Annales UMCS Informatica AI XII, 3 (2012) 55–64
DOI: 10.2478/v10065-012-0020-4

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

A Remark on Hierarchical Threshold Secret Sharing

Renata Kawa*, Mieczysław Kula†

Institute of Mathematics, University of Silesia,
Bankowa 14, 40-007 Katowice, Poland.

Abstract – The main results of this paper are theorems which provide a solution to the open problem posed by Tassa [**1**]. He considers a specific family Γ_v of hierarchical threshold access structures and shows that two extreme members $\Gamma_\wedge$ and $\Gamma_\vee$ of Γ_v are realized by secret sharing schemes which are ideal and perfect. The question posed by Tassa is whether the other members of Γ_v can be realized by ideal and perfect schemes as well. We show that the answer in general is negative. A precise definition of secret sharing scheme introduced by Brickell and Davenport in [**2**] combined with a connection between schemes and matroids are crucial tools used in this paper. Brickell and Davenport describe secret sharing scheme as a matrix $\mathbf{M}$ with $n+1$ columns, where n denotes the number of participants, and define ideality and perfectness as properties of the matrix $\mathbf{M}$. The auxiliary theorems presented in this paper are interesting not only because of providing the solution of the problem. For example, they provide an upper bound on the number of rows of $\mathbf{M}$ if the scheme is perfect and ideal.

1 Introduction

An idea of secret sharing was introduced independently by Blackley [**3**] and Shamir [**4**] in 1979. The basic idea is to distribute pieces of information (shares) about the secret among a finite set of participants, so that only some sets of them can recover the secret by pooling together their shares. Such a set of participants is said to be *authorized*. The family Γ of all authorized sets of participants is referred to as the *access structure* of the scheme.

Before we present a formal definition, we introduce some notions that will be used throughout this paper. Let P be a finite set of participants and for $p \in P$ let $S(p)$ denote the set of all possible shares which can be given to the participant p. It is

*renata.kawa@us.edu.pl
†kula@math.us.edu.pl

sometimes convenient to consider a special participant p_0 (called a dealer) who shares a secret. We will use P^o to denote $P \cup \{p_0\}$. Obviously $S = S(p_0)$ is the set of all possible secrets.

It is a trivial observation that an access structure Γ of a secret sharing scheme has the monotonicity property, i.e.

$$A \subseteq B, A \in \Gamma \Longrightarrow B \in \Gamma. \tag{1}$$

We define Γ_{min} as the family of all minimal sets of Γ.

A secret sharing scheme is said to be *connected* if every participant is a member of a certain minimal authorized set. It is easy to see that if a secret sharing scheme is not connected, then the shares of a certain participant are useless. All secret sharing schemes considered in this paper are connected.

In practical implementation, secret sharing schemes are expected to be secure and easy in use. These requirements are satisfied if no information on secrets leaks to unauthorized sets and shares are as small as possible. Let us introduce the following definitions.

We say that secret sharing scheme is *perfect* if each unauthorized set of participants cannot reveal any information about the secret. It is not hard to show that for every perfect secret sharing scheme $|S(p)| \geq |S|$ for all $p \in P$. A secret sharing scheme is said to be *ideal* if $|S(p)| = |S|$ for all $p \in P$. Without loss of generality we can assume that in ideal secret sharing schemes we have $S = S(p)$ for every $p \in P$.

Obviously, when we have a fixed secret sharing scheme, we are able to describe its access structure. However, investigations concerning secret sharing scheme problems refer also to the situations where a family $\Gamma \subseteq 2^P$ with monotonicity property is defined and the goal is to find a secret sharing scheme such that Γ is its access structure. In such a situation we say that Γ is *realized* by a secret sharing scheme. It is not easy to find a suitable scheme that realizes given monotone family of sets of participants if we require ideality and perfectness. A partial solution to this problem can be found in the following theorem.

Theorem 1 (**[5]**)**.** For any monotone family $\Gamma \subseteq 2^P$ there exists a perfect secret sharing scheme with Γ as its access structure.

Unfortunately, a perfect secret sharing scheme constructed by the authors of Theorem 1 for any $\Gamma \subseteq 2^P$ is not ideal, each share is a vector with many entries. It is known that there exist monotone families of sets of participants which are not realized by a secret sharing scheme both ideal and perfect (see **[6]**, p.33, Theorem 3).

The idea of hierarchical secret sharing, in which P is composed of levels:

$$P = P_1 \dot{\cup} \cdots \dot{\cup} P_l. \tag{2}$$

was introduced by Shamir in **[4]**. He considered a scheme for a weighted threshold access structure. That is, every participant has a weight (a positive integer) and a set is qualified if and only if its weight sum is at least a given threshold. Simmons in **[7]**

studied the comparmented access structure:

$$\Gamma = \{A \subseteq P : \forall_{i\in\{1,2,\ldots,l\}} |A \cap P_i| \geq k_i, |A| \geq k_0\} \tag{3}$$

where $\{k_i\}_{i=0}^{l}$ is a sequence of integers such that $k_0 \geq \sum_{i=1}^{l} k_i$, and the multilevel access structure:

$$\Gamma_\vee = \{A \subseteq P : \exists_{i\in\{1,2,\ldots,l\}} |A \cap (\cup_{j=1}^{i} P_j)| \geq k_i\} \tag{4}$$

where $\{k_i\}_{i=1}^{l}$ is a monotonically increasing sequence of integers. An access structure $\Gamma_\vee$ was also considered by Tassa in [**1**], who called it a disjunctive access structure and in the same paper he studied a conjunctive access structure:

$$\Gamma_\wedge = \{A \subseteq P : \forall_{i\in\{1,2,\ldots,l\}} |A \cap (\cup_{j=1}^{i} P_j)| \geq k_i\}. \tag{5}$$

Moreover, Tassa notices that the above access structures are two extreme members of a family $\{\Gamma_v : v = 1, \ldots, l\}$ of the hierarchical threshold access structures:

$$\Gamma_v = \{A \subseteq P : |A \cap (\cup_{j=1}^{i} P_j)| \geq k_i \text{ for at least } v \text{ values of } i \in \{1, \ldots, l\}\}. \tag{6}$$

The question posed by Tassa is whether the other members of Γ_v can be realized by ideal and perfect schemes as well. We show that the answer in general is negative. It is worth pointing out that Farràs and Padró (see [**8**]) managed to characterize the ideal hierarchical access structures, that is, those admitting an ideal secret sharing scheme. Among other things, their work also contains an answer to the question of Tassa, however, our solution is different and simpler.

2 Secret sharing scheme as a matrix

Brickell and Davenport introduced in [**2**] the following general and precise definition of a secret sharing scheme.

Definition 1. Secret sharing scheme with n participants is a matrix $\mathbf{M}$ with $n+1$ columns and entries from a finite set, such that no two rows of $\mathbf{M}$ are identical.

The first column of the matrix is assigned to p_0, this is the column of secrets. The other columns are assigned to participants, they are columns of shares. The matrix $\mathbf{M}$ is publicly known and each participant knows which column belongs to him or her. Before we describe procedures of sharing a secret and pooling shares, we introduce a few useful notations. Let:

- $\mathbf{M}(r, p)$ be the entry in row r and column p.
- $\mathbf{M}(r, A)$ be the row r restricted to the columns indexed by A, $A \subseteq P^o$.
- $S(p)$ be the set of elements occurring in column p (it does not contradict the previous definition).
- $S(A) = \{\mathbf{M}(r, A) : r \text{ is a row of } \mathbf{M}\}$, $A \subseteq P^o$.

If the dealer wants to share out a secret $s \in S(p_0)$ among the participants in P, he/she:

(1) picks randomly a row $\hat{r}$ in which $\mathbf{M}(\hat{r}, p_0) = s$ using the uniform distribution over all such rows;
(2) gives the share $\alpha_p := \mathbf{M}(\hat{r}, p)$ to the participant p for every $p \in P$ using safe channel.

If participants in $A \subseteq P$ want to recover the secret $s \in S(p_0)$:

(1) they pool their shares together;
(2) they take one of the rows r such that $\alpha_p := \mathbf{M}(r, p)$ for all $p \in A$;
(3) they assume that $s = \mathbf{M}(r, p_0)$ is the secret.

There is a question whether the value obtained by the participants is always the secret chosen by the dealer, i.e., when A is an authorized set of participants. In the matrix settings we are able to give precise definitions of notions mentioned in Section 1. To do that, we need some additional notions.

We say that the participants in $A \subseteq P$ *have no information about the share* given to a participant $p \in P^o \setminus A$ if

$$\bigwedge_{r} \bigwedge_{\beta \in S(p)} \bigvee_{\hat{r}} \Big(\mathbf{M}(r, A) = \mathbf{M}(\hat{r}, A) \text{ and } \mathbf{M}(\hat{r}, p) = \beta \Big) \tag{7}$$

or equivalently

$$\bigwedge_{v \in S(A)} \bigwedge_{\beta \in S(p)} \bigvee_{r} \Big(\mathbf{M}(r, A) = v \text{ and } \mathbf{M}(r, p) = \beta \Big). \tag{8}$$

Otherwise, we say that A *has some information* about the share given to p. In these situations we write $A \nrightarrow p$ and $A \to p$ respectively. In the other words, $A \to p$ if for at least one vector $v \in S(A)$ some values in $S(p)$ cannot be taken as $\mathbf{M}(r, p)$ when $\mathbf{M}(r, A) = v$.

We say that participants in $A \subseteq P$ *know the share* given to a participant $p \in P^o \setminus A$, denoted by $A \Rightarrow p$, if

$$\bigwedge_{r} \bigwedge_{\hat{r}} \Big(\mathbf{M}(r, A) = \mathbf{M}(\hat{r}, A) \implies \mathbf{M}(r, p) = \mathbf{M}(\hat{r}, p) \Big). \tag{9}$$

Using the above notation a subset $A \subseteq P$ is *authorized* if $A \Rightarrow p_0$ and the access structure can be described as $\Gamma = \{A \subseteq P \colon A \Rightarrow p_0\}$. A secret sharing scheme is said to be *perfect* if

$$\bigwedge_{A \subseteq P} \Big(A \to p_0 \implies A \Rightarrow p_0 \Big). \tag{10}$$

Let us recall that a secret sharing scheme is said to be *ideal* if $|S(p)| = |S(p_0)|$ for all $p \in P$.

The next theorem says that in ideal and perfect secret sharing schemes the partial information about someone's share never occurs.

Theorem 2 ([**2**], p.126, Theorem 3)**.** Let $\mathbf{M}$ be an ideal and perfect secret sharing scheme. Let $A \subseteq P$ and $p \in P^o$. If $A \to p$, then $A \Rightarrow p$.

Let P^o be the set of participants of a secret sharing scheme $\mathbf{M}$. A set $A \subseteq P^o$ is said to be *dependent* if there is $p \in A$ such that $(A \setminus \{p\}) \Rightarrow p$. Otherwise, A is called *independent*. Let $\mathcal{D}(\mathbf{M})$ denote the family of all dependent sets of $\mathbf{M}$. It is obvious that if $A \subseteq P$ is an authorized set, then $A \cup \{p_0\}$ is dependent. It can be seen easily that every minimal authorized set is independent.

3 Auxiliary results

In this section we shall prove some relations between the cardinalities of maximal unauthorized sets and independent ones. Let us denote throughout this paper $q = |S|$.

Theorem 3. If $\mathbf{M}$ is an ideal and perfect secret sharing scheme, then the number of rows in $\mathbf{M}$ is not greater than $q^{|B|+1}$ for every maximal unauthorized set $B \subseteq P$.

Proof. Let $\mathbf{M}$ be an ideal and perfect secret sharing scheme and let $B \subseteq P$ be a maximal unauthorized set. Suppose, contrary to our claim, that $\mathbf{M}$ has more than $q^{|B|+1}$ rows. Then there exist two different rows $\tilde{r}$, $\hat{r}$ in $\mathbf{M}$ such that

$$\mathbf{M}(\tilde{r}, B \cup \{p_0\}) = \mathbf{M}(\hat{r}, B \cup \{p_0\}). \tag{11}$$

Denote $v = \mathbf{M}(\tilde{r}, B) = \mathbf{M}(\hat{r}, B) \in S^{|B|}$. From the fact that no two rows of $\mathbf{M}$ are identical we obtain

$$\mathbf{M}(\tilde{r}, p) \neq \mathbf{M}(\hat{r}, p) \tag{12}$$

for a certain participant $p \in P \setminus B$. Obviously $B \cup \{p\}$ is an authorized set, as B is a maximal unauthorized set. Thus for every vector $(v, \alpha) \in S(B \cup \{p\})$ the secret is determined uniquely. Let us assume that the participants in B try to guess the secret testing all $\alpha \in S(p)$. Since $\mathbf{M}$ is an ideal scheme and for two different shares $\mathbf{M}(\tilde{r}, p)$ and $\mathbf{M}(\hat{r}, p)$ the participants in B get the same secret $\mathbf{M}(\tilde{r}, p_0) = \mathbf{M}(\hat{r}, p_0)$, there is at least one value of the secret which cannot be obtained in this way. This shows that B has some information on the secret, which implies that B is an authorized set, as $\mathbf{M}$ is a perfect scheme. This contradiction completes the proof. □

Let us recall the following lemma which can be used for lower bound of the number of rows of a secret sharing matrix.

Lemma 1 ([**2**], p.129, Lemma 4)**.** Let $\mathbf{M}$ be an ideal and perfect secret sharing scheme. If A is a minimal authorized set of participants, then $|S(A)| = q^{|A|}$.

The lemma combined with Theorem 3 implies the following corollary.

Corollary 1. If $\mathbf{M}$ is an ideal and perfect secret sharing scheme, then for every maximal unauthorized set $B \subseteq P$ and for every minimal authorized set $A \subseteq P$ we have $|A| \leq |B| + 1$.

PROOF. Let $\mathbf{M}$ be an ideal and perfect secret sharing scheme and let A and B be sets of participants described in the assumptions of the theorem. Since A is a minimal authorized set, from Lemma 1 we deduce that $\mathbf{M}$ has at least $q^{|A|}$ rows. On the other hand, according to Theorem 3 the number of rows in $\mathbf{M}$ does not exceed $q^{|B|+1}$. Hence $q^{|A|} \leq q^{|B|+1}$ which implies the claim. □

Lemma 2. Let $\mathbf{M}$ be an ideal and perfect secret sharing scheme. If $A \subseteq P^o$ is an independent set, then for every $v \in S^{|A|}$ there is a row r such that $\mathbf{M}(r, A) = v$.

PROOF. Let $\mathbf{M}$ be an ideal and perfect secret sharing scheme. We proceed by induction on $k = |A|$. For $k = 1$ the statement is true as the scheme is perfect. Let $A = \{p_1, \ldots, p_k\}$ be an independent set with $k \geq 2$. Let us note that $\bar{A} = A \setminus \{p_k\}$ is also independent. Consider $(\alpha_1, \ldots, \alpha_{k-1}, \alpha_k) \in S^k$. By the induction hypothesis there is a row $\bar{r}$ such that $\mathbf{M}(\bar{r}, \bar{A}) = (\alpha_1, \ldots, \alpha_{k-1})$. Since A is independent, the participants in $\bar{A}$ have no information about the share given to p_k, i.e., there is a row r such that $\mathbf{M}(r, \bar{A}) = \mathbf{M}(\bar{r}, \bar{A})$ and $\mathbf{M}(r, p_k) = \alpha_k$. This completes the proof. □

Let us recall that every minimal authorized set is independent, so the above lemma is a generalization of Lemma 1. The next theorem is strengthening of Corollary 1.

Theorem 4. Let $\mathbf{M}$ be an ideal and perfect secret sharing scheme. If $A \subseteq P$ is an independent set, then $|A| \leq |B| + 1$ for every maximal unauthorized set $B \subseteq P$. Moreover, if $A \subseteq P$ is unauthorized and independent, then $|A| \leq |B|$ for every maximal unauthorized set $B \subseteq P$.

PROOF. The proof of the first statement is similar to the proof of Corollary 1 - instead of Lemma 1 we use Lemma 2.

To prove the second statement, we deduce from Lemma 2 that $|S(A)| = q^{|A|}$. Since A is unauthorized, for every $v \in S(A)$ and for every $\alpha \in S(p_0)$ there exists a row r such that $\mathbf{M}(r, A) = v$ and $\mathbf{M}(r, p_0) = \alpha$. Hence $\mathbf{M}$ has at least $q^{|A|+1}$ rows. We now apply Theorem 3 to obtain $q^{|A|+1} \leq q^{|B|+1}$ which implies the claim. □

4 Secret sharing schemes and matroids

Before we present a connection between the secret sharing schemes and the matroids, we should recall one of many equivalent ways of defining matroids (see [**9**]).

A matroid $\mathbb{M}$ is an ordered pair $(E, \mathcal{I})$ consisting of a finite set E and $\mathcal{I} \subseteq 2^E$ satisfying the following conditions:

(1) $\emptyset \in \mathcal{I}$.
(2) If $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$.
(3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then there exists an element $e \in I_2 \setminus I_1$ such that $I_1 \cup \{e\} \in \mathcal{I}$.

The members of $\mathcal{I}$ are called the *independent* sets of $\mathbb{M}$. A subset of E that is not in $\mathcal{I}$ is called *dependent*. A maximal independent set in $\mathbb{M}$ is called a *base*. A minimal dependent set in $\mathbb{M}$ is called a *circuit*.

Lemma 3 ([**9**], p.17, Lemma 1.2.2)**.** If B_1 and B_2 are bases of a matroid $\mathbb{M}$, $x \in B_2 \setminus B_1$, then there exists $y \in B_1 \setminus B_2$, such that a set $(B_2 \setminus \{x\}) \cup \{y\}$ is also a base of $\mathbb{M}$.

Lemma 4 ([**9**], p.16, Lemma 1.2.1)**.** If B_1 and B_2 are bases of a matroid, then $|B_1| = |B_2|$.

The number of elements of an arbitrary base of a matroid $\mathbb{M}$ is called the *rank* of $\mathbb{M}$.

A relation between the secret sharing scheme and the matroids is described in the following theorem.

Theorem 5 ([**2**], p.126, Theorem 1)**.** If $\mathbf{M}$ is an ideal and perfect secret sharing scheme, then $\mathcal{D}(\mathbf{M})$ is a family of all dependent sets of a connected matroid.

Let us recall that the *connected matroid* is a matroid $(E, \mathcal{I})$ in which for any two different elements $x, y \in E$ there exists a circuit $\mathcal{C}$ such that $x, y \in \mathcal{C}$. The matroid determined by dependent sets of a secret sharing scheme $\mathbf{M}$ will be called the *matroid associated with the scheme* $\mathbf{M}$ and denoted by $\mathfrak{M}$. Obviously, $\mathfrak{M}$ is uniquely determined by $\mathbf{M}$.

5 Hierarchical Threshold Secret Sharing Schemes

For given positive integers $k < n$, a (k, n)-*threshold* secret sharing scheme is a scheme such that the set of participants P has n elements and the family $\Gamma = \{A \subseteq P : |A| \geq k\}$ is its access structure. There are many constructions of threshold secret sharing schemes. The most prominent one is the Shamir scheme [**4**] which is ideal and perfect. A finite field $\mathbb{F}_q$ (q is a power of a prime) is both the set of secrets and the sets of shares of the scheme.

The entries of the matrix $\mathbf{M}$ of a (k, n)-threshold Shamir scheme are elements of a finite field $\mathbb{F}_q$. The participants $p_0, p_1, \ldots, p_n$ are identified by different elements $x_0 = 0, x_1, \ldots, x_n \in \mathbb{F}_q$. The rows of the matrix are labelled by polynomials over $\mathbb{F}_q$ of degree less than k. For such a polynomial f the corresponding row of $\mathbf{M}$ equals $(f(0), f(x_1), \ldots, f(x_n))$. Obviously, $f(0)$ is a secret. Every set of at least k participants can pool their shares together and using the Lagrange interpolation finds a unique polynomial of degree less than k which identifies a suitable row of the matrix and consequently, they determine the secret.

Tassa [**1**] considers the problem of secret sharing among a group of participants with the hierarchical structure. In such a setting P is composed of levels:

$$P = P_1 \dot{\cup} \cdots \dot{\cup} P_l. \tag{13}$$

The access structure is constructed in such a way that if A is an authorized set, then any participant in $A \cap P_i$ can be replaced by a participant from P_j with $j \leq i$ and the resulting set remains authorized. For every level $i \in \{1, \ldots, l\}$ of the hierarchy a threshold k_i is defined. It is assumed that $0 < k_1 < \ldots < k_l$. A set $A \subseteq P$ is said to satisfy the *threshold property of level* i (which we abbreviate to TP_i) if $|A \cap \bigcup_{s=1}^{i} P_s| \geq k_i$. The notation $TP_i(A)$ denotes that A satisfies TP_i.

The access structures considered by Tassa are the following:

$$\Gamma_\wedge = \{A \subseteq P \colon \forall_{i \in \{1,2,\ldots,l\}} TP_i(A)\}, \tag{14}$$

$$\Gamma_\vee = \{A \subseteq P \colon \exists_{i \in \{1,2,\ldots,l\}} TP_i(A)\}. \tag{15}$$

The main results described in [**1**] are the constructions of ideal and perfect secret sharing schemes that realize $\Gamma_\wedge$ and $\Gamma_\vee$. Moreover, Tassa notices that the above access structures are two extreme members of a family $\{\Gamma_v \,:\, v = 1, \ldots, l\}$ of the hierarchical threshold access structures:

$$\Gamma_v = \{A \subseteq P \,:\, TP_i(A) \text{ for at least } v \text{ values of } i \in \{1, \ldots, l\}\}. \tag{16}$$

Indeed, $\Gamma_1 = \Gamma_\vee$ and $\Gamma_l = \Gamma_\wedge$. The open problem posed by Tassa is whether there exists an ideal and perfect secret sharing scheme realizing Γ_v for $v \in \{2, \ldots, l-1\}$. We shall show in Theorem 6 that in general the answer is negative.

For simplicity of notation, we define $\sigma(A) = (t_1, t_2, \ldots, t_l)$ with $t_i = |A \cap P_i|$.

Theorem 6. Let $0 = k_0 < k_1 < \ldots < k_l$ be a sequence of integers. Let $P = P_1 \dot\cup \ldots \dot\cup P_l$ be a hierarchical structure in a set of participants with $|P_i| \geq k_i - k_{i-1}$ for every $i = 1, \ldots l$. If $v \in \{2, \ldots, l-1\}$, $|P_{l-v+1}| \geq k_l$ and $|P_{l-v+2}| \geq k_l - k_1$ then the access structure Γ_v is not realized by any ideal and perfect secret sharing scheme.

Proof. Let us fix $v \in \{2, \ldots, l-1\}$ and suppose that there exists ideal and perfect secret sharing scheme $\mathbf{M}$ that realizes Γ_v.

We begin by proving that a rank of the associated matroid $\mathfrak{M}$ is at most k_l. Let us consider a set of participants $A \subseteq P$ such that $\sigma(A) = (t_1, t_2, \ldots, t_l)$, where

$$t_i = \begin{cases} k_1 & \text{for } i = 1; \\ k_i - k_{i-1} - 1 & \text{for } i = v; \\ k_i - k_{i-1} & \text{otherwise.} \end{cases} \tag{17}$$

We will show that A is the maximal unauthorized set of participants. If $1 < j \leq v - 1$ then

$$|A \cap (\bigcup_{i=1}^{j} P_i)| = \sum_{i=1}^{j} t_i = k_j. \tag{18}$$

If $v \leq j < l$ then

$$|A \cap (\bigcup_{i=1}^{j} P_i)| = \sum_{i=1}^{j} t_i = k_j - 1. \tag{19}$$

This shows that A does not satisfy TP_j for $j \geq v$, so A is unauthorized. However, adding an arbitrary participant $p \in P \setminus A$ to A makes it authorized as $A \cup \{p\}$ fulfils

TP_j for all $j \leq v-1$ and $j \geq i$ if $p \in P_i$. From the fact that $|A| = k_l - 1$ and Theory 4 we deduce that the rank of the associated matroid $\mathfrak{M}$ is at most k_l.

Our next goal is to show that a rank of the associated matroid $\mathfrak{M}$ is equal exactly k_l. We achieve it by indicating a minimal authorized set of participants with k_l elements. Let us consider a set $B_1 \subseteq P$ such that

$$\sigma(B_1) = (\underbrace{0, \ldots, 0}_{l-v}, k_l, 0, \ldots, 0). \tag{20}$$

It is easily seen that B_1 fulfils TP_i, for $i = l-v+1, l-v+2, \ldots, l$. Moreover, any proper subset of B_1, does not fulfil TP_l. This shows that B_1 is a minimal authorized set, so it is an independent set in the associated matroid $\mathfrak{M}$. Thus we get that the rank of $\mathfrak{M}$ is exactly k_l and B_1 is a base.

Next we consider a set B_2 such that

$$\sigma(B_2) = (k_1, \underbrace{0, \ldots, 0}_{l-v}, k_l - k_1, 0, \ldots, 0) \tag{21}$$

and show that B_2 is also a base in the associated matroid $\mathfrak{M}$. It is easy to check that it fulfils TP_i for $i = 1, l-v+2, \ldots, l$, i.e., exactly for v values of i. Additionally, the set $B_2 \setminus \{p\}$ does not fulfil TP_1 or TP_l accordingly to $p \in P_1 \cap B_2$ or $p \in P_{l-v+2} \cap B_2$.

Now we are in a position to apply Lemma 3. For $p \in B_2 \cap P_1$ there exists $p' \in B_1$ such that $B_3 = (B_2 \setminus \{p\}) \cup \{p'\}$ is a base and consequently B_3 is independent. It is easy to see that

$$\sigma(B_3) = (k_1 - 1, \underbrace{0, \ldots, 0}_{l-v-1}, 1, k_l - k_1, 0, \cdots, 0) \tag{22}$$

as $B_1 \subseteq P_{l-v+1}$. It is obvious that B_3 fulfils TP_i only for $i = l-v+2, \ldots, l$, which shows that B_3 is unauthorized. According to the second part of Theorem 4, we have $k_l = |B_3| \leq |A| = k_l - 1$. This contradiction finishes the proof. □

6 Conclusions

In Theorem 6 we have proved that in general the problem of Tassa has negative solution, but still in some cases not covered by Theorem 6, the problem whether Γ_v, $v \in \{2, \ldots, l-1\}$, is realized as the access structure of an ideal and perfect secret sharing scheme remains open.

The information rate of a secret sharing scheme is defined by

$$\rho := \min_{i \in \{1,\ldots,n\}} \frac{\log_2 |S|}{\log_2 |U_i|}, \tag{23}$$

where U_i is a set of all possible shares of participant p_i. If there does not exist an associated matroid of a secret sharing scheme, then the information rate of such a scheme is at most 2/3 (see **[10]**). The information rate of an access structure Γ is the supremum of the information rates of all secret sharing schemes realizing the access structure with a finite domain of shares. We do not know if Γ_v, $2 \leq v \leq l-1$,

can be realized by a secret sharing scheme for which an associated matroid exists. Summarising, the question is what is the actual information rate of Γ_v for $2 \leq v \leq l-1$.

References

[1] Tassa T., Hierarchical Threshold Secret Sharing, Journal of Cryptology 20 (2007): 237.
[2] Brickell E., Davenport D., On the Classification of Ideal Secret Sharing Schemes, Journal of Cryptology 4 (1991): 123.
[3] Blakley G. R., Safeguarding Cryptographic Keys, Proceedings of the National Computer Conference 48 (1979): 313.
[4] Shamir A., How to Share a Secret, Communications of the ACM 22 (1979): 612.
[5] Ito M., Saito A., Nishizeki T., Secret Sharing Scheme Realizing General Access Structure, Proceedings of the IEEE Global Telecommunications Conference (1987): 99.
[6] Benaloh J., Leichter J., Generalized Secret Sharing and Monotone Functions, Proceedings of the Annual International Cryptology Conference on Advances in Cryptology (1988): 27.
[7] Simmons G.J., How to (really) Share a Secret, Advances in Cryptology - CRYPTO 88 (1990): 390.
[8] Farràs O. Padró C., Ideal Hierarchical Secret Sharing Schemes, Theory of Cryptography 5978 (2010): 219.
[9] Oxley J. G., Matroid Theory, Oxford University Press, New York (1992).
[10] Martí-Farré J., Padró C., Secret Sharing Schemes on Sparse Homogeneous Access Structures with Rank Three, The electronic journal of combinatorics 11 (2004): 1.