Characterizing Ideal Weighted Threshold Secret Sharing

Amos Beimel[1], Tamir Tassa[1,2], and Enav Weinreb[1]

[1] Dept. of Computer Science, Ben-Gurion University, Beer Sheva, Israel.
[2] Division of Computer Science, The Open University, Ra'anana, Israel.

Abstract. Weighted threshold secret sharing was introduced by Shamir in his seminal work on secret sharing. In such settings, there is a set of users where each user is assigned a positive weight. A dealer wishes to distribute a secret among those users so that a subset of users may reconstruct the secret if and only if the sum of weights of its users exceeds a certain threshold. A secret sharing scheme is ideal if the size of the domain of shares of each user is the same as the size of the domain of possible secrets (this is the smallest possible size for the domain of shares). The family of subsets authorized to reconstruct the secret in a secret sharing scheme is called an access structure. An access structure is ideal if there exists an ideal secret sharing scheme that realizes it.
It is known that some weighted threshold access structures are not ideal, while other nontrivial weighted threshold access structures do have an ideal scheme that realizes them. In this work we characterize all weighted threshold access structures that are ideal. We show that a weighted threshold access structure is ideal if and only if it is a hierarchical threshold access structure (as introduced by Simmons), or a tripartite access structure (these structures, that we introduce here, generalize the concept of bipartite access structures due to Padró and Sáez), or a composition of two ideal weighted threshold access structures that are defined on smaller sets of users. We further show that in all those cases the weighted threshold access structure may be realized by a linear ideal secret sharing scheme. The proof of our characterization relies heavily on the strong connection between ideal secret sharing schemes and matroids, as proved by Brickell and Davenport.

1 Introduction

A *threshold secret sharing scheme* enables a dealer to distribute a secret among a set of users, by giving each user a piece of information called a *share*, such that only large sets of users will be able to reconstruct the secret from the shares that they got, while smaller sets gain no information on the secret. Threshold secret sharing schemes were introduced and efficiently implemented, independently, by Blakley [6] and Shamir [26]. Efficient threshold secret sharing schemes were used in many cryptographic applications, e.g., Byzantine agreement [24], secure multiparty computations [4, 11], and threshold cryptography [13].

In this paper we deal with *weighted* threshold secret sharing schemes. In these schemes, considered already by Shamir [26], the users are not of the same status.

That is, each user is assigned a positive weight and a set can reconstruct the secret if the sum of weights assigned to its users exceeds a certain threshold. As a motivation, consider sharing a secret among the shareholders of some company, each holding a different amount of shares. Such settings are closely related to the concept of *weighted threshold functions*, which play an important role in complexity theory and learning theory.

Ito, Saito, and Nishizeki [14] generalized the notion of secret sharing such that there is an arbitrary monotone collection of authorized sets, called the *access structure*. The requirements are that only sets in the access structure are allowed to reconstruct the secret, while sets that are not in the access structure should gain no information on the secret. A simple argument shows that in every secret sharing scheme, the domain of possible shares for each user is at least as large as the domain of possible secrets (see [17]). Shamir's threshold secret sharing scheme is *ideal* in the sense that the domain of shares of each user coincides with the domain of possible secrets. Ideal secret sharing schemes are the most space-efficient schemes. Some access structures do not have any ideal secret sharing schemes that realizes them [5]. Namely, some access structures demand share domains that are larger than the domain of secrets. Access structures that may be realized by an ideal secret sharing scheme are called ideal. Ideal secret sharing schemes and ideal access structures have been studied in, e.g., [1, 7, 8, 15, 18, 19, 21, 23, 25, 30, 33]. Ideal access structures are known to have certain combinatorial properties. In particular, there is a strong relation between ideal access structures and matroids [8].

While threshold access structures are ideal, weighted threshold access structures are not necessarily so. For example, the access structure on four users with weights 1, 1, 1, and 2, and a threshold of 3, has no ideal secret sharing scheme (see Example 1 for a proof). Namely, in any perfect secret sharing scheme that realizes this access structure, the share domain of at least one user is larger than the domain of secrets. On the other hand, there exist ideal weighted threshold access structures, other than the trivial threshold ones. For example, consider the access structure on nine users, where the weights are 16, 16, 17, 18, 19, 24 ,24 ,24, and 24 and the threshold is 92. Even though this access structure seems more complicated than the above access structure, it has an ideal secret sharing scheme (see the full version of this paper [2]). Another example of an ideal weighted threshold access structure is the one having weights 1, 1, 1, 1, 1, 3, 3, and 3 and threshold 6 (see Example 2).

We give a combinatorial characterization of ideal weighted threshold access structures. We show that a weighted threshold access structure is ideal if and only if it is a hierarchical threshold access structure (as introduced by Simmons [27]), or a tripartite access structure (these structures, that we introduce here, generalize the bipartite access structures of Padró and Sáez [23]), or a composition of two ideal weighted threshold access structures that are defined on smaller sets of users. We further show that in all those cases the weighted threshold access structure may be realized by a linear ideal secret sharing scheme. The present study generalizes the work of Morillo, Padró, Sáez, and Villar [21] who characterized the ideal weighted threshold access structures in which all the minimal

authorized sets have at most two users. The proof of our characterization relies heavily on the strong connection between ideal secret sharing schemes and matroids, as presented in [8]. We utilize results regarding the structure of matroids to understand and characterize the structure of ideal weighted threshold access structures. An important tool in our analysis is composition of ideal access structures, previously studied in, e.g., [1, 5, 9, 12, 20, 32].

Efficiency of Secret Sharing Schemes. Secret sharing schemes for general access structures were defined by Ito, Saito, and Nishizeki in [14]. More efficient schemes were presented in, e.g., [5, 7, 16, 29]. We refer the reader to [28, 31] for surveys on secret sharing. However, for most access structures the known secret sharing schemes are highly inefficient, that is, the size of the shares is exponential in n, the number of users. It is not known if better schemes exist. For weighted threshold access structures the situation is better. In a recent work [3], secret sharing schemes were constructed for arbitrary weighted threshold access structures in which the shares are of size $O(n^{\log n})$. Furthermore, under reasonable computational assumptions, a secret sharing scheme with computational security was constructed in [3] for every weighted threshold access structure with a polynomial share size.

Organization. We begin in Section 2 by supplying the necessary definitions. Then, in Section 3, we state our characterization theorem and outline its proof. We proceed to describe in Section 4 the connection between matroids and ideal secret sharing, and then prove, in Section 5, several properties of matroids that are associated with weighted-threshold access structures. Thereafter, we discuss the connection between ideal weighted threshold access structures and two families of access structures: hierarchical threshold access structures in Section 6, and tripartite access structures in Section 7. Finally, in Section 8 we complete the proof of the characterization theorem by proving that if an ideal weighted threshold access structure is not hierarchical nor tripartite then it is a composition of two access structures on smaller sets of users. For lack of space, some proofs are omitted. All proofs may be found in the full version of the paper [2].

2 Definitions and Notations

Definition 1 (Access Structure). *Let $U = \{u_1, \ldots, u_n\}$ be a set of users. A collection $\Gamma \subseteq 2^U$ is* monotone *if $B \in \Gamma$ and $B \subseteq C$ imply that $C \in \Gamma$. An* access structure *is a monotone collection $\Gamma \subseteq 2^U$ of non-empty subsets of U. Sets in Γ are called* authorized*, and sets not in Γ are called* unauthorized*. A set B is called a* minterm *of Γ if $B \in \Gamma$, and for every $C \subsetneq B$, the set C is unauthorized. A user u is called* self-sufficient *if $\{u\} \in \Gamma$. A user is called* redundant *if there is no minterm that contains it. An access structure is called* connected *if it has no redundant users.*

Definition 2 (Secret-Sharing Scheme). *Let S be a finite set of secrets, where $|S| \geq 2$. An n-user* secret-sharing scheme *Π with* domain of secrets *S is a*

randomized mapping from S to a set of n-tuples $\prod_{i=1}^{n} S_i$, where S_i is called the share-domain *of u_i. A dealer shares a secret $s \in S$ among the n users of some set U according to Π by first sampling a vector of* shares *$\Pi(s) = (s_1, \ldots, s_n) \in \prod_{i=1}^{n} S_i$, and then privately communicating each share s_i to the user u_i. We say that Π* realizes *an access structure $\Gamma \subseteq 2^U$ if the following requirements hold:*

CORRECTNESS. *The secret s can be reconstructed by any authorized set of users. That is, for any set $B \in \Gamma$ (where $B = \{u_{i_1}, \ldots, u_{i_{|B|}}\}$), there exists a* reconstruction function $\text{RECON}_B : S_{i_1} \times \ldots \times S_{i_{|B|}} \rightarrow S$ *such that for every $s \in S$ and for every possible value of $\Pi_B(s)$, the restriction of $\Pi(s)$ to its B-entries, $\text{RECON}_B(\Pi_B(s)) = s$.*

PRIVACY. *Every unauthorized set can learn nothing about the secret (in the information theoretic sense) from their shares. Formally, for any set $C \notin \Gamma$, for every two secrets $a, b \in S$, and for every possible $|C|$-tuple of shares $\langle s_i \rangle_{u_i \in C}$,*

$$\Pr[\, \Pi_C(a) = \langle s_i \rangle_{u_i \in C} \,] = \Pr[\, \Pi_C(b) = \langle s_i \rangle_{u_i \in C} \,].$$

In every secret-sharing scheme, the size of the domain of shares of each user is at least the size of the domain of the secrets [17], namely $|S_i| \geq |S|$ for all $i \in [n]$. This motivates the next definition.

Definition 3 (Ideal Access Structure). *A secret-sharing scheme with domain of secrets S is* ideal *if the domain of shares of each user is S. An access structure Γ is* ideal *if for some finite domain of secrets S there exists an ideal secret sharing scheme realizing it.*

Most previously known secret sharing schemes are *linear*. The concept of linear secret sharing schemes was introduced by Brickell [7] in the ideal setting and was latter generalized to non-ideal schemes. Linear schemes are equivalent to monotone span programs [16]. In an ideal linear secret sharing scheme, the secret is an element of a finite field, and each share is a linear combination of the secret and some additional random field elements.

In this paper we concentrate on special access structures, so-called weighted threshold access structures, that were already introduced in [26].

Definition 4 (Weighted Threshold Access Structure – WTAS). *Let $w : U \rightarrow \mathbb{N}$ be a weight function on U and $T \in \mathbb{N}$ be a threshold. Define $w(A) := \sum_{u \in A} w(u)$ and $\Gamma = \{A \subseteq U : w(A) \geq T\}$. Then Γ is called a* weighted threshold access structure (WTAS) *on U.*

Terminology and notations. Throughout this paper we assume that the users are ordered in a nondecreasing order according to their weights, i.e., $w(u_1) \leq w(u_2) \leq \cdots \leq w(u_n)$. Let $A = \{u_{i_j}\}_{1 \leq j \leq k}$ be an ordered subset of U, where $1 \leq i_1 < \cdots < i_k \leq n$. In order to avoid two-levelled indices, we will denote the users in such a subset with the corresponding lower-case letter, namely, $A = \{a_j\}_{1 \leq j \leq k}$. We denote the first (lightest) and last (heaviest) users of A by

$A_{\min} = a_1$ and $A_{\max} = a_k$ respectively. For an arbitrary ordered subset A we let $A_{s,t} = \{a_j\}_{s \le j \le t}$ denote a run-subset. If $s > t$ then $A_{s,t} = \emptyset$. Two types of runs that we shall meet frequently are prefixes and suffixes. A prefix of a subset A is a run-subset of the form $A_{1,\ell}$, while a suffix takes the form $A_{\ell,k}$, $1 \le \ell \le k$. A suffix $A_{\ell,k}$ is a proper suffix of $A_{1,k}$ if $\ell > 1$. We conclude this section by introducing the precedence relation $\prec$. When applied to users, $u_i \prec u_j$ indicates that $i < j$ (and, in particular, $w(u_i) \le w(u_j)$). This relation induces a lexicographic order on subsets of U in the natural way.

3 Characterizing Ideal WTASs

The main result of this paper is a combinatorial characterization of ideal WTASs. We define in Definitions 5–7 the building blocks that play an essential role in this characterization. Using these definitions, we state Theorem 1, our main result, that characterizes ideal WTASs. We also outline the proof of that theorem, where the full proof is given in the subsequent sections.

3.1 Building Blocks

Definition 5 (Hierarchical Threshold Access Structure – HTAS). *Let m be an integer, $U = \bigcup_{i=1}^{m} L_i$ be a partition of the set of users into a hierarchy of m disjoint levels, and $\{k_i\}_{1 \le i \le m}$ be a sequence of decreasing thresholds, $k_1 > k_2 > \cdots > k_m$. These hierarchy and sequence of thresholds induce a* hierarchical threshold access structure (HTAS) on U*:*

$$\Gamma_H = \left\{ A \subseteq U : \textit{There exists } i \in [m] \textit{ such that } \left| A \cap \cup_{j=i}^{m} L_j \right| \ge k_i \right\}.$$

That is, a set $A \subseteq U$ is in Γ_H if and only if it contains at least k_i users from the ith level and above, for some $i \in [m]$. The family of HTASs was introduced by Simmons in [27] and further studied by Brickell who proved their ideality [7]. An explicit ideal scheme for these access structures was constructed in [33].

Remark 1. Without loss of generality, we assume that

$$|L_i| > k_i - k_{i+1} \text{ for every } i \in [m-1], \text{ and } |L_m| \ge k_m.$$

Indeed, if $|L_i| \le k_i - k_{i+1}$ for some $i \in [m-1]$, then the ith threshold condition in the HTAS definition implies the $(i+1)$th threshold condition and, consequently, the ith condition is redundant.

Definition 6 (Tripartite Access Structure – TPAS). *Let U be a set of n users, such that $U = A \cup B \cup C$, where A, B, and C are disjoint, and A and C are nonempty. Let m, d, t be positive integers such that $m > t$. Then the following is a* tripartite access structure (TPAS) *on U:*

$$\Delta_1 = \{ X \subseteq U : (|X| \ge m \textit{ and } |X \cap (B \cup C)| \ge m - d) \textit{ or } |X \cap C| \ge t \},$$

Namely, a set X is in Δ_1 if either it has at least m users, $(m-d)$ of which are from $B \cup C$, or it has at least t users from C. If $|B| \leq d+t-m$, then the following is also a tripartite access structure:

$$\Delta_2 = \{X \subseteq U : (|X| \geq m \text{ and } |X \cap C| \geq m-d) \text{ or } |X \cap (B \cup C)| \geq t\}.$$

That is, $X \in \Delta_2$ if either it has at least m users, $(m-d)$ of which are from C, or it has at least t users from $B \cup C$.

TPASs, introduced herein, generalize the concept of bipartite access structure that was presented in [23]. We show that TPASs are ideal by constructing a linear ideal secret sharing scheme that realizes them. Our scheme is a generalization of a scheme from [23] for bipartite access structures.

Definition 7 (Composition of Access Structures). *Let U_1 and U_2 be disjoint sets of users and let Γ_1 and Γ_2 be access structures over U_1 and U_2 respectively. Let $u_1 \in U_1$, and set $U = U_1 \cup U_2 \setminus \{u_1\}$. Then the* composition *of Γ_1 and Γ_2 via u_1 is*

$$\Gamma = \{X \subseteq U : X \cap U_1 \in \Gamma_1 \text{ or } (X \cap U_2 \in \Gamma_2 \text{ and } (X \cap U_1) \cup \{u_1\} \in \Gamma_1)\}.$$

3.2 The Characterization

Recall that the set U is viewed as a sequence which is ordered in a monotonic non-decreasing order according to the weights. Let M be the lexicographically minimal minterm of Γ (that is, $M \in \Gamma$ is a minterm and $M \prec M'$ for all other minterms $M' \in \Gamma$). It turns out that the form of M plays a significant role in the characterization of Γ.

If M is a prefix of U, namely $M = U_{1,k}$ for some $k \in [n]$, then, as we prove in Section 6.1, the access structure is a HTAS of at most three levels. If M is a lacunary prefix, in the sense that $M = U_{1,k} \setminus \{u_\ell\}$ for $1 \leq \ell < k \leq n$, then, as we discuss in Section 7, the access structure is a TPAS. Otherwise, if M is neither a prefix nor a lacunary prefix, the access structure is a composition of two weighted threshold access structures over smaller sets. More specifically, we identify a prefix $U_{1,k}$, where $1 < k < n$, that could be replaced by a single substitute user u, and then show that Γ is a composition of a WTAS on $U_{1,k}$ and another WTAS on $U_{k+1,n} \cup \{u\}$. Since Γ is ideal, so are the two smaller WTASs, as implied by Lemma 13. Hence, this result, which we prove in Section 8, completes the characterization of ideal WTASs in a recursive manner. Our main result in this paper is as follows.

Theorem 1 (Characterization Theorem). *Let U be a set of users, w be a weight function, T be a threshold, and Γ be the corresponding WTAS. Then Γ is ideal if and only if one of the following three conditions holds:*

- *The access structure Γ is a HTAS.*
- *The access structure Γ is a TPAS.*
- *The access structure Γ is a composition of Γ_1 and Γ_2, where Γ_1 and Γ_2 are ideal WTASs defined over sets of users smaller than U.*

In particular, if Γ is an ideal WTAS then there exists a linear ideal secret sharing scheme that realizes it.

4 Matroids and Ideal Secret Sharing Schemes

Ideal secret sharing schemes and matroids are strongly related [8]. If an access structure is ideal, there is a matroid that reflects its structure. On the other hand, every matroid that is representable over some finite field is the reflection of some ideal access structure. In this section we review some basic results from the theory of matroids and describe their relation to ideal secret sharing schemes. For more background on matroid theory the reader is referred to [22].

Matroids are a combinatorial structure that generalizes both linear spaces and the set of circuits in an undirected graph. They are a useful tool in several fields of theoretical computer science, e.g., optimization algorithms. A matroid $\mathcal{M} = \langle V, \mathcal{I} \rangle$ is a finite set V and a collection $\mathcal{I}$ of subsets of V that satisfy the following three axioms: **(I1)** $\emptyset \in \mathcal{I}$. **(I2)** If $X \in \mathcal{I}$ and $Y \subseteq X$ then $Y \in \mathcal{I}$. **(I3)** If X and Y are members of $\mathcal{I}$ with $|X| = |Y| + 1$ then there exists an element $x \in X \backslash Y$ such that $Y \cup \{x\} \in \mathcal{I}$. The elements of V are called the *points* of the matroid and the sets in $\mathcal{I}$ are called the *independent* sets of the matroid. A *dependent set* of the matroid is any subset of V that is not independent. The minimal dependent sets are called *circuits*. A matroid is said to be *connected* if for any two points there exists a circuit that contains both of them.

We now discuss the relations between ideal secret sharing schemes and matroids. Let Γ be an access structure over a set of users $U = \{u_1, \ldots, u_n\}$. If Γ is ideal, then, by the results of [8, 19], there exists a matroid $\mathcal{M}$ corresponding to Γ. The points of $\mathcal{M}$ are the users in U together with an additional point, denoted u_0, that could be thought of as representing the dealer. We denote hereinafter by $\mathcal{C}_0 = \{X \cup \{u_0\} : X \text{ is a minterm of } \Gamma\}$ the set of all Γ-minterms, supplemented by u_0.

Theorem 2 ([8, 19]). *Let Γ be a connected ideal access structure. Then there exists a connected matroid $\mathcal{M}$ such that $\mathcal{C}_0$ is exactly the set of circuits of $\mathcal{M}$ containing u_0.*

The next result implies the uniqueness of the matroid $\mathcal{M}$ that corresponds to a given connected ideal access structure, as discussed in Theorem 2, and it provides means to identify *all* the circuits of that matroid.

Lemma 1 ([22, Theorem 4.3.2]). *Let e be an element of a connected matroid $\mathcal{M}$ and let $\mathcal{C}_e$ be the set of circuits of $\mathcal{M}$ that contain e. Then* all *of the circuits of $\mathcal{M}$ that do not contain e are the* minimal *sets of the form $(C_1 \cup C_2) \backslash \bigcap \{C_3 : C_3 \in \mathcal{C}_e, C_3 \subseteq C_1 \cup C_2\}$ where C_1 and C_2 are distinct circuits in $\mathcal{C}_e$.*

The unique matroid whose existence and uniqueness are guaranteed by Theorem 2 and Lemma 1 is referred to as *the matroid corresponding to Γ*. The next definition will enable us to explicitly define the matroid corresponding to Γ using the authorized sets in Γ.

Definition 8 (Critical User). *Let M_1 and M_2 be distinct minterms of Γ. A user $x \in M_1 \cup M_2$ is* critical *for $M_1 \cup M_2$ if the set $M_1 \cup M_2 \backslash \{x\}$ is unauthorized.*

In addition, we define

$$D(M_1, M_2) = (M_1 \cup M_2) \setminus \{x \in M_1 \cup M_2 : x \text{ is critical for } M_1 \cup M_2\}.$$

Corollary 1. *Let M_1 and M_2 be two distinct minterms of Γ. Then $D(M_1, M_2)$ is a dependent set of $\mathcal{M}$.*

Note that $D(M_1, M_2)$ is a dependent set of $\mathcal{M}$, but is not necessarily a circuit of $\mathcal{M}$.

Lemma 2 ([22, Lemma 1.1.3]). *Let C_1 and C_2 be two distinct circuits in a matroid and $e \in C_1 \cap C_2$. Then there exists a circuit $C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$.*

Finally, the next lemma is applicable when adding an element to an independent set results in a dependent set.

Lemma 3. *Let I be an independent set in a matroid $\mathcal{M}$ and let e be an element of $\mathcal{M}$ such that $I \cup \{e\}$ is dependent. Then $\mathcal{M}$ has a* unique *circuit contained in $I \cup \{e\}$ and that circuit contains e.*

Example 1. This example shows how to use the above statements in order to demonstrate that a given access structure is not ideal. Consider the WTAS Γ on the set $U = \{u_1, u_2, u_3, u_4\}$ with weights $w(u_1) = w(u_2) = w(u_3) = 1$ and $w(u_4) = 2$ and threshold $T = 3$. The minterms of Γ are $\{u_1, u_2, u_3\}$, $\{u_1, u_4\}$, $\{u_2, u_4\}$, and $\{u_3, u_4\}$. It follows from Benaloh and Leichter [5] that this access structure is not ideal.[3] Assume that it is ideal and consider the minterms $M_1 = \{u_1, u_4\}$ and $M_2 = \{u_2, u_4\}$. The set $\{u_1, u_2\}$ is unauthorized and thus u_4 is critical for $M_1 \cup M_2$. On the other hand, the users u_1 and u_2 are not critical for $M_1 \cup M_2$. Therefore, by Corollary 1, the set $D(M_1, M_2) = \{u_1, u_2\}$ is a dependent set of $\mathcal{M}$, the matroid corresponding to Γ. However, the set $\{u_1, u_2, u_3\}$ is a minterm of Γ and, consequently, it is independent in $\mathcal{M}$. Since $\{u_1, u_2\} \subset \{u_1, u_2, u_3\}$, we arrive at the absurd conclusion that a dependent set is contained in an independent set.

Definition 9 (Restriction). *Let $Y, X \subseteq U$ be two disjoint subsets of users. The* restriction *of Γ that is induced by Y on X is defined as the following access structure: $\Gamma_{Y,X} = \{Z \subseteq X : Z \cup Y \in \Gamma\}$.*

In other words, $\Gamma_{Y,X}$ consists of all subsets of X that complete Y to an authorized set in Γ. Since $\Gamma_{Y,X}$ is defined over a smaller set of users, restrictions can be helpful in recursively characterizing the structure of Γ. The following known result assures us that if Γ is ideal, $\Gamma_{Y,X}$ is ideal as well.

Lemma 4. *Let Γ be an access structure over a set of users U. Let $Y, X \subseteq U$ be sets such that $Y \notin \Gamma$ and $X \cap Y = \emptyset$. If Γ is ideal, then $\Gamma_{Y,X}$ is ideal. Furthermore, if Y is independent in the matroid corresponding to Γ and if a set $I \subseteq X$ is independent in the matroid corresponding to $\Gamma_{Y,X}$, then I is independent in the matroid corresponding to Γ.*

[3] In [10] it was shown that if the domain of secrets is S, the size of the domain of shares of at least one user in that access structure must be at least $|S|^{1.5}$. That result improved upon previous bounds that were derived in [9].

Lemma 5. *Let $X, Y \in U$ such that $X \cap Y = \emptyset$. If Γ is a WTAS, then $\Gamma_{Y,X}$ is a WTAS.*

5 WTASs and Matroids

In this section we prove several properties of matroids that are associated with ideal WTASs. These properties will serve us later in characterizing ideal WTASs. Let Γ be an ideal WTAS on $U = \{u_1, \ldots, u_n\}$ corresponding to a weight function $w : U \to \mathbb{N}$ and a threshold T. Let $\mathcal{M}$ be the matroid corresponding to Γ.

Lemma 6. *If $X = \{x_1, \ldots, x_k\} \in \Gamma$, it contains a suffix minterm, namely, there exists $i \in [k]$ such that $X_{i,k} = \{x_i, \ldots, x_k\}$ is a minterm.*

Lemma 7. *Let M be a minterm of Γ. Let $y \in U \backslash M$ be a user such that $w(M_{\min}) \leq w(y)$. Then $M \cup \{y\}$ is a dependent set of $\mathcal{M}$.*

Proof. Let $X = (M \backslash \{M_{\min}\}) \cup \{y\}$ be the set that is obtained by replacing the minimal user in M with y. Since $w(X) \geq w(M)$, the set X is authorized and, thus, it contains a minterm M'. Moreover, $M \neq M'$ since $M_{\min} \in M \setminus M'$. Therefore, by Corollary 1, the set $M \cup M' = M \cup \{y\}$ is dependent in $\mathcal{M}$. □

We show in the next lemma that whenever two minterms have the same minimal member they must be of the same size.

Lemma 8. *Let X and Y be minterms of the access structure Γ such that $X_{\min} = Y_{\min}$. Then $|X| = |Y|$.*

Proof. As X and Y are minterms, they are independent sets of the matroid $\mathcal{M}$. Assume, w.l.o.g., that $|X| < |Y|$. Then, by Axiom **(I3)** of the matroid definition, there exists $y \in Y \backslash X$ such that the set $X \cup \{y\}$ is independent. However, as $X_{\min} = Y_{\min}$ is a user with the minimal weight in both X and Y, we have that $w(X_{\min}) \leq w(y)$. Consequently, in view of Lemma 7, the set $X \cup \{y\}$ is dependent. This contradiction implies that $|X| = |Y|$. □

It turns out that the lexicographic order on the minterms of Γ, with respect to the relation $\prec$, is strongly related to dependence in $\mathcal{M}$. This is demonstrated through the following definition and lemmas.

Definition 10 (Canonical Complement). *Let P be a prefix of some minterm of Γ. Let $Y \subseteq U$ be the lexicographically minimal set such that: (1) $P_{\max} \prec Y_{\min}$, and (2) The set $P \cup Y$ is a minterm of Γ. Then the set Y is called the* canonical complement *of P.*

The following lemma shows that replacing the canonical complement by a user that precedes the first user of the canonical complement results in a dependent set.

Lemma 9. *Let P be a prefix of some minterm of Γ. Let $Y = \{y_1, \ldots, y_t\}$ be the canonical complement of P, and b be a user such $P_{\max} \prec b \prec y_1$. Then $P \cup \{b\}$ is dependent. Furthermore, the set $P \cup \{b\}$ includes a unique circuit that contains b.*

Proof. If $P = \emptyset$, then, since Γ is connected, there exists a minterm that starts with u_1, whence $y_1 = u_1$. Therefore, it cannot be that $b \prec y_1$ and thus the claim is trivially true. Otherwise, if $P \neq \emptyset$, denote by M_1 the minterm $M_1 = P \cup Y$. Let $X_2 = (M_1 \setminus \{P_{\max}\}) \cup \{b\}$ be the set resulting from replacing $P_{\max}$ with b in M_1. Since $w(P_{\max}) \leq w(b)$, the set X_2 is authorized (though not necessarily a minterm). Let M_2 be the suffix minterm contained in X_2 (such a minterm exists in view of Lemma 6). It must be that $b \in M_2$, since otherwise $M_2 \subseteq Y$, where Y is a proper subset of a minterm and thus is unauthorized.

Let $A = M_1 \cup M_2 = P \cup \{b\} \cup Y$. We proceed to show that every user in Y is critical for A. This will show that $D(M_1, M_2) \subseteq (M_1 \cup M_2) \setminus Y = P \cup \{b\}$. By Corollary 1, the set $D(M_1, M_2)$ is dependent, thus, this will imply that also $P \cup \{b\}$ is dependent. We also observe that it suffices to show that $Y_{\min} = y_1$ is critical for A; this will imply that also all other members of Y, having weight that is no smaller than $w(y_1)$, are also critical for A.

In view of the above, we show that y_1 is critical for A. Suppose this is not the case, namely, the set $A \setminus \{y_1\}$ is authorized. Since $A \setminus \{y_1\}$ results from M_1 by replacing y_1 by b where $w(b) \leq w(y_1)$, and since M_1 is a minterm, it must be that $A \setminus \{y_1\}$ is also a minterm. But this is a contradiction to the choice of y_1 as the first user in the canonical complement of P. Hence, all the elements of Y are critical for A, and, consequently, $P \cup \{b\}$ is dependent. Since P is part of a minterm, it must be that P is independent. Thus, by Lemma 3, the set $P \cup \{b\}$ must contain a unique circuit that contains b. □

The next lemma is a generalization of Lemma 9. Its proof, as well as the other missing proofs in this paper, can be found in the full version of this paper [2].

Lemma 10. *Let P be a prefix of some minterm of Γ. Let $Y = \{y_1, \ldots, y_t\}$ be the canonical complement of P, and $B = \{b_1, \ldots, b_j\}$ be a set such that $P_{\max} \prec B_{\min}$ and $b_j \prec y_j$. Then, the set $P \cup B$ is dependent.*

6 WTASs and HTASs

In this section we discuss the family of hierarchical threshold access structures (HTASs), from Definition 5, and their relation to WTASs. We show that if an ideal WTAS Γ has a minterm in the form of a prefix of U, then Γ is an HTAS.

When discussing a HTAS over some set $U = \{u_1, \ldots, u_n\}$, we shall assume that the users in U are ordered according to their position in the hierarchy, from the lowest level to the highest. Namely, that

$$L_i = U_{\ell_i, \ell_{i+1}-1} = \{u_{\ell_i}, \ldots, u_{\ell_{i+1}-1}\} \quad \forall i \in [m] \tag{1}$$

for some sequence $\ell_1 = 1 < \ell_2 < \cdots < \ell_m < \ell_{m+1} = n + 1$. Given a nonempty subset $A \subseteq U$, if $A_{\min} \in L_i$, then A is said to be of level i and it is denoted

by $L(A) = i$. Since any HTAS Γ_H is ideal [7, 33], Theorem 2 implies that there exists a matroid $\mathcal{M}$ that is associated with it.

Lemma 11. *Let Γ_H and $\mathcal{M}$ be an HTAS and its associated matroid. Then U_{1,k_1+1} is a circuit of $\mathcal{M}$.*

Let U be a set of users and let Γ be a monotone access structure over U that is both a WTAS and a HTAS. Namely, on one hand, there exist a weight function $w : U \to \mathbb{N}$ and a threshold $T \in \mathbb{N}$ such that Γ is the corresponding WTAS, and, on the other hand, there exists a hierarchy in U, where $U = \bigcup_{i=1}^{m} L_i$, and thresholds $k_1 > k_2 > \cdots > k_m$ such that Γ is also the corresponding HTAS.

Lemma 12. *Let Γ be both a WTAS and an HTAS. Then the HTAS-parameters of Γ satisfy one of the following conditions: (1) $m = 1$. (2) $m = 2$ and $k_1 = k_2 + 1$. (3) $m = 2$ and $|L_1| = k_1 - k_2 + 1$. (4) $m \in \{2, 3\}$, the level L_m is trivial, and the restriction of Γ_H to the first $m - 1$ levels is of the form that is described in cases (1)-(3).*

By constructing the appropriate weight function and threshold in each case, it can be shown that any HTAS with parameters as described in Lemma 12 is also a WTAS.

6.1 Ideal WTASs with a Prefix Minterm are HTASs

In this section we make the first step towards proving Theorem 1. Let Γ be an ideal WTAS over a set U of n users, corresponding to a weight function $w : U \to \mathbb{N}$ and a threshold T. Assume that U possesses a prefix minterm $U_{1,k}$ for some $k \in [n]$ (namely, there exists $k \in [n]$ such that the k users of smallest weights form a minterm). We claim that Γ is an HTAS. We first describe the partition of U into levels and determine the corresponding thresholds. Denoting the resulting HTAS by Γ_H, we proceed to prove that $\Gamma = \Gamma_H$.

The decomposition of U to levels will respect the order of users according to their weights. Namely, each level will be a run of U and our goal is to determine the transition points between one level and the subsequent one. Since $U_{1,k}$ is a minterm, $U_{1,i}$ is authorized for every $i \in \{k, \ldots, n\}$. By Lemma 6, for every such i there exists a run-minterm ending at u_i. Let us denote the length of that run-minterm by μ_i. By the non-decreasing monotonicity of the weights, we infer that the sequence of lengths $\boldsymbol{\mu} = (\mu_i)_{k \le i \le n}$ is monotonically non-increasing. Denote by m the number of distinct values assumed by the sequence $\boldsymbol{\mu}$, and let us denote those values by $k_1 > \cdots > k_m$. Then the HTAS Γ_H is defined as follows: m is the number of levels and k_i is the ith threshold. As for the levels, we denote by ℓ_i, where $i \in [m]$, the index of the first user in the first run-minterm of length k_i (e.g., $\ell_1 = 1$ since $U_{1,k}$ is the first run-minterm of length $k = k_1$ and its first user is u_1); then the ith level in the hierarchy is $L_i = U_{\ell_i, \ell_{i+1}-1}$, where $\ell_{m+1} = n + 1$.

We denote by U_{s_i,t_i} the right-most run-minterm whose length is k_i, where $i \in [m]$, and consider the set $A_i = U_{s_i+1,\ell_{i+1}-1}$. As U_{s_i,t_i} is the last minterm that contains k_i users and U_{ℓ_{i+1},t_i+1} is the first minterm that contains k_{i+1} users, the

set A_i consists of the last $k_i - k_{i+1}$ users in L_i (where $k_{m+1} = 1$). An important observation is that given $i \in [m]$ and $u_h \in A_i$, there is no run-minterm of the WTAS Γ that starts with u_h; indeed, if $U_{h,j}$ was a run-minterm then it would be a proper subset of the minterm U_{s_i,t_i} if $j \leq t_i$, or a proper superset of the minterm U_{ℓ_{i+1},t_i+1} if $j \geq t_i + 1$. An illustration of the construction of the levels of the HTAS appears in Fig. 1. Next, we prove that the WTAS Γ coincides with the HTAS Γ_H described above.

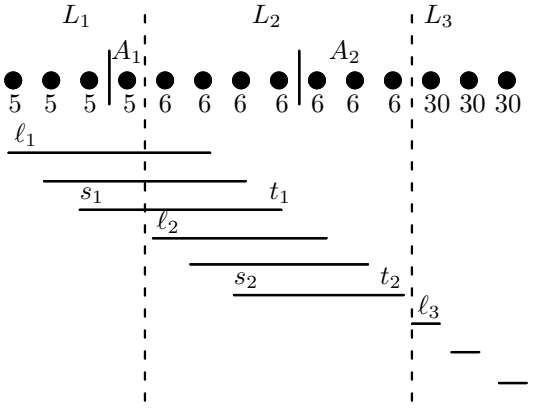

Fig. 1. A WTAS that is also an HTAS. The example is of a WTAS with 14 users of weights $5, 5, 5, 5, 6, 6, 6, 6, 6, 6, 6, 30, 30, 30$ and threshold $T = 30$. The vertical dashed lines indicate the three levels in the corresponding HTAS (the third one being a trivial one) and the horizontal lines indicate all of the run-minterms in that access structure.

Theorem 3. *Let Γ be an ideal WTAS over U that has a prefix minterm. Then Γ is an HTAS.*

Proof. Let Γ_H be the HTAS as described above. We will prove that $\Gamma = \Gamma_H$, thus showing that Γ is an HTAS. We start with proving that $\Gamma_H \subseteq \Gamma$. Let $X \in \Gamma_H$. Then for some $i \in [m]$ the set X has at least k_i users from $\bigcup_{j=i}^{m} L_j$. Letting $B_i = U_{\ell_i,\ell_i+k_i-1}$ denote the set of the first k_i users from $\bigcup_{j=i}^{m} L_j$, the non-decreasing monotonicity of the weights implies that $w(X) \geq w(B_i)$. By the construction of levels in Γ_H, the set B_i is a minterm of Γ, whence $w(B_i) \geq T$. Therefore, $w(X) \geq T$ and, consequently, $X \in \Gamma$.

Conversely, assume that $X \notin \Gamma_H$. Then X has at most $k_i - 1$ users from $\bigcup_{j=i}^{m} L_j$, for every $i \in [m]$. Consider the set $A = \bigcup_{i=1}^{m} A_i$. By the definition of A, it has exactly $k_i - 1$ users from $\bigcup_{j=i}^{m} L_j$, for every $i \in [m]$. Moreover, A is the set with the maximal weight among the sets that are unauthorized in the HTAS and thus $w(X) \leq w(A)$. Therefore, it suffices to show that $A \notin \Gamma$ in order to conclude that $X \notin \Gamma$ and, thus, complete the proof.

To this end, assume that $A \in \Gamma$. Then A contains some minterm $M \in \Gamma$. Assume that M is of level i, $L(M) = i$, namely, i is the lowest level for which $M \cap L_i \neq \emptyset$. Then $M \cap A_i$ is a prefix of M. In order to arrive at a contradiction,

we proceed to show that there can be no minterm that has a prefix which is a non-empty subset of A_i.

Assume, by contradiction, that there are such minterms, and let M' be the lexicographically minimal minterm of that sort. Let $u_h = M'_{\min}$ and let j be the maximal index such that $M' = U_{h,j} \cup Z$ for some $Z \subset U$. Since $u_h \in A_i$ and we observed earlier that no run-minterm starts in A_i, we conclude that $Z \neq \emptyset$ (and $u_{j+1} \prec Z_{\min}$ because of the maximality of j). We claim that $j < t_i$. Indeed, if $j \geq t_i$, then M' is a proper superset of $\hat{M} = U_{\ell_{i+1},t_i} \cup \{Z_{\min}\}$. Since $w(\hat{M}) \geq w(U_{\ell_{i+1},t_i+1}) \geq T$, we get a contradiction since a minterm M' cannot be a proper superset of an authorized set $\hat{M}$.

Next, define $Q = M' \cup \{u_{j+1}\} \setminus \{u_j\}$. The set Q is authorized and, by Lemma 6, it contains a suffix minterm M'' that must contain u_{j+1}, for otherwise it would be a proper subset of M'. Therefore, $M' \cup M'' = M' \cup \{u_{j+1}\} = U_{h,j} \cup \{u_{j+1}\} \cup Z$. We claim that all members of Z are critical for this union. Assume, by contradiction, that $M^* = M' \cup \{u_{j+1}\} \setminus \{z\}$ is authorized, for some $z \in Z$. Since $w(u_{j+1}) \leq w(z)$ and M' was a minterm, also M^* is a minterm. But M^* is a minterm that starts within A_i and $M^* \prec M'$, thus contradicting our choice of M'. Hence, by Corollary 1, the set $U_{h,j+1}$ is dependent in $\mathcal{M}$. However, since $s_i < h$ and $j + 1 \leq t_i$, this dependent set is properly contained in the minterm U_{s_i,t_i}, leading to a contradiction. Hence, $A \notin \Gamma$. □

7 Ideal WTASs and TPASs

In the previous section we dealt with the case where the lexicographically minimal minterm of Γ is a prefix of U. Here, we handle the case where the lexicographically minimal minterm of Γ is a lacunary prefix, namely, it takes the form $M = U_{1,d} \cup U_{d+2,k}$ for some $1 \leq d \leq k-2$ and $k \leq n$. We assume that there is at least one minterm starting with the user u_2, and that there are no self-sufficient users. If this is not the case, then Γ is a simple composition of access structures as shown in Lemma 14. We show that under these conditions, Γ is a tripartite access structure, as defined in Definition 6. The idea of the proof is as follows: first we show that $U_{2,k}$ must be a minterm of Γ. Thus, the restriction of Γ to $U_{2,n}$ has a prefix minterm, and consequently, by Theorem 3, it is an HTAS. This fact enables us to deduce that Γ is a TPAS.

Theorem 4. *Let Γ be an ideal WTAS with $M = U_{1,d} \cup U_{d+2,k}$ being its lexicographical minimal minterm for some $1 \leq d \leq k-2$ and $k \leq n$. If there exists a minterm in Γ that has u_2 as its minimal member and Γ has no self-sufficient users, then Γ is a TPAS.*

8 A Recursive Characterization of Ideal WTASs by Means of Composition

8.1 WTASs and Composition of Access Structures

We begin with the following lemma that asserts that a composition of two access structures is ideal if and only if those two access structures are ideal.

Lemma 13. *Let U_1 and U_2 be disjoint sets. Let $u_1 \in U_1$, and define $U = U_1 \cup U_2 \setminus \{u_1\}$. Suppose Γ_1 and Γ_2 are access structures over U_1 and U_2 respectively such that u_1 is not redundant in Γ_1 and $\Gamma_2 \neq \emptyset$. Furthermore, let Γ be the composition of Γ_1 and Γ_2 via u_1. Then Γ is ideal if and only if both Γ_1 and Γ_2 are ideal. Moreover, if both Γ_1 and Γ_2 have an ideal linear secret sharing schemes, then Γ has an ideal linear secret sharing scheme.*

The recursive characterization of ideal WTASs will be obtained by distinguishing between two types of users. Specifically, we shall identify a subset of so-called strong users that takes the form of a suffix, $S = U_{k,n}$, where $k \geq 3$, and then the complement subset will be thought of as the subset of weak users, $W = U_{1,k-1}$. A subset of strong users will be called S-cooperative if it is unauthorized, but it may become authorized if we add to it some weak users.

Definition 11 (Cooperative Set). *Given $Y \subseteq S$, if $Y \notin \Gamma$ but $W \cup Y \in \Gamma$, then Y is called an S-*cooperative *set.*

By Lemma 5, the access structure $\Gamma_{Y,W}$, the restriction of Γ induced by Y on W, is a WTAS for any partition $U = W \cup S$ and $Y \subseteq S$. We proceed to define a condition on the set S, such that if it is satisfied for some suffix $S = U_{k,n}$, where $k \geq 3$, the access structure Γ is a composition of two ideal WTASs that are defined on sets smaller than U.

Definition 12 (Strong Set). *If for any two S-cooperative sets $Y_1, Y_2 \subseteq S$, the corresponding restrictions of Γ to W coincide, i.e. $\Gamma_{Y_1,W} = \Gamma_{Y_2,W}$, the set S is called a* strong *set of users.*

If S is a strong set of users, there exists an access structure on W, denoted Γ_W, such that $\Gamma_W = \Gamma_{Y,W}$ for all cooperative subsets $Y \subset S$. In that case, every minterm $M \in \Gamma$ is either contained in S or $M \cap W \in \Gamma_W$. The following theorem shows that if S is a strong set of users, Γ is a composition of two ideal WTASs.

Theorem 5. *Let Γ be an ideal WTAS over U. Suppose $S = U_{k,n}$, for some $k \geq 3$, is a strong set of users. Then Γ is a composition of two ideal WTASs, where each access structure is defined on a set smaller than U.*

Simple compositions. We identify two simple cases where an ideal WTAS is a composition of two ideal WTASs defined on sets smaller than U. If Γ has no minterm that starts with u_2 then every minterm that contains u_1 must contain also u_2 (otherwise, we could have replaced u_1 by u_2 in order to get a minterm that starts with u_2). Hence, for every $U_{3,n}$-cooperative set, $Y \subseteq U_{3,n}$, the access structure that Y induces on $U_{1,2}$ is the same, $\Gamma_{Y,U_{1,2}} = \{U_{1,2}\}$. Therefore, $U_{3,n}$ is a strong set of users in this case. Hence, by Theorem 5, the access structure Γ is a composition of two ideal WTASs that are defined on sets smaller than U. If u_n is a self-sufficient user, it can be shown easily that Γ is a composition of two ideal access structures, defined over smaller sets of users. To conclude, we get the following lemma:

Lemma 14. *Let Γ be an ideal WTAS over U. If Γ has self-sufficient users, or u_2 starts no minterm of Γ, then Γ is a composition of two ideal WTASs that are defined on sets smaller than U.*

8.2 Identifying Composition Structures

In this section we show that if Γ is an ideal WTAS, but it is not one of the access structures that were characterized in Sections 6.1 and 7, then it is a composition of two ideal WTASs as described in Section 8.1. In view of Lemma 14, we assume hereinafter that u_2 is the minimal user in some minterm of Γ.

Let M_1 be the lexicographically minimal minterm in Γ. Let u_r be the maximal user in M_1. Then since Γ is neither an HTAS nor a TPAS, there must be at least two users in $U_{1,r-1}$ that are not in M_1. Let u_ℓ be the *minimal* user in M_1 such that at least two users in $U_{1,\ell-1}$ are missing from M_1, and let u_d be the *maximal* user in M_1 such that $U_{1,d} \subset M_1$. We denote the users in $M_1 \cap U_{d+1,\ell-1}$, if there are any, by $Y = \{y_1, \ldots, y_t\}$. Note that if Y is not empty then Y is a run of U, and $y_1 = u_{d+2}$. Next, if $Y \neq \emptyset$ we denote the set of users of $U \backslash M_1$ between y_t and u_ℓ (excluding those two users) by $X = \{x_1, \ldots, x_s\}$. Otherwise, we denote the set $U_{d+2,\ell-1}$ as $X = \{x_1, \ldots, x_s\}$. Finally, we denote the users of $M_1 \cap U_{\ell,n}$ by $Z = \{z_1, \ldots, z_m\}$. Note that the sets X and Z are never empty, and that $z_1 = u_\ell$. The above notations are depicted in Fig. 2.

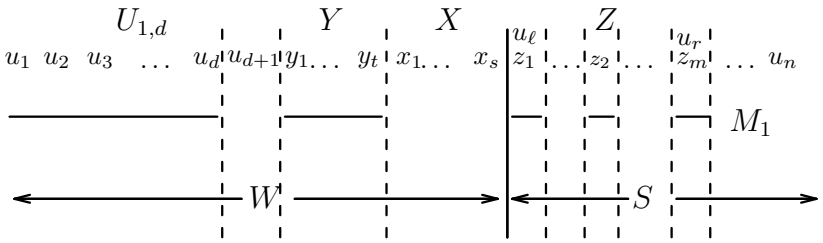

Fig. 2. Notations for the composition.

We claim that either $U_{\ell,n}$ or $U_{d+2,n}$ is a strong set of users. We start by partitioning U into $W = U_{1,\ell-1}$ and $S = U_{\ell,n}$. We show that if all the S-cooperative sets are of the same size, then $\Gamma_{Y_1,W} = \Gamma_{Y_2,W}$ for every two cooperative sets $Y_1, Y_2 \subseteq S$, namely, S is a set of strong users. If, however, that condition does not hold, we shall show that $U_{d+2,n}$ is a strong set.

Lemma 15. *Every minterm of the access structure Γ that intersects W contains at least m users from S.*

Proof. Assume towards contradiction that M is a minterm that intersects W such that $|M \cap S| < m$. The minterm M_1 is an independent set of size $d+t+m$, and thus, by Axiom **(I3)**, every independent set of $\mathcal{M}$ that is smaller than $d + t + m$ can be expanded to an independent set of size $d + t + m$. Therefore, if $|M| < d + t + m$, the minterm M can be expanded to an independent set I of size $d + t + m$; otherwise, we set $I = M$. By Lemma 7, this expansion can only be done by adding to M users that precede $M_{\min}$. As M intersects W, the users in $I \backslash M$ are all from W. Hence, $|I \cap S| = |M \cap S| \leq m - 1$. Therefore, $|I \cap W| = |I| - |I \cap S| \geq d + t + m - (m - 1) = d + t + 1$. Next, we view M_1 as

the canonical complement of the empty set (see Definition 10). Its $(d+t+1)$th element is z_1. By Lemma 10 for $P = \emptyset$, $Y = M_1$, and $j = d+t+1$, any $d+t+1$ members of W form a dependent set. Hence I, which was assumed to be independent, contains a dependent set, a contradiction. □

When all S-cooperative sets are of the same size. Here we show that if all S-cooperative sets are of the same size, namely $|Z| = m$, the set S is a strong set. We accomplish this by showing that all the S-cooperative sets of size m induce the same access structure on W, which is the access structure induced by the S-cooperative set Z.

Lemma 16. *Let $V \subseteq S$ be an S-cooperative set. Then $w(V) \geq w(Z)$.*

Proof. Assume towards contradiction that $w(V) < w(Z)$ and consider the set $W \cup Z$. Since Z is S-cooperative, the set $W \cup Z$ is authorized. Thus, by Lemma 6, it must contain a suffix minterm of the form $B \cup Z$, where B is a suffix of W. There are two possible cases: either $B \cup V$ is authorized, or not.

If $B \cup V$ is authorized, then, since $w(V) < w(Z)$, the set $B \cup V$ is a minterm. Hence, as $B \cup V$ and $B \cup Z$ are two minterms that have the same minimal user, $B_{\min}$, Lemma 8 implies that $|V| = |Z| = m$. The set $B \cup V$ is independent in $\mathcal{M}$. If $|B \cup V| < d+t+m$, Axiom **(I3)** implies that $B \cup V$ can be expanded to an independent set I of size $d+t+m$; if $|B \cup V| \geq d+t+m$, we set $I = B \cup V$. By Lemma 7, all users in $I \backslash (B \cup V)$ must be from W. Hence, I includes at least $d+t$ users from W. On the other hand, since $|V| = |Z| = m$ and $w(V) < w(Z)$, there must be an index j such that $v_j \prec z_j$. Since M_1 is the canonical complement of the empty set $\emptyset$, we get from Lemma 10, applied to $P = \emptyset$, $Y = M_1$ and $B = I_{1,d+t+j}$, that the latter set is dependent. This is impossible since I is independent. Therefore, $B \cup V$ cannot be authorized.

If $B \cup V$ is unauthorized, we let Q be the canonical complement of B. Using Lemma 8, Lemma 15, and Lemma 10, we get that $B \cup V$ is dependent. On the other hand, since V is S-cooperative and B is a suffix of W, the set $B \cup V$ may be expanded to an authorized superset by adding to it users that precede $B_{\min}$, one by one, until the first time that we get an authorized set. This construction, where in each stage we add a new user that is smaller than all current users in the set, guarantees that we end up with a minterm. But a minterm of Γ cannot contain a dependent set. Therefore, this case is not possible either. We conclude that $w(V) \geq w(Z)$. □

Lemma 17. *Let V be an S-cooperative set of size m. Then $\Gamma_{V,W} = \Gamma_{Z,W}$.*

Proof. By Lemma 16, $w(V) \geq w(Z)$. If $w(V) = w(Z)$, the claim is trivial, since Γ is a WTAS. Therefore, we assume that $w(V) > w(Z)$. We first show that $U_{1,d} \cup Y \cup V$ is a minterm of Γ. Since $M_1 = U_{1,d} \cup Y \cup Z$ is authorized, the set $U_{1,d} \cup Y \cup V$ is authorized as well. Assume it is not a minterm. Then, by Lemma 6 it contains a suffix minterm of the form $B \cup V$, where B is a suffix of $U_{2,d} \cup Y$. Let Q be the canonical complement of B. Using Lemma 8, Lemma 15, and Lemma 10, we get that the set $B \cup Z$ is dependent. However, this set is

contained in $U_{1,d} \cup Y \cup Z$, which is a minterm. This contradiction implies that $U_{1,d} \cup Y \cup V$ is a minterm of Γ. Consequently, since $U_{1,d} \cup Y \cup Z$ is a minterm and $U_{2,d} \cup Y \cup V$ is unauthorized (being a proper subset of a minterm), we infer that $w(Z) + w(u_1) > w(V)$.

We are now ready to prove that $\Gamma_{Z,W} = \Gamma_{V,W}$. Since we deal with the case where $w(Z) < w(V)$, the inclusion $\Gamma_{Z,W} \subseteq \Gamma_{V,W}$ is obvious. For the opposite inclusion, it is sufficient to concentrate on minterms of $\Gamma_{V,W}$. Let M be a minterm of $\Gamma_{V,W}$. Thus, $M \cup V \in \Gamma$, and since $M \cup V \setminus M_{\min} \notin \Gamma$, the set $M \cup V$ is a minterm in Γ. There are two possible cases: If $u_1 \in M$, the minterm $M \cup V$ must be of the same size as M_1 by Lemma 8. Since $|M_1| = d + t + m$ and $|V| = m$, we get that $|M| = d + t$. As $M_1 = U_{1,d} \cup Y \cup Z$ is the minimal minterm in Γ in terms of the precedence order $\prec$, the weight of $U_{1,d} \cup Y$ is minimal among all sets of size $d + t$ that are contained in a minterm. This implies that $w(M) \geq w(U_{1,d} \cup Y)$. This, in turn, implies that $M \cup Z \in \Gamma$ and thus $M \in \Gamma_{Z,W}$.

The second case is when $u_1 \notin M$. Assume, towards contradiction, that $M \cup Z \notin \Gamma$. Let Q be the canonical complement of M. Using Lemma 8, Lemma 15, and Lemma 10, we get that the set $M \cup Z$ is dependent. However, since $M \cup V \in \Gamma$ and $w(Z) + w(u_1) > w(V)$, we get that $\{u_1\} \cup M \cup Z \in \Gamma$. Moreover, it must be a minterm since any proper subset of $\{u_1\} \cup M \cup Z$ is of weight that does not exceed that of the unauthorized set $M \cup Z$. Hence, the dependent set $M \cup Z$ is contained in a minterm. This contradiction implies that $M \cup Z$ is authorized, and thus $M \in \Gamma_{Z,W}$. □

Corollary 2. *If there are no S-cooperative sets of size larger than m, then S is a strong set.*

Example 2. Consider the set $U = \{u_1, \ldots, u_8\}$, and let Γ be a WTAS where the weights are 1, 1, 1, 1, 1, 3 ,3 , 3 and the threshold is 6. The lexicographically minimal minterm is $\{u_1, u_2, u_3, u_6\}$, and so there is no prefix minterm and no lacunary minterm. In this example $W = U_{1,5}$ and $S = U_{6,8}$ and the access structure is a composition of a 3-out-of-5 threshold access structure on the week side W and a 2-out-of-4 threshold access structure on $S \cup \{u'\}$, where u' is an additional dummy user.

When large S-cooperative sets exist. The conclusion from Corollary 2 is that whenever all S-cooperative sets for $S = U_{\ell,n}$ are of the same size (i.e., $|Z| = m$), the set S is a strong set and, hence, by Theorem 5, the access structure Γ is a composition of ideal WTASs that are defined over two smaller sets. Here, we continue to deal with the case where there are S-cooperative sets of size larger than m. In that case we identify another strong set. Specifically, we show that $U_{d+2,n}$ is a strong set of users. The analysis of the structure of Γ when large S-cooperative sets exist is technically involved, and is omitted due to lack of space. It appears in the full version of the paper [2].

The following lemma summarizes the results in this case.

Lemma 18. *Suppose there is an S-cooperative set of size larger than m, and there is a minterm of Γ that starts with u_2. Then $U_{d+2,n}$ is a strong set of users.*

8.3 Proof of Theorem 1 – The Characterization Theorem

Let Γ be an ideal WTAS defined on a set of users U and let M_1 be its lexicographically minimal minterm. If either Γ has self-sufficient users or u_2 starts no minterm of Γ, then, by Lemma 14, the access structure Γ is a composition of two ideal WTASs on smaller sets of users.

If M_1 is a prefix then, by Theorem 3, the access structure Γ is an HTAS. If M_1 is a lacunary prefix, namely, $M_1 = U_{1,d} \cup U_{d+2,k}$ for some $1 \leq d \leq k-2$ and $k \leq n$, then, by Theorem 4, the access structure Γ is a TPAS. Otherwise, by Corollary 2 and Lemma 18, there exists within U a subset of strong users, and, by Theorem 5, the access structure Γ is a composition of two ideal WTASs that are defined on sets smaller than U.

As for the other direction, HTASs are ideal and may be realized by linear secret sharing schemes, as shown in [7, 33]. TPASs are also ideal and may be realized by linear secret sharing schemes, as shown in the full version of this paper [2]. Finally, given two ideal access structures, we showed in Lemma 13 how to construct an ideal secret sharing scheme for their composition. Hence, the composition is also ideal. Furthermore, by Lemma 13, if the secret sharing schemes for the two basic access structures are linear, so is the resulting scheme for the composition of the two access structures. This completes the proof of the characterization theorem. □

References

1. A. Beimel and B. Chor. Universally ideal secret sharing schemes. *IEEE Trans. on Information Theory*, 40(3):786–794, 1994.
2. A. Beimel, T. Tassa, and E. Weinreb. Characterizing ideal weighted threshold secret sharing. Technical Report 04-05, Dept. of Computer Science, Ben-Gurion University, 2004. Available at: www.cs.bgu.ac.il/∼beimel/pub.html.
3. A. Beimel and E. Weinreb. Monotone circuits for weighted threshold functions, 2004. In preparation.
4. M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computations. In *20th STOC*, 1–10, 1988.
5. J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *CRYPTO '88*, volume 403 of *LNCS*, pages 27–35. 1990.
6. G. R. Blakley. Safeguarding cryptographic keys. *Proc. of the 1979 AFIPS National Computer Conference*, pages 313–317. 1979.
7. E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.
8. E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4(73):123–134, 1991.
9. E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. of Cryptology*, 5(3):153–166, 1992.
10. R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *J. of Cryptology*, 6(3):157–168, 1993.
11. D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In *Proc. of the 20th ACM STOC*, pages 11–19, 1988.

12. R. Cramer, I. Damgård, and U. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 316–334. 2000.
13. Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In *CRYPTO '91*, volume 576 of *LNCS*, pages 457–469. 1992.
14. M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Proc. of Globecom 87*, pages 99–102, 1987.
15. W. Jackson, K. M. Martin, and C. M. O'Keefe. Ideal secret sharing schemes with multiple secrets. *J. of Cryptology*, 9(4):233–250, 1996.
16. M. Karchmer and A. Wigderson. On span programs. In *Proc. of the 8th IEEE Structure in Complexity Theory*, pages 102–111, 1993.
17. E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. on Information Theory*, 29(1):35–41, 1983.
18. J. Martí-Farré and C. Padró. Secret sharing schemes on access structures with intersection number equal to one. *3rd SCN*, vol. 2576 of *LNCS*, pp. 354–363. 2002.
19. K. M. Martin. *Discrete Structures in the Theory of Secret Sharing.* PhD thesis, University of London, 1991.
20. K. M. Martin. New secret sharing schemes from old. *J. Combin. Math. Combin. Comput.*, 14:65–77, 1993.
21. P. Morillo, C. Padró, G. Sáez, and J. L. Villa. Weighted threshold secret sharing schemes. *Inform. Process. Lett.*, 70(5):211–216, 1999.
22. J. G. Oxley. *Matroid Theory.* Oxford University Press, 1992.
23. C. Padró and G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. on Information Theory*, 46:2596–2605, 2000.
24. M. O. Rabin. Randomized Byzantine generals. In *Proc. of the 24th IEEE Symp. on Foundations of Computer Science*, pages 403–409, 1983.
25. P. D. Seymour. On secret-sharing matroids. *J. of Combinatorial Theory, Series B*, 56:69–73, 1992.
26. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.
27. G. J. Simmons. How to (really) share a secret. In *CRYPTO '88*, volume 403 of *LNCS*, pages 390–448. 1990.
28. G. J. Simmons. An introduction to shared secret and/or shared control and their application. In *Contemporary Cryptology, The Science of Information Integrity*, pages 441–497. IEEE Press, 1992.
29. G. J. Simmons, W. Jackson, and K. M. Martin. The geometry of shared secret schemes. *Bulletin of the ICA*, 1:71–88, 1991.
30. J. Simonis and A. Ashikhmin. Almost affine codes. *Designs, Codes and Cryptography*, 14(2):179–197, 1998.
31. D. R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2:357–390, 1992.
32. D. R. Stinson. New general lower bounds on the information rate of secret sharing schemes. In *CRYPTO '92*, volume 740 of *LNCS*, pages 168–182. 1993.
33. T. Tassa. Hierarchical threshold secret sharing. In M. Naor, editor, *First Theory of Cryptography Conference, TCC 2004*, volume 2951 of *LNCS*, pages 473–490. 2004.