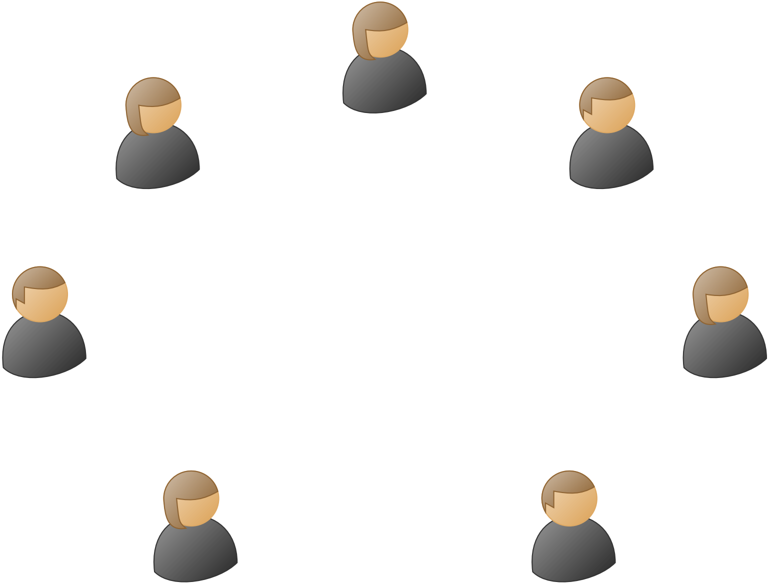
Designing Efficient Algorithms for Combinatorial Repairable Threshold Schemes

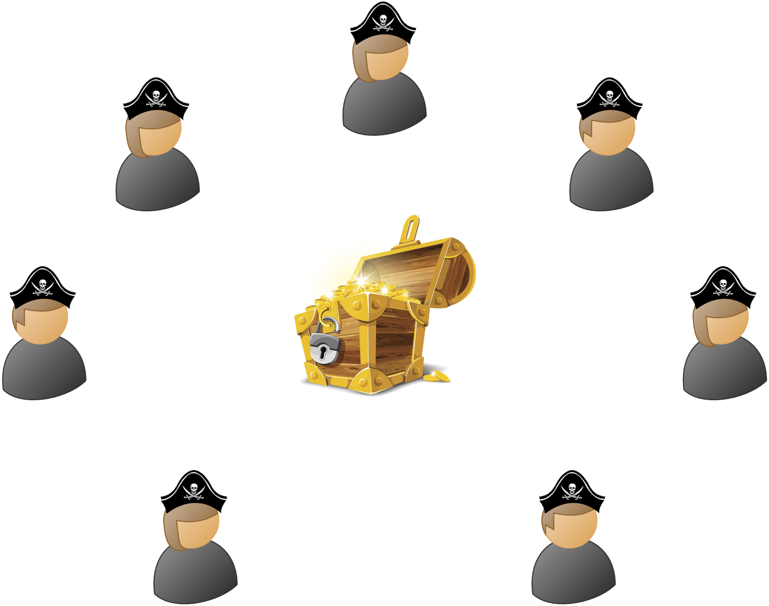
Bailey Kacsmar

University of Waterloo

Threshold Schemes



Threshold Schemes



Threshold Schemes and Repairability

A *(τ, n)-Threshold Scheme* has n participants and threshold τ

- Any subset of participants of size τ can determine the secret from combining their shares.
- No subset of players consisting of fewer than τ players learns the secret.

(τ, n)-TS exists for any τ and n such that $\tau \leq n$.

Definition

A threshold scheme is *repairable* if it has a defined repairing algorithm such that a participant with a failed share can communicate with a subset of the n participants to reconstruct the failed share. Additionally, after a repair no coalition is able to learn information they did not have before the repair.

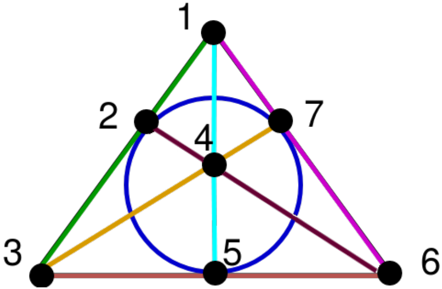
Outline

- Reliability of Combinatorial Threshold Schemes
- Algorithms for Performing a Repair
- Extending to use Different Designs

Balanced Incomplete Block Design (BIBD)

Let v, k, λ be integers, $v > k \geq \lambda$. A $(\mathbf{v}, \mathbf{k}, \lambda)-$**BIBD** is a design such that:

1. $|X| = v$, number of elements in the set X is v
2. each block contains exactly k points, and
3. every pair of distinct points is contained in exactly λ blocks.



$(7, 3, 1)-$BIBD

Steiner Triple Systems

Definition

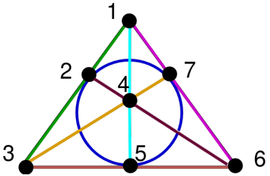
A Steiner triple system is a $(v, 3, 1)$-BIBD. There exists an $STS(v)$ if and only if $v \equiv 1, 3 \pmod 6$, $v \geq 7$.

Definition

Every point in a (v, k, λ)-BIBD occurs in exactly

$$r = \frac{\lambda(v-1)}{k-1}$$

blocks. The value r is termed the *replication number*.



Constructing a Repairable (2,7)-Threshold Scheme

Base Scheme

Construct a $(5, 7)$-threshold scheme. The shares from the base scheme are $S_1, S_2 \ldots, S_7$.

Distribution Design

Assign the blocks of the $(7, 3, 1)$-BIBD as follows:

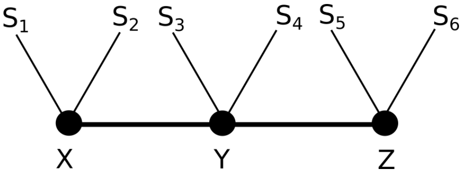
$P_1 \leftrightarrow 123$	$P_3 \leftrightarrow 167$	$P_5 \leftrightarrow 257$	$P_7 \leftrightarrow 356$
$P_2 \leftrightarrow 145$	$P_4 \leftrightarrow 246$	$P_6 \leftrightarrow 347$	

Expanded Scheme

Distribute each S_i to players with point i from the block design.

P_1's expanded share S_1, S_2, S_3.
P_2's expanded share S_1, S_4, S_5.
P_3's expanded share S_1, S_6, S_7.
P_4's expanded share S_2, S_4, S_6.
P_5's expanded share S_2, S_5, S_7.
P_6's expanded share S_3, S_4, S_7.
P_7's expanded share S_3, S_5, S_6.

The Existence of Available Repair Sets



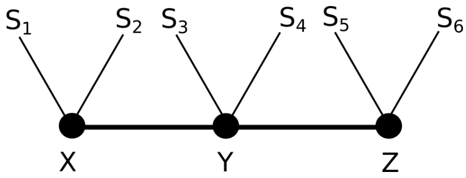
Example

Let the share xyz in an $STS(7)$ require repair. Let $S_1, \ldots, S_6$, be shares that intersect xyz. Let p be the probability that a participant is available and let $\mathcal{R}(p) = Pr\{\text{a repair set exists}\}$.

Pr{at least one of $\{S_1, S_2\}$ is available} is

$$1 - (1 - p)^2 = 2p - p^2$$

The Existence of Available Repair Sets



Example

Let the share xyz in an $STS(7)$ require repair. Let $S_1, \ldots, S_6$, be shares that intersect xyz. Let p be the probability that a participant is available and let $\mathcal{R}(p) = Pr\{\text{a repair set exists}\}$.

Pr{at least one of $\{S_1, S_2\}$ is available} is

$$1 - (1 - p)^2 = 2p - p^2$$

$$\mathcal{R}(p) = (2p - p^2)^3$$

Existence of An Available Repair Set for an $STS(7)$

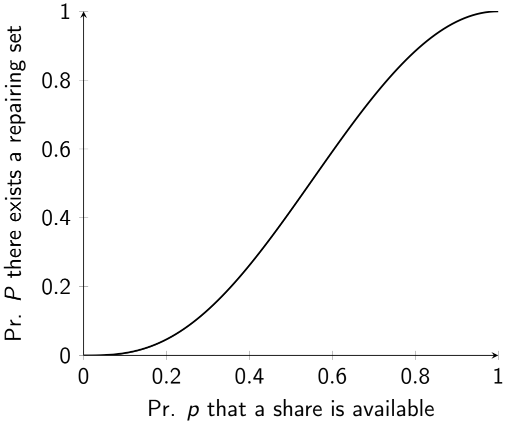


Figure: Existence of an available repair set for $STS(7)$

Generalized Existence of Available Repair Sets

$$r = \frac{\lambda(v-1)}{k-1}$$

Theorem

For an $STS(v)$, the probability that there exists at least one repairing set is:

$$\mathcal{R}(p) = (1-(1-p)^{r-1})^3.$$

Theorem

For a $(v, k, 1) - BIBD$, the probability that there exists at least one repairing set is:

$$\mathcal{R}(p) = (1-(1-p)^{r-1})^k.$$

Generalizing the Expected Available Repair Sets

Linearity of Expectation asserts that the expected value of a sum of random variables is equal to the sum of the expected values for each of the random variables.

$$r = \frac{\lambda(v-1)}{k-1}$$

Theorem

The expected number of available repair sets for an $STS(v)$ is:

$$(r-1)^3 p^3.$$

Theorem

The expected number of available repairing sets for a $(v, k, \lambda) - BIBD$ is

$$(r-1)^k p^k.$$

Expectation Graph

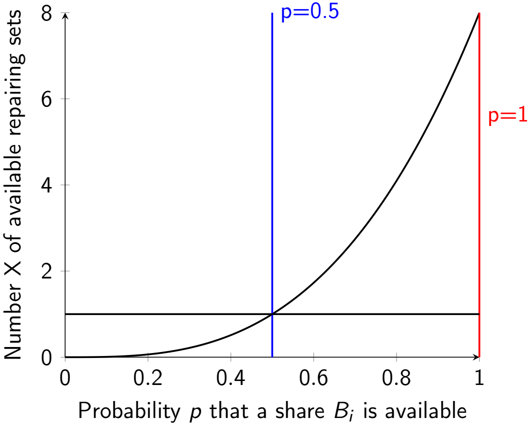


Figure: Expected number of available repair sets for $STS(7)$

Algorithms

Who you gonna call?

In solving the problem of finding a repair set we need to consider:

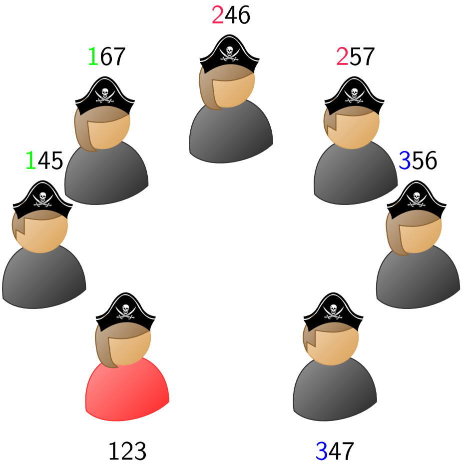
- The Probability Model
  - Transient Fault
  - Permanent Fault
- The Storage requirements
- The Complexity analysis

Algorithm 1

Random Participants

Model: Transient Fault Storage: Own share

- P_ℓ lost the shares for 123
- P_ℓ contacts a random P_j and wait time T for a response
- If P_j responds ask for any of 123
- Repeat until all subshares are repaired

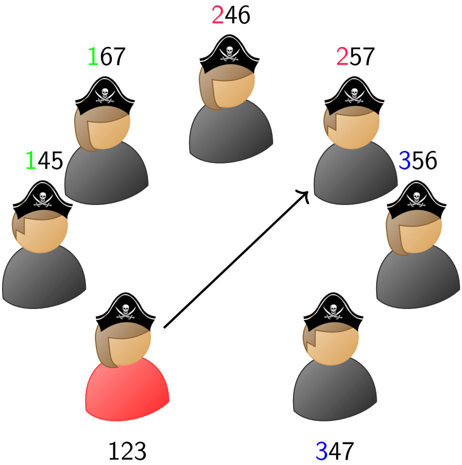


Algorithm 1

Random Participants

Model: Transient Fault   Storage: Own share

- P_ℓ lost the shares for 123
- P_ℓ contacts a random P_j and wait time T for a response
- If P_j responds ask for any of 123
- Repeat until all subshares are repaired

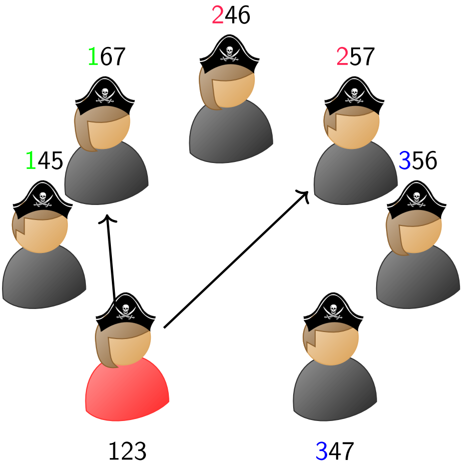


Algorithm 1

Random Participants

Model: Transient Fault   Storage: Own share

- P_ℓ lost the shares for 123
- P_ℓ contacts a random P_j and wait time T for a response
- If P_j responds ask for any of 123
- Repeat until all subshares are repaired

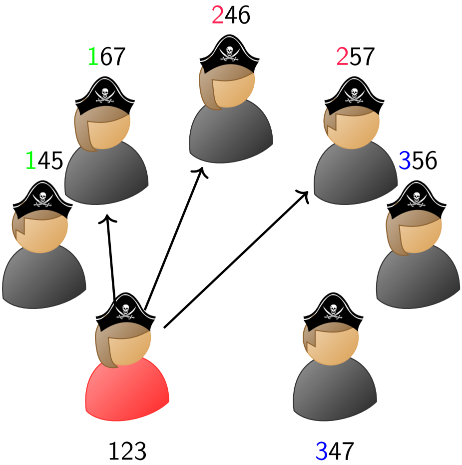


Algorithm 1

Random Participants

Model: Transient Fault Storage: Own share

- P_ℓ lost the shares for 123
- P_ℓ contacts a random P_j and wait time T for a response
- If P_j responds ask for any of 123
- Repeat until all subshares are repaired

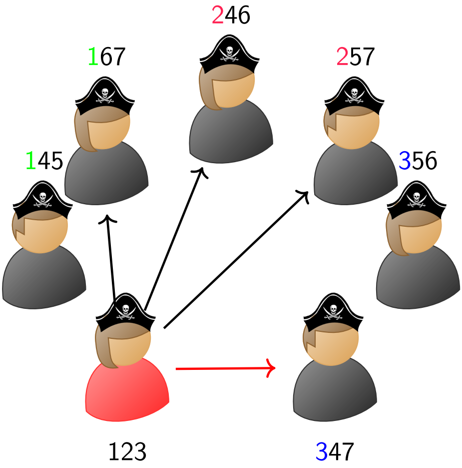


Algorithm 1

Random Participants

Model: Transient Fault   Storage: Own share

- P_ℓ lost the shares for 123
- P_ℓ contacts a random P_j and wait time T for a response
- If P_j responds ask for any of 123
- Repeat until all subshares are repaired

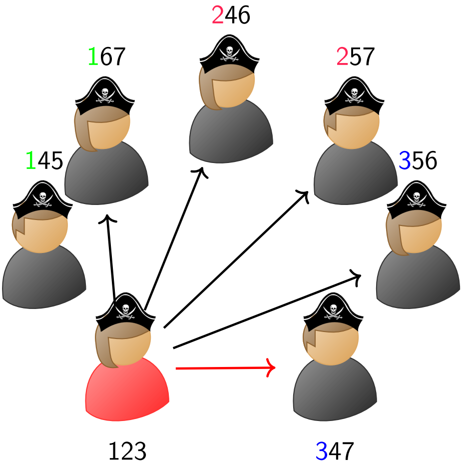


Algorithm 1

Random Participants

Model: Transient Fault Storage: Own share

- P_ℓ lost the shares for 123
- P_ℓ contacts a random P_j and wait time T for a response
- If P_j responds ask for any of 123
- Repeat until all subshares are repaired



Algorithm 1

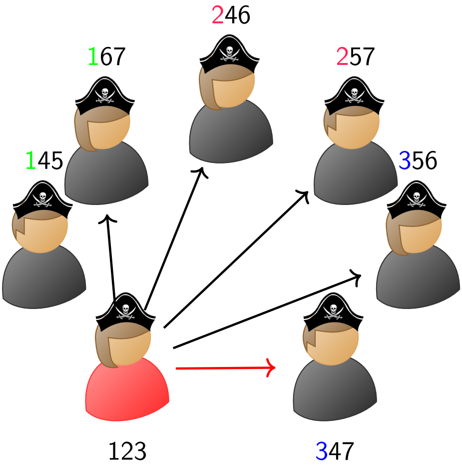
Random Participants

Model: Transient Fault Storage: Own share

Recall:

- This is a variation of the classic coupon collector problem
- There are n participants corresponding to $b = \frac{vr}{k}$ blocks
- Each share consists of $k = 3$ subshares

the expected time $= T\dfrac{b}{p(r-1)}\ln k$

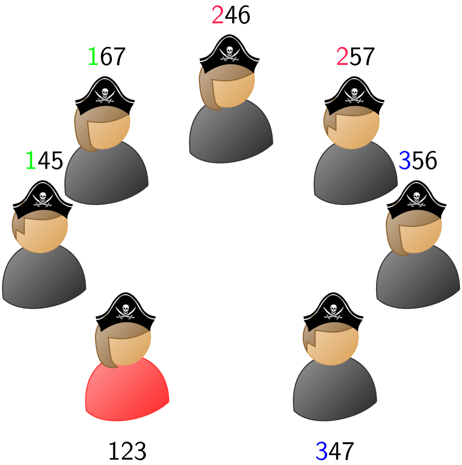


Algorithm 2

Stored Intersecting Participants

Model: Transient Fault   Storage: Own share, $\mathcal{R} \subset \mathcal{P}$

- P_ℓ lost the shares for 123
- P_ℓ contacts a random P_j who has an intersecting share and waits time T for a response
- If P_j responds ask for any of 123
- Repeat until all subshares are repaired

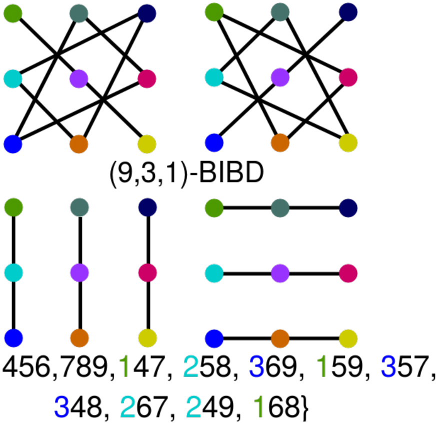


Algorithm 2

Stored Intersecting Participants

Model: Transient Fault Storage: Own share, $\mathcal{R} \subset \mathcal{P}$

- P_ℓ lost the shares for 123
- P_ℓ contacts a random P_j who has an intersecting share and waits time T for a response
- If P_j responds ask for any of 123
- Repeat until all subshares are repaired



Algorithm 2

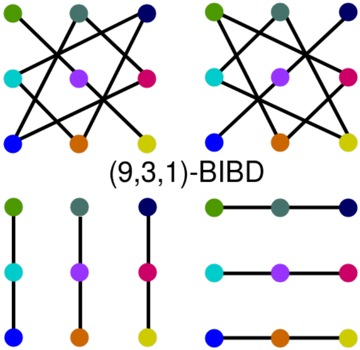
Stored Intersecting Participants

Model: Transient Fault   Storage: Own share, $\mathcal{R} \subset \mathcal{P}$

Recall:

- Also a variant of the coupon collector problem
- There are $k(r-1)$ participants intersecting participants
- Each share consists of $k = 3$ subshares

the expected time $= \dfrac{k \ln k}{p}$



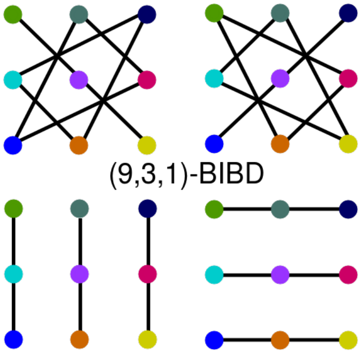
{123, 456,789,147, 258, 369, 159, 357, 348, 267, 249, 168}

Algorithm 3

Stored Grouped Participants

Model: Permanent Fault   Storage: Own share, $\mathcal{R} = \{\{P_3, P_6, P_{11}\}, \ldots$

- P_ℓ lost the shares for 123
- To repair a subshare s, P_ℓ contacts P_j who has s in common and waits time T for a response
- If P_j responds ask for s
- Repeat for each subshare s that requires repair



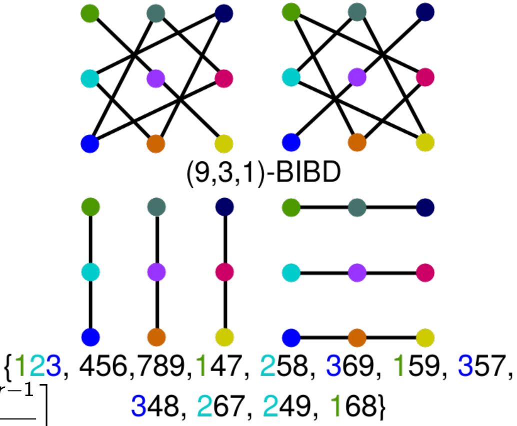
{123, 456,789,147, 258, 369, 159, 357, 348, 267, 249, 168}

Algorithm 3

Stored Grouped Participants

Model: Permanent Fault Storage: Own share, $\mathcal{R} = \{\{P_3, P_6, P_{11}\}, \ldots$

- For each subshare there is a list of $r-1$ participants that can repair it
- Each share consists of $k = 3$ subshares
- The replication number r is how many times a point occurs in the design



the expected time $=$

$$kT\left[\frac{1-(p(r-1)+1)(1-p)^{r-1}}{p}\right]$$

Algorithm 4

Generate Intersecting Participants

Example

Let the design be a $(7,3,1)$-BIBD with the base block $\mathcal{B} = \{013\}$ and blocks labelled $\{B_0, B_1, B_2, B_3, B_4, B_5, B_6\}$. The resulting blocks are:

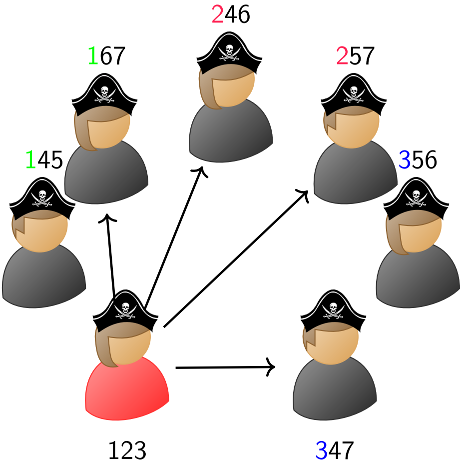
$$\{013, 124, 235, 346, 450, 561, 602\}.$$

These blocks correspond to players

$$\{P_0, P_1, P_2, P_3, P_4, P_5, P_6\}.$$

The block B_3 would be generated by computing $\{0 + 3 \pmod 7, 1 + 3 \pmod 7, 3 + 3 \pmod 7\}$, which is block 346.

What if a participant could ask for more than one subshare?



From 2-Designs to t-Designs

Definition

A (v, k, λ)-*Balanced Incomplete Block Design*, is a design such that:

1. $|X| = v$,
2. each block contains exactly k points, and
3. every pair of distinct points is contained in exactly λ blocks.

From 2-Designs to t-Designs

Definition

A (v, k, λ)-*Balanced Incomplete Block Design*, (a $2-(v, k, \lambda)$ design) is a design such that:

1. $|X| = v$,
2. each block contains exactly k points, and
3. every pair (set of 2) of distinct points is contained in exactly λ blocks.

From 2-Designs to t-Designs

Definition

A $t-(v,k,\lambda)$ *design* is a design where:

1. $|X| = v$,
2. Each block is of size k,
3. Every set of t points from the set X occurs in exactly λ blocks.

Definition

A $3-(v,4,1)$ design is a *Steiner quadruple system* of order v, denoted $SQS(v)$. For all $SQS(v)$, $v \equiv 2,4 \pmod 6$.

2-Designs and 3-Designs

Example

A $2-(13,4,1)$ design with the set $X=\{0,1,2,3,4,5,6,7,8,9,a,b,c\}$

0139	028c
0457	06ab
124a	1568
17bc	235b
2679	346c
378a	489b
598a	

Example

A $3-(8,4,1)$ design with the set $X=\{1,2,3,4,5,6,7,8\}$

1234	5678
1256	3478
1278	3456
1357	2468
1368	2457
1458	2367
1467	2358

Reliability for a $SQS(8)$

Example

$A_1 = 1234 \quad A_2 = 5678$

$B_1 = 1256 \quad B_7 = 3478$

$B_2 = 1278 \quad B_8 = 3456$

$B_3 = 1357 \quad B_9 = 2468$

$B_4 = 1368 \quad B_{10} = 2457$

$B_5 = 1458 \quad B_{11} = 2367$

$B_6 = 1467 \quad B_{12} = 2358$

Reliability for a $SQS(8)$

Example

$A_1 = 1234 \quad A_2 = 5678$

$B_1 = 1256 \quad B_7 = 3478$

$B_2 = 1278 \quad B_8 = 3456$

$B_3 = 1357 \quad B_9 = 2468$

$B_4 = 1368 \quad B_{10} = 2457$

$B_5 = 1458 \quad B_{11} = 2367$

$B_6 = 1467 \quad B_{12} = 2358$

We can define *cutsets* as follows:

$$C_1 = \{B_1, B_2, B_3, B_4, B_5, B_6\}$$
$$C_2 = \{B_1, B_2, B_9, B_{10}, B_{11}, B_{12}\}$$
$$C_3 = \{B_3, B_4, B_7, B_8, B_{11}, B_{12}\}$$
$$C_4 = \{B_5, B_6, B_7, B_8, B_9, B_{10}\}.$$

Reliability for a $SQS(8)$

Example

$A_1 = 1234 \quad A_2 = 5678$

$B_1 = 1256 \quad B_7 = 3478$

$B_2 = 1278 \quad B_8 = 3456$

$B_3 = 1357 \quad B_9 = 2468$

$B_4 = 1368 \quad B_{10} = 2457$

$B_5 = 1458 \quad B_{11} = 2367$

$B_6 = 1467 \quad B_{12} = 2358$

We can define *cutsets* as follows:

$$C_1 = \{B_1, B_2, B_3, B_4, B_5, B_6\}$$
$$C_2 = \{B_1, B_2, B_9, B_{10}, B_{11}, B_{12}\}$$
$$C_3 = \{B_3, B_4, B_7, B_8, B_{11}, B_{12}\}$$
$$C_4 = \{B_5, B_6, B_7, B_8, B_9, B_{10}\}.$$

$$Pr\{a\ repair\ set\ exists\} = 1 - Pr\{\text{at least one } C_i \text{ fails}\}$$

Any C_i fails for an $SQS(8)$

The *inclusion-exclusion principle* states that given two sets A and B,

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$\begin{aligned}
C_1 &= \{B_1, B_2, B_3, B_4, B_5, B_6\} & |C_1| &= 6 \\
C_2 &= \{B_1, B_2, B_9, B_{10}, B_{11}, B_{12}\} & |C_1 \cup C_2| &= 10 \\
C_3 &= \{B_3, B_4, B_7, B_8, B_{11}, B_{12}\} & |C_1 \cup C_2 \cup C_3| &= 12 \\
C_4 &= \{B_5, B_6, B_7, B_8, B_9, B_{10}\}. & |C_1 \cup C_2 \cup C_3 \cup C_4| &= 12
\end{aligned}$$

Therefore, the probability a repair set exists for an $SQS(8)$ is

$$1 - Pr\{\text{at least one } C_i \text{ fails}\} = 1 - 4(1-p)^{6} + 6(1-p)^{10} - 3(1-p)^{12}$$

Generalizing Existence for $SQS(v)$

$$r_1 = \frac{\binom{v-1}{2}}{3} \qquad r_2 = \frac{\binom{v-2}{1}}{2}$$

Theorem

Let $q = 1 - p$, where p is the probability that a share is available. Then, the generalized formula for the probability of the existence of a repair set for an $SQS(v)$ is:

$$1 - 4q^{r_1-1} + 6q^{2r_1-r_2-1} - 4q^{3r_1-3r_2} + q^{4r_1-6r_2+2}.$$

Generalizing Existence for t-Designs

$$r_j = \frac{\binom{v-j}{t-j}}{\binom{k-j}{t-j}}$$

Theorem

Let $q = (1-p)$, where p is the probability that a share is available. Then, the generalized formula for the probability of existence of a repair set for an $t-(v,k,1)$ design is:

$$Pr\{\text{a repair set exists}\} = 1 - \binom{k}{1} q^{e_1} + \binom{k}{2} q^{e_2} - \binom{k}{3} q^{e_3} + \cdots + \binom{k}{k} q^{e_k}$$

where

$$e_i = \sum_{j=1}^{i} (-1)^{j+1} \binom{i}{j} (r_j - 1).$$

Comparing Existence for $t = 2$ and $t = 3$

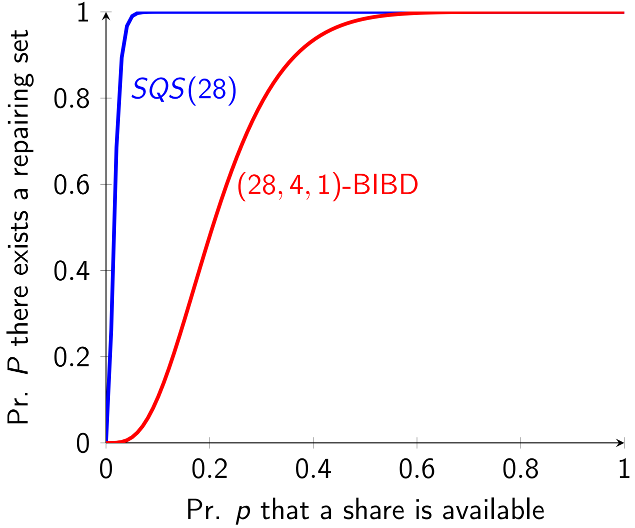


Figure: Existence of a repair set for: $SQS(28)$ and $(28, 4, 1)$-BIBD

Comparing Existence for $t = 2$ and $t = 3$

Table: Repair Set Existence Comparison for $t-(v,k,1)$ Designs

t	v	k	λ	b	r_1	r_2	Value of p for $P \geq 0.99$
2	13	4	1	13	4	1	0.87
2	16	4	1	20	5	1	0.78
2	25	4	1	50	8	1	0.58
2	28	4	1	63	9	1	0.53
3	14	4	1	91	26	6	0.22
3	16	4	1	140	35	7	0.17
3	26	4	1	650	100	12	0.06
3	28	4	1	819	117	13	0.06

What is a Repair Set for a Steiner Quadruple System?

Example

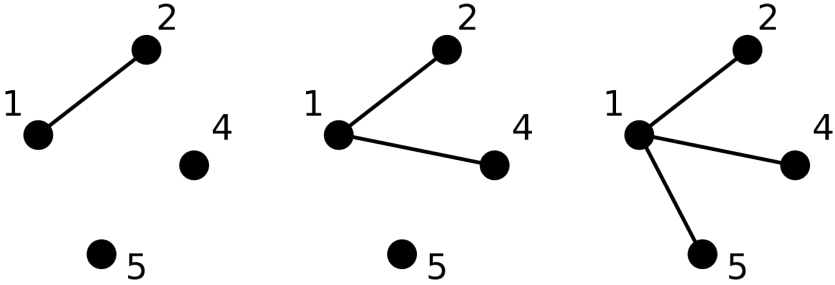
Let P_ℓ require a repair for their share 1256.

1. Assume P_ℓ contacts 1234. This provides the pair 12.
2. The next P_j, may provide 56, 16, 25, 15, or 26.
3. If the repair was not completed at the previous stage, P_ℓ will contact P_k to receive either 5 or 6.

Minimal repair sets for a $SQS(v)$ can take the following forms:

1. "pair, pair"
2. "pair, point, point"
3. "point, point, point, point"

"Pair, Point, Point" forms for $SQS(v)$



(a) Basic (b) Mixed (c) Connected

Figure: "Pair, Point, Point" Repair Set Types

Expected Number of Available Repair Sets

The expected number of minimal repair sets for an $SQS(v)$ can be computed as the sum of:

- The expected number of "pair, pair" repair sets

  Clearly, $3(r_2 - 1)^2 p^2$
- The expected number of "point, point, point, point" repair sets

  Clearly, $((r_1 - 1) - 3(r_2 - 1))^4 p^4$
- The expected number of "pair, point, point" repair sets

  Expands into three forms
  - ★ Basic
  - ★ Mixed
  - ★ Connected

The expected number of minimal repair sets of size two, three, or four for an $SQS(v)$ can be computed as:

$$3(r_2-1)^2p^2+2(r_2-1)(3r_1^2-12r_1r_2+6r_1+11r_2^2-10r_2+2)p^3+(r_1-3r_2+2)^4p^4$$

Contacting Repair Sets for t-Designs

Grouping Intersecting Participants

Let the design be an $SQS(10)$. Let P_ℓ correspond to block 1245.

$$R_1 = \{1237, 1358, 1468, 1567, \ldots, 1289, 1590, 1369, 1340, 1260\}$$

$$R_2 = \{1237, 2356, 2348, 2469, \ldots 1289, 2580, 2390, 1260, 2470\}$$

$$R_4 = \{2348, 2469, 3467, 2469, \ldots, 1468, 1479, 4890, 1340, 2470\}$$

$$R_5 = \{1358, 2356, 3459, 3570, \ldots 5689, 1567, 2579, 2580, 1590\}$$

Contacting Repair Sets for t-Designs

Grouping Intersecting Participants

Let the design be an $SQS(10)$. Let P_ℓ correspond to block 1245.

$$R_1 = \{1237, 1358, 1468, 1567, \ldots, 1289, 1590, 1369, 1340, 1260\}$$
$$R_2 = \{1237, 2356, 2348, 2469, \ldots 1289, 2580, 2390, 1260, 2470\}$$
$$R_4 = \{2348, 2469, 3467, 2469, \ldots, 1468, 1479, 4890, 1340, 2470\}$$
$$R_5 = \{1358, 2356, 3459, 3570, \ldots 5689, 1567, 2579, 2580, 1590\}$$

$$R_{12} = \{1237, 1260, 1289\}$$
$$R_{45} = \{3459, 4578, 4560\}$$
$$R_{14} = \{1340, 1468, 1479\}$$
$$R_{15} = \{1358, 1567, 1590\}$$
$$R_{24} = \{2348, 2469, 2470\}$$
$$R_{25} = \{2356, 2579, 2580\}$$

Contacting Repair Sets for t-Designs

Grouping Intersecting Participants

Let the design be an $SQS(10)$. Let P_ℓ correspond to block 1245.

$$R_1 = \{1237, 1358, 1468, 1567, \ldots, 1289, 1590, 1369, 1340, 1260\}$$

$$R_2 = \{1237, 2356, 2348, 2469, \ldots 1289, 2580, 2390, 1260, 2470\}$$

$$R_4 = \{2348, 2469, 3467, 2469, \ldots, 1468, 1479, 4890, 1340, 2470\}$$

$$R_5 = \{1358, 2356, 3459, 3570, \ldots 5689, 1567, 2579, 2580, 1590\}$$

$$R_{12} = \{1237, 1260, 1289\}$$

$$R_{45} = \{3459, 4578, 4560\} \qquad R_1^* = \{1780, 1369\}$$

$$R_{14} = \{1340, 1468, 1479\} \qquad R_2^* = \{2678, 2390\}$$

$$R_{15} = \{1358, 1567, 1590\} \qquad R_4^* = \{3467, 4890\}$$

$$R_{24} = \{2348, 2469, 2470\} \qquad R_5^* = \{3570, 5689\}$$

$$R_{25} = \{2356, 2579, 2580\}$$

Summary

- Evaluated and generalized reliability with respect to the existence and the expected number of available sets of participants sufficient to perform a repair.
- Designed and analyzed algorithms for contacting participants sufficient to perform a repair with trade-offs between storage and complexity
- Presented and evaluated t-designs, for $t \geq 2$, as distribution designs.

Summary

- Evaluated and generalized reliability with respect to the existence and the expected number of available sets of participants sufficient to perform a repair.
- Designed and analyzed algorithms for contacting participants sufficient to perform a repair with trade-offs between storage and complexity
- Presented and evaluated t-designs, for $t \geq 2$, as distribution designs.

Photo credit: @EverythingGoats

t-Designs for $\tau = 2$

Theorem

An $SQS(v)$ can be used as a $(2,4,6)$-distribution design to produce a $(2,2,b)$-repairable threshold scheme, where $b = \frac{vr}{k}$ is the number of blocks in the $SQS(v)$.

Theorem

A $t-(v,k,1)$ design can be used as a $(3,2k,3k-3(t-1))$ distribution design to produce a $(3,\lceil \frac{k}{t-1} \rceil, b)$-repairable threshold scheme if $k \geq 3t-2$, where b is the number of blocks in the $t-(v,k,1)$ design.

t-Designs for $\tau = 3$

Definition

An *inversive plane* is a $3-(q^2, q+1, 1)$ design where q is a prime number.

Theorem

For all prime powers q, there exists a $3-(q^2, q+1, 1)$ design.

Theorem

An inversive plane can be used as a $(3, 2(q+1), 3q-3)$-distribution design to produce a $(3, \lceil \frac{q+1}{2} \rceil, b)$-repairable threshold scheme if $q \geq 6$ is a prime power.

t-Designs for $\tau = 3$

Definition

A *spherical geometry* is a $3-(q^n+1, q+1, 1)$ design where q is a prime number and $n \geq 2$.

Theorem

Known infinite families of $t-(v,k,1)$ *designs include* $3-(q^n+1, q+1, 1)$ *designs where* q *is a prime number and* $n \geq 2$*.*

Theorem

A spherical geometry can be used as a $(3, 2(q+1), 3(q+1)-6)$*-distribution design to produce a* $(3, \lceil \frac{q+1}{2} \rceil, b)$*-repairable threshold scheme if* $q \geq 6$*.*

t-Designs for τ

Theorem

A $t-(v,k,1)$ design can be used as a $(\tau,(\tau-1)k,\tau k-\binom{\tau}{2}(t-1))$ distribution design to produce a $(\tau,\lceil\frac{k}{t-1}\rceil,b)$-repairable threshold scheme if $k\geq\binom{\tau}{2}(t-1)+1$, where b is the number of blocks in the $t-(v,k,1)$ design.

Generalizing Expectation Beyond $SQS(v)$

Example

Consider a $3-(v, 5, 1)$ design. Minimal repair sets could take the following forms:

- pair, pair, point
- pair, point, point, point
- point, point, point, point, point

"pair, pair, point" and "pair, point, point, point" would each have sub-cases

Example

Consider a $3-(v, 6, 1)$ design. Minimal repair sets could take the following forms:

- pair, pair, pair
- pair, pair, point, point
- pair, point, point, point, point
- point, point, point, point, point, point

"pair, pair, point, point" and "pair, point, point, point, point" would each have sub-cases

Generalizing Expectation Beyond $SQS(v)$

Example

Consider a $4-(v,5,1)$ design.
Minimal repair set forms:

- triple, pair
- triple, point, point
- pair, pair, point
- pair, point, point, point
- point, point, point, point, point

All but "point, point, point, point, point" will have multiple sub-cases.

Example

Consider a $4-(v,6,1)$ design.
Minimal repair set forms:

- triple, triple
- triple, pair, point,
- triple point, point, point
- pair, pair, pair
- pair, pair, point, point
- pair, point, point, point, point
- point, point, point, point, point, point

In this case, all but "triple, triple" and "point, point, point, point, point, point" have sub-cases.

The Expected Number of Available Repair Sets

Table: Repair Set Probability Distribution for $STS(7)$

Number of sets X	1	2	4	8
Pr of X	$(2p-2p^2)^3$	$3(2p-2p^2)^2p^2$	$3(2p-2p^2)p^4$	p^6

Let X be the number of available repairing sets. Then,

$$E(X) = 1(2p-2p^2)^3 + 2\cdot 3(2p-2p^2)^2p^2 + 4\cdot 3(2p-2p^2)p^4 + 8p^6$$

$$= 8p^3$$

$$= 2^3p^3$$

Comparing Repair Set Forms for $SQS(10)$

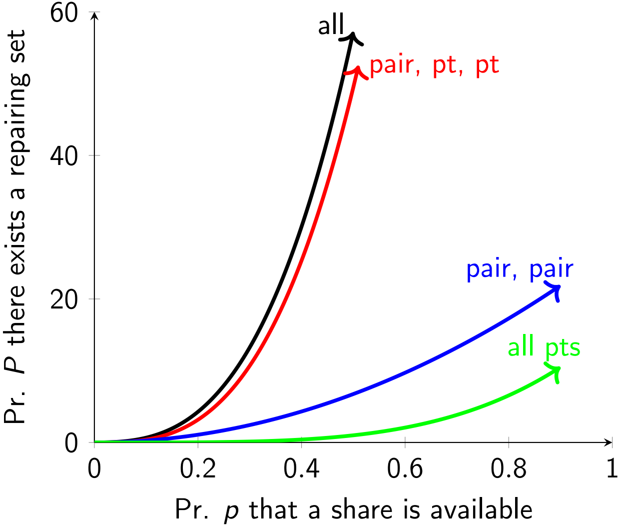


Figure: Expected number of Repair Sets By Type: $SQS(10)$

A Comparison for $SQS(28)$ and $(28, 4, 1)$-BIBD

Table: Available Repair Sets of Different Sizes for $v = 28$

	Value of p for $\mathbf{X \geq 1}$		**X for $\mathbf{p = 0.5}$**	
Repair Set Size	**$\mathbf{2-(28,4,1)}$**	**SQS(28)**	**$\mathbf{2-(28,4,1)}$**	**SQS(28)**
2	-	0.049	-	108
3	-	0.012	-	75744
4	0.130	0.013	256	2560000
any	0.130	0.010	256	2635850