Advances in Mathematics of Communications
Volume 13, No. 4, 2019, 601–612
doi:10.3934/amc.2019037

A NETWORK RELIABILITY APPROACH TO THE ANALYSIS OF COMBINATORIAL REPAIRABLE THRESHOLD SCHEMES

Bailey Kacsmar and Douglas R. Stinson*

David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada

Abstract. A *repairable threshold scheme* (which we abbreviate to *RTS*) is a (τ, n)-threshold scheme in which a subset of players can "repair" another player's share in the event that their share has been lost or corrupted. This will take place without the participation of the dealer who set up the scheme. The repairing protocol should not compromise the (unconditional) security of the threshold scheme. *Combinatorial repairable threshold schemes* (or *combinatorial RTS*) were recently introduced by Stinson and Wei [8]. In these schemes, "multiple shares" are distributed to each player, as defined by a suitable combinatorial design called the *distribution design*. In this paper, we study the *reliability* of these combinatorial repairable threshold schemes in a setting where players may not be available to take part in a repair of a given player's share. Using techniques from network reliability theory, we consider the probability of existence of an available repair set, as well as the expected number of available repair sets, for various types of distribution designs.

1. Introduction to combinatorial repairability

Suppose that τ and n are positive integers such that $\tau \leq n$. Informally, a (τ, n)-*threshold scheme* is a method whereby a *dealer* chooses a *secret* and distributes a *share* to each of n *players* (denoted by $P_1, \dots, P_n$) such that the following two properties are satisfied:

reconstruction: Any subset of τ players can compute the secret from the shares that they collectively hold, and

secrecy: No subset of $\tau - 1$ players can determine any information about the secret.

We call τ the *threshold* of the scheme.

In this paper, we are only interested in schemes that are *unconditionally secure*. That is, all security results are valid against adversaries with unlimited computational power.

The efficiency of secret sharing is often measured in terms of the *information rate* of the scheme, which is defined to be the ratio $\rho = \log_2 |\mathcal{K}| / \log_2 |\mathcal{S}|$ (where $\mathcal{S}$ is the set of all possible shares and $\mathcal{K}$ is the set of all possible secrets). That is, the information rate is the ratio of the size of the secret to the size of a share. For a threshold scheme, a fundamental result states that $\rho \leq 1$.

2010 *Mathematics Subject Classification:* Primary: 94A62; Secondary: 05B05, 90B25.
Key words and phrases: Threshold scheme, combinatorial repairability, reliability.
The second author is supported by NSERC discovery grant RGPIN-03882.
* Corresponding author: Douglas R. Stinson.

We briefly describe a standard construction for threshold schemes with optimal information rate, namely, the classical Shamir threshold scheme [6]. The construction takes place over a finite field $\mathbb{F}_Q$, where $Q \geq n+1$.

1. In the **Initialization Phase**, the dealer, denoted by D, chooses n distinct, non-zero elements of $\mathbb{F}_Q$, denoted x_i, $1 \leq i \leq n$. The values x_i are public. For $1 \leq i \leq n$, D gives the value x_i to player P_i.
2. In the **Share Distribution** phase, D chooses a secret
$$K = a_0 \in \mathbb{F}_Q.$$
Then D secretly chooses (independently and uniformly at random)
$$a_1, \dots, a_{\tau-1} \in \mathbb{F}_Q.$$
Finally, for $1 \leq i \leq n$, D computes the share $y_i = a(x_i)$, where
$$a(x) = \sum_{j=0}^{\tau-1} a_j\, x^j,$$
and gives it to player P_i.

Reconstruction is easily accomplished using the Lagrange interpolation formula (see, e.g., [7, §11.5.1]).

The problem of *share repairability* has been considered by several authors in recent years (see Laing and Stinson [5] for a survey on this topic). The problem setting is that a certain player P_ℓ (in a (τ, n)-threshold scheme, say) loses their share. The goal is to find a "secure" protocol involving P_ℓ and a subset of the other players that allows the missing share y_ℓ to be reconstructed. (Of course the dealer could simply re-send the share to P_ℓ, but we are considering a setting where the dealer is no longer present in the scheme after the initial setup.) In general, we will assume secure pairwise channels linking pairs of players.

A combinatorial solution to this problem was proposed by Stinson and Wei [8]. These schemes are termed *combinatorial RTS*. The construction is based on an old technique from [1, Theorem 1], namely, giving each player a subset of shares from an underlying threshold scheme called a *base scheme*.[1]

Suppose the base scheme is an (σ, m)-threshold scheme, say a Shamir scheme, implemented over a finite field $\mathbb{F}_Q$. We then give each player a certain subset of d of the m shares. A set system (or *design*) consisting of n blocks of size d, defined on a set of m points, will be used to do this. This design is termed the *distribution design*.

We will call the shares of the base (σ, m)-threshold scheme *subshares*. Each share in the resulting (τ, n)-threshold scheme, which we call the *expanded scheme*, consists of d subshares. Suppose the shares in the base scheme are denoted $s_1, \dots, s_m$, and suppose that the points in the distribution design are denoted $1, \dots, m$. Each player P_i corresponds to a block B_i of the distribution design. For each point $x \in B_i$, the player P_i is given the subshare s_x. The points in a block are indices of subshares received by a given player. The blocks are public information, while the values of the shares and subshares are secret.

[1] Actually, there are situations where there are efficiency advantages to use a *ramp scheme* as the base scheme, instead of a threshold scheme. This is addressed in some detail in [8]. However, for the purposes of repairability, it is irrelevant if we use a ramp scheme, as opposed to a threshold scheme. So we do not discuss the use of ramp schemes in this paper.

We need to ensure that the relevant threshold property is satisfied for the expanded threshold scheme. We also need to be able to repair the share of any player in the expanded scheme by appropriately choosing a certain set of other players, who will then send appropriate subshares to the player whose share is being repaired.

Let the blocks in the distribution design be denoted $B_1, \ldots, B_n$ and let X denote the set of m points on which the design is defined. The desired threshold property for the expanded scheme will be satisfied provided that the following two conditions hold in the distribution design:

$$\text{the union of any } \tau \text{ blocks contains at least } \sigma \text{ points} \tag{1}$$

and

$$\text{the union of any } \tau - 1 \text{ blocks contains at most } \sigma - 1 \text{ points.} \tag{2}$$

Summarizing, we have the following theorem from [8].

Theorem 1.1. *Suppose $(X, \mathcal{B})$ is a distribution design with $|X| = m$ and $|\mathcal{B}| = n$. Let τ and σ be positive integers and suppose (1) and (2) are satisfied for the given distribution design. Then, if we use a base (σ, m)-threshold scheme in conjunction with the given distribution design, we obtain an expanded (τ, n)-threshold scheme.*

1.1. REPAIRING A SHARE. Now, suppose we want to repair the share for a player P_ℓ corresponding to the block B_ℓ. For each point $x \in B_\ell$, we find another block that contains x. The corresponding player can send the subshare s_x corresponding to x to P_ℓ. We illustrate the technique with an example.

Example 1.1. Suppose we start with a $(9, 3, 1)$-BIBD (an affine plane of order 3), which has $n = 12$ blocks of size $d = 3$. There are $m = 9$ points in the design. We associate a block of the design with each player:

$$\begin{array}{lll} P_1 \leftrightarrow B_1 = \{1,2,3\} & P_2 \leftrightarrow B_2 = \{4,5,6\} & P_3 \leftrightarrow B_3 = \{7,8,9\} \\ P_4 \leftrightarrow B_4 = \{1,4,7\} & P_5 \leftrightarrow B_5 = \{2,5,8\} & P_6 \leftrightarrow B_6 = \{3,6,9\} \\ P_7 \leftrightarrow B_7 = \{1,5,9\} & P_8 \leftrightarrow B_8 = \{2,6,7\} & P_9 \leftrightarrow B_9 = \{3,4,8\} \\ P_{10} \leftrightarrow B_{10} = \{1,6,8\} & P_{11} \leftrightarrow B_{11} = \{2,4,9\} & P_{12} \leftrightarrow B_{12} = \{3,5,7\} \end{array}$$

Each player gets $d = 3$ shares from a $(5, 9)$-threshold 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 player; thus P_1 has the shares s_1, s_2 and s_3. Each block contains three points and the union of any two blocks contains at least five points. Thus (1) and (2) are satisfied for $\tau = 2$ and $\sigma = 5$ and therefore the expanded scheme is a $(2, 12)$-threshold scheme.

Now suppose P_1 wishes to repair their share. P_1 requires the subshares s_1, s_2 and s_3. The subshare s_1 can be obtained from P_4, P_7 or P_{10}; the subshare s_2 can be obtained from P_5, P_8 or P_{11}; and the subshare s_3 can be obtained from P_6, P_9 or P_{12}. □

In general, it is not a requirement that the d subshares are obtained from d different blocks. For example, it could happen that $d = 3$, one block contributes two subshares, and one block contributes one subshare during the repairing process. See Section 3 for further discussion of this idea.

It is quite simple to analyze the security of combinatorial repairability. The main point to observe is that the information collectively held by any subset of players (after the repairing protocol is completed) consists only of their shares in the expanded scheme. They did not obtain any information collectively that they did not already possess before the execution of the repairing protocol. So, it is immediate that a set $\tau - 1$ players cannot compute the secret after the repairing of a share occurs.

The paper [8] provides several constructions for combinatorial RTS. Different distribution designs are studied and analyzed according to various metrics. Here, we are only interested in repairability properties, so we do not address these other metrics.

1.2. RELIABILITY. Given a player P_ℓ in a combinatorial RTS, a subset of players that can repair P_ℓ's share is called a *repair set* for P_ℓ. A repair set $\mathcal{P}$ for a player P_ℓ is *minimal* if no proper subset of $\mathcal{P}$ is a repair set for P_ℓ. In Example 1.1, there are $3^3 = 27$ minimal repair sets for any given player.

We are interested in studying the situation where some of the players might not be available when asked to provide a subshare to repair another player's share. We will make the assumption that any player is available with a fixed probability p (and therefore unavailable with probability $1 - p$). We also assume that the availability of any player is independent of the availability of any other player. A repair set is *available* if every player in the set is available.

In the above setting, we can ask two basic questions for a given player associated with a given distribution design:

1. What is the probability $\mathcal{R}(p)$ that there is at least one available repair set?
2. What is the expected number $E(p)$ of available minimal repair sets?

We illustrate these concepts by considering the distribution design presented in Example 1.1.

Example 1.2. There is an available repair set for P_1 if and only if

- at least one of P_4, P_7 or P_{10} is available,
- at least one of P_5, P_8 or P_{11} is available, and
- at least one of P_6, P_9 or P_{12} is available.

Therefore, for P_1,

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

In fact, $\mathcal{R}(p)$ takes on the same value for any player in this RTS.

To compute the expected number of minimal repair sets, we observe that there are 27 minimal repair sets, each of which is available with probability p^3. By linearity of expectation, $E(p) = 27p^3$. Again, this value is the same for any player in the scheme. □

1.3. DESIGN THEORY DEFINITIONS. We now review some standard definitions and basic results from design theory. Most of these results can be found in standard references such as [3].

Definition 1.2. Suppose $2 \leq k < v$. A (v, k, λ)-*balanced incomplete block design*, or (v, k, λ)-BIBD, is a design $(X, \mathcal{B})$ such that:

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

Theorem 1.3. *Every point in a* (v, k, λ)-BIBD *occurs in exactly*

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

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

Theorem 1.4. *A (v, k, λ)-BIBD has exactly*

$$b = \frac{vr}{k} = \frac{\lambda(v^2 - v)}{k^2 - k}$$

blocks of size k.

Definition 1.5. A *Steiner triple system*, or $\mathsf{STS}(v)$, is a $(v, 3, 1)$-BIBD.

Theorem 1.6. *There exists an $\mathsf{STS}(v)$ if and only if $v \equiv 1, 3 \pmod 6$, $v \geq 7$.*

Definition 1.7. A t-(v, k, λ)-*design* is a design where:

1. $|X| = v$,
2. each block $B \in \mathcal{B}$ contains exactly k points, and
3. every set of t points from the set X occurs in exactly λ blocks.

Definition 1.8. A 3-$(v, 4, 1)$-design is a *Steiner quadruple system* of order v, denoted $\mathsf{SQS}(v)$.

Theorem 1.9. *An $\mathsf{SQS}(v)$ exists if and only if $v \equiv 2, 4 \pmod 6$.*

Theorem 1.10. [3, Theorem II.4.8] *The i^{th}* replication number*, denoted r_i, of a t-$(v, k, 1)$-design is defined to be the number of blocks containing any given set of i points. It is known that*

$$r_i = \frac{\lambda\binom{v-i}{t-i}}{\binom{k-i}{t-i}},$$

for $1 \leq i \leq t$.

Theorem 1.11. *The number of blocks in a t-$(v, k, 1)$-design is*

$$b = \frac{\binom{v}{t}}{\binom{k}{t}} = \frac{vr_1}{k}.$$

Definition 1.12. An *inversive geometry* is a 3-$(n^d+1, n+1, 1)$-design, where $d \geq 2$.

Theorem 1.13. *An inversive geometry exists for any $d \geq 2$ if n is a prime power.*

1.4. ORGANIZATION OF THE PAPER. The remaining sections of the paper are organized as follows. In Section 2, we study the reliability metrics for BIBDs. In Section 3, we turn to t-designs with $t > 2$, which have not previously been studied as distribution designs. After addressing the possible thresholds that can be obtained, we again consider the reliability metrics. Finally, Section 4 is a brief summary.

2. USING BIBDS AS DISTRIBUTION DESIGNS

Stinson and Wei [8] examined several types of BIBDs with $\lambda = 1$ for use as distribution designs in combinatorial RTS. They studied the thresholds of these RTS as well as their efficiency with respect to storage, communication complexity and computational complexity. In this section, we study the reliability of these RTS using the measures defined in Section 1.2.

Before proceeding further, we define some notation that will be used in the rest of the paper.

Definition 2.1. Suppose $(X, \mathcal{B})$ is a distribution design for a combinatorial RTS. For any fixed block $B_i \in \mathcal{B}$, let P_i be the corresponding player in the RTS. Further, for any $x_j \in B_i$, define

$$\mathcal{C}_j = \{B \in \mathcal{B} \setminus \{B_i\} : x_j \in B\}.$$

Finally, let $\mathcal{P}_j = \{P_i : B_i \in \mathcal{C}_j\}$.

Example 2.1. We refer to Examples 1.1 and 1.2. For the block $B_1 = \{1, 2, 3\}$, we have

$$\begin{aligned}
\mathcal{C}_1 &= \{B_4, B_7, B_{10}\}\\
\mathcal{C}_2 &= \{B_5, B_8, B_{11}\}\\
\mathcal{C}_3 &= \{B_6, B_9, B_{12}\}
\end{aligned}$$

and therefore

$$\begin{aligned}
\mathcal{P}_1 &= \{P_4, P_7, P_{10}\}\\
\mathcal{P}_2 &= \{P_5, P_8, P_{11}\}\\
\mathcal{P}_3 &= \{P_6, P_9, P_{12}\}.
\end{aligned}$$

□

As in Section 1.2, we define $\mathcal{R}(p)$ to be the probability that there is at least one available repair set for a given player.

Theorem 2.2. *Suppose $(X, \mathcal{B})$ is a $(v, k, 1)$-BIBD that is used as a distribution design for a combinatorial RTS, and let P_i be any player in the scheme. Then*

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

Proof. Let the block corresponding to P_i be $B_i = \{x_1, \ldots, x_k\}$. Consider the sets $\mathcal{C}_j$, for $1 \leq j \leq k$, as defined in Definition 2.1. Clearly $|\mathcal{C}_j| = r - 1$ for $1 \leq j \leq k$ and $\mathcal{C}_j \cap \mathcal{C}_{j'} = \emptyset$ if $j \neq j'$.

The probability that at least one player in $\mathcal{P}_j$ is available is $1 - (1 - p)^{r-1}$. Then, since the sets $\mathcal{P}_j$ are disjoint, the probability that at least one player in each $\mathcal{P}_j$ is available is $(1 - (1 - p)^{r-1})^k$. □

Now we consider the expected number of repair sets when using a $(v, k, 1)$-BIBD as a distribution design.

Theorem 2.3. *Suppose $(X, \mathcal{B})$ is a $(v, k, 1)$-BIBD that is used as a distribution design for a combinatorial RTS, and let P_i be any player in the scheme. Then*

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

Proof. Let $B_i = \{x_1, \ldots, x_k\}$. The minimal repair sets are precisely the sets in $\mathcal{P}_1 \times \cdots \times \mathcal{P}_k$. The number of minimal repair sets is therefore $(r - 1)^k$. The probability that a given minimal repair set is available is p^k.

Let the minimal repair sets be enumerated as $\mathcal{M}_1, \ldots, \mathcal{M}_s$, where $s = (r - 1)^k$. For $1 \leq i \leq s$, let the random variable $\mathbf{X_i}$ be defined as

$$\mathbf{X_i} = \begin{cases} 1, & \text{if } \mathcal{M}_i \text{ is available} \\ 0, & \text{otherwise.} \end{cases}$$

Clearly $E[\mathbf{X_i}] = p^k$ for all i. Define

$$\mathbf{X} = \mathbf{X_1} + \mathbf{X_2} + \cdots + \mathbf{X_s};$$

then

$$E[\mathbf{X}] = E[\mathbf{X_1}] + E[\mathbf{X_2}] + \cdots + E[\mathbf{X_s}]$$

by linearity of expectation. Therefore,

$$E(p) = E[\mathbf{X}] = sp^k = (r-1)^k p^k.$$

□

It would of course be possible to use a (v, k, λ)-BIBD as a distribution design even if $\lambda > 1$. Unfortunately, there do not seem to be general formulas, analogous to Theorems 2.2 and 2.3, for these designs.

3. Using t-designs as distribution designs

It is also possible to use t-$(v, k, 1)$-designs with $t > 2$ as distribution designs. This idea has not previously been discussed in the literature. One possible advantage over just using 2-designs is that blocks can intersect in more than one point, so a repair may be possible by contacting a smaller number of other players. Since blocks in a t-$(v, k, 1)$-design can intersect in up to $t-1$ points, it follows that a repair can be carried out by contacting $\lceil \frac{k}{t-1} \rceil$ other players, if they are available.

First, we determine the thresholds that can be achieved, in particular, by Steiner quadruple systems and inversive geometries. Later in this section we analyze the reliability of the RTS derived from them.

3.1. Distribution designs and thresholds. For a given distribution design, it is of interest to determine the thresholds that can be realized in an expanded scheme. This involves choosing values for τ and σ in such a way that (1) and (2) are satisfied, and then applying Theorem 1.1. We provide some results along this line in this section. We note that similar techniques were used in [8] for 2-designs.

Theorem 3.1. *An* $\mathsf{SQS}(v)$ *can be used as a distribution design to produce an RTS with threshold* 2.

Proof. Let $\tau = 2$ and $\sigma = 6$. It is clear that one block in an $\mathsf{SQS}(v)$ contains exactly four points. Two blocks contain at least six points, because two blocks intersect in at most two points. Therefore, (1) and (2) are satisfied when $\tau = 2$ and $\sigma = 6$, and we obtain an expanded scheme with threshold 2. □

Now, we show how to construct RTS with threshold 3 from certain t-designs.

Theorem 3.2. *A* t-$(v, k, 1)$*-design can be used as a distribution design to produce an RTS with threshold* 3 *if* $k \geq 3t - 2$.

Proof. Let $\tau = 2$ and $\sigma = 3k - 3(t-1)$. Clearly the union of any two blocks contains at most $2k$ points. Now consider three blocks. If any two of these blocks have $t-1$ points in common, and these three intersections are disjoint, then the three blocks contain $3k - 3(t-1)$ points, which is the minimum possible. In order for (1) and (2) to be satisfied, we require $3k - 3(t-1) \geq 2k + 1$, which is equivalent to $k \geq 3t - 2$. If this inequality is satisfied, then the expanded scheme has threshold 3. □

More generally, we have the following result, which has a similar proof.

Theorem 3.3. *A* t-$(v, k, 1)$*-design can be used as a distribution design to produce an RTS with threshold* τ *if* $k \geq \binom{\tau}{2}(t-1) + 1$.

Proof. Let $\sigma = \tau k - \binom{\tau}{2}(t-1)$. Clearly $\tau - 1$ blocks contain at most $(\tau-1)k$ points. For a set of τ blocks, the minimum size of their union results when any two of them contain $t-1$ common points, and these intersections are all disjoint. So the union contains at least $\tau k - \binom{\tau}{2}(t-1)$ points. In order for (1) and (2) to be satisfied, we require $\tau k - \binom{\tau}{2}(t-1) \geq (\tau-1)k + 1$, which is equivalent to $k \geq \binom{\tau}{2}(t-1) + 1$. If this inequality is satisfied, then the expanded scheme has threshold τ. $\square$

The inversive geometries allow us to construct RTS with any desired threshold. Taking $t = 3$ in Theorem 3.3, we have the following corollary.

Corollary 1. *A 3-$(v, k, 1)$-design can be used as a distribution design to produce an RTS with threshold τ if $k \geq \tau(\tau - 1) + 1$.*

Remark 1. In order to obtain $\tau = 3$, we require $k \geq 7$ in Corollary 1; to obtain $\tau = 4$, we require $k \geq 13$, etc.

3.2. RELIABILITY. In our analysis, to compute the reliability metrics for repair sets, we employ the use of *cutsets* from network reliability theory (see Colbourn [2] for basic results and terminology relating to network reliability). When using BIBDs as distribution designs, we were able to easily compute reliability formulas in Section 2 without the use of this methodology because the sets $\mathcal{C}_j$ were disjoint. However, it is advantageous to use cutsets to analyze the reliability of the RTS constructed using distribution designs with $t \geq 3$.

In this section, for brevity, we will conflate the notion of players and blocks and express all our arguments in terms of blocks of the distribution design $(X, \mathcal{B})$.

Definition 3.4. A *cutset* for a block B is a minimal subset of blocks $\mathcal{B}'$ such that a repair is not possible if all the blocks in $\mathcal{B}'$ are not available. A cutset *fails* if every block in the cutset is not available.

Lemma 3.5. *Let $B = \{x_1, \ldots, x_k\}$ be a block in the distribution design. Then the sets $\mathcal{C}_j$, for $1 \leq j \leq k$, are the cutsets.*

Example 3.1. Here are the blocks in an 3-$(8, 4, 1)$-design:

$$
\begin{aligned}
A_1 &= \{1,2,3,4\} & A_2 &= \{5,6,7,8\} \\
B_1 &= \{1,2,5,6\} & B_2 &= \{1,2,7,8\} \\
B_3 &= \{1,3,5,7\} & B_4 &= \{1,3,6,8\} \\
B_5 &= \{1,4,5,8\} & B_6 &= \{1,4,6,7\} \\
B_7 &= \{3,4,7,8\} & B_8 &= \{3,4,5,6\} \\
B_9 &= \{2,4,6,8\} & B_{10} &= \{2,4,5,7\} \\
B_{11} &= \{2,3,6,7\} & B_{12} &= \{2,3,5,8\}
\end{aligned}
$$

Suppose A_1 wants to repair their share. Then, the relevant cutsets are

$$
\begin{aligned}
\mathcal{C}_1 &= \{B_1, B_2, B_3, B_4, B_5, B_6\} \\
\mathcal{C}_2 &= \{B_1, B_2, B_9, B_{10}, B_{11}, B_{12}\} \\
\mathcal{C}_3 &= \{B_3, B_4, B_7, B_8, B_{11}, B_{12}\} \\
\mathcal{C}_4 &= \{B_5, B_6, B_7, B_8, B_9, B_{10}\}.
\end{aligned}
$$

$\square$

Lemma 3.6. *Let $B = \{x_1, \ldots, x_k\}$ be a block in the distribution design $(X, \mathcal{B})$. There exists an available repair set for B if and only if no $\mathcal{C}_j$, for $1 \leq j \leq k$, fails.*

3.3. Existence of available repair sets for t-$(v,k,1)$ designs. First, we consider Steiner quadruple systems, as a warmup. Then we generalize our formulas to arbitrary t-$(v,k,1)$ designs.

Theorem 3.7. *Suppose $(X,\mathcal{B})$ is an $\mathsf{SQS}(v)$ and let $B=\{x_1,x_2,x_3,x_4\}\in\mathcal{B}$. Let $q=1-p$, where p is the probability that a block is available. Then*

$$\mathcal{R}(p)=1-4q^{r_1-1}+6q^{2r_1-r_2-1}-4q^{3r_1-3r_2}+q^{4r_1-6r_2+2},$$

where $r_1=\binom{v-1}{2}/3$ and $r_2=\binom{v-2}{1}/2$ are the replication numbers of the SQS.

Proof. From Lemma 3.6, a repair set exists if no $\mathcal{C}_j$ fails, $1\leq j\leq 4$. Therefore,

$$\mathcal{R}(p)=1-\Pr[\text{at least one } \mathcal{C}_j \text{ fails}].$$

For $1\leq j\leq 4$, let E_j denote the event that $\mathcal{C}_j$ fails. We have

$$\Pr[\text{at least one } \mathcal{C}_j \text{ fails}]=\Pr[E_1 \text{ or } E_2 \text{ or } E_3 \text{ or } E_4].$$

We note the following.

1. $|\mathcal{C}_j|=r_1-1$ for $1\leq j\leq 4$. Therefore,
$$\Pr[E_i]=q^{r_1-1}.$$
2. $|\mathcal{C}_j\cup\mathcal{C}_{j'}|=2(r_1-1)-(r_2-1)=2r_1-r_2-1$, for all $j,j',j\neq j'$. Therefore,
$$\Pr[E_j \text{ and } E_{j'}]=q^{2r_1-r_2-1}.$$
3. $|\mathcal{C}_j\cup\mathcal{C}_{j'}\cup\mathcal{C}_{j''}|=3(r_1-1)-3(r_2-1)=3r_1-3r_2$, for all distinct j,j',j'' such that $1\leq j,j',j''\leq 4$. Therefore,
$$\Pr[E_j \text{ and } E_{j'} \text{ and } E_{j''}]=q^{3r_1-3r_2}.$$
4. $|\mathcal{C}_1\cup\mathcal{C}_2\cup\mathcal{C}_3\cup\mathcal{C}_4|=4(r_1-1)-6(r_2-1)=4r_1-6r_2+2$. Therefore,
$$\Pr[E_1 \text{ and } E_2 \text{ and } E_3 \text{ and } E_4]=q^{4r_1-6r_2+2}.$$

Applying the principle of inclusion-exclusion, we have

$$\Pr[E_1 \text{ or } E_2 \text{ or } E_3 \text{ or } E_4]=\binom{4}{1}q^{r_1-1}-\binom{4}{2}q^{2r_1-r_2-1}+\binom{4}{3}q^{3r_1-3r_2}-\binom{4}{4}q^{4r_1-6r_2+2}.$$

Therefore,

$$\mathcal{R}(p)=1-4q^{r_1-1}+6q^{2r_1-r_2-1}-4q^{3r_1-3r_2}+q^{4r_1-6r_2+2}.$$

$\square$

The following can be proven in a similar manner.

Theorem 3.8. *Suppose $(X,\mathcal{B})$ is a t-$(v,k,1)$ design and let $B\in\mathcal{B}$. Let $q=1-p$, where p is the probability that a block is available. Then*

$$\mathcal{R}(p)=1-\binom{k}{1}q^{e_1}+\binom{k}{2}q^{e_2}-\binom{k}{3}q^{e_3}+\cdots+(-1)^{k+1}\binom{k}{k}q^{e_k},$$

where $r_j=\frac{\binom{v-j}{t-j}}{\binom{k-j}{t-j}}$, for $1\leq j\leq t$, are the replication numbers of the design, and

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

for $1\leq i\leq k$.

Proof. We use similar notation as in the proof of Theorem 3.7. We compute

$$\Pr[\text{at least one } \mathcal{C}_j \text{ fails}] = \Pr[E_1 \text{ or } E_2 \text{ or } E_3 \text{ or } E_4 \text{ or } \cdots \text{ or } E_k].$$

Let e_i denote the cardinality of the union of i of the sets $\mathcal{C}_1, \dots, \mathcal{C}_k$. We will apply the principle of inclusion-exclusion to compute the values of the e_i's. Note that we make use of the fact that no block intersects B in more than $t-1$ points, so the intersection of t or more of the sets $\mathcal{C}_1, \dots, \mathcal{C}_k$ is empty. Therefore,

$$\begin{aligned} e_1 &= r_1 - 1 \\ e_2 &= 2(r_1 - 1) - (r_2 - 1) \\ e_3 &= 3(r_1 - 1) - 3(r_2 - 1) + (r_3 - 1), \end{aligned}$$

etc., where no sum contains terms past r_{t-1}. In general,

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

for $1 \leq i \leq k$.

Now that we have computed e_i for each i, we can evaluate the probability that any number of C_i's fail. Recall that $q = 1 - p$, where p is the probability the player with that share is available. A second application of the principle of inclusion-exclusion yields the desired result:

$$\mathcal{R}(p) = 1 - \binom{k}{1} q^{e_1} + \binom{k}{2} q^{e_2} - \binom{k}{3} q^{e_3} + \cdots + (-1)^{k+1} \binom{k}{k} q^{e_k}.$$

□

3.4. EXPECTED NUMBER OF MINIMAL REPAIR SETS FOR SQS. In general, we can determine the expected number of repair sets for a given distribution design if we know all the minimal repair sets. The following formula, which is proven in the same fashion as Theorem 2.3, can be used.

Theorem 3.9. *Suppose $(X, \mathcal{B})$ is a distribution design and let the minimal repair sets be enumerated as $\mathcal{M}_1, \dots, \mathcal{M}_s$. Then*

$$E(p) = \sum_{j=1}^{s} p^{|\mathcal{M}_i|}.$$

Of course, for an arbitrary distribution design, there can be minimal repair sets of various sizes. For example, in the case of Steiner quadruple systems, minimal repair sets can be of size two, three or four.

We illustrate the computation of the expected number of available minimal repair sets on a particular design, namely, the $\mathsf{SQS}(10)$.

Example 3.2. Here is the (unique) 3-$(10, 4, 1)$-design:

$A_0 = \{1, 2, 4, 5\}$	$B_0 = \{1, 2, 3, 7\}$	$C_0 = \{1, 3, 5, 8\}$
$A_1 = \{2, 3, 5, 6\}$	$B_1 = \{2, 3, 4, 8\}$	$C_1 = \{2, 4, 6, 9\}$
$A_2 = \{3, 4, 6, 7\}$	$B_2 = \{3, 4, 5, 9\}$	$C_2 = \{3, 5, 7, 0\}$
$A_3 = \{4, 5, 7, 8\}$	$B_3 = \{4, 5, 6, 0\}$	$C_3 = \{4, 6, 8, 1\}$
$A_4 = \{5, 6, 8, 9\}$	$B_4 = \{5, 6, 7, 1\}$	$C_4 = \{5, 7, 9, 2\}$
$A_5 = \{6, 7, 9, 0\}$	$B_5 = \{6, 7, 8, 2\}$	$C_5 = \{6, 8, 0, 3\}$

$$\begin{array}{lll} A_6 = \{7,8,0,1\} & B_6 = \{7,8,9,3\} & C_6 = \{7,9,1,4\} \\ A_7 = \{8,9,1,2\} & B_7 = \{8,9,0,4\} & C_7 = \{8,0,2,5\} \\ A_8 = \{9,0,2,3\} & B_8 = \{9,0,1,5\} & C_8 = \{9,1,3,6\} \\ A_9 = \{0,1,3,4\} & B_9 = \{0,1,2,6\} & C_9 = \{0,2,4,7\} \end{array}$$

Suppose we want to repair the block $A_0 = \{1,2,4,5\}$. We consider minimal repair sets of sizes $2, 3$ and 4 in turn. All the computations are applications of Theorem 3.9.

A repair 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 for these two blocks is $3 \times 3 \times 3 = 27$ (there are three subcases, and in each subcase there are three choices of each of the two blocks). Therefore, the expected number of minimal repair sets of size two is $27p^2$.

A minimal repair 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, so the total number of choices is $2^4 = 16$. Therefore, the expected number of minimal repair sets of size four is $16p^4$.

A minimal repair 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 repair sets of size three is seen to be

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

Finally, we have

$$E(p) = 27p^2 + 396p^3 + 16p^4.$$

□

The general case of an $\mathsf{SQS}(v)$ is similar. We tabulate the expected number of minimal repair sets of the various types in the Table 1.

We can now combine the expected number of repair sets for each size and type to produce the expected number of repair sets, which we record in the following theorem.

Theorem 3.10. *Suppose $(X, \mathcal{B})$ is an $\mathsf{SQS}(v)$ and let $B \in \mathcal{B}$. Let $q = 1 - p$, where p is the probability that a block is available. Then*

$$E(p) = 3(r_2-1)^2p^2 + 2(r_2-1)(3{r_1}^2 - 12r_1r_2 + 6r_1 + 11{r_2}^2 - 10r_2 + 2)p^3 + (r_1 - 3r_2 + 2)^4p^4.$$

TABLE 1. Expected number of repair sets for $\mathsf{SQS}(v)$

size	type	expected number
2		$3(r_2-1)^2p^2$
3	pair-pair-pair	$4(r_2-1)^3p^3$
3	pair-pair-point	$12(r_2-1)^2(r_1-3r_2+2)p^3$
3	pair-point-point	$6(r_2-1)(r_1-3r_2+2)^2p^3$
4		$(r_1-3r_2+2)^4p^4$

4. DISCUSSION AND SUMMARY

The material in this paper is from the Masters Thesis of the first author [4].

We have introduced the problem of studying reliability of combinatorial RTS. We employed techniques from network reliability theory to aid in the derivation of some of our formulas. Perhaps this approach will prove useful in other combinatorial design problems that can be phrased in terms of network reliability.

A separate but related question is how to design efficient algorithms to actually find a repair set for various kinds of distribution designs. This problem is discussed in detail in [4] where algorithms are developed for the various types of designs we have considered. We note that different fault models for node failures (i.e., permanent vs transient faults) are discussed in [4]. Various metrics are also analyzed, such as storage requirements and communication complexity, as well as tradeoffs between these metrics.

REFERENCES

[1] J. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, *Lecture Notes in Computer Science*, **403** (1990), 27–35 (CRYPTO '88 Proceedings).

[2] C. J. Colbourn, *The Combinatorics of Network Reliability*, Oxford University Press, 1987.

[3] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs, Second Edition,* Chapman & Hall/CRC, Boca Raton, FL, 2007.

[4] B. Kacsmar, *Designing Efficient Algorithms for Combinatorial Repairable Threshold Schemes*, Masters Thesis, University of Waterloo, 2018.

[5] T. M. Laing and D. R. Stinson, A survey and refinement of repairable threshold schemes, *Journal of Mathematical Cryptology*, **12** (2018), 57–81.

[6] A. Shamir, How to share a secret, *Communications of the ACM*, **22** (1979), 612–613.

[7] D. R. Stinson and M. B. Paterson, *Cryptography. Theory and Practice*, Chapman & Hall/CRC, Boca Raton, 2019.

[8] D. R. Stinson and R. Wei, Combinatorial repairability for threshold schemes, *Designs, Codes and Cryptography*, **86** (2018), 195–210.

Received November 2018; revised January 2019.

E-mail address: bkacsmar@uwaterloo.ca
E-mail address: dstinson@uwaterloo.ca