New cyclic PBIBD(2)s obtained using finite field cyclotomy

Laura Johnson (School of Mathematics and Statistics - University of St. Andrews)

CoDesCo'24

Joint work with Sophie Huczynska (Mathematics and Statistics - St. Andrews)

July 19, 2024

Background

Definition

A **Balanced Incomplete Block Design** (or **BIBD**) is a design that is;

- defined on v varieties (or points),
- consists of b blocks (or sets),
- each block is of size k,
- each variety occurs in r blocks,
- each pair of varieties occur together in precisely λ blocks.

- It is not always possible to construct BIBDs for particular sets of parameters.
- When it is not possible to construct a BIBD for a particular set of parameters, PBIBD(n)s can be used as an alternative design.

Plan of talk

- Introduce PBIBD(2)s.
- Explain the connection between PDSs and PBIBD(2)s.
- Define DPDFs and explain how they can be used to generate new PBIBD(2) constructions.
- Demonstrate how finite field cyclotomy can be used to build DPDFs that in turn produce PBIBD(2)s with "desirable" parameters.

What are PBIBD(2)s?

PBIBD(2)s slightly compromise on the requirement that all pairs of varieties must co-occur in precisely λ blocks of the design.

Definition

A **Partially Balanced Incomplete Block Design with 2 association classes** (or **PBIBD(2)**) is a 2-design which is;

- based on a set of v varieties, with an underlying 2-class association scheme,
- consists of b blocks,
- each block is of size k,
- each variety occurs in r blocks of the design,
- any pair of first associates occur λ_1 times in the same block,
- any pair of second associates occur λ_2 times in the same block.

Example of a PBIBD(2)

In $\mathbb{Z}_5$ there exists an association scheme in which the first associates of;

0 are 1 and 4
1 are 0 and 2
2 are 1 and 3
3 are 2 and 4
4 are 3 and 0

The set of second associates of each element of $\mathbb{Z}_5$ is the set of elements that are not first associates of that particular element i.e. the second associates of 1 are 3 and 4.

Under this association scheme, we can see that the following blocks form a PBIBD(2): $\{1,4\},\{2,0\},\{3,1\},\{4,2\},\{0,3\}$.

Definition

A set $S \subset \mathrm{G}$ is a **Partial Difference Set** (or **PDS**), if each element of S occurs as a pairwise difference between distinct elements of S precisely λ times, and each element of $\mathrm{G}^* \backslash S$ occurs precisely μ times as a pairwise difference between elements of S. S is said to be a **regular** PDS if $0 \notin S$ and $S = -S$.

Proposition (Ma (1984))

A PDS, S, is regular if and only if S forms an association scheme in which the first associates of a variety g are the elements of the set $g + S$, and the second associates are all non-identity elements of G not contained in this set. (These are now known as cyclic association schemes.)

Relationship between cyclic PBIBD(2)s and PDSs

In this talk, we will particularly be focussing on constructing cyclic PBIBDs. A PBIBD is said to be **cyclic** if the underlying association scheme is cyclic.

Theorem

The development of a regular PDS is a PBIBD(2).

Definition

The **development** of a collection of subsets, S', in a group G is the series of blocks found by adding each element of G in turn to each of the blocks in S'.

Partial Difference Set Example

Example

The set $\{1,4\}$ forms a regular PDS in the group $\mathbb{Z}_5$ in which $\lambda = 0$ and $\mu = 1$.

-	1	4
1	-	2
4	3	-

Using this PDS, we can generate an association scheme under which the first associates of 1 are $1 + \{1,4\} = \{2,0\}$ and the second associates of 1 are $\{3,4\}$. Since $\{1,4\}$ is a regular PDS in $\mathbb{Z}_5$, when we develop this subset we form the PBIBD in our initial example.

Disjoint Partial Difference Families

Internal difference = pairwise difference between elements contained within the same subset.

Definition (Huczynska and J. (2023))

A **Disjoint Partial Difference Family** (or **DPDF**), $S' = \{D_1, \ldots, D_m\} \subset \mathrm{G}$ (where G is a group) is;

- a collection of disjoint k-subsets comprising elements of G^*,
- the multiset of all internal differences within the component sets of S' comprises λ copies of every element in $S = \cup_{i=1}^{m} D_i$,
- the multiset of all internal differences within the component sets of S' comprises μ copies of every element in $\mathrm{G}^* \backslash S$.

Theorem (J. (Upcoming Preprint))

Let S' be a DPDF partitioning a regular PDS, S. Then the development of S' is a cyclic PBIBD(2).

Introducing finite field cyclotomy

Definition

In the finite field $\mathrm{GF}(q)$ of order $q = ef + 1$, let $0 \leq i \leq e - 1$ and α be a primitive element of $\mathrm{GF}(q)$. We define the i^{th} **cyclotomic class** of order e, C_i^e, in $\mathrm{GF}(q)$ to be the set:

$$C_i^e = \alpha^i \langle \alpha^e \rangle.$$

Cyclotomic Numbers

Let $\mathrm{GF}(q)$ be a finite field of order $q = ef + 1$ and let α be a primitive element of $\mathrm{GF}(q)$. For a fixed $0 \leq i, j \leq e - 1$, the **cyclotomic number** $(i, j)_e$ is the number of ordered pairs (s, t) (where $0 \leq s, t \leq f - 1$) such that

$$\alpha^{es+i} = \alpha^{et+j} - 1,$$

where $\alpha^{es+i} \in C_i^e$ and $\alpha^{et+j} \in C_j^e$.

Constructing DPDFs using finite field cyclotomy

Below I have rewritten the elements of the pairwise differences between distinct elements of C_i^e in terms of an element of C_i^e multiplying an element of $C_0^e - 1 = \{\alpha^{me} - 1 | \alpha^{me} \in C_0^e\}$.

-	1	$\alpha^{\epsilon+i}$	$\alpha^{2\epsilon+i}$	$\dots$	$\alpha^{\epsilon+i(f-1)}$
1	-	$\alpha^{\epsilon+i}(\alpha^{\epsilon(f-1)}-1)$	$\alpha^{2\epsilon+i}(\alpha^{\epsilon(f-2)}-1)$	$\dots$	$\alpha^{\epsilon(f-1)+i}(\alpha^{\epsilon}-1)$
$\alpha^{\epsilon+i}$	$\alpha^{i}(\alpha^{\epsilon}-1)$	-	$\alpha^{2\epsilon+i}(\alpha^{\epsilon(f-1)}-1)$	$\dots$	$\alpha^{\epsilon+i(f-1)}(\alpha^{2\epsilon}-1)$
$\alpha^{2\epsilon+i}$	$\alpha^{i}(\alpha^{2\epsilon}-1)$	$\alpha^{\epsilon+i}(\alpha^{\epsilon}-1)$	-	$\dots$	$\alpha^{\epsilon(f-1)+i}(\alpha^{3\epsilon}-1)$
$\alpha^{3\epsilon+i}$	$\alpha^{i}(\alpha^{3\epsilon}-1)$	$\alpha^{\epsilon+i}(\alpha^{2\epsilon}-1)$	$\alpha^{2\epsilon+i}(\alpha^{\epsilon}-1)$	$\dots$	$\alpha^{\epsilon(f-1)+i}(\alpha^{4\epsilon}-1)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\alpha^{\epsilon(f-1)+i}$	$\alpha^{i}(\alpha^{\epsilon(f-1)}-1)$	$\alpha^{\epsilon+i}(\alpha^{\epsilon(f-2)}-1)$	$\alpha^{2\epsilon+i}(\alpha^{\epsilon(f-3)}-1)$	$\dots$	-

This framework was developed in my joint paper with S. Huczynska entitled "Disjoint and External Partial Difference Families".

Constructing DPDFs using finite field cyclotomy

In this way, we can partition a larger cyclotomic class C_0^ϵ into a series of smaller $C_0^e, C_\epsilon^e, \ldots, C_{e-\epsilon}^e$. We can then view "diagonals" running through each of the multisets as copies of some cyclotomic class C_i^ϵ.

$$\begin{array}{c|ccccc} & C_0^e & C_1^e & C_2^e & \cdots \\ \hline C_0^e & \Delta(C_0^e) & & & \cdots \\ C_1^e & & \Delta(C_\epsilon^e) & & \cdots \\ C_2^e & & & \Delta(C_{2\epsilon}^e) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

If we can identify which cyclotomic class the value of $0 \leq i \leq \epsilon - 1$ satisfying $\alpha^{er} - 1 \in C_i^\epsilon$ for each $0 \leq r \leq f - 1$, we can determine whether $C_0^e, C_\epsilon^e, \ldots, C_{e-\epsilon}^e$ forms a DPDF.

Relevant cyclotomic DPDF results

The most "useful" PBIBD(2)s are PBIBD(2)s in which the values of λ and μ are close. For this reason, in my research into using DPDFs to construct new PBIBD(2)s has focussed on DPDFs that partition the Paley PDS.

Theorem (Paley (1933))

Let $\mathrm{GF}(q)$ be a finite field of order $q \equiv 1 \mod 4$, then C_0^2 is a PDS in which $\lambda' = \frac{q-5}{4}$ and $\mu' = \frac{q-1}{4}$.

Theorem Summary (Huczynska and J. 2023)

Let $\mathrm{GF}(q)$ be a finite field of order $q \equiv 1 \mod 4$ and $(C_0^2)' = \{C_0^e, C_2^e, \ldots, C_{e-2}^e\}$ be a partition of the squares into smaller cyclotomic classes. Then $(C_0^2)'$ is a DPDF.

The literature focusses on PBIBD(2)s focusses on constructions in which $2 \leq k \leq 10$, so I have focussed on constructing DPDFs with set sizes in this range.

Relevant cyclotomic DPDF results

In the paper "Difference systems of sets and cyclotomy", Mutoh and Tonchev implictly obtain the λ and μ values for all DPDFs which partition the Paley PDSs and in which the component sets have cardinality in the range $[2,6]$.

Sample Theorem (J. (Upcoming Preprint))

Let $\mathrm{GF}(p)$ be a finite field of order $p = 3e + 1 \equiv 1 \mod 4$, where p is prime and $e = \frac{p-1}{3}$ is even. Let $(C_0^2)' = \{C_0^e, C_2^e, \ldots, C_{e-2}^e\}$, then $(C_0^2)'$ is;

(i) a DPDF in which $\lambda = 2$ and $\mu = 0$ when $(-3)^{\frac{e-1}{4}} \equiv 1 \mod p$,

(ii) a DPDF in which $\lambda = 0$ and $\mu = 2$ when $(-3)^{\frac{e-1}{4}} \equiv -1 \mod p$.

Intuition behind the proof of this result

This result essentially works by computing the values of $\alpha^e - 1$ (and therefore $\alpha^{2e} - 1$).

Steps of the proof

(i) By Lagrange's Theorem, $\alpha^{3e} - 1 = (\alpha^e - 1)(\alpha^2 e + \alpha^e + 1) = 0$, this means $\alpha^{2e} + 1 = -\alpha^e$.

(ii) This means $(\alpha^e - 1)^2 = \alpha^{2e} - 2\alpha^e + 1 = -3\alpha^e$, so $\alpha^e - 1$ will be a square if and only if $-3\alpha^e$ is a fourth power.

(iii) Since $p \equiv 1 \mod 4$, we can deduce $e \equiv 0 \mod 4$ and so α^e is fourth power, so the result is determined by whether -3 is a fourth power or a square.

Using similar finite field properties, I have identify the expand upon these DPDF results to obtain λ and μ values for $7 \leq f \leq 10$.

Further Work/Research Questions

- Verify new PBIBD(2) parameters that can be obtained using these techniques.
- Can we produce overarching DPDF results for values of $2 \leq f \leq 10$, when the DPDFs in question partition cyclotomic PDSs which are not the squares?
- Can the cyclotomic results that we have produced as part of this project be used to generate any other types of interesting designs?
- Can we use similar properties of finite fields to obtain results in finite fields of order q, where q is a prime power?
- Can we improve upon our current cyclotomic results to produce slicker results for $2 \leq f \leq 10$?

Thank you for listening to my talk!