Characterizing Ideal Weighted Threshold Secret Sharing

Amos Beimel* Tamir Tassa† Enav Weinreb‡

October 2, 2006

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. On one hand, there are nontrivial weighted threshold access structures that have an ideal scheme – a scheme in which 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). On the other hand, other weighted threshold access structures are not ideal. 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 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 [5] and Shamir [28]. Efficient threshold secret sharing schemes were used in many cryptographic applications, e.g., Byzantine agreement [26], secure multiparty computations [3, 10], and threshold cryptography [13].

In this paper we deal with *weighted* threshold secret sharing schemes. In these schemes, considered already by Shamir [28], 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.[1]

*Dept. of Computer Science, Ben-Gurion University, Beer-Sheva 84105, Israel. E-mail: beimel@cs.bgu.ac.il. .

†Division of Computer Science, The Open University, Tel-Aviv, Israel, and Dept. of Computer Science, Ben-Gurion University, Beer-Sheva 84105, Israel.

‡Dept. of Computer Science, Ben-Gurion University, Beer-Sheva 84105, Israel. E-mail: weinrebe@cs.bgu.ac.il.

[1]A weighted threshold function is a boolean function $f : \{0,1\}^n \to \{0,1\}$ where each variable is assigned a positive weight and $f(x_1, \ldots, x_n) = 1$ iff the sum of weights that are assigned to the variables whose value is 1 exceeds a given threshold.

Ito, Saito, and Nishizeki [16] 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 [19]). 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. However, some access structures do not have an ideal secret sharing schemes that realizes them [4]. 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, 6, 7, 17, 20, 21, 23, 25, 27, 32, 35]. Ideal access structures are known to have certain combinatorial properties. In particular, there is a strong relation between ideal access structures and matroids [7].

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 4.9 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 previous one, it has an ideal secret sharing scheme (see Example 7.5). 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 8.10).

In this paper we give a combinatorial characterization of ideal weighted threshold access structures. We show that if a weighted threshold access structure is ideal then one of the following statements hold:

1. It is a *multilevel* or *hierarchical* threshold access structure. This type of access structures was introduced by Simmons in [29]. In such settings, the users are divided into a hierarchy of levels, and each level has an associated threshold. A set of users is authorized if it has a subset whose size is at least the threshold that corresponds to the level of the lowest member in that subset.

2. It is a *tripartite* access structure. In such access structures, the set of users is partitioned into three classes, and a given subset is authorized iff the sizes of its intersection with each of the three classes satisfy some threshold conditions (See Section 7 for details).

3. The set of users is composed of *strong* users (users with larger weights) and *weak* users (users with smaller weights) and the access structure is a combinatorial composition of two ideal weighted threshold access structures, one that is defined on the subset of strong users and another that is defined on the subset of weak users.

(Formal definitions are given in Section 3.)

Most of the access structures that play part in our characterization are well known [25, 29, 35]. Tripartite access structures were considered by collins [11], who gave a necessary condition for a tripartite access structure to be ideal. We consider a specific family of tripartite access structures and design ideal secret sharing schemes for this family. Following our work, Herranz and Saez [15] constructed ideal secret sharing schemes to a wider family of tripartite access structures and Farràs, Martí-Farré, and Padró [14] exactly characterize the tripartite access structures that are ideal.

The present study generalizes the work of Morillo, Padró, Sáez, and Villar [23] 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 [7]. We utilize results regarding the structure of matroids in order to understand the structure of ideal weighted threshold access structures. An important tool in our analysis is composition of ideal access structures. When composing two access structures, defined on two disjoint sets, one gets an access structure on a larger set of users. The resulting access structure is ideal if and only if the original two are ideal. This enables us to characterize ideal weighted threshold access structures in a recursive manner, as described above. Composition of access structures was studied, e.g., in [1, 4, 8, 12, 22, 34].

Related Work. Secret sharing schemes for general access structures were defined by Ito, Saito, and Nishizeki in [16]. More efficient schemes were presented in, e.g., [4, 6, 18, 31]. We refer the reader to [30, 33] for extensive surveys on secret sharing schemes. 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 whether better schemes exist. For weighted threshold access structures the situation is somewhat better. Shamir [28] proposed a weighted threshold secret sharing scheme that is based on his ideal threshold secret sharing scheme. In that scheme, the ratio between the share size of each user and the size of the secret equals the weight assigned to that user, which may be exponential in the number of users n. In a recent work [2], 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 [2] 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 ideal weighted threshold access structures on smaller sets of users.

2 Definitions and Notations

2.1 Secret Sharing

Definition 2.1 (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 2.2 (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 two 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[2] $\textsc{Recon}_B : S_{i_1} \times \cdots \times S_{i_{|B|}} \to S$ *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,*

$$\textsc{Recon}_B(\Pi_B(s)) = s.$$

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 $\langle s_i \rangle_{u_i \in C}$:*

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

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 [19], namely $|S_i| \geq |S|$ for all $i \in [n]$. This motivates the next definition.

Definition 2.3 (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 [6] in the ideal setting and was latter generalized to non-ideal schemes. Linear schemes are equivalent to monotone span programs [18]. For simplicity we only define ideal linear schemes.

Definition 2.4 (Ideal Linear Secret Sharing Scheme) *Let $\mathbb{F}$ be a finite field. An ideal* linear secret sharing scheme *over $\mathbb{F}$ takes the following form: The domain of secrets and shares is $S = \mathbb{F}$. The scheme is specified by $n+1$ vectors in $\mathbb{F}^t$ for some integer t: a vector $\mathbf{T_i}$ per user $u_i \in U$, where $i \in [n]$, and a so-called target vector $\mathbf{T}$. To share a secret $s \in \mathbb{F}$, the dealer chooses a random vector $\mathbf{R} \in \mathbb{F}^t$ such that $\mathbf{R} \cdot \mathbf{T} = s$ and then the share of user u_i is $\mathbf{R} \cdot \mathbf{T_i}$.*

The next theorem characterizes the access structure that is realized by a linear secret sharing scheme.

Theorem 2.5 ([6, 18]) *A linear secret sharing scheme with vectors $\{\mathbf{T_i}\}_{i \in [n]}$ and $\mathbf{T}$ realizes the following access structure Γ:*

$$A \in \Gamma \textit{ if and only if } \mathbf{T} \in \text{span}\,\{\mathbf{T_i} : u_i \in A\}.$$

[2] We stress that there is no requirement that $\textsc{Recon}_B$ can be efficiently implemented. However, this is the case for all the secret sharing schemes designed in this paper.

2.2 Weighted Threshold Access Structures

In this paper we concentrate on special access structures, so-called weighted threshold access structures, that were already introduced in [28].

Definition 2.6 (Weighted Threshold Access Structure – WTAS) *Let $w : U \to \mathbb{N}$ 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.*

It is easy to see that Definition 2.6 does not restrict generality when assuming that the weights and the threshold are integers. In other words, given a WTAS with real positive weights and threshold, there exist integer weights and threshold that induce the very same access structure.

2.3 Terminology and Notations

First, for a positive integer n, we denote by $[n]$ the set $\{1, 2, \ldots, n\}$. Throughout this paper we assume that the users are ordered in a nondecreasing order according to their weights, i.e.,

$$0 < w(u_1) \leq w(u_2) \leq \cdots \leq w(u_n).$$

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-leveled 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 $A_{s,t} = \{a_j\}_{s \leq j \leq t}$ 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 $A_{\ell,k}$, where $1 \leq \ell \leq k$. 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, $w(u_i) \leq w(u_j)$). This relation induces the following lexicographic order on subsets of U:

- $\emptyset \prec A$ for all $A \subseteq U$ such that $A \neq \emptyset$.
- If $a_1 \prec b_1$ then $A \prec B$; if $b_1 \prec a_1$ then $B \prec A$; otherwise, $A \prec B$ if and only if $(A \setminus \{a_1\}) \prec (B \setminus \{b_1\})$.

3 Characterizing Ideal WTASs

The main result of this paper is a combinatorial characterization of ideal WTASs. We define in Definitions 3.1–3.4 the building blocks that play an essential role in this characterization. Using these definitions, we state Theorem 3.5, our main result, that characterizes ideal WTASs. We then outline the proof of that theorem, where the full proof is given in the subsequent sections.

3.1 Building Blocks

Definition 3.1 (Hierarchical Threshold Access Structure – HTAS) *Let m be an integer, U be a set of users, and $\{L_i\}_{1 \leq i \leq m}$ be a partition of U into a hierarchy of m disjoint levels, i.e., $U = \bigcup_{i=1}^{m} L_i$. Furthermore, let $\{k_i\}_{1 \leq i \leq m}$ 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*:*

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

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 [29] and further studied by Brickell who proved their ideality [6]. An explicit ideal scheme for these access structures was constructed in [35].

Remark 3.2 Without loss of generality, we assume that $|L_i| > k_i - k_{i+1}$ for every $i \in [m-1]$, and $|L_m| \geq k_m$. Indeed, if $|L_i| \leq k_i - k_{i+1}$ 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 $(i+1)$th condition is redundant.

We next present tripartite access structures (TPASs), which are a generalization of bipartite access structures that were presented in [25]. In a *bipartite* access structure, the set of users is partitioned into two classes, and a subset is authorized if the sizes of its intersection with each of these classes satisfy some predefined conditions. In a *tripartite* access structure, the set of users is partitioned into three classes, and, similarly to bipartite access structures, a given subset is authorized if the sizes of its intersection with each of these classes satisfy some conditions. In the next definition we describe two special types of tripartite access structures. We would like to stress that there exist other types of tripartite access structures, but herein we concentrate only on those two types, since only they are relevant for the characterization of ideal WTASs. Later on we prove that these types of TPASs are ideal by constructing a linear ideal secret sharing scheme that realizes them. That scheme is a generalization of a scheme from [25] for bipartite access structures. Following our work, Farràs, Martí-Farrée, and Padró [14] exactly characterize the tripartite access structures that are ideal.

Definition 3.3 (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 $m \geq t$. Then the following is a* tripartite access structure (TPAS) *on* U*:*

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

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 another type of a tripartite access structure:

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

That is, a set X is in Δ_2 if either it has at least m users, $(m-d)$ of which are from C, or it has at least t users from $B \cup C$.

Definition 3.4 (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 on 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*

$$\Gamma = \{X \subseteq U : X_1 \in \Gamma_1 \textit{ or } (X_2 \in \Gamma_2 \textit{ and } X_1 \cup \{u_1\} \in \Gamma_1) \textit{ where } X_1 = X \cap U_1 \textit{ and } X_2 = X \cap U_2\};$$

namely, $X \subseteq U$ is authorized in this access structure if either $X_1 = X \cap U_1$ is authorized in Γ_1, or $X_1 \cup \{u_1\}$ is authorized in Γ_1 and $X_2 = X \cap U_2$ is authorized in Γ_2.

The motivation behind this definition is as follows. We start with an access structure Γ_1 on U_1. Then, we allow the replacement of one of the users in U_1, denoted u_1, by *substitute* users of a disjoint set U_2, where Γ_2 specifies the subsets of U_2 that are legitimate substitutes for u_1. Hence, in the set $U = U_1 \cup U_2 \setminus \{u_1\}$ that is obtained from U_1 after replacing u_1 with U_2, a subset is authorized if it is either a subset in Γ_1 that does not include u_1 or it was obtained from a subset in Γ_1 that did include u_1, by replacing u_1 with an authorized subset of substitutes from Γ_2. In Lemma 8.1 we show that Γ is ideal if and only if both Γ_1 and Γ_2 are ideal.

3.2 The Characterization

Following the notation convention in Section 2.3, 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 an ideal weighted threshold access structure Γ.

If M is a prefix of U, namely $M = U_{1,k} = \{u_1, \ldots, u_k\}$ for some $k \in [n]$, then, as we prove in Section 6.3, 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 prove 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 on 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 8.1. Hence, this result, which we prove in Section 8, completes the characterization of ideal WTASs in a recursive manner.

Hence, our main result in this paper is as follows.

Theorem 3.5 (The Characterization Theorem) *Let U be a set of users, $w : U \to \mathbb{N}$ 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 of at most three levels.*
- *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 on 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.

Remark 3.6 In the ideal schemes for weighted threshold access structures that we construct in this paper, the size of the domain of secrets is at most $2^{\mathrm{poly}(n)}$. This is the field size needed for the HTAS constructions of [35] and for the TPAS construction introduced in Section 7. As the composition of ideal access structures does not change the size of the underlying field, we get that the field size for our entire construction is bounded by $2^{\mathrm{poly}(n)}$. This is a comfortable bound since it implies that both the secret and the shares may be represented by $\mathrm{poly}(n)$ bits.

4 Matroids and Ideal Secret Sharing Schemes

Ideal secret sharing schemes and matroids are strongly related. If an access structure is ideal, then 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 [24].

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. Axiom (I1) assures that there is at least one independent set in $\mathcal{I}$. Axiom (I2) asserts that the collection $\mathcal{I}$ is closed under containment. Finally, Axiom (I3) enables the expansion of every small independent set in $\mathcal{I}$. 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 on a set of users $U = \{u_1, \ldots, u_n\}$. If Γ is ideal, then, by the results of [7, 21], 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 4.1 ([7, 21]) *Let Γ be a connected ideal access structure on U. Then there exists a connected matroid $\mathcal{M}$ on $U \cup \{u_0\}$ 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 4.1, and, additionally, it provides means to identify *all* the circuits of that matroid.

Lemma 4.2 ([24, 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 4.1 and Lemma 4.2 is referred to as *the matroid corresponding to* Γ.

This next definition will enable us to explicitly define the matroid corresponding to Γ using the authorized sets in Γ.

Definition 4.3 (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 $M_1 \cup M_2 \setminus \{x\}$ is unauthorized. In addition, we define*

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

With this definition, the following corollary is a straightforward result of Theorem 4.1 and Lemma 4.2.

Corollary 4.4 *Let Γ be a connected ideal access structure on U. Then there exists a unique connected matroid $\mathcal{M}$ on $U \cup \{u_0\}$ such that $\mathcal{C}_0$ is exactly the set of circuits of $\mathcal{M}$ containing u_0. Furthermore, the minimal sets in $\{D(M_1, M_2) : M_1, M_2$ are distinct minterms of $\Gamma\}$ are the circuits of the matroid that do not contain u_0.*

In the sequel we use the following simple consequence of Corollary 4.4.

Corollary 4.5 *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 $\mathcal{M}$. The following basic result from matroid theory provides another way of establishing the dependency of a set in a matroid.

Lemma 4.6 ([24, Page 16]) *Let C_1 and C_2 be two distinct circuits in a matroid, $e \in C_1 \cap C_2$, and $d \in C_1 \setminus C_2$ such that $d \neq e$. Then there exists a circuit $C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$, where $d \in C_3$.*

In most applications of the lemma we will ignore d and the fact that $d \in C_3$. Since every minterm of Γ is properly contained in a circuit of $\mathcal{M}$, it forms an independent set of $\mathcal{M}$. However, these are not necessarily the only independent sets in $\mathcal{M}$. The following claim is a simple corollary of Axiom (I3) in the matroid definition.

Claim 4.7 *Let $\mathcal{M}$ be a matroid and I be an independent set of size m. Then any independent set of size $\ell < m$ can be extended to an independent set of size m.*

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

Lemma 4.8 *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.*

To prove that an access structure is not ideal we use the above results that define the dependent sets in the matroid corresponding to Γ. In particular, we use the basic fact that an independent set of $\mathcal{M}$ cannot contain a dependent set (see Axiom (I2)). By Theorem 4.1, for every minterm $M \in \Gamma$, the set $M \cup \{u_0\}$ is a circuit of $\mathcal{M}$. Thus, the set M is an independent set of $\mathcal{M}$. Therefore, if D is a dependent set of $\mathcal{M}$, it cannot be contained in any minterm of Γ. The next example shows how to use the above statements in order to demonstrate that a given access structure is not ideal.

Example 4.9 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 [4] that this access structure is not ideal.[3] We first give a simple proof, based on Corollary 4.5, showing that Γ is not ideal. Assume that it is ideal and consider the

[3] In [9] 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 [8].

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 4.5, 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. This contradiction implies that Γ is not ideal.

We proceed to sketch an alternative proof for the non-ideality of Γ, similar to the proof that was given in [4]. We present this proof for two reasons. First, we want to show that using matroids simplifies and shortens the proofs substantially. Matroid-based proofs, however, tend to be technical and, consequently, not very intuitive. The alternative proof that we present herein reveals some of the intuition that is sometimes obfuscated in matroid-based proofs.

Assume towards a contradiction that Γ has an ideal secret sharing scheme over some domain of secrets S. Letting s_i denote the share of user u_i for $1 \le i \le 4$, we will show that s_2 may be computed from s_1 (this statement is equivalent to the statement in the first proof that the set $\{u_1, u_2\}$ is dependent). Having shown that, we will conclude that $\{u_1, u_3\}$ can reconstruct the secret (since $\{u_1, u_2, u_3\}$ is an authorized set and u_2 is unnecessary in the presence of u_1), in a contradiction with the definition of Γ.

We need to show that s_2 is uniquely determined by s_1. Assume, by contradiction, that there exists $s_1 \in S_1$ and $s_2, s'_2 \in S_2$, where $s_2 \neq s'_2$, such that both assignments of shares to $\{u_1, u_2\}$, namely $\langle s_1, s_2\rangle$ and $\langle s_1, s'_2\rangle$, are possible. Since $\{u_1, u_2\}$ is unauthorized, that set cannot learn any information on the secret from its shares. Hence, given the pair of shares $\langle s_1, s_2\rangle$, every secret is possible. Hence, for every $s \in S$, there exists at least one share $s_4(s)$ for u_4 such that $\langle s_1, s_2, s_4(s)\rangle$ is a possible assignment of shares to $\{u_1, u_2, u_4\}$ given the secret s. On the other hand, since the shares of $\{u_1, u_2, u_4\}$ determine the secret, $s_4(s)$ must be unique, since otherwise the domain of shares of u_4 would be larger than the domain of secrets, in a contradiction with ideality. Similarly, for every $s \in S$ there exists a unique share $s'_4(s)$ such that $\langle s_1, s'_2, s'_4(s)\rangle$ is another possible assignment of shares to $\{u_1, u_2, u_4\}$ given the secret s.

In view of the above, the sets $\{s_4(s) : s \in S\}$ and $\{s'_4(s) : s \in S\}$ are of size $|S|$. However, since they are both subsets of S_4 and, by ideality, $|S_4| = |S|$, they both equal S_4. One conclusion is that each secret $s \in S$ is consistent with each share $s_4 \in S_4$. Another conclusion is that there are secrets $a, b \in S$ such that $s_4(a) = s'_4(b) := s_4$. If $a \neq b$, then the pair of shares $\langle s_1, s_4\rangle$ is insufficient to determine whether the secret is a or b, in a contradiction with the correctness requirement that $\{u_1, u_4\} \in \Gamma$ should be able to reconstruct the secret. Thus, $a = b$, whence both pairs of shares $\langle s_2, s_4\rangle$ and $\langle s'_2, s_4\rangle$ are possible assignments of shares to $\{u_2, u_4\}$ given that the secret is a. But this implies that the size of S_2 is at least $|S| + 1$ (by going over all secrets $s \in S$ and looking for a corresponding assignment of shares where the share of u_4 is s_4) thus contradicting ideality.

4.1 Restrictions

Definition 4.10 (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 on 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. For completeness, we give a proof herein.

Lemma 4.11 *Let Γ be an access structure on a set of users U. Let $Y, X \subseteq U$ be sets such that $X \cap Y = \emptyset$. If Γ is ideal, then $\Gamma_{Y,X}$ is ideal.*

Proof: Let $Y = \{u_{i_1}, \ldots, u_{i_{|Y|}}\}$. We construct an ideal secret sharing scheme Π' for $\Gamma_{Y,X}$ using an ideal scheme Π for Γ. Fix an arbitrary secret $s' \in S$, and let $s_Y = \langle s'_{i_1}, \ldots, s'_{i_{|Y|}} \rangle = \Pi_Y(s')$ be a possible vector of shares for the users of Y. Let $s \in S$ be a secret to be distributed by Π'. The scheme Π' randomly chooses an n-tuple $\Pi(s) = \langle s_1, \ldots, s_n \rangle$ such that $s_{i_j} = s'_{i_j}$ for all $1 \leq j \leq |Y|$ (such a selection is possible because Y is unauthorized, whence every assignment of shares to Y is consistent with every secret). Every user $u_j \in X$ is then assigned by Π' the share s_j. (The shares of Y, namely $\langle s'_{i_1}, \ldots, s'_{i_{|Y|}} \rangle$, are considered "publicly known".)

The scheme is correct since if $Z \in \Gamma_{Y,X}$ then $Y \cup Z \in \Gamma$, and thus the members of Z, who know the shares s_Y of Y, can reconstruct the secret as in the scheme Π for Γ. Similarly, the scheme is private, since if $Z \notin \Gamma_{Y,X}$, then $Y \cup Z \notin \Gamma$, and thus the users of Z, who know the shares of Y, will not have any information regarding the secret. The scheme is ideal since the share-domain of all the users is the same as in the original ideal scheme. □

The following result gives a relation between the matroids corresponding to Γ and $\Gamma_{Y,X}$.

Lemma 4.12 *Let Γ be an ideal access structure on a set of users U. Let $Y, X \subseteq U$ be sets such that $X \cap Y = \emptyset$, and Y is independent in the matroid corresponding to Γ. Then if a set $I \subseteq X$ is independent in the matroid corresponding to $\Gamma_{Y,X}$, it is also independent in the matroid corresponding to Γ.*

Proof: Let $\mathcal{M} = \langle U \cup \{u_0\}, \mathcal{I} \rangle$ be the matroid associated with Γ. We define the matroid $\mathcal{M}' = \langle X \cup \{u_0\}, \mathcal{I}' \rangle$ as follows: A set $Z \subseteq X \cup \{u_0\}$ is in $\mathcal{I}'$ if and only if $Y \cup Z \in \mathcal{I}$. This is indeed a matroid: Axiom (I1) holds because $Y \in \mathcal{I}$ so that $\emptyset \in \mathcal{I}'$. As for Axiom (I2), $Y \cup B \in \mathcal{I}$ for every $B \in \mathcal{I}'$; therefore, if $A \subseteq B$ then $Y \cup A \in \mathcal{I}$ whence $A \in \mathcal{I}'$. Axiom (I3) holds as well. Let $A, B \in \mathcal{I}'$ be such that $|A| > |B|$. Since $Y \cup A \in \mathcal{I}$ and $Y \cup B \in \mathcal{I}$ while $|Y \cup A| > |Y \cup B|$, there must be an element $x \in A \backslash B$ such that $Y \cup (B \cup \{x\}) \in \mathcal{I}$. Therefore, $B \cup \{x\} \in \mathcal{I}'$, as required.

We claim that $\mathcal{M}'$ is the unique matroid corresponding to $\Gamma_{Y,X}$. That is, for every $M \subseteq X$, the set $M \cup \{u_0\}$ is a circuit of $\mathcal{M}'$ if and only if M is a minterm of $\Gamma_{Y,X}$. Proving that, we get that if $I \in \mathcal{I}'$ then $Y \cup I \in \mathcal{I}$ and, therefore, I itself is independent in $\mathcal{M}$.

Suppose $M \cup \{u_0\}$ is a circuit of $\mathcal{M}'$. Then $Y \cup M \cup \{u_0\}$ is dependent in $\mathcal{M}$, and, consequently must contain a circuit of $\mathcal{M}$. That circuit must contain $M \cup \{u_0\}$ because otherwise there would be a proper subset $B \subset M \cup \{u_0\}$ such that $Y \cup B$ is dependent in $\mathcal{M}$, thus implying that B is dependent also in $\mathcal{M}'$, in a contradiction with our assumption that $M \cup \{u_0\}$ is a circuit of $\mathcal{M}'$. Let $Y' \cup M \cup \{u_0\}$ be that circuit of $\mathcal{M}$, where $Y' \subseteq Y$. Hence, by the characterization of the matroid that corresponds to a given access structure, $Y' \cup M$ is a minterm of Γ. Hence, $Y \cup M$ is in Γ, and, consequently, $M \in \Gamma_{Y,X}$. It is left to show that M is a minterm of $\Gamma_{Y,X}$. Let M' be a proper subset of M. Since $M \cup \{u_0\}$ is a circuit of $\mathcal{M}'$, the set $M' \cup \{u_0\}$ is independent in $\mathcal{M}'$. This implies that $Y \cup M' \cup \{u_0\}$ is independent in $\mathcal{M}$. Therefore $Y \cup M' \notin \Gamma$, and thus $M' \notin \Gamma_{Y,X}$. This completes the proof of the first direction.

For the second direction, assume that M is a minterm of $\Gamma_{Y,X}$. We next prove that $M \cup \{u_0\}$ is dependent in $\mathcal{M}'$. The set $Y \cup M$ is authorized in Γ. Let $Y' \subseteq Y$ be such that $Y' \cup M \in \Gamma$ and $|Y'|$ is minimal (it is possible that $Y' = \emptyset$). We claim that $Y' \cup M$ is a minterm of Γ: indeed, every user in Y' is critical in $Y' \cup M$, as implied by the minimality of $|Y'|$; on the other hand, every user in M is critical, for otherwise M would have a proper subset $M' \subset M$ such that $Y \cup M' \in \Gamma$ thus contradicting our assumption that M is a minterm of $\Gamma_{Y,X}$. It follows that $Y' \cup M \cup \{u_0\}$ is a circuit of $\mathcal{M}$. Therefore, the set $Y \cup M \cup \{u_0\}$ is dependent in $\mathcal{M}$. This implies that $M \cup \{u_0\}$ is dependent in $\mathcal{M}'$.

To complete the proof we need to prove that $M \cup \{u_0\}$ is a circuit in $\mathcal{M}'$. Assume towards a contradiction that $M \cup \{u_0\}$ properly contains a circuit of $\mathcal{M}'$. If this circuit is of the form $M' \cup \{u_0\}$, for some $M' \subset M$, then by the proof of the first direction, M' is a minterm of $\Gamma_{Y,X}$, contradicting the fact that M is a minterm of $\Gamma_{Y,X}$. Therefore, the circuit is some $M' \subseteq M$. This implies that $Y \cup M'$ is dependent in $\mathcal{M}$. Hence, there exists $Y'' \subseteq Y$, such that $Y'' \cup M'$ is a circuit of $\mathcal{M}$. However, as shown earlier, $Y' \cup M \cup \{u_0\}$ is a circuit of $\mathcal{M}$ as well, for some $Y' \subseteq Y$. Applying Lemma 4.6 for these two circuits, with e being an arbitrary user in M', and $d = u_0$, we get that there is a circuit contained in $(M \setminus \{e\}) \cup Y \cup \{u_0\}$, that contains u_0. This implies that $(M \setminus \{e\}) \cup Y \in \Gamma$, whence $(M \setminus \{e\}) \in \Gamma_{Y,X}$, in a contradiction to our assumption that M is a minterm of $\Gamma_{Y,X}$. □

A special family of restrictions of Γ are restrictions in which $Y = \emptyset$, i.e. $\Gamma_{\emptyset,X}$. Such a restriction consists of all subsets of X that are authorized in Γ. We shall refer to such a restriction simply as *the restriction of* Γ *to* X. We conclude with a trivial claim regarding restrictions of WTASs.

Claim 4.13 *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.

An authorized set of Γ may contain many different minterms. The following simple lemma shows that one of these minterms is a suffix of the set.

Lemma 5.1 *Any $X \in \Gamma$ contains a suffix minterm. Namely, if $X = \{x_1, \ldots, x_k\}$ and $X \in \Gamma$, then there exists $i \in [k]$ such that $X_{i,k} = \{x_i, \ldots, x_k\}$ is a minterm.*

Proof: Let $s \in [k]$ be the largest index such that $X_{s,k}$ is authorized. We claim that $X_{s,k}$ is a minterm. Indeed, x_s is critical for $X_{s,k}$ since removing it from $X_{s,k}$ we get $X_{s+1,k}$, which is unauthorized by the choice of s. Consequently, every user $x_i \in X_{s,k}$ is critical because x_s has the smallest weight in $X_{s,k}$. Therefore, $X_{s,k}$ is a minterm. □

We saw that minterms of Γ are independent sets of $\mathcal{M}$. Different minterms of Γ may be of different sizes. By Claim 4.7, if M and M' are minterms and $|M| < |M'|$, we can add (at least $|M'| - |M|$) users to M such that the resulting set is still an independent set of $\mathcal{M}$. The next lemma asserts that the users that may be added to M must have a smaller weight than the weight of every member of M:

Lemma 5.2 *Let M be a minterm of Γ. Let $y \in U \setminus M$ be a user such that $w(M_{\min}) \leq w(y)$. Then $M \cup \{y\}$ is a dependent set of $\mathcal{M}$.*

Proof: Let $X = (M \setminus \{M_{\min}\}) \cup \{y\}$ be the set that is obtained by replacing the minimal element of 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 4.5, the set $M \cup M' = M \cup \{y\}$ is dependent in $\mathcal{M}$. □

While Γ may have minterms of different cardinalities, we show in the next lemma that whenever two minterms have the same minimal member they must be of the same size.

Lemma 5.3 *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 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 $w(X_{\min}) \le w(y)$. Consequently, in view of Lemma 5.2, the set $X \cup \{y\}$ is dependent. This contradiction implies that $|X| \ge |Y|$. Arguing along the same lines we conclude that also $|X| \le |Y|$, whence both minterms are of the same size. $\square$

In the matroid $\mathcal{M}$ corresponding to an access structure Γ, each minterm M of Γ defined a circuit $M \cup \{u_0\}$ in $\mathcal{M}$. This may be viewed as a *local* relation between the minterms of Γ and the dependent sets of $\mathcal{M}$. However, when dealing with WTASs, the *global* structure of Γ enables us to prove the dependency of various sets in $\mathcal{M}$. It turns out that the lexicographic order on the minterms of Γ, with respect to the relation $\prec$ (defined in Section 2.3), is strongly related to dependence in $\mathcal{M}$. This is demonstrated through the following definition and lemmas.

Definition 5.4 (Canonical Complement) *Let P be a prefix of some minterm of Γ. Let $Y \subseteq U$ be the lexicographically minimal set such that:*

- *$P_{\max} \prec Y_{\min}$, and*
- *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 element of the canonical complement results in a dependent set.

Lemma 5.5 *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, and that circuit 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 $X_2 = (M_1 \backslash \{P_{\max}\}) \cup \{b\}$ be the set resulting from replacing $P_{\max}$ with b in M_1. Since $w(P_{\max}) \le w(b)$, 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 5.1). It must be that $b \in M_2$, since otherwise $M_2 \subseteq Y$, where Y – the canonical complement of P – 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 $D(M_1, M_2) \subseteq (M_1 \cup M_2) \setminus Y = P \cup \{b\}$. But since, by Corollary 4.5, the set $D(M_1, M_2)$ is dependent, this will imply that also $P \cup \{b\}$ is dependent. We also observe that it is sufficient 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, it suffices to show that y_1 is critical for A. Suppose this is not the case, namely, the set $A \backslash \{y_1\}$ is authorized. Since $A \backslash \{y_1\}$ results from M_1 by replacing y_1 by b where $w(b) \le w(y_1)$, and since M_1 is a minterm, it must be that $A \backslash y_1$ is also a minterm. But this is a contradiction to the choice of y_1 as the first element 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 Claim 4.8, the set $P \cup \{b\}$ must contain a unique circuit, and that circuit contains b. $\square$

The next lemma is a generalization of Lemma 5.5. Given a prefix P of some minterm, it gives a sufficient condition for a set $B \subseteq U$ so that $P \cup B$ is dependent in $\mathcal{M}$. It plays an essential role is our study of the characterization of ideal WTASs.

Lemma 5.6 *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.*

Proof: The proof is by induction on j. The case $j = 1$ is handled by Lemma 5.5. We assume that the lemma holds for all $i \in [j-1]$ and proceed to prove it for $i = j$. If $b_i \prec y_i$ for some $i \in [j-1]$, then the statement of the lemma holds by induction (in fact, in that case we conclude that $P \cup B_{1,i}$ is dependent, which is a stronger claim that what we need to show). Therefore, we may assume hereinafter that $y_i = b_i$ or $y_i \prec b_i$ for all $i \in [j-1]$.

Assume towards a contradiction that $P \cup B$ is independent. Denote $D = P \cup \{y_1\} \cup B$ and $P' = P \cup \{y_1\}$. The canonical complement of P' is $Y_{2,t}$. On the other hand, since $P'_{\max} = y_1 \preceq b_1 \prec b_2$, and $b_j \prec y_j$, the induction hypothesis, applied to P' and $B_{2,j}$, implies that $P' \cup B_{2,j}$ is dependent. Since $P' \cup B_{2,j} \subseteq D$, the set D is also dependent. Therefore, since we assumed that $P \cup B$ is independent, Claim 4.8 implies that D contains a unique circuit C. The uniqueness of the circuit C in D and the fact that $P' \cup B_{2,j}$ is a dependent subset of D, imply that $C \subseteq P' \cup B_{2,j}$. This, in turn, implies that $b_1 \notin C$, unless $y_1 = b_1$. This will allow us to derive a contradiction.

There are three possible cases regarding the position of b_1 with respect to the members of Y: $y_1 = b_1$, or $y_1 \prec b_1 \prec y_2$, or $y_2 \preceq b_1$. The first case is trivial: if $y_1 = b_1$ then $P \cup B = P' \cup B_{2,j}$ and, thus, it is dependent, in a contradiction to our assumption.

If $y_1 \prec b_1 \prec y_2$ then by Lemma 5.5, applied to P' and b_1, the set $P' \cup \{b_1\}$ is dependent and contains a circuit C' that contains b_1. As $b_1 \in C'$ and $b_1 \notin C$, we conclude that $C \neq C'$. However, as $C' \subseteq D$, this contradicts the uniqueness of the circuit C in D.

The only case left is $y_2 \preceq b_1$. As P' is independent, there must be an index $s \in \{2, \ldots, j\}$ such that $b_s \in C$ (for, otherwise, as $b_1 \notin C$, $C \cap B = \emptyset$, and, consequently, $C \subseteq P'$). Consider the set $B^s = B \setminus \{b_s\}$. Since $|B^s| = j-1$, $P'_{\max} = y_1 \prec b_1 = B^s_{\min}$, and the $(j-1)$th element of B^s (which is either b_j, if $s < j$, or b_{j-1}) precedes the $(j-1)$th element of the canonical complement of P' (which is y_j), we conclude, by the induction hypothesis, that $P' \cup B^s$ is dependent. Therefore, it contains a circuit C'' that does not contain b_s. Since $b_s \in C$ but $b_s \notin C''$, we infer that $C \neq C''$. However, as $C'' \subseteq D$, this contradicts the uniqueness of C in D. This completes the proof that the set $P \cup B$ is dependent. $\square$

6 WTASs and HTASs

In this section we discuss the family of hierarchical threshold access structures (HTASs), from Definition 3.1, and their relation to WTASs. In Section 6.1 we prove certain properties of the matroids associated with such access structures. In Section 6.2 we characterize the intersection between HTASs and WTASs. Finally, in Section 6.3, we show that if an ideal WTAS has a minterm in the form of a prefix of U, then it is in fact an HTAS.

When discussing a HTAS on 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 $L(A) = i$.

6.1 The Matroid Associated with HTASs

Since any HTAS Γ_H is ideal [6, 35], Theorem 4.1 implies that there exists a matroid $\mathcal{M}$ that is associated with it. We derive herein some properties of such matroids that will be used later in our study of the structure of matroids corresponding to ideal WTASs.

Claim 6.1 *Let Γ_H and $\mathcal{M}$ be an HTAS and its associated matroid. Then every circuit of $\mathcal{M}$ not containing u_0 is a union of two distinct minterms.*

Proof: By Corollary 4.4, the circuits of the matroid $\mathcal{M}$ that do not contain u_0 are the union of two minterms of Γ_H, excluding users that are critical to that union. All that needs to be shown is that if M_1, M_2 are two minterms in Γ_H, no user in their union, $u \in M_1 \cup M_2$, is critical. Assume, without loss of generality, that $L(M_1) = i \leq L(M_2)$. Then, as M_1 is a minterm, we conclude that it satisfies the ith threshold condition with an equality, namely, M_1 has k_i users from $\bigcup_{j=i}^m L_j$. Hence, since $M_2 \subseteq \bigcup_{j=i}^m L_j$ and $M_2 \neq \emptyset$, the union $M_1 \cup M_2$ has at least $k_i + 1$ users from $\bigcup_{j=i}^m L_j$. Therefore, we can remove any user from $M_1 \cup M_2$ and still have an authorized set. Hence, no user $u \in M_1 \cup M_2$ is critical for the union. $\square$

Claim 6.2 *Let Γ_H and $\mathcal{M}$ be an HTAS and its associated matroid. Then U_{1,k_1+1} is a circuit of $\mathcal{M}$.*

Proof: Consider the two sets U_{1,k_1} and U_{2,k_1+1}. The first one is a minterm of Γ_H. Regarding the second, there are two options: either U_{2,k_1+1} is a minterm (satisfying the k_1-threshold condition), or it satisfies already the k_2-threshold condition (this may happen only if $|L_1| = \ell_2 - 1 = k_1 - k_2 + 1$, which is the minimal possible value for the size of that level). In both cases, U_{2,k_1+1} contains a minterm that includes u_{k_1+1}. Hence, U_{1,k_1+1} is a union of two distinct minterms and, therefore, by Corollary 4.5, it is dependent. We claim that it is actually a circuit. If not, then it must contain a circuit C of size smaller than $k_1 + 1$. By Claim 6.1, this circuit is a union of two minterms. Since its size is smaller than $k_1 + 1$, it must be a union of two minterms from levels L_2 and above. However, by Remark 3.2, $|L_1| \geq k_1 - k_2 + 1$, or, equivalently, $|U_{1,k_1+1}| - |L_1| \leq k_2$. This implies that the set U_{1,k_1+1} contains at most k_2 users from levels L_2 and above. Since any minterm from levels L_2 and above must be of size at least k_2, we infer that U_{1,k_1+1} can contain at most one minterm from those levels. This contradicts our earlier conclusion that it is a union of two minterms from those levels. We therefore conclude that C must be a circuit of $\mathcal{M}$. $\square$

6.2 The Intersection of WTASs and HTASs

Let U be a set of users and let Γ be a monotone access structure on 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 on U 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 on U. Our goal herein is to characterize such access structures that belong to those two classes of access structures.

It should be noted that in the following discussion we can not assume that the levels of U in the HTAS are nicely organized in a monotonic order as in (1).

We proceed with some notation. Let A_i, where $i \in [m-1]$, denote a subset of $k_i - k_{i+1}$ users of largest weights in L_i, and let A_m be a subset of $k_m - 1$ users of largest weights in L_m. We also let a_i denote a user of minimal weight in L_i, for all $i \in [m]$. Note that, by Remark 3.2, we have that $a_i \in L_i \setminus A_i$ for every $i \in [m]$.

We set $A = \bigcup_{i=1}^{m} A_i$ and $B = A_m \cup \{a_m\}$. The set A is unauthorized since it fails to satisfy each of the threshold conditions by exactly one user, while B is authorized since it is composed of k_m users of level L_m. Therefore $w(A) < T$ and $w(B) \geq T$. But as $B = A \cup \{a_m\} \setminus (A \setminus A_m)$, we infer that

$$w(A \setminus A_m) < w(a_m) \,. \tag{2}$$

We refer to the last level L_m in an HTAS as trivial if $k_m = 1$ (namely, all users of such a level are self-sufficient). We proceed to characterize access structures that are both WTAS and HTAS.

Lemma 6.3 *If the last level is not trivial, then the number of levels m in the HTAS is at most 2.*

Proof: Assume that $m \geq 3$ and that the last level is not trivial, i.e., $k_m \geq 2$. Let Z_m be a subset of $k_m - 2 \geq 0$ users of largest weight in L_m. Define $Z_{m-1} = A_{m-1} \cup \{a_{m-1}\}$ and $Z_{m-2} = A_{m-2} \cup \{a_{m-2}\}$. Their union $Z = Z_{m-2} \cup Z_{m-1} \cup Z_m$ is authorized since its cardinality is $|Z| = |A_{m-2}| + |A_{m-1}| + k_m = k_{m-2}$, and consequently, it satisfies the $(m-2)$th threshold condition.

Next, consider the set $B = Z \cup \{a_m\} \setminus (A_{m-1} \cup A_{m-2}) = Z_m \cup \{a_{m-2}, a_{m-1}, a_m\}$. Since, by (2), $w(A_{m-1} \cup A_{m-2}) < w(a_m)$, the definition of B implies that $w(B) > w(Z)$. Therefore, as Z is authorized, so is B. However, while B is authorized in the WTAS, it is unauthorized in the HTAS, as implied by the following inequalities: $|B \cap L_m| = |Z_m \cup \{a_m\}| = k_m - 1 < k_m$, $|B \cap (L_{m-1} \cup L_m)| = k_m < k_{m-1}$, and $|B| = k_m + 1 < k_{m-2}$. This contradiction implies that either $m \leq 2$ or the last level is trivial. $\square$

According to Lemma 6.3, access structures that are both WTAS and HTAS and have no self-sufficient users have a very simple hierarchical structure: either there is one level (in which case the access structure is a simple threshold access structure) or two levels. In the latter case, we show below that if the difference between k_1 and k_2 is larger than 1, the size of the first level is minimal (see Remark 3.2).

Lemma 6.4 *If the last level is not trivial, $m = 2$, and $k_1 - k_2 > 1$, then $|L_1| = k_1 - k_2 + 1$.*

Proof: Assume towards a contradiction that $|L_1| > k_1 - k_2 + 1$. Let Z_2 be a subset with $k_2 - 2$ users of largest weight in L_2 and $Z_1 = A_1 \cup \{b_1, b_2\}$, where b_1 and b_2 are two users in $L_1 \setminus A_1$ (note that our assumptions imply that Z_1 and Z_2 are well defined). Their union $Z = Z_1 \cup Z_2$ is authorized since $|Z| = k_1$. Next, consider the set $B = Z \cup \{a_2\} \setminus A_1 = Z_2 \cup \{a_2, b_1, b_2\}$. Since, by (2), $w(A_1) < w(a_2)$, we conclude that B is also authorized. Hence, it must be also authorized in the HTAS. However, as $|B \cap L_2| = k_2 - 1$ and $|B| = k_2 + 1 < k_1$, the set B is unauthorized in the HTAS. $\square$

Lemmas 6.3 and 6.4 imply that if Γ is an access structure on U that is both a WTAS and an HTAS, and U has no self-sufficient users (i.e., the last level in the HTAS is not trivial), then either $m = 1$ or $m = 2$, where in the latter case either $k_1 = k_2 + 1$ or $|L_1| = k_1 - k_2 + 1$. If, on the other hand, the access structure has self-sufficient users, i.e., the last level in the HTAS is trivial, then its restriction to the first $m-1$ levels is still a WTAS as well as an HTAS, and, in addition, that restriction has no self-sufficient users. This implies that the structure of that restriction is as described above. This is summarized as follows:

Claim 6.5 *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).*

To complete the characterization we proceed to prove the converse. Namely, that any HTAS with parameters as described in Claim 6.5 is also a WTAS. This is shown by constructing the appropriate weight function and threshold in each case.

Claim 6.6 *Let* Γ_H *be an HTAS that satisfies one of the conditions in Claim 6.5. Then there exist a weight function and a threshold such that* Γ_H *coincides with the corresponding WTAS.*

Proof: Case (1) is a simple threshold, so we can assign each user the weight 1, and set the threshold to k_1. In case (2), the weight assigned to every user in L_1 is k_2, the weight assigned to users in L_2 is k_1, and the threshold is $k_1 \cdot k_2$. In case (3), the weight assigned to users in L_1 and L_2 is 1 and $k_1 - k_2 + 1$, respectively, while the threshold is $k_2(k_1 - k_2 + 1)$. In case (4), we assign weights to the users in the first $m - 1$ levels and set an appropriate threshold according to the condition that is satisfied by the restriction of Γ_H to the first $m - 1$ levels and the rules that were described above for the first three cases; in addition, we assign to every user in the trivial level a weight that equals the threshold. In all four cases it is a straightforward matter to verify that the induced WTAS coincides with the original HTAS. $\square$

6.3 Ideal WTASs with a Prefix Minterm are HTASs

In this section we make the first step towards proving our main result, Theorem 3.5. Let Γ be an ideal WTAS on 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 5.1, 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 $\ell_{m+1} = n + 1$.

In addition, 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 $k_{m+1} = 1$. (Note that if u is the last element of the *last* k_i-long minterm and u' is the last element in the *first* k_{i+1}-long minterm then u and u' are consecutive elements.) An important observation regarding those subsets 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

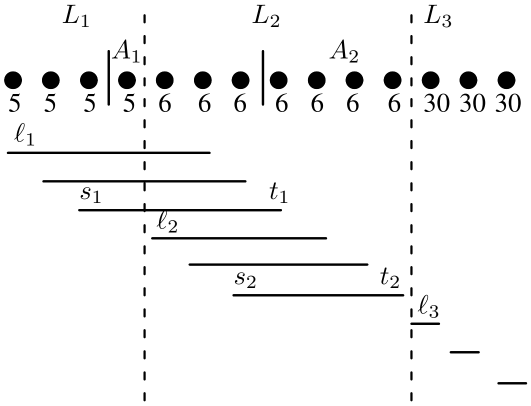

Figure 1: A WTAS that is also an HTAS.

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 Figure 1. The example in the illustration 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.

Next, we prove that the WTAS Γ coincides with the HTAS Γ_H described above.

Theorem 6.7 *Let Γ be an ideal WTAS on 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 of Γ that has a prefix which is a subset of A_i for some $i \in [m]$.

Assume, by contradiction, that there are such minterms, and let M' be the lexicographically minimal minterm of Γ 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 $u_h \in A_i$ for some $i \in [m]$, and we observed earlier that no run-minterm of Γ 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 $\hat{M} = U_{\ell_{i+1},t_i} \cup \{Z_{\min}\}$. As $w(\hat{M}) \geq w(U_{\ell_{i+1},t_i+1}) \geq T$, we conclude that $\hat{M} \in \Gamma$. But then 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 in Γ and, by Lemma 5.1, 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 of Γ, also M^* is a minterm of Γ. But M^* is a minterm of Γ that starts within A_i and $M^* \prec M'$, thus contradicting our choice of M'. Hence, by Corollary 4.5, 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, $A \notin \Gamma$, and the proof is thus complete. $\square$

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 $k \leq n$. Throughout this section 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 Section 8.2. The section is organized as follows: first we show that $U_{2,k}$ must be a minterm of Γ. Consequently, we show that Γ is one of the two tripartite access structure (TPASs) that were defined in Definition 3.3. Finally, in Section 7.1, we design linear ideal secret sharing schemes that realize TPASs.

Consider the set $U_{2,k}$. As $U_{2,k} = M \cup \{u_{d+1}\} \setminus \{u_1\}$ and $w(u_{d+1}) \geq w(u_1)$, the set $U_{2,k}$ is authorized. We proceed to show that it is in fact a minterm of Γ.

Claim 7.1 *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 $k \leq n$. Then if there exists a minterm that has u_2 as its minimal user, $U_{2,k}$ is a minterm of Γ.*

Proof: Let M' be the lexicographically minimal minterm starting with u_2. Assume towards a contradiction that the authorized set $U_{2,k}$ is not a minterm. The minterm M' cannot be a run-minterm since $U_{2,k-1}$ is unauthorized (as its weight does not exceed that of $M \setminus \{u_1\}$ which is a proper subset of the minterm M) and $U_{2,k}$ is already an authorized set (since $w(U_{2,k}) \geq w(M)$) that is not a minterm. Let s be the maximal index such that $U_{2,s} \subset M'$. In that case, as M' is not a run-minterm, $M' = U_{2,s} \cup Z$ where $Z \neq \emptyset$ and $u_{s+1} \prec Z_{\min}$. We claim that $s \leq k-2$. Assume, towards a contradiction, that $s \geq k-1$. Then $w(M') \geq w(U_{2,k-1}) + w(Z) \geq w(U_{2,k})$. However, as explained earlier, $U_{2,k}$ is an authorized subset that is not a minterm. Hence, if we remove from $U_{2,k}$ its minimal user – u_2 – we are left with a set that is still authorized. But M' weighs more than $U_{2,k}$ and it also contains u_2, whence also $M' \setminus \{u_2\}$ is authorized. But this contradicts the fact that M' is a minterm. We conclude that M' – the lexicographically minimal minterm starting with u_2 – takes the form $M' = U_{2,s} \cup Z$ where $s \leq k-2$ and Z is a non-empty set with $Z_{\min} \succ u_{s+1}$.

As Z is the canonical complement of $U_{2,s}$, Lemma 5.5 implies that the set $U_{2,s+1}$ is dependent. Hence, it contains a circuit C_1 of the corresponding matroid $\mathcal{M}$. The circuit C_1 must include the user u_{d+1} (the user that is missing in the minterm M), since, otherwise, as $s+1 \leq k-1$, the circuit C_1 would be a subset of the minterm $M = U_{1,d} \cup U_{d+2,k}$. We claim, and prove in the next paragraph, that $U_{1,d+1}$ is also a circuit of $\mathcal{M}$. Since $u_1 \in U_{1,d+1}$ but $u_1 \notin C_1$, the sets C_1 and $U_{1,d+1}$ are two distinct circuits. In addition, both circuits include u_{d+1}. Therefore, by Lemma 4.6, the set $C_1 \cup U_{1,d+1} \setminus \{u_{d+1}\}$ is dependent. However, this set is contained in the minterm $M = U_{1,d} \cup U_{d+2,k}$, which is an independent set of the matroid $\mathcal{M}$. This contradiction implies that $U_{2,k}$ is a minterm in Γ.

Hence, we need only to show that $U_{1,d+1}$ is a circuit of $\mathcal{M}$. Let $Y = U_{d+2,k}$, $X = U_{1,d+1}$ and consider $\Gamma_{Y,X}$, namely, the restriction of Γ induced by Y on X. By Lemma 4.11, it is an ideal WTAS, and $U_{1,d}$ is a prefix minterm in that access structure. Therefore, by Theorem 6.7, the access structure $\Gamma_{Y,X}$ is an HTAS, and, by Claim 6.2, the set $U_{1,d+1}$ is a circuit in the matroid corresponding to $\Gamma_{Y,X}$. By Lemma 5.5, applied with $P = U_{1,d}$, the set $U_{d+2,k}$ as the canonical complement of P, and $b = u_{d+1}$, the set $P \cup b = U_{1,d+1}$ is dependent in $\mathcal{M}$. Assume, by contradiction that it is not a circuit. Therefore, it possesses a proper subset $C' \subset U_{1,d+1}$ that is a circuit. By Lemma 4.12, the set C' would have to be dependent in the matroid corresponding to $\Gamma_{Y,X}$. But as $U_{1,d+1}$ is a circuit in that matroid, this is impossible. Hence, $U_{1,d+1}$ is also a circuit in $\mathcal{M}$. This completes the proof. $\square$

In view of the above, as we assume herein that there are minterms that start with u_2, we conclude that $U_{2,k}$ is a minterm. This is a prefix minterm in the restriction of Γ to $U_{2,n}$, denoted hereinafter Γ'. Since Γ' is ideal by Lemma 4.11, and a WTAS by Claim 4.13, and it has a prefix minterm, Theorem 6.7 implies that it is also an HTAS. Since we assumed that Γ has no self-sufficient users, then by Claim 6.5, the HTAS Γ' has at most two levels.

We separate our discussion to two cases, according to the number of levels in Γ'. First, we consider the case where Γ' is a simple threshold access structure.

Claim 7.2 *If Γ' is an HTAS of one level (i.e., it is a threshold access structure), then a set $X \subseteq U$ is in Γ if and only if $|X| \geq k-1$ and $|X \cap U_{d+2,n}| \geq k-1-d$.*

Proof: Let us begin with sets X that do not include the user u_1, namely, $X \subseteq U_{2,n}$. For such sets, the second threshold condition ($|X \cap U_{d+2,n}| \geq k-1-d$) is implied by the first one ($|X| \geq k-1$). Since we assumed that Γ', which is the restriction of Γ to $U_{2,n}$, is a simple threshold access structure, and the value of the threshold equals $|U_{2,k}| = k-1$, the statement is straightforward in this case.

Next, consider sets X such that $u_1 \in X$. If X satisfies the two conditions in the claim, then its weight is no less than the weight of $M = U_{1,d} \cup U_{d+2,k}$. As $w(M) \geq T$, we conclude that $X \in \Gamma$. Conversely, assume that $X \in \Gamma$ but it fails to satisfy one of the two conditions in the claim. Without loss of generality, we may assume that X is a minterm of Γ. Thus, by Lemma 5.3, $|X| = |M| = k-1$. Therefore, X may violate only the second condition in the claim, namely, $|X \cap U_{d+2,n}| < k-1-d$. But then $U_{1,d+1} \subset X$ and that cannot be since then $X \prec M = U_{1,d} \cup U_{d+2,k}$ and M was assumed to be the lexicographically minimal minterm in Γ. $\square$

The access structure that is described in Claim 7.2 is a tripartite access structure of type Δ_1 (see Definition 3.3) with

$$A = U_{1,d+1},\ B = U_{d+2,n-1},\ C = U_n,\ m = k-1,\ t = 2.$$

It should be noted that a set X belongs to Δ_1 if it satisfies at least one of two threshold conditions. The second condition is $|X \cap C| \geq t$, which, in our case, is an empty condition (as $|C| = 1 < t = 2$). Hence, that access structure is in fact *bipartite*, namely, the question whether X is authorized or not is determined only by the two numbers $|X \cap A|$ and $|X \cap (B \cup C)|$.

We are left with the case where Γ' is an HTAS of exactly two levels. Assume that $X \in \Gamma'$ if it has at least k_1 users from $U_{2,n}$ or at least k_2 users from $U_{r+1,n}$ for some $3 \leq r \leq n-2$. As $U_{2,k}$ is a minterm, $k_1 = k-1$.

Claim 7.3 *Under the above assumptions, a set $X \subseteq U$ is in Γ if and only if $|X \cap U_{r+1,n}| \geq k_2$ or both $|X| \geq k_1$ and $|X \cap U_{d+2,n}| \geq k_1 - d$.*

Proof: Assume first that $X \subseteq U$ satisfies one of the above two threshold conditions. If $|X \cap U_{r+1,n}| \geq k_2$ then $X \in \Gamma'$ and thus $X \in \Gamma$. If X satisfies the second condition then it also belongs to Γ since the set of minimal weight X that satisfies both $|X| \geq k_1$ and $|X \cap U_{d+2,n}| \geq k_1 - d$ is $X = M = U_{1,d} \cup U_{d+2,k}$, and $M \in \Gamma$.

Assume next that $X \in \Gamma$. Without loss of generality, we may assume that X is a minterm and prove that it satisfies one of the two threshold conditions in the claim. We separate the discussion into two cases. If $u_1 \notin X$ then $X \in \Gamma'$. Thus either $|X \cap U_{r+1,n}| \geq k_2$ or $|X| \geq k_1$. If $|X| \geq k_1$ then, as $u_1 \notin X$, it must be that $|X \cap U_{d+2,n}| \geq k_1 - d$. If, on the other hand, $u_1 \in X$, then by Lemma 5.3, we get that $|X| = k_1$. But then, since no minterm contains $U_{1,d+1}$, it must be that $|X \cap U_{d+2,n}| \geq k_1 - d$. □

The access structure Γ, as appears in Claim 7.3, coincides with one of the two TPASs in Definition 3.3. In case $r \geq d+1$, we set $A = U_{1,d+1}$, $B = U_{d+2,r}$, $C = U_{r+1,n}$ and then Γ is of type Δ_1,

$$\Gamma = \{X \subseteq U : (|X| \geq k_1 \text{ and } |X \cap (B \cup C)| \geq k_1 - d) \text{ or } |X \cap C| \geq k_2\}.$$

If, on the other hand, $r < d+1$, we claim that Γ is of type Δ_2. To that end, we set $A = U_{1,r}$, $B = U_{r+1,d+1}$, and $C = U_{d+2,n}$. By Claim 7.3, the structure of Γ is

$$\Gamma = \{X \subseteq U : (|X| \geq k_1 \text{ and } |X \cap C| \geq k_1 - d) \text{ or } |X \cap (B \cup C)| \geq k_2\}.$$

It remains to show that the size of the set B is bounded, in accord with Definition 3.3.

Claim 7.4 *If $r < d+1$, then $|B| < d + k_2 - k_1$.*

Proof: The access structure Γ', the restriction of Γ to $U_{2,n}$, is an HTAS of two levels. A set X is in Γ' if it has at least k_1 users from $U_{2,n}$ or at least k_2 users from $U_{r+1,n}$. Therefore, $U_{2,k} = U_{2,k_1+1}$ is a minterm and so is $U_{r+1,r+k_2}$. Consequently, $r + k_2 > k_1 + 1$ (since otherwise the second minterm would have been a proper subset of the first one). As $|B| = |U_{r+1,d+1}| = d + 1 - r$, we infer that $|B| < d + k_2 - k_1$. □

Example 7.5 Consider the set $U = \{u_1, \ldots, u_9\}$, and let Γ be a WTAS where the weights are 16, 16, 17, 18, 19, 24 ,24 ,24, and 24 and the threshold is 92. First note that there is no prefix minterm as $w(U_{1,5}) = 16 + 16 + 17 + 18 + 19 = 86 < 92$ and $w(U_{2,6}) = 16 + 17 + 18 + 19 + 24 = 94 \geq 92$, and thus $U_{1,6}$ is not a minterm. The lexicographically minimal minterm is $U_{1,3} \cup U_{5,6}$, and so $d = 3$ and $k = 6$. The HTAS structure resulting from the restriction of Γ to $U_{2,9}$ is composed of two levels $U_{2,5}$ and $U_{6,9}$, that is $r = 5$, with thresholds $k_1 = 5$ and $k_2 = 4$. Since $r > d+1$, the access structure is of type Δ_1. Setting $A = U_{1,4}$, $B = \{u_5\}$, and $C = U_{6,9}$, a set is authorized if it has at least 4 users from C, or if it has at least 5 users, where at least 2 of whom are from $B \cup C$.

We summarize this section in the next theorem.

Theorem 7.6 *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.*

7.1 Ideal Linear Secret Sharing Schemes for TPASs

We now turn to describe ideal linear secret sharing schemes that implement the TPASs Δ_1 and Δ_2 in Definition 3.3. Those schemes extend the ideas of the schemes that were presented in [25] for bipartite access structures. In fact, if we take $B = \emptyset$ then our schemes coincide with the schemes of [25].

Let us first briefly recall the definition of those access structures. Assume that $|U| = n$ and $U = A \cup B \cup C$, where A, B, and C are disjoint, and $A, C \neq \emptyset$. Let $m, d, t \in \mathbb{N}$ be positive integers such that $m \geq t$. Then

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

and

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

where in Δ_2 the size of B is restricted to $|B| \leq d + t - m$.

Let $\mathbb{F}$ be a sufficiency large finite field. For a $\lambda \in \mathbb{F}$ and an integer s define the Vandermonde vector $\mathbf{V}_s(\lambda) := (1, \lambda, \lambda^2, \ldots, \lambda^{s-1})$ (for clarity, we denote hereinafter all vectors with bold-faced letters). Recall that for any set $A \subseteq \mathbb{F}$ if $|A| \leq s$ then the vectors $\{\mathbf{V}_s(\lambda) : \lambda \in A\}$ are linearly independent. Thus, for any set $A \subseteq \mathbb{F}$ if $|A| \geq s$, the vectors $\{\mathbf{V}_s(\lambda) : \lambda \in A\}$ span the entire space $\mathbb{F}^s$. Let $E = \mathbb{F}^m$ and E_1 and E_2 be subspaces of E of dimensions d and t, respectively, such that if $d + t \geq m$ then $E = E_1 + E_2$, otherwise $E_1 \cap E_2 = \{\vec{0}\}$. Denote $r = \dim(E_1 \cap E_2) = \max(0, d + t - m)$. If $r > 0$, let $\Lambda = \{\lambda_1, \ldots, \lambda_r\}$ be a set of elements from $\mathbb{F}$, otherwise $\Lambda = \emptyset$. Let

$$\boldsymbol{\varphi}_1 : \mathbb{F}^d \to E_1 \text{ and } \boldsymbol{\varphi}_2 : \mathbb{F}^t \to E_2$$

be two isomorphisms such that

$$\boldsymbol{\varphi}_1(\mathbf{V}_d(\lambda_i)) = \boldsymbol{\varphi}_2(\mathbf{V}_t(\lambda_i)) \quad \forall \lambda_i \in \Lambda\ . \tag{3}$$

Finally, we define the functions $\mathbf{a} : \mathbb{F} \to E_1$ and $\mathbf{b} : \mathbb{F} \to E_2$ as follows:

$$\mathbf{a}(\lambda) = \boldsymbol{\varphi}_1(\mathbf{V}_d(\lambda)) \text{ and } \mathbf{b}(\lambda) = \boldsymbol{\varphi}_2(\mathbf{V}_t(\lambda)) \qquad \forall \lambda \in \mathbb{F}\ .$$

The target vector in the ideal linear secret sharing schemes that we construct below is $\mathbf{b}(\lambda_T)$ for some $\lambda_T \in \mathbb{F} \backslash \Lambda$. Note that the target vector is in $E_2 \backslash E_1$.

Next, we describe the function $\boldsymbol{\eta} : U \to E$ that assigns vectors from E to users in U, so that the vectors of authorized subsets span the target vector, while the vectors of unauthorized subsets do not, i.e., $\mathbf{b}(\lambda_T) \in \text{span}\{\boldsymbol{\eta}(S)\}$ iff $S \in \Gamma$. By Theorem 2.5, this implies that the scheme realizes Γ. The technique we use is similar for both types of access structures, $\Gamma = \Delta_1$ and $\Gamma = \Delta_2$. We assign the vectors to users one at a time and prove correctness by induction. Assume that we already assigned vectors to all users in $U' \subset U$ and that we wish to find a proper assignment of a vector to an additional user $u \in U \setminus U'$. We shall denote this stage in the assignment by $\langle U', u \rangle$. The goal is to find an assignment $\boldsymbol{\eta}(u)$ of a vector, so that the following conditions hold:

C1. If $S \subseteq U'$, $S \notin \Gamma$ but $S' := S \cup \{u\} \in \Gamma$, then $\boldsymbol{\eta}(u)$ should be such that $\mathbf{b}(\lambda_T) \in \text{span}\{\boldsymbol{\eta}(S')\}$.

C2. If $S \subseteq U'$, $S \notin \Gamma$ and $S' := S \cup \{u\} \notin \Gamma$, then $\boldsymbol{\eta}(u)$ should be such that $\mathbf{b}(\lambda_T) \notin \text{span}\{\boldsymbol{\eta}(S')\}$.

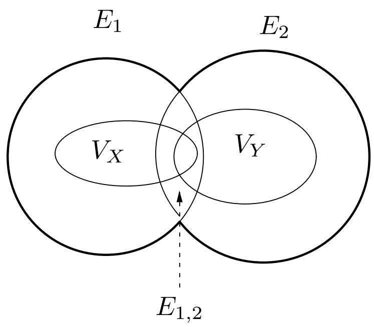

Figure 2: The linear spaces in the proof of Lemma 7.7.

We shall always look for the vector $\boldsymbol{\eta}(u)$ in a single-parameterized family of vectors $\{\boldsymbol{\zeta}(\lambda) \in E : \lambda \in \mathbb{F}\}$ (in the constructions that we present here, $\boldsymbol{\zeta}(\lambda)$ is one of $\mathbf{a}(\lambda)$, $\mathbf{b}(\lambda)$, and $\mathbf{V}_m(\lambda)$). Using Lemma 7.7 below, we shall show that at each stage of the assignment, $\langle U', u\rangle$, and for every $S \subseteq U'$, where $S \notin \Gamma$, there are finitely many bad choices of the parameter λ that give rise to vectors $\boldsymbol{\eta}(u) = \boldsymbol{\zeta}(\lambda)$ that would violate the relevant condition above. Hence, since $|2^{U'} \setminus \Gamma|$ is bounded, there exists a good choice of λ such that $\boldsymbol{\eta}(u) = \boldsymbol{\zeta}(\lambda)$ satisfies all necessary conditions, provided that the field is sufficiently large. Thus, in the rest of the proof we bound the number of bad values for a specific set S.

Similarly to [25], it can be verified that the size of the field that our schemes require, which is the size of the domain of secrets and shares, is $2^{O(n)}$.

Lemma 7.7 *Let $X \subseteq \mathbb{F}$ and $Y \subseteq \mathbb{F}\backslash\Lambda$ be such that $|X| < d$ and $|X|+|Y| < m$. Let $V = \text{span}\{\mathbf{a}(x), \mathbf{b}(y) : x \in X, y \in Y\}$. Then $E_1\backslash V \neq \emptyset$.*

Proof: Hereinafter, let $V_X = \text{span}\{\mathbf{a}(x) : x \in X\}$, $V_Y = \text{span}\{\mathbf{b}(y) : y \in Y\}$, and $E_{1,2} = E_1 \cap E_2$ (see Figure 2 for an illustration of those linear spaces) . Let us begin with the fairly easy case when $m \geq d+t$. In that case, since $E_1 \cap E_2 = \{\vec{0}\}$, we claim that $V \cap E_1 = V_X$, whence $\dim(E_1\backslash V) = \dim E_1 - \dim V_X = d - |X| > 0$. Indeed, let $\mathbf{u}$ be an arbitrary vector from $V \cap E_1$. Then, on one hand, $\mathbf{u} = \mathbf{v}_x + \mathbf{v}_y$ for some $\mathbf{v}_x \in V_X$ and $\mathbf{v}_y \in V_Y$, and on the other hand $\mathbf{u} \in E_1$. Therefore, $\mathbf{v}_y = \mathbf{u} - \mathbf{v}_x \in E_1 - V_X = E_1$. But since $\mathbf{v}_y \in V_Y \subseteq E_2$ and $E_1 \cap E_2 = \{\vec{0}\}$, we infer that $\mathbf{v}_y = \vec{0}$. This implies that $\mathbf{u} = \mathbf{v}_x \in V_X$.

Next, we prove the claim for the case where $r = d + t - m > 0$. Without loss of generality, we may assume that $|Y| = t - k$ for some $0 \leq k \leq r$. Indeed, if $|Y| > t$ it may be reduced to $Y^- \subset Y$ of size $|Y^-| = t$ without affecting V. If, on the other hand, $|Y| < t - r$, it may be extended to a superset $Y^+ \supset Y$ of size $|Y^+| = t - r$. Since $|X| + |Y^+| < d + t - r = m$, we may prove the statement for X and Y^+ and then infer that it also holds for X and Y.

Assume, towards a contradiction, that $E_1 \subseteq V$, whence $\dim(V \cap E_1) = \dim E_1 = d$. We claim that this assumption implies the following two statements:

$$\dim(V_Y \cap E_{1,2}) = r - k \quad \text{and} \quad \dim(V_X \cap E_{1,2}) < k\ . \tag{4}$$

After proving these two statements, we may derive the sought-after contradiction as follows. Since we assumed that $E_1 \subseteq V = V_X + V_Y$, all vectors $e \in E_{1,2}$ may be expressed as $e = x + y$ where $x \in V_X$ and $y \in V_Y$. But since $\dim E_{1,2} = r > \dim(V_X \cap E_{1,2}) + \dim(V_Y \cap E_{1,2})$, as implied by the two statements in (4), there exists at least one vector $e \in E_{1,2}$, such that $e = x + y$, for which either $x \in E_1\backslash E_2$ or

$y \in E_2 \backslash E_1$. Without loss of generality, we assume that $x \in E_1 \backslash E_2$. But then $x = e - y \in E_{1,2} + V_Y \subseteq E_2$, as opposed to our assumption that $x \notin E_2$.

Next, we prove the statements in (4). Let us begin with the equality in (4). The dimension of $E_{1,2} + V_Y$ is t since the $t-k$ base vectors of V_Y, namely $\{\mathbf{b}(y) : y \in Y\}$, may be extended to a full basis of E_2 by any k base vectors of $E_{1,2}$ of the form $\mathbf{b}(\lambda)$, $\lambda \in \Lambda$ (recall that $|\Lambda| = r \geq k$ and that $Y \subset \mathbb{F} \setminus \Lambda$). Therefore,

$$\dim(V_Y \cap E_{1,2}) = \dim V_Y + \dim E_{1,2} - \dim(E_{1,2} + V_Y) = (t-k) + r - t = r - k \ .$$

In order to prove the inequality in (4), we first prove that

$$\dim(V_X + E_{1,2}) = d. \tag{5}$$

Since $V_X + E_{1,2} \subseteq E_1$ and $\dim E_1 = d$, all we need to show is that $E_1 \subseteq V_X + E_{1,2}$. We assumed that $E_1 \subseteq V = V_X + V_Y$. Hence, for each $e \in E_1$ there exist $x \in V_X$ and $y \in V_Y$ such that $e = x + y$. But then $y = e - x \in E_1 + V_X = E_1$. Since $y \in V_Y \subset E_2$ we conclude that $y \in E_{1,2}$. This implies that $e \in V_X + E_{1,2}$, whence we arrive at the required conclusion that $E_1 \subseteq V_X + E_{1,2}$. Finally, the inequality in (4) is a straightforward consequence of (5). Indeed,

$$\dim(V_X \cap E_{1,2}) = \dim V_X + \dim E_{1,2} - \dim(V_X + E_{1,2}) = |X| + r - d \ ;$$

recalling that $|X| < m - |Y| = m - t + k$ and $r = t + d - m$ we infer that $\dim(V_X \cap E_{1,2}) < k$. That concludes the proof. $\square$

7.1.1 Realizing Δ_1

Here, Γ is an access structure of type Δ_1. We assign the vectors in three stages. We first describe the assignment $\boldsymbol{\eta}(u)$ for all $u \in C$, then for $u \in A$ and finally for $u \in B$.

Step 1: Assigning vectors to users in C. Let $C = \{c_i\}_{1 \leq i \leq |C|}$, and let γ_i, where $1 \leq i \leq |C|$, be distinct elements of $\mathbb{F} \backslash \Lambda$, all different from λ_T. Then

$$\boldsymbol{\eta}(c_i) = \mathbf{b}(\gamma_i) \qquad 1 \leq i \leq |C| \ .$$

This is essentially the Shamir t-out-of-$|C|$ scheme. Therefore, every t users in C can reconstruct $\mathbf{b}(\lambda_T)$ while no $t-1$ users can.

Step 2: Assigning vectors to users in A. Let $A = \{a_i\}_{1 \leq i \leq |A|}$. Our claim is that, assuming $\mathbb{F}$ is large enough, we may find $\alpha_i \in \mathbb{F}$, where $1 \leq i \leq |A|$, so that the assignment $\boldsymbol{\eta}(a_i) = \mathbf{a}(\alpha_i)$ is consistent with Γ, restricted to $A \cup C$, and, in addition, for any $S \subseteq A \cup C$ where $S \notin \Gamma$, the following equality holds,

$$\dim \operatorname{span}\{\boldsymbol{\eta}(S)\} = |S \cap (B \cup C)| + \min(|S \cap A|, d) \ . \tag{6}$$

(Herein, we could have replaced $S \cap (B \cup C)$ with $S \cap C$ since S does not include users from B.) Namely, whenever we augment an unauthorized set $S \subseteq A \cup C$ with an additional user from A, the dimension of the corresponding subspace that is spanned by the vectors owned by S increases by 1, up to a limit of d users from A (i.e., all users from A beyond the first d ones are redundant). Using (6) we guarantee that if $S \in \Gamma$ and $|S \cap C| < t$ then the vectors assigned to S span E, and in particular, span the target vector $\mathbf{b}(\lambda_T)$. We shall prove this claim by induction. Assume that we already assigned vectors to $A_{1,j} := \{a_1, \ldots, a_j\}$ for some $0 \leq j < |A|$, so that Γ is respected and (6) holds for all $S \in 2^{U'} \backslash \Gamma$, where $U' = A_{1,j} \cup C$. This assumption is obviously true for $j = 0$. We proceed to look for an assignment $\boldsymbol{\eta}(a_{j+1}) = \mathbf{a}(\alpha_{j+1})$ for the next user from A so that conditions *C1* and *C2* hold for all $S \in 2^{U'} \setminus \Gamma$ (in order to keep respecting Γ) and equality (6) holds for all $S \in 2^{U' \cup \{a_{j+1}\}} \backslash \Gamma$. As explained earlier, it suffices to concentrate on a single set $S \in 2^{U'} \setminus \Gamma$ and bound the number of bad choices of $\alpha_{j+1} \in \mathbb{F}$ for that specific set.

Let $S \in 2^{U'} \backslash \Gamma$ be such that $S' := S \cup \{a_{j+1}\} \in \Gamma$. Since $|S'| = |S|+1$ but $|S' \cap (B \cup C)| = |S \cap (B \cup C)|$, the fact that $S \notin \Gamma$ and $S' \in \Gamma$ implies that $|S| = m - 1$ and $|S \cap (B \cup C)| \geq m - d$. This, in turn, implies that $|S \cap A_{1,j}| < d$. Therefore, by Lemma 7.7, applied to $X = \{\alpha_i\}_{1 \leq i \leq j}$ and $Y = \{\gamma_i\}_{1 \leq i \leq |C|}$, the vectors owned by S span a subspace of E_1 of dimension $d - 1$ at the most. Hence, for all but at most $d - 1$ values of $\alpha_{j+1} \in \mathbb{F}$, we have $\dim \operatorname{span}\{\boldsymbol{\eta}(S')\} = \dim \operatorname{span}\{\boldsymbol{\eta}(S)\} + 1$. Now, by the induction hypothesis, the set S satisfies equality (6). Therefore, since $|S \cap A| = |S \cap A_{1,j}| < d$, we get that

$$\dim \operatorname{span}\{\boldsymbol{\eta}(S)\} = |S \cap C| + \min(|S \cap A|, d) = |S \cap C| + |S \cap A| = |S| = m - 1 .$$

This implies that $\dim \operatorname{span}\{\boldsymbol{\eta}(S')\} = m = \dim E$ so that $\mathbf{b}(\lambda_T) \in \operatorname{span}\{\boldsymbol{\eta}(S')\}$ and *C1* holds.

Let $S \in 2^{U'} \setminus \Gamma$ be such that $S' := S \cup \{a_{j+1}\} \notin \Gamma$. If $|S \cap A_{1,j}| \geq d$, then $\operatorname{span}\{\boldsymbol{\eta}(S')\} = \operatorname{span}\{\boldsymbol{\eta}(S)\}$ for any choice of α_{j+1}; hence, no matter how we chose α_{j+1} in this case, the augmented set S' will remain incapable of spanning the target vector. Also, since any d vectors of the form $\mathbf{a}(\alpha_i)$ span the same subspace E_1, any choice of α_{j+1} will result with an assignment that keeps respecting equality (6).

Hence, we restrict our attention to subsets $S \in 2^{U'} \setminus \Gamma$ for which $|S \cap A_{1,j}| < d$. We claim that in this case $|S| \leq m - 2$. Assume, by contradiction, that $|S| \geq m - 1$. As $|S \cap A_{1,j}| < d$ we infer that $|S \cap C| \geq m - d$. Since $|S' \cap C| = |S \cap C| \geq m - d$ and $|S'| = |S| + 1 \geq m$, we infer that $S' \in \Gamma$, as opposed to our assumption. Hence, $|S| \leq m - 2$. Our goal is to find α_{j+1} so that the target vector is not in $\operatorname{span}\{\boldsymbol{\eta}(S')\}$ (in order to keep respecting Γ) and that equality (6) still holds for all $S \in 2^{U'} \backslash \Gamma$. Concentrating on the first part of our mission, we want to find α_{j+1} so that $\mathbf{a}(\alpha_{j+1}) \notin \operatorname{span}\{\boldsymbol{\eta}(S) \cup \{\mathbf{b}(\lambda_T)\}\}$. By Lemma 7.7, for $X = \{\alpha_i\}_{1 \leq i \leq j}$ and $Y = \{\gamma_i\}_{1 \leq i \leq |C|} \cup \{\lambda_T\}$, the space $\operatorname{span}\{\boldsymbol{\eta}(S) \cup \{\mathbf{b}(\lambda_T)\}\} \cap E_1$ is a subspace of E_1 of dimension $d - 1$ at the most. We infer that for all but possibly $d - 1$ values of $\alpha_{j+1} \in \mathbb{F}$, the vector $\mathbf{a}(\alpha_{j+1})$ increases the dimension of $\operatorname{span}\{\boldsymbol{\eta}(S) \cup \{\mathbf{b}(\lambda_T)\}\}$ by 1. It is easy to see that for all such selections, we get an assignment that will also respect equality (6). This completes the proof that a proper assignment of vectors exists for all users in $A \cup C$. We are ready to proceed to the third and final stage in the assignment.

Step 3: Assigning vectors to users in B. Here we assign vectors to the users in B (note that B may be empty). Let $B = \{b_i\}_{1 \leq i \leq |B|}$. As before, we claim that, provided $\mathbb{F}$ is large enough, there exist $\beta_i \in \mathbb{F}$, where $1 \leq i \leq |B|$, so that the assignment $\boldsymbol{\eta}(b_i) = \mathbf{V}_m(\beta_i)$ is consistent with Γ, and, in addition, for any $S \notin \Gamma$, equality (6) holds. Namely, whenever we augment an unauthorized set S with an additional user from B, the corresponding subspace that is spanned by the vectors owned by S increases by 1. We shall prove this claim by induction. Assume that we already assigned vectors to $B_{1,j} := \{b_1, \ldots, b_j\}$ for some $0 \leq j < |B|$, so that Γ is respected and (6) holds for all $S \in 2^{U'} \backslash \Gamma$, where $U' = B_{1,j} \cup A \cup C$. This assumption is obviously true for $j = 0$. Next, we look for an assignment for the next user from B, that is $\boldsymbol{\eta}(b_{j+1}) = \mathbf{V}_m(\beta_{j+1})$, so that conditions *C1* and *C2* hold for all $S \in 2^{U'} \setminus \Gamma$ (in order to keep respecting Γ) and equality (6) holds for all $S \in 2^{U' \cup \{b_{j+1}\}} \backslash \Gamma$. Again, we concentrate on a single set $S \in 2^{U'} \setminus \Gamma$ and bound the number of bad choices of $\beta_{j+1} \in \mathbb{F}$ for that specific set.

Let $S \in 2^{U'} \setminus \Gamma$ be such that $S' := S \cup \{b_{j+1}\} \in \Gamma$. Since $S \notin \Gamma$ but $S' \in \Gamma$, and the added user b_{j+1} is from B, we conclude that while S fails to satisfy the first of the two threshold conditions in the definition of Δ_1, i.e., $|S| < m$ or $|S \cap (B \cup C)| < m - d$, the set S' does satisfy that condition, namely, $|S'| \geq m$

and $|S' \cap (B \cup C)| \geq m - d$. There are two cases to consider here, according to which of the two threshold conditions were violated by S:

1. $|S| = m - 1$.
2. $|S| \geq m$ but $|S \cap (B \cup C)| = m - d - 1$.

In the first case, we claim that $|S \cap A| \leq d$. Indeed, since $|S' \cap (B \cup C)| \geq m - d$ and $|S' \cap (B \cup C)| = |S \cap (B \cup C)| + 1$, we have $|S \cap (B \cup C)| \geq m - d - 1$, whence $|S \cap A| = |S| - |S \cap (B \cup C)| \leq (m - 1) - (m - d - 1) = d$. Applying the induction hypothesis to S, we get by equality (6) that

$$\dim \operatorname{span}\{\boldsymbol{\eta}(S)\} = |S \cap (B \cup C)| + \min(|S \cap A|, d) = |S \cap (B \cup C)| + |S \cap A| = |S| = m - 1 \, .$$

Therefore, for all but $m - 1$ values of β_{j+1}, we get that $\dim \operatorname{span}\{\boldsymbol{\eta}(S')\} = \dim \operatorname{span}\{\boldsymbol{\eta}(S)\} + 1 = m$, whence $\mathbf{b}(\lambda_T) \in \operatorname{span}\{\boldsymbol{\eta}(S')\}$.

Next, we show how to reduce the second case to the first case. In the second case $|S \cap A| = |S| - |S \cap (B \cup C)| \geq m - (m - d - 1) = d + 1$. Hence, S includes too many users from A, since for all $a \in A$, the vector $\boldsymbol{\eta}(a)$ is chosen from the d-dimensional space E_1. Let $a \in S \cap A$ and define $S_1 = S \setminus \{a\}$ and $S_1' = S_1 \cup \{b_{j+1}\}$. Obviously, $S_1 \notin \Gamma$ and, as can be easily verified, $S_1' \in \Gamma$. Since $\operatorname{span}\{\boldsymbol{\eta}(S)\} = \operatorname{span}\{\boldsymbol{\eta}(S_1)\}$ and $\operatorname{span}\{\boldsymbol{\eta}(S')\} = \operatorname{span}\{\boldsymbol{\eta}(S_1')\}$, if β_{j+1} is chosen properly for S_1, it will be also an appropriate choice for S. Hence, we may repeat this reduction stage until we reach a set S_1 of size $|S_1| = m - 1$, and then apply the arguments of the first case to conclude that all but $m - 1$ values of β_{j+1} are appropriate choices.

Let $S \in 2^{U'} \setminus \Gamma$ be such that $S' := S \cup \{b_{j+1}\} \notin \Gamma$. Arguing along the same lines as above, we may assume, without loss of generality, that $|S \cap A| \leq d$, since any d members of A span E_1. We claim that $|S| \leq m - 2$. Indeed, if $|S| \geq m - 1$ then $|S \cap (B \cup C)| \geq m - 1 - d$, as $|S \cap A| \leq d$. This implies that $|S' \cap (B \cup C)| \geq m - d$ and $|S'| \geq m$, whence $S' \in \Gamma$, in a contradiction to our assumption. Therefore, the dimension of $\operatorname{span}\{\boldsymbol{\eta}(S) \cup \{\mathbf{b}(\lambda_T)\}\}$ is at most $m - 2 + 1$. Consequently, for all but possibly $m - 1$ values of $\beta_{j+1} \in \mathbb{F}$, we have $\mathbf{V}_m(\beta_{j+1}) \notin \operatorname{span}\{\boldsymbol{\eta}(S) \cup \{\mathbf{b}(\lambda_T)\}\}$. Hence, for all but possibly $m - 1$ values of $\beta_{j+1} \in \mathbb{F}$, we get that $\mathbf{b}(\lambda_T) \notin \operatorname{span}\{\boldsymbol{\eta}(S) \cup \{\mathbf{V}_m(\beta_{j+1})\}\}$. Clearly, all such selections yield assignments that respect equality (6).

This concludes the description of the assignment $\boldsymbol{\eta} : U \rightarrow E$ and the proof that it yields an ideal linear sharing scheme that realizes a given access structure Γ of type Δ_1.

7.1.2 Realizing Δ_2

Here we propose an ideal linear secret sharing scheme for access structures Γ that are a TPAS of type Δ_2. Recall that, by Definition 3.3, in such access structures $|B| \leq |\Lambda| = r = d + t - m$. We concentrate on cases where $r > 0$ (if $r = 0$ then $B = \emptyset$ and then we get a bipartite access structure).

Step 1: Assigning vectors to users in $B \cup C$. The users in B and C are assigned distinct vectors of the form $\mathbf{b}(\beta_i)$ and $\mathbf{b}(\gamma_i)$, respectively, where $\{\beta_i\}_{1 \leq i \leq |B|} \subset \Lambda$ and $\{\gamma_i\}_{1 \leq i \leq |C|} \subset \mathbb{F} \setminus (\Lambda \cup \{\lambda_T\})$. Clearly, any t users from $B \cup C$ may reconstruct $\mathbf{b}(\lambda_T)$ while no $t - 1$ users can.

Step 2: Assigning vectors to users in A. Let $A = \{a_i\}_{1 \leq i \leq |A|}$. Our claim is that, assuming $\mathbb{F}$ is large enough, we may find $\alpha_i \in \mathbb{F}$, where $1 \leq i \leq |A|$, so that the assignment $\boldsymbol{\eta}(a_i) = \mathbf{a}(\alpha_i)$ is consistent with Γ, and, in addition, for any $S \subseteq U$ where $S \notin \Gamma$, the following equality holds,

$$\dim \operatorname{span}\{\boldsymbol{\eta}(S)\} = |S \cap C| + \min(|S \cap (A \cup B)|, d) \, . \tag{7}$$

We shall prove this claim by induction. Assume that we already assigned vectors to $A_{1,j} := \{a_1, \ldots, a_j\}$ for some $0 \le j < |A|$, so that Γ is respected and (7) holds for all $S \in 2^{U'} \setminus \Gamma$, where $U' = A_{1,j} \cup B \cup C$. This assumption is true for $j = 0$ since then, on one hand, $\dim \operatorname{span}\{\boldsymbol{\eta}(S)\} = |S|$, while on the other hand $S \cap A = \emptyset$ and $|S \cap B| \le |B| \le d + t - m \le d$. We proceed to look for an assignment $\boldsymbol{\eta}(a_{j+1}) = \mathbf{a}(\alpha_{j+1})$ for the next user from A, so that conditions *C1* and *C2* hold for all $S \in 2^{U'} \setminus \Gamma$ and equality (7) holds for all $S \in 2^{U' \cup \{a_{j+1}\}} \setminus \Gamma$.

Let $S \in 2^{U'} \setminus \Gamma$ be such that $S' := S \cup \{a_{j+1}\} \in \Gamma$. We infer that $|S| = m - 1$ and $|S \cap C| \ge m - d$. This implies that $|S \cap (A \cup B)| = |S| - |S \cap C| \le d - 1$. By Lemma 7.7, applied to $X = \{\alpha_i\}_{1 \le i \le j} \cup \{\beta_i\}_{1 \le i \le |B|}$ and $Y = \{\gamma_i\}_{1 \le i \le |C|}$ (here we use the fact that $\beta_i \in \Lambda$ so that, in view of (3), $\mathbf{a}(\beta_i) = \mathbf{b}(\beta_i)$), the vectors owned by S span a subspace of E_1 of dimension $d - 1$ at the most. Hence, for all but $d - 1$ values of $\alpha_{j+1} \in \mathbb{F}$, $\dim \operatorname{span}\{\boldsymbol{\eta}(S')\} = \dim \operatorname{span}\{\boldsymbol{\eta}(S)\} + 1$. Now, by the induction hypothesis, the set S satisfies equality (7). Therefore, since $|S \cap (A \cup B)| < d$, we get that

$$
\begin{aligned}
\dim \operatorname{span}\{\boldsymbol{\eta}(S)\} &= |S \cap C| + \min(|S \cap (A \cup B)|, d) \\
&= |S \cap C| + |S \cap (A \cup B)| = |S| \ = \ m - 1.
\end{aligned}
$$

This implies that $\dim \operatorname{span}\{\boldsymbol{\eta}(S')\} = m$ so that $\mathbf{b}(\lambda_T) \in \operatorname{span}\{\boldsymbol{\eta}(S')\}$.

Let $S \in 2^{U'} \setminus \Gamma$ be such that $S' := S \cup \{a_{j+1}\} \notin \Gamma$. There are two cases to consider here. If $|S \cap (A \cup B)| \ge d$, then any choice of α_{j+1} is good. This is because, in view of (3), the vectors given to users in B are $\mathbf{b}(\beta_i) = \mathbf{a}(\beta_i)$ where $\beta_i \in \Lambda$, and, consequently, if $|S \cap (A \cup B)| \ge d$, the vectors held by the users of S already span all of E_1. Hence, for any choice of α_{j+1}, $\operatorname{span}\{\boldsymbol{\eta}(S')\} = \operatorname{span}\{\boldsymbol{\eta}(S)\}$ and S' will still satisfy equality (7).

This leaves us with the case $|S \cap (A \cup B)| < d$. In that case $|S| \le m - 2$ (since if $|S| \ge m - 1$ then $|S \cap C| = |S| - |S \cap (A \cup B)| \ge m - d$ and $|S'| = |S| + 1 \ge m$, and consequently, S' would have been authorized). Our goal is to find α_{j+1} so that the target vector is not in $\operatorname{span}\{\boldsymbol{\eta}(S')\}$ (in order to keep respecting Γ) and that equality (7) still holds. Concentrating on the first part of our mission, we want to find α_{j+1} so that $\mathbf{a}(\alpha_{j+1}) \notin \operatorname{span}\{\boldsymbol{\eta}(S) \cup \{\mathbf{b}(\lambda_T)\}\}$. By Lemma 7.7, for $X = \{\alpha_i\}_{1 \le i \le j} \cup \{\beta_i\}_{1 \le i \le |B|}$ and $Y = \{\gamma_i\}_{1 \le i \le |C|} \cup \{\lambda_T\}$, the space $\operatorname{span}\{\boldsymbol{\eta}(S) \cup \{\mathbf{b}(\lambda_T)\}\} \cap E_1$ is a subspace of E_1 of dimension $d - 1$ at the most. Hence, for all but possibly $d - 1$ values of $\alpha_{j+1} \in \mathbb{F}$, the vector $\mathbf{a}(\alpha_{j+1})$ increases the dimension of $\operatorname{span}\{\boldsymbol{\eta}(S) \cup \{\mathbf{b}(\lambda_T)\}\}$ by 1. It is easy to see that for all such selections, we get an assignment that will also respect equality (7).

8 A Recursive Characterization of Ideal WTASs by Means of Composition

In this section we show that if Γ is an ideal WTAS that is not one of the structures that we identified in Sections 6.3 and 7, namely, an HTAS or a TPAS, then it is a composition of two ideal WTASs that are defined on smaller sets of users. By doing so, we obtain a recursive characterization of ideal WTASs.

8.1 WTASs and Composition of Access Structures

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

Lemma 8.1 *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 on 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.

Proof: Assume that Γ_1 and Γ_2 are ideal. We show that Γ is ideal by describing an ideal secret sharing scheme that realizes it. Given a secret s, we share it among the users of U_1 using an ideal secret sharing scheme for Γ_1. Then, if s_1 is the share of u_1 in that scheme, we share it among the users of U_2 using an ideal secret sharing scheme for Γ_2. The resulting scheme is clearly ideal, and its correctness and perfect security stem from the correctness and perfect security of the two schemes for Γ_1 and Γ_2. It is easy to verify that if both secret sharing schemes for Γ_1 and for Γ_2 are linear, then so is the resulting scheme for Γ.

Conversely, suppose that Γ is ideal. Let $M \subset U$ be a minterm of Γ and let $M = M_1 \cup M_2$ where $M_1 = M \cap (U_1 \setminus \{u_1\})$ and $M_2 = M \cap U_2$. We choose M for which $M_2 \neq \emptyset$ (since u_1 is not redundant in Γ_1 and $\Gamma_2 \neq \emptyset$ such a minterm exists). By Definition 3.4, $M \in \Gamma$ if and only if $M_1 \cup \{u_1\} \in \Gamma_1$ and $M_2 \in \Gamma_2$. Furthermore,

$$M_1 \cup M_2' \in \Gamma \text{ iff } M_2' \in \Gamma_2 \quad \text{and} \quad M_1' \cup M_2 \in \Gamma \text{ iff } M_1' \cup \{u_1\} \in \Gamma_1 \, . \tag{8}$$

From the first observation above we conclude that Γ_2 coincides with Γ_{M_1,U_2} – the restriction of Γ that M_1 induces on U_2. Since by Lemma 4.11 any restriction of an ideal access structure is ideal, we infer that Γ_2 is ideal. As for Γ_1, let x be an arbitrary element of M_2, let $U' = U_1 \setminus \{u_1\} \cup \{x\}$, and consider the restriction

$$\Gamma' := \Gamma_{M_2\setminus\{x\},U'} = \{Q \subseteq U' : (M_2 \setminus \{x\}) \cup Q \in \Gamma\}.$$

We claim, and prove below, that Γ' is isomorphic to Γ_1 under the natural bijection from 2^{U_1} to $2^{U'}$ (i.e., $A \subseteq U_1$ is mapped to $A' := A\setminus\{u_1\} \cup \{x\} \in U'$ if $u_1 \in A$, and to $A' = A$ otherwise). Therefore, since Γ' is a restriction of Γ, it is ideal, as implied by Lemma 4.11, and, consequently, so is Γ_1.

We conclude with a proof of the isomorphism. Assume that $A \in \Gamma_1$. If $u_1 \notin A$ then $A \in \Gamma$. Hence, also $A' = A \in \Gamma$ and, in particular, $A' \in \Gamma'$. If $u_1 \in A$ then $(A \setminus \{u_1\}) \cup M_2 \in \Gamma$ (this is implied by the second observation in (8)); hence, $A' \cup (M_2\setminus\{x\}) \in \Gamma$ and, therefore, $A' \in \Gamma'$. Conversely, assume that $A' \in \Gamma'$, namely, $(M_2 \setminus \{x\}) \cup A' \in \Gamma$. If $x \notin A'$ then $A' \subseteq U_1\setminus\{u_1\}$. As M_2 is a minterm of Γ_2 (this is implied by the first observation in (8)), $M_2\setminus\{x\} \notin \Gamma_2$. Hence, by Definition 3.4, we conclude that $A' \in \Gamma_1$. But in that case $A = A'$ so that $A \in \Gamma_1$. If $x \in A'$ then $(A' \setminus \{x\}) \cup M_2 \in \Gamma$ from which it follows that $A = (A' \setminus \{x\}) \cup \{u_1\} \in \Gamma_1$. □

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 8.2 (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 Claim 4.13, 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 8.3 (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, otherwise, $M \cap W \in \Gamma_{M \cap S,W}$. In the second case we infer that $M \cap S$ is S-cooperative, and since S is strong we get that $M \cap W \in \Gamma_W$. The following theorem shows that if S is a strong set of users, Γ is a composition of two ideal WTASs.

Theorem 8.4 *Let Γ be an ideal WTAS on 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, each of which is defined on a smaller set than U (one is defined on W and the other is defined on S supplemented by an additional user).*

Proof: Let Y be an arbitrary S-cooperative set, $Q \subseteq W$ be a minterm of $\Gamma_{Y,W}$, and x be an arbitrary element of Q. Both $\Gamma_{Y,W}$ and $\Gamma_{Q\setminus\{x\},S\cup\{x\}}$ are restrictions of Γ. Thus, by Lemma 4.11, they are both ideal, and by Claim 4.13 they are both WTASs. Let Δ be the composition of $\Gamma_{Q\setminus\{x\},S\cup\{x\}}$ and $\Gamma_{Y,W}$ via x (since x belongs to the domains of both access structures, W and $S \cup \{x\}$, we may define the composition by first replacing the user x in $\Gamma_{Q\setminus\{x\},S\cup\{x\}}$ with a copy x' and then compose $\Gamma_{Q\setminus\{x\},S\cup\{x\}}$ and $\Gamma_{Y,W}$ via x'). We note that Δ, like Γ, is defined on $U = W \cup S$. We proceed to show that $\Gamma = \Delta$, thus proving the lemma (note that $\Gamma_{Y,W}$ is defined on W, whose size is $k - 1 < n$, and Γ' is defined on $S \cup \{x\}$ whose size is $n - k + 2 < n$).

Let M be a minterm of Γ. Then either $M \subseteq S$, or $M \cap W \neq \emptyset$. If $M \subseteq S$, then $M \in \Gamma_{Q\setminus\{x\},S\cup\{x\}}$. Since $x \notin M$ we conclude, by Definition 3.4, that $M \in \Delta$. If, on the other hand, $M \cap W \neq \emptyset$, define $M_W = M \cap W$ and $M_S = M \cap S$. Therefore, M_S is an S-cooperative set. Since S is a strong set of users, we infer that $\Gamma_{M_S,W} = \Gamma_{Y,W}$, whence $M_W \in \Gamma_{Y,W}$. In addition, $Q \in \Gamma_{Y,W} = \Gamma_{M_S,W}$. This implies that $M_S \cup Q \in \Gamma$ and, consequently, that $M_S \cup \{x\} \in \Gamma_{Q\setminus\{x\},S\cup\{x\}}$. Therefore, by Definition 3.4, $M = M_W \cup M_S \in \Delta$.

For the other direction, let M be a minterm of Δ, and, as before, $M_S = M \cap S$ and $M_W = M \cap W$. Then either $M_S \in \Gamma_{Q\setminus\{x\},S\cup\{x\}}$ or both $M_W \in \Gamma_{Y,W}$ and $M_S \cup \{x\} \in \Gamma_{Q\setminus\{x\},S\cup\{x\}}$. We separate the discussion to these two cases:

If $M_S \in \Gamma_{Q\setminus\{x\},S\cup\{x\}}$, then $M_S \cup (Q\setminus\{x\}) \in \Gamma$. That means that $Q\setminus\{x\} \in \Gamma_{M_S,W}$. On the other hand, as Q is a minterm of $\Gamma_{Y,W}$, it must hold that $Q\setminus\{x\} \notin \Gamma_{Y,W}$. Hence, $\Gamma_{M_S,W} \neq \Gamma_{Y,W}$. This implies that M_S is not S-cooperative. But since $M_S \cup (Q\setminus\{x\}) \in \Gamma$, the only way M_S is not S-cooperative is if M_S is authorized by itself in Γ. However, $M = M_W \cup M_S$ was a minterm of Δ. Therefore, M_W must be empty whence $M = M_S$. This brings us to the sought-after conclusion that $M \in \Gamma$.

Now suppose that $M_S \notin \Gamma_{Q\setminus\{x\},S\cup\{x\}}$ but $M_W \in \Gamma_{Y,W}$ and $M_S \cup \{x\} \in \Gamma_{Q\setminus\{x\},S\cup\{x\}}$. Since $M_S \cup \{x\} \in \Gamma_{Q\setminus\{x\},S\cup\{x\}}$ we get that $Q \cup M_S \in \Gamma$. On the other hand, $M_S \notin \Gamma_{Q\setminus\{x\},S\cup\{x\}}$, and thus $M_S \notin \Gamma$. Therefore, M_S is S-cooperative. Since $M_W \in \Gamma_{Y,W}$, and S is a strong set of users, this implies that $M_W \in \Gamma_{M_S,W}$. Therefore $M_W \cup M_S \in \Gamma$, and thus $M \in \Gamma$. □

8.2 Simple Compositions

In this section we show that in two simple cases, an ideal WTAS is a composition of two ideal WTASs defined on sets smaller than U. The first case is when there are self-sufficient users and the second is where u_2 starts no minterm of Γ.

Suppose u_n is a self-sufficient user. Let $\Gamma' = \Gamma_{\emptyset,U_{1,n-1}}$ be the restriction of Γ to $U_{1,n-1}$ (namely, all authorized sets that do not include u_n). By Lemma 4.11, the access structure Γ' is ideal, and by Claim 4.13,

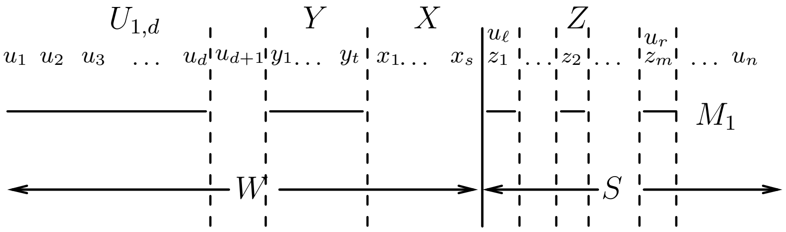

Figure 3: Notations for the composition.

it is an ideal WTAS. Let $\Gamma_\vee$ be the simple 1-out-of-2 access structure on the set $\{u', u_n\}$, where u' is an additional dummy user. $\Gamma_\vee$ is clearly an ideal WTAS. It is easy to see that Γ is the composition of Γ' and $\Gamma_\vee$ via 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 8.4, the access structure Γ is a composition of two ideal WTASs that are defined on sets smaller than U.

To conclude, we proved the following lemma:

Lemma 8.5 *Let Γ be an ideal WTAS on 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.*

8.3 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 Theorems 6.7 (HTAS) and 7.6 (TPAS), then it is a composition of two ideal WTASs as described in Section 8.1. In view of Lemma 8.5, 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. Since Γ is neither an HTAS nor a TPAS, then, by Theorems 6.7 and 7.6, 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 $X = \{x_1, \ldots, x_s\}$. (Note that $X = U_{d+t+2,\ell-1}$.) 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 Figure 3.

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.

An important result in our study is that all S-cooperative sets are at least as large as Z, namely, their size is at least m.

Claim 8.6 *Let $W = U_{1,\ell-1}$, $S = U_{\ell,n}$, and M be minterm of the access structure Γ. If $M \cap W \neq \emptyset$, then M contains at least m users from S.*

Proof: Assume towards a contradiction that M is a minterm that intersects W such that $|M \cap S| < m$. Recall that every minterm of Γ is an independent set of $\mathcal{M}$, the matroid associated with Γ. Hence, the minterm M_1 is an independent set of size $d+t+m$ of $\mathcal{M}$, and thus, by Claim 4.7, 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 5.2, 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 5.4). Its $(d+t+1)$th element is z_1. By Lemma 5.6 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. This contradiction implies that $|M \cap S| \geq m$. □

8.3.1 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. We begin by showing that the weight of every S-cooperative set is at least the weight of Z.

Claim 8.7 *Let $V \subseteq S$ be an S-cooperative set. Then $w(V) \geq w(Z)$.*

Proof: Assume towards a 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 5.1, 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 5.3 implies that $|V| = |Z| = m$. The set $B \cup V$ is independent in $\mathcal{M}$. If $|B \cup V| < d+t+m$, Claim 4.7 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 5.2, 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 5.6, 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. Since $B \cup Z$ is a minterm, we get from Lemma 5.3 that $|Q| = |Z| = m$. On the other hand, by Claim 8.6, since V is S-cooperative, $|V| \geq m$. Since $B \cup V \notin \Gamma$ but $B \cup Q \in \Gamma$, we infer that $w(V) < w(Q)$. Therefore, there must be an index $j \in [m]$ such that $v_j \prec q_j$. Thus, by Lemma 5.6, 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 are lead to the conclusion that $w(V) \geq w(Z)$. □

We are now ready to prove that all the cooperative sets of size m induce the same access structure on W.

Claim 8.8 *Let V be an S-cooperative set of size m. Then $\Gamma_{V,W} = \Gamma_{Z,W}$.*

Proof: By Claim 8.7, $w(V) \geq w(Z)$. 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 5.1 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. Since $B \cup V$ is a minterm, by Lemma 5.3, it must be that $|Q| = |V| = m = |Z|$. Since $B \cup Q$ is authorized and $B \cup Z$ is unauthorized, $w(Z) < w(Q)$. Therefore, there must be an index $j \in [m]$ for which $z_j \prec q_j$. Thus, by Lemma 5.6, 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 5.3. 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 a contradiction, that $M \cup Z \notin \Gamma$. Let Q be the canonical complement of M. By Lemma 5.3, $|Q| = |V| = m = |Z|$. Since $M \cup Z \notin \Gamma$ and $M \cup Q \in \Gamma$, $w(Z) < w(Q)$. Therefore, there must be an index $j \in [m]$ such that $z_j \prec q_j$. Thus, by Lemma 5.6, $M \cup Z$ 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 $M \cup Z$. We have arrived at the absurd situation where the dependent set $M \cup Z$ is contained in a minterm. This contradiction implies that $M \cup Z$ is authorized, so $M \in \Gamma_{Z,W}$. □

Combining Claims 8.6 and 8.8 we arrive at the following corollary.

Corollary 8.9 *If there are no S-cooperative sets of size larger than m, then S is a strong set.*

Example 8.10 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 , and 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 2-out-of-4 threshold access structure on $S \cup \{u'\}$ and 3-out-of-5 threshold access structure on the week side W, where u' is an additional dummy user.

8.3.2 When Large S-Cooperative Sets Exist

The conclusion from the previous section 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 8.4, the access structure Γ is a composition of ideal WTASs that are defined on 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.

Recall that we assume that there are minterms that start with u_2. In order to prove that $U_{d+2,n}$ is a strong set we show that for every $U_{d+2,n}$-cooperative set, V, the access structure that it induces on $U_{1,d+1}$, namely $\Gamma_{V,U_{1,d+1}}$, is a d-out-of-$(d+1)$ threshold access structure. The proof has two stages:

- First we show that if M is a minterm of Γ such that $|M \cap S| > m$ then $M \cap U_{1,d+1} = \emptyset$ (Claim 8.15). This immediately implies that V, being a $U_{d+2,n}$-cooperative set, intersects S in exactly m users (Corollary 8.16).
- In the second stage, we analyze the restricted access structure that Z induces on W, namely $\Gamma_{Z,W}$, and conclude that $\Gamma_{V,U_{1,d+1}}$ is a d-out-of-$(d+1)$ access structure.

We start with two technical claims. The following claim shows that the weight of z_1 is much larger than the weights of the users preceding it.

Claim 8.11 $w(u_{d+1}) + w(x_1) < w(z_1)$.

Proof: Suppose the claim is false and $w(u_{d+1}) + w(x_1) \geq w(z_1)$. Then we can replace z_1 by u_{d+1} and x_1 in the minterm M_1, and get an authorized set M_1'. By Lemma 5.1, this set contains a suffix minterm. This minterm must intersect W, since Z by itself is unauthorized. But then M_1' would be a minterm that contains only $m - 1$ elements of S, in a contradiction to Claim 8.6. □

Claim 8.12 *The sets $U_{1,d} \cup Y \cup \{x_1\}$ and $U_{1,d+1}$ are circuits of $\mathcal{M}$ – the matroid that corresponds to Γ.*

Proof: We start with the set $V := U_{1,d} \cup Y \cup \{x_1\}$. Denote by Γ' the restriction $\Gamma_{Z,W\setminus\{u_{d+1}\}}$. By Lemma 4.11 and Claim 4.13, Γ' is an ideal WTAS. Moreover, the set $U_{1,d} \cup Y$ is a prefix minterm of this access structure. Therefore, by Theorem 6.7, Γ' is a HTAS. Thus, by Claim 6.2, V is a circuit of the matroid that corresponds to Γ' and its size is $|V| = d + t + 1$. As M_1 is the canonic complement of the empty set, z_1 is its $(d + t + 1)$th element, and $x_1 \prec z_1$, we conclude by Lemma 5.6 that V is dependent in $\mathcal{M}$. It must be a circuit in $\mathcal{M}$ for, otherwise, by Lemma 4.12, we would get a contradiction to the fact that it is a circuit in the matroid that corresponds to the restriction Γ'.

The proof for $U_{1,d+1}$ is similar. Let $\Gamma'' = \Gamma_{Y\cup Z,U_{1,d+1}}$ be the restriction that $Y \cup Z$ induces on $U_{1,d+1}$. It is an ideal WTAS and $U_{1,d}$ is a prefix minterm in it. Thus, by Claim 6.2, $U_{1,d+1}$ is a circuit of the matroid that corresponds to Γ''. As u_{d+1}, which is the $(d + 1)$th user in $U_{1,d+1}$, precedes the $(d + 1)$th user in the canonical complement of the empty set (which is y_1, or z_1 if $Y = \emptyset$), we infer by Lemma 5.6 that $U_{1,d+1}$ is dependent in $\mathcal{M}$. Finally, by Lemma 4.12, the set $U_{1,d+1}$ must be a circuit of $\mathcal{M}$. □

We now turn to show that large S-cooperative sets are not contained in minterms that intersect $U_{1,d+1}$. This is done in two steps. First we show that if V is an S-cooperative set of size larger than m, there exists a suffix B of Y such that $B \cup V$ is a minterm. Then, relying upon this result, we show that no minterm of $\Gamma_{V,W}$ intersects $U_{1,d+1}$. This completes the first stage of the proof outlined above

Claim 8.13 *If there exists an S-cooperative set V of size larger than m, there exists a suffix B of Y such that $B \cup V$ is a minterm.*

Proof: Consider the set $A := U_{1,d} \cup Y \cup V$. Since $|V| > |Z|$, the set A cannot be a minterm, as implied by Lemma 5.3. By Claim 8.7, $w(V) \geq w(Z)$. Thus, the set A is authorized and, consequently, it contains a suffix minterm of the form $B \cup V$ where B is a proper suffix of $U_{1,d} \cup Y$.

In order to prove the claim, we need to show that $B \subseteq Y$. Assume, towards a contradiction, that it is not, namely, that $B_{\min} \in U_{1,d}$. Let $Q = B\setminus\{B_{\min}\} \cup \{x_1\}$. Since $B_{\min} \prec x_1$, the weight of Q is at least the weight of B, and therefore, $Q \cup V$ is an authorized set. Hence, it has a suffix minterm that must contain $\{x_1\} \cup V$. The union of this minterm and the minterm $B \cup V$ is $B \cup \{x_1\} \cup V$. We claim that all the users in V are critical for $B \cup \{x_1\} \cup V$, in the sense of Definition 4.3. Let $v_i \in V$ and assume that it is not critical, i.e., $B \cup \{x_1\} \cup V \backslash \{v_i\} \in \Gamma$. Since $B \cup V \backslash \{B_{\min}\} \notin \Gamma$ (because $B \cup V$ is a minterm), we conclude that $w(B \cup V \backslash \{B_{\min}\}) < w(B \cup \{x_1\} \cup V \backslash \{v_i\})$, whence $w(v_i) < w(B_{\min}) + w(x_1)$. Therefore, as $w(z_1) \leq w(v_i)$ and $w(B_{\min}) \leq w(u_{d+1})$, we arrive at the conclusion that $w(z_1) < w(u_{d+1}) + w(x_1)$, in a contradiction with Claim 8.11. This implies that all of the users of V are critical for $B \cup \{x_1\} \cup V$. Thus, by Corollary 4.5, the set $B \cup \{x_1\}$ is dependent. However, $B \cup \{x_1\}$ is properly contained in $U_{1,d} \cup Y \cup \{x_1\}$, which , by Claim 8.12, is a circuit of $\mathcal{M}$. This contradiction implies that B does not intersect $U_{1,d}$ and it is therefore a suffix of Y. □

Remark 8.14 If there is an S-cooperative set V of size larger than m, the set Y is not empty. Otherwise, the set B in Claim 8.13 would be empty, whence V is a minterm in a contradiction to our assumption that V is S-cooperative. Therefore, in the rest of this section we assume that Y is not empty.

Claim 8.15 *If V is an S-cooperative set of size larger than m and A is a minterm of $\Gamma_{V,W}$, then $A \cap U_{1,d+1} = \emptyset$.*

Proof: Suppose there is a minterm $A \in \Gamma_{V,W}$ such that $A \cap U_{1,d+1} \neq \emptyset$. We pick a minterm A of that sort having the property that $A \cap (Y \cup X) \preceq M \cap (Y \cup X)$ for all minterms $M \in \Gamma_{V,W}$ such that$M \cap U_{1,d+1} \neq \emptyset$. By Claim 8.13, there is a suffix B of Y such that $B \in \Gamma_{V,W}$. Therefore, as A is a minterm of $\Gamma_{V,W}$, it must be that $Y \not\subseteq A$ (otherwise, if $Y \subseteq A$, the minterm $A \cup V$ would have been a proper superset of the minterm $B \cup V$ since A includes in addition users from $U_{1,d+1}$). Let j be the smallest index such that $y_j \notin A$ (recall that $Y \neq \emptyset$) and consider the set $Q = A \setminus \{A_{\min}\} \cup \{y_j\}$. Since $A_{\min} \in U_{1,d+1}$, we conclude that $w(A_{\min}) \leq w(y_j)$. Thus $Q \cup V$ is authorized in Γ and must contain a suffix minterm M' that contains y_j. The union of $A \cup V$ and M' is $A \cup \{y_j\} \cup V$. The discussion now separated two cases: either A is a run of U or it is not.

If A is a run of U, then we first claim that every user of V is critical for $A \cup \{y_j\} \cup V$. Let $v_i \in V$ and assume that it is not critical for $A \cup \{y_j\} \cup V$, i.e., $A \cup \{y_j\} \cup V \setminus \{v_i\} \in \Gamma$. Since $A \cup V \setminus \{A_{\min}\} \notin \Gamma$ (as $A \cup V$ is a minterm), we conclude, by comparing the weights of the two latter sets, that $w(v_i) < w(A_{\min}) + w(y_j)$. However, since $w(z_1) \leq w(v_i)$, $w(y_j) \leq w(x_1)$, and $w(A_{\min}) \leq w(u_{d+1})$, we get that $w(z_1) < w(u_{d+1}) + w(x_1)$, in a contradiction with Claim 8.11. Therefore, all users in V are critical for $A \cup \{y_j\} \cup V$. Thus, by Corollary 4.5, the set $A \cup \{y_j\}$ is dependent. Since we are now dealing with the case where A is a run of U, the set $A \cup \{y_j\}$ must be contained in $U_{1,d+1} \cup Y$. Since $A \cup \{y_j\}$ is dependent, it includes a circuit C. That circuit must include the user u_{d+1}, for, otherwise, C would have been a subset of the independent set $U_{1,d} \cup Y$. Moreover, the circuit C must also contain y_j, for otherwise $C \subseteq A$ while A is contained in a minterm and thus is independent. On the other hand, by Claim 8.12, the set $U_{1,d+1}$ is a circuit of $\mathcal{M}$ that does not contain y_j. Therefore, u_{d+1} is in the intersection of the two distinct circuits $U_{1,d+1}$ and C. Hence, by Lemma 4.6, the set $U_{1,d+1} \cup C \setminus \{u_{d+1}\}$ is dependent. But that latter set is contained in the independent set $U_{1,d} \cup Y$. This contradiction settles the statement whenever A is a run of U.

If A is a not run of U, we claim that every user $a_i \in A$ such that $y_j \prec a_i$ is critical for $A \cup \{y_j\} \cup V$. Otherwise we could replace the user a_i in the minterm $A \cup V$ with the user y_j and still get a minterm that intersects $U_{1,d+1}$. But this would contradict our choice of A as a minterm that is lexicographically minimal in $Y \cup X$. This implies that all users of $A \cup \{y_j\} \cup V$ that have weight greater than or equal to y_j are critical for that set. In particular, the subset $(A \cap X) \cup V$ consists of only critical users and, consequently, by Claim 4.5, the set $A \backslash X \cup \{y_j\}$ is dependent. Since A is contained in a minterm, this dependent set must contain a circuit C that contains y_j. Since $U_{1,d} \cup Y$ is an independent set of $\mathcal{M}$, it must be that $u_{d+1} \in C$, otherwise C is properly contained in an independent set. However, since $U_{1,d+1}$ is a circuit of $\mathcal{M}$, we get that u_{d+1} is in the intersection of two distinct circuits, C and $U_{1,d+1}$ (note that $y_j \in C$ but $y_j \notin U_{1,d+1}$).

Therefore, by Lemma 4.6, the set $C \cup U_{1,d+1} \setminus \{u_{d+1}\}$ is dependent. However, this set is properly contained in $U_{1,d} \cup Y$ which is an independent set of $\mathcal{M}$, and thus we arrive at a similar contradiction as in the previous case. $\square$

Corollary 8.16 *Every $U_{d+2,n}$-cooperative set intersects S in exactly m users.*

Proof: Let B be a $U_{d+2,n}$-cooperative set. Then there exists a non-empty set $A \subseteq U_{1,d+1}$ such that $M := A \cup B$ is a minterm of Γ. Denote $M_W = M \cap W$ and $M_S = M \cap S$, so that $M = A \cup B = M_W \cup M_S$. As $U_{1,d+1} \subset W$ and $U_{d+2,n} \supset S$, we infer that $M_W \cap U_{1,d+1} = A \neq \emptyset$ and $M_S = B \cap S$.

On one hand, Claim 8.6 implies that $|M_S| \geq m$, since $M_W \neq \emptyset$. On the other hand, by Claim 8.15, if $|M_S| > m$ then $M_W \cap U_{1,d+1} = \emptyset$. But as $M_W \cap U_{1,d+1} \neq \emptyset$ we conclude that $|M_S| = |B \cap S| = m$. $\square$

We now turn to the second stage of showing that $U_{d+2,n}$ is a strong set. We will show that the existence of large S-cooperative sets and the existence of minterms that start with u_2 imply that $U_{d+2,n}$ is a strong set. By Claim 8.15, every $U_{d+2,n}$-cooperative set intersects S in exactly m users. By Claim 8.8, if V is an S-cooperative set of size m then $\Gamma_{V,W} = \Gamma_{Z,W}$. Therefore, it is enough to study the minterms in $\Gamma_{Z,W}$ that intersect $U_{1,d+1}$. Somehow, surprisingly, the existence of a large S-cooperative set affects the structure of $\Gamma_{Z,W}$. The next two claims will serve us in characterizing the structure of $\Gamma_{Z,W}$ in Claim 8.19.

Claim 8.17 *If there is an S-cooperative set V of size larger than m, there exists a non-empty suffix B of Y such that $B \cup \{x_1\} \in \Gamma_{Z,W}$.*

Proof: By Claim 8.13, there exists a suffix B of Y such that $B \cup V$ is a minterm of Γ. We next prove that $B \cup \{x_1\} \cup V \setminus \{v_1\} \in \Gamma$. Replacing $B_{\min}$ with x_1 in $B \cup V$, we get an authorized set. Denote by M' the suffix minterm contained in that set and note that the union of M' and $B \cup V$ is exactly $B \cup \{x_1\} \cup V$. We claim that v_1 cannot be critical for $B \cup \{x_1\} \cup V$. If it was critical, then every user in V would also be critical for that set and thus, by Corollary 4.5, the set $B \cup \{x_1\}$ would be dependent in $\mathcal{M}$. However, the set $B \cup \{x_1\}$ is properly contained in $U_{1,d} \cup Y \cup \{x_1\}$, which is a circuit by Claim 8.12. Therefore, $B \cup \{x_1\}$ is independent, and thus v_1 cannot be critical for $B \cup \{x_1\} \cup V$. Hence, the set $B \cup \{x_1\} \cup V \setminus \{v_1\}$ is authorized. But since it is obtained from the minterm $B \cup V$ by replacing v_1 with $x_1 \prec v_1$, it must be also a minterm.

We now prove the claim by induction on the size of V. If $|V| = m + 1$, then since $B \cup \{x_1\} \cup V \setminus \{v_1\}$ is a minterm, we conclude that $B \cup \{x_1\}$ is in $\Gamma_{V',W}$, where $V' = V \setminus \{v_1\}$ is an S-cooperative set of size m. But since, in view of Claim 8.8, $\Gamma_{V',W} = \Gamma_{Z,W}$, we arrive at the sought-after conclusion that $B \cup \{x_1\} \in \Gamma_{Z,W}$. If $|V| > m + 1$, then V' is an S-cooperative set of size $|V| - 1$. Hence, we may apply the induction hypothesis to conclude that there exists a suffix B of Y such that $B \cup \{x_1\} \in \Gamma_{Z,W}$. $\square$

The other assumption that affects the structure of $\Gamma_{Z,W}$ is that there are minterms of Γ that start with u_2.

Claim 8.18 *If u_2 is the minimal user in some minterm of Γ, then $U_{2,d+1} \cup Y$ is a minterm of $\Gamma_{Z,W}$.*

Proof: The access structure $\Gamma_{Z,W}$ is an ideal WTAS and its lexicographically minimal minterm is $U_{1,d} \cup Y$. Let M be a minterm of Γ that starts with u_2. In particular, M intersects W. By Claims 8.6 and 8.15, the minterm M contains exactly m members of S. Thus, By Claim 8.8, $\Gamma_{M \cap S,W} = \Gamma_{Z,W}$. This implies that $M \cap W$ is a minterm of $\Gamma_{Z,W}$ that starts with u_2. Recall that, by Remark 8.14, $Y \neq \emptyset$. Hence, Claim 7.1 applies to the access structure $\Gamma_{Z,W}$, and the set $U_{2,d+1} \cup Y$ is a minterm of $\Gamma_{Z,W}$. $\square$

We may now describe the structure of $\Gamma_{Z,W}$. Since we assume that there exists a minterm of Γ that starts with u_2, the set $U_{2,d+1} \cup Y$ is a minterm of $\Gamma_{Z,W}$, as implied by Claim 8.18. As $U_{2,d+1} \cup Y$ is a run, and it is a prefix in $W\setminus\{u_1\}$, we get that the restriction $\Gamma_{Z,W\setminus\{u_1\}}$ has a prefix minterm. Therefore, by Theorem 6.7, it is an HTAS. The threshold of the first level is $|U_{2,d+1}\cup Y| = d+t$. By Claim 8.17, the run minterm of this HTAS that ends with x_1 starts with an element of Y. Therefore, the transition between the first and the second level in that HTAS (if exists) occurs within Y. This enables us to prove that $U_{d+2,n}$ is a strong set of users.

Claim 8.19 *Suppose there is an S-cooperative set of size larger than m, and that there is a minterm of Γ that starts with u_2. Then $U_{d+2,n}$ is a strong set of users.*

Proof: In order to show that $U_{d+2,n}$ is a strong set of users, we show that for any $U_{d+2,n}$-cooperative set V, the corresponding restriction induced by V on $U_{1,d+1}$, namely $\Gamma_{V,U_{1,d+1}}$, is a d-out-of-$(d+1)$ threshold access structure. Let V be a $U_{d+2,n}$-cooperative set. Hence, there exists a non-empty set $A\subseteq U_{1,d+1}$ such that $A\cup V$ is a minterm of Γ. Denote $V_W = V\cap W$ and $V_S = V\cap S$. Note that the set V_S is S-cooperative. Moreover, since $A\cup V$ is a minterm of Γ, then $A\cup V_W$ is a minterm of $\Gamma_{V_S,W}$ that intersects $U_{1,d+1}$. Therefore, by Claim 8.15, we conclude that $|V_S| = m$. Thus, by Claim 8.8, $\Gamma_{V_S,W} = \Gamma_{Z,W}$. Consequently, since $A\cup V_W$ is a minterm of $\Gamma_{V_S,W}$, it is also a minterm of $\Gamma_{Z,W}$.

We claim that the size of that minterm is $|A\cup V_W| = d+t$. Indeed, if the minimal user in $A\cup V_W$ is u_1 then, by Lemma 5.3, $|A\cup V_W\cup V_S| = |M_1| = d+t+m$, so, as $|V_S| = m$, we get that $|A\cup V_W| = d+t$. Otherwise, $A\cup V_W\subseteq W\setminus\{u_1\}$ and, consequently, $A\cup V_W\in\Gamma_{Z,W\setminus\{u_1\}}$. But the latter access structure was shown above to be an HTAS; furthermore, we showed that the first level in that HTAS includes all of $U_{2,d+1}$ and the corresponding threshold is $d+t$. Since $A\cup V_W$ starts within $U_{2,d+1}$, it is of size $d+t$.

First, we show that for any $D\subseteq U_{1,d+1}$ of size d, $D\cup V\in\Gamma$. Since $w(D)\geq w(U_{1,d})$, we need only to show that $U_{1,d}\cup V\in\Gamma$. We know that $M_1 = U_{1,d}\cup Y\cup Z\in\Gamma$. Since $A\subseteq U_{1,d+1}$ it must be that $|A|\leq d$ (otherwise $A = U_{1,d+1}$ and then $A\cup V$ would be a minterm that precedes M_1 with respect to the lexicographical order). Hence, $|V_W|\geq t$. Since Y consists of the first t users in $U_{d+2,n}$, we conclude that $w(V_W)\geq w(Y)$. Therefore V_W can replace Y in M_1 and so $U_{1,d}\cup V_W\in\Gamma_{Z,W} = \Gamma_{V_S,W}$. This implies that $U_{1,d}\cup V_W\cup V_S = U_{1,d}\cup V\in\Gamma$, as required. Hence, every subset of d users from $U_{1,d+1}$ completes V to an authorized set.

Finally, we need to show that no smaller subset of $U_{1,d+1}$ completes V to an authorized set. To that end, let B be a minterm of $\Gamma_{V,U_{1,d+1}}$. We proceed to show that $|B|\geq d$. Using the above notations, $B\cup V_W\cup V_S$ is a minterm of Γ, or, equivalently, $B\cup V_W$ is a minterm of $\Gamma_{V_S,W} = \Gamma_{Z,W}$. Arguing along the same lines as we did for $A\cup V_W$, we conclude that $|B\cup V_W| = d+t$. Assume towards a contradiction that $|B| < d$. Then $|V_W| > t$ and, consequently, as $V_W\subset U_{d+2,n}$, we get that $w(V_W)\geq w(Y\cup\{x_1\})$. But according to Claim 8.17, $Y\cup\{x_1\}\in\Gamma_{Z,W}$. Hence, since $\Gamma_{Z,W} = \Gamma_{V_S,W}$, we infer that $Y\cup\{x_1\}\cup V_S\in\Gamma$. This implies that also $V_W\cup V_S = V$ is authorized, in a contradiction to our assumption that V is a $U_{d+2,n}$-cooperative set. That completes the proof. $\square$

8.4 Proof of Theorem 3.5 – 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 8.5, 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 6.7, 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 7.6, the access structure Γ is a TPAS. Otherwise, by Corollary 8.9 and Claim 8.19, there exists within U a subset of strong users. In this case, we conclude by Theorem 8.4 that 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 [6, 35]. TPASs are also ideal and may be realized by linear secret sharing schemes, as shown herein in Section 7.1. Finally, given two ideal access structures, we showed in Lemma 8.1 how to construct an ideal secret sharing scheme for their composition. Hence, the composition is also ideal. Furthermore, by Lemma 8.1, 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 and E. Weinreb. Monotone circuits for monotone weighted threshold functions. *Inform. Process. Lett.*, 97(1):12–18, 2006. Conference version: *Proc. of 20th Annu. IEEE Conf. on Computational Complexity*, pages 67-75, 2005.

[3] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for noncryptographic fault-tolerant distributed computations. In *Proc. of the 20th ACM Symp. on the Theory of Computing*, pages 1–10, 1988.

[4] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advances in Cryptology – CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer-Verlag, 1990.

[5] G. R. Blakley. Safeguarding cryptographic keys. In R. E. Merwin, J. T. Zanca, and M. Smith, editors, *Proc. of the 1979 AFIPS National Computer Conference*, volume 48 of *AFIPS Conference proceedings*, pages 313–317. AFIPS Press, 1979.

[6] E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.

[7] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4(73):123–134, 1991.

[8] 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.

[9] 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.

[10] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In *Proc. of the 20th ACM Symp. on the Theory of Computing*, pages 11–19, 1988.

[11] M. J. Collins. A note on ideal tripartite access structures. Technical Report 2002/193, Cryptology ePrint Archive, 2002. `http://eprint.iacr.org/`.

[12] R. Cramer, I. Damgård, and U. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In B. Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 316–334. Springer-Verlag, 2000.

[13] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In J. Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 457–469. Springer-Verlag, 1992.

[14] O. Farràs, J. Martí-Farré, and C. Padró. Ideal multipartite secret sharing schemes. Technical Report 2006/292, Cryptology ePrint Archive, 2006. `http://eprint.iacr.org/`.

[15] J. Herranz and G. Saez. New results on multipartite access structures. Technical Report 2006/048, Cryptology ePrint Archive, 2006. `http://eprint.iacr.org/`.

[16] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Proc. of the IEEE Global Telecommunication Conf., Globecom 87*, pages 99–102, 1987. Journal version: Multiple assignment scheme for sharing secret. *J. of Cryptology*, 6(1):15-20, 1993.

[17] 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.

[18] M. Karchmer and A. Wigderson. On span programs. In *Proc. of the 8th IEEE Structure in Complexity Theory*, pages 102–111, 1993.

[19] E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. on Information Theory*, 29(1):35–41, 1983.

[20] J. Martí-Farré and C. Padró. Secret sharing schemes on access structures with intersection number equal to one. In *The third Conference on Security in Communication Networks '02*, volume 2576 of *Lecture Notes in Computer Science*, pages 354–363. Springer-Verlag, 2002.

[21] K. M. Martin. *Discrete Structures in the Theory of Secret Sharing*. PhD thesis, University of London, 1991.

[22] K. M. Martin. New secret sharing schemes from old. *Journal of Combin. Math. and Combin. Comput.*, 14:65–77, 1993.

[23] P. Morillo, C. Padró, G. Sáez, and J. L. Villar. Weighted threshold secret sharing schemes. *Inform. Process. Lett.*, 70(5):211–216, 1999.

[24] J. G. Oxley. *Matroid Theory*. Oxford University Press, 1992.

[25] C. Padró and G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. on Information Theory*, 46:2596–2605, 2000.

[26] M. O. Rabin. Randomized Byzantine generals. In *Proc. of the 24th IEEE Symp. on Foundations of Computer Science*, pages 403–409, 1983.

[27] P. D. Seymour. On secret-sharing matroids. *J. of Combinatorial Theory, Series B*, 56:69–73, 1992.

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

[29] G. J. Simmons. How to (really) share a secret. In S. Goldwasser, editor, *Advances in Cryptology – CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 390–448. Springer-Verlag, 1990.

[30] G. J. Simmons. An introduction to shared secret and/or shared control and their application. In G. J. Simmons, editor, *Contemporary Cryptology, The Science of Information Integrity*, pages 441–497. IEEE Press, 1992.

[31] G. J. Simmons, W. Jackson, and K. M. Martin. The geometry of shared secret schemes. *Bulletin of the ICA*, 1:71–88, 1991.

[32] J. Simonis and A. Ashikhmin. Almost affine codes. *Designs, Codes and Cryptography*, 14(2):179–197, 1998.

[33] D. R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2:357–390, 1992.

[34] D. R. Stinson. New general lower bounds on the information rate of secret sharing schemes. In E. F. Brickell, editor, *Advances in Cryptology – CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 168–182. Springer-Verlag, 1993.

[35] T. Tassa. Hierarchical threshold secret sharing. In M. Naor, editor, *Proc. of the First Theory of Cryptography Conference – TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 473–490. Springer-Verlag, 2004.