Partially Balanced Incomplete Block Designs

Sushmita Ruj

Indian Statistical Institute, Kolkata
E-mail: sush@isical.ac.in
Homepage: http://www.isical.ac.in/~sush
Outline

1. Introduction
2. Association Schemes
3. PBIBD
4. Two-Associate class PBIBDs
5. Practical Application of PBIBD
A *BIBD*\((v, b, r, k, \lambda)\), is a *design* which satisfy the following conditions:

1. \(|X| = v, |A| = b|,
2. Each subset in \(A\) contains exactly \(k\) elements,
3. Each variety in \(X\) occurs in \(r\) many blocks,
4. Each pair of varieties in \(X\) is contained in exactly \(\lambda\) blocks in \(A\).
A $BIBD(v, b, r, k, \lambda)$ is a design which satisfy the following conditions:

1. $|X| = v$, $|\mathcal{A}| = b$,
2. Each subset in $\mathcal{A}$ contains exactly $k$ elements,
3. Each variety in $X$ occurs in $r$ many blocks,
4. Each pair of varieties in $X$ is contained in exactly $\lambda$ blocks in $\mathcal{A}$.

$X = \{0, 1, 2, 3, 4, 5\}$

$\mathcal{A} = \{\{0, 1, 2\}, \{0, 1, 3\}, \{0, 2, 4\}, \{0, 3, 5\}, \{0, 4, 5\}, \{1, 2, 5\}, \{1, 3, 4\}, \{1, 4, 5\}, \{2, 3, 4\}, \{2, 3, 5\}\}$

The above design is a $(6, 10, 5, 3, 2)$-design.
Balanced Incomplete BLock Designs

- A *BIBD* \((v, b, r, k, \lambda)\), is a design which satisfy the following conditions:
  1. \(|X| = v, |A| = b\),
  2. Each subset in \(A\) contains exactly \(k\) elements,
  3. Each variety in \(X\) occurs in \(r\) many blocks,
  4. Each pair of varieties in \(X\) is contained in exactly \(\lambda\) blocks in \(A\).

- \(X = \{0, 1, 2, 3, 4, 5\}\)
- \(A = \{\{0, 1, 2\}, \{0, 1, 3\}, \{0, 2, 4\}, \{0, 3, 5\}, \{0, 4, 5\}, \{1, 2, 5\}, \{1, 3, 4\}, \{1, 4, 5\}, \{2, 3, 4\}, \{2, 3, 5\}\}\)
- The above design is a \((6, 10, 5, 3, 2)\)-design
- \(\lambda\) has one value - balanced
- Partially balanced: Many values of \(\lambda\).
Partially Balanced Incomplete Block Designs

- Proposed by R. C. Bose
- Earlier work by Nair, Shimamoto, Clatworthy, C R Rao
- Practical and theoretical interests
- Theoretical: proving existence results of BIBDs
- Constructions of Transversal designs etc
- Practical: Group testing
- Designing Visual Secret sharing schemes
- Key management in WSN
Association schemes

Def: Association schemes

Association scheme with \( m \)-associate classes on a \( v \)-set \( X \) is a family of symmetric, anti-reflexive binary relations on \( X \), such that

- Any two distinct elements are \( i^{th} \) associate for exactly one value of \( i \), where \( 1 \leq i \leq m \),
- Each element of \( X \) has \( n_i \) \( i \)-th associates \( 1 \leq i \leq m \),
- For each \( i \), \( 1 \leq i \leq m \), if \( x \) and \( y \) are \( i \)-th associates, then there are \( p_{ji}^l \) elements of \( X \) which are both \( j \)-th associates of \( x \) and \( l \)-th associates of \( y \).

\( v, n_i \ (1 \leq i \leq m) \) and \( p_{ji}^l \ (1 \leq i, j, l \leq m) \) are called the parameters of the association scheme.
### Association schemes-example

\[ X = \{1, 2, 3, 4, 5, 6\} \]

<table>
<thead>
<tr>
<th>Element</th>
<th>Associates</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2,3</td>
<td>4</td>
<td>5,6</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1,3</td>
<td>5</td>
<td>4,6</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1,2</td>
<td>6</td>
<td>4,5</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>5,6</td>
<td>1</td>
<td>2,3</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>4,6</td>
<td>2</td>
<td>1,3</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>4,5</td>
<td>3</td>
<td>1,2</td>
<td></td>
</tr>
</tbody>
</table>
Association schemes-example

\[ X = \{1, 2, 3, 4, 5, 6\} \]

<table>
<thead>
<tr>
<th>Element</th>
<th>First</th>
<th>Second</th>
<th>Third</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2,3</td>
<td>4</td>
<td>5,6</td>
</tr>
<tr>
<td>2</td>
<td>1,3</td>
<td>5</td>
<td>4,6</td>
</tr>
<tr>
<td>3</td>
<td>1,2</td>
<td>6</td>
<td>4,5</td>
</tr>
<tr>
<td>4</td>
<td>5,6</td>
<td>1</td>
<td>2,3</td>
</tr>
<tr>
<td>5</td>
<td>4,6</td>
<td>2</td>
<td>1,3</td>
</tr>
<tr>
<td>6</td>
<td>4,5</td>
<td>3</td>
<td>1,2</td>
</tr>
</tbody>
</table>

- Any two distinct elements are \(i^{th}\) associate for exactly one value of \(i\), where \(1 \leq i \leq m\), \(\sqrt{\text{✓}}\)
- Each element of \(X\) has \(n_I\) \(i^{th}\) associates \(1 \leq i \leq m\), \(n_1 = 2, n_2 = 1, n_3 = 2\)
- For each \(i, 1 \leq i \leq m\), if \(x\) and \(y\) are \(i^{th}\) associates, then there are \(p_{jl}^i\) elements of \(X\) which are both \(j^{th}\) associates of \(x\) and \(l^{th}\) associates of \(y\).

\[
P_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 0 \\ 2 & 0 & 0 \end{pmatrix}, \quad P_3 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}
\]
A PBIBD($v, k, r, k; \lambda_1, \lambda_2, \ldots, \lambda_m$), PBIBD *with m associate class* is a design on a set $X$, such that

- $|X| = v$,
- Number of blocks is $b$,
- Each block contains $k$ elements,
- Each element is repeated in $r$ blocks,
- If $x$ and $y$ are the $i$-th associates, for $1 \leq i \leq m$, then they occur together in $\lambda_i$ blocks.
PBIBD-example

<table>
<thead>
<tr>
<th>Element</th>
<th>First</th>
<th>Second</th>
<th>Third</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2,3</td>
<td>4</td>
<td>5,6</td>
</tr>
<tr>
<td>2</td>
<td>1,3</td>
<td>5</td>
<td>4,6</td>
</tr>
<tr>
<td>3</td>
<td>1,2</td>
<td>6</td>
<td>4,5</td>
</tr>
<tr>
<td>4</td>
<td>5,6</td>
<td>1</td>
<td>2,3</td>
</tr>
<tr>
<td>5</td>
<td>4,6</td>
<td>2</td>
<td>1,3</td>
</tr>
<tr>
<td>6</td>
<td>4,5</td>
<td>3</td>
<td>1,2</td>
</tr>
</tbody>
</table>

Design:

124 134 235 456
125 136 236 456

\( v = 6, \ b = 8, \ r = 4, \ k = 3 \)

\( \lambda_1 = \lambda_2 = 2, \ \lambda_3 = 1 \)
Parameters of PBIBD

The parameters of a PBIBD must satisfy the following conditions:

- \( vr = bk \),
- \( \sum_{i=1}^{m} n_i = v - 1 \),
- \( \sum_{i=1}^{m} n_i \lambda_i = r(k - 1) \),
- \( n_i p_{jh}^i = n_j p_{ih}^j \).
Two-Associate class PBIBDs

Most widely used
- Group-divisible ✓
- Triangular ✓
- Latin-square-type
- Cyclic
- Partial Geometry type
Group-Divisible PBIBD

Def: Group Divisible Association scheme

Let $X$ be a set of $v$ elements, such that, $G_i \subseteq X$, $1 \leq i \leq m$, and $G_i \cap G_j = \emptyset$ for $i \neq j$, and $X = \bigcup_{i=1}^{m} G_i$. An association scheme on $X$ is said to be group divisible, if the elements in the same group are first associates and those in different groups are second associates.

\[ X = \{1, 2, \ldots, 12\}, \quad m = 4 \]

\[ G_1 = \{1, 2, 3\} \]
\[ G_2 = \{4, 5, 6\} \]
\[ G_3 = \{7, 8, 9\} \]
\[ G_4 = \{10, 11, 12\} \]

<table>
<thead>
<tr>
<th>Element</th>
<th>First</th>
<th>Associates</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>First</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2, 3</td>
</tr>
<tr>
<td>2</td>
<td>1, 3</td>
<td>4, 5, 6, 7, 8, 9, 10, 11, 12</td>
</tr>
<tr>
<td>3</td>
<td>1, 2</td>
<td>4, 5, 6, 7, 8, 9, 10, 11, 12</td>
</tr>
<tr>
<td>4</td>
<td>5, 6</td>
<td>1, 2, 3, 7, 8, 9, 10, 11, 12</td>
</tr>
<tr>
<td>5</td>
<td>4, 6</td>
<td>1, 2, 3, 7, 8, 9, 10, 11, 12</td>
</tr>
<tr>
<td>6</td>
<td>4, 5</td>
<td>1, 2, 3, 7, 8, 9, 10, 11, 12</td>
</tr>
<tr>
<td>7</td>
<td>8, 9</td>
<td>1, 2, 3, 4, 5, 6, 10, 11, 12</td>
</tr>
<tr>
<td>8</td>
<td>7, 9</td>
<td>1, 2, 3, 4, 5, 6, 10, 11, 12</td>
</tr>
<tr>
<td>9</td>
<td>7, 8</td>
<td>1, 2, 3, 4, 5, 6, 10, 11, 12</td>
</tr>
<tr>
<td>10</td>
<td>11, 12</td>
<td>1, 2, 3, 4, 5, 6, 7, 8, 9</td>
</tr>
<tr>
<td>11</td>
<td>10, 12</td>
<td>1, 2, 3, 4, 5, 6, 7, 8, 9</td>
</tr>
<tr>
<td>12</td>
<td>10, 11</td>
<td>1, 2, 3, 4, 5, 6, 7, 8, 9</td>
</tr>
</tbody>
</table>
### Group divisible PBIBD-example

<table>
<thead>
<tr>
<th>$G_1$</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_2$</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>$G_3$</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>$G_4$</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$B_1$</th>
<th>1</th>
<th>4</th>
<th>7</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$B_2$</td>
<td>1</td>
<td>5</td>
<td>8</td>
<td>11</td>
</tr>
<tr>
<td>$B_3$</td>
<td>1</td>
<td>6</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>$B_4$</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>$B_5$</td>
<td>2</td>
<td>5</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>$B_6$</td>
<td>2</td>
<td>6</td>
<td>7</td>
<td>12</td>
</tr>
<tr>
<td>$B_7$</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>11</td>
</tr>
<tr>
<td>$B_8$</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>12</td>
</tr>
<tr>
<td>$B_9$</td>
<td>3</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
</tbody>
</table>

What design is this?

Transversal design!
Group divisible PBIBD-example

\begin{align*}
G_1 & : 1 \quad 2 \quad 3 \\
G_2 & : 4 \quad 5 \quad 6 \\
G_3 & : 7 \quad 8 \quad 9 \\
G_4 & : 10 \quad 11 \quad 12 \\
B_1 & : 1 \quad 4 \quad 7 \quad 10 \\
B_2 & : 1 \quad 5 \quad 8 \quad 11 \\
B_3 & : 1 \quad 6 \quad 9 \quad 12 \\
B_4 & : 2 \quad 4 \quad 8 \quad 12 \\
B_5 & : 2 \quad 5 \quad 9 \quad 10 \\
B_6 & : 2 \quad 6 \quad 7 \quad 12 \\
B_7 & : 3 \quad 4 \quad 9 \quad 11 \\
B_8 & : 3 \quad 5 \quad 7 \quad 12 \\
B_9 & : 3 \quad 6 \quad 8 \quad 10
\end{align*}

What design is this? Transversal design!
Group-divisible PBIBD: TD

- Parameters: $\lambda_1 = 0$, $\lambda_2 = 1$
- $n_1 = n - 1$, $n_2 = n(m - 1)$
- $P_1 = \begin{pmatrix} n - 2 & 0 \\ 0 & n(m - 1) \end{pmatrix}$ $P_2 = \begin{pmatrix} 0 & n - 1 \\ n - 1 & n(m - 2) \end{pmatrix}$
The existence of a $PBIBD - (mn, nk; \lambda_1 = r, \lambda_2 = \lambda)$ design is equivalent to the existence of a $BIBD(m, k, \lambda)$. 

Proof: Delete an element $x$ and all occurrences from all the $r$ blocks that contain $x$. 

Results on Group-divisible PBIBDs
Results on Group-divisible PBIBDs

Theorem
The existence of a $PBIBD - (mn, nk; \lambda_1 = r, \lambda_2 = \lambda)$ design is equivalent to the existence of a $BIBD(m, k, \lambda)$.

Theorem
Given a $BIBD(v, k, 1)$, there exists a group divisible $PBIBD(v - 1, k; 0, 1)$.

Proof: Delete an element $x$ and all occurrences from all the $r$ blocks that contains $x$. 
Triangular PBIBD

- $X$ be a set of $v = n(n - 1)/2$ elements
- Arrange the elements in a symmetrical $n \times n$ array with diagonal elements as blanks
- Association is *triangular* if the first associates are elements in the same row and column, and second associates are the remaining elements
**Triangular PBIBD**

- Let $X$ be a set of $v = n(n - 1)/2$ elements.
- Arrange the elements in a symmetrical $n \times n$ array with diagonal elements as blanks.
- Association is *triangular* if the first associates are elements in the same row and column, and second associates are the remaining elements.
- $n_1 = 2(n - 2)$ and $n_2 = (n - 2)(n - 3)/2$

\[
P_1 = \begin{pmatrix}
  n - 2 & n - 3 \\
  n - 3 & (n - 3)(n - 4)/2 \\
\end{pmatrix}
\]

\[
P_2 = \begin{pmatrix}
  4 & 2n - 8 \\
  2n - 8 & (n - 4)(n - 5)/2 \\
\end{pmatrix}
\]
### Triangular PBIBD-example

<table>
<thead>
<tr>
<th>Triangular array</th>
<th>Blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 1 2 3 4</td>
<td>0 1 2 7 8</td>
</tr>
<tr>
<td>1 * 5 6 7</td>
<td>0 1 3 5 9</td>
</tr>
<tr>
<td>2 5 * 8 9</td>
<td>0 1 2 5 6</td>
</tr>
<tr>
<td>3 6 8 * 0</td>
<td>1 4 6 8 9</td>
</tr>
<tr>
<td>4 7 9 0 *</td>
<td>2 3 6 7 9</td>
</tr>
<tr>
<td></td>
<td>3 4 5 7 8</td>
</tr>
</tbody>
</table>
What is predistribution?

Distributing keys in nodes prior to deployment.

key-pool

\{0, 1, 2, 3, 4, 5, 6\}.  

Connectivity Ratio = 27/28 = 0.9643
What is predistribution?

Distributing keys in nodes prior to deployment.

**key-pool**

\{0, 1, 2, 3, 4, 5, 6\}.

Nodes and link between them
Probabilistic pairwise key establishment

  - Naive scheme, with pairwise keys between neighboring nodes
  - Good for static networks
  - Bad for mobile networks

- Q-Composite:
  - Distribute keys randomly like EG-scheme
  - Two nodes communicate when they share more than $q$ common keys

- Other schemes traded between memory, resilience to node compromise
Metrics to evaluate key predistribution schemes

- Memory
- Computation while key establishment
- Communication overheads
- Key Connectivity (probability of key share)
- Resilience to node compromise
Deterministic schemes

- Deterministic way of selecting keys from key pool or constructing common keys
- Easy to find common keys between two nodes
- Limited scalability
- Two broad classes
  - Polynomial based
  - Combinatorial design based
BIBD and Sensor nodes

Correspondence between a $\lambda - (v, b, r, k)$ design and sensor network.

- $v =$ key-pool size
- $b =$ number of sensor nodes
- $r =$ number of nodes in which a given key occurs
- $k =$ number of keys in a node (key-chain length)
- $\lambda =$ number of nodes which contain a given pair of keys

2-(6,10,5,3) :

Key-pool = \{0, 1, 2, 3, 4, 5\}

- $n_1 : \{0, 1, 2\}$
- $n_2 : \{0, 1, 3\}$
- $n_3 : \{0, 2, 4\}$
- $n_4 : \{0, 3, 5\}$
- $n_5 : \{0, 4, 5\}$
- $n_6 : \{1, 2, 5\}$
- $n_7 : \{1, 3, 4\}$
- $n_8 : \{1, 4, 5\}$
- $n_9 : \{2, 3, 4\}$
- $n_{10} : \{2, 3, 5\}$
Combinatorial Design based solutions

Combinatorial Design based solutions

- Camtepe and Yener (2004) : Generalized Quadrangles
- Lee and Stinson (2005) : Transversal Designs
- Chakrabarty, Maitra and Roy (2006) : Merging Blocks
- Ruj and Roy (2007) : Partially Balanced Incomplete Block Designs (PBIBDs)
- Ruj and Roy (2008) : Reed-Solomon codes
- Blackburn, Etzion, Martin and Paterson (2008) : Costas Arrays
- Ruj and Roy (2009) : Deterministic deployment
- Martin, Paterson, Stinson (2010) : Group Deployment
- Ruj, Nayak, Stojmenovic (2011) : Combinatorial trades
**Key predistribution using PBIBD**

A 2 - associate class PBIBD.
Firsts Associates : Elements belonging to the same row or column
Second Associates: Rest of the elements
First associate of 1 : 2, 3, 4, 5, 6, 7. Second associate of 1: 8, 9, 10

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>*</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>*</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>10</td>
<td>*</td>
<td>13</td>
<td>14</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>11</td>
<td>13</td>
<td>*</td>
<td>15</td>
</tr>
<tr>
<td>5</td>
<td>9</td>
<td>12</td>
<td>14</td>
<td>15</td>
<td>*</td>
</tr>
</tbody>
</table>

N8 = { 1, 6, 7, 8, 9, 4, 11, 13, 15 }
Key predistribution using PBIBD

A 2 - associate class PBIBD.
Firsts Associates: Elements belonging to the same row or column
Second Associates: Rest of the elements
First associate of 1: 2, 3, 4, 5, 6, 7. Second associate of 1: 8, 9, 10
Block 1: (2, 3, 4, 5, 6, 7) Block 2: (1, 3, 4, 5, 8, 9)
Block 3: (1, 2, 4, 6, 8, 10) Block 4: (1, 2, 3, 7, 9, 10)
Block 5: (1, 2, 6, 7, 8, 9) Block 6: (1, 3, 5, 7, 8, 10)
Block 7: (2, 4, 5, 6, 9, 10) Block 8: (2, 3, 5, 6, 9, 10)
Block 9: (2, 4, 5, 7, 8, 10) Block 10: (3, 4, 6, 7, 8, 9)

Main contribution resilience is better than existing schemes.
Food for thought

- Construction of new designs
- Finding existence results for different classes of designs
- New Applications
References

Curiouser and curiouser!!