A Combinatorial Design Method for Repairing Shares in Threshold Schemes

Douglas R. Stinson

David R. Cheriton School of Computer Science
University of Waterloo

Conference on Combinatorics and its Applications
In Celebration of Charlie Colbourn’s 65th Birthday

Singapore, July 16, 2018

This talk is based on joint work with Ruizhong Wei and Bailey Kacsmar
(t, n)-Threshold Schemes

• We informally define a \((t, n)\)-threshold scheme.
• Let \(t\) and \(n\) be positive integers, \(t \leq n\).
• A secret \(K\) is “split” into \(n\) shares, denoted \(s_1, \ldots, s_n\).
• The following two properties should hold:
  1. a reconstruction algorithm can be used to reconstruct the secret, given any \(t\) of the \(n\) shares,
  2. no \(t - 1\) shares reveal any information as to the value of the secret.

• Threshold schemes were invented independently by Blakley and Shamir in 1979.
• Shamir’s threshold scheme is based on polynomial interpolation over \(\mathbb{Z}_p\), where \(p \geq n + 1\) is prime.
• It is really a Reed-Solomon code in disguise.
Shamir Threshold Scheme

- In an **initialization phase**, \( x_1, x_2, \ldots, x_n \) are defined to be \( n \) distinct non-zero elements of \( \mathbb{Z}_p \).
- the **dealer** gives \( x_i \) to **user** \( U_i \), for all \( i, \ 1 \leq i \leq n \).
- The \( x_i \)’s are **public** information.
- For a given secret \( K \in \mathbb{Z}_p \), shares are created as follows:
  1. Let \( a(x) \in \mathbb{Z}_p[x] \) be a **random polynomial** of degree at most \( t - 1 \), such that the constant term is the secret, \( K \).
  2. For \( 1 \leq i \leq n \), the share \( s_i = a(x_i) \) (so the shares are evaluations of the polynomial \( a(x) \) at \( n \) non-zero points).
- Suppose we have \( t \) shares \( s_{i_j} = a(x_{i_j}), \ 1 \leq j \leq t \).
- Since \( a(x) \) is a polynomial of degree at most \( t - 1 \), we can determine \( a(x) \) by **Lagrange interpolation**.
- Then \( K \) is computed by substituting \( x = 0 \) into \( a(x) \).
Repairability

• Suppose that an arbitrary user $U_\ell$ (in a $(t, n)$-threshold scheme, say) loses their share.

• The goal is to find a secure protocol, involving $U_\ell$ and a subset of the other users, that allows the missing share $s_\ell$ to be reconstructed.

• We are considering a setting where the dealer is no longer present in the scheme after the initial setup.

• We will assume secure pairwise channels linking pairs of users.

• Three techniques for repairing shares:
  1. the enrollment scheme (Nojoumian, 2012)
  2. secure regenerating codes (Shah, Rashmi and Kumar, 2011)
  3. combinatorial schemes (Stinson and Wei, 2018)

• For a survey of these techniques, see (Laing and Stinson, 2018).

• In this talk, we discuss the third technique.
Repairable Threshold Schemes

• A \((t, n, d)\)-repairable threshold scheme, which we abbreviate to \((t, n, d)\)-RTS, is a \((t, n)\)-threshold scheme which permits the share of an arbitrary user \(P_\ell\) to be repaired as follows.

• Certain subsets of \(d\) users (not including \(P_\ell\)) send a message to \(P_\ell\).

• The messages received by \(P_\ell\) allow \(P_\ell\)'s share to be reconstructed.

• We note that \(d \geq t\) is an obvious necessary condition for the existence of such a scheme.

• If \(t - 1\) users could repair a share, then they would have \(t\) shares and they could reconstruct the secret, which is not allowed.
Goals of Combinatorial Repairability

- Our method employs a base scheme in which users receive multiple shares.
- A certain distribution design specifies which shares are given to which users.
- We study three problems:
  1. **Thresholds**: What properties of the distribution design ensure that the resulting scheme is in fact a $(t, n, d)$-RTS?
  2. **Scalability**: How can we accommodate various numbers of users from one specific distribution design?
  3. **Reliability**: What can we say about the probability of successful repair, in a scenario where users are available with some probability $p$?
A Combinatorial RTS based on a \((9, 3, 1)\)-BIBD

- As an example, we construct a \((2, 12, 3)\)-RTS.
- Start with a \((9, 3, 1)\)-BIBD (an affine plane of order 3), which has 12 blocks.
- This is the distribution design, which is public.
- We associate a block of the design with each user:

\[
\begin{align*}
U_1 & \leftrightarrow \{1, 2, 3\} & U_2 & \leftrightarrow \{4, 5, 6\} & U_3 & \leftrightarrow \{7, 8, 9\} \\
U_4 & \leftrightarrow \{1, 4, 7\} & U_5 & \leftrightarrow \{2, 5, 8\} & U_6 & \leftrightarrow \{3, 6, 9\} \\
U_7 & \leftrightarrow \{1, 5, 9\} & U_8 & \leftrightarrow \{2, 6, 7\} & U_9 & \leftrightarrow \{3, 4, 8\} \\
U_{10} & \leftrightarrow \{1, 6, 8\} & U_{11} & \leftrightarrow \{2, 4, 9\} & U_{12} & \leftrightarrow \{3, 5, 7\}
\end{align*}
\]

- Each user gets three shares from a \((5, 9)\)-threshold scheme (the base scheme), as specified by the associated block.
- This threshold scheme has nine shares, denoted \(s_1, \ldots, s_9\).
- Each block lists the indices of shares held by a given user.
- Thus \(U_1\) has the shares \(s_1, s_2\) and \(s_3\), etc.
Thresholds

- The base scheme has threshold equal to 5.
- The resulting RTS has threshold equal to 2.
- This is explained as follows:

Any **two blocks** of the distribution design contain **at least five points**, whereas **one block** contains only **three points**.

- Therefore, in the resulting RTS, any **two users** can reconstruct the secret, since they (collectively) have at least **five** distinct shares from the base scheme.
- However, **one user** cannot reconstruct the secret, because it only has **three** shares from the base scheme (which is less than the required threshold of five shares).
Repairability

- When a user wants to repair their share, they contact $d = 3$ other users who have the relevant subshares.
- For example, $U_1$ could contact $U_4$ to obtain subshare #1, $U_8$ to obtain subshare #2 and $U_{12}$ to obtain subshare #3:

$$
U_1 \leftarrow \{1, 2, 3\} \quad U_2 \leftarrow \{4, 5, 6\} \quad U_3 \leftarrow \{7, 8, 9\}
$$
$$
U_4 \leftarrow \{1, 4, 7\} \quad U_5 \leftarrow \{2, 5, 8\} \quad U_6 \leftarrow \{3, 6, 9\}
$$
$$
U_7 \leftarrow \{1, 5, 9\} \quad U_8 \leftarrow \{2, 6, 7\} \quad U_9 \leftarrow \{3, 4, 8\}
$$
$$
U_{10} \leftarrow \{1, 6, 8\} \quad U_{11} \leftarrow \{2, 4, 9\} \quad U_{12} \leftarrow \{3, 5, 7\}
$$
Scalability

• The described RTS is a scheme for 12 users, where 12 is the number of blocks in the distribution design.

• We can use a subset of the 12 blocks, and thereby reduce the number of users, provided that we can still repair shares.

• It suffices to choose a subset of blocks such that each point is contained in at least two blocks.

• Here, we can take the first six blocks, along with any subset of the last six blocks.

• This allows us to construct a $(2, m, 3)$-RTS for any $m \in \{6, \ldots, 12\}$.

• Note that the first six blocks comprise two parallel classes of the design, so every point occurs exactly twice in these blocks.
Required Properties of a Distribution Design

In order to be able to construct an RTS with threshold $t$, the distribution design must satisfy the property that

the number of points in the union of any $t$ blocks is greater than the number of points in the union of any $t - 1$ blocks.

In order to provide scalability, (i.e., construct an RTS for a variable number of users), we identify a “small” basic repairing set, i.e.,

a set of blocks in the distribution design such that every point is contained in at least two of these blocks.

Remark: As in the previous example, taking two parallel classes from a resolvable design will yield a basic repairing set of minimum possible size.
Lemma 1
The union of any $t-1$ blocks (lines) in a projective plane of order $q$ contain at most $q(t - 1) + 1$ points.

Proof.
Denote the $t - 1$ lines by $A_0, \ldots, A_{t-2}$. Each $A_i$ ($i \geq 1$) contains a point in $A_0$, so

$$\left| \bigcup_{i=0}^{t-2} A_i \right| \leq q + 1 + (t - 2)q = q(t - 1) + 1.$$ 

Remark: Equality occurs if and only if the $t - 1$ lines all contain a common point.
Lemma 2

For $t \leq q + 1$, the union of any $t$ lines in a projective plane of order $q$ contain at least $t(q + 1 - (t - 1)/2)$ points.

Proof.

Denote the $t$ lines by $A_0, \ldots, A_{t-1}$. Each $A_i$ contains $q + 1 - i$ points that are not in $\bigcup_{h=0}^{i-1} A_h$. It follows that

$$\left| \bigcup_{i=0}^{t-1} A_i \right| \geq \sum_{i=0}^{t-1} (q + 1 - i) = t(q + 1) - \frac{t(t - 1)}{2}.$$

Remark: Equality occurs if and only if no three of the $t$ lines are collinear, so they form the dual of a $t$-arc.
• Consider a projective plane of order 5.
• One block contains 6 points.
• Two blocks contain 11 points.
• Three blocks contain \textbf{at least} 15 and \textbf{at most} 16 points.
• Four blocks contain \textbf{at least} 18 and \textbf{at most} 21 points.
• Five blocks contain \textbf{at least} 20 points.
• We can construct RTS with the following thresholds:
  • \( t = 2 \) (since 6 < 11),
  • \( t = 3 \) (since 11 < 15), and
  • \( t = 4 \) (since 16 < 18)
• However \( t = 5 \) does not work (because 21 \( \geq \) 20).
Basic Repairing Sets in Projective Planes

• Recall that a basic repairing set is a subset of blocks (lines) that contains every point at least twice.

• In the context of a projective plane, this is precisely the dual of a 2-blocking set (see, e.g., Ball and Blokhuis, 1996).

• A simple construction: Choose any three noncollinear points \(x, y\) and \(z\) of the projective plane, and take all the lines that contain at least one of these points. This yields a basic repairing set of size \(3q\).

• Another construction: Suppose that \(q\) is a square of a prime power. Start with two disjoint Baer subplanes in \(PG(2, q)\) and take all the lines that contain a line from either of these two subplanes. This yields a basic repairing set of size \(2(q + \sqrt{q} + 1)\), which is an improvement asymptotically over the previous construction.
More Efficient Repairing

- Suppose we use a $t$-design with $t > 2$ as a distribution design.
- This could permit a more efficient repairing process.
- For example, suppose we use a $3-(v, 4, 1)$-design (a Steiner quadruple system).
- Since some pairs of blocks intersect in two points, a user’s share (which consists of four subshares) could be repaired using information supplied by two other users, each of which contributes two subshares.
- This reduces the number of messages sent (but not the total size of the messages).
- It could also have a positive effect on the reliability of the scheme (to be discussed a bit later).
- Two blocks contain at least six points, and one block contains four points.
- Therefore, because $6 > 4$, we obtain a $(2, n, 2)$-RTS, where $n$ is the number of blocks in the design.
The 3-(8, 4, 1)-design

\[ A_1 \leftrightarrow \{1, 2, 3, 4\} \]
\[ A_2 \leftrightarrow \{5, 6, 7, 8\} \]
\[ B_1 \leftrightarrow \{1, 2, 5, 6\} \]
\[ B_2 \leftrightarrow \{1, 2, 7, 8\} \]
\[ B_3 \leftrightarrow \{1, 3, 5, 7\} \]
\[ B_4 \leftrightarrow \{1, 3, 6, 8\} \]
\[ B_5 \leftrightarrow \{1, 4, 5, 8\} \]
\[ B_6 \leftrightarrow \{1, 4, 6, 7\} \]
\[ B_7 \leftrightarrow \{3, 4, 7, 8\} \]
\[ B_8 \leftrightarrow \{3, 4, 5, 6\} \]
\[ B_9 \leftrightarrow \{2, 4, 6, 8\} \]
\[ B_{10} \leftrightarrow \{2, 4, 5, 7\} \]
\[ B_{11} \leftrightarrow \{2, 3, 6, 7\} \]
\[ B_{12} \leftrightarrow \{2, 3, 5, 8\} \]

- Suppose \( A_1 \) wants to repair their share.
- They could contact \( B_1 \) to get subshares \# 1 and \# 2, and \( B_7 \) to get subshares \# 3 and \# 4.
A Network Reliability Model

- When a user contacts other users in an attempt to repair their share, the other users may not be available.
- Suppose that each user is available with probability $p$ and unavailable with probability $q = 1 - p$, independent of any other users.
- We consider two interesting and natural questions that arise when a user wants to repair their share:
  1. What is the probability $R(p)$ that there is at least one set of available users that can repair the given share?
  2. What is the expected number $E(p)$ of (minimal) sets of available users that can repair the given share?
- $R(p)$ and $E(p)$ are reliability polynomials in the variable $p$ (or $q$).
Repairing RTS Based on BIBDs with $\lambda = 1$

- Suppose a fixed user $U_\ell$ wants to repair a share corresponding to the block $\{x_1, \ldots, x_k\}$.
- Each point of the BIBD is in $r = (v - 1)/(k - 1)$ blocks.
- For $1 \leq i \leq k$, there are $r - 1$ users other than $U_\ell$ who has subshare $\# x_i$; call this subset $\mathcal{U}(x_i)$.
- The subsets $\mathcal{U}(x_1), \ldots, \mathcal{U}(x_k)$ are disjoint.
- Consider the $(9, 3, 1)$-BIBD:

$$
\begin{align*}
U_1 & \leftrightarrow \{1, 2, 3\} & U_2 & \leftrightarrow \{4, 5, 6\} & U_3 & \leftrightarrow \{7, 8, 9\} \\
U_4 & \leftrightarrow \{1, 4, 7\} & U_5 & \leftrightarrow \{2, 5, 8\} & U_6 & \leftrightarrow \{3, 6, 9\} \\
U_7 & \leftrightarrow \{1, 5, 9\} & U_8 & \leftrightarrow \{2, 6, 7\} & U_9 & \leftrightarrow \{3, 4, 8\} \\
U_{10} & \leftrightarrow \{1, 6, 8\} & U_{11} & \leftrightarrow \{2, 4, 9\} & U_{12} & \leftrightarrow \{3, 5, 7\}
\end{align*}
$$

- Suppose $U_1$ wants to repair their share.
- Then $\mathcal{U}(1) = \{U_4, U_7, U_{10}\}$, $\mathcal{U}(2) = \{U_5, U_8, U_{11}\}$ and $\mathcal{U}(3) = \{U_6, U_9, U_{12}\}$
The probability that at least one user in a specific $U(x_i)$ is available is $1 - q^3$.

$R(p)$ is the probability that at least one user in every $U(x_i)$ is available, so we have

$$R(p) = (1 - q^3)^3.$$ 

Computing the expected number of minimal repairing sets is even easier; it follows from linearity of expectation that

$$E(p) = (3p)^3.$$ 

In general, for a $(v, k, 1)$-BIBD, we have

$$R(p) = (1 - q^{r-1})^k$$

and

$$E(p) = ((r - 1)p)^k.$$
For SQS, the situation is more complicated, as there are various types of repairing sets to consider.

A minimal repairing set could have size 2, 3 or 4.

A standard technique from network reliability proves useful in computing the reliability polynomials.

A cut is a minimal set of users with the property that repairing is impossible if all the users in the cut are unavailable; in this case we say that the cut fails.

Suppose a user $U_\ell$ wants to repair a share corresponding to the block $\{x_1, \ldots, x_k\}$; then the cuts are $U(x_i)$, $1 \leq i \leq k$.

The cuts for an SQS are not disjoint.
Cuts in the 3-(8, 4, 1)-design

\[ A_1 \leftrightarrow \{1, 2, 3, 4\} \quad A_2 \leftrightarrow \{5, 6, 7, 8\} \]
\[ B_1 \leftrightarrow \{1, 2, 5, 6\} \quad B_2 \leftrightarrow \{1, 2, 7, 8\} \]
\[ B_3 \leftrightarrow \{1, 3, 5, 7\} \quad B_4 \leftrightarrow \{1, 3, 6, 8\} \]
\[ B_5 \leftrightarrow \{1, 4, 5, 8\} \quad B_6 \leftrightarrow \{1, 4, 6, 7\} \]
\[ B_7 \leftrightarrow \{3, 4, 7, 8\} \quad B_8 \leftrightarrow \{3, 4, 5, 6\} \]
\[ B_9 \leftrightarrow \{2, 4, 6, 8\} \quad B_{10} \leftrightarrow \{2, 4, 5, 7\} \]
\[ B_{11} \leftrightarrow \{2, 3, 6, 7\} \quad B_{12} \leftrightarrow \{2, 3, 5, 8\} \]

Suppose \( A_1 \) wants to repair their share; then

\[ \mathcal{U}(1) = \{B_1, B_2, B_3, B_4, B_5, B_6\} \]
\[ \mathcal{U}(2) = \{B_1, B_2, B_9, B_{10}, B_{11}, B_{12}\} \]
\[ \mathcal{U}(3) = \{B_3, B_4, B_7, B_8, B_{11}, B_{12}\} \]
\[ \mathcal{U}(4) = \{B_5, B_6, B_7, B_8, B_9, B_{10}\}. \]
Computing $\mathcal{R}(p)$ for the 3-(8, 4, 1)-design

- Repairing fails if and only if at least one of the four cuts fails, so we can compute $\mathcal{R}(p)$ using the **principle of inclusion-exclusion (PIE)**.

- $|\mathcal{U}(i)| = 6$ for all $i$, so the probability that a cut $\mathcal{U}(i)$ fails is $q^6$ (recall $q = 1 - p$).

- The probability that two given cuts both fail is $q^{10}$, because $|\mathcal{U}(i) \cup \mathcal{U}(j)| = 10$ for all $1 \leq i < j \leq 4$.

- The probability that three or four given cuts all fail is $q^{12}$.

- Applying **PIE**, we obtain

\[
1 - \mathcal{R}(p) = 4q^6 - \binom{4}{2}q^{10} + \binom{4}{3}q^{12} - \binom{4}{4}q^{12}
\]

- Hence,

\[
\mathcal{R}(p) = 1 - 4q^6 + 6q^{10} - 3q^{12}.
\]
Graphing $\mathcal{R}(p)$ for 2-(13, 4, 1), 2-(16, 4, 1), and 3-(10, 4, 1)-designs.
Computing $\mathcal{E}(p)$ for the 3-(10, 4, 1)-design

<p>| | | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_0$</td>
<td>$\leftrightarrow$</td>
<td>${1, 2, 4, 5}$</td>
<td>$B_0$</td>
<td>$\leftrightarrow$</td>
<td>${1, 2, 3, 7}$</td>
<td>$C_0$</td>
<td>$\leftrightarrow$</td>
<td>${1, 3, 5, 8}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_1$</td>
<td>$\leftrightarrow$</td>
<td>${2, 3, 5, 6}$</td>
<td>$B_1$</td>
<td>$\leftrightarrow$</td>
<td>${2, 3, 4, 8}$</td>
<td>$C_1$</td>
<td>$\leftrightarrow$</td>
<td>${2, 4, 6, 9}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_2$</td>
<td>$\leftrightarrow$</td>
<td>${3, 4, 6, 7}$</td>
<td>$B_2$</td>
<td>$\leftrightarrow$</td>
<td>${3, 4, 5, 9}$</td>
<td>$C_2$</td>
<td>$\leftrightarrow$</td>
<td>${3, 5, 7, 0}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_3$</td>
<td>$\leftrightarrow$</td>
<td>${4, 5, 7, 8}$</td>
<td>$B_3$</td>
<td>$\leftrightarrow$</td>
<td>${4, 5, 6, 0}$</td>
<td>$C_3$</td>
<td>$\leftrightarrow$</td>
<td>${4, 6, 8, 1}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_4$</td>
<td>$\leftrightarrow$</td>
<td>${5, 6, 8, 9}$</td>
<td>$B_4$</td>
<td>$\leftrightarrow$</td>
<td>${5, 6, 7, 1}$</td>
<td>$C_4$</td>
<td>$\leftrightarrow$</td>
<td>${5, 7, 9, 2}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_5$</td>
<td>$\leftrightarrow$</td>
<td>${6, 7, 9, 0}$</td>
<td>$B_5$</td>
<td>$\leftrightarrow$</td>
<td>${6, 7, 8, 2}$</td>
<td>$C_5$</td>
<td>$\leftrightarrow$</td>
<td>${6, 8, 0, 3}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_6$</td>
<td>$\leftrightarrow$</td>
<td>${7, 8, 0, 1}$</td>
<td>$B_6$</td>
<td>$\leftrightarrow$</td>
<td>${7, 8, 9, 3}$</td>
<td>$C_6$</td>
<td>$\leftrightarrow$</td>
<td>${7, 9, 1, 4}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_7$</td>
<td>$\leftrightarrow$</td>
<td>${8, 9, 1, 2}$</td>
<td>$B_7$</td>
<td>$\leftrightarrow$</td>
<td>${8, 9, 0, 4}$</td>
<td>$C_7$</td>
<td>$\leftrightarrow$</td>
<td>${8, 0, 2, 5}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_8$</td>
<td>$\leftrightarrow$</td>
<td>${9, 0, 2, 3}$</td>
<td>$B_8$</td>
<td>$\leftrightarrow$</td>
<td>${9, 0, 1, 5}$</td>
<td>$C_8$</td>
<td>$\leftrightarrow$</td>
<td>${9, 1, 3, 6}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_9$</td>
<td>$\leftrightarrow$</td>
<td>${0, 1, 3, 4}$</td>
<td>$B_9$</td>
<td>$\leftrightarrow$</td>
<td>${0, 1, 2, 6}$</td>
<td>$C_9$</td>
<td>$\leftrightarrow$</td>
<td>${0, 2, 4, 7}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This design has a cyclic automorphism generated by $x \mapsto x + 1 \mod 10$. 
Computing $E(p)$ for the 3-(10, 4, 1)-design: minimal repairing sets of size two

- Suppose we want to repair the block $A_0 = \{1, 2, 4, 5\}$.
- We consider minimal repairing sets of sizes two, three and four.
- A repairing set of size two consists of
  - a block containing 1, 2 and a block containing 4, 5; or
  - a block containing 1, 4 and a block containing 2, 5; or
  - a block containing 1, 5 and a block containing 2, 4.
- The total number of choices is $3 \times 3 \times 3 = 27$.
- Therefore, the expected number of repairing sets of size two is $27p^2$. 
Minimal repairing sets of size two

\[
\begin{align*}
A_0 \leftrightarrow \{1, 2, 4, 5\} & \quad B_0 \leftrightarrow \{1, 2, 3, 7\} & \quad C_0 \leftrightarrow \{1, 3, 5, 8\} \\
A_1 \leftrightarrow \{2, 3, 5, 6\} & \quad B_1 \leftrightarrow \{2, 3, 4, 8\} & \quad C_1 \leftrightarrow \{2, 4, 6, 9\} \\
A_2 \leftrightarrow \{3, 4, 6, 7\} & \quad B_2 \leftrightarrow \{3, 4, 5, 9\} & \quad C_2 \leftrightarrow \{3, 5, 7, 0\} \\
A_3 \leftrightarrow \{4, 5, 7, 8\} & \quad B_3 \leftrightarrow \{4, 5, 6, 0\} & \quad C_3 \leftrightarrow \{4, 6, 8, 1\} \\
A_4 \leftrightarrow \{5, 6, 8, 9\} & \quad B_4 \leftrightarrow \{5, 6, 7, 1\} & \quad C_4 \leftrightarrow \{5, 7, 9, 2\} \\
A_5 \leftrightarrow \{6, 7, 9, 0\} & \quad B_5 \leftrightarrow \{6, 7, 8, 2\} & \quad C_5 \leftrightarrow \{6, 8, 0, 3\} \\
A_6 \leftrightarrow \{7, 8, 0, 1\} & \quad B_6 \leftrightarrow \{7, 8, 9, 3\} & \quad C_6 \leftrightarrow \{7, 9, 1, 4\} \\
A_7 \leftrightarrow \{8, 9, 1, 2\} & \quad B_7 \leftrightarrow \{8, 9, 0, 4\} & \quad C_7 \leftrightarrow \{8, 0, 2, 5\} \\
A_8 \leftrightarrow \{9, 0, 2, 3\} & \quad B_8 \leftrightarrow \{9, 0, 1, 5\} & \quad C_8 \leftrightarrow \{9, 1, 3, 6\} \\
A_9 \leftrightarrow \{0, 1, 3, 4\} & \quad B_9 \leftrightarrow \{0, 1, 2, 6\} & \quad C_9 \leftrightarrow \{0, 2, 4, 7\}
\end{align*}
\]
Minimal repairing sets of size four

- A minimal repairing set of size four consists of four blocks having the following form:
  - a block containing 1, but none of 2, 4, 5
  - a block containing 2, but none of 1, 4, 5
  - a block containing 4, but none of 1, 2, 5
  - a block containing 5, but none of 1, 2, 4

- There are two choices for each of these four blocks.
- The total number of choices is $2^4 = 16$.
- Therefore, the expected number of minimal repairing sets of size four is $16p^4$. 
Minimal repairing sets of size four (cont.)

\[ A_0 \leftrightarrow \{1, 2, 4, 5\} \quad B_0 \leftrightarrow \{1, 2, 3, 7\} \quad C_0 \leftrightarrow \{1, 3, 5, 8\} \]
\[ A_1 \leftrightarrow \{2, 3, 5, 6\} \quad B_1 \leftrightarrow \{2, 3, 4, 8\} \quad C_1 \leftrightarrow \{2, 4, 6, 9\} \]
\[ A_2 \leftrightarrow \{3, 4, 6, 7\} \quad B_2 \leftrightarrow \{3, 4, 5, 9\} \quad C_2 \leftrightarrow \{3, 5, 7, 0\} \]
\[ A_3 \leftrightarrow \{4, 5, 7, 8\} \quad B_3 \leftrightarrow \{4, 5, 6, 0\} \quad C_3 \leftrightarrow \{4, 6, 8, 1\} \]
\[ A_4 \leftrightarrow \{5, 6, 8, 9\} \quad B_4 \leftrightarrow \{5, 6, 7, 1\} \quad C_4 \leftrightarrow \{5, 7, 9, 2\} \]
\[ A_5 \leftrightarrow \{6, 7, 9, 0\} \quad B_5 \leftrightarrow \{6, 7, 8, 2\} \quad C_5 \leftrightarrow \{6, 8, 0, 3\} \]
\[ A_6 \leftrightarrow \{7, 8, 0, 1\} \quad B_6 \leftrightarrow \{7, 8, 9, 3\} \quad C_6 \leftrightarrow \{7, 9, 1, 4\} \]
\[ A_7 \leftrightarrow \{8, 9, 1, 2\} \quad B_7 \leftrightarrow \{8, 9, 0, 4\} \quad C_7 \leftrightarrow \{8, 0, 2, 5\} \]
\[ A_8 \leftrightarrow \{9, 0, 2, 3\} \quad B_8 \leftrightarrow \{9, 0, 1, 5\} \quad C_8 \leftrightarrow \{9, 1, 3, 6\} \]
\[ A_9 \leftrightarrow \{0, 1, 3, 4\} \quad B_9 \leftrightarrow \{0, 1, 2, 6\} \quad C_9 \leftrightarrow \{0, 2, 4, 7\} \]
Minimal repairing sets of size three

- A **minimal** repairing set of size three can have three possible forms:
  - **type pair - pair - pair**: three pairs intersecting in a point, e.g., $12, 14, 15$. There are **four** configurations of this type.
  - **type pair - pair - point**: two pairs intersecting in a point, and a disjoint point e.g., $12, 14, 5$. There are **twelve** configurations of this type.
  - **type pair - point - point**: one pair, and two disjoint points, e.g., $12, 4, 5$. There are **six** configurations of this type.

- After some counting, the expected number of minimal repairing sets of size three is seen to be

$$
(4 \times 3^3 + 12 \times 3^2 \times 2 + 6 \times 3 \times 2^2)p^3 = 396p^3.
$$

- Therefore,

$$
\mathcal{E}(p) = 27p^2 + 396p^3 + 16p^4.
$$
Summary and Open Problems

1. We have a formula to compute $R(p)$ for any $t-(v, k, 1)$-design. However, we only have formulas for $E(p)$ for $2-(v, k, 1)$-designs and for $3-(v, 4, 1)$-designs.

2. Are there probabilistic existence results for “good” distribution designs?

3. What other types of combinatorial structures yield “good” distribution designs?

4. By using ramp schemes for the base scheme, it is possible to get more efficient RTS for certain distribution designs; see Stinson and Wei (2018).

5. We have also been investigating how to design efficient algorithms to find a repairing set (Kacsmar and Stinson).
Happy Birthday Charlie!