Linear Secret-Sharing Schemes for $k$-uniform access structures

Younjin Kim$^1$, Jihye Kwon$^2$, and Hyang-Sook Lee$^3$

June 29, 2021

$^1$ Institute of Mathematical Sciences, Ewha Womans University, Seoul, South Korea
  younjinkim@ewha.ac.kr

$^2$ Department of Mathematics, Ewha Womans University, Seoul, South Korea
  jhkwon74@ewhain.net

$^3$ Department of Mathematics, Ewha Womans University, Seoul, South Korea
  hsl@ewha.ac.kr

Abstract

A $k$-uniform hypergraph $H = (V, E)$ consists of a set $V$ of vertices and a set $E$ of hyperedges ($k$-hyperedges), which is a family of $k$-subsets of $V$. A forbidden $k$-homogeneous (or forbidden $k$-hypergraph) access structure $A$ is represented by a $k$-uniform hypergraph $H = (V, E)$ and has the following property: a set of vertices (participants) can reconstruct the secret value from their shares in the secret sharing scheme if they are connected by a $k$-hyperedge or their size is at least $k + 1$. A forbidden $k$-homogeneous access structure has been studied by many authors under the terminology of $k$-uniform access structures. In this paper, we provide efficient constructions on the total share size of linear secret sharing schemes for sparse and dense $k$-uniform access structures for a constant $k$ using the hypergraph decomposition technique and the monotone span programs.

Keywords secret sharing schemes, graph access structures, hypergraph decomposition

1 Introduction

A secret sharing scheme is a tool used in many cryptographic protocols. A secret sharing scheme involves a dealer who has a secret, a set of $n$ participants, and a collection $\mathcal{F}$ of subsets of participants defined as the access structure. A secret sharing scheme for $\mathcal{F}$ is a method by which the dealer distributes shares of a secret value $k$ to the set of $n$ participants such that any subset in $\mathcal{F}$ can reconstruct the secret value $k$ from their shares and any subset not in $\mathcal{F}$ cannot reveal any information about the secret value $k$. When any subset in $\mathcal{F}$ can reconstruct the secret value $k$ from their shares by using a linear mapping, the secret sharing scheme is called a...
linear secret sharing scheme. The qualified subsets in the secret sharing scheme is defined as the subsets of participants who can reconstruct the secret value $k$ from their shares. A collection of qualified subsets of participants called the access structure of the secret sharing scheme. In other words, the unqualified subsets or forbidden subsets in the secret sharing scheme are defined as the subsets of participants who cannot have any information about the secret value $k$ from their shares.

In 1979, Shamir \cite{42} introduced a $(t, n)$-threshold secret sharing scheme as the first works about the secret sharing, in which the qualified subsets are formed by all the subsets with at least $t$ participants in a set of $n$ participants and the size of each share is the size of the secret. It means that $(t, n)$-threshold secret sharing scheme is determined by the basis consisting of all subsets with exactly $t$ different participants from a set of $n$ participants. There have been further constructions of secret sharing schemes for any access structures, and in 1987, Ito, Saito, and Nishizeki \cite{33} constructed secret sharing schemes for general access structures. However, their constructions are very inefficient because the size of the shares much larger than the size of the secret in general. Later, in 1988, Benaloh and Leichter \cite{12} constructed a much more efficient secret sharing scheme for general access structure based on monotone formulate than the scheme of Ito, Saito, and Nishizeki \cite{33}.

All the above secret-sharing schemes are linear in which the secret is an element of the field and each share is a vector over the field whose each coordinate is expressed as a linear combination of the secret, and the coordinates of the random strings which are taken from some finite field. In 1993, Karchmer and Wigderson \cite{35} introduced the monotone span programs from which the linear secret sharing schemes can be constructed. They obtained that every monotone span program over finite fields implies a linear secret sharing scheme for an access structure consisting of all sets accepted by the monotone span program. Later, in 1993, Bertilsson and Ingemarsson \cite{13} generalized their linear schemes derived from the monotone span programs to the multilinear schemes based on the generalized monotone span programs in which the secret is some vector over the field. The best-known lower bound on the total share size of secret sharing schemes realizing a general access structure was given by Csirmaz \cite{20} in 1997. Also, the best-known upper bound on the total share size of secret sharing scheme realizing a general access structure was given by Applebaum, Beimel, Farrás, Nir, and Peter \cite{2} in 2020, which is highly inefficient with the size $2^{0.637n}$.

An access structure is defined as a graph access structure determined by a graph $G = (V, E)$ if a pair of vertices connected by an edge can reconstruct the secret and the set of non-adjacent vertices in the graph $G$ does not get any information on the secret. The motivation for studying graph secret sharing schemes is that they are simpler than secret sharing schemes for general access structures and later generalized to general access structures. Secret sharing schemes realizing graph access structures were studied in many papers \cite{5,16,19,21,25,27,29} Also, many authors were interested in forbidden graph access structures as specific families of access structures. An access structure is defined as a forbidden graph access structure determined by a graph $G = (V, E)$ if a pair of vertices can reconstruct the secret if it is connected by an edge or its size is at least 3. In 2014, Beimel, Ishai, Kumaresan, and Kushilevitz \cite{9} constructed a secret sharing scheme realizing all forbidden graph access structures with the total share size $O(n^{3/2})$. Later, in 2015, a linear secret sharing scheme for all forbidden graph access structures was given by Gay, Kerenidis, and Wee \cite{32} in which the total share size is $O(n^{5/2})$. Recently, in 2017, Liu, Vaikuntanathan, and Wee \cite{36} proved that every forbidden graph access structure could be realized by a non-linear secret
sharing scheme with the total share size $n^{1+o(1)}$. For the forbidden dense graph access structures having at least $\binom{n}{2} - n^{1+\beta}$ edges, where $0 \leq \beta < \frac{1}{2}$, Beimel, Farras, and Peter [7] constructed a linear secret sharing scheme with the total share size $O(n^{7/6+2\beta/3})$. Later, in 2020, Beimel, Farras, Mintz, and Peter [6] provided efficient constructions on the share size of linear secret schemes for forbidden sparse and dense graph access structures based on the monotone span programs.

A hypergraph is a generalization of a graph in which hyperedges may connect more than two vertices. A $k$-uniform hypergraph is a hypergraph in which each hyperedge has exactly $k$ vertices. An access structure is defined as a $k$-hypergraph access structure determined by a $k$-uniform hypergraph $\mathcal{H}$ if the set of vertices connected by a $k$-hyperedge can reconstruct the secret and the set of non-adjacent vertices in the hypergraph $\mathcal{H}$ does not get any information on the secret. The access structures of these schemes are also called $k$-homogeneous. For example, graph access structures are 2-homogeneous access structures. A $k$-homogeneous access structure is determined by the family of minimal qualified subsets with exactly $k$ different participants or $k$-uniform hypergraphs $\mathcal{H}(V, E)$, where $V$ is a vertex set, and $E \subseteq 2^V$ is an edge set of hyperedges of cardinality $k$. The secret sharing schemes for $k$-homogeneous access structures have been constructed by many authors based on various techniques. In 1990, Benaloh and Leichter [12] constructed a secret sharing scheme for the $k$-homogeneous access structure with total share size $O(n^k/\log n)$. For the dense $k$-homogeneous access structure, a much more efficient secret sharing scheme was constructed by Beimel, Farras, and Mintz [5] in 2012, in which the total share size is $\tilde{O}(2^k k^k n^{2+\beta})$. Recently, in 2020, Beimel and Farras [4] constructed a secret sharing scheme for almost all $k$-homogeneous access structures with maximum share size $2^{\tilde{O}(\sqrt{k \log n})}$.

An access structure is defined as forbidden $k$-homogeneous (or forbidden $k$-hypergraph) determined by a hypergraph $\mathcal{H}$ if a set of vertices can reconstruct the secret if it is connected by a $k$-hyperedge or its size is at least $k + 1$. We study the complexity of realizing a forbidden $k$-hypergraph access structure by linear secret sharing schemes. A forbidden $k$-homogeneous access structure has been studied by many authors [1,2,10,45] under the terminology of $k$-uniform access structures. Recently, in 2018, Applebaum and Arkis constructed an efficient secret sharing scheme for $k$-uniform access structures using multiparty Conditional Disclosure of Secrets (CDS). Later, in 2018, Beimel and Peter [11] obtained that every $k$-uniform access structure with a binary secret could be realized by a secret sharing scheme in which the share size $\min\{O(n/k)^{(k-1)/2}, O(n \cdot 2^{n/2})\}$. By improving their result, in 2019, Applebaum, Beimel, Farras, Nir, and Peter [2] obtained that every $k$-uniform access structure with a binary secret could be realized by a secret sharing scheme in which the share size is $2^{O(\sqrt{k \log n})}$ by combining the CDS protocol and transformations. In 2020, Beimel, Farras, Mintz, and Peter [6] obtained the lower bound on the max share size for sharing a one-bit secret in every linear secret sharing scheme realizing $k$-uniform access structures using CDS protocol. In this paper, we provide efficient constructions on the share size of linear secret sharing schemes for sparse and dense $k$-uniform access structures (or forbidden $k$-homogeneous access structures) for a constant $k$ using the hypergraph decomposition technique and the monotone span programs as follows.
Theorem 1.1. Let $\Gamma$ be a sparse $k$-uniform access structure whose size is at most $n^{1+\beta}$, where $0 \leq \beta < 1$. Then there exists a linear secret sharing scheme for an access structure $\Gamma$ with the total share size
\[ O \left( \frac{k^2 - 3k + 2}{n^2 - 2k + 2} \cdot \left( \frac{k^2 - 3k + 2}{k^2 - 2k + 2} \right)^\beta \log^{k+1} n \right). \]

Theorem 1.2. Let $\Gamma$ be a dense $k$-uniform access structure whose size is at least $(\binom{n}{k}) - n^{1+\beta}$, where $0 \leq \beta < 1$. Then there exists a linear secret sharing scheme for an access structure $\Gamma$ with the total share size
\[ O \left( \frac{k^2 - 3k + 2}{n^2 - 2k + 2} \cdot \left( \frac{k^2 - 3k + 2}{k^2 - 2k + 2} \right)^\beta \log^{k+1} n \right). \]

Our paper is organized as follows. In Section 2, we introduce the definition of Secret Sharing Scheme and two interesting secret sharing schemes which are Shamir’s Threshold Secret Sharing Scheme and Monotone Span Programs. In Section 3, we introduce several access structures related to this paper. In Section 4 and Section 5, we present the results and lemmas, which are necessary for proving our main theorems. In Section 6 and Section 7, we give the proof of Theorem 1.1 and Theorem 1.2.

2 Secret Sharing Scheme

A secret sharing scheme involves a dealer who has a secret, a set of $n$ participants, and a collection $F$ of subsets of participants defined as the access structure. A secret sharing scheme for $F$ is a method by which the dealer distributes shares of a secret value $k$ to the set of $n$ participants such that any qualified subset in $F$ can reconstruct the secret value $k$ from their shares and any unqualified subset not in $F$ cannot reveal any information about the secret value $k$. By using the entropy function we define the secret sharing scheme.

For the given random variable $X$, we define the entropy of $X$ as
\[ H(X) = -\sum Pr(X = x) \log Pr(X = x), \]
where the sum is taken over all values $x$ and $Pr(X = x) > 0$. For the two random variables $X$ and $Y$, we define the conditional entropy as $H(X|Y) = H(XY) - H(Y)$. Clearly we obtain that $0 \leq H(X|Y) \leq H(X)$ and the following two properties hold: (1) two random variables $X$ and $Y$ are independent iff $H(X|Y) = H(X)$ and (2) the value of $Y$ implies the value of $X$ iff $H(X|Y) = 0$.

Let $P$ be a set of $n$ participants where $P = \{p_1, p_2, \ldots, p_n\}$. Let $F$ be a collection of subsets of participants defined as an access structure. It means that sets in $F$ are qualified and sets not in $F$ are unqualified. Assume that there is the probability distribution on the domain of secrets. We also consider the probability distribution on the vector of share of any subset of $n$ participants. We
define the random variable denoting the secret as $S$. Let us define the random variable denoting the share values of any subset $X$ of $n$ participants as $S_X$.

**Definition 2.1** (Secret Sharing Scheme). For the given probability distribution on the secrets, we say that a distribution scheme is a Secret Sharing Scheme realizing an access structure if the following two requirements hold:

**Correctness.** For every qualified set $B \in \mathcal{F}$,

$$H(S \mid S_B) = 0.$$  

**Privacy.** For every unqualified set $T \notin \mathcal{F}$,

$$H(S \mid S_T) = H(S).$$  

The one parameter for measuring the efficiency of a secret sharing scheme is the information rate, which is defined as the ratio between the length of secret and the maximum length of the shares given to the participants. Since the length of any share is greater than or equal to the length in a secret sharing scheme, the information rate cannot be greater than one. Secret sharing schemes with an information rate equal to one are called *ideal secret sharing schemes*. The following Shamir’s threshold secret sharing scheme is ideal.

### 2.1 Shamir’s Threshold Secret Sharing Scheme

In 1979, Shamir [42] introduced a $(t, n)$-threshold secret sharing scheme as the first works about the secret sharing, in which the qualified subsets are formed by all the subsets with at least $t$ participants in a set of $n$ participants. Let $P$ be a set of $n$ participants where $P = \{p_1, p_2, \ldots, p_n\}$. Let $\mathcal{F}_t = \{A \subseteq \{p_1, p_2, \ldots, p_n\} \mid |A| \geq t\}$, where $1 \leq t \leq n$ is an integer, be a collection of subsets of participants defined as an access structure. It means that sets in $\mathcal{F}_t$ are qualified and sets not in $\mathcal{F}_t$ are unqualified. The domain of secrets and shares is defined as the elements of a finite field $\mathbb{F}_q$ for some prime power $q > n$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be $n$ elements of a finite field $\mathbb{F}_q$ corresponding to each participant $p_i$, where $1 \leq i \leq n$. To distribute shares of a secret value $k$ to the set of $n$ participants, a dealer chooses $t - 1$ random elements $a_1, a_2, \ldots, a_{t-1}$ uniformly and independently from the finite field $\mathbb{F}_q$ to define the following polynomial of degree at most $t - 1$.

$$P(x) = k + \sum_{i=1}^{t-1} a_i x^i$$

where $k$ is a secret which is in the field $\mathbb{F}_q$.

We define the value of $s_j = P(\alpha_j)$ as the share of each participant $p_j$, where $1 \leq j \leq t$. Note that the size of each share is same as the size of the secret. We claim that every set $B = \{p_{i_1}, p_{i_2}, \ldots, p_{i_t}\}$ of size $t$ among $n$ participants can reconstruct the secret value $k$. Let us consider the following polynomial of degree at most $t - 1$.
\[ Q(x) = \sum_{l=1}^{t} s_i \prod_{1 \leq j \leq t, j \neq l} \frac{\alpha_{ij} - x}{\alpha_{ij} - \alpha_i}. \]

Note that \( P(\alpha_{i}) = s_i = Q(\alpha_{i}) \) for all \( 1 \leq l \leq t \). By using the Lagrange’s interpolation theorem, the polynomial \( Q \) are equivalent to the polynomial \( P \) and \( Q(0) = P(0) = k \). It means that every set \( B \) can reconstruct the secret value \( k \) by computing

\[ k = Q(0) = \sum_{l=1}^{t} s_i \prod_{1 \leq j \leq t, j \neq l} \frac{\alpha_{ij}}{\alpha_{ij} - \alpha_i} \]

which is a linear combination of the shares and \( \prod_{1 \leq j \leq t, j \neq l} \frac{\alpha_{ij}}{\alpha_{ij} - \alpha_i} \) depends only on the set \( B \). Therefore, it satisfies the first requirement.

For any unqualified set \( T = \{p_{j_1}, p_{j_2}, \ldots, p_{j_{t-1}}\} \) with size \( t - 1 \), there exists an unique polynomial \( P_a \) of degree at most \( t - 1 \) with \( P_a(0) = a \) and \( P_a(\alpha_{j}) = s_{j} \) for every secret \( a \in \mathbb{F}_q \), where \( 1 \leq j \leq t - 1 \), such that the probability computing a vector of shares is same as \( \frac{1}{q^{t-1}} \) for every secret \( a \in \mathbb{F}_q \). Therefore, it satisfies the second requirement.

### 2.2 The Monotone Span Programs

In 1993, Karchmer and Wigderson [35] introduced the monotone span programs from which the linear secret sharing schemes can be constructed. In the linear secret sharing schemes, the secret is an element of the field and each share is a vector over the field whose each coordinate is expressed as a linear combination of the secret and the coordinates of the random strings which are taken from some finite field. Let \( P \) be a set of \( n \) participants where \( P = \{p_1, p_2, \ldots, p_n\} \). Let \( \mathcal{F} \) be a collection of subsets of participants defined as an access structure.

**Definition 2.2** (Monotone Span Program). Let \( \mathbb{F} \) be a finite field. Let \( M \) be an \( \alpha \times \beta \) matrix over the field \( \mathbb{F} \) where \( \rho : \{1, 2, \ldots, \alpha\} \rightarrow \{p_1, p_2, \ldots, p_n\} \) labels each row of the Matrix \( M \) by one participant among \( n \) participants. For any subset \( X \subseteq \{p_1, p_2, \ldots, p_n\} \), we denote \( M_X \) be the sub matrix obtained from the matrix \( M \) by restricting all \( \alpha \) rows to the rows labeled by participants in \( X \). A Monotone Span Program \( \mathcal{M} \) over the finite field \( \mathbb{F} \) consists of above triple \( (\mathbb{F}, M, \rho) \). We say that the Monotone Span Program \( \mathcal{M} \) accepts the set \( B \subseteq \{p_1, p_2, \ldots, p_n\} \) if the rows of the submatrix \( M_B \) span a vector \( e_1 = (1, 0, 0, \ldots, 0) \) or a target vector \( v \).

In the following Lemma, Karchmer and Wigderson [35] proved that every monotone span program over finite fields implies a linear secret sharing scheme for an access structure consisting of all sets which are accepted by the monotone span program \( \mathcal{M} \).

**Lemma 2.3** (Karchmer and Wigderson [35]). Let \( \mathcal{M} \) be a monotone span program accepting all sets in an access structure \( \mathcal{F} \) consisting of a finite field \( \mathbb{F} \), an \( \alpha \times \beta \) matrix \( M \), and a function \( \rho \) labeling \( j \)-th rows of \( M \) by a participant \( p_j \). Then there exists a linear secret sharing scheme for an access structure \( \mathcal{F} \) such that the share of a participant \( p_j \) is a vector in \( \mathbb{F}^{\alpha j} \).
Proof. For the given monotone span program $M$, we define a linear secret sharing scheme as follows. Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be $n$ elements of a finite field $F$ corresponding to each participant $p_i$, where $1 \leq i \leq n$. To distribute shares of a secret value $k$ to the set of $n$ participants, a dealer chooses $b - 1$ random elements $r_2, r_3, \cdots, r_b$ uniformly and independently from the finite field $F$ to define $r = (k, r_2, r_3, \cdots, r_b)$. We define the value of $s_j$ satisfying the following equation as the share of each participant $p_j$, where $1 \leq j \leq t$.

$$(s_1, s_2, \cdots, s_\alpha) = Mr.$$ 

We claim that every set $B$ in an access structure $\mathcal{F}$ can reconstruct the secret value $k$. Let us consider the submatrix $M_B$ obtained by restricting all $\alpha$ rows of the matrix $M$ to the rows labeled by participants in $B$. Since there exists some vector $v$ such that $e_1 = vM_B$, the rows of the submatrix $M_B$ span the vector $e_1 = (1, 0, 0, \cdots, 0)$. Therefore, we say that the Monotone Span Program $\mathcal{M}$ accepts every set $B$ in an access structure $\mathcal{F}$. The shares $s_i$ of every participant $p_i$ in the set $B$ satisfies $(s_1, s_2, \cdots, s_{|B|}) = M_B r$. Then we conclude that

$$v(M_BR) = (vM_B)r = e_1 \cdot r = k.$$ 

It means that every set $B$ in an access structure $\mathcal{F}$ can reconstruct the secret value $k$ by computing $v(M_BR)$.

Now we claim that for every set $T \notin \mathcal{F}$ the rows of $M_T$ do not span the vector $e_1$. We denote the matrix containing all rows of $M_T$ and additional row $e_1$ by $\left( M_T \atop e_1 \right)$. From the property $\text{rank}(M_T) < \text{rank}(\left( M_T \atop e_1 \right))$, we say that there exists some vector $w \in F^b$ such that $(M_T)w = 0$ and $e_1 \cdot w = 1$.

To distribute shares of a secret value $k \in F$ to every participant, we define $r = (k, r_2, r_3, \cdots, r_b)$ with $b - 1$ random elements which are chosen by a dealer. Since the shares of every participant $p_i$ in the set $T$ are $(s_1, s_2, \cdots, s_{|T|}) = M_TR$, we conclude that

$$(M_T)r' = M_T(r - kw) = (M_T)r + k(M_T)w = (M_T)r = (s_1, s_2, \cdots, s_{|T|})$$

for $r' = r - kw$.

It means that the probability that the shares are generated is the same for every secret $k \in F$. 

3 Access Structures

The qualified subsets in the secret sharing scheme are the subsets of participants who can reconstruct the secret value from their shares. A collection of qualified subsets of participants called the access structure of the secret sharing scheme. In other words, the unqualified subsets in the secret sharing scheme are the collection of participants who cannot have any information about the secret value from their shares. In any secret sharing scheme, an access structure is considered to be monotone, in which the superset of the qualified subsets is a qualified subset and determined by the family of minimal qualified subsets of participants. A collection of minimal qualified subsets of
participants called the basis of the access structure. In a secret sharing scheme, every participant must be in at least one minimal qualified subset amongst them.

### 3.1 Graph Access Structures

A graph access structure is represented by a graph $G = (V, E)$ and has the following property: a pair of vertices (participants) connected by an edge can reconstruct the secret value from their shares in the secret sharing scheme and independent vertices (participants) in the graph $G$ does not get any information on the secret value. A trivial secret sharing scheme realizing a graph access structure shares the secret value independently for each edge in which the total share size is $O(n^2)$. An improved linear secret sharing scheme realizing every graph access structure was given by Erdos and Pyber [28] in which the total share size is $O(n^2 / \log n)$. Secret sharing schemes realizing graph access structures have been studied by many authors [5, 16–19, 21–25, 27, 29].

The motivation for studying secret sharing schemes for graph access structures is that they are simpler than secret sharing schemes for general access structures and later generalized to general access structures. Recently, in 2020, Peter [31] proved that for every constant $0 < c < \frac{1}{2}$ a secret sharing scheme for graph access structure with the share size $O(n^c)$ implies a secret sharing scheme for any access structure with the share size $2^{O(0.5+c)n}$. It means that improved secret sharing schemes in the share size for all graph access structures will result in improved secret sharing schemes for all access structures. For the dense graph access structures having at least $\left(\binom{n}{2} - n^{1+\beta}\right)$ edges, where $0 \leq \beta < 1$, Beimel, Farras, and Mintz [5] constructed a linear secret sharing scheme with the total share size $O(n^{5/4 + 3\beta/4})$.

### 3.2 Forbidden Graph Access Structures

In 1997, Sun and Shieh [45] introduced secret sharing schemes for forbidden graph access structures in which the participants correspond to the vertices of the graph $G$ and a pair of vertices can reconstruct the secret value from their shares in the secret sharing scheme if they are connected by an edge or their size is at least 3. Secret sharing schemes for graph access structures and forbidden graph access structures are very similar. However, graph access structures are harder to realize than forbidden graph access structures. From the given secret sharing scheme realizing graph access structures, we can construct secret sharing schemes realizing forbidden graph access structures by giving a share of the graph secret sharing schemes and a share of $(3, n)$-threshold secret sharing schemes. However, the total share size of the new scheme is slightly greater than the former scheme. It means that bounds on the share size of secret sharing schemes for graph access structures imply the bounds on the share size of secret sharing schemes for forbidden graph access structures.

In 2014, Beimel, Ishai, Kumaresan, and Kushilevitz [9] constructed a secret sharing scheme realizing all forbidden graph access structures with the total share size $O(n^{3/2})$. Later, in 2015, a linear secret sharing scheme for all forbidden graph access structures was given by Gay, Kerenidis, and Wee [32] in which the total share size is $O(n^{3/2})$. Recently, in 2017, Liu, Vaikuntanathan, and Wee [36] proved that every forbidden graph access structure could be realized by a non-linear secret sharing scheme with the total share size $n^{1+o(1)}$. For the forbidden dense graph access structures having at least $\left(\binom{n}{2} - n^{1+\beta}\right)$ edges, where $0 \leq \beta < \frac{1}{2}$, Beimel, Farras, and Peter [7] constructed a linear
secret sharing scheme with the total share size $O(n^{7/6+2\beta/3})$. Later, in 2020, Beimel, Farras, Mintz, and Peter [6] provided efficient constructions on the share size of linear secret sharing schemes for forbidden sparse and dense graph access structures based on the monotone span programs.

### 3.3 $k$-homogeneous access structures

A hypergraph is a generalization of a graph in which hyperedges may connect more than two vertices. A $k$-uniform hypergraph (or $k$-hypergraph) is a hypergraph in which each hyperedge has exactly $k$ vertices (or $k$-hyperedge). In particular, the complete $k$-uniform hypergraph on $n$ vertices has all $k$-subsets of $\{1, 2, \cdots, n\}$ as $k$-hyperedges. A $k$-hypergraph access structure is represented by a $k$-uniform hypergraph $\mathcal{H}$ in which the participants correspond to the vertices of the hypergraph $\mathcal{H}$, and a set of vertices can reconstruct the secret value from their shares if they are connected by a $k$-hyperedge, and the set of non-adjacent vertices does not get any information on the secret. A $k$-hypergraph access structure is also called a $k$-homogeneous access structure.

A $k$-homogeneous access structure is determined by the family of minimal qualified subsets with exactly $k$ different participants or $k$-uniform hypergraphs $\mathcal{H}$. Recall that the qualified subsets in the $(k, n)$-threshold secret sharing scheme are formed by all the subsets with at least $k$ participants in the set of $n$ participants. For example, if we consider the access structure on a set of five participants $P = \{p_1, p_2, p_3, p_4, p_5\}$ having minimal qualified subsets $A_1 = \{p_1, p_2, p_3\}$, $A_2 = \{p_2, p_3, p_4\}$, $A_3 = \{p_3, p_4, p_5\}$, we check that it is not $(3, n)$-threshold but $3$-homogeneous. Note that there is a one-to-one correspondence between $k$-uniform hypergraphs and $k$-homogeneous access structures. Also, there is a one-to-one correspondence between complete $k$-uniform hypergraphs and $(k, n)$-threshold access structures.

The secret sharing schemes for $k$-homogeneous access structures have been constructed by many authors based on various techniques. In 1990, Benaloh and Leichter [12] constructed a secret sharing scheme for the $k$-homogeneous access structure with total share size $O(n^k/\log n)$. For the dense $k$-homogeneous access structure, a much more efficient secret sharing scheme was constructed by Beimel, Farras, and Mintz [5] in 2012, in which the total share size is $\tilde{O}(2^k k n^{2+\beta})$. Recently, in 2020, Beimel and Farras [4] proved that for almost all $k$-homogeneous access structures there exists a secret sharing scheme with maximum share size $2^{\tilde{O}(\sqrt{k \log n})}$, a linear secret sharing scheme with normalized maximum share size $\tilde{O}(n^{(k-1)/2})$, and a multi-linear secret sharing scheme with normalized maximum share size $\tilde{O}(\log^{k-1} n)$ for exponentially long secrets using Conditional Disclosure of Secrets (CDS) protocol.

### 3.4 $k$-uniform access structures

An access structure is defined as forbidden $k$-homogeneous (or forbidden $k$-hypergraph) determined by a $k$-uniform hypergraph $\mathcal{H}$ in which the set of vertices can reconstruct the secret value from their shares in the secret sharing scheme if they are connected by a $k$-hyperedge or their size is at least $k + 1$. We study the complexity of realizing a forbidden $k$-homogeneous access structure by linear secret sharing schemes. A forbidden $k$-homogeneous access structure has been studied by many authors [1, 2, 10, 45] under the terminology of $k$-uniform access structures. Secret sharing schemes for $k$-homogeneous structures and $k$-uniform structures are very similar. However, $k$-homogeneous access structures are harder to realize than $k$-uniform access structures. From
the given secret sharing scheme realizing \(k\)-homogeneous access structures, we can construct secret sharing schemes realizing \(k\)-uniform access structures by giving a share of the secret sharing schemes realizing \(k\)-homogeneous access structures and a share of \((k+1,n)\)-threshold secret sharing schemes. However, the total share size of the new scheme is slightly greater than the former scheme.

Recently, in 2018, Applebaum and Arkis \[1\] constructed an efficient secret sharing scheme for \(k\)-uniform access structures using multiparty Conditional Disclosure of Secrets (CDS) protocol. Later, in 2018, Beimel and Peter \[11\] obtained that every \(k\)-uniform access structure with a binary secret could be realized by a secret sharing scheme in which the share size is \(\min\{((O(n/k))^{(k-1)/2},O(n \cdot 2^{n/2})\})\). By improving their result, in 2019, Applebaum, Beimel, Farras, Nir, and Peter \[2\] obtained that every \(k\)-uniform access structure with a binary secret could be realized by a secret sharing scheme with share size \(2^O(\sqrt{k\log n})\) by combining CDS protocols and transformations. In 2020, Beimel, Farras, Mintz, and Peter \[6\] obtained the lower bound on the max share size for sharing an one-bit secret in every linear secret sharing scheme realizing \(k\)-uniform access structures using multiparty Conditional Disclosure of Secrets (CDS) protocol. In this paper, we provide efficient constructions on the share size of linear secret sharing schemes for sparse \(k\)-uniform access structure having at most \(n^{1+\beta}\) and dense \(k\)-uniform access structure having at least \(\binom{n}{k} - n^{1+\beta}\), where \(0 \leq \beta < 1\), for a constant \(k\) based on the hypergraph decomposition technique and the monotone span programs.

4 Hypergraph Decomposition

In this section, we describe the technique of hypergraph decomposition which plays an important role for proving the main theorem. A hypergraph decomposition technique is a generalization of graph decomposition studied in \[1,16,26,44\] and first introduced in \[16\]. A hypergraph is defined as a pair \((V,E)\) where \(V\) is a non-empty set of vertices and \(E\) is a set of non-empty subsets of \(V\) called hyperedges. A \(k\)-uniform hypergraph is a hypergraph in which each hyperedge has exactly \(k\) vertices. In the hypergraph decomposition technique, we first represent \(k\)-homogeneous access structure (or \(k\)-uniform access structure) as a \(k\)-uniform hypergraph \(\mathcal{H}\). Then we decompose the \(k\)-uniform hypergraph in smaller sub-hypergraphs \(H_1, H_2, \ldots, H_m\) for which we construct efficient secret sharing schemes and such that all the hyperedges in \(\mathcal{H}\) belong to at least one of \(H_i\), where \(1 \leq i \leq m\). The secret sharing schemes for \(k\)-uniform hypergraphs are obtained as an union of the secret sharing schemes for all sub-hypergraphs \(H_1, H_2, \ldots, H_m\). The following is the definition of the hypergraph decomposition in the graph theory.

**Definition 4.1 (Hypergraph Decomposition).** Let \(\mathcal{H} = (V,E)\) be a hypergraph and let \(\mathcal{H}_i(V_i,E_i)\) be a sub-hypergraph of a hypergraph \(\mathcal{H}\) such that \(V_i \subset V\) and \(E_i \subset E\), where \(1 \leq i \leq m\). The set \(\mathcal{F} = \{\mathcal{H}_1,\mathcal{H}_2,\ldots,\mathcal{H}_m\}\) is said to be a decomposition of \(\mathcal{H}\) if and only if each hyperedge in the hypergraph \(\mathcal{H}\) belongs to at least one \(\mathcal{H}_i\), where \(1 \leq i \leq m\).

In this paper, we consider sub-hypergraphs as the class of \(k\)-partite \(k\)-uniform hypergraphs for \(k \geq 2\). A \(k\)-uniform hypergraph is said to be \(k\)-partite if its vertex set can be partitioned into \(k\) nonempty sets \(V_1, V_2, \ldots, V_k\) in such a way that every hyperedge intersects every set \(V_i\) of the partition in exactly one vertex, where \(1 \leq i \leq k\). In this paper, we utilize the following result that every \(k\)-uniform hypergraph can be decomposed into the set of sub-hypergraphs consisting of \(O(\log n)\) \(k\)-partite \(k\)-uniform hypergraphs. It means that \(k\)-uniform hypergraph is covered by \(k\)-partite \(k\)-uniform hypergraphs of size \(O(\log n)\).
Lemma 4.2. Let $H = (V, E)$ be a $k$-uniform hypergraph and let $H_i(V_i, E_i)$ be a $k$-partite $k$-uniform sub-hypergraph of a hypergraph $H$ such that $V_i \subset V$ and $E_i \subset E$, where $1 \leq i \leq m$. Then the $k$-uniform hypergraph $H$ is covered by the set $F = \{H_1, H_2, \cdots, H_m\}$ consisting of $k$-partite $k$-uniform hypergraphs, where $m = \Theta(\log n)$.

Proof. For every $i \in [\Theta(\log n)]$, take random mapping $\phi_i : V \rightarrow \{1, 2, \cdots, k\}$. For $i \in [\Theta(\log n)]$, let $X_i$ be the indicator random variable for the event the given hyperedge $e = (v_1, v_2, \cdots, v_k)$ in the hypergraph $H$ appears as a hyperedge in the sub-hypergraph $H_i$. For the random variable $X$ satisfying $X = \sum_{i=1}^{\Theta(\log n)} X_i$, we have

$$E(X) = \sum_{i=1}^{\Theta(\log n)} Pr(\{\phi_i(v_1), \phi_i(v_2), \cdots, \phi_i(v_k)\} \text{ covers } [k]) = \sum_{i=1}^{\Theta(\log n)} \frac{k!}{k^k} = O(\log n) \cdot \frac{k!}{k^k}$$

Using the second variant of Chernoff bound, we obtain

$$Pr\left( X \leq \left(1 - \left(1 - \frac{k^2}{k^k+1}\right)\cdot O(\log n) \cdot \frac{k!}{k^k}\right) \right) = Pr\left( X \leq O(\log n) \cdot \frac{k!}{k^k+1} \right)$$

$$\leq e^{-\frac{(1 - \frac{k^2}{k^k+1})^2 \cdot O(\log n) \cdot \frac{k!}{k^k}}{2}} \leq e^{-1.5\log(n^k)} = n^{-1.5k}.$$ 

Therefore, we derive that

$$n^k \cdot Pr\left( X \leq O(\log n) \cdot \frac{k!}{k^k+1} \right) \leq n^k \cdot n^{-1.5k} = n^{-\frac{k}{2}} < 1$$

We conclude that each hyperedge in the $k$-uniform hypergraph $H$ belongs to at least one $k$-partite $k$-uniform sub-hypergraph $H_i$, where $1 \leq i \leq O(\log n)$. It means that the $k$-uniform hypergraph $H$ is covered by the set $F = \{H_1, H_2, \cdots, H_m\}$ consisting of $k$-partite $k$-uniform hypergraphs, where $m = O(\log n)$.

5 Constructions for $k$-partite $k$-uniform hypergraphs

To study the complexity of realizing a $k$-uniform access structure by linear secret sharing schemes, we utilize the technique of hypergraph decomposition in which secret sharing schemes for $k$-uniform hypergraphs are obtained as a union of the secret sharing schemes for all $k$-partite $k$-uniform sub-hypergraphs. In 1993, Karchmer and Wigderson proved that if an access structure can be described by a monotone span program, then it has an efficient linear secret sharing scheme. In this section, we first construct the linear secret sharing schemes for $k$-partite $k$-uniform hypergraphs using monotone span programs. Using these constructions, we give more efficient linear secret sharing schemes for sparse and dense $k$-uniform hypergraphs in Section 6. In order to do so, we first need the following lemma about the construction of linear spaces corresponding to vertices.
Lemma 5.1. Let $\mathcal{H}(V,E)$ be a $k$-partite $k$-uniform hypergraph, where $V$ is a set of vertices and $E$ is a set of hyperedges satisfying the following condition. Suppose that $V$ is partitioned into $A_1 \cup A_2 \cup \cdots \cup A_k$ with $|A_i| = m_i$. Let $E$ be the family of subsets with exactly one vertex in common with each $A_i$ as follows.

$$E = \{(a_{1,i_1}, \ldots, a_{k,i_k}) \mid a_{1,i_1} \in A_1, \ldots, a_{k,i_k} \in A_k\}.$$  

Suppose that every vertex in $A_k$ is contained in at most $d$ members in $E$ for some $d \leq n$. Let $\mathbf{F}$ be a finite field with $|\mathbf{F}| \geq m_1 + \cdots + m_{k-1}$. Let us denote $A_j = \{a_{j,1}, \ldots, a_{j,m_j}\}$, where $1 \leq j \leq k$. For every $1 \leq j \leq k-1$, there exist a linear space $V_{j,t} \subseteq \mathbf{F}^{(d+1)^{k-1}}$ corresponding to a vertex $a_{j,t}$ in the set $A_j$, where $1 \leq t \leq m_j$. Also, there exists a vector $z_{k,i_k} \in \mathbf{F}^{(d+1)^{k-1}}$ corresponding to each vertex $a_{k,i_k}$ in the set $A_k$ such that

$$z_{k,i_k} \in V_{i_1,j_1}, \ldots, z_{k,i_k} \in V_{k-1,i_{k-1}} \iff (a_{1,i_1}, \ldots, a_{k-1,i_{k-1}}, a_{k,i_k}) \in Q.$$  

where $1 \leq i_1 \leq m_1, \ldots, 1 \leq i_k \leq m_k$.

Proof. Let $v = (v_{(0,\ldots,0)}, v_{(j_1,\ldots,j_{k-1})}, \ldots, v_{(d,\ldots,d)})$ be a vector in the finite field $\mathbf{F}^{(d+1)^{k-1}}$, where $0 \leq j_1, \ldots, j_{k-1} \leq d$. First, we construct the following polynomial of degree $(k-1)d$ whose coefficients correspond to coordinates of the vector $v$.

$$v(X_1, \ldots, X_{k-1}) = \sum_{0 \leq j_1, \ldots, j_{k-1} \leq d} \gamma_{j_1,\ldots,j_{k-1}} X_1^{j_1} \cdots X_{k-1}^{j_{k-1}} \in \mathbf{F}[X_1, \ldots, X_{k-1}]$$

in which the coefficient $\gamma_{j_1,\ldots,j_{k-1}}$ is same as the coordinate $v_{(j_1,\ldots,j_{k-1})}$ in a vector $v$ in $\mathbf{F}^{(d+1)^{k-1}}$, where $0 \leq j_1, \ldots, j_{k-1} \leq d$.

For $1 \leq j \leq k$, let us consider an element $a_{j,i_j}$ in the field $\mathbf{F}$ corresponding to a vertex $a_{j,i_j}$ in $A_j$, where $1 \leq i_j \leq m_j$. Now we define a linear space $V_{j,i_j} \subseteq \mathbf{F}^{(d+1)^{k-1}}$ corresponding to a vertex $a_{j,i_j}$ in $A_j$, where $1 \leq j \leq k-1$, as follows. For every $1 \leq j \leq k-1$, let us define the linear space $V_{j,i_j}$ as the space of polynomials $P(X_1, \ldots, X_{k-1})$ of degree $(k-1)d$ satisfying $P(X_1, \ldots, X_{j-1}, a_{j,i_j}, X_{j+1}, \ldots, X_{k-1}) = 0$, where $1 \leq i_j \leq m_j$.

Since every vertex in $A_k$ is contained in at most $d$ members in $Q$ for some $d \leq n$, for each vertex $a_{k,i_k}$ in $A_k$, where $1 \leq i_k \leq m_k$, first we define the family of sets in $Q$ containing $a_{k,i_k}$ as

$$Q_{i_k} = \{(a_{1,i_1,t}, \ldots, a_{k-1,i_{k-1},t}, a_{k,i_k}) \mid a_{1,i_1,t} \in A_1, \ldots, a_{k-1,i_{k-1},t} \in A_{k-1} and 1 \leq t \leq d'\}$$

for some $d' \leq d$.

Now let us define a vector $z_{k,i_k} \in \mathbf{F}^{(d+1)^{k-1}}$ corresponding to each vertex $a_{k,i_k}$ in the set $A_k$, where $1 \leq i_k \leq m_k$, whose coordinates correspond to the coefficients of the following polynomial of degree $(k-1)d$. 

12
There exists a linear secret sharing scheme for a k-partite k-uniform hypergraphs satisfying the following condition based on the monotone span programs. We utilize the following lemma for constructing more efficient linear secret sharing schemes for spare k-partite k-uniform hypergraphs in Section 6, when the size of all k parts is the same.

**Lemma 5.2.** Let \( \mathcal{H}(V, E) \) be a k-partite k-uniform hypergraph, where \( V \) is a set of vertices and \( E \) is a set of hyperedges satisfying the following condition. Suppose that \( V \) is partitioned into \( A_1 \cup A_2 \cup \cdots \cup A_k \) with \( |A_i| = m_i \). Let \( E \) be the family of subsets with exactly one vertex in common with each \( A_i \) as follows.

\[
E = \{(a_{1,i_1}, \cdots, a_{k,i_k}) \mid a_{1,i_1} \in A_1, \cdots, a_{k,i_k} \in A_k\}.
\]

Suppose that every vertex in \( A_k \) is contained in at most \( d \) members in \( E \) for some \( d \leq n \). Then there exists a linear secret sharing scheme for a k-uniform access structure \( \Gamma \) determined by \( \mathcal{H}(V, E) \) with total share size \( m_k + (d + 1)^{k-1}(m_1 + \cdots + m_{k-1}) \).

**Proof.** Let \( \Gamma \) be a k-uniform access structure determined by \( \mathcal{H}(V, E) \). First, we construct a monotone span program accepting this k-uniform access structure \( \Gamma \) using \( (d + 1)^{k-1} \) rows labeled by \( a_{j,i_j} \), where \( 1 \leq j \leq k-1 \) and \( 1 \leq i_j \leq m_j \), and one row labeled by \( a_{k,i_k} \), where \( 1 \leq i_k \leq m_k \). Using Lemma 5.1, there exists a linear space \( V_{j,i_j} \subseteq \mathbb{F}^{(d+1)^{k-1}} \) corresponding to a vertex \( a_{j,i_j} \) in the set \( A_j \), where \( 1 \leq j \leq k-1 \). Let us denote the basis of the linear space \( V_{j,i_j} \subseteq \mathbb{F}^{(d+1)^{k-1}} \) as \( \{v_{j,i_j,1}, \cdots, v_{j,i_j,(d+1)^{k-1}-1}\} \).

To construct \( (d + 1)^{k-1} \) rows labeled by \( a_{j,i_j} \), we consider the following vector in \( \mathbb{F}^{(d+1)^{k-1}+k} \)

\[
\{v'_{j,i_j,1}, \cdots, v'_{j,i_j,(d+1)^{k-1}-1}, e_j' = (e_{k-j+1}, 0, 0, \cdots, 0)\}.
\]  

(5.1)

where \( v'_{j,i_j,l} = (0, \cdots, 0, v_{j,i_j,l}) \) is a vector in \( \mathbb{F}^{(d+1)^{k-1}+k} \) and \( e_1, \cdots, e_k \) are standard basis vectors in \( \mathbb{F}^k \).
To construct one row labeled by $a_{k,i_k}$, we consider the following vector in $\mathbb{F}^{(d+1)^{k-1}+k}$

$$z'_{k,i_k} = (1, 0, \cdots, 0, z_{k,i_k})$$ (5.2)

where the vector $z_{k,i_k} \in \mathbb{F}^{(d+1)^{k-1}}$ is obtained in Lemma 5.1

Let us set a target vector in $\mathbb{F}^{(d+1)^{k-1}+k}$ as

$$(1, 1, \cdots, 1, 0_{(d+1)^{k-1}})$$

where $0_{(d+1)^{k-1}}$ is a zero vector in $\mathbb{F}^{(d+1)^{k-1}}$.

Using Lemma 5.1, we obtain that

$$z_{k,i_k} \in V_{1,j_1}, \cdots, z_{k,i_k} \in V_{k-1,i_{k-1}}.$$ 

Then the target vector $(1, 1, \cdots, 1, 0_{(d+1)^{k-1}})$ must be in the span of all vectors in (5.1) and (5.2).

Therefore we conclude that a $k$-uniform access structure $\Gamma$ can be accepted by this monotone span program, then it has an efficient linear secret sharing scheme with total share size $m_k + (d+1)^{k-1}(m_1 + \cdots + m_{k-1})$.

Also, we investigate a linear secret sharing scheme for $k$-partite $k$-uniform hypergraphs satisfying the following condition based on the monotone span programs. We utilize the following lemma for constructing more efficient linear secret sharing schemes for dense $k$-partite $k$-uniform hypergraphs in Section 6, when the size of all $k$ parts is the same.

**Lemma 5.3.** Let $\mathcal{G}(V,E)$ be a $k$-partite $k$-uniform hypergraph, where $V$ is a set of vertices and $E$ is a set of hyperedges satisfying the following condition. Suppose that $V$ is partitioned into $A_1 \cup \cdots \cup A_k$ with $|A_1|=\cdots=|A_{k-1}|= n, |A_k|= m_k \leq n$. Let $E$ be the family of subsets with exactly one vertex in common with each $A_i$ as follows.

$$E = \{(a_{1,i_1}, \cdots, a_{k,i_k}) \mid a_{1,i_1} \in A_1, \cdots, a_{k,i_k} \in A_k\}.$$ 

Suppose that every vertex in $A_k$ is contained in at least $n - d$ members in $E$ for some $d \leq n$. Then there exists a linear secret sharing scheme for a $k$-uniform access structure $\Gamma'$ determined by $\mathcal{G}(V,E)$ with total share size $2m_k + (d + 1)^{k-1}(k - 1)n$.

**Proof.** Let $\mathcal{U}$ be the family of all subsets with exactly one vertex in common with each part $A_i$, where $1 \leq i \leq k$. First, let us consider the complement of a family $E$, which is denoted by $\overline{E}$, consisting of all subsets in the given universal family $\mathcal{U}$ that are not in $E$. Since every vertex in $A_k$ is contained in at least $n - d$ members in $E$, every vertex in $A_k$ must be contained in at most $d$ members in $\overline{E}$.

Using Lemma 5.1, there exist a linear space $V_{j,i_j} \subseteq \mathbb{F}^{(d+1)^{k-1}}$ corresponding to a vertex $a_{j,i_j}$ in $A_j$, where $1 \leq i_j \leq m_j$, $1 \leq j \leq k - 1$, and a vector $z_{k,i_k} \in \mathbb{F}^{(d+1)^{k-1}}$ corresponding to a vertex $a_{k,i_k}$ in the set $A_k$ such that

$$z_{k,i_k} \in V_{1,i_1}, \cdots, z_{k,i_k} \in V_{k-1,i_{k-1}} \iff (a_{1,i_1}, \cdots, a_{k-1,i_{k-1}}, a_{k,i_k}) \in \overline{E}.$$ (5.3)
where \(1 \leq i_1, \cdots, i_{k-1} \leq n, 1 \leq i_k \leq m_k\).

Let \(\Gamma'\) be a \(k\)-uniform access structure determined by \(G(V, E)\). Now we construct a monotone span program accepting this \(k\)-uniform access structure \(\Gamma'\) using \((d + 1)^{k-1}\) rows labeled by \(a_{j,i_j}\), where \(1 \leq j \leq k - 1\) and \(1 \leq i_j \leq n\), and two rows labeled by \(a_{k,i_k}\), where \(1 \leq i_k \leq m_k\). Let us denote the basis of the linear space \(V_{j,i_j} \subseteq F^{(d+1)^k}\) as \(\{ v_{j,i_j,1}, \cdots, v_{j,i_j,(d+1)^{k-1}-1} \}\), where \(1 \leq j \leq k - 1\).

To construct \((d + 1)^{k-1}\) rows labeled by \(a_{j,i_j}\), where \(1 \leq j \leq k - 1\) and \(1 \leq i_j \leq n\), we consider the following vectors in \(F^{(d+1)^{k-1}+k}\)

\[
\{ v'_{j,i_j,1}, \cdots, v'_{j,i_j,(d+1)^{k-1}-1}, e_j = (e_{k-j+1}, 0, \cdots, 0) \}. \tag{5.4}
\]

where \(v'_{j,i_j,l} = (0, \cdots, 0, v_{j,i_j,l})\) is a vector in \(F^{(d+1)^{k-1}+k}\) and \(e_1, \cdots, e_k\) are standard basis vectors in \(F^k\).

To construct two rows labeled by \(a_{k,i_k}\), we consider the following two vectors in \(F^{(d+1)^{k-1}+k}\)

\[
z'_{k,i_k} = (0, 0, \cdots, 0, z_{k,i_k}), \quad (1, 0, \cdots, 0, 0_{(d+1)^{k-1}}) \tag{5.5}
\]

where \(0_{(d+1)^{k-1}}\) is a zero vector in \(F^{(d+1)^{k-1}}\).

Let us set a target vector in \(F^{(d+1)^{k-1}+k}\) as

\[(1, 1, \cdots, 1, w)\]

for some vector \(w\) in \(F^{(d+1)^{k-1}}\) which is not in all linear spaces \(V_{j,i_j}\), where \(1 \leq i_j \leq m_j, 1 \leq j \leq k - 1\).

Using the equation \((5.3)\), \((a_1,i_1, \cdots, a_{k-1,i_{k-1}}, a_{k,i_k}) \in E\) is equivalent to the following statement

\[z_{k,i_k} \not\in V_{1,i_1}, \cdots, z_{k,i_k} \not\in V_{k-1,i_{k-1}}\]

Now let us consider a vector \(w\) in the span of \(\{ z_{k,i_k}, V_{1,i_1}, \cdots, V_{k-1,i_{k-1}} \}\), where \(w \not\in V_{j,i_j}\) for every \(1 \leq j \leq k - 1\) and \(1 \leq i_j \leq n\). Then the target vector \((1, 1, \cdots, 1, w)\) must be in the span of all vectors in \((5.4)\) and \((5.5)\). Therefore we conclude that a \(k\)-uniform access structure \(\Gamma'\), which is determined by \(G(V, E)\), can be accepted by this monotone span program, then it has an efficient linear secret sharing scheme with total share size \(2m_k + (d + 1)^{k-1}(k - 1)n\).

\[\Box\]

6 Proof of Theorem 1.1

In this section, we prove Theorem 1.1 by providing efficient constructions on the share size of linear secret sharing schemes for sparse \(k\)-uniform access structures for a constant \(k\). To prove Theorem 1.1 we utilize the technique of hypergraph decomposition in which secret sharing schemes for \(k\)-uniform hypergraphs are obtained as a union of the secret sharing schemes for all \(k\)-partite \(k\)-uniform sub-hypergraphs. We need the following lemma for constructing more efficient linear secret sharing schemes for sparse \(k\)-partite \(k\)-uniform hypergraphs when the size of all \(k\) parts is the
Lemma 6.1. Let $\mathcal{H}(V, E)$ be a $k$-partite $k$-uniform hypergraph, where $V$ is a set of vertices and $E$ is a set of hyperedges satisfying the following condition. Suppose that $V$ is partitioned into $A_1 \cup \cdots \cup A_k$ with $|A_i| = m_i$. Let $E$ be the family of subsets with exactly one vertex in common with each $A_i$ as follows.

$$E = \{(a_{1,i_1}, \ldots, a_{k,i_k}) \mid a_{1,i_1} \in A_1, \ldots, a_{k,i_k} \in A_k\}.$$  

Suppose that $m_1 = \cdots = m_{k-1} = n$, $m_k \leq n$, and every vertex in $A_k$ is contained in at most $d$ members in $E$ for some $d \leq n$. If $d|A_k|^{k-1} \geq n^{k-1} \log^{k^2-2k+2} n$, then there exists a linear secret sharing scheme for a $k$-uniform access structure $\Gamma$, which is determined by $\mathcal{H}(V, E)$, with total share size

$$O\left(n^{k-2k+2} \sqrt{n^{k-1} |A_k|^{k^3-3k+3} d(k-1)^2} \log^{k-1} n\right).$$

Proof. Let $d = n^\tau$ and $|A_k| = n^\lambda \leq n$, where $\tau = \log d$ and $\lambda = \log |A_k|$. From the condition $d|A_k|^{k-1} \geq n^{k-1} \log^{k^2-2k+2} n$, we obtain

$$n^{\frac{k-2k+2}{k^2-2k+2} + \frac{(k-1)\lambda}{k^2-2k+2} - \frac{k-1}{k^2-2k+2}} \geq \log n.$$  

(6.1)

Let $\alpha = \frac{\lambda}{k^2-2k+2} - \frac{(k-1)\tau}{k^2-2k+2} + \frac{k^2-2k+1}{k^2-2k+2}$. In order to prove Lemma 6.1, first we prove that there exists a partition of $A_i$ into $l$ parts $A_{i,1}, \ldots, A_{i,l}$ of size $n^\alpha$ for $1 \leq i \leq k-1$, where $l = 2n^{1-\alpha} \ln n$, satisfying that for every $1 \leq i, \ldots, i_k \leq l$, every vertex in $A_k$ is contained in at most $2n^{(k-1)\alpha + \tau - k+1}$ members in

$$E_{i_1, \ldots, i_{k-1}} = \{(a_{1,i_1}, \ldots, a_{k-1,i_{k-1}}, a_{k,i_k}) \mid a_{1,i_1} \in A_{1,i_1}, \ldots, a_{k-1,i_{k-1}} \in A_{k-1,i_{k-1}}, a_{k,i_k} \in A_k\}.$$  

Now we choose $A_{1,i_1}, \ldots, A_{k-1,i_{k-1}}$ of size $n^\alpha$ independently with uniform distribution for every $1 \leq i_1, \ldots, i_k \leq l$. Then we have

$$Pr(A_i \not\subseteq \bigcup_{j=1}^l A_{i,j}) = \sum_{a \in A_i} \prod_{j=1}^l Pr(a \not\in A_{i,j})$$

$$= \sum_{a \in A_i} \left(1 - \frac{n^\alpha}{n}\right)^l \leq \sum_{a \in A_i} e^{-n^\alpha l} = n \cdot \frac{1}{n^2} = \frac{1}{n}$$  

(6.2)

for every $1 \leq i \leq k-1$.

Let $x_{(i_1, \ldots, i_k)}$ be a value in $X_{(i_1, \ldots, i_k)}$. For every vector $x = (x_{(j_1, \ldots, j_k)})_{(j_1, \ldots, j_k) \neq (i_1, \ldots, i_k)}$, let us consider

$$p_x = Pr\left(X_{(i_1, \ldots, i_k)} = 1 \mid X_{(j_1, \ldots, j_k)} = x_{(j_1, \ldots, j_k)} \text{ for all } (j_1, \ldots, j_k) \neq (i_1, \ldots, i_k)\right).$$

From the equation $n^{\frac{\lambda}{k^2-2k+2} + \frac{(k-1)\tau}{k^2-2k+2} + \frac{k^2-2k+1}{k^2-2k+2}} \geq \log n$, we obtain that

$$n^\alpha = n^{\frac{\lambda}{k^2-2k+2} + \frac{(k-1)\tau}{k^2-2k+2} + \frac{k^2-2k+1}{k^2-2k+2}} \leq n^{\frac{\lambda}{k-1}} n < \frac{n}{k-1}.$$
Then we obtain that
\[ n^{k-1} - n^{(k-1)\alpha} \leq \frac{k^2 - 2k}{k^2 - 2k + 1} n^{k-1}. \]
Then we have
\[ p_x \leq \frac{n^\tau}{n^{k-1} - n^{(k-1)\alpha}} \leq \frac{k^2 - 2k + 1}{k^2 - 2k} n^{k-1-\tau}. \]
Now let us define the independent random variables as follows.
\[ X'_{(i_1,\ldots,i_k)} = \begin{cases} 1 & \text{if } x_{(i_1,\ldots,i_k)} = 1 \\ 1 \text{ with probability } \left( \frac{(k^2 - 2k + 1 - \tau}{n^{k-1-\tau}} \right) & \text{if } x_{(i_1,\ldots,i_k)} = 0 \\ 0 & \text{otherwise} \end{cases} \]
Then we obtain that
\[ Pr \left( X'_{(i_1,\ldots,i_k)} = 1 \mid X_{(j_1,\ldots,j_k)} = x_{(j_1,\ldots,j_k)} \text{ for all } (j_1,\ldots,j_k) \neq (i_1,\ldots,i_k) \right) \]
\[ = \frac{k^2 - 2k + 1}{k^2 - 2k} \cdot \frac{1}{n^{k-1-\tau}}. \]
Then we have the expectation of the random variable
\[ X' = \sum_{i_1=1}^{n^\alpha} \cdots \sum_{i_{k-1}=1}^{n^\alpha} X'_{(i_1,\ldots,i_{k-1})}, \]
\[ \mathbb{E}(X') = \frac{k^2 - 2k + 1}{k^2 - 2k} \frac{n^{(k-1)\alpha} - 1}{n^{k-1-\tau}} = \frac{k^2 - 2k + 1}{k^2 - 2k} n^{(k-1)\alpha+\tau-k+1}. \]
From the equation
\[ n^\frac{\tau}{k^2 - 2k + 1} \cdot \frac{(k^2 - 2k + 1)}{k^2 - 2k + 2} \geq \log n, \]
we obtain that
\[ n^{(k-1)\alpha+\tau-k+1} = n^\frac{\tau}{k^2 - 2k + 1} \cdot \frac{(k^2 - 2k + 1)}{k^2 - 2k + 2} \geq \log n. \]
By applying a chernoff bound to the random variable \( X' \), we conclude that
\[ Pr(X > 2n^{(k-1)\alpha+\tau-k+1}) \leq Pr(X' > 2n^{(k-1)\alpha+\tau-k+1}) \leq 2^{-2(2n^{(k-1)\alpha+\tau-k+1})} \leq 2^{-2\log n} = \frac{1}{n^2}. \]

Using the equations (6.2) and (6.3), there exist \( A_{i_1,\ldots,i_k} \subset A_i \) of size \( n^\alpha \) for \( 1 \leq i \leq k-1 \), where \( l = 2n^{1-\alpha} \log n \), such that the following holds: (1) \( \bigcup_{i=1}^l A_i = A_i \) for \( 1 \leq i \leq k-1 \) (2) For every \( 1 \leq i_1,\ldots,i_k \leq l \), every vertex in \( A_k \) is contained in at most \( 2n^{(k-1)\alpha+\tau-k+1} \) members in \( E_{(i_1,\ldots,i_{k-1})} = \{ (a_{i_1,\ldots,i_{k-1},k} \mid a_{i_1,\ldots,i_{k-1}} \in A_{i_1,\ldots,i_{k-1}}, a_{k-1,i_{k-1}} \in A_{k-1,i_{k-1}}, a_{k,i_k} \in A_k \}. \)

Now we are ready to prove Theorem 6.1. Apply Lemma 5.2 with \( E_{(i_1,\ldots,i_{k-1})} \). Then we conclude that there exists a linear secret sharing scheme for a \( k \)-uniform access structure \( \Gamma \), which is
Then there exists a linear secret sharing scheme for a sparse set of hyperedges satisfying the following condition. Suppose that with \(|A| = 0\), we derive that the number of participants in the following total share size

\[
\sum_{i_1=1}^{l} \cdots \sum_{i_{k-1}=1}^{l} \left( |A_{k}| + (2n^{(k-1)\alpha + \tau - k + 1} + 1) \right)^{k-1} \left( |A_{1,i_1}| + \cdots |A_{k-1,i_{k-1}}| \right)
\]

\[= O \left( n^{(k-1)(1-\alpha)} \log^{k-1} n \left( n^\alpha + n^{(k-1)^2 + \alpha} \right) \right) \]

\[= O \left( \frac{k^2 - 2k + \beta}{n^{k-1}} |A_k|^{k^2 - 3k + 3d(k-1)^2} \log^{k-1} n \right).
\]

This completes the proof of Lemma 6.1.

Using Lemma 6.1, we give the following efficient linear secret sharing scheme for sparse \(k\)-uniform access structure when the size of all \(k\) parts is same.

**Lemma 6.2.** Let \(G(V, E)\) be a \(k\)-partite \(k\)-uniform hypergraph, where \(V\) is a set of vertices and \(E\) is a set of hyperedges satisfying the following condition. Suppose that \(V\) is partitioned into \(A_1 \cup \cdots \cup A_k\) with \(|A_i| = m_i\). Let \(E\) be the family of subsets with exactly one vertex in common with each \(A_i\) as follows.

\[E = \{ (a_{1,i_1}, \ldots, a_{k,i_k}) \mid a_{1,i_1} \in A_1, \ldots, a_{k,i_k} \in A_k \}.\]

Suppose that \(m_1 = \cdots = m_k = n\) and there are at most \(n^{1+\beta}\) subsets for some \(0 \leq \beta < 1\) in \(E\). Then there exists a linear secret sharing scheme for a sparse \(k\)-uniform access structure \(\Gamma\), which is determined by \(G(V, E)\), with total share size

\[O(\frac{n^{2-2k+\beta}}{2^{s+1}} + (\frac{n^{2-2k+\beta}}{2^{s+1}})^\beta \log^{k} n).\]

**Proof.** Let us consider a partition of the participants in \(A_k\) into \(\log n\) sets according to the number of sets in \(E\) containing each participant. Let us define the \(s\)-th set \(A_k^{(s)}\) as

\[A_k^{(s)} = \{ v \in P \mid \frac{n}{2^{s+1}} \leq \text{number of members in } E \text{ containing a participant } v \leq \frac{n}{2^s} \}\]

for \(s = 0, 1, \ldots, \log n - 1\). Since there are at most \(n^{1+\beta}\) subsets for some \(0 \leq \beta < 1\) in \(Q\) and the number of members in \(E\) containing every participant in the \(s\)-th set \(A_k^{(s)}\) is at least \(\frac{n}{2^{s+1}}\), we derive that the number of participants in the \(s\)-th set \(A_k^{(s)}\) is at most \(\frac{n^{1+\beta}}{2^{s+1}} = 2^{s+1}n^\beta\) for \(s = 0, 1, \ldots, \log n - 1\).

If we apply Lemma 6.1 with

\[Q_s = \{(a_{1,i_1}, \ldots, a_{k-1,i_{k-1}}, a_{k,i_k}) \mid a_{1,i_1} \in A_1, \ldots, a_{k-1,i_{k-1}} \in A_{k-1}, a_{k,i_k} \in A_k^{(s)}\},\]

where \(|A_1| = \cdots = |A_{k-1}| = n\) and \(|A_k^{(s)}| \leq 2^{s+1}n^\beta\), then we conclude that there exists a linear secret sharing scheme for a \(k\)-uniform access structure \(\Gamma\), which is determined by \(G(V, E)\), with the following total share size

\[O(\frac{n^{2-2k+\beta}}{2^{s+1}} + (\frac{n^{2-2k+\beta}}{2^{s+1}})^\beta \log^{k} n).\]

18
\[
O \left( k^{2-2k+2} \sqrt{n^{-k+1} |A_k(s)| k^{2-3k+3} d(k) \log^{k-1} n} \right) \times \log n
\]
\[
= O \left( k^{2-2k+2} \sqrt{n^{-k+1} 2^{k+1} n^{\beta} k^{2-3k+3} \frac{n}{2^{k+1}} \log^{(k-1)} n} \right) \times \log n
\]
\[
= O \left( k^{2-2k+2} \sqrt{n k^{2-3k+3} 2^{\beta(k-3k+3)} \log k} \right).
\]
This completes the proof of Lemma 6.2.

To prove Theorem 1.1, now we utilize the technique of hypergraph decomposition described in Section 4. Using Lemma 4.2, we obtain that every \( k \)-uniform hypergraph can be decomposed into the set of sub-hypergraphs consisting of \( O(\log n) \) \( k \)-partite \( k \)-uniform hypergraphs. It means that \( k \)-uniform hypergraph is covered by \( k \)-partite \( k \)-uniform hypergraphs of size \( O(\log n) \). Let us consider the collection of the sets of participants into \( k \) parts \( A_1^t, \cdots, A_k^t \) for every \( 1 \leq t \leq O(\log n) \). For every \( 1 \leq t \leq O(\log n) \), let us define the family \( E_t \) of subsets with exactly one vertex in common with each \( A_i^t \) as
\[
E_t = \{ (a_{1,i_1}, \cdots, a_{k,i_k}) \mid a_{1,i_1} \in A_1^t, \cdots, a_{k,i_k} \in A_k^t \},
\]
where \( |A_1^t| = \cdots = |A_k^t| \).

Applying Lemma 6.2 with \( E_t \), we conclude that there exists a linear secret sharing scheme for a \( k \)-uniform access structure \( \Gamma \), which is determined by \( E = \bigcup_{t=1}^{O(\log n)} E_t \), with the following total share size
\[
O \left( k^{2-2k+2} \sqrt{n k^{2-3k+3} 2^{\beta(k-3k+3)} \log^{k+1} n} \right).
\]
This completes the proof of Theorem 1.1.

### 7 Proof of Theorem 1.2

In this section, we prove Theorem 1.2 by providing efficient constructions on the share size of linear secret sharing schemes for dense \( k \)-uniform access structures for a constant \( k \). To prove Theorem 1.2, we utilize the technique of hypergraph decomposition in which secret sharing schemes for \( k \)-uniform hypergraphs are obtained as a union of the secret sharing schemes for all \( k \)-partite \( k \)-uniform sub-hypergraphs. We need the following lemma for constructing more efficient linear secret sharing schemes for dense \( k \)-partite \( k \)-uniform hypergraphs when the size of all \( k \) parts is the same.

**Lemma 7.1.** Let \( H(V,E) \) be a \( k \)-partite \( k \)-uniform hypergraph, where \( V \) is a set of vertices and \( E \) is a set of hyperedges satisfying the following condition. Suppose that \( V \) is partitioned into \( A_1 \cup \cdots \cup A_k \) with \( |A_i| = m_i \). Let \( E \) be the family of subsets with exactly one vertex in common with each \( A_i \) as follows.
\[
E = \{ (a_{1,i_1}, \cdots, a_{k,i_k}) \mid a_{1,i_1} \in A_1, \cdots, a_{k,i_k} \in A_k \}.
\]
Suppose that \( m_1 = \cdots = m_{k-1} = n \), \( m_k \leq n \), and every vertex in \( A_k \) is contained in at least \( n - d \) members in \( E \) for some \( d \leq n \). If \( d|A_k|^{k-1} \geq n^{k-1} \log^{k-2k+2} n \), then there exists a linear secret sharing scheme for a \( k \)-uniform access structure \( \Gamma \), which is determined by \( H(V, E) \), with total share size

\[
O\left( \sqrt{n^{k-1}}|A_k|^{k-3k+3}d(k-1)^2 \log^{k-1} n \right).
\]

Proof. Let \( U \) be the family of all subsets with exactly one vertex in common with each part \( A_i \), where \( 1 \leq i \leq k \). First, let us consider the complement of a family \( E \), which is denoted by \( \overline{E} \), consisting of all subsets in the given universal family \( U \) that are not in \( E \). Since every participant in \( A_k \) is contained in at least \( n - d \) members in \( E \), every participant in \( A_k \) must be contained in at most \( d \) members in the complement \( \overline{E} \). Now we apply Lemma 6.1.

Let \( d = n^\tau \) and \( |A_k| = n^\lambda \leq n \), where \( \tau = \log n d \) and \( \lambda = \log n |A_k| \). From the condition \( d|A_k|^{k-1} \geq n^{k-1} \log^{k-2k+2} n \), we obtain

\[
n^k \tau - 2k+2 \geq \frac{\lambda(k-1)}{k^2-2k+2} \geq \log n. \tag{7.1}
\]

Let \( \alpha = \frac{\lambda}{k^2-2k+2} - \frac{(k-1)\tau}{k^2-2k+2} + \frac{k_2-2k+2}{k^2-2k+2} \). In the same way of the proof of Lemma 6.1 there exist \( A_{i,1}, \cdots, A_{i,l} \subset A_i \) of size \( n^\alpha \) for \( 1 \leq i \leq k-1 \), where \( l = 2n^{1-\alpha} \ln n \), such that the following holds: (1) \( \bigcup_{j=1}^{l} A_{i,j} = A_i \) for \( 1 \leq i \leq k-1 \) (2) For every \( 1 \leq i_1, \cdots, i_k \leq l \), every participant in \( A_k \) is contained in at most \( 2n^{(k-1)\alpha+\tau-k+1} \) members in \( \overline{E}_{i_1,\cdots,i_{k-1}} \subset \overline{E} \), where \( \overline{E}_{i_1,\cdots,i_{k-1}} = \{(a_1,i_1, \cdots, a_{k-1}, i_{k-1}, a_{k,i_k}) | a_1,i_1, \cdots, a_{k-1}, i_{k-1} \in A_{k-1}, i_{k-1} \in A_{k} \} \).

Let us consider the complement of the family \( \overline{E}_{i_1,\cdots,i_{k-1}} \), which is denoted by \( E_{i_1,\cdots,i_{k-1}} \), consisting of all subsets in the universal family that are not in \( \overline{E}_{i_1,\cdots,i_{k-1}} \). Since every participant in \( A_k \) is contained in at least \( n^\alpha - 2n^{(k-1)\alpha+\tau-k+1} \) members in \( E_{i_1,\cdots,i_{k-1}} \subset E \), every participant in \( A_k \) is contained in at least \( n^\alpha - 2n^{(k-1)\alpha+\tau-k+1} \) members in \( E_{i_1,\cdots,i_{k-1}} \subset E \).

Apply Lemma 5.3 with \( E_{i_1,\cdots,i_{k-1}} \). Then we conclude that there exists a linear secret sharing scheme for a \( k \)-uniform access structure \( \Gamma \), which is determined by \( E \), with the following total share size

\[
\sum_{i_1=1}^{l} \sum_{i_2=1}^{l} \cdots \sum_{i_{k-1}=1}^{l} \left( 2|A_k|^{k-1} \left( 2n^{(k-1)\alpha+\tau-k+1} + 1 \right)^{k-1} \right).
\]

This completes the proof of Lemma 7.1.

Using Lemma 7.1, we give the following efficient linear secret sharing scheme for dense \( k \)-uniform access structure when the size of all \( k \) parts is same.
Lemma 7.2. Let $G(V, E)$ be a $k$-partite $k$-uniform hypergraph, where $V$ is a set of vertices and $E$ is a set of hyperedges satisfying the following condition. Suppose that $V$ is partitioned into $A_1 \cup \cdots \cup A_k$ with $|A_i| = m_i$. Let $E$ be the family of subsets with exactly one vertex in common with each $A_i$ as follows.

$$E = \{ (a_{1,i_1}, \cdots, a_{k,i_k}) \mid a_{1,i_1} \in A_1, \cdots, a_{k,i_k} \in A_k \}.$$ 

Suppose that $m_1 = \cdots = m_k = n$ and there are at least $\binom{n}{k} - n^{1+\beta}$ subsets for some $0 \leq \beta < 1$ in $E$. Then there exists a linear secret sharing scheme for a $k$-uniform access structure $\Gamma$, which is determined by $G(V, E)$, with total share size

$$O\left(\left(\frac{k^2-3k+2}{k^2-2k+2}\right)^{\beta} \log k \cdot n\right).$$

Proof. Let $U$ be the family of all subsets with exactly one vertex in common with each part $A_i$, where $1 \leq i \leq k$. First, let us consider the complement of a family $E$, which is denoted by $\overline{E}$, consisting of all the subsets in the given universal family $U$ that are not in $E$. Since there are at least $\binom{n}{k} - n^{1+\beta}$ subsets for some $0 \leq \beta < 1$ in $E$, there are at most $n^{1+\beta}$ subsets for some $0 \leq \beta < 1$ in the complement $\overline{E}$. Now we apply Lemma 6.2.

In the same way of the proof of Lemma 6.2, let us consider a partition of the vertices in $A_k$ into $\log n$ sets according to the number of sets in $\overline{E}$ containing each vertex. Let us define the $s$-th set $A_{k}^{(s)}$ as

$$A_{k}^{(s)} = \{ v \in \mathcal{P} \mid \frac{n}{2^{s+1}} \leq \text{number of members in } \overline{E} \text{ containing a vertex } v \leq \frac{n}{2^s} \}$$

for $s = 0, 1, \cdots, \log n - 1$. Since there are at most $n^{1+\beta}$ subsets for some $0 \leq \beta < 1$ in $\overline{E}$ and the number of members in $\overline{E}$ containing every vertex in the $s$-th set $A_{k}^{(s)}$ is at least $\frac{n}{2^{s+1}}$, we derive that the number of vertices in the $s$-th set $A_{k}^{(s)}$ is at most $\frac{n^{1+\beta}}{2^{s+1}} = 2^{s+1}n^\beta$ for $s = 0, 1, \cdots, \log n - 1$.

For $s = 0, 1, \cdots, \log n - 1$, let us define the family $\overline{E}_s \subseteq \overline{E}$ of subsets with exactly one vertex in common with $A_1, \cdots, A_{k-1}, A_{k}^{(s)}$ as

$$\overline{Q}_s = \{(a_{1,i_1}, \cdots, a_{r-1,i_{r-1}}, a_{r,i_r}) \mid a_{1,i_1} \in A_1, \cdots, a_{r-1,i_{r-1}} \in A_{r-1}, a_{r,i_r} \in A_{k-1}, a_{k,i_k} \in A_{k}^{(s)} \} \subseteq \overline{E},$$

where $|A_1| = \cdots = |A_{k-1}| = n$ and $|A_{k}^{(s)}| \leq 2^{s+1}n^\beta$. Let us consider the complement of the family $\overline{E}_s$, which is denoted by $E_s$, consisting of all subsets in the universal family that are not in $\overline{E}_s$.

Since every participant in $A_k$ is contained in at most $\frac{n}{2^s}$ in $\overline{E}_s$, every participant in $A_k$ is contained in at least $n - \frac{n}{2^s}$ in $E_s$. If we apply Lemma 7.1 with $E_s$, then we conclude that there exists a linear secret sharing scheme for a $k$-uniform access structure $\Gamma$, which is determined by $E$, with the following total share size.
This completes the proof of Lemma 7.2.

To prove Theorem 1.2, now we utilize the technique of hypergraph decomposition described in Section 4. Using Lemma 4.2, a $k$-uniform hypergraph is covered by $k$-partite $k$-uniform hypergraphs of size $O(\log n)$. Let us consider the collection of the sets of participants into $k$ parts $A_{t1}^{1}, \ldots, A_{tk}^{k}$ for every $1 \leq t \leq O(\log n)$. For every $1 \leq t \leq O(\log n)$, let us define the family $E_t \subseteq E$ of subsets with exactly one vertex in common with each $A_{ti}^i$ as

$$E_t = \{(a_{1,i_1}, \ldots, a_{k,i_k}) \mid a_{1,i_1} \in A_{t1}^{1}, \ldots, a_{k,i_k} \in A_{tk}^{k}\},$$

where $|A_{t1}^{1}| = \cdots = |A_{tk}^{k}|$.

Applying Lemma 7.2 with $E_t$, we conclude that there exists a linear secret sharing scheme for a $k$-uniform access structure $\Gamma$, which is determined by $E = \bigcup_{t=1}^{O(\log n)} E_t$, with the following total share size

$$O \left( k^{2-2k+2} \sqrt{n^{-k+1} |A_k(s)| k^2-3k+3 d(k-1)^2 \log^{k-1} n} \right) \times \log n$$

This completes the proof of Theorem 1.2.

8 Conclusion

In this paper, we investigated efficient constructions on the total share size of linear secret sharing schemes for sparse and dense $k$-uniform access structures (or forbidden $k$-homogeneous access structures) for a constant $k$ using the hypergraph decomposition technique and the monotone span programs.

An access structure is ideal if there exists an ideal secret sharing scheme realizing it. The characterization of the ideal access structures is one of the important problems in the secret sharing scheme. The characterization problems of ideal access structures have been studied by many authors [25, 30, 31, 34, 43, 46]. An open problem is the search for new techniques to characterize the ideal $k$-homogeneous access structures.
References

[1] B. Applebaum and B. Arkis, *On the power of amortization in secret sharing: d-uniform secret sharing and CDS with constant information rate*, in: TCC 2018, LNCS, vol. 11239 (2018) 317-344.

[2] B. Applebaum, A. Beimel, O. Farrás, O. Nir, and N. Peter, *Secret-sharing schemes for general and uniform access structures*, in: EUROCRYPT 2019, LNCS, vol. 11478 (2019) 441-471.

[3] B. Applebaum, A. Beimel, O. Nir, and N. Peter, *Better secret sharing via robust conditional disclosure of secrets*, in: 52nd STOC, ACM, (2020) 280-293.

[4] A. Beimel and O. Farrás, *The share size of Secret-Sharing Schemes for almost all access structures and graphs*, Cryptology ePrint Archive (2020) https://eprint.iacr.org/2020/664

[5] A. Beimel, O. Farrás, and Y. Mintz, *Secret Sharing Schemes for very dense graphs*, Journal of Cryptology, 29(2) (2016) 336-362.

[6] A. Beimel, O. Farrás, Y. Mintz, and N. Peter, *Linear Secret-Sharing Schemes for forbidden graph access structures*, Cryptology ePrint Archive (2020) https://eprint.iacr.org/2017/940

[7] A. Beimel, O. Farrás, and N. Peter, *Secret sharing schemes for dense forbidden graphs*, in: SCN 2016, LNCS, vol. 9841 (2016) 509-528.

[8] A. Beimel, A. Gál, and M. Paterson, *Lower bounds for monotone span programs*, Computational Complexity, 6(1) (1997) 29-45.

[9] A. Beimel, Y. Ishai, R. Kumaresan, and E. Kushilevitz, *On the cryptographic complexity of the worst functions*, in: TCC 2014, LNCS, vol. 8349 (2014) 317-342.

[10] A. Beimel, E. Kushilevitz, and P. Nissim, *The complexity of multiparty PSM protocols and related models*, in: EUROCRYPT 2018, LNCS, vol. 10821 (2018) 287-318.

[11] A. Beimel and N. Peter, *Optimal linear multiparty conditional disclosure of secrets protocols*, in: ASIACRYPT 2018, LNCS, vol.11274 (2018) 332-362.

[12] J. Benaloh and J. Leichter, *Generalized Secret Sharing and monotone functions*, in: CRYPTO’88, LNCS, vol. 403 (1988) 27-35.

[13] M. Bertilsson and I. Ingemarsson, *A construction of practical secret sharing schemes using linear block codes*, in: AUSCRYPT 1992, LNCS, vol. 718 (1992) 67-79.

[14] C. Blundo, A.D. Santis, A.G. Gaggia, and U. Vaccaro, *New bounds on the information rate of secret sharing schemes*, IEEE Trans. on Information Theory, 41(2) (1995) 549-553.

[15] C. Blundo, A.D. Santis, R. D. Simone, and U. Vaccaro, *Tight bounds on the information rate of secret sharing schemes*, Designs Codes and Cryptography, 11(2) (1997) 107-122.

[16] C. Blundo, A.D. Santis, D.R. Stinson, and U. Vaccaro, *Graph decomposition and secret sharing schemes*, Journal of Cryptology, 8(1) (1995) 39-64.
[17] E.F. Brickell and D.M. Davenport, *On the classification of ideal secret sharing schemes*, Journal of Cryptology, **4**(73) (1991) 123-134.

[18] E.F. Brickell and D.R. Stinson, *Some improved bounds on the information rate of perfect secret sharing schemes*, Journal of Cryptology, **5**(3) (1992) 153-166.

[19] R.M. Capocelli, A.D. Santis, L. Gargano, and U. Vaccaro, *On the size of shares for secret sharing schemes*, Journal of Cryptology, **6**(3) (1993) 157-168.

[20] L. Csirmaz, *The size of a share must be large*, Journal of Cryptology, **10**(4) (1997) 223-231.

[21] L. Csirmaz, *Secret sharing schemes on graphs*, Cryptology ePrint Archive (2005) https://eprint.iacr.org/2005/059

[22] L. Csirmaz, *Secret sharing schemes on the d-dimensional cube*, Designs Codes and Cryptography, **74**(3) (2015) 719-729.

[23] L. Csirmaz, *An impossibility result on graph secret sharing*, Designs Codes and Cryptography, **53**(3) (2009) 195-209.

[24] L. Csirmaz and P. Ligeti, *Secret sharing on large girth graphs*, Cryptogr.Commun., **11**(3) (2019) 399-410.

[25] L. Csirmaz and G. Tardos, *Optimal information rate of secret sharing schemes on trees*, IEEE Trans. on Information Theory, **59**(4) (2013) 2527-2530.

[26] G.D. Crescenzo and C. Galdi, *Hypergraph decomposition and secret sharing*, Discrete Applied Mathematics, **157** (2009) 928-946.

[27] M.V. Dijk, *On the information rate of perfect secret sharing schemes*, Designs Codes and Cryptography, **6** (1995) 143-169.

[28] P. Erdős and L. Pyber, *Covering a graph by complete bipartite graphs*, Discrete Mathematics, **170**(1-3) (1997) 249-251.

[29] O. Farras, T. Kaced, S. Martín, and C. Padró, *Improving the linear programming technique in the search for lower bounds in secret sharing*, in: EUROCRYPT 2018, LNCS (2018) 597-621.

[30] J.M. Farré and C. Padró, *Secret sharing schemes with three or four minimal qualified subsets*, Designs Codes and Cryptography, **34** (2005) 17-34.

[31] J.M. Farré and C. Padró, *Ideal secret sharing scheme whose minimal qualified subsets have at most three participants*, Designs Codes and Cryptography, **52** (2009) 1-14.

[32] R. Gay, I. Kerenidis, and H. Wee, *Communication complexity of conditional disclosure of secrets and attribute-based encryption*, in: CRYPTO 2015, LNCS, vol. **9216** (2015) 485-502.

[33] M. Ito, A. Saito, and T. Nishizeki, *Secret sharing schemes realizing general access structure*, in: Globecom 87, LNCS (1987) 99-102. Journal version: *Multiple assignment scheme for sharing secret*, Journal of Cryptology, **6**(1) (1993) 15-20.
[34] S. Janbaz, A. Zaghian, and B. Bagherpour, *Ideal secret sharing schemes on graph-based 3-homogeneous access structures*, Transactions on Combinatorics, **10**(2) (2021) 107-120.

[35] M. Karchmer and A. Wigderson, *On span programs*, In 8th Structures in Complexity Theory (1993) 102-111.

[36] T. Liu, V. Vaikuntanathan, and H. Wee, *Conditional disclosure of secrets via non-linear reconstruction*, in: CRYPTO 2017, LNCS vol. **10401** (2017) 758-790.

[37] J. Martí-Farré and C. Padró, *Secret sharing schemes on sparse homogeneous access structures with rank three*, The Electronic Journal of Combinatorics, **11** (2004) #R72.

[38] J. Martí-Farré and C. Padró, *Secret sharing schemes on access structures with intersection number equal to one*, Discrete Applied Mathematics, **154** (2006) 552-563.

[39] J. Martí-Farré, *A note on secret sharing schemes with three homogeneous access structures*, Information Processing Letters, **102** (2007) 133-137.

[40] Y. Mintz, *Information ratios of graph secret-sharing schemes*, Master’s thesis, Dept. of Computer Science, Ben Gurion University (2012).

[41] N. Peter, *Secret-Sharing Schemes and Conditional Disclosure of Secret Protocols*, PhD thesis, Ben-Gurion University of the Negev (2020).

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

[43] D.R. Stinson, *An explanation of secret sharing schemes*, Designs Codes and Cryptography, (1992) 157-390.

[44] D.R. Stinson, *Decomposition construction for secret sharing schemes*, IEEE Trans. on Information Theory, **40**(1) (1994) 118-125.

[45] H.M. Sun and S.P. Shieh, *Secret sharing in graph-based prohibited structures*, in: INFOCOM’97, (1997) 718-724.

[46] T. Tassa and N. Dyn, *Multipartite secret sharing by bivariate interpolation*, Journal of Cryptology, **22** (2009) 227-258.