} \times (\mathbb{Z}_2)^2$.

Nonabelian groups

The only known non-abelian groups that are known to have a near-factorization are:

- de Caen et al. The (s, t)-near-factorizations of the dihedral group D_n mentioned earlier,

  $$D_n = \langle a, b : a^2 = 1, b^n = 1, aba = b^{-1} \rangle$$

  for all $st = (n-1)$.
- Pêcher's $(7, 7)$-near-factorization of $D_5 \times C_5$.

  $$D_5 \times C_5 = \left\langle a, b, c : a^2 = b^5 = abab = c^5 = e, ac = ca, bc = cb \right\rangle .$$

- Pêcher's $(7, 7)$-near-factorization of $C_5^2 \rtimes_2 C_2$

  $$C_5^2 \rtimes_2 C_2 = \langle a, b, c | a^5 = b^5 = c^2 = e, cac = a^{-1}, cbc = b^{-1}, bc = cb \rangle$$

Pêcher checked all non-abelain groups of order at most 50.
See Kreher, Paterson and Stinson [4] and Pêcher [7].

λ-mates

- Let G be a finite group with identity e
- We say that (S, T) is a λ-fold near-factorization of G if $|S| \times |T| = \lambda(|G| \setminus \{e\})$ and each element of $G \setminus \{e\}$ occurs λ times in the **product** ST.

$$ST = \lambda(G \setminus \{e\})$$

- In the case where we have an additive group $(G, +)$ with identity 0, then each element of $G \setminus \{0\}$ occurs λ times in the **sum** $S + T$.

$$S + T = \lambda(G \setminus \{0\}).$$

- Necessarily $\lambda \leq s$ and $\lambda \leq t$.
- If (S, T) is a λ-fold near-factorization, then we say that T is a λ-mate of S.

What? They need not be symmetric?

There is an 2-fold $(3,4)$-near-factorization (S,T) of $\mathbb{Z}_7$.

$$S = \{0,1,3\} \quad \text{and} \quad T = \{1,2,3,5\}$$

$+$	1	2	3	5
0	1	2	3	5
1	2	3	4	6
3	4	5	6	1

There is not a symmetric 2-fold near-factorization (S,T) of $\mathbb{Z}_7$.

Proof.

Let (S,T) be a symmetric 2-fold $(3,4)$-near factorization of $\mathbb{Z}_7$.

- $|S| = 3 \Rightarrow S = \{0,x,-x\}$.
- (S',T'), where $S' = Sx^{-1} = \{0,1,-6\}$ and $T' = xT$ is also a 2-fold near-factorization of $\mathbb{Z}_7$.
- Because $0 \notin S' + T' \Rightarrow 0,1,6 \notin T' \Rightarrow T' = \{2,3,4,5\}$
- But $S' + T'$ contains $0+3 = 1+2 = 6+4 = 3$, and 3 should occur twice. □

λ-fold(s,t) near factorizations with $\lambda > 2$, $n \leq 35$

Symmetric

n	group	s	t	λ
9	$(\mathbb{Z}_3)^2$	4	4	2
13	$\mathbb{Z}_{13}$	6	6	3
15	$\mathbb{Z}_{15}$	4	7	2
16	$(\mathbb{Z}_4)^2$	6	10	4
16	$(\mathbb{Z}_2)^4$	6	10	4
17	$\mathbb{Z}_{17}$	8	8	4
21	$\mathbb{Z}_{21}$	4	10	2
25	$(\mathbb{Z}_5)^2$	4	12	2
25	$(\mathbb{Z}_5)^2$	12	12	6
27	$\mathbb{Z}_9 \times \mathbb{Z}_3$	4	13	2
27	$(\mathbb{Z}_3)^3$	8	13	4
29	$\mathbb{Z}_{29}$	14	14	7
33	$\mathbb{Z}_{33}$	4	16	2
35	$\mathbb{Z}_{35}$	4	17	2

Non-symmetric

n	group	s	t	λ
7	$\mathbb{Z}_7$	3	4	2
11	$\mathbb{Z}_{11}$	5	6	3
13	$\mathbb{Z}_{13}$	4	9	3
15	$\mathbb{Z}_{15}$	7	8	4
16	$\mathbb{Z}_8 \times \mathbb{Z}_2$	5	9	3
16	$\mathbb{Z}_8 \times \mathbb{Z}_2$	6	10	4
16	$\mathbb{Z}_4 \times (\mathbb{Z}_2)^2$	6	10	4
19	$\mathbb{Z}_{19}$	9	10	5
21	$\mathbb{Z}_{21}$	5	16	4
21	$\mathbb{Z}_{21}$	8	10	4
23	$\mathbb{Z}_{23}$	11	12	6
27	$(\mathbb{Z}_3)^3$	13	14	7
28	$\mathbb{Z}_{14} \times \mathbb{Z}_2$	9	12	4
31	$\mathbb{Z}_{31}$	6	20	4
31	$\mathbb{Z}_{31}$	6	25	5
35	$\mathbb{Z}_{35}$	8	17	4
35	$\mathbb{Z}_{35}$	17	18	9

If $S \subseteq G$, then $S^{-1} = \{x^{-1} : x \in S\}$.
(If G is abelian and written additively, $S^{-1} = -S = \{-x : x \in S\}$.)

A (v, k, λ)-difference set in the group G is a k-element subset S of G such that the identity e occurs k times in the product SS^{-1} and each non-identity element occurs λ times.

Theorem 3. Suppose there is a (v, k, λ)-difference set S in a group G of order v. If $T = G \setminus S^{-1}$. Then (S, T) is a $(k - \lambda)$-fold $(k, v - k)$-near factorization.

Example
A $(11, 5, 2)$-difference set in $\mathbb{Z}_{11}$ is
$S = \{1, 3, 4, 5, 9\}$

$S^{-1} = -S = \{10, 8, 7, 6, 2\} \Rightarrow$
$T = \{0, 1, 3, 4, 5, 9\}$

$S + T = 3(\mathbb{Z}_{11} \setminus \{0\})$

$-$	1	3	4	5	9
1	0	9	8	7	3
3	2	0	10	9	6
4	3	1	0	10	5
5	4	2	1	0	7
9	8	6	5	4	0

$+$	0	1	3	4	5	9
1	1	2	4	5	6	10
3	3	4	6	7	8	1
4	4	5	7	8	9	2
5	5	6	8	9	10	3
9	9	10	1	2	3	7

The group ring $\mathbb{Z}[G]$.

Let G be a finite group. The group ring $\mathbb{Z}[G]$ is

$$\mathbb{Z}[G] = \{ \sum_{g \in G} c_g g : c_g \in \mathbb{Z}, g \in G \}$$

Then the multi-subset S of G, is denoted in the group ring as $S = \sum_{g \in S} n_j g$, where n_g is the number of times g occurs in S

Example: $G = C_7 = \{1, \alpha, \alpha^2, \cdots, \alpha^6\}$, the cyclic group of order 7 generated by α. Then

$$\{1, \alpha, \alpha, \alpha^3\} \text{ in } G \equiv 1 + 2\alpha + \alpha^3 \in \mathbb{Z}[G]$$

addition:

$$(1 + \alpha + \alpha^5) + (\alpha + \alpha^6) = (1 + 2\alpha + \alpha^5 + \alpha^6)$$

mutiplication:

$$\begin{aligned} (1 + \alpha + \alpha^5)(\alpha + \alpha^6) &= 1(\alpha + \alpha^6) + \alpha(\alpha + \alpha^6) + \alpha^5(\alpha + \alpha^6) \\ &= (\alpha + \alpha^6) + (\alpha^2 + e) + (\alpha^6 + \alpha^4) \\ &= 1 + \alpha + \alpha^2 + \alpha^4 + 2\alpha^6 \end{aligned}$$

The group ring $\mathbb{Z}[G]$. Continued

If $S \subset G$, let $S = \sum_{g \in S} g$, then (S, T) is a λ-fold near-factorization of G, if and only if in the group ring

$$ST = \lambda(G - e)$$

Example in $\mathbb{Z}[C_7]$:

$$\begin{aligned}
(e + \alpha + \alpha^3)(\alpha + \alpha^2 + \alpha^3 + \alpha^5) &= e(\alpha + \alpha^2 + \alpha^3 + \alpha^5) \\
&\quad +\alpha(\alpha + \alpha^2 + \alpha^3 + \alpha^5) \\
&\quad +\alpha^3(\alpha + \alpha^2 + \alpha^3 + \alpha^5) \\
&= (\alpha + \alpha^2 + \alpha^3 + \alpha^5) \\
&\quad +(\alpha^2 + \alpha^3 + \alpha^4 + \alpha^6) \\
&\quad +(\alpha^4 + \alpha^5 + \alpha^6 + \alpha) \\
&= 2(G_7 - 1)
\end{aligned}$$

The group ring $\mathbb{Z}[G]$ is a convenient algebraic way to handle multi-sets.

Proof of Theorem 3

If $S \subset G$, then $S^{(-1)} = \sum_{g \in S} g^{-1}$.

A k-element subset $D \subseteq G$ is a (v, k, λ)-difference set if and only if

$$DD^{(-1)} = ke + \lambda(G - e)$$

Theorem 3. Suppose there is a (v, k, λ)-difference set D in a group G of order v. If $S = D$ and $T = G \setminus S^{-1} = \{g \in G : g^{-1} \notin S\}$, then (S, T) is a $(k - \lambda)$-fold $(k, v - k)$-near factorization.

Proof.

First: $SG = kG$

Next: $SS^{(-1)} = ke + \lambda(G - e)$

Hence:
$$\begin{aligned} ST &= S(G - S^{(-1)}) \\ &= kG - \big(ke + \lambda(G - e)\big) \\ &= (k - \lambda)(G - e) \end{aligned}$$

□

Remark

Suppose the k-element subset $S \subseteq G$ is a (v, k, λ)-difference set then

$$SS^{(-1)} = ke + \lambda(G - e)$$

- **The "inverse" is also a difference set.**

  $$S^{(-1)}S = ke + \lambda(G - e)$$

  So $S^{(-1)}$ is also a difference set.

- **The complement is also a difference set**
  Let $T = G \setminus S$, where S is a a (v, k, λ)-difference set, let $t = |T| = v - k$.

  $$\begin{aligned} TT^{(-1)} &= (G - S^{(-1)})(G - S^{(-1)})^{(-1)} = (G - S^{(-1)})(G - S) \\ &= GG - GS - S^{(-1)}G + S^{(-1)}S \\ &= (v)G - kG - kG + \big(ke + \lambda(G - e)\big) \\ &= (t - k)G + ke + \lambda(G - e) \\ &= (t + \lambda - k)(G - e) + te \end{aligned}$$

The converse is true

Theorem 3 converse.
Suppose (S, T) is λ-fold (s, t)-near factorization of G, where $|G| = s + t$. Then S is an $(s + t, s, s - \lambda)$-difference set in G and $T = G \setminus S^{-1}$ is an $(s + t, t, t - \lambda)$-difference set in G.

Proof.

In the $\mathbb{Z}[G]$, $T = G - S^{(-1)}$.

$$SS^{(-1)} = S(G - T) = sG - ST = sG - \lambda(G - e)$$
$$= (sG - e) + se - \lambda(G - e) = (s - \lambda)(G - e) + se$$

Therefore S is a $(s + t, s, s - \lambda)$-difference set.
and T is a $(s + t, t, t - \lambda)$-difference set,
because T is the complement of S^{-1}. □

Partial difference set

A (v, k, λ, μ)-partial difference set (or PDS) in a group G of order v is a subset $D \subseteq G \setminus \{e\}$ such that $|D| = k$ and the following group ring equation is satisfied:

$$\begin{aligned} DD^{(-1)} &= (k-\mu)e + (\lambda-\mu)D + \mu G, \\ &= ke + \lambda D + \mu(G - D - e) \end{aligned}$$

The set $D = \{1, 3, 4, 9, 10, 12\}$ is a $(13, 6, 2, 3)$-PDS in $\mathbb{Z}_{13}$.

$-$	1	3	4	9	10	12
1	0	11	10	5	4	2
3	2	0	12	7	6	4
4	3	1	0	8	7	5
9	8	6	5	0	12	10
10	9	7	6	1	0	11
12	11	9	8	3	2	0

PDS construction

Theorem 4. Suppose D is a $(s+t+1, s, s-\lambda-1, s-\lambda)$-PDS in a group G, where $|G| = s+t+1$ and $e \notin D$. Let $S = D$ and $T = G \setminus S^{(-1)} \setminus \{e\}$. Then (S, T) is a λ-fold (s, t)-near-factorization of G.

Proof.

Computing in $\mathbb{Z}[G]$ we see that

$$\begin{aligned} ST &= S\big(G - S^{(-1)} - e\big) \\ &= SG - SS^{(-1)} - Se \\ &= sG - \Bigg(se + (s-\lambda-1)S + (s-\lambda)(G - S - e)\Bigg) - S \\ &= sG - se - (s-\lambda-1)S - (s-\lambda)(G - S - e) - S \\ &= \lambda G - \lambda e \\ &= \lambda(G - e) \end{aligned}$$

□

Example and converse

From the (13,6,2,3)-PDS given in the Example a 3-fold (6,6)-near-factorization of $\mathbb{Z}_{13}$ is obtained. The near-factorization has

$$S = \{1, 3, 4, 9, 10, 12\} \text{ and } T = \{2, 5, 6, 7, 8, 11\}.$$

Theorem 4 converse.
If (S, T) is an λ-fold (s, t)-near-factorization of G and $|G| = s + t + 1$. Then S is an $(s + t + 1, s, s - \lambda - 1, s - \lambda)$-PDS in G and T is an $(s + t + 1, t, t - \lambda - 1, t - \lambda)$-PDS

Theorem 5. Suppose p and q are any positive odd integers greater than 1. Then there exists a 2-fold $(4,(n-1)/2)$-near-factorization (S,T) of $\mathbb{Z}_p \times \mathbb{Z}_q$.

The construction: Take

$$S = \{(1,1),(1,-1),(-1,1),(-1,-1)\}.$$

Set $C_i^j = \{4i+j, 4i+j+1\}$.

Case 1: $p = 1+4a$, $q = 1+4b$.

$$T = \left(\left(\bigcup_{i=0}^{a-1} C_i^0 \cup \{4a\}\right) \times \left(\bigcup_{j=0}^{b-1} C_j^2\right)\right) \cup \left(\left(\bigcup_{i=0}^{a-1} C_i^2\right) \times \left(\bigcup_{j=0}^{b-1} C_j^0 \cup \{4b\}\right)\right)$$

Case 2: $p = 1+4a$, $q = -1+4b$.

$$T = \left(\left(\bigcup_{i=0}^{a-1} C_i^0 \cup \{4a\}\right) \times \left(\bigcup_{j=0}^{b-2} C_j^3 \cup \{0\}\right)\right) \cup \left(\left(\bigcup_{i=0}^{a-1} C_i^2\right) \times \left(\bigcup_{j=0}^{b-1} C_j^1\right)\right)$$

Case 3: $p = -1+4a$, $q = -1+4b$.

$$T = \left(\left(\bigcup_{i=0}^{a-2} C_i^3 \cup \{0\}\right) \times \left(\bigcup_{j=0}^{b-1} C_j^1\right)\right) \cup \left(\left(\bigcup_{i=0}^{a-1} C_i^1\right) \times \left(\bigcup_{j=0}^{b-2} C_j^3 \cup \{0\}\right)\right)$$

Example $\mathbb{Z}_{45} = \mathbb{Z}_5 \times \mathbb{Z}_9$

$S = \{(1,1), (1,8), (4,1), (4,8)\}.$

$$C_0^0 = \{0,1\} \qquad C_1^0 = \{4,5\}.$$
$$C_0^2 = \{2,3\} \qquad C_1^2 = \{6,7\}.$$

Case 1: $p = 1 + 4a$, $q = 1 + 4b$, where $a = 1$, $b = 2$

$$\begin{aligned}
T &= \left(\left(\bigcup_{i=0}^{a-1} C_i^0 \cup \{4a\}\right) \times \left(\bigcup_{j=0}^{b-1} C_j^2\right)\right) \cup \left(\left(\bigcup_{i=0}^{a-1} C_i^2\right) \times \left(\bigcup_{j=0}^{b-1} C_j^0 \cup \{4b\}\right)\right) \\
&= \left(\left(C_0^0 \cup \{4\}\right) \times \left(C_0^2 \cup C_1^2\right)\right) \cup \left(\left(C_0^2\right) \times \left(C_0^0 \cup C_1^0 \cup \{8\}\right)\right) \\
&= \left(\{0,1,4\} \times \{2,3,6,7\}\right) \cup \left(\{2,3\} \times \{0,1,4,5,8\}\right) \\
&= \left\{ \begin{matrix} (0,2), (0,3), (0,6), (0,7), (1,2), (1,3), (1,6), (1,7), (4,2), (4,3), (4,6) \\ (4,7), (2,0), (2,1), (2,4), (2,5), (2,8), (3,0), (3,1), (3,4), (3,5), (3,8) \end{matrix} \right\}
\end{aligned}$$

Example Continued

Thus

$$S = \{(1,1),(1,8),(4,1),(4,8)\}.$$
$$T = \begin{Bmatrix} (0,2),(0,3),(0,6),(0,7),(1,2),(1,3),(1,6),(1,7),(4,2),(4,3),(4,6) \\ (4,7),(2,0),(2,1),(2,4),(2,5),(2,8),(3,0),(3,1),(3,4),(3,5),(3,8) \end{Bmatrix}$$

is (supposedly) a 2-fold $(4,22)$-Near-factorization of $\mathbb{Z}_5 \times \mathbb{Z}_9$.
$(1,1)$ generates $\mathbb{Z}_5 \times \mathbb{Z}_9$ and 1 generates $\mathbb{Z}_{45}$ and so $\psi : (x,x) \mapsto x$ is an isomorphism. For example $(1,8) = (26,26)$ So $\pi(1,8) = 26$.
Thus

$$\psi(S) = \{1, 26, 19, 44\}.$$
$$\psi(T) = \begin{Bmatrix} 6, 8, 11, 13, 15, 16, 17, 18, 20, 21, 22, \\ 23, 24, 25, 27, 28, 29, 30, 32, 34, 37, 39 \end{Bmatrix}$$

is (supposedly) a 2-fold $(4,22)$-Near-factorization of $\mathbb{Z}_{45}$.

Lets check!

Example continued

$$S' = \psi(S) = \{1, 26, 19, 44\}.$$

$$T' = \psi(T) = \begin{Bmatrix} 6, 8, 11, 13, 15, 16, 17, 18, 20, 21, 22, \\ 23, 24, 25, 27, 28, 29, 30, 32, 34, 37, 39 \end{Bmatrix}$$

is (supposedly) a 2-fold $(4, 22)$-Near-factorization of $\mathbb{Z}_{45}$.

Lets check!

	6	8	11	13	15	16	17	18	20	21	22	23	24	25	27	28	29	30	32	34	37	39
1	7	9	12	14	16	17	18	19	21	22	23	24	25	26	28	29	30	31	33	35	38	40
19	25	27	30	32	34	35	36	37	39	40	41	42	43	44	1	2	3	4	6	8	11	13
26	32	34	37	39	41	42	43	44	1	2	3	4	5	6	8	9	10	11	13	15	18	20
44	5	7	10	12	14	15	16	17	19	20	21	22	23	24	26	27	28	29	31	33	36	38

and it is.

n	group	s	t	λ	Sym.?	Authority
7	$\mathbb{Z}_7$	3	4	2	no	Theorem 3, $D = \{$ 0, 1, 3$\}$
9	$(\mathbb{Z}_3)^2$	4	4	2	yes	Theorem 5
11	$\mathbb{Z}_{11}$	5	6	3	no	Theorem 3, $D = \{$ 0, 1, 2, 4, 7$\}$
13	$\mathbb{Z}_{13}$	4	9	3	no	Theorem 3, $D = \{$ 0, 1, 3, 9$\}$
13	$\mathbb{Z}_{13}$	6	6	3	yes	Theorem 4, $D = \{$1, 3, 4, 12, 10, 9$\}$
15	$\mathbb{Z}_{15}$	4	7	2	yes	Theorem 5
15	$\mathbb{Z}_{15}$	7	8	4	no	Theorem 3, $D = \{$ 0, 1, 2, 4, 5, 8, 10$\}$
16	$(\mathbb{Z}_4)^2$	6	10	4	yes	Theorem 3, $D = \{$(0,1), (1,0), (1,1), (0,3), (3,0), (3,3)$\}$
16	$\mathbb{Z}_4 \times (\mathbb{Z}_2)^2$	6	10	4	yes	Theorem 3, $D = \{$(0,0,0), (0,0,1), (0,1,0), (2,1,1), (1,0,0), (3,0,0)$\}$
16	$\mathbb{Z}_8 \times \mathbb{Z}_2$	5	9	3	no	$S = \{$(0,0), (0,1), (1,0), (3,0), (4,0)$\}$, $T = \{$(7,1), (6,0), (5,1), (4,1), (3,0), (3,1), (2,0), (1,0), (1,1)$\}$
16	$\mathbb{Z}_8 \times \mathbb{Z}_2$	6	10	4	no	Theorem 3, $D = \{$(0,0), (0,1), (1,0), (2,0), (5,0), (6,1)$\}$
17	$\mathbb{Z}_{17}$	8	8	4	yes	Theorem 4, $D = \{$1, 2, 4, 8, 16, 15, 13, 9$\}$
19	$\mathbb{Z}_{19}$	9	10	5	no	Theorem 3, $D = \{$ 0, 1, 2, 3, 5, 7, 12, 13, 16$\}$
21	$\mathbb{Z}_{21}$	4	10	2	yes	Theorem 5
21	$\mathbb{Z}_{21}$	5	16	4	no	Theorem 3, $D = \{$ 0, 1, 4, 14, 16$\}$
21	$\mathbb{Z}_{21}$	8	10	4	no	$S = \{$ 0, 1, 3, 6, 7, 10, 13, 15$\}$, $T = \{$ 17, 13, 12, 9, 7, 5, 4, 3, 2, 1$\}$
23	$\mathbb{Z}_{23}$	11	12	6	no	Theorem 3, $D = \{$ 0, 1, 2, 3, 5, 7, 8, 11, 12, 15, 17$\}$

n	group	s	t	λ	Sym.?	Authority
25	$(\mathbb{Z}_5)^2$	4	12	2	yes	Theorem 5
25	$(\mathbb{Z}_5)^2$	12	12	6	yes	Theorem 4, $D=\{$(0,1), (0,2), (1,0), (1,1), (2,0), (2,2), (0,4), (0,3), (4,0), (4,4), (3,0), (3,3)$\}$
27	$(\mathbb{Z}_3)^3$	8	13	4	yes	$S = \{$(0,0,1), (0,1,0), (1,0,0), (1,1,1), (0,0,2), (0,2,0), (2,0,0), (2,2,2)$\}$, $T = \{$(0,0,0), (0,2,1), (0,1,2), (2,0,1), (2,2,1), (2,1,0), (2,1,2), (2,1,1), (1,0,2), (1,2,0), (1,2,2), (1,2,1), (1,1,2)$\}$
27	$(\mathbb{Z}_3)^3$	13	14	7	no	Theorem 3, $D=\{$(0,0,0), (0,0,1), (0,0,2), (0,1,0), (0,1,1), (0,2,0), (1,0,0), (1,0,1), (1,1,0), (2,0,1), (2,1,2), (2,2,0), (2,2,2)$\}$
27	$\mathbb{Z}_9\times\mathbb{Z}_3$	4	13	2	yes	Theorem 5
28	$\mathbb{Z}_{14}\times\mathbb{Z}_2$	9	12	4	no	$S=\{$(0,0), (0,1), (1,0), (2,0), (3,1), (4,1), (7,1), (12,0), (13,0)$\}$, $T=\{$(13,1), (12,1), (11,0), (9,0), (9,1), (8,1), (6,1), (5,0), (4,1), (3,0), (3,1), (1,1)$\}$
29	$\mathbb{Z}_{29}$	14	14	7	yes	Theorem 4, $D=\{$1, 4, 5, 6, 7, 9, 13, 28, 25, 24, 23, 22, 20, 16$\}$
31	$\mathbb{Z}_{31}$	6	20	4	no	$S=\{$ 0, 1, 2, 4, 8, 16$\}$, $T=\{$ 28, 26, 25, 24, 22, 21, 19, 17, 16, 14, 13, 12, 11, 8, 7, 6, 4, 3, 2, 1$\}$
31	$\mathbb{Z}_{31}$	6	25	5	no	Theorem 3, $D=\{$ 0, 1, 3, 8, 12, 18$\}$
31	$\mathbb{Z}_{31}$	15	16	8	no	Theorem 3, $D=\{$ 0, 1, 2, 3, 5, 6, 8, 9, 13, 16, 21, 22, 23, 25, 27$\}$
33	$\mathbb{Z}_{33}$	4	16	2	yes	Theorem 5
33	$\mathbb{Z}_{33}$	12	16	6	no	$S=\{$ 0, 1, 3, 4, 6, 10, 12, 15, 21, 22, 25,

[1] D. de Caen, D. A. Gregory, I. G. Hughes, and D. L. Kreher, *Near-factors of finite groups*, *Ars Combin.*, **29** (1990), 53–63.

[2] D. L. Kreher, S. Li, and D. R. Stinson, λ-Mates in near-factorizations, *Ready for 5th pythagoreans*.
https://doi.org/10.48550/arXiv.2503.09325

[3] D. L. Kreher, M. B. Paterson and D. R. Stinson, Strong external difference families and classification of α-valuations, to appear in JCD (?)
https://doi.org/10.48550/arXiv.2406.09075

[4] D. L. Kreher, M. B. Paterson and D. R. Stinson, Near-factorizations of dihedral groups, submitted for publication.
https://doi.org/10.48550/arXiv.2411.15884

[5] D. L. Kreher, W. J. Martin, and D. R. Stinson, Uniqueness and explicit computation of mates in near-factorizations, submitted for publication.
https://doi.org/10.48550/arXiv.2411.15890

[6] M.B. Paterson and D.R. Stinson, Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families, *Discrete Math.*, **339** (2016), 2891–2906.

[7] A. Pêcher, Cayley partitionable graphs and near-factorizations of finite groups, *Discr. Math.*, **276** (2004), 295–311.

Thank you