J Cryptol (2016) 29:336–362
DOI: 10.1007/s00145-014-9195-8

Journal of CRYPTOLOGY

Secret-Sharing Schemes for Very Dense Graphs*

Amos Beimel · Yuval Mintz
Ben Gurion University of the Negev, Be'er Sheva, Israel
email: amos.beimel@gmail.com; yuvalmin@cs.bgu.ac.il

Oriol Farràs†
Universitat Rovira i Virgili, Tarragona, Spain
email: oriol.farras@urv.cat

Communicated by Ronald Cramer.

Received 26 June 2013
Online publication 24 December 2014

Abstract. A secret-sharing scheme realizes a graph if every two vertices connected by an edge can reconstruct the secret while every independent set in the graph does not get any information on the secret. Similar to secret-sharing schemes for general access structures, there are gaps between the known lower bounds and upper bounds on the share size for graphs. Motivated by the question of what makes a graph "hard" for secret-sharing schemes (that is, they require large shares), we study very dense graphs, that is, graphs whose complement contains few edges. We show that if a graph with n vertices contains $\binom{n}{2} - n^{1+\beta}$ edges for some constant $0 \le \beta < 1$, then there is a scheme realizing the graph with total share size of $\tilde{O}(n^{5/4+3\beta/4})$. This should be compared to $O(n^2/\log(n))$, the best upper bound known for the total share size in general graphs. Thus, if a graph is "hard," then the graph and its complement should have many edges. We generalize these results to nearly complete k-homogeneous access structures for a constant k. To complement our results, we prove lower bounds on the total share size for secret-sharing schemes realizing very dense graphs, e.g., for linear secret-sharing schemes, we prove a lower bound of $\Omega(n^{1+\beta/2})$ for a graph with $\binom{n}{2} - n^{1+\beta}$ edges.

Keywords. Secret-sharing, Share size, Graph access structures, Complete bipartite covers, Equivalence covers.

* This work was supported by ISF Grant 938/09. A preliminary version of this paper appeared in *Advances in Cryptology CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 144–161. Springer-Verlag, 2012.

† Partly supported by the Spanish Government through projects TIN201127076-C03-01, 2010 CSD2007-00004, and by the Catalan Government through Grant 2009 SGR 1135. Part of his work was done while at Ben Gurion University.

© International Association for Cryptologic Research 2014

1. Introduction

A secret-sharing scheme, introduced by [10,35,50], is a method by which a dealer, which holds a secret string, can distribute strings, called shares, to a set of participants, enabling only predefined subsets of participants to reconstruct the secret from their shares. The collection of predefined subsets authorized to reconstruct the secret is called the access structure. We consider perfect schemes, in which any unauthorized set of participants should learn nothing about the secret from their combined shares (even if they have unlimited power). Secret-sharing schemes are useful cryptographic building blocks, used in many secure protocols, e.g., multiparty computation [8,19,21], threshold cryptography [28], access control [46], attribute-based encryption [34,58], and oblivious transfer [51,57].

For a scheme to be efficient and be useful for the above-mentioned applications, the size of the shares should be small (i.e., polynomial in the number of participants). On the one hand, there are access structures that have efficient schemes, e.g., the threshold access structure, in which the authorized sets are all sets containing at least ℓ participants (for some threshold ℓ) [10,50]. On the other hand, the best known schemes for general access structures, e.g., [9,15,35,38,52], are highly inefficient, that is, for most access structures, the size of shares is $2^{O(n)}$, where n is the number of parties in the access structure. The best lower bound known on the total share size for an explicit or implicit access structure is $\Omega(n^2/\log(n))$ [23]. Thus, there exists a large gap between the known upper and lower bounds. Bridging this gap is one of the most important questions in the study of secret-sharing schemes. We lack sufficient methods for proving lower bounds on the share size. Furthermore, we lack the sufficient understanding of which access structures are "hard," that is, which access structures require large shares (if any). In contrast to general secret-sharing schemes, super-polynomial lower bounds are known for *linear* secret-sharing schemes, that is, for schemes where the shares are generated using a linear transformation—there exists an explicit access structure such that the total share size of any linear secret-sharing scheme realizing it is $n^{\Omega(\log(n))}$ [3,32,33]. Linear secret-sharing schemes are important as most known secret-sharing schemes are linear, and many cryptographic applications require that the scheme is linear. For more background on secret sharing, see [4].

In this paper, we consider a special family of access structures, in which all minimal authorized sets are of size 2. These access structures can be described by a graph, where each participant is represented by a vertex and each minimal authorized set is represented by an edge. Graph access structures are useful and interesting and have been studied in, e.g., [12,14,16,24,25,27,29,42,54,56]. Some of the results that were discovered for graph access structures, using graph theory, were later extended to all access structures.

Example 1.1. Blundo et al. [14] proved that the best share size of a scheme for a graph access structures is either the size of the secret or at least 1.5 times larger than that size. This was generalized later to many other families of access structures. Martí-Farré and Padró [43] proved that the share size of every access structure that is not *matroidal* is at least 1.5 times larger than the size of the secret.

Other results on graph access structures have been extended to homogeneous access structures [41,48,53], which are access structures whose minimal authorized subsets are of the same size, and to other access structures described by simple hypergraphs [22, 55].

Every graph access structure can be realized by a secret-sharing scheme in which the total share size is $O(n^2/\log(n))$ [13,17,30]; this scheme is linear. The best lower bound for the total share size required to realize a graph access structure by a general secret-sharing scheme is $\Omega(n \log(n))$ [12,24,29]. The best lower bound for the total share size required to realize a graph access structure by a linear secret-sharing scheme is $\Omega(n^{3/2})$ [6]. Although the gap between the lower and upper bounds for these access structures is smaller than that of general access structures, studying this gap might reveal new insight that could be applied to the share size of general access structures.

There are three main techniques for proving lower bounds on the size of shares in linear secret-sharing schemes, namely the self-avoiding criterion [6], Gál's criterion [32], and Gál and Pudlák's criterion [33]. Mintz [44] studied the limitations of these techniques for proving lower bounds for linear secret-sharing schemes realizing graphs. He proved that the criteria of [6] and [33] cannot prove lower bounds better than $\Omega(n^{3/2})$, and Gál's criterion [32] cannot improve upon this lower bound under some restriction (namely using rank 1 matrices). All applications of Gál's criterion are under this restriction. The conclusion from Mintz's results is that proving a lower bound of $\omega(n^{3/2})$ on the size of shares in linear schemes realizing graph access structures requires some new ideas.

1.1. *Our Results*

In this work, we study a natural family of graphs—the very dense graphs. These are graphs that have $\binom{n}{2} - \ell$ edges for $\ell \ll n^2$ (where n is the number of vertices in the graph). The motivation for this work is trying to understand which graphs are "hard," that is, which graphs require total share size of $\Omega(n^2/\operatorname{polylog} n)$ (if any). For example, if a graph contains ℓ edges, then it can be realized by a trivial secret-sharing scheme in which the total share size is 2ℓ times the size of the secret [35]. Thus, if there exists a "hard" graph, then it has to have $\Omega(n^2/\operatorname{polylog} n)$ edges. We are interested in the question if these "hard" graphs can be very dense. Our results show that this is not possible.

Our main result is that if a graph has $\binom{n}{2} - n^{1+\beta}$ edges for some $0 \leq \beta < 1$, then it can be realized by a secret-sharing scheme in which the total share size is $\tilde{O}(n^{5/4+3\beta/4})$;[1] this scheme is linear. In particular, if β is a constant smaller than 1, the total share size is $\ll n^2$, that is, these are not "hard" graphs as discussed above. Similarly, if $\beta < 1/3$, then the total share size is $o(n^{3/2})$; thus, these graphs are easier than the graphs for which [6] proved their lower bounds for linear secret-sharing schemes. Our results can be translated to upper bounds on the size of monotone formula realizing graphs (that is, Boolean functions whose minterms have size 2): If a graph has $\binom{n}{2} - n^{1+\beta}$ edges for some $0 \leq \beta < 1$, then it can be realized by a monotone formula of size $\tilde{O}(n^{5/4+3\beta/4})$. As a corollary of our main result, we prove that if a graph has $\binom{n}{2} - \ell$ edges, where $\ell < n/2$, then it can be realized by a scheme in which the total share size is $n + \tilde{O}(\ell^{5/4})$.

[1] We use the $\tilde{O}$ notation, which ignores polylogarithmic factors.

Thus, if $\ell \ll n^{4/5}$, then the total share size is $n+o(n)$, which is optimal up to an additive factor of $o(n)$.

We extend the techniques used in these results to the study of two additional problems. First, we consider the following scenario: We start with a graph and remove few edges from it. The question is how much the share size of a secret-sharing scheme realizing the graph can grow as a result of the removed edges. If we add edges, then trivially the share size grows at most linearly in the number of added edges. We show that also when removing edges, the share size does not increase too much. We study this problem also for general access structures, considering the removal of minimal authorized subsets for any access structure. We show that for certain access structures, the share size does not increase too much either. Second, we study the removal of minimal authorized subsets from k-out-of-n threshold access structures and present a construction in which the size of each share is reasonably small for $k \ll n$.

To complement our results, we prove lower bounds on the total share size of secret-sharing schemes realizing very dense graphs. For graph access structures, the known lower bounds for general secret-sharing schemes [12,24,29] and linear secret-sharing schemes [6] use sparse graphs with $\theta(n \log(n))$ edges and $\theta(n^{3/2})$ edges, respectively. Using the above lower bounds, we prove lower bounds of $\Omega(\beta n \log(n))$ and $\Omega(n^{1+\beta/2})$ for general and linear secret-sharing schemes, respectively, for some graphs with $\binom{n}{2} - n^{1+\beta}$ edges. In addition, we prove lower bounds of $n + \ell$ for graphs with $\binom{n}{2} - \ell$ edges, where $\ell < n/2$. Our lower bounds are not tight; however, they prove, as can be expected, that for linear secret-sharing schemes the total share size grows as a function of the number of excluded edges. The lower bounds for linear schemes are interesting as most known secret-sharing schemes, including the schemes constructed in this paper, are linear.

1.2. *Techniques*

Brickell and Davenport [16] proved that a connected graph has an ideal scheme (that is, a scheme in which the total share size is n times the size of the secret) if and only if the graph is a complete multipartite graph.[2] To construct a scheme realizing a very dense graph, we cover the graph by complete multipartite graphs (in particular, complete bipartite graphs), that is, we construct a sequence of multipartite graphs $G_1, G_2, \ldots, G_r$ such that each graph G_i is a subgraph of G and each edge of G is an edge in at least one graph G_i. We next, for every i, share the secret independently using an ideal secret-sharing scheme realizing G_i. The total share size in the resulting scheme is the sum of the number of vertices in the graphs $G_1, G_2, \ldots, G_r$. This idea of covering a graph was used in previous schemes, e.g., [13,14]. The contribution of this paper is how to find a "good" cover for every dense graph.

Our starting point is constructing a scheme for graphs in which every vertex is adjacent to nearly all other vertices, that is, graphs where the degree of every vertex in the complement graph is bounded by some $d \ll n$. We cover such graphs by complete

[2] A graph is a complete multipartite if its vertices can be partitioned into disjoint sets, called parts, such that there is an edge between two vertices iff they are from different parts. For additional graph terminology used in the rest of this section, see Sect. 2.2.

bipartite graphs. The size of the shares of the resulting scheme is $O(d \log(n))$. We show a similar result covering such graphs by equivalence graphs, that is, graphs which are union of disjoint cliques. Alon [1] proved, using a probabilistic proof, that every such graph can be covered by $O(d^2 \log(n))$ equivalence graphs. We improve on this result and prove, using a different probabilistic proof, that every such graph can be covered by $O(d \log(n))$ equivalence graphs.

We use the above scheme to realize very dense graphs. We first cover all vertices whose degree in the complement graph is "big." There are not too many such vertices in the complement graph, and the share size in realizing each star (namely a vertex and the edges incident with it) is at most n. Once we removed all edges incident with vertices whose degree is "big," we use covers of bipartite graphs of [37] to cover the remaining edges.

Our results can be translated to upper bounds on the size of monotone formula realizing graphs (that is, Boolean functions whose minterms have size 2). In our construction, we cover graphs by complete bipartite graphs and realize each graph by an ideal secret-sharing scheme. Clearly, each complete bipartite graph can be realized by a monotone formula whose size is the number of vertices in the graphs; this is the total share size of realizing the bipartite graph by a secret-sharing scheme. Therefore, our results remain valid also for monotone formulas, that is, if a graph has $\binom{n}{2} - n^{1+\beta}$ edges for some $0 \leq \beta < 1$, then it can be realized by a monotone formula of size $\tilde{O}(n^{5/4+3\beta/4})$.

Additional Related and Followup Works. Sun and Shieh [55] consider access structures that are defined by a *forbidden graph*, where each party is represented by a vertex, and 2 parties are an unauthorized set iff their vertices are connected by an edge. They give a construction with information ratio of $n/2$. In [55], every set of size 3 can reconstruct the secret. Our problem is much harder as every independent set in the graph is unauthorized. Recently, Beimel et al. [7] showed that forbidden graph access structures (where every set of size 3 is in the access structure) can be realized by a secret-sharing scheme in which the size of the share is $\tilde{O}(n^{3/2})$.

In another recent work, Csirmaz et al. [26] studied covers of graphs and hypergraphs by bipartite graphs. We mention two of their results that are most relevant to our paper. They gave a new, constructive proof with a small explicit constant to the Erdös-Pyber theorem [30], which says that the edges of a graph on n vertices can be partitioned into complete bipartite subgraphs so that every vertex is covered at most $O(n/\log(n))$ times. This theorem is used to show that each graph access structure can be realized by a secret-sharing scheme in which the size of the share of each party is $O(n/\log(n))$. In the case that the degree of every vertex in the complement graph is at most d, they proved the existence of a fractional covering of the edges by complete bipartite graphs such that every vertex is covered at most $O(d/\log(d))$ times (using the terminology of Definition 2.5 this is a λ-cover with r bipartite graphs such that $\lambda/r = O(d/\log(d))$). Alas, in their construction, the size of the cover λ is exponential in n, which results in a secret-sharing scheme with secrets of length exponential in n. Thus, the last result is not applicable for reasonable usage of secret-sharing schemes.

2. Preliminaries

In this section, we define secret-sharing schemes and provide some background material used in this work.

Notation 2.1. *We denote the logarithmic function with base* 2 *and base* e *by* log *and* ln*, respectively.*

2.1. *Secret Sharing*

We present a definition of secret sharing as given in [5,20].

Definition 2.2. Let $P = \{p_1, \dots, p_n\}$ be a set of parties. A collection $\Gamma \subseteq 2^P$ is *monotone* if $B \in \Gamma$ and $B \subseteq C$ imply that $C \in \Gamma$. An *access structure* is a monotone collection $\Gamma \subseteq 2^P$ of non-empty subsets of P. Sets in Γ are called *authorized*, and sets not in Γ are called *unauthorized*. The family of minimal authorized subsets is denoted by $\min \Gamma$.

A *distribution scheme* $\Sigma = \langle \Pi, \mu \rangle$ with domain of secrets K is a pair, where μ is a probability distribution on some finite set R called the set of random strings and Π is a mapping from $K \times R$ to a set of n-tuples $K_1 \times K_2 \times \cdots \times K_n$, where K_j is called the *domain of shares* of p_j. A dealer distributes a secret $k \in K$ according to Σ by first sampling a random string $r \in R$ according to μ, computing a vector of *shares* $\Pi(k, r) = (s_1, \dots, s_n)$, and privately communicating each share s_j to party p_j. For a set $A \subseteq P$, we denote $\Pi_A(s, r)$ as the restriction of $\Pi(s, r)$ to its A-entries.

Given a distribution scheme, the *size* of the secret is $\log(|K|)$, the (normalized) *size* of the share of the party p_j is $\log(|K_j|)/\log(|K|)$, and the (normalized) *total share size* of the distribution scheme is $\sum_{1 \le j \le n} \log(|K_j|)/\log(|K|)$.

Definition 2.3. (*Secret Sharing*) Let K be a finite set of secrets, where $|K| \geq 2$. A distribution scheme $\langle \Pi, \mu \rangle$ with domain of secrets K is a *secret-sharing scheme* realizing an access structure Γ if the following two requirements hold:
Correctness. The secret k can be reconstructed by any authorized set of parties. That is, for any set $B = \{p_{i_1}, \dots, p_{i_{|B|}}\} \in \Gamma$, there exists a *reconstruction function* $\mathrm{Recon}_B : K_{i_1} \times \cdots \times K_{i_{|B|}} \to K$ such that for every $k \in K$,

$$\Pr\Big[\mathrm{Recon}_B\Big(\Pi_B(k, r)\Big) = k \Big] = 1. \tag{1}$$

Privacy. Every unauthorized set cannot learn anything about the secret (in the information theoretic sense) from their shares.

Formally, for any set $T \notin \Gamma$, for every two secrets $a, b \in K$, and for every possible vector of shares $\langle s_j \rangle_{p_j \in T}$,

$$\Pr[\ \Pi_T(a, r) = \langle s_j \rangle_{p_j \in T}\ ] = \Pr[\ \Pi_T(b, r) = \langle s_j \rangle_{p_j \in T}\ ]. \tag{2}$$

Remark 2.4. There is an alternative definition of secret-sharing schemes (e.g., [18, 39]) using the entropy function. For that definition, it is assumed that there is some known probability distribution on the domain of secrets K, and the definition requires that the secret and the shares of every unauthorized subset are independent random variables (this can be formulated, e.g., using the entropy function). The two definitions are equivalent [4].

In this work, we mainly consider graph access structures. Let $G = (V, E)$ be an undirected graph. We consider the graph access structure, where the parties are the vertices of the graph and the minimal authorized sets are the edges. In other words, a set of vertices can reconstruct the secret if it contains an edge, and a set is unauthorized if it is an independent set in G. In the rest of the paper, we will not distinguish between the graph and the access structure it describes, and we will not distinguish between vertices and parties.

2.2. *Graph Terminology*

We define the graph terminology that we use throughout this paper. The *degree* of a graph is the maximum degree of vertices in a graph. A graph $G' = (V', E')$ is a *subgraph* of a graph $G = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E$. We next define covers of graphs, which are used in our construction of secret-sharing schemes.

Definition 2.5. Let $G = (V, E)$ be a graph. We say that a collection of graphs $G_1 = (V_1, E_1), \ldots, G_r = (V_r, E_r)$ is a λ-*cover* of G if each G_i is a subgraph of G, and each edge in E is in at least λ graphs of the collection. A *cover* of a graph is a 1-cover of the graph.

A k-*partite* graph $G = (V_1, \ldots, V_k, E)$, where $V_1, \ldots, V_k$ are disjoint, is a graph whose vertices are $V = \cup_{i=1}^{k} V_k$, such that if $(u, v) \in E$, then there are indices $i \neq j$ such that $u \in V_i$ and $v \in V_j$ (that is, there are edges only between vertices in different parts). A k-partite graph is *complete* if it contains all edges between vertices in different parts. A graph is a *multipartite* graph if it is k-partite for some k. For example, a clique is a complete n-partite graph, where n is the number of vertices in the clique. A complete bipartite graph in which $|V_1| = 1$ is called a *star*; the vertex in V_1 is the *center* and the ones in V_2 are the *leaves*.

2.3. *Graphs and Secret Sharing*

Brickell and Davenport [16] presented a construction of ideal secret-sharing schemes for multipartite graphs. As we use this construction, we describe it below.

Theorem 2.6. [16] *Let $G = (V_1, \ldots, V_k, E)$ be a complete multipartite graph and $p > k$ be a prime. There is a linear secret-sharing scheme realizing G where the domain of secrets and the domain of shares of each party are* $\{0, \ldots, p-1\}$.

Proof. Let $s \in \{0, \ldots, p-1\}$ be the secret. We first generate shares in Shamir's 2-out-of-k secret-sharing scheme [50] for the secret s. That is, we choose $a \in \{0, \ldots, p-1\}$ at random with uniform distribution, and we compute the share $s_i = a \cdot i + s \bmod p$ for

$1 \le i \le k$. Next, we give s_i to all vertices in V_i. Two vertices from different parts, say V_i and V_j, can reconstruct the secret as follows: $s = (j \cdot s_i - i \cdot s_j)/(j - i)$ (where the arithmetic is in $\mathbb{F}_p$—the finite field with p elements).

On the other hand, if a set T is unauthorized, then it is contained in some V_i, and all the vertices in T hold the same share in Shamir's scheme and do not have any information on the secret, that is, this share is uniformly distributed in $\{0, \ldots, p - 1\}$. □

Remark 2.7. Complete bipartite graphs admit a secret-sharing scheme whose domains of secrets and shares are $\{0, \ldots, j - 1\}$ for every $j \ge 2$. Let $s \in \{0, \ldots, j - 1\}$ be the secret. We choose $a \in \{0, \ldots, j - 1\}$ at random with uniform distribution, and we compute the share $s_1 = a$ and $s_2 = (a + s) \bmod j$.

Remark 2.8. Our main result, Theorem 4.4, uses the construction in the previous remark, and so there are no restrictions on the size of the domain of secrets. However, other results use the construction in Theorem 2.6 for $k = n$. The total share size of the scheme in Theorem 2.6 is n, but it requires $p > n$, and so the secret size has to be at least $\log(n)$. If the secret is shorter, then the share size and the total share size would increase by a factor of $\log(n)$ (by [40], this factor is unavoidable when the secret is one bit long). This work is focused on the study of the share size and the total share size of the schemes, but we will mention additional restrictions on the secret size where they are relevant.

In the rest of the paper, we will construct schemes, where we choose subgraphs of G which are multipartite and share the secret s independently for each subgraph. The following is a well-known lemma.

Lemma 2.9. *Let $G = (V, E)$ be a graph and $G_1 = (V_1, E_1), \ldots, G_r = (V_r, E_r)$ be a cover of G such that each G_i is a complete multipartite graph. Then, there exists a secret-sharing scheme realizing G with secret size $O(\log(r))$ in which the total share size is $\sum_{i=1}^{r} |V_i| \le nr$ and the size of each share is at most* $\max_i |\{j : v_i \in V_j\}| \le r$. *If each G_i is bipartite, then the size of the secret is 1; otherwise, the size of the secret is $O(\log(n))$.*

Proof. Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| \ge n$ (if every graph in the cover is bipartite, then we can take $\mathbb{F} = \mathbb{F}_2$). We share a secret $s \in \mathbb{F}$ independently for each G_i using the multipartite scheme.

We claim that the resulting scheme realizes G. First, let $(u, v) \in E$ be a minimal authorized set. Then, there exists at least one i such that $(u, v) \in E_i$ and u, v can reconstruct the secret from the shares of the secret-sharing scheme realizing G_i. On the other hand, let T be an unauthorized set in G, that is, T is an independent set in G. Since $E_i \subseteq E$ for every i, the parties in T get at most one different share in the scheme realizing G_i. As in each scheme we share the secret s independently (i.e., choose a independently), the unauthorized set T gets at most r random elements independent of each other; thus, they have no information on the secret.

For every i, in the scheme realizing G_i we give each party in V_i a share whose size is the size of the secret; thus, the total share size to realize all the graphs in the cover is $\sum_{i=1}^{r} |V_i|$. $\square$

We next describe a special case of Stinson decomposition techniques [54], implying that if we use a λ-cover by complete multipartite graphs, then we can save a factor of $1/\lambda$ in the share size compared with the secret-sharing scheme that uses a 1-cover of the same size.

Lemma 2.10. *Let $G = (V, E)$ be a graph and $G_1 = (V_1, E_1), \ldots, G_r = (V_r, E_r)$ be a λ-cover of G such that each G_i is a complete multipartite graph. Then, there exists a secret-sharing scheme realizing G with secret size $O(\lambda \log(\max\{r, n\}))$ in which the total share size is $\sum_{i=1}^{r} |V_i|/\lambda \leq nr/\lambda$ and the size of each share is at most* $\max_i |\{j : v_i \in V_j\}|/\lambda \leq r/\lambda$.

Proof. Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| \geq \max\{r, n\}$. Now, we use Stinson decomposition techniques [54] to construct a scheme for G over $\mathbb{F}$. Let $s = (s_1, \ldots, s_\lambda) \in \mathbb{F}^\lambda$ be the secret. First, we use a $(0, \lambda)$-ramp secret-sharing scheme to generate r shares $s_1, \ldots, s_r \in \mathbb{F}$ of the secret s [11].[3]

Then, for every graph G_i of the cover, we generate shares of s_i in the ideal scheme realizing G_i and distribute the shares among the parties of G_i. Since every edge is in at least λ graphs, every edge can obtain at least λ values s_i and so recover the secret. As in each graph G_i each party in V_i gets one element from $\mathbb{F}$, the size of each share of the resulting scheme is at most $\max_i |\{j : v_i \in V_j\}|/\lambda \leq r/\lambda$ and the total share size is at most $\sum_{i=1}^{r} |V_i|/\lambda \leq nr/\lambda$. $\square$

2.4. *Description of the Problem*

In this work, we study the problem of realizing a graph access structure, where the graph has few excluded edges. Specifically, let $G = (V, E)$ be an undirected graph with $|V| = n$ and $|E| = \binom{n}{2} - \ell$ for some $0 < \ell < \binom{n}{2}$. We consider the complement graph $\overline{G} = (V, \overline{E})$, where $e \in \overline{E}$ iff $e \notin E$. We call $\overline{G}$ the *excluded graph* and call its edges the *excluded edges*. In the rest of the paper, the excluded graph $\overline{G}$ is a sparse graph with $\ll \binom{n}{2}$ edges.

Example 2.11. Assume $\ell = 1$, that is, there is one excluded edge, say (v_{n-1}, v_n). In this case, the graph can be realized by an ideal scheme as the graph is the complete $(n-1)$-partite graph, where v_{n-1}, v_n are in the same part.

Example 2.12. Assume $\ell = 2$, and there are two adjacent excluded edges, say (v_{n-2}, v_n) and (v_{n-1}, v_n). In this case, the graph G is not a complete multipartite graph; hence, it cannot be realized by an ideal scheme [16]. However, it can be realized by a

[3] Let $\alpha_1, \ldots, \alpha_r$ be r distinct elements in $\mathbb{F}$. Compute the polynomial $Q(x)$ of degree $\lambda - 1$ such that $Q(\alpha_i) = s_i$ for $1 \leq i \leq \lambda$ and the share of p_i is $s_i = Q(\alpha_i)$.

scheme in which each of the parties $v_1, \ldots, v_{n-3}, v_n$ gets a share whose size is the size of the secret and v_{n-2}, v_{n-1} get a share whose size is twice the size of the secret. Thus, the total share size is $n + 2$.

The scheme is as follows: Generate shares according to Shamir's 2-out-of-$(n-2)$ secret-sharing scheme, and give party v_i the ith share in Shamir's scheme for $1 \le i \le n-2$. In addition give to v_{n-1} and v_n the $(n-2)$th share in Shamir's scheme. Using the above shares, every pair of parties, except for pairs contained in $\{v_{n-2}, v_{n-1}, v_n\}$, can reconstruct the secret. As the only authorized pair in $\{v_{n-2}, v_{n-1}, v_n\}$ is (v_{n-2}, v_{n-1}), we give them additional shares: We choose two random strings r_1 and r_2 whose exclusive-or is the secret and give r_1 to v_{n-2} and r_2 to v_{n-1}.

The above scheme is a special case of the complete multipartite cover scheme, where we cover the graph G by two graphs: A graph $G_1 = (V_1, E_1)$ with $V_1 = \{v_{n-2}, v_{n-1}\}$ and $E_1 = \{(v_{n-2}, v_{n-1})\}$ (that is, G_1 is the complete 2-partite graph on V_1), and the complete $(n-2)$-partite graph where every v_i, for $1 \le i \le n-3$, is a part, and $\{v_{n-2}, v_{n-1}, v_n\}$ is a part.

By [13], the total share size of the schemes realizing the graph G restricted to $\{v_{n-3}, v_{n-2}, v_{n-1}, v_n\}$ is at least 5. Therefore, the total share size of secret-sharing schemes realizing G is at least $n + 1$. That is, the above scheme is nearly optimal.

3. Constructions for Bounded Degree Excluded Graphs

In this work, we give an upper bound on the total share size for every graph with ℓ excluded edges, where the upper bound is a function of n and ℓ. If the excluded graph contains few edges, then the average degree of its vertices is small. We first construct a scheme for graphs such that the degree of all vertices in its excluded graph is bounded by some d. In Sect. 4, we show how we can use this construction for any graph with few excluded edges.

The construction of a secret-sharing scheme for a graph G whose excluded graph $\overline{G}$ has bounded degree uses a cover of G by complete bipartite graphs such that each vertex is contained in a relatively small number of graphs. In Sect. 5, we also provide an alternative construction that uses a cover by cliques.

3.1. *Complete Bipartite Covers*

Definition 3.1. (Complete bipartite cover and bipartite complement) Let G be a graph. A *complete bipartite cover* of G is a cover $H_1 = (U_1, V_1, E_1), \ldots, H_r = (U_r, V_r, E_r)$ of H such that each H_i is a complete bipartite graph.

The *bipartite complement* of a bipartite graph $H = (U, V, E)$ is the bipartite graph $\overline{H} = (U, V, \overline{E})$, where every $u \in U$ and $v \in V$ satisfy $(u, v) \in \overline{E}$ iff $(u, v) \notin E$.

Note that the bipartite complement of a bipartite graph is a bipartite graph and it differs from the complement of the bipartite graph. We next show the existence of small bipartite $\ln(n)$-covers for bipartite graphs whose bipartite complement graph has bounded degree.

We use techniques developed by Jukna [37, Theorem 1] to proof the existence of small bipartite $\ln(n)$-covers.[4]

Lemma 3.2. *Let $H = (U, V, E)$ be a bipartite graph such that $|U| \leq |V| = n$ and the degree of every vertex in V in the bipartite complement graph $\overline{H}$ is at most d. Then, there exists a $\ln(n)$-cover of H with $O(d \ln(n))$ complete bipartite graphs.*

Proof. The existence of the equivalence $\ln(n)$-cover of G is proved by using the *probabilistic method* (see, e.g., [2]). That is, to prove the existence of the desired cover, use a randomized process to choose the graphs and prove that with positive probability they are a cover.

Let $p = 1/d$ and $r = 8\ln(|E|)/(p(1-p)^d) = O(d\ln(n))$. We choose the complete bipartite graphs $H_1, \ldots, H_r$ as follows. Choose a set $U_i \subseteq U$ such that for every $u \in U$ add u to U_i with probability p independently of all other choices. Construct V_i as the set of all vertices in V that are adjacent to every $u \in U_i$ (that is, $v \in V_i$ iff $(u, v) \in E$ for every $u \in U_i$).

For an edge $(u, v) \in E$, define a Boolean random variable X_i, where $X_i = 1$ if (u, v) is in H_i, and $X_i = 0$ otherwise. Let $X = \sum_{i=1}^{r} X_i$. Notice that $X_i = 1$ if $u \in U_i$ and each of the neighbors of v in $\overline{H}$ is not in U_i (there are at most d such neighbors). Thus,

$$E(X) \geq rp(1-p)^d = 8\ln(|E|) > 8\ln(n).$$

By a Chernoff bound [45, Theorem 4.5],

$$\Pr[X \leq \ln(n)] \leq \Pr[X \leq E(X)/8] \leq e^{-E(X)(1-1/8)^2/2} < e^{-3\ln(n)} = 1/n^3.$$

By the union bound, the probability that there is an edge covered by less than $\ln(n)$ graphs of the complete bipartite cover is less than $1/(2n)$. In particular, there exists a cover as promised in the lemma. □

Remark 3.3. Note that in the above process, the construction of the bipartite graphs is efficient, that is, it can be computed in probabilistic polynomial time as we next explain. First, we choose a collection of graphs as described in Lemma 3.2. Next, we check whether the collection of bipartite graphs cover H, that is, we check that for every edge $(u, v) \in E$, there is at least one graph in the collection that covers (u, v). If this is not the case, we repeat the process of choosing r random graphs until we find a cover. As the probability of not choosing a cover is $1/n$, the expected number of times that we need to repeat this process is less than 2.

Lemma 3.4. *Let $G = (V, E)$ be a graph such that the degree of every vertex in its excluded graph $\overline{G}$ is at most d. Then, there exists a complete bipartite $\ln(n)$-cover of G with $O(d\ln(n))$ complete bipartite graphs.*

---

[4] Jukna proved this result for 1-covers, and we use a similar proof to prove the result for $\ln(n)$-covers (with a bigger constant in the size of the cover).

Proof. Let $V = U_1 = \{1, \dots, n\}$ and $U_2 = \{n+1, \dots, 2n\}$. Let $H = (U_1, U_2, F)$ be the bipartite graph with $F = \{(i, j+n) : (i, j) \in E\}$. For every $i \in V$, the degree of i in G is the same as the degree of i and $i+n$ in H. Hence, the bipartite complement of H has degree at most d.

By Lemma 3.2, there exists a complete bipartite $\ln(n)$-cover $(U_{1,1}, U_{1,2}, F_1), \dots, (U_{r,1}, U_{r,2}, F_r)$ of H with $r = O(d \ln(n))$. For $i = 1, \dots, r$, define $V_{i,1} = U_{i,1}$ and $V_{i,2} = \{j - n : j \in U_{i,2}\}$. Observe that $V_{i,1} \cap V_{i,2} = \emptyset$, and so each bipartite graph $H_i = (V_{i,1}, V_{i,2}, E_i)$ with $E_i = \{(i, j-n) : (i, j) \in F_i\}$ is complete and is a subgraph of G. Therefore, $H_1, \dots, H_r$ is a complete bipartite $\ln(n)$-cover of G. □

3.2. *Construction of Secret-Sharing Schemes for Graphs with Bounded Degree*

In this section, as a step in constructing a secret-sharing scheme realizing graphs with few excluded edges, we show how to use complete bipartite covers to realize two families of graphs: (1) graphs such that the degree of every vertex is big and (2) bipartite graphs such that one of their parts is small and the degree of each vertex in the other part is big.

Lemma 3.5. *Let $G = (V, E)$ be a graph such that the maximum vertex degree in $\overline{G} = (V, \overline{E})$ is less or equal to d. Then, G can be realized by a secret-sharing scheme with secret size $O(\ln^2(n))$ in which the size of each share is $O(d)$ and the total share size is $O(dn)$. Furthermore, G can be realized by a secret-sharing scheme with secret size* 1 *in which the size of each share is $O(d \ln(n))$ and the total share size is $O(dn \log(n)) = \tilde{O}(dn)$.*

Proof. By Lemma 3.4, there exists a complete bipartite $\ln(n)$-cover of G with $r = O(d \ln(n))$ graphs. Thus, by Lemma 2.10, there exists a secret-sharing scheme realizing G in which the secret size is $O(\ln^2(n))$, the size of each share is $O(d)$, and the total share size is $O(dn)$.

As every $\ln(n)$-cover of G is a cover, by Lemma 2.9, there exists a secret-sharing scheme realizing G in which the secret size is 1, the size of each share is $O(d \ln(n))$, and the total share size is $O(dn \ln(n))$. □

Lemma 3.6. *Let $d < n$ and $H = (U, V, E)$ be a bipartite graph such that $|U| = k \le n$, $|V| \le n$, and the degree of every vertex in U in $\overline{H}$ is at most d. Then, H can be realized by a secret-sharing scheme in which the total share size is $\tilde{O}(n + k^{3/2}d)$. If $k = (n/d)^{2/3}$, the total share size is $\tilde{O}(n)$.*

Proof. Let $D = \left\{v \in V : \text{There exists } u \in U \text{ such that } (u, v) \in \overline{E}\right\}$. As the degree of every vertex in U in $\overline{H}$ is at most d, the size of D is at most dk. Furthermore, the complete bipartite graph $H_1 = (U, V \setminus D, U \times (V \setminus D))$ is a subgraph of H. We realize H_1 by an ideal scheme in which the total share size is at most $|U| + |V| = O(n)$.

Now, define $D_2 = \left\{v \in D : \text{The degree of } v \text{ in } \overline{H} \text{ is at least } \sqrt{k}\right\}$. As $\overline{H}$ contains at most dk edges, $|D_2| \le d\sqrt{k}$. Let $H_2 = (U, D_2, E \cap (U \times D_2))$. The number of edges in H_2 is less than $|U||D_2| \le k^{3/2}d$; thus, we can realize H_2 by a secret-sharing scheme in which the total share size is $O(k^{3/2}d)$.

Finally, let $V_3 = D \setminus D_2$ and $H_3 = (U, V_3, E \cap (U \times V_3))$. The degree of each vertex in V_3 in the graph $\overline{H_3}$ is at most $\sqrt{k}$; thus, by Lemma 3.5, we can realize H_3 by a secret-sharing scheme in which the total share size is $O(\sqrt{k}(|U| + |V_3|) \ln(|U| + |V_3|)) = O(k^{3/2} d \ln(n))$.

As H_1, H_2, and H_3 cover H, we constructed a scheme realizing H in which the total share size is $\tilde{O}(n + k^{3/2}d)$. Taking $k = (n/d)^{2/3}$, the total share size is $\tilde{O}(n)$. □

4. Constructions for Excluded Graph with Few Edges

We next show how to use the schemes of Lemmas 3.5 and 3.6 to realize excluded graphs with $\ell = n^{1+\beta}$ edges, where $0 \leq \beta < 1$. We will start with a simple approach and then use more complicated constructions to achieve better upper bounds. We construct our scheme in steps, where in each step: (1) We choose a set of vertices $V' \subseteq V$. (2) We give shares to the parties in V' and the rest of the parties, such that each edge incident with a party in V' can reconstruct the secret, and all other pairs of parties (i.e., unauthorized pairs containing parties in V' and all pairs disjoint with V') get no information on the secret. (3) We remove the vertices in V' and all their incident edges from the graph. We repeat the following step until all vertices in $\overline{G}$ have small degree and then use the complete bipartite cover scheme of Sect. 3 to realize the remaining graph. In this process, we will ensure that the total share size remains relatively small. In the following, n will always refer to the number of vertices in the original graph.

Our first step is removing all vertices whose degree in $\overline{G}$ is "high."

Lemma 4.1. *Let G be a graph such that its excluded graph $\overline{G}$ contains at most $n^{1+\beta}$ edges, where $0 \leq \beta < 1$. Then, for every $d < n$, we can give shares of size $O(n^{1+\beta}/d)$ to each vertex and remove a set of vertices from G and all the incident edges and obtain an induced subgraph G' of G such that $\overline{G'}$ contains at most $n^{1+\beta}$ edges and the degree of $\overline{G'}$ is at most d.*

Proof. We choose a vertex v whose degree in $\overline{G}$ is greater than d and consider the star whose center is v, and its leaves are all neighbors of v in G. We realize this star using an ideal scheme and remove v and its incident edges from G.

We choose another vertex whose degree in $\overline{G}$ is greater than d and do the same until no vertices with degree greater than d exist in $\overline{G}$. As in the beginning, there are $n^{1+\beta}$ edges in $\overline{G}$, and in each step, we remove at least d edges from $\overline{G}$, the number of steps is at most $n^{1+\beta}/d$. Thus, the size of each share of the resulting scheme for the removed vertices is $O(n^{1+\beta}/d)$. □

Using Lemmas 4.1 and 3.5, we can get a non-trivial scheme realizing dense graphs.

Theorem 4.2. *Let $G = (V, E)$ be a graph with $|V| = n$ and $|E| = \binom{n}{2} - n^{1+\beta}$ for some $0 \leq \beta < 1$. There exists a secret-sharing scheme realizing G in which the size of each share is $\tilde{O}(n^{1/2+\beta/2})$ and the total share size is $\tilde{O}(n^{3/2+\beta/2})$.*

Proof. Let $d = \sqrt{n^{1+\beta}}$. We first apply Lemma 4.1 and remove all vertices whose degree in $\overline{G}$ is greater than $n^{1/2+\beta/2}$; the size of the share of each vertex is $O(n^{1+\beta}/d)$. After this step, we obtain a graph G' such that the degree of $\overline{G'}$ is at most d. Then, we use Lemma 3.5 to realize the remaining graph G'; the size of the share of each vertex is $O(d\ln(n))$. Thus, the size of each share in the resulting scheme G is $O(n^{1+\beta}/d + d\ln(n)) = \tilde{O}(n^{1/2+\beta/2})$, and the total share size is $\tilde{O}(n^{3/2+\beta/2})$. □

We use further intermediate steps to improve the total share size compared to the above construction.

Lemma 4.3. *Let $\alpha' < \alpha \leq 1$ such that $\alpha \geq 0.25$ and $G = (V, E)$ be a graph such that the degree of $\overline{G}$ is at most n^{α} and $\overline{G}$ contains ℓ edges. Then, we can remove a set of vertices and all incident edges from the graph and obtain a graph G' such that the degree of $\overline{G'}$ is at most $n^{\alpha'}$, the graph $\overline{G'}$ contains $\ell - \ell'$ excluded edges for some $\ell' > 0$, and the total share size for the removed edges is $\tilde{O}(\ell' n^{1/3+2\alpha/3-\alpha'})$.*

Proof. Our task is to remove from G all vertices whose degree in $\overline{G}$ is greater than $n^{\alpha'}$. We remove the vertices of degree larger than $n^{\alpha'}$ in steps, where in each step we choose a set F of vertices and remove F and all edges incident to F. There are two types of such edges, edges with two endpoints in F and edges with one endpoint in F and one endpoint in $V \setminus F$. On the one hand, we would like to minimize the number of steps, thus, choose large sets F. On the other hand, we would like to minimize the number of edges in G incident only to vertices in F, thus, choose small sets F. To optimize the share size, we take sets F of size $(n/d)^{2/3}$.

Formally, let $d = n^{\alpha}$ and $d' = n^{\alpha'}$. We remove the vertices of degree larger than d' in steps. In each step, we choose an arbitrary set F of $k = (n/d)^{2/3}$ vertices of degree at least d' in $\overline{G}$ (if the number of vertices of degree d' is smaller than k, then we take the remaining vertices of degree d' and put them in F). First, consider all edges whose two edges are in F, there are less than $k^2 = n^{4/3}/d^{4/3} \leq n$ such edges (since $d \geq n^{1/4}$). We can realize the graph $(F, E \cap (F \times F))$ with a scheme in which the total share size is $2|E \cap (F \times F)| \leq 2k^2 = O(n)$. Next, consider the bipartite graph $H = (F, V \setminus F, E \cap (F \times (V \setminus F)))$. By Lemma 3.6, we can realize H with a scheme in which the total share size is $\tilde{O}(n)$. Thus, we can remove the vertices in F and all edges incident with them, and the total share size of the scheme for every step is $\tilde{O}(n)$.

To give an upper bound on the total share size for the removed edges, we need to give an upper bound on the number of steps. Let ℓ' be the total number of edges we removed from $\overline{G}$ in these steps until the degree of $\overline{G}$ is at most d'. As each vertex we remove has degree at least d' in $\overline{G}$, the number of vertices we remove is at most ℓ'/d'. In each step, except for the last, we remove a set F with $(n/d)^{2/3}$ vertices; thus, the number of sets we remove is at most $1 + \ell'/(d'(n/d)^{2/3}) = O(\ell' d^{2/3}/(d' n^{2/3}))$. As in each step the share size is $\tilde{O}(n)$, the total share size for the edges we removed from G is $\tilde{O}\left(\ell' n^{1/3} d^{2/3}/d'\right) = \tilde{O}(\ell' n^{1/3+2\alpha/3-\alpha'})$. □

We next show how to construct secret-sharing schemes for graphs with few excluded edges using the three building blocks presented so far: (1) initial degree reductions using stars, (2) $O(\log\log(n))$ steps of degree reduction using complete bipartite graphs and stars, and (3) using the complete bipartite cover construction on the graph with reduced degree. The total share size of the resulting scheme is lower than the total share size of the scheme constructed in Theorem 4.2 (however, the size of each share can be bigger).

Theorem 4.4. *Let $G = (V, E)$ be a graph with $|V| = n$ and $|E| = \binom{n}{2} - n^{1+\beta}$ for some $0 \leq \beta < 1$. There exists a secret-sharing scheme realizing G with secret size 1 and total share size $\tilde{O}(n^{5/4+3\beta/4})$.*

Proof. Let α_0 be a constant to be determined later. We first apply Lemma 4.1 with $d = n^{\alpha_0}$ and obtain a graph G such that the degree of $\overline{G}$ is at most d. The total share size in this step is

$$O(n^{2+\beta}/d) = O(n^{2+\beta-\alpha_0}). \tag{3}$$

Next define $\alpha_i = (3 - 2(2/3)^i)\alpha_0 - 2 + 2(2/3)^i$ for $1 \leq i \leq \log\log(n)$. We choose these constants such that$2\alpha_i/3 - \alpha_{i+1} = 2/3 - \alpha_0$.

We next repeatedly apply the degree reduction in Lemma 4.3; we apply it $\log\log(n)$ times. In the ith invocation of the lemma, where $0 \leq i < \log\log(n)$, we take $\alpha = \alpha_i$ and $\alpha' = \alpha_{i+1}$. The cost of each invocation is

$$\tilde{O}\left(\ell_i n^{\frac{1}{3}+\frac{2\alpha_i}{3}-\alpha_{i+1}}\right) = \tilde{O}(\ell_i n^{1-\alpha_0}),$$

where ℓ_i is the number of edges removed from $\overline{G}$ in the ith invocation. As the number of edges removed in all invocations is at most $n^{1+\beta}$, the total share size in all these invocations is

$$\tilde{O}(n^{1+\beta}n^{1-\alpha_0}) = \tilde{O}(n^{2+\beta-\alpha_0}). \tag{4}$$

After the $\log\log(n)$ invocations of Lemma 4.3, the degree of each vertex in $\overline{G}$ is at most $n^{\alpha_{\log\log(n)}} = O(n^{3\alpha_0-2})$. In the final stage, we use Lemma 3.5 and realize the graph with total share size

$$\tilde{O}(nn^{3\alpha_0-2}) = \tilde{O}(n^{3\alpha_0-1}). \tag{5}$$

The total share of realizing G (by (3), (4), and (5)) is $O(n^{2+\beta-\alpha_0}) + \tilde{O}(n^{2+\beta-\alpha_0}) + \tilde{O}(n^{3\alpha_0-1})$. To minimize this expression, we require that $2 + \beta - \alpha_0 = 3\alpha_0 - 1$; thus, $\alpha_0 = 3/4 + \beta/4$ and the total share size in the scheme is $\tilde{O}(n^{5/4+3\beta/4})$. □

Remark 4.5. It can be checked that the construction of the cover of G by bipartite graphs, as done in Theorem 4.2 and Theorem 4.4, can be done by a probabilistic algorithm in expected polynomial time. Thus, the computation of the dealer and the parties in our scheme is efficient.

Remark 4.6. We can also prove that there exists a secret-sharing scheme realizing G with secret size $O(\ln^2(n))$ in which the size of each share is $O(n^{1/2+\beta/2})$ and the total share size is $O(n^{3/2+\beta/2})$ (that is, we get rid of logarithmic factors). The proof is analogous, but using the $\ln(n)$-cover in Lemma 3.5 instead of the 1-cover. Similarly, there exists a secret-sharing scheme realizing G with secret size $O(\ln^2(n))$ in which the total share size is $O(n^{5/4+3\beta/4})$.

In Theorem 4.4, we showed how to realize a graph where the number of excluded edges is small; however, it is at least n. We next show how to realize graphs where the number of excluded edges is less than n.

Corollary 4.7. *Let $G = (V, E)$ be a graph with $|V| = n$ and $|E| = \binom{n}{2} - \ell$ for some $0 < \ell < n/2$. There exists a secret-sharing scheme realizing G with secret size $O(\ln(n))$ in which the size of each share is $\tilde{O}(\ell^{1/2})$ and with total share size $n + \tilde{O}(\ell^{3/2})$. Furthermore, there exists a secret-sharing scheme realizing G with secret size $O(\ln(n))$ and total share size $n + \tilde{O}(\ell^{5/4})$.*

Proof. Let $V' \subseteq V$ be the set of vertices incident with the excluded edges. As there are ℓ excluded edges, the size of V' is at most 2ℓ. Without loss of generality, let $V = \{v_1, \ldots, v_n\}$ and $V' = \{v_t, \ldots, v_n\}$ for some $t > n - 2\ell$. We first execute Shamir's 2-out-of-t secret-sharing scheme and give the share s_i to party v_i for $1 \le i < t$ and give the share s_t to v_i for $t \le i \le n$.

Let V'' be such that $V' \subseteq V''$ and $|V''| = 2\ell$. Furthermore, let $G' = (V'', E')$ be the subgraph of G induced by V''. The graph G' has $n' = 2\ell$ vertices and $\ell \le n'$ excluded edges; thus, by Theorem 4.2, it can be realized by a scheme in which the size of each share is $\tilde{O}(\ell^{1/2})$ and total share size $\tilde{O}(\ell^{3/2})$. As every vertex in $V \setminus V''$ gets a share in Shamir's scheme, the total share size in the scheme realizing G is $n + \tilde{O}(\ell^{3/2})$.

Moreover, by Theorem 4.4 (with $\beta = 0$), G' can also be realized by a scheme in which the total share size is $\tilde{O}(\ell^{5/4})$. The total share size in realizing G is, therefore, $n + \tilde{O}(\ell^{5/4})$. □

5. Constructions for Homogeneous Access Structures

In this section, we extend the techniques used in the construction of graph secret-sharing schemes to the construction of schemes for homogeneous access structures, which are access structures whose minimal authorized subsets are of the same size. Every k-homogeneous access structure has a monotone formula of size $O(n^k/\log(n))$ (see [59, Theorem 7.3]); thus, by [9], it can be realized by a secret-sharing scheme with total share size $O(n^k/\log(n))$. Other upper bounds for homogeneous access structures are presented in [41,48,53]; however, they are useful for sparse access structures. We present constructions for dense k-homogeneous access structures for a constant k. We will describe these access structures by hypergraphs.

A *hypergraph* is a pair $H = (V, E)$ where V is a set of vertices and $E \subseteq 2^V \setminus \{\emptyset\}$ is the set of *hyperedges*. In this work, we only consider hypergraphs in which no hyperedge properly contains any other hyperedge. A hypergraph is *k-uniform* if $|e| = k$ for every $e \in E$. A k-uniform hypergraph is *complete* if $E = \binom{V}{k} = \{e \subseteq V : |e| = k\}$. For any k-uniform hypergraph, we define the *complement* hypergraph $\overline{H} = (V, \overline{E})$, with $\overline{E} = \binom{V}{k} \setminus E$. Observe that there is a one-to-one correspondence between uniform hypergraphs and homogeneous access structures and that complete uniform hypergraphs correspond to threshold access structures.

First, we present a combinatorial technique for obtaining clique covers of a graph G whose excluded graph $\overline{G}$ has bounded degree. This technique uses a clique cover of G that is obtained using colorings of the excluded graph $\overline{G}$. Then, we extend this technique to hypergraphs, and we present a technique to cover k-uniform hypergraphs with complete k-uniform hypergraphs. Finally, we construct secret-sharing schemes for homogeneous access structures using these techniques.

5.1. *Equivalence Covers*

Definition 5.1. An *equivalence graph* is a vertex-disjoint union of cliques. An *equivalence cover* of $G = (V, E)$ is a cover $G_1 = (V, E_1), \dots, G_r = (V, E_r)$ of G such that each G_i is an equivalence graph.

A *coloring* of a graph $\overline{G} = (V, \overline{E})$ with c colors is a mapping $\mu : V \to \{1, \dots, c\}$ such that $\mu(u) \neq \mu(v)$ for every $(u, v) \in \overline{E}$.

Lemma 5.2. *Let $G = (V, E)$ be a graph such that the degree of every vertex in its excluded graph $\overline{G}$ is at most d. Then, there exists an equivalence $\ln(n)$-cover of G with $O(d \ln(n))$ equivalence graphs.*

Proof. An equivalence cover of G can be described by a coloring of $\overline{G}$ and vice versa: given a coloring μ of $\overline{G}$, we construct an equivalence graph $G' = (V, E')$, which is a subgraph of G, where two vertices in G' are connected if they are colored by the same color, that is, $E' = \{(u, v) : \mu(u) = \mu(v)\}$. For every color, the set of vertices colored by such color is an independent set in $\overline{G}$, hence a clique in G.

As in the proof of Lemma 3.2, the existence of the equivalence $\ln(n)$-cover of G is proved by using the probabilistic method. We choose $r = 64d \ln(n)$ random colorings $\mu_1, \dots, \mu_r$ of $\overline{G}$ with $4d$ colors. That is, each coloring is chosen independently with uniform distribution among all colorings of $\overline{G}$ with $4d$ colors. For every coloring μ_i, we consider the equivalence graph G_i as described above. We next prove that with probability at least half $G_1, \dots, G_r$ is an equivalence cover of G.

Let $(u, v) \in E$. We first fix i and compute the probability that u and v have the same color in the random coloring μ_i. Fix an arbitrary coloring of all vertices except for u and v. We prove that conditioned on this coloring, the probability that u and v are colored in the same color is at least $1/(8d)$: On the one hand, the number of colorings for u and v completing the partial coloring is at most $16d^2$. On the other hand, the number of colors not used by the neighbors of u and v is at least $2d$; thus, there are at least $2d$ colorings for u and v completing the partial coloring in which u and v are colored by the same color. That is, with probability at least $1/(8d)$, the edge (u, v) is covered by the graph G_i.

For every edge $(u, v) \in E$, define a Boolean random variable X_i, where $X_i = 1$ iff in the ith coloring u and v are colored in the same color, and $X_i = 0$ otherwise. Let $X = \sum_{i=1}^{64d \ln(n)} X_i$. Notice that $E(X) \geq 64d \ln(n)/8d = 8 \ln(n)$. By a Chernoff bound [45, Theorem 4.5],

$$\Pr[X \leq \ln(n)] \leq \Pr[X \leq E(X)/8] \leq e^{-E(X)(1-1/8)^2/2} < e^{-2\ln(n)} = 1/n^2.$$

Thus, by the union bound, the probability that there exists an edge $(u, v) \in E$ that in less than $\ln(n)$ colorings u and v are colored in the same color is less than $\binom{n}{2}/n^2 < 1/2$. In particular, such a cover with r equivalence graphs exists. □

Remark 5.3. The existence of the equivalence cover in Lemma 5.2 is not constructive as we need to choose a random coloring of a graph of bounded degree. Such coloring can be chosen with nearly uniform distribution in polynomial time using a Markov process [36,49]. Given a collection of equivalence graphs, it is easy to check that for every edge $(u, v) \in E$ there is at least one graph in the collection that covers (u, v). If this is not the case, we repeat the process of choosing r random colorings until we find a good collection. The expected number of collections of colorings that have to be chosen before finding a good one is $O(1)$. Thus, we get a probabilistic polynomial-time algorithm to construct the equivalence cover.

Alon [1] observed that the size of the smallest equivalence cover of a graph G is smaller than the smallest clique cover of G. He further proved that if the degree of every vertex in $\overline{G}$ is at most d, then G can be covered by $O(d^2 \ln(n))$ cliques. We directly analyze the size of the smallest equivalence cover and get an equivalence cover of size $O(d \ln(n))$. To the best of our knowledge, such bound was not known prior to our work.

By analogy to graphs, we define an *equivalence* k-hypergraph as a vertex-disjoint union of complete k-uniform hypergraphs, and the *equivalence cover* of a k-uniform hypergraph $H = (V, E)$ as a collection of equivalence k-hypergraphs $H_1 = (V, E_1), \ldots, H_r = (V, E_r)$ with $E_i \subseteq E$ for $i = 1, \ldots, r$ and $\cup_{1 \leq i \leq r} E_i = E$. A *weak* coloring with c colors of a hypergraph $H = (V, E)$ is a mapping $\mu : V \to \{1, \ldots, c\}$ such that for every $e \in E$ there exist $u, v \in e$ with $\mu(u) \neq \mu(v)$.

Lemma 5.4. *Let $H = (V, E)$ be a k-uniform hypergraph such that the degree of every vertex in its excluded hypergraph is at most d. Then, there exists an equivalence cover of H with $r = 2^k k^k d^{k-1} \ln(n)$ equivalence hypergraphs.*

Proof. The proof of this lemma is similar to the one of Lemma 5.2 and is also based on the probabilistic method. Given a coloring μ of $\overline{H}$, we construct an equivalence k-hypergraph $H' = (V, E')$, which is the sub-hypergraph of H, where $\{v_1, \ldots, v_k\} \subset V$ is in E' if and only if $\mu(v_i) = \mu(v_j)$ for $1 \leq i < j \leq k$. For every color, the set of vertices colored by such a color is a complete k-uniform sub-hypergraph of H.

We choose r random colorings $\mu_1, \ldots, \mu_r$ of $\overline{H}$ with $2kd$ colors, and for each coloring, we consider the equivalence hypergraph as described above. With probability at least $1 - 1/(k!)$, the collection $H_1, \ldots, H_r$ is an equivalence cover of H:

Let $e = (v_1, \ldots, v_k) \in E$. Following arguments analogous to the ones in Lemma 5.2, we obtain that for each μ_i the hyperedge e is monochromatic with probability at least $\frac{1}{2(2kd)^{k-1}}$. By the same Chernoff bound, the probability that an edge $e \in E$ is not covered by the r random equivalence k-hypergraphs $H_1, \ldots, H_r$ is at most $1/n^k$. Thus, by the union bound, the probability that there exists an edge in E not covered by the r random equivalence k-hypergraphs is less than $\binom{n}{k}/n^k < 1/(k!)$. □

5.2. *Secret-Sharing for Uniform Hypergraphs with Few Excluded Sets*

We first present an alternative proof of Lemma 3.5, which states that if the excluded graph has degree at most d, then it can be realized with total share size $\tilde{O}(dn)$. The alternative proof uses cliques instead of bipartite graphs. The secret size of the following construction, as well as the ones in Lemma 5.5, Theorem 5.7, and Corollary 5.8, is $O(\ln(n))$. In Lemma 3.5, the secret size is 1 in the relevant scheme.

Alternative proof of Lemma 3.5. Consider an equivalence 1-cover of G with $r = O(d \ln(n))$ equivalence graphs (as guaranteed by Lemma 5.2). We realize the access structure of each equivalence graph G_i in the collection by an ideal scheme: For every clique C in G_i, generate shares in Shamir's 2-out-of-$|C|$ secret-sharing scheme and distribute the shares among the parties of C.

For every excluded edge $(u, v) \notin E$, the vertices u and v are in different cliques in each G_i (as G_i is a subgraph of G). Thus, in the above scheme, u and v do not get any information. On the other hand, every edge $(u, v) \in E$ is covered by at least one graph G_i, that is, u and v are in the clique in G_i; thus, u and v can reconstruct the secret. As in each graph G_i each party gets one share, the size of each share of the resulting scheme is $r = O(d \ln(n))$ and the total share size is $O(dn \ln(n)) = \tilde{O}(dn)$.

To get a scheme with total share size $O(dn)$ (rather than $\tilde{O}(dn)$), we consider an equivalence $\ln(n)$-cover of G with $O(d \ln(n))$ equivalence graphs (as guaranteed by Lemma 5.2). Then, apply Lemma 2.10. The secret size in this case is $O(\ln^2 n)$. □

Lemma 5.5. *Let $H = (V, E)$ be a k-uniform hypergraph such that the maximum vertex degree of $\overline{H} = (V, \overline{E})$ is at most d. There exists a secret-sharing scheme realizing H in which the size of each share is $O(2^k k^k d^{k-1} \ln(n))$ and the total share size is $\tilde{O}(2^k k^k d^{k-1} n)$.*

Proof. Take the equivalence cover of H of size $r = 2^k k^k d^{k-1} \ln(n)$ guaranteed by Lemma 5.4. Now, we realize each equivalence k-hypergraph H_i in the collection by an ideal scheme: For every complete hypergraph C in H_i, generate shares in Shamir's k-out-of-$|C|$ secret-sharing scheme. Using arguments similar to the ones used in the alternative proof of Lemma 3.5, we obtain that this scheme realizes H, and the size of each share of the resulting scheme is r, and the total share size is $rn = \tilde{O}(2^k k^k d^{k-1} n)$. □

In Theorem 5.7 below, we construct a secret-sharing scheme for every excluded hypergraph with few edges. For this purpose, we use a recursive argument based on the construction illustrated in the following example.

Example 5.6. Let $H = (V, E)$ be a hypergraph and let $v \in V$ be a vertex satisfying that $v \in e$ for every $e \in E$. Consider the hypergraph $H' = (V', E')$ with $V' = V \setminus \{v\}$ and $E' = \{e \setminus \{v\} : e \in E\}$. Given a secret-sharing scheme realizing H', we can construct a scheme for H as follows. In order to share a secret s, the dealer chooses at random s_1 and s_2 satisfying $s = s_1 + s_2$, sends s_1 to v, and shares s_2 among V' using the scheme realizing H'. Observe that the size of the shares of $v' \in V'$ is the same in both schemes, and the size of the share of v is 1.

Theorem 5.7. *Let $H = (V, E)$ be a k-hypergraph with $|V| = n$ and $|E| = \binom{n}{k} - n^{1+\beta}$ for some $0 \le \beta < k-1$. There exists a secret-sharing scheme realizing H in which the size of each share is $\tilde{O}(2^k k^k n^{1+\beta})$ and the total share size is $\tilde{O}(2^k k^k n^{2+\beta})$.*

Proof. By induction on k, we prove that for every $H = (V, E)$ satisfying the hypothesis there exists a secret-sharing scheme in which the size of each share is $\tilde{O}(2^k k^k \ell^{1-\varepsilon_k})$, where $\ell = n^{1+\beta}$ and ε_k is defined by the equation $\varepsilon_{i+1} = \frac{\varepsilon_i}{i+\varepsilon_i}$ and $\varepsilon_1 = 1$. By Theorem 4.2, this property is satisfied for $k = 2$. Let $H = (V, E)$ be a k-hypergraph with $k > 2$. Define $d = \ell^{\frac{1}{k-1+\varepsilon_{k-1}}}$.

We choose a vertex v incident with $\ell_1 > d$ excluded hyperedges. By the hypothesis, there is a secret-sharing scheme in which the size of each share is $\tilde{O}(2^{k-1}(k-1)^{k-1}\ell_i^{1-\varepsilon_{k-1}})$ for the $(k-1)$-hypergraph $H' = (V', E')$, with $V' = V \setminus \{v\}$ and $E' = \{e \in \binom{V'}{k-1} : e \cup \{v\} \in E\}$. Following Example 5.6, we construct a scheme for the sub-hypergraph determined by all hyperedges incident with v. Then, we remove v and its incident hyperedges from H. We choose another vertex v' incident with $\ell_2 > d$ excluded hyperedges and do the same until no vertices with degree greater than d in $\overline{H}$ exist.

In the beginning, there are ℓ excluded hyperedges, and in each step we remove $\ell_i > d$ hyperedges, so the number of steps is at most ℓ/d. Thus, the size of each share in the resulting scheme is

$$\tilde{O}\left(2^{k-1}(k-1)^{k-1}\sum_{i=1}^{\ell/d}\ell_i^{1-\varepsilon_{k-1}}\right).$$

As $\sum_{i=1}^{\ell/d}\ell_i \le \ell$, the above expression is maximized when $\ell_1 = \cdots = \ell_{\ell/d} = d$, so the size of each share is $\tilde{O}(2^{k-1}(k-1)^{k-1}\ell/d^{\varepsilon_{k-1}})$.

Finally, since the degree of $\overline{H}$ is at most d, we use Lemma 5.4 to construct a secret-sharing scheme realizing H in which the size of each share is $\tilde{O}(2^k k^k d^{k-1})$. □

Corollary 5.8. *Let $H = (V, E)$ be a k-uniform hypergraph with $|V| = n$ and $|E| = \binom{n}{k} - \ell$ for some $0 < \ell < n/k$. There exists a secret-sharing scheme realizing H in which the size of each share is $\tilde{O}(2^k k^{k+1}\ell)$ and the total share size is $n + \tilde{O}(2^k k^{k+2}\ell^2)$.*

Proof. Define $W \subseteq V$ as the set of vertices of degree zero in $\overline{H}$. Since $\ell k < n$, $|W| > 0$. Consider the k-hypergraph $H' = (V, E')$ with $E' = \{e \in \binom{V}{k} : |e \cap W| \ge 1\}$. Observe that $H' \subseteq H$. By [47], there exists an ideal secret-sharing scheme realizing H'. Now, it remains to find a secret-sharing scheme for $H \setminus H'$, a hypergraph defined on $V \setminus W$ whose complement has at most ℓk vertices and ℓ hyperedges. The proof is completed by using Theorem 5.7. □

Remark 5.9. By [31], the scheme used in the first step of the proof of Corollary 5.8 can be constructed over any finite field $\mathbb{F}$ with $|\mathbb{F}| > \binom{n+1}{k}$.

6. Removing Few Authorized Sets from Access Structures

Our main result (Theorem 4.4) shows that if we start with the complete graph and remove "few" edges, then the share size required to realize the new graph is not "too big." We then generalize these results to complete uniform hypergraphs. In this section, we address the effect of removing few authorized sets from other access structures. We first consider arbitrary graph access structures and then consider access structures where the minimal authorized sets are small and, for each party, we remove few sets containing the party (this generalizes the case where the complement graph has constant degree). We remark that the size of the secret in the secret-sharing schemes presented in this section can be large, because we use secret-sharing schemes realizing various access structures.

6.1. *Removing Few Edges from an Arbitrary Graph*

We show that if we start with any graph and remove "few" edges, then the total share size required to realize the new graph is not much larger than the total share size required to realize the original graph.

Theorem 6.1. *Let $G = (V, E)$ and $G' = (V, E')$ be two graphs with $E' \subset E$, $|E \setminus E'| = \ell$, and $|V| = n$. Assume G can be realized by a scheme in which the total share size is m (clearly, $m \leq \binom{n}{2}$). If $\ell > m/n$, then G' can be realized by a secret-sharing scheme in which the total share size is $\tilde{O}(\sqrt{\ell mn})$. If $\ell \leq m/n$, then G' can be realized by a scheme in which the total share size is $m + 2\ell n \leq 3m$.*

Proof. Let Σ be a secret-sharing scheme realizing G with total share size m. Suppose that $\ell > m/n$. Define $d = \sqrt{\ell n/m}$. Let $G'' = (V, E'')$ be the graph satisfying that $e \in \overline{E''}$ if and only if $e \in E \setminus E'$ (that is, $\overline{G''}$ is the graph of the excluded edges, and G'' is its complement).

First, we construct a scheme similar to the one described in the proof of Lemma 4.1. For every party v incident with at least d excluded edges, we consider the star whose center is v and its leaves are all neighbors in G'. We realize this star using an ideal scheme, and we remove v and its incident edges from G' and from G''. The total share size in this step is at most n. We do the same process until all vertices have less than d excluded vertices. The total share size of the resulting scheme is $O(n\ell/d) = O(\sqrt{\ell mn})$.

Now, the degree of every vertex in G'' is at most d. By Lemma 5.2, there exists an equivalence 1-cover of G'' with $O(d \ln(n))$ equivalence graphs. For every equivalence graph, and for every clique C in it, we independently share the secret s among the parties in C using Σ, that is, we generate shares of s using Σ and give the shares only to the participants of C. In this way, an edge contained in C is authorized if and only if it is contained in E. Since $E'' \cap E = E'$, the resulting scheme realizes G'. The total share size of realizing each equivalence graph is m (since each participant is in a single clique); thus, the total share size of realizing all graphs in the cover is $O(md \ln(n)) = \tilde{O}(md) = \tilde{O}(\sqrt{\ell mn})$.

If $\ell < m/n$, we first execute Σ and give shares to parties not incident with excluded edges. The total share size in this step is less than m. For every party v incident to at least one excluded edge, we construct a secret-sharing scheme realizing the star whose center is v and the leaves are those $u \in V$ with $(u, v) \in E'$. As there are at most 2ℓ such vertices, the total share size in realizing the stars is less than $2\ell n$. The total share size in both steps is $m + 2\ell n \leq 3m$. □

In the interesting case in Theorem 6.1 when $\ell > m/n$, the total share size is $\tilde{O}(\sqrt{\ell mn})$. This is better than the trivial scheme giving shares of total size $O(n^2/\log n)$ only when ℓ is not too large, namely $\ell \ll n^3/m$. Using the same techniques, we also obtain an upper bound on the size of each share.

Corollary 6.2. *Let $G = (V, E)$ and $G' = (V, E')$ be two graphs with $E' \subset E$, $|E \setminus E'| = \ell$, and $|V| = n$. Assume G can be realized by a scheme in which the size of each share is at most q. If $\ell > q$, then G' can be realized by a scheme in which the size of each share is $O(\sqrt{\ell q}\ln(n))$ and the total share size is $O(\sqrt{\ell q}\, n \ln(n))$.*

Proof. The scheme for G' can be constructed by following the steps of the proof of Theorem 6.1, taking $d = \sqrt{\ell/q}$. In the first step, we remove vertices of degree greater than d. Thus, there are at most $\ell/d = \sqrt{\ell q}$ removed vertices. For each removed vertex, each vertex in the graph gets at most one element. All together, the size of each share is $O(\ell/d) + O(qd\ln(n)) = O(\sqrt{\ell q}\ln(n))$. □

6.2. *Construction for General Access Structures*

In the previous sections, we studied access structures in which the minimal subsets are of the same size. In this section, we use some of these techniques to study a more general scenario: We start with an access structure, and we delete some minimal authorized subsets of it. The question is how much the share size of the schemes realizing the access structure grows as a result of the removed subsets.

Example 6.3. Let Γ be an access structure on P, and let $A \in \min\Gamma$ with $|A| = k$. Let Γ' be the access structure on P with $\min\Gamma' = \min\Gamma \setminus \{A\}$. Given a secret-sharing scheme Σ realizing Γ with total share size m, we can construct a secret-sharing scheme for Γ' with total share size km.

For every $p \in A$, we generate the shares of the secret according to Σ, and each participant in $P \setminus \{p\}$ receives his share. Observe that a subset can recover the secret if it contains a subset $B \in \min\Gamma$ with $p \notin B$. Therefore, the authorized subsets of the resulting scheme are those containing a subset in $\min\Gamma \setminus \{A\}$.

We next consider removing authorized sets from general homogenous access structures. We say that access structure Γ is of *degree d* if for every $p \in P$ there are at most d subsets in $\min\Gamma$ containing p. We will remove authorized sets described by an access structure with a small degree.

Theorem 6.4. *Let Γ_1 and Γ_2 be two access structures on P with $\min\Gamma_2 \subset \min\Gamma_1$ satisfying that $|A| \leq k$ for every $A \in \min\Gamma_1$. Suppose that there exists a scheme realizing Γ_1 in which the size of each share is at most q and the total share size is m. If Γ_2 is of degree d, then the access structure determined by $\min\Gamma_1 \setminus \min\Gamma_2$ can be realized by a* *secret-sharing scheme in which the size of each share is* $O(\lambda q \ln(n))$ *and the total share size is* $\tilde{O}(\lambda m)$, *where* $\lambda = 2^k k^k d^{k-1}$.

Proof. Let $H = (P, E)$ and $H' = (P, E')$ be the hypergraphs defined by $\min \Gamma_1$ and $\min \Gamma_2$, respectively. By the hypothesis, the hyperedges of H are of size smaller or equal than k, and H' is a sub-hypergraph of H of degree less or equal to d. Let Σ be the scheme realizing H, and let $H'' = (P, E'')$ be the hypergraph with $E'' = E \setminus E'$, which is the hypergraph associated with $\min \Gamma_1 \setminus \min \Gamma_2$. We construct a secret-sharing scheme realizing H''.

Define $r = \lambda \ln(n)$. Following the arguments in the proof of Lemma 5.4, it is clear that there exists a family of r weak colorings $\mu_1, \ldots, \mu_r$ of H' with $2kd$ colors satisfying the following property: For every $e \in E''$, there exists $i \in \{1, \ldots, r\}$ with $\mu_i(u) = \mu_i(v)$ for every $u, v \in e$.

At this point, we can describe H'' as follows: A set $e \subseteq V$ is in E'' if and only if $e \in E$, and there exists a coloring μ_i for which e is monochromatic. Hence, we can construct a secret-sharing scheme for H'' by sharing the secret independently, for every coloring μ_i and for every color $j \in \{1, \ldots, 2kd\}$, with Σ restricted to $V_{i,j} = \{u \in P : \mu_i(u) = j\}$. Then, the size of each share is at most rq and the total share size is $rm = \tilde{O}(\lambda m)$. □

Observe that if $k \ll n$, the removal of minimal authorized subsets from an access structure does not increase so much the share size. Therefore, for $k \ll n$, access structures close to an access structure realized by an efficient scheme are not "hard." In particular, if Γ_1 admits a linear secret-sharing scheme with $m = n^{O(\ln(n))}$, $k = O(\ln(n))$, and $d = O(\ln(n))$, then $\min \Gamma_1 \setminus \min \Gamma_2$ can be realized by a secret-sharing scheme in which the total share size is $n^{O(\ln(n))}$.

7. Lower Bounds for Very Dense Graphs

In this section, we show lower bounds on the total share size for realizing very dense graphs. Recall that the best lower bound on the total share size for realizing a graph is $\Omega(n \log(n))$ [12,24,29] and the best lower bound on the total share size for realizing a graph by a linear scheme is $\Omega(n^{3/2})$ [6]. However, these lower bounds use sparse graphs with $\Theta(n \log(n))$ and $\Omega(n^{3/2})$ edges, respectively. In this section, we will show how to use these sparse graphs to prove lower bounds for very dense graphs. In particular, we show that there exists a graph with $n^{1+\beta}$ excluded edges such that in every linear secret-sharing scheme realizing it, the total share size is $\Omega(n^{1+\beta/2})$ (for every $0 \leq \beta < 1$). This lower bound shows that the total share size grows as a function of β. However, there is still a gap between our upper and lower bounds.

We start with a lower bound for graphs with less than n excluded edges.

Theorem 7.1. *For every* n *and every* $2 < \ell < n/2$, *there exists a graph with* n *vertices and* ℓ *excluded edges such that the total share size of every secret-sharing scheme realizing it is at least* $n + \ell$.

Proof. We construct a graph $G = (V, E)$ with $n \geq 2\ell + 1$ vertices. We denote the vertices of the graph by $V = \{a, b_0, \ldots, b_{\ell-1}, c_0, \ldots, c_{\ell-1}, v_{2\ell+2}, \ldots, v_n\}$. The graph G has all edges except for the following ℓ excluded edges: $\overline{E} = \{(a, c_i) : 0 \leq i \leq \ell - 1\}$.

For every $0 \leq i \leq \ell - 1$, consider the graph G restricted to the vertices $a, b_i, c_i, c_{(i+1)\bmod \ell}$. This graph has two excluded edges (a, c_i) and $(a, c_{(i+1)\bmod \ell})$. Blundo et al. [13] proved that in any secret-sharing scheme realizing this graph, the sum of the sizes of the shares of b_i and c_i is at least 3 times the size of the secret. Thus, in any secret-sharing scheme realizing G, the sum of the sizes of the shares of b_i and c_i is at least 3 times the size of the secret. By [39], the size of the share of each party in any secret-sharing realizing any graph with no isolated vertices is at least the size of the secret. Thus, the total share size in any secret-sharing scheme realizing G is at least $n + \ell$. □

Theorem 7.2. *For every β, where $0 \leq \beta < 1$, there exists a graph with n vertices and less than $n^{1+\beta}$ excluded edges, such that the total share size in any* linear *secret-sharing scheme realizing it is $\Omega(n^{1+\beta/2})$.*

Proof. By [6], for every n there exists a graph with n vertices such that the total share size in any linear secret-sharing scheme realizing it is $\Omega(n^{3/2})$. We use this graph to construct a dense graph $G = (V, E)$ with n vertices. We partition the vertices of G into $n^{1-\beta}$ disjoint sets of vertices $V_1, \ldots, V_{n^{1-\beta}}$, where $|V_i| = n^\beta$ for $1 \leq i \leq n^{1-\beta}$. We construct the edges as follows: First, for every 2 vertices u and v such that $u \in V_i$ and $v \in V_j$ for $i \neq j$, we add the edge (u, v) to E, i.e., there is an edge connecting every 2 vertices from different parts. Second, for every i (where $1 \leq i \leq n^{1-\beta}$), we construct a copy of the graph from [6] with n^β vertices among the vertices of V_i. We denote this graph by G_i.

Since all excluded edges in the above construction are between vertices in the same part, the number of excluded edges is at most $\binom{n^\beta}{2} n^{1-\beta} < n^{1+\beta}$. The total share size of any linear secret-sharing scheme realizing G_i (for $1 \leq i \leq n^{1-\beta}$) is $\Omega((n^\beta)^{3/2}) = \Omega(n^{3\beta/2})$. Thus, the total share size of any linear secret-sharing scheme realizing G is at least $\Omega(n^{1-\beta} n^{3\beta/2}) = \Omega(n^{1+\beta/2})$. □

Theorem 7.3. *For every β, where $0 < \beta < 1$, there exists a graph with n vertices and less than $n^{1+\beta}$ excluded edges such that the share size of any secret-sharing scheme realizing it is $\Omega(\beta n \log(n))$.*

Proof. We use the construction from the proof of Theorem 7.2, where for every $1 \leq i \leq n^{1-\beta}$ we set G_i to be a $\log(n^\beta)$-dimensional cube. By [24], any secret-sharing scheme realizing G_i has a total share size of $\Omega(\beta n^\beta \log(n))$. Thus, any secret-sharing scheme realizing G must have a total share size of $\Omega((n^{1-\beta}) \cdot \beta n^\beta \log(n))) = \Omega(\beta n \log(n))$. □

Acknowledgements

We thank Noga Alon and Stasys Jukna for discussions on equivalence covering, and Ilan Orlov for useful discussions and suggestions. We also thank the anonymous reviewers for their detailed suggestions for improving the paper.

References

[1] N. Alon. Covering graphs by the minimum number of equivalence relations. *Combinatorica*, 6(3):201–206, 1986.

[2] N. Alon and J. H. Spencer. *The Probabilistic Method*. John Wiley & Sons, 3rd edition, 2008.

[3] L. Babai, A. Gál, and A. Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19(3):301–319, 1999.

[4] A. Beimel. Secret-sharing schemes: A survey. In *IWCC 2011*, volume 6639 of *Lecture Notes in Computer Science*, pages 11–46, 2011.

[5] A. Beimel and B. Chor. Universally ideal secret sharing schemes. *IEEE Trans. on Information Theory*, 40(3):786–794, 1994.

[6] A. Beimel, A. Gál, and M. Paterson. Lower bounds for monotone span programs. *Computational Complexity*, 6(1):29–45, 1997. Conference version: FOCS '95.

[7] A. Beimel, Y. Ishai, R. Kumaresan, and E. Kushilevitz. On the cryptographic complexity of the worst functions. In Y. Lindell, editor, *Proc. of the Eleventh Theory of Cryptography Conference– TCC 2014*, volume 8349 of *Lecture Notes in Computer Science*, pages 317–342. Springer-Verlag, 2014.

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

[9] 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.

[10] 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.

[11] G. R. Blakley and C. Meadows. The security of ramp schemes. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology – CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 242–268. Springer-Verlag, 1985.

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

[13] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro. On the information rate of secret sharing schemes. *Theoretical Computer Science*, 154(2):283–306, 1996.

[14] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decomposition and secret sharing schemes. *J. of Cryptology*, 8(1):39–64, 1995.

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

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

[17] S. Bublitz. Decomposition of graphs and monotone formula size of homogeneous functions. *Acta Informatica*, 23:689–696, 1986.

[18] 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.

[19] 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.

[20] B. Chor and E. Kushilevitz. Secret sharing over infinite domains. *J. of Cryptology*, 6(2):87–96, 1993.

[21] 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.

[22] G. Di Crescenzo and C. Galdi. Hypergraph decomposition and secret sharing. *Discrete Applied Mathematics*, 157(5):928–946, 2009.

[23] L. Csirmaz. The size of a share must be large. *J. of Cryptology*, 10(4):223–231, 1997.

[24] L. Csirmaz. Secret sharing schemes on graphs. Technical Report 2005/059, Cryptology ePrint Archive, 2005. eprint.iacr.org/.

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

[26] L. Csirmaz, P. Ligeti, and G. Tardos. Erdös-pyber theorem for hypergraphs and secret sharing. *Graphs and Combinatorics*, 2014.

[27] L. Csirmaz and G. Tardos. Secret sharing on trees: problem solved. *IACR Cryptology ePrint Archive*, 2009:71, 2009.

[28] 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.

[29] M. van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography*, 6:143–169, 1995.

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

[31] O. Farràs, J. Martí-Farré, and C. Padró. Ideal multipartite secret sharing schemes. *J. of Cryptology*, 25(1):434–463, 2012.

[32] A. Gál. A characterization of span program size and improved lower bounds for monotone span programs. In *Proc. of the 30th ACM Symp. on the Theory of Computing*, pages 429–437, 1998.

[33] A. Gál and P. Pudlák. A note on monotone complexity and the rank of matrices. *Inform. Process. Lett.*, 87:321–326, 2003.

[34] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proc. of the 13th ACM Conference on Computer and Communications Security*, pages 89–98, 2006.

[35] 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.

[36] M. Jerrum. A very simple algorithm for estimating the number of k-colorings of a low-degree graph. *Random Structures & Algorithms*, 7:157–166, 1995.

[37] S. Jukna. On set intersection representations of graphs. *Journal of Graph Theory*, 61:55–75, 2009.

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

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

[40] J. Kilian and N. Nisan. Private communication, 1990.

[41] J. Martí-Farré and C. Padró. Secret sharing schemes on sparse homogeneous access structures with rank three. *Electr. J. Comb.*, 11(1), 2004.

[42] J. Martí-Farré and C. Padró. Secret sharing schemes with three or four minimal qualified subsets. *Designs, Codes and Cryptography*, 34(1):17–34, 2005.

[43] J. Martí-Farré and C. Padró. On secret sharing schemes, matroids and polymatroids. *Journal of Mathematical Cryptology*, 4(2):95–120, 2010.

[44] Y. Mintz. Information ratios of graph secret-sharing schemes. Master's thesis, Dept. of Computer Science, Ben Gurion University, 2012.

[45] M. Mitzenmacher and E. Upfal. *Probability and Computing*. Cambridge University Press, 2005.

[46] M. Naor and A. Wool. Access control and signatures via quorum secret sharing. In *3rd ACM Conf. on Computer and Communications Security*, pages 157–167, 1996.

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

[48] C. Padró and G. Sáez. Lower bounds on the information rate of secret sharing schemes with homogeneous access structure. *Inf. Process. Lett.*, 83(6):345–351, 2002.

[49] J. Salas and A. D. Sokal. Absence of phase transition for antiferromagnetic Potts models via the Dobrushin uniqueness theorem. *J. Statist. Phys.*, 86:551–579, 1997.

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

[51] B. Shankar, K. Srinathan, and C. Pandu Rangan. Alternative protocols for generalized oblivious transfer. In *Proceedings of the 9th International Conference on Distributed Computing and Networking (ICDCN'08)*, volume 4904 of *Lecture Notes in Computer Science*, pages 304–309. Springer-Verlag, 2008.

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

[53] 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.

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

[55] H. Sun and S. Shieh. Secret sharing in graph-based prohibited structures. In *INFOCOM '97*, pages 718–724, 1997.

[56] H.-M. Sun, H. Wang, B.-H. Ku, and J. Pieprzyk. Decomposition construction for secret sharing schemes with graph access structures in polynomial time. *SIAM J. Discret. Math.*, 24:617–638, 2010.

[57] T. Tassa. Generalized oblivious transfer by secret sharing. *Des. Codes Cryptography*, 58(1):11–21, 2011.

[58] B. Waters. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In *Proc. of the 14th International Conference on Practice and Theory in Public Key Cryptography*, volume 6571 of *Lecture Notes in Computer Science*, pages 53–70. Springer-Verlag, 2011.

[59] I. Wegener. *The Complexity of Boolean Functions*. Wiley-Teubner, 1987.