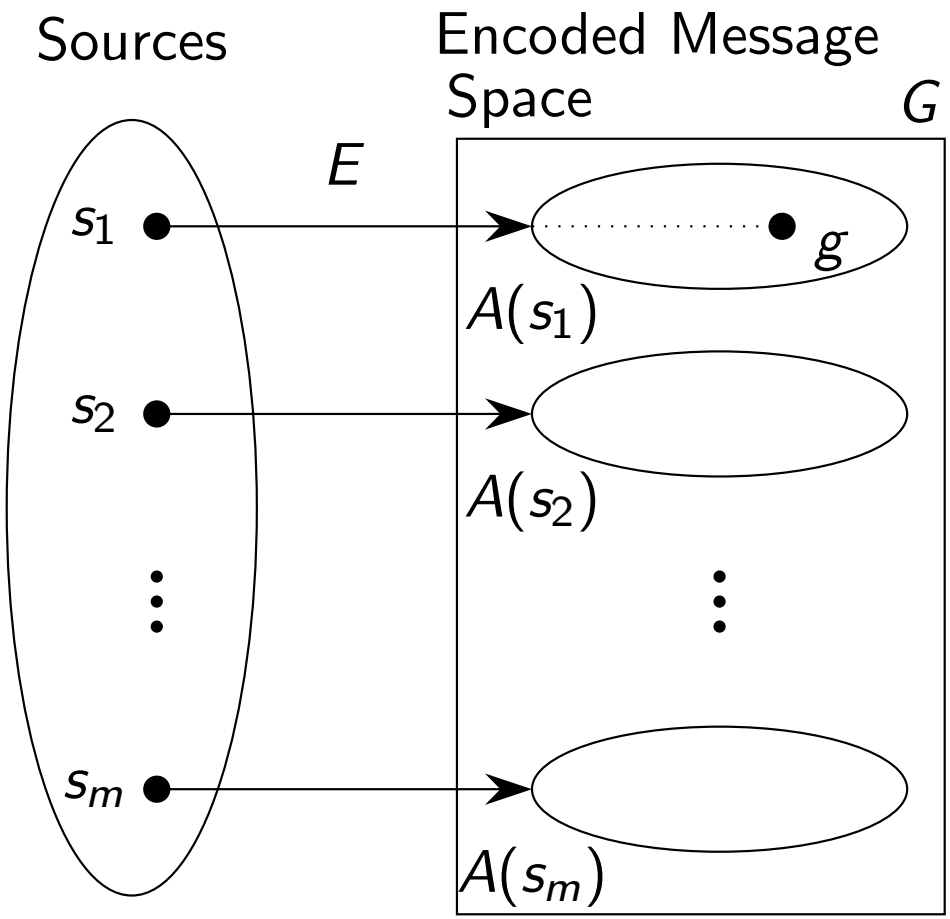
New Circular External Difference Families and Related Constructions

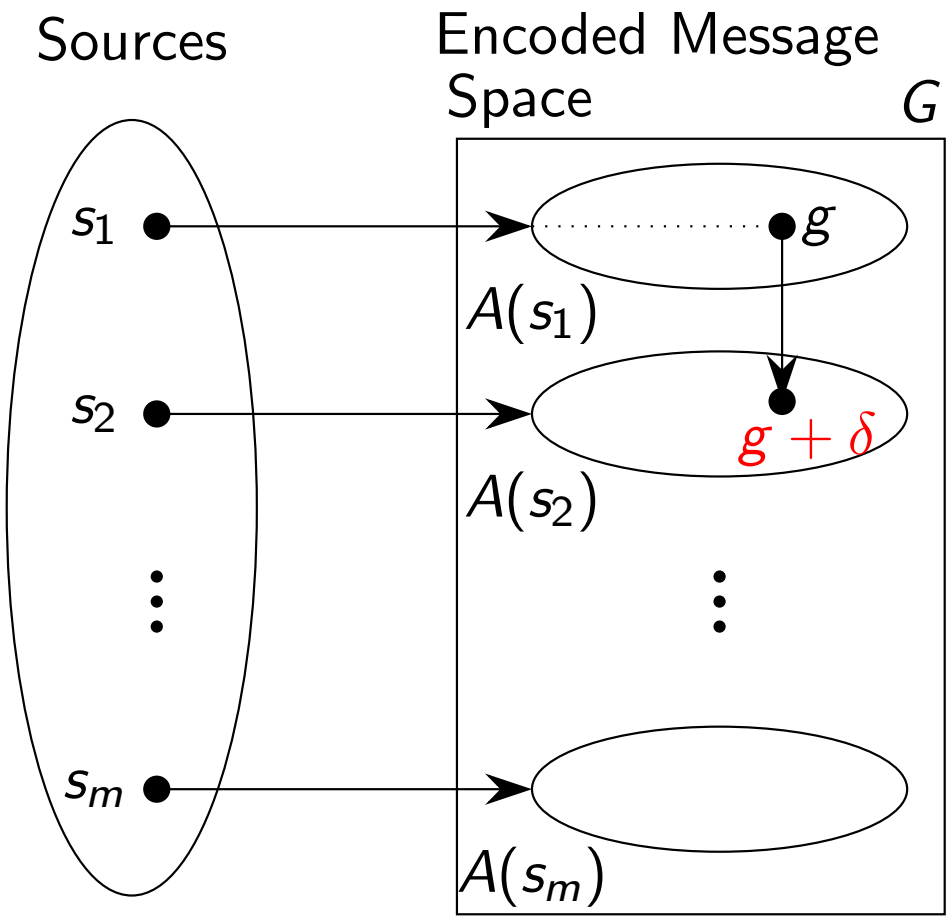
Struan McCartney (St Andrews)

Joint work with Sophie Huczynska and Chris Jefferson

AMD Code Diagram



AMD Code Diagram (with adversary)



AMD Codes

In 2008 Cramer et. al. defined an (n, m, ϵ)-AMD code as the encoding function along with the decoding function for this scenario, where $n = |G|$ and ϵ is the maximum probability of adversary sucess.

l-Regular AMD Codes

An AMD code is l regular if all source encryption spaces have size l. We will be considering l-regular codes.

R-Optimal AMD Codes

A (n, m, l, ϵ)-weak AMD code is R-optimal if the maximal probability of adversary success is equal to the average probability of success. This occurs when:

$$\epsilon = \frac{l(m-1)}{(n-1)}$$

EDFs

Definition

An (n, m, l, λ)-EDF in a group G where $n = |G|$, is a set of m (≥ 2) disjoint subsets of G with size l such that each non-zero element from G occurs precisely λ times as a difference between two distinct sets.

Example

$\{A_0 = \{0, 1\}, A_1 = \{2, 4\}\}$ is a (9,2,2,1)-EDF in $\mathbb{Z}_9$

-	0 1	2 4
0 1		7 5 8 6
2 4	2 1 4 3	

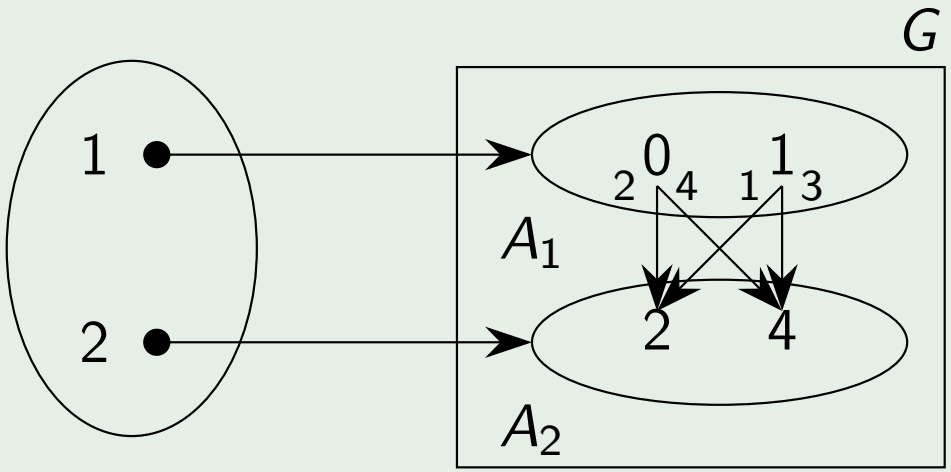
Connecting AMD Codes and EDFs

Maura B. Paterson, Douglas R. Stinson (2016)

An (R-optimal) weak (n, m, l, ϵ)-AMD code is equivalent to an (n, m, l, λ)-EDF where $\lambda = \frac{l^2 m(m-1)}{n-1}$.

Example

$\{\{0, 1\}, \{2, 4\}\}$ is equivalent to a $(9, 2, 2, \frac{1}{4})$-AMD code



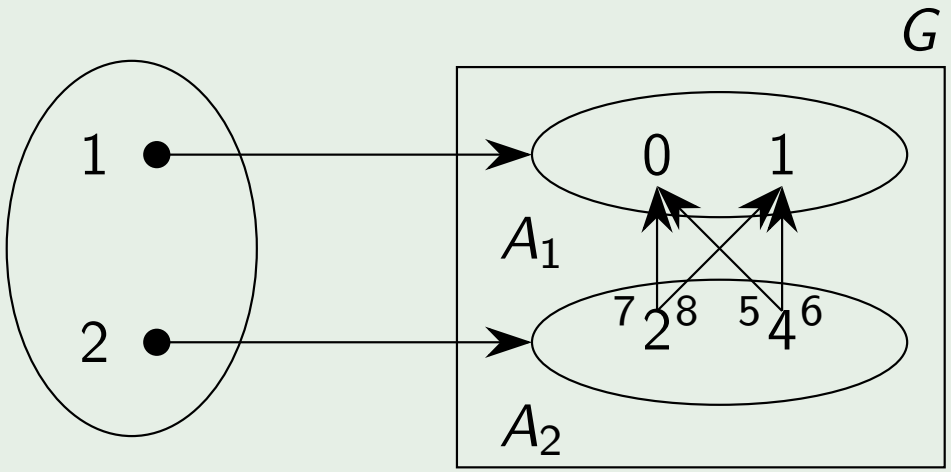
Connecting AMD Codes and EDFs

Maura B. Paterson, Douglas R. Stinson (2016)

An (R-optimal) weak (n, m, l, ϵ)-AMD code is equivalent to an (n, m, l, λ)-EDF where $\lambda = \frac{l^2 m(m-1)}{n-1}$.

Example

$\{\{0, 1\}, \{2, 4\}\}$ is equivalent to a $(9, 2, 2, \frac{1}{4})$-AMD code



Strong External and Circular Difference Families

Along with EDFs we also define strong EDFs:

Definition

A strong $(n, m, l, \lambda)-$EDF in a group G is a set of m disjoint subsets of G with size l such that for each $0 \leq i \leq m-1$ every non-zero element from G occurs precisely λ times as a difference between A_i and A_j for each $0 \leq j \leq m-1, i \neq j$.

In 2023 Stinson and Veitch defined a new EDF construction based on non-malleable AMD codes:

Definition

An $(n, m, l, \lambda)-c-$circular EDF in a group G is a set of m disjoint subsets of G with size l such that each non-zero element from G occurs precisely λ times in the differences between all sets A_i and A_j where

$$j \equiv i + c \mod m.$$

A New Digraph Framework for EDFs

We define a new generalised framework for EDFs defined in terms of the directed edges of a digraph.

Definition

Let G be a group of order n, and let $\mathcal{A} = (A_0, A_1, \ldots, A_{m-1})$ be disjoint subsets of G of size l. Let H be a labelled digraph on m vertices $\{0, 1, \ldots, m-1\}$ and let $\overrightarrow{E}(H)$ be the set of directed edges of H. Then $\mathcal{A}$ is said to be an $(n, m, l, \lambda; H)-$EDF if the following multiset equation holds:

$$\bigcup_{(i,j)\in\overrightarrow{E}(H)} \Delta(A_j, A_i) = \lambda(G\backslash\{0\}).$$

We call this an $H-$defined EDF.

EDFs and Circular EDFs

Definition: Complete Graph K_m

We define the complete graph K_m as $V(K_m) = \{0, 1, \ldots, m-1\}$ and $\overrightarrow{E}(K_m) = \{(i,j) : 0 \leq i,j \leq m-1, i \neq j\}$.

Theorem (2025, *SH\CJ\SM*)

A $(n, m, l, \lambda; K_m)-$EDF is precisely a $(n, m, l, \lambda)-$EDF.

Definition: Directed Cycle $\overrightarrow{C}_m$

We define the directed cycle $\overrightarrow{C}_m$ as $V(\overrightarrow{C}_m) = \{0, 1, \ldots, m-1\}$ and $\overrightarrow{E}(\overrightarrow{C}_m) = \{(i, i+1 \mod m) : 0 \leq i \leq m-1\}$.

Theorem (2025, *SH\CJ\SM*)

A $(n, m, l, \lambda; \overrightarrow{C}_m)-$EDF is precisely a $(n, m, l, \lambda)-1-$circular EDF (CEDF).

Bipartite and Strong EDFs

We also define a new type of EDF defined using this digraph framework.

Definition: Complete bipartite digraph $\overrightarrow{K}_{a,b}$

We define the oriented complete bipartite digraph $\overrightarrow{K}_{a,b}$: bipartition $A \cup B$ where $A = \{0, \ldots, a-1\}$ and $B = \{a, \ldots, a+b-1\}$; the standard set of directed edges will be $\overrightarrow{E}(\overrightarrow{K}_{a,b}) := \{(i,j) : i \in A, j \in B\}$.

Here we show the digraph framework way to describe a strong EDF:

Definition

Let $\mathcal{A} = \{A_0, \ldots, A_{m-1}\}$ be a collection of disjoint l-subsets of a group G. $\mathcal{A}$ is an (n, m, l, λ)-strong EDF (SEDF) precisely if, for each i, $(A_0, A_1, \ldots, A_{i-1}, A_{i+1}, \ldots A_{m-1}; A_i)$ is,an $(n, m, l, \lambda; \overrightarrow{K}_{m-1,1})$-EDF.

Directed and Undirected Digraph Defined EDFs

Theorem (2025, *SH\CJ\SM*)

Let G be a group of order n. Let H be a graph on m vertices and let $\overrightarrow{H}$ denote any orientation of H. If $\mathcal{A}$ is an $(n, m, l, \lambda; \overrightarrow{H})$-EDF, then $\mathcal{A}$ is an $(n, m, l, 2\lambda; H)$-EDF.

Theorem (2025, *SH\CJ\SM*)

Let G be a group of order n. Let H be a graph on m vertices and let $\overrightarrow{H}$ denote any orientation of H. If $\mathcal{A} = (A_0, \ldots, A_{m-1})$ is an $(n, m, l, \lambda; H)$-EDF and $\Delta(A_i, A_j) = \Delta(A_j, A_i)$ for all $0 \leq i \neq j \leq m-1$ then λ is even and $\mathcal{A}$ is an $(n, m, l, \lambda/2; \overrightarrow{H})$-EDF.

Strong Circular External Difference Families

Definition: Shannon Veitch and Douglas R. Stinson (2023)

A strong $(n, m, l, \lambda)-$circular EDF in a group G is a set of m disjoint subsets of G with size l such that each non-zero element from G occurs precisely λ times as a difference between A_i and A_j where

$$j \equiv i + c \mod m$$

for each $0 \leq j \leq m - 1$.

Theorem: Huawei Wu, Jing Yang and Keqin Feng (2024)

An $(n, m, l; \lambda) - 1-$SCEDF in a finite abelian group G exists only when $m = 2$.

Theorem: Huawei Wu, Jing Yang and Keqin Feng (2024)

All SCEDFs are constructed by patching together several SEDFs with the parameter $m = 2$.

Maura B. Paterson and Douglas R. Stinson (2024)

Theorem

If $m \equiv 0 \mod 4$, *then there is an* $(ml^2+1, m, l; 1) - 1-CEDF$ *on an additive abelian group for any* $l \geq 1$.

Theorem

If $m \equiv 2 \mod 4$, *then there is an* $(ml^2+1, m, l; 1) - 1-CEDF$ *on an additive abelian group for any* $l \geq 1$.

Theorem

If l *and* m *are odd then there is no* $(ml^2+1, m, l; 1) - 1-CEDF$ *in an additive abelian group.* *(Update: in a cyclic group)*

CEDF Construction

Shannon Veitch, Douglas R. Stinson (2023)

Let $q = 4m + 1$ be a prime power, let $\alpha \in \mathbb{F}_q$ be a primitive element. Define

$$A_0 = \{1, \alpha^{2m}\}$$

and for $1 \leq j \leq m - 1$ define

$$A_j = \alpha^{2j} A_0.$$

Then $\{A_0, A_1, \ldots A_{m-1}\}$ is a $(q, m, 2, 1) - 1-$CEDF in $\mathbb{F}_q$ if and only if $\alpha^4 - 1$ is a quadratic non-residue.

Example

Let $m = 4$ then $q = \mathbb{Z}_{17}$, $\alpha = 3$ is a primitive element, $\alpha^4 - 1 = 12$ is a quadratic non-residue so the following sets form a $(17, 4, 2, 1) - 1-$CEDF:

$$A_0 = \{1, 16\}, A_1 = \{9, 8\}, A_2 = \{13, 4\}, A_3 = \{15, 2\}$$

-	1 16	9 8	13 4	15 2
1 16				3 16 1 14
9 8	8 10 7 9			
13 4		4 5 12 13		
15 2			2 11 6 15	

Non-Cyclic CEDFs

Theorem (2025, *SH\CJ\SM*)

Let $l \equiv 3 \mod 4$ ($l \in \mathbb{N}$). Denote $z = \frac{3}{4}(l-1)^2 \in \mathbb{N}$. Define the following subsets of $\mathbb{Z}_{\frac{3l^2+1}{2}} \times \mathbb{Z}_2$:

- $A_0 = \bigcup_{i=0}^{l-1}\{(i,0)\}$
- $A_1 = \bigcup_{i=0}^{l-1}\{(z(i-1)-l-i, i+1\}$
- $A_2 = \bigcup_{i=0}^{l-1}\{(zi-l, i\}$.

Then (A_0, A_1, A_2) form a $(3l^2+1, 3, l, 1)$-1-CEDF in the non-cyclic abelian group $\mathbb{Z}_{\frac{3l^2+1}{2}} \times \mathbb{Z}_2$.

New CEDF Construction

Theorem (2025, $SH\backslash CJ\backslash SM$)

Let $m = 2$, $l \in \mathbb{Z}$ and let d be a divisor of l. Define $\mathcal{A} = (A_0, A_1)$, where A_0 and A_1 are subsets of $\mathbb{Z}_{2l^2+1}$ defined as:

- $A_0 = \{i : 0 \leq i \leq l-1\}$;
- $A_1 = \bigcup_{j=0}^{d-1} \{\frac{l^2(2j+1)}{d} + (i+1)l : 0 \leq i \leq \frac{l}{d} - 1\}$.

$\mathcal{A}$ is a $(2l^2+1, 2, l, 1) - 1-$CEDF in $\mathbb{Z}_{2l^2+1}$.

Example

$\{A_0 = \{0, 1, 2\}, A_1 = \{12, 15, 18\}\}$ and
$\{B_0 = \{0, 1, 2\}, B_1 = \{6, 12, 18\}\}$ are (19,2,3,1)-EDF in $\mathbb{Z}_{19}$.

d=1	0 1 2	12 15 18
0		7 4 1
1		8 5 2
2		9 6 3
12	12 11 10	
15	15 14 13	
18	18 17 16	

d=3	0 1 2	6 12 18
0		13 7 1
1		14 8 2
2		15 9 3
6	6 5 4	
12	12 11 10	
18	18 17 16	

For two (n, m, l, λ)-c-CEDFs in G $\mathcal{A} = (A_0, \ldots, A_{m-1})$ and $\mathcal{B} = (B_0, \ldots, B_{m-1})$, there is a notion of equivalence such that if $\mathcal{A}$ is equivalent to $\mathcal{B}$ then the difference multisets have the 'same structure'.

New CEDF Construction and CEDF Equivalence

Example

$\{A_0 = \{0, 1, 2\}, A_1 = \{12, 15, 18\}\}$ and
$\{B_0 = \{0, 1, 2\}, B_1 = \{6, 12, 18\}\}$ are (19,2,3,1)-EDF in $\mathbb{Z}_{19}$.

d=1	0 1 2	12 15 18
0		7 4 1
1		8 5 2
2		9 6 3
12	12 11 10	
15	15 14 13	
18	18 17 16	

d=3	0 1 2	6 12 18
0		13 7 1
1		14 8 2
2		15 9 3
6	6 5 4	
12	12 11 10	
18	18 17 16	

For two (n, m, l, λ)-c-CEDFs in G $\mathcal{A} = (A_0, \ldots, A_{m-1})$ and $\mathcal{B} = (B_0, \ldots, B_{m-1})$, there is a notion of equivalence such that if $\mathcal{A}$ is equivalent to $\mathcal{B}$ then the difference multisets have the 'same structure'.

More New CEDF Constructions

Theorem (2025, *SH\CJ\SM*)

Let $m \in \mathbb{Z}$ be even and let $l \in \mathbb{Z}$.
Define $\mathcal{A} = (A_0, A_1, A_2, \ldots, A_{m-3}, A_{m-2}, A_{m-1})$ to be the following (ordered) collection of sets in $\mathbb{Z}_{ml^2+1}$:

- $A_0 = \{i : 0 \leq i \leq l-1\}$;
- $A_1 = \{l^2 + (i+1)l : 0 \leq i \leq l-1\}$;
- for $1 \leq r \leq \frac{m}{2} - 1$,

$$A_{2r} = \{(2r-1)l^2 + i : 0 \leq i \leq l-1\} \text{ and}$$

$$A_{2r+1} = \{(\frac{m}{2} + r)l^2 + (i+1)l : 0 \leq i \leq l-1\}.$$

when $m \in \{2, 4, 6, 8\}$, $\mathcal{A}$ is a $(ml^2+1, m, l, 1)$-1-CEDF in $\mathbb{Z}_{ml^2+1}$.

Adjacent-Disjoint CEDFs

Definition

An $(n, m, l, \lambda) - \textit{adjacent} - \textit{disjoint} - c -$ circular EDF in a group G is a set $\{A_0, A_1, \ldots, A_{m-1}\}$ of subsets of G with size l such that the multiset of differences between all pairs of sets A_i and A_j where

$$j \equiv i + c \mod m$$

consists of λ copies of $G \backslash \{0\}$.

This construction is similar to an CEDF, without the condition that non-adjacent sets are disjoint.

Adjacent-Disjoint CEDF Constructions

Theorem (2025, *SH\CJ\SM*)

Let $m \in \mathbb{Z}$ be even and let $l \in \mathbb{Z}$.
Define $\mathcal{A} = (A_0, A_1, A_2, \ldots, A_{m-3}, A_{m-2}, A_{m-1})$ to be the following (ordered) collection of sets in $\mathbb{Z}_{ml^2+1}$:

- $A_0 = \{i : 0 \leq i \leq l-1\}$;
- $A_1 = \{l^2 + (i+1)l : 0 \leq i \leq l-1\}$;
- for $1 \leq r \leq \frac{m}{2} - 1$,

$$A_{2r} = \{(2r-1)l^2 + i : 0 \leq i \leq l-1\} \text{ and}$$

$$A_{2r+1} = \{(\frac{m}{2} + r)l^2 + (i+1)l : 0 \leq i \leq l-1\}.$$

$\mathcal{A}$ is a $(ml^2+1, m, l, 1)$-1-Adjacent-Disjoint-CEDF in $\mathbb{Z}_{ml^2+1}$.

More Adjacent-Disjoint Constructions

Theorem (2025, *SH\CJ\SM*)

Let m be even and $l(>1) \in \mathbb{Z}$. Consider the following subsets of $\mathbb{Z}_{ml^2+1}$:

- $A_0 = \{i : 0 \leq i \leq l-1\}$;
- for $1 \leq r \leq (m-4)/2$, $A_r = \{2l^2r + l + i : 0 \leq i \leq l-1\}$;
- $A_{(m-2)/2} = \{(m-2)l^2 + i : 0 \leq i \leq l-1\}$;
- $A_{m/2} = \{(m-2)l^2 + 2l(i+1) : \ 0 \leq i \leq l-1\}$.

Then $(A_0, A_{m/2}, A_1, A_{m/2}, \ldots, A_{(m-2)/2}, A_{m/2})$ is an $(ml^2+1, m, l, 1)$-adjacent disjoint CEDF.

Remark

With the same set $A_{m/2}$ occurring multiple times this is also equivalent to a $(ml^2+1, m/2+1, l, 1; K_{m/2,1})$- EDF where the sets are $(A_0, A_1, \ldots, A_{(m-2)/2}; A_{m/2})$.

Equivalence in Adjacent-Disjoint Constructions

Theorem (2025, SM)

Let m be even and $l, d \in \mathbb{Z}$ where d divides l then define the following sets in $\mathbb{Z}_{ml^2+1}$:

- $A_0 = \{i : 0 \leq i \leq l-1\}$
- for $0 \leq r \leq \frac{m}{2} - 1$,

$$A_{2r+1} = \bigcup_{k=0}^{d-1} \{\frac{(2k+1)l^2}{d} + 2rl^2 + (i+1)l : 0 \leq i \leq \frac{l}{d} - 1\}$$

- for $0 \leq r \leq \frac{m}{2} - 2$,

$$A_{2(r+1)} = \{\frac{l^2}{d} + i : 0 \leq i \leq l-1\}$$

Then $(A_0, A_1, \ldots, A_{m-2}, A_{m-1})$ is a $(ml^2+1, m, l, 1)$ adjacent-disjoint CEDF in $\mathbb{Z}_{ml^2+1}$, where each distinct value of d corresponds to a non-equivalent adjacent-disjoint CEDF.

Non-Abelian CEDFs

Example

Here is a $(D_{28}, 3, 3, 1)-$CEDF:$\{A_0 = \{id, r^{11}, r^8\}, A_1 = \{r^4, sr^2, sr^6\}, A_2 = \{r^3, r^5, sr^4\}\}$

-	id r^{11} r^8	r^4 sr^2 sr^6	r^3 r^5 sr^4
id r^{11} r^8			r^{11} r^9 sr^4 r^8 r^6 sr^7 r^5 r^3 sr^{10}
r^4 sr^2 sr^6	r^4 r^{10} r^7 $sr^2 sr^8 sr^5$ $sr^6 sr^{12} sr^9$		
r^3 r^5 sr^4		$r^{13} sr^{13} sr^3$ r sr^{11} sr s r^{12} r^2	

Further Information

- CEDF background: "Circular external difference families, graceful labellings and cyclotomy", Maura B. Paterson and Douglas R. Stinson, Discrete Mathematics 347 (2024),
- Our recent work: "Digraph-defined external difference families and new circular external difference families", Sophie Huczynska, Christopher Jefferson, Struan McCartney , ArXiV preprint arXiv:2504.20959.

Further Work

- Continue investigating non-cyclic and non-abelian CEDFs.
- Working with External Difference Families in a directed graph theoretical framework.
  -Bipartite Graphs
  -Tournaments
  -Bidirectional Cycles
  -Paths
- Consider in which groups can we obtain a directed graph defined EDF for a specific digraph H.