SIAM J. DISCRETE MATH.
Vol. 24, No. 2, pp. 617–638

DECOMPOSITION CONSTRUCTION FOR SECRET SHARING SCHEMES WITH GRAPH ACCESS STRUCTURES IN POLYNOMIAL TIME*

HUNG-MIN SUN†, HUAXIONG WANG‡, BYING-HE KU†, AND JOSEF PIEPRZYK§

Abstract. The purpose of this paper is to describe a new decomposition construction for perfect secret sharing schemes with graph access structures. The previous decomposition construction proposed by Stinson is a recursive method that uses small secret sharing schemes as building blocks in the construction of larger schemes. When the Stinson method is applied to the graph access structures, the number of such "small" schemes is typically exponential in the number of the participants, resulting in an exponential algorithm. Our method has the same flavor as the Stinson decomposition construction; however, the linear programming problem involved in the construction is formulated in such a way that the number of "small" schemes is polynomial in the size of the participants, which in turn gives rise to a polynomial time construction. We also show that if we apply the Stinson construction to the "small" schemes arising from our new construction, both have the same information rate.

Key words. secret sharing scheme, graph access structure, linear programming, information rate

AMS subject classifications. 94A60, 94A62, 90C05, 54C70, 05C20

DOI. 10.1137/080733802

1. Introduction.

A secret sharing scheme is a method of protecting a *secret* among a group of *participants* in such a way that only certain specified subsets of the participants (those belonging to an *access structure*) can reconstruct the secret. A secret sharing scheme is perfect if unqualified subsets of participants (those not in the access structure) obtain no information about the secret in the information theoretic sense [3, 11, 22]. A secret sharing scheme is usually initialized by a trusted *dealer* who securely transfers a piece of information relating to the secret, called a *share*, to each participant in the scheme. Secret sharing schemes have become an indispensable basic cryptographic tool in any security environment where active entities are groups rather than individuals.

The first secret sharing schemes proposed by Shamir [22] and Blakley [4] in 1979 were (t, w)-*threshold schemes*, where the access structure consists of all subsets of at least t (out of a total number of w) participants. Since then, many approaches to the construction of threshold schemes have been proposed (see, for example, [19, 32, 3, 16, 23]). Threshold schemes are a special class of secret sharing schemes.

*Received by the editors August 29, 2008; accepted for publication (in revised form) March 23, 2010; published electronically June 18, 2010.

http://www.siam.org/journals/sidma/24-2/73380.html

†Department of Computer Science, National Tsing Hua University, Hsinchu 30013, Taiwan (hmsun@cs.nthu.edu.tw, alley@is.cs.nthu.edu.tw). The work of the first and third authors was supported in part by the National Science Council, Taiwan, under contracts NSC 97-2221-E-007-055-MY3 and NSC 96-2628-E-007-025-MY3.

‡Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore (hxwang@ntu.edu.sg) and Department of Computing, Macquarie University NSW 2109, Australia. This author's work was supported by the Singapore National Research Foundation under research grant NRF-CRP2-2007-03 and the Australian Research Council under ARC Discovery Project DP0665035.

§Department of Computing, Macquarie University NSW 2109, Australia (josef@ics.mq.edu.au). This author's work was supported by ARC grant DP0987734.

Ito, Saito, and Nishizeki generalized the concept of threshold schemes and proposed a method of realizing secret sharing schemes for any monotone access structure [11, 12]. Later, Benaloh and Leichter [2] gave a simpler and more efficient algorithm, using a monotone formula that implements secret sharing for any monotone access structure. The theory of secret sharing schemes has received considerable attention in the literature in recent years.

In a perfect secret sharing scheme, the size of each share is at least as large as the size of the secret. A secret sharing scheme is called *ideal* if the size of each share is the same as the size of the secret. For example, the Shamir (t, w)-threshold scheme is an ideal secret sharing scheme. It is well known, however, that there are access structures that cannot be realized by *ideal* secret sharing schemes. Many works have been devoted to studying the relation between an access structure and the secret sharing scheme that can efficiently realize it (see, for example, [1, 9, 20]). As there is no general method for efficient implementation of secret sharing for an arbitrary access structure, various approaches have been developed. They typically target a specific class of access structures. For example, the class for four participants is considered in [13], the class for five participants is studied in [24], and the class of access structures defined by minimal sets with three or four participants is examined in [18]. From a practical point of view, access structures over minimal sets with two participants are of special interest. These access structures are investigated using a graph theory approach. In this approach, vertices indicate participants, and edges determine pairs of participants from the access structure. A graph that represents the access structure is referred to as a *graph access structure*. Graphical structures are interesting because an access structure with minimal qualified subset of size two can be naturally represented by graphs. Secret sharing schemes that realize graph access structures have been studied by many researchers (for example, [6, 9, 11, 17, 10]). Brickell and Davenport showed in [7] that there exists an ideal perfect secret sharing scheme for the graph access structure G if and only if G is a complete multipartite graph.

In [25], Stinson proposed a method of λ-decomposition constructions for general secret sharing schemes. The λ-decomposition construction is a recursive method that uses small schemes as building blocks in order to construct larger schemes. The main idea of λ-decomposition of a graph access structure Γ is to find a collection of subgraphs of Γ such that every edge of Γ must appear in at least λ subgraphs. However, when this method is applied, the number of the "small" schemes (subgraphs) is typically exponential in the number of participants (vertices), resulting in an exponential time construction. Stinson also applied this method to show that for any graph G with w vertices and the maximum degree d, there exists a perfect secret sharing scheme for the graph access structure based on G such that the information rate is at least $2/(d+1)$. Blundo et al. [5] proved that this lower bound is tight. Since then, there have been many generalizations of λ-decomposition construction. Sun and Shieh [27] proposed recursive constructions for perfect secret sharing schemes with access structures of a constant rank, where the rank of an access structure Γ is the maximum cardinality of a minimal qualified subset. They gave lower bounds on the information rate $6/((w-1)^2+2)$ for rank 3 on w ($w \geq 5$) participants and the information rate $m!(w-m+1)!/w!$ for rank m on w participants. Padro and Saez [21] provided two new lower bounds on the optimal information rate, using constructions of secret sharing schemes with homogeneous access structures. They introduced a new parameter, the k-degree of a participant, the number of different k-subsets that are contained in a minimal qualified subset together with the participant. Csirmaz and Ligeti [10] studied the decomposition into stars and showed that the information rate is equal to

$2 - \frac{1}{d}$ for graphs with maximum degree d that satisfy the following three conditions: (1) every vertex has at most one neighbor of degree 1, (2) vertices of degree at least 3 are not connected by an edge, and (3) the girth of the graph is at least 6.

Now we describe the works that are related to the generalizations of λ-decomposition constructions. Van Dijk, Jackson, and Martin [30] introduced a (λ, γ)-*decomposition* of access structure (Γ, Δ), where Γ is the collection of all *qualified* groups (sets of participants in Γ that can reconstruct the secret) and Δ is a collection of all *forbidden* groups (sets of participants in Δ that must not obtain any new information about the secret). For a (λ, γ)-decomposition, the following two conditions hold: (1) if $A \in \Gamma$, then $A \in \Gamma^i$ for at least λ distinct values of i, and (2) if $A \in \Delta$, then $A \notin \Delta^i$ for at most γ distinct values of i. The implementation of (λ, γ)-decomposition was demonstrated on three connected graphs [31]. Sun and Chen [26] proposed *weighted decomposition constructions* for secret sharing schemes with general access structures. The construction allows $W(\Gamma_w)$ secrets of the same size to be shared among a set of participants $\mathcal{P}$ in such a way that each subset of participants, X, can exactly recover $W(X)$ secrets out of the $W(\Gamma_w)$ secrets. They improved the information rates in some cases; however, the case of connected graphs with six vertices was left unsolved. Note that the realization of both (λ, γ)-decomposition and weighted decomposition constructions needs exponential complexity to find suitable subgraphs for a given graph.

In this paper, we propose an algorithm, called *StarDC*, for λ-decomposition. As mentioned above, the enumeration of all the subgraphs in the Stinson decomposition construction has exponential complexity in the number of vertices for a given graph access structure. Another difficulty is that identifying ideal schemes is equivalent to finding the complete multipartite subgraphs for a given graph, which is a well-known NP-complete problem. For this reason, we consider the decomposition into stars (a special subclass of complete multipartite subgraphs of type $K_{1,n}$). Unfortunately, the enumeration of all star subgraphs is also exponential in the number of vertices. The contribution of this paper is that our proposed algorithm, StarDC, can find the best star λ-decomposition for a given graph in polynomial time, even though the number of the small subgraphs is exponential in the number of vertices. The new method has the same flavor as the Stinson decomposition construction, but the underlying linear programming problem is modified in such a way that the number of "small" schemes is polynomial in the number of participants. This gives rise to a construction with polynomial complexity. More precisely, the running time of the new construction reduces from exponential complexity of the Stinson method to polynomial complexity $O(|V|^6 L)$, where $G = (V, E)$ is the underlying graph of the access structure. Referring to [15], L is defined as the number of bits needed to encode the linear programming problem. We also show that if we apply both the Stinson construction and our new construction to the same "small" schemes, then both achieve the same information rate and the same average information rate.

The paper is organized as follows. In section 2, we briefly describe the concepts of information rates and graph-based decomposition constructions. We then give the new proposed method in section 3. In section 4, we give some examples to illustrate the performance and to compare them with the previous constructions. In section 5, we analyze the correctness and efficiency of the proposed algorithm. Finally, we conclude the paper in section 6.

2. Preliminaries.

2.1. Information rates. A secret sharing scheme is a method for distributing a secret K among a set of participants $\mathcal{P} = \{P_1, P_2, \ldots, P_w\}$, where K is the finite

set of secrets. Denote by S_i the finite set of the shares allocated to participant P_i, $1 \leq i \leq w$. The secret sharing scheme assures that only the qualified subsets of $\mathcal{P}$ can reconstruct the value of K from their shares (S_i's). Since the security level of the system is determined mainly by the amount of information that must be kept secret (or the length of the secret), the size of the share (S_i) given to participant (P_i) is a key concern in the design of secret sharing schemes. Therefore, the efficiency of a secret sharing scheme is often measured by the information rate. For a given secret sharing scheme defined by an access structure Γ, the information rate of participant P_i is defined by

$$\rho_i = \frac{\log_2 |K|}{\log_2 |S_i|}. \tag{2.1}$$

The information rate of the corresponding secret sharing scheme is then defined as

$$\rho = \min\{\rho_i : 1 \leq i \leq w\}. \tag{2.2}$$

We also consider the average information rate $\widetilde{\rho}$ measured for all participants and expressed by the following relation:

$$\widetilde{\rho} = \frac{w}{\sum_{i=1}^{w}(\frac{1}{\rho_i})} = \frac{w \log_2 |K|}{\sum_{i=1}^{w} \log_2 |S_i|}. \tag{2.3}$$

For an access structure Γ, we denote ρ_Γ^* and $\widetilde{\rho}_\Gamma^*$ (or simply ρ^* and $\widetilde{\rho}^*$) to be the infimum information rate and average information rate of a perfect secret sharing scheme with the access structure Γ. $PS(\Gamma, \rho, q)$ denotes a perfect secret sharing scheme with access structure Γ and information rate ρ for a set of q keys. A secret sharing scheme is ideal if $\rho^* = \widetilde{\rho}^* = 1$. Moreover, an access structure Γ is said to be ideal if there exists an ideal scheme for Γ.

2.2. Graph-based decomposition. Let G be a graph. We denote the vertex set of G by $V(G)$ and the edge set by $E(G)$. In graph G, two vertices u and v are called *connected* if G contains a path from u to v. G is called connected if every pair of distinct vertices in G is connected. In a graph access structure, participants correspond to vertices, and pairs of participants correspond to edges. We denote the resulting access structure for the graph G by Γ_G.

A complete multipartite graph $K_{w_1,w_2,\ldots,w_s}$ is a graph with $\sum_{i=1}^{s} w_i$ vertices, where w_i is the number of vertices in the ith subset. Given two vertices u and v, $u\bar{v}$ is an edge if and only if the vertices are in different subsets of the partition. An alternative way to characterize a complete multipartite graph is to say that the complementary graph is a vertex-disjoint union of cliques. The following result characterizes ideal graph access structures, and its proof can be found in [7].

THEOREM 2.1. *Let G be a graph and Γ_G the corresponding graph access structure. Then Γ_G is an ideal access structure if and only if G is a complete multipartite graph.*

We say that $\pi = \{G_1, \ldots, G_n\}$ is a complete multipartite covering (CMC) of G if $G_1, \ldots, G_n$ are complete multipartite subgraphs of G and $E(G) = \cup_1^n E(G_i)$. We consider the access structure Γ_G. From Theorem 2.1, we know there is an ideal scheme for each Γ_{G_i}. We then independently construct n secret sharing schemes for the same secret key, each with access structure Γ_{G_i}, which results in a secret sharing scheme for the general access structure Γ_G. Such a construction, called the CMC construction, was proposed by Brickell and Stinson [8]. Blundo et al. [6] proposed

the multiple CMC construction in which several CMCs are used in order to have a better information rate than a single CMC. Stinson [25] proposed a new and powerful construction, called the decomposition construction, which is a generalization of the multiple CMC construction. Next we describe Stinson's decomposition construction.

Suppose Γ is an access structure with the basis Γ_0, where Γ_0 is the set of minimal authorized subsets of Γ. Let $\lambda \geq 1$ be an integer. A λ-decomposition of Γ_0 consists of a collection $\{\Gamma_1, \ldots, \Gamma_n\}$ such that the following conditions are satisfied.

1. $\Gamma_h \subseteq \Gamma_0$ for $1 \leq h \leq n$.
2. For each $B \in \Gamma_0$, there exist at least λ indices $i_1 < \cdots < i_\lambda$ such that $B \in \Gamma_{i_j}$ for $1 \leq j \leq \lambda$.

Several examples of the λ-decomposition method are given in [25] to show that the method outperforms other previously known constructions.

2.3. The Stinson method. Given an access structure Γ, the first step of the Stinson method is to produce a list of m "small" (ideal or with a high information rate) schemes, denoted as $PS(\Gamma_h, \rho, q)$, where $\Gamma_h \subseteq \Gamma$, $1 \leq h \leq m$. The goal of the Stinson method is to determine a nonnegative integral combination $(\breve{\alpha}_h)$ of the schemes $PS(\Gamma_h, \rho, q)$ such that the overall information rate (or average information rate) is maximized subject to the λ-decomposition constraints; i.e., for each element (edge) in Γ_0, the total number of copies in the decomposition must be at least λ.

Note that in the Stinson method "optimal" means that the information rate for a given decomposition is maximized with a suitable choice of small schemes. Thus, different choices of small schemes will give different solutions. From graph theory, we know that the enumeration of all possible small schemes is exponential. This is also true even if we consider the small schemes with the star topology only. Therefore, it is difficult to find the global optimal solution efficiently using the Stinson method.

In the following, we describe the Stinson method in more detail. We also give an illustrative example of the Stinson method in Example 4.1.

2.3.1. Information rates for the Stinson method. For $1 \leq h \leq m$, let ρ_{ih} denote the information rate for the participant P_i in the perfect secret sharing scheme $PS(\Gamma_h, \rho, q)$, where $P_i \in \mathcal{P}_h$ and $\mathcal{P}_h$ is the set of participants for the access structure Γ_h.

Let $\Gamma_0 = \{B_1, \ldots, B_k\}$. For $1 \leq i \leq w$, $1 \leq h \leq m$, define

$$c_{ih} = \begin{cases} 1/\rho_{ih} & \text{if } P_i \in \mathcal{P}_h, \\ 0 & \text{otherwise.} \end{cases} \tag{2.4}$$

To simplify the formulation of the linear programming problem, we assume that $PS(\Gamma_h, \rho, q)$ is an ideal scheme and that $\rho_{ih} = 1$.

For $1 \leq j \leq k$ and $1 \leq h \leq m$, we define

$$b_{jh} = \begin{cases} 1 & \text{if } B_j \in \Gamma_h, \\ 0 & \text{otherwise.} \end{cases} \tag{2.5}$$

Given the access structure Γ_G represented by a graph, a λ-decomposition of Γ_G induces a set of graph access structures $\Gamma_{G_1}, \Gamma_{G_2}, \ldots, \Gamma_{G_m}$ represented by the corresponding graphs $G_1, G_2, \ldots, G_m$, respectively. The matrix $\boldsymbol{B} = (b_{ih})_{k \times m}$ is then determined by the edges of the graphs G_i, while the matrix $\boldsymbol{C} = (c_{ih})_{w \times m}$ is determined by the vertices of the graphs G_i. Suppose the decomposition is constructed

with $\check{\alpha}_h$ copies of Γ_h, where each $\check{\alpha}_h$ is a nonnegative integer. Let

$$\lambda = \min_j \left\{ \sum_{h=1}^{m} b_{jh}\check{\alpha}_h \right\}. \tag{2.6}$$

Then, from the Stinson decomposition method, we have

$$\sum_{h=1}^{m} b_{jh}\check{\alpha}_h \geq \lambda, \quad 1 \leq j \leq k, \tag{2.7}$$

and the total number of shares (for λ copies of the same secret) distributed to every participant P_i is

$$S_i = \sum_{h=1}^{m} c_{ih}\check{\alpha}_h, \quad 1 \leq i \leq w. \tag{2.8}$$

Let $S = \max\{S_i\}$. Then

$$S \geq \sum_{h=1}^{m} c_{ih}\check{\alpha}_h, \quad 1 \leq i \leq w. \tag{2.9}$$

The optimization problem is defined as follows: find the optimal linear combination of the Γ_h's that maximizes the information rate $R = \lambda/S$. More precisely,

$$\begin{array}{lll} \text{maximize } \lambda/S & & \\ \text{subject to} & \check{\alpha}_h \geq 0, & 1 \leq h \leq m, \\ & \displaystyle\sum_{h=1}^{m} b_{jh}\check{\alpha}_h \geq \lambda, & 1 \leq j \leq k, \\ & \displaystyle\sum_{h=1}^{m} c_{ih}\check{\alpha}_h \leq S, & 1 \leq i \leq w. \end{array} \tag{2.10}$$

Let $\alpha_h = \check{\alpha}_h/S$. Then (2.10) can be transformed to the following linear programming problem:

$$\begin{array}{lll} \text{maximize } R & & \\ \text{subject to} & \alpha_h \geq 0, & 1 \leq h \leq m, \\ & \displaystyle\sum_{h=1}^{m} b_{jh}\alpha_h \geq R, & 1 \leq j \leq k, \\ & \displaystyle\sum_{h=1}^{m} c_{ih}\alpha_h \leq 1, & 1 \leq i \leq w. \end{array} \tag{2.11}$$

Note that the α_h's are nonnegative rational numbers.

2.3.2. Average information rates from the Stinson method. We consider the case of the average information rate. Let $\tilde{S} = \sum_{i=1}^{w} S_i/w$. Denote

$$d_h = \frac{|\mathcal{P}_h|}{\tilde{\rho_h}}, \tag{2.12}$$

where $\tilde{\rho_h}$ is the average information rate of the scheme $PS(\Gamma_h, \rho, q)$. Then the total number of shares (for λ copies of the secret) distributed to the participants is

$$\sum_{h=1}^{m} d_h \check{\alpha}_h = w \cdot \tilde{S}. \tag{2.13}$$

Let

$$\tilde{R} = \frac{\lambda}{w \cdot \tilde{S}}. \tag{2.14}$$

The optimization problem can be stated as follows: find the optimal linear combination of Γ_h's that maximizes the average information rate

$$\tilde{R} \cdot w = \frac{\lambda}{w \cdot \tilde{S}} \cdot w = \frac{\lambda}{\sum_{i=1}^{w} S_i} \cdot w. \tag{2.15}$$

That is,

$$\begin{array}{lll} \text{maximize } \lambda/\tilde{S} & & \\ \text{subject to} & \check{\alpha}_h \geq 0, & 1 \leq h \leq m, \\ & \displaystyle\sum_{h=1}^{m} b_{jh} \check{\alpha}_h \geq \lambda, & 1 \leq j \leq k, \\ & \displaystyle\sum_{h=1}^{m} d_h \check{\alpha}_h = w \cdot \tilde{S}. & \end{array} \tag{2.16}$$

Let $\alpha_h = \check{\alpha}_h/(w \cdot \tilde{S})$. Then (2.16) can be translated to the following linear programming problem:

$$\begin{array}{lll} \text{maximize } \tilde{R} \cdot w & & \\ \text{subject to} & \alpha_h \geq 0, & 1 \leq h \leq m, \\ & \displaystyle\sum_{h=1}^{m} b_{jh} \alpha_h \geq \tilde{R}, & 1 \leq j \leq k, \\ & \displaystyle\sum_{h=1}^{m} d_h \alpha_h = 1. & \end{array} \tag{2.17}$$

Note that the description of the average information rate from the Stinson method is slightly different from that in [25]. In fact, the strict equality constraint, $\sum d_h \alpha_h = 1$, can be replaced by two simultaneous inequalities of form $\geq$ and $\leq$ with the same right-hand side value. That is, $\sum d_h \alpha_h \geq 1$ and $\sum d_h \alpha_h \leq 1$. Furthermore, constraint $\sum d_h \alpha_h \geq 1$ can be removed because the optimal solutions under the reduced constraints always make $\sum d_h \alpha_h = 1$. The resulting linear programming problem is then exactly the same as that in [25].

3. Proposed graph decomposition construction. The Stinson method for decomposition construction is a recursive construction that uses "small" schemes as building blocks in the construction of larger schemes by solving corresponding linear programming problems. However, the enumeration of all the small schemes has an exponential complexity in the number of participants. In the worst case, all the possible schemes have to be considered. Another difficulty is to efficiently find all

the ideal schemes for a given graph, which is equivalent to the problem of finding the complete multipartite subgraphs for a given graph. This is a well-known NP-complete problem. For this reason, we consider a special subclass of complete multipartite subgraphs of type $K_{1,n}$, which is an ideal graph access structure. We will call the schemes from these subgraphs the star schemes.

DEFINITION 3.1. *A* star scheme *is a secret sharing scheme with a graph access structure from a complete bipartite graph $K_{1,n}$, where the center contains a single vertex.*

Note that for a star scheme with a single edge, i.e., $K_{1,1}$, we randomly select one vertex as its center. Note also that the number of star schemes in a given graph $G = (V, E)$ is $O(2^{|V|})$. Thus, if we consider the star schemes in the Stinson method, it is inefficient to enumerate all the schemes.

We propose a new λ-decomposition algorithm, called StarDC, to find the best λ-decomposition among all λ-decompositions that use only star schemes for every given graph. Such decompositions are called *star λ-decompositions*. Even though the number of star subgraphs is exponential in the number of vertices, the algorithm runs in polynomial time. StarDC consists of two stages: *linear programming* and *splitting*.

The idea of StarDC is based on the fact that every star scheme of a graph can be translated into a weight distribution on the directed edges of the graph. Given an access structure G, we use $u\bar{v}$ to denote the edge between u and v, where $u, v \in V(G)$. We associate each undirected $u\bar{v}$ of G with two directed edges $u\vec{v}$ and $v\vec{u}$. We can then obtain a new directed graph $\vec{G}$. The weight distribution on the directed edges of the graph $\vec{G}$ is constructed by assigning two weights, $\check{\alpha}_{u\vec{v}}$ and $\check{\alpha}_{v\vec{u}}$, to every edge $u\bar{v}$ of the graph G (Figure 4.1 illustrates the construction of the directed graph $\vec{G_{13}}$ from the undirected graph G_{13}). After obtaining the best weights of every directed edge of the graph $\vec{G}$, an iterative splitting algorithm is presented to translate the directed graph $\vec{G}$ into star λ-decompositions. In the following, we present our StarDC algorithm in detail.

3.1. Information rates from StarDC.

3.1.1. Linear programming. The linear programming problem is formulated to maximize the information rate of feasible solutions (i.e., the secret sharing schemes that realize the access structure Γ). StarDC constructs a decomposition with $\check{\alpha}_{u\vec{v}}+\check{\alpha}_{v\vec{u}}$ copies for each edge $u\bar{v}$ in G ($\check{\alpha}_{u\vec{v}}$ for $u\vec{v}$ and $\check{\alpha}_{v\vec{u}}$ for $v\vec{u}$), where $\check{\alpha}_{u\vec{v}}$ and $\check{\alpha}_{v\vec{u}}$ are nonnegative integers. Let

$$\lambda = \min_{u\bar{v}}\{\check{\alpha}_{u\vec{v}} + \check{\alpha}_{v\vec{u}}\} \quad \forall u\bar{v} \in E(G). \tag{3.1}$$

Then, for each edge $u\bar{v} \in E(G)$, we have

$$\check{\alpha}_{u\vec{v}} + \check{\alpha}_{v\vec{u}} \geq \lambda. \tag{3.2}$$

Let S_u be the number of shares distributed to participant (vertex) u. We have (see Example 4.2)

$$S_u = \max_{v}\{\check{\alpha}_{u\vec{v}} | u\vec{v} \in E(\vec{G})\} + \sum_{v} \check{\alpha}_{v\vec{u}}. \tag{3.3}$$

Assume $S = \max\{S_u | \forall u \in V(G)\}$. Then

$$S \geq \max_{v}\{\check{\alpha}_{u\vec{v}} | u\vec{v} \in E(\vec{G})\} + \sum_{v} \check{\alpha}_{v\vec{u}} \quad \forall u \in V(G). \tag{3.4}$$

The optimization problem is then formulated in order to maximize the information rate $R = \lambda/S$:

$$
\begin{array}{ll}
\text{maximize } \lambda/S & \\
\text{subject to} & \\
\check{\alpha}_{u\vec{v}} + \check{\alpha}_{v\vec{u}} \geq \lambda & \forall u\bar{v} \in E(G), \\
S \geq \max\limits_{v}\{\check{\alpha}_{u\vec{v}} | u\vec{v} \in E(\vec{G})\} + \sum\limits_{v} \check{\alpha}_{v\vec{u}} & \forall u \in V(G), \\
\check{\alpha}_{u\vec{v}} \geq 0, \quad \check{\alpha}_{v\vec{u}} \geq 0 & \forall u\bar{v} \in E(G).
\end{array} \tag{3.5}
$$

Let $\alpha_{u\vec{v}} = \check{\alpha}_{u\vec{v}}/S$. The linear programming problem (3.5) can be transformed into the following:

$$
\begin{array}{ll}
\text{maximize } R & \\
\text{subject to} & \\
\alpha_{u\vec{v}} + \alpha_{v\vec{u}} \geq R & \forall u\bar{v} \in E(G), \\
\max\limits_{v}\{\alpha_{u\vec{v}} | u\vec{v} \in E(\vec{G})\} + \sum\limits_{v} \alpha_{v\vec{u}} \leq 1 & \forall u \in V(G), \\
\alpha_{u\vec{v}} \geq 0, \quad \alpha_{v\vec{u}} \geq 0 & \forall u\bar{v} \in E(G).
\end{array} \tag{3.6}
$$

Note that the constraint $\max_v \{\alpha_{u\vec{v}} | u\vec{v} \in E(\vec{G})\} + \sum_v \alpha_{v\vec{u}} \leq 1$ can be easily converted to the linear form. For example, a vertex A in an access structure has two adjacent vertices B and C. The constraint

$$\max\{\alpha_{\vec{AB}}, \alpha_{\vec{AC}}\} + \alpha_{\vec{BA}} + \alpha_{\vec{CA}} \leq 1 \tag{3.7}$$

can be transformed to

$$
\begin{array}{l}
\alpha_{\vec{AB}} + \alpha_{\vec{BA}} + \alpha_{\vec{CA}} \leq 1, \\
\alpha_{\vec{AC}} + \alpha_{\vec{BA}} + \alpha_{\vec{CA}} \leq 1.
\end{array} \tag{3.8}
$$

3.1.2. Splitting. Denote by d the least common denominator of all $\alpha_{u\vec{v}}$'s. Let $\beta_{u\vec{v}} = d \cdot \alpha_{u\vec{v}}$ $\forall u\vec{v} \in E(\vec{G})$. That is, $\beta_{u\vec{v}}$ is an integer obtained from $\alpha_{u\vec{v}}$ by multiplying the least common denominator of all $\alpha_{u\vec{v}}$'s. Note that taking a scalar multiple of all the $\alpha_{u\vec{v}}$'s does not affect the value of the resultant information rate R [25]. This can be justified easily as follows. According to (3.1)

$$\lambda^* = \min_{u\bar{v}}\{\beta_{u\vec{v}} + \beta_{v\vec{u}}\} \quad \forall u\bar{v} \in E(G). \tag{3.9}$$

Similarly, from (3.3),

$$S_u^* = \max_{v}\{\beta_{u\vec{v}} | u\vec{v} \in E(\vec{G})\} + \sum_{v} \beta_{v\vec{u}}, \tag{3.10}$$

$$S^* = \max\{S_u^* | \forall u \in V(G)\}. \tag{3.11}$$

It is obvious that $\lambda^* = d \cdot \lambda$ and $S^* = d \cdot S$. Accordingly, the information rate does not change due to $R = \lambda^*/S^* = \lambda/S$. Hence, we can multiply by an appropriate factor so as to make all the $\alpha_{u\vec{v}}$'s integral.

Let $M_u = \{u\vec{v} | v \in V(G) \text{ and } \beta_{u\vec{v}} > 0\}$ be the set of vectors connecting vertices u and v (i.e., the set of all outgoing vectors from vertex u). Let $H_u = \{\beta_{u\vec{v}} | u\vec{v} \in M_u \text{ and } \beta_{u\vec{v}} > 0\}$. Denote by $I(u, H_u, M_u)$ the graph with center u and $\beta_{u\vec{v}}$ copies of vector $u\vec{v}$ $\forall u\vec{v} \in M_u$ (an example is shown in Figure 4.3). In the splitting stage, a set of star schemes $\boldsymbol{Z}[u]$ is iteratively constructed using a greedy method as follows.

Input: $\bigcup_{\forall u \in V(G)} I(u, H_u, M_u)$.
Output: $\boldsymbol{Z} = \bigcup_{\forall u \in V(G)} \boldsymbol{Z}[u]$.

(1) Initially assign $\boldsymbol{Z} = \emptyset$ and $\boldsymbol{Z}[u] = \emptyset$ $\forall u \in V(G)$.
For each $u \in V(G)$, repeat steps (2)–(5) until $H_u = \phi$.

(2) Choose the smallest integer δ_u from H_u, where

$$\delta_u = \min_{\beta_{u\vec{v}} \in H_u} \{\beta_{u\vec{v}}\}. \tag{3.12}$$

(3) Obtain $R(u, \delta_u, M_u)$ from $I(u, H_u, M_u)$, where $R(u, \delta_u, M_u)$ is the graph with center u and δ_u copies of $u\vec{v}$ $\forall u\vec{v} \in M_u$ (an example is shown in Figure 4.4). Add $R(u, \delta_u, M_u)$ to $Z[u]$. That is,

$$\boldsymbol{Z}[u] = \boldsymbol{Z}[u] \bigcup \{R(u, \delta_u, M_u)\}. \tag{3.13}$$

(4) For all $u\vec{v} \in M_u$, update $\beta_{u\vec{v}}$ as follows:

$$\beta_{u\vec{v}} = \beta_{u\vec{v}} - \delta_u. \tag{3.14}$$

If $\beta_{u\vec{v}} = 0$, remove its corresponding elements from H_u and M_u, respectively.

(5) Update $I(u, H_u, M_u)$.

StarDC finally outputs the construction results in $\boldsymbol{Z}$, i.e., all star schemes in $\boldsymbol{Z}$, for the decomposition construction.

3.2. Average information rates from StarDC. We proceed to compute the average information rates. Let $\tilde{S} = \sum_u S_u / w$. The optimization problem in stage one can be modified as follows:

$$\begin{aligned}
&\text{maximize } \lambda/\tilde{S} \\
&\text{subject to} \\
&\check{\alpha}_{u\vec{v}} + \check{\alpha}_{v\vec{u}} \geq \lambda && \forall u\bar{v} \in E(G), \\
&S_u \geq \max_v \{\check{\alpha}_{u\vec{v}} | u\vec{v} \in E(\vec{G})\} + \sum_v \check{\alpha}_{v\vec{u}} && \forall u \in V(G), \\
&w \cdot \tilde{S} = \sum_u S_u \\
&\check{\alpha}_{u\vec{v}} \geq 0, \quad \check{\alpha}_{v\vec{u}} \geq 0 && \forall u\bar{v} \in E(G).
\end{aligned} \tag{3.15}$$

Let $\tilde{R} = \lambda/(\tilde{S} \cdot w)$, $\alpha_{u\vec{v}} = \check{\alpha}_{u\vec{v}}/(\tilde{S} \cdot w)$, $y_u = S_u/(\tilde{S} \cdot w)$. The linear programming problem (3.15) can be transformed to the following:

$$\begin{aligned}
&\text{maximize } \tilde{R} \cdot w \\
&\text{subject to} \\
&\alpha_{u\vec{v}} + \alpha_{v\vec{u}} \geq \tilde{R} && \forall u\bar{v} \in E(G), \\
&\max_v \{\alpha_{u\vec{v}} | u\vec{v} \in E(\vec{G})\} + \sum_v \alpha_{v\vec{u}} \leq y_u && \forall u \in V(G), \\
&\sum_u y_u = 1 \\
&\alpha_{u\vec{v}} \geq 0, \quad \alpha_{v\vec{u}} \geq 0 && \forall u\bar{v} \in E(G).
\end{aligned} \tag{3.16}$$

Note that similarly to (2.17), the strict equality constraint, $\sum_u y_u = 1$, can be reduced to $\sum_u y_u \leq 1$.

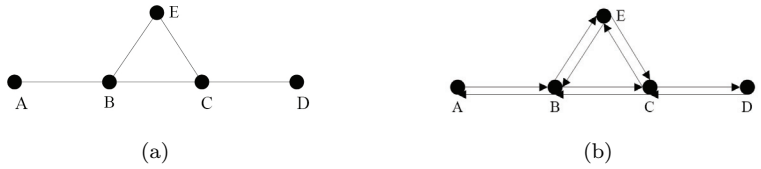

FIG. 4.1. (a) G_{13}; (b) $\vec{G_{13}}$.

4. Some examples and results. We give the example of a simple graph G_{13} in [29] (see Figure 4.1(a)) and compute the information rates and average information rates with both the Stinson method and StarDC.

4.1. The case of the information rate.

Example 4.1. In this example, we examine the information rate for the access structure from graph G_{13}, using the Stinson method with all star schemes. Here are the Γ_h's:

$$\begin{aligned}
\Gamma_1 &= \{\{A,B\}\},\\
\Gamma_2 &= \{\{B,C\}\},\\
\Gamma_3 &= \{\{B,E\}\},\\
\Gamma_4 &= \{\{C,E\}\},\\
\Gamma_5 &= \{\{C,D\}\},\\
\Gamma_6 &= \{\{A,B\},\{B,E\}\},\\
\Gamma_7 &= \{\{B,C\},\{B,E\}\},\\
\Gamma_8 &= \{\{A,B\},\{B,C\}\},\\
\Gamma_9 &= \{\{A,B\},\{B,C\},\{B,E\}\},\\
\Gamma_{10} &= \{\{B,C\},\{C,E\}\},\\
\Gamma_{11} &= \{\{C,E\},\{C,D\}\},\\
\Gamma_{12} &= \{\{B,C\},\{C,D\}\},\\
\Gamma_{13} &= \{\{B,C\},\{C,E\},\{C,D\}\},\\
\Gamma_{14} &= \{\{B,E\},\{C,E\}\}.
\end{aligned}$$

The matrices $\boldsymbol{C} = (c_{ih})$ and $\boldsymbol{B} = (b_{jh})$ are shown as follows:

$$\boldsymbol{B} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0\\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1\\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0
\end{pmatrix},$$

$$\boldsymbol{C} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0\\
1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1\\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0\\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1
\end{pmatrix}.$$

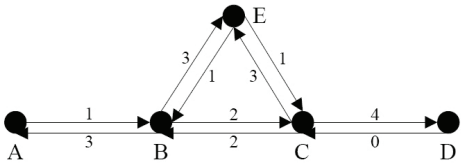

FIG. 4.2. *Normalized graph.*

The optimal solution from the Stinson method is

$$\alpha_h = \begin{cases} 1/7 & \text{if } h \in \{8, 9, 12, 13, 14\}, \\ 2/7 & \text{if } h \in \{6, 11\}, \\ 0 & \text{otherwise} \end{cases}$$

with information rate 4/7.

Next we apply StarDC decomposition construction. Example 4.2 shows that the information rates from StarDC and the Stinson method with all star schemes are both the same.

Example 4.2. We use G_{13} to compute the information rate for StarDC. Initially, we convert each undirected edge $u\bar{v}$ in G_{13} into two vectors $\vec{uv}$ and $\vec{vu}$ with corresponding coefficients $\alpha_{\vec{uv}}$ and $\alpha_{\vec{vu}}$. The resultant $\vec{G_{13}}$ is shown in Figure 4.1(b). After step (1) of StarDC, the optimal solution to the linear program is

$$\alpha_{\vec{uv}} = \begin{cases} 1/7 & \text{if } \vec{uv} \in \{\vec{AB}, \vec{EB}, \vec{EC}\}, \\ 2/7 & \text{if } \vec{uv} \in \{\vec{BC}, \vec{CB}\}, \\ 3/7 & \text{if } \vec{uv} \in \{\vec{BA}, \vec{BE}, \vec{CE}\}, \\ 4/7 & \text{if } \vec{uv} \in \{\vec{CD}\}, \\ 0 & \text{otherwise} \end{cases}$$

with information rate 4/7.

Next, we normalize these $\alpha_{\vec{uv}}$ to integer coefficients $\beta_{\vec{uv}}$ by multiplying by 7 as depicted in Figure 4.2. We obtain

$$\begin{aligned} M_A &= \{\vec{AB}\}, \\ M_B &= \{\vec{BA}, \vec{BE}, \vec{BC}\}, \\ M_C &= \{\vec{CB}, \vec{CE}, \vec{CD}\}, \\ M_D &= \emptyset, \\ M_E &= \{\vec{EB}, \vec{EC}\}. \end{aligned}$$

Consider the vectors with nonzero coefficients ($\beta_{\vec{uv}} > 0$) in Figure 4.2. For each vertex u, a list of subgraphs $I(u, H_u, M_u)$ is constructed with the vectors that connect vertex u to vertex v, where $\vec{uv} \in M_u$. The results are shown in Figure 4.3. For each $I(u, H_u, M_u)$ in Figure 4.3, the splitting step of StarDC is applied to obtain the λ-decomposition results. For example, in Figure 4.3(c), $I(C, H_C, M_C)$ has three vectors $\vec{CB}$, $\vec{CE}$, and $\vec{CD}$ with $\beta_{\vec{CB}} = 2$, $\beta_{\vec{CE}} = 3$, and $\beta_{\vec{CD}} = 4$, respectively. Then, after

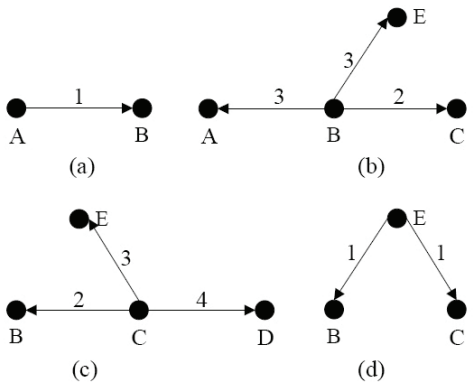

FIG. 4.3. $I(u, H_u, M_u)$: (a) $I(A, H_A, M_A)$; (b) $I(B, H_B, M_B)$; (c) $I(C, H_C, M_C)$; and (d) $I(E, H_E, M_E)$.

the splitting step, we have

$$\begin{aligned}\boldsymbol{Z}[C] = \{&R(C, 2, \{\vec{CB}, \vec{CE}, \vec{CD}\}),\\ &R(C, 1, \{\vec{CE}, \vec{CD}\}),\\ &R(C, 1, \{\vec{CD}\})\},\end{aligned}$$

as shown in Figures 4.4(d)–(f).

Figure 4.4 depicts the λ-decomposition $\boldsymbol{Z} = \bigcup \boldsymbol{Z}[u]$, $u \in \{A, B, C, E\}$. Therefore, the participant C is given seven shares, where two shares are counted by $R(C, 2, \{\vec{CB}, \vec{CE}, \vec{CD}\})$, one share is counted by $R(C, 1, \{\vec{CE}, \vec{CD}\})$, one share is counted by $R(C, 1, \{\vec{CD}\})$, two shares are counted by $R(B, 2, \{\vec{BA}, \vec{BE}, \vec{BC}\})$, and one share is counted by $R(E, 1, \{\vec{EB}, \vec{EC}\})$.

Comparing Figure 4.3 with Figure 4.4, we find that the number of shares is equal to the summation of all $\beta_{v\vec{C}}$ plus $\max_v\{\beta_{\vec{Cv}}\}$. This suggests that the number of shares distributed to participant C can be determined by Figure 4.3. That is why we calculate the number of shares using (3.3).

The next example shows that the Stinson method fails to output the optimal solution if only the star schemes are applied. Note that the information rate obtained from Example 4.3 is 3/5 and the information rate obtained from Example 4.2 is 4/7.

Example 4.3. Consider the Stinson method for a trivial complete multipartite subgraph, triangle (Γ_{15}). Here are the Γ_h's:

$$\begin{aligned}\Gamma_1 &= \{\{A, B\}\},\\ \Gamma_2 &= \{\{B, C\}\},\\ \Gamma_3 &= \{\{B, E\}\},\\ \Gamma_4 &= \{\{C, E\}\},\\ \Gamma_5 &= \{\{C, D\}\},\\ \Gamma_6 &= \{\{A, B\}, \{B, E\}\},\\ \Gamma_7 &= \{\{B, C\}, \{B, E\}\},\\ \Gamma_8 &= \{\{A, B\}, \{B, C\}\},\\ \Gamma_9 &= \{\{A, B\}, \{B, C\}, \{B, E\}\},\end{aligned}$$

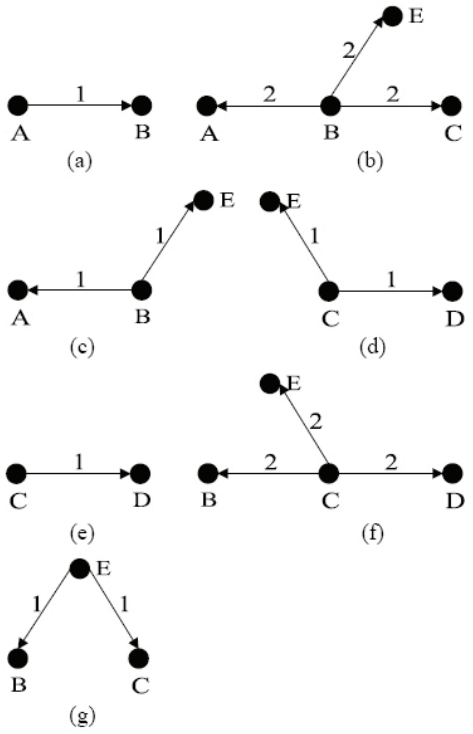

FIG. 4.4. *Split graphs* (a) $R(A,1,\{\vec{AB}\})$; (b) $R(B,2,\{\vec{BA},\vec{BE},\vec{BC}\})$; (c) $R(B,1,\{\vec{BA},\vec{BE}\})$; (d) $R(C,1,\{\vec{CE},\vec{CD}\})$; (e) $R(C,1,\{\vec{CD}\})$; (f) $R(C,2,\{\vec{CB},\vec{CE},\vec{CD}\})$; *and* (g) $R(E,1,\{\vec{EB},\vec{EC}\})$.

$$\Gamma_{10} = \{\{B,C\},\{C,E\}\},$$
$$\Gamma_{11} = \{\{C,E\},\{C,D\}\},$$
$$\Gamma_{12} = \{\{B,C\},\{C,D\}\},$$
$$\Gamma_{13} = \{\{B,C\},\{C,E\},\{C,D\}\},$$
$$\Gamma_{14} = \{\{B,E\},\{C,E\}\},$$
$$\Gamma_{15} = \mathbf{\{\{B,C\},\{B,E\},\{C,E\}\}}.$$

The matrices $\boldsymbol{C} = (c_{ih})$ and $\boldsymbol{B} = (b_{jh})$ are shown as follows:

$$\boldsymbol{B} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix},$$

$$\boldsymbol{C} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

The optimal solution to the linear problem in the Stinson method is

$$\alpha_h = \begin{cases} 1/5 & \text{if } h \in \{8, 12, 15\}, \\ 2/5 & \text{if } h \in \{6, 11\}, \\ 0 & \text{otherwise} \end{cases}$$

with information rate 3/5.

4.2. The case of the average information rate.

Example 4.4. The average information rate for G_{13} can be determined by the Stinson method with all star schemes from (2.17). The matrices $\boldsymbol{C} = (c_{ih})$ and $\boldsymbol{B} = (b_{jh})$ are the same as in Example 4.1. The optimal solution from the Stinson method is

$$\alpha_h = \begin{cases} 1/7 & \text{if } h \in \{6, 13\}, \\ 0 & \text{otherwise} \end{cases}$$

with average information rate 5/7.

Example 4.5. The average information rate for G_{13} can also be determined by StarDC from (3.16). The optimal solution to the resultant linear program is

$$\alpha_{u\vec{v}} = \begin{cases} 1/7 & \text{if } u\vec{v} \in \{\vec{BA}, \vec{BE}, \vec{CB}, \vec{CD}, \vec{CE}\}, \\ 0 & \text{otherwise} \end{cases}$$

with average information rate 5/7.

5. Analysis.

5.1. Correctness. In this section we show that the information rate of the optimal decomposition from the Stinson method with star schemes is the same as that of the optimal decomposition from StarDC (Theorem 5.3). We also give a similar result for the average information rate (Theorem 5.4).

DEFINITION 5.1. *A solution satisfying the constraints of the linear programming problem is called a* feasible solution *of the problem. A* feasible decomposition *is a decomposition construction from a feasible solution.*

THEOREM 5.1. *For any feasible decomposition from the Stinson method (described in section* 2.3.1*) with star schemes, there exists a corresponding feasible decomposition from StarDC (described in section* 3.1*) such that the information rate of the former is smaller than or equal to the information rate of the latter.*

Proof. (Part I) We claim that, given a feasible decomposition from the Stinson method with star schemes, we can construct a feasible decomposition for StarDC.

Suppose $\{\Gamma_1, \Gamma_2, \ldots, \Gamma_m\}$ is a set of star schemes for the access structure Γ_G of graph G. Let $r_h \in V(G)$ be the center of star scheme Γ_h. If a star scheme contains only a single edge, we randomly assign one vertex as its center. Let F_u be the set of indices of star schemes where vertex u serves as their common center. That is,

$$F_u = \{h | u \in V(\Gamma_h), u = r_h, 1 \leq h \leq m\}. \tag{5.1}$$

Let L_u be the set of indices of star schemes where vertex u appears, i.e., $u \in V(\Gamma_h)$, but does not serve as their center. That is,

$$L_u = \{h | u \in V(\Gamma_h), u \neq r_h, 1 \leq h \leq m\}. \tag{5.2}$$

Assume that a feasible decomposition in the Stinson method contains m star schemes $\Gamma_1, \Gamma_2, \ldots, \Gamma_m$ with corresponding coefficients $\check{\alpha}_1, \check{\alpha}_2, \ldots, \check{\alpha}_m$, as well as the parameter λ, implicitly. For each $\bar{uv} \in E(G)$, define

$$b^h_{\bar{uv}} = \begin{cases} 1 & \text{if } \bar{uv} \in E(\Gamma_h), \\ 0 & \text{otherwise.} \end{cases} \tag{5.3}$$

Here $b^h_{\bar{uv}} = 1$ means edge $\bar{uv}$ appears in the star scheme Γ_h; otherwise, $b^h_{\bar{uv}} = 0$. According to (2.7), we know that $\sum_{h=1}^{m} b^h_{\bar{uv}} \check{\alpha}_h \geq \lambda$. For each $\bar{uv} \in E(G)$, we construct the corresponding solution in StarDC as follows:

$$\begin{aligned} \check{\alpha}_{\vec{uv}} &= \sum_{h \in F_u} b^h_{\bar{uv}} \check{\alpha}_h, \\ \check{\alpha}_{\vec{vu}} &= \sum_{h \in L_u} b^h_{\bar{uv}} \check{\alpha}_h. \end{aligned} \tag{5.4}$$

In addition, the corresponding solution for S is assigned by

$$S_u = \max_v \{\check{\alpha}_{\vec{uv}} | \vec{uv} \in E(\vec{G})\} + \sum_v \check{\alpha}_{\vec{vu}},$$

$$S = \max_u \{S_u\}. \tag{5.5}$$

It is clear that $\check{\alpha}_{\vec{uv}} \geq 0,\ \check{\alpha}_{\vec{vu}} \geq 0$, and

$$\begin{aligned} \check{\alpha}_{\vec{uv}} + \check{\alpha}_{\vec{vu}} &= \sum_{h \in F_u} b^h_{\bar{uv}} \check{\alpha}_h + \sum_{h \in L_u} b^h_{\bar{uv}} \check{\alpha}_h \\ &= \sum_{h=1}^{m} b^h_{\bar{uv}} \check{\alpha}_h \geq \lambda. \end{aligned} \tag{5.6}$$

Therefore, $\check{\alpha}_{\vec{uv}}$ and $\check{\alpha}_{\vec{vu}}$ satisfy the linear constraints in StarDC (see (3.5)). The corresponding feasible decomposition in StarDC is then constructed with the coefficients $\check{\alpha}_{\vec{uv}}$ of vector $\vec{uv}$ by the splitting stage in StarDC.

For example, suppose Γ_1, Γ_2, and Γ_3 are three star schemes with coefficients $\check{\alpha}_1, \check{\alpha}_2$, and $\check{\alpha}_3$ shown in Figure 5.1(a). So the sets of indices in (5.1) and (5.2) are as follows:

$$\begin{array}{ll} F_A = \emptyset, & L_A = \{1\}, \\ F_B = \{3\}, & L_B = \{1, 2\}, \\ F_C = \{1, 2\}, & L_C = \{3\}, \\ F_D = \emptyset, & L_D = \{1, 3\}, \\ F_E = \emptyset, & L_E = \{2\}. \end{array}$$

The corresponding solution (before splitting) in StarDC is shown in Figure 5.1(b).

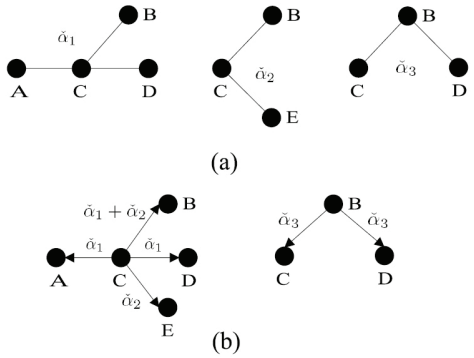

FIG. 5.1. *An illustration for the construction of the corresponding feasible decomposition in StarDC from a feasible decomposition in the Stinson method with star schemes.* (a) $\{\Gamma_1, \Gamma_2, \Gamma_3\}$; (b) *the corresponding solution (before splitting) in StarDC.*

By (5.4), the corresponding solution in StarDC is as follows:

$$\begin{aligned}
&\check{\alpha}_{\vec{CA}} = b^1_{\vec{CA}}\check{\alpha}_1 + b^2_{\vec{CA}}\check{\alpha}_2 = \check{\alpha}_1,\\
&\check{\alpha}_{\vec{AC}} = 0,\\
&\check{\alpha}_{\vec{CD}} = b^1_{\vec{CD}}\check{\alpha}_1 + b^2_{\vec{CD}}\check{\alpha}_2 = \check{\alpha}_1,\\
&\check{\alpha}_{\vec{DC}} = 0,\\
&\check{\alpha}_{\vec{CE}} = b^1_{\vec{CE}}\check{\alpha}_1 + b^2_{\vec{CE}}\check{\alpha}_2 = \check{\alpha}_2,\\
&\check{\alpha}_{\vec{EC}} = 0,\\
&\check{\alpha}_{\vec{CB}} = b^1_{\vec{CB}}\check{\alpha}_1 + b^2_{\vec{CB}}\check{\alpha}_2 = \check{\alpha}_1 + \check{\alpha}_2,\\
&\check{\alpha}_{\vec{BC}} = b^3_{\vec{BC}}\check{\alpha}_3 = \check{\alpha}_3,\\
&\check{\alpha}_{\vec{BD}} = b^3_{\vec{BD}}\check{\alpha}_3 = \check{\alpha}_3,\\
&\check{\alpha}_{\vec{DB}} = 0.
\end{aligned}$$

The numbers of shares distributed to vertex u, $u \in \{A, B, C, D, E\}$, in the corresponding feasible decomposition of StarDC are

$$\begin{aligned}
S_A &= \check{\alpha}_{\vec{CA}} = \check{\alpha}_1,\\
S_B &= \max\{\check{\alpha}_{\vec{BC}}, \check{\alpha}_{\vec{BD}}\} + \check{\alpha}_{\vec{CB}} = \check{\alpha}_1 + \check{\alpha}_2 + \check{\alpha}_3,\\
S_C &= \max\{\check{\alpha}_{\vec{CA}}, \check{\alpha}_{\vec{CB}}, \check{\alpha}_{\vec{CD}}, \check{\alpha}_{\vec{CE}}\} + \check{\alpha}_{\vec{BC}} = \check{\alpha}_1 + \check{\alpha}_2 + \check{\alpha}_3,\\
S_D &= \check{\alpha}_{\vec{CD}} + \check{\alpha}_{\vec{BD}} = \check{\alpha}_1 + \check{\alpha}_3,\\
S_E &= \check{\alpha}_{\vec{CE}} = \check{\alpha}_2,\\
S &= \check{\alpha}_1 + \check{\alpha}_2 + \check{\alpha}_3.
\end{aligned}$$

(Part II) Next, we show that the information rate of the corresponding feasible decomposition in StarDC either increases or is unchanged.

Let R_1 be the information rate of the feasible decomposition in the Stinson method with star schemes, and let R_2 be the information rate of the corresponding feasible decomposition in StarDC.

For each $u \in V(\Gamma_h), 1 \le h \le m$, define

$$c_{uh} = \begin{cases} 1 & \text{if } u \in V(\Gamma_h),\\ 0 & \text{otherwise.} \end{cases} \tag{5.7}$$

Here $c_{uh} = 1$ means vertex u appears in star scheme Γ_h; otherwise, $c_{uh} = 0$. Then, $R_1 = \lambda/S'$, where $S' = \max\{S'_u | u \in V(G)\}$ and $S'_u = \sum_{h=1}^{m} c_{uh}\check{\alpha}_h$.

For any $u \in V(G)$, the number of shares distributed to u in the decomposition of the Stinson method with star schemes is

$$S'_u = \sum_{h=1}^{m} c_{uh}\check{\alpha}_h = \sum_{h\in F_u} \check{\alpha}_h + \sum_{h\in L_u} \check{\alpha}_h. \tag{5.8}$$

Then, for the corresponding decomposition in StarDC, we have

$$\max_v\{\check{\alpha}_{u\vec{v}}\} = \max_v \left\{ \sum_{h\in F_u} b^h_{u\vec{v}}\check{\alpha}_h \right\} \le \sum_{h\in F_u} \check{\alpha}_h. \tag{5.9}$$

In addition, in the star scheme Γ_h, where $h \in L_u$, the vertex u (here u does not serve as the center in Γ_h) is adjacent to the center r_h, i.e., $b^h_{u\vec{v}} = 1$, only when $v = r_h$. This implies

$$\sum_v b^h_{u\vec{v}}\check{\alpha}_h = \check{\alpha}_h. \tag{5.10}$$

Therefore,

$$\begin{aligned} \sum_v \check{\alpha}_{v\vec{u}} &= \sum_v \sum_{h\in L_u} b^h_{u\vec{v}}\check{\alpha}_h \\ &= \sum_{h\in L_u} \sum_v b^h_{u\vec{v}}\check{\alpha}_h = \sum_{h\in L_u} \check{\alpha}_h. \end{aligned} \tag{5.11}$$

By (5.9) and (5.11), the number of shares distributed to u in the corresponding feasible decomposition in StarDC is

$$S_u = \max_v\{\check{\alpha}_{u\vec{v}}\} + \sum_v \check{\alpha}_{v\vec{u}} \le \sum_{h\in F_u} \check{\alpha}_h + \sum_{h\in L_u} \check{\alpha}_h = S'_u, \tag{5.12}$$

$$S = \max_u\{S_u\} \le \max_u\{S'_u\} = S', \tag{5.13}$$

$$R_1 = \frac{\lambda}{S'} \le \frac{\lambda}{S} = R_2. \tag{5.14}$$

Thus, the information rate of the corresponding feasible decomposition in StarDC is nondecreasing. □

THEOREM 5.2. *For any feasible decomposition in StarDC (described in section* 3.1*), there exists a corresponding feasible decomposition in the Stinson method (described in section* 2.3.1*) with star schemes such that both have the same information rate.*

Proof. This is trivial, because the feasible decomposition in StarDC is also a feasible decomposition in the Stinson method with star schemes. Thus the information rate is unchanged. □

THEOREM 5.3. *The information rate of the optimal decomposition from the Stinson method (described in section* 2.3.1*) with star schemes is the same as that from StarDC (described in section* 3.1*).*

Proof. By Theorems 5.1 and 5.2, the result follows immediately. ∎

THEOREM 5.4. *The average information rate of the optimal decomposition from the Stinson method (described in section* 2.3.2*) with star schemes is the same as that from StarDC (described in section* 3.2*).*

Proof. The proof is similar to that of Theorem 5.3. We need only prove that, for any feasible decomposition from the Stinson method with star schemes in section 2.3.2, there exists a corresponding feasible decomposition from StarDC in section 3.2 such that the average information rate of the former is smaller than or equal to the average information rate of the latter.

(Part I) We claim that, given a feasible decomposition from the Stinson method with star schemes in section 2.3.2, we can construct a feasible decomposition for StarDC in section 3.2. Basically, this is the same as that in Theorem 5.1 except that (5.5) needs to be replaced by

$$\begin{aligned} S_u &= \max_v\{\check{\alpha}_{u\vec{v}} | u\vec{v} \in E(\vec{G})\} + \sum_v \check{\alpha}_{v\vec{u}}, \\ \tilde{S} &= \sum_u S_u/w. \end{aligned} \tag{5.15}$$

(Part II) Next, we show that the average information rate of the corresponding feasible decomposition in StarDC either increases or is unchanged. Basically, this is the same as in Part II of Theorem 5.1.

Let $\tilde{R}_1 w$ be the average information rate of the feasible decomposition in the Stinson method with star schemes, and let $\tilde{R}_2 w$ be the average information rate of the corresponding feasible decomposition in StarDC. Then

$$\tilde{R}_1 = \frac{\lambda}{w\tilde{S}'}, \quad \tilde{R}_2 = \frac{\lambda}{w\tilde{S}},$$

where

$$\tilde{S}' = \sum_u S'_u/w, \quad \tilde{S} = \sum_u S_u/w.$$

By (5.12), we have

$$S_u \le S'_u \quad \forall u \in V(G).$$

Therefore,

$$\tilde{S}' = \sum_u S'_u/w \ge \sum_u S_u/w = \tilde{S},$$

$$\tilde{R}_1 w = \lambda/\tilde{S}' \le \lambda/\tilde{S} = \tilde{R}_2 w. \tag{5.16}$$ ∎

5.2. Complexity. Khachian in [15] gave a polynomial time algorithm to solve linear programming problems by the ellipsoid method. The algorithm has the worst case complexity, $O(N_c N_v^3 L)$, where N_c is the number of inequalities excluding those simple bound constraints for variables (i.e., nonnegativity constraints); N_v is the number of variables; and L is defined as the number of bits needed to encode the linear programming problem. Karmarkar presented an interior point algorithm which requires $O((N_c^{1.5} N_v^2 + N_c^2 N_v)L)$ arithmetic operations [14]. Vaidya in [28] gave an algorithm for the linear programming problem which requires $O(((N_c + N_v)N_v^2 + (N_c + N_v)^{1.5} N_v)L)$ arithmetic operations. Here we consider the worst case when $|E| = O(|V|^2)$ for a graph $G = (V, E)$. Also we analyze only the case of the information rate from the Stinson method and StarDC. As for the case of the average information rate, we can easily obtain the same result in a similar way.

5.2.1. The Stinson method. We analyze the time complexity in terms of the variables and inequalities used in linear programming. In the Stinson method with star schemes, $O(2^{|V|})$ variables and $|E| + |V|$ inequalities are required:

$$\begin{aligned} &N_v = O(2^{|V|}), \\ &N_c = |E| + |V| = O(|V|^2). \end{aligned} \tag{5.17}$$

Thus the time complexity is

$$\begin{aligned} &O(((N_c + N_v)N_v^2 + (N_c + N_v)^{1.5}N_v)L) \\ &= O((((|V|^2 + 2^{|V|})2^{2|V|} + (|V|^2 + 2^{|V|})^{1.5}2^{|V|})L) \\ &= O(2^{3|V|}L). \end{aligned} \tag{5.18}$$

5.2.2. StarDC. StarDC uses $2|E| + 1$ variables. Now we count the number of inequalities excluding nonnegativity constraints in (3.6). It is clear that we have $|E|$ inequalities for $\alpha_{u\vec{v}} + \alpha_{v\vec{u}} \geq R \ \forall u\bar{v} \in E(G)$. Let n_u be the degree of vertex u in G. Thus the out-degree and in-degree of vertex u in $\vec{G}$ are also n_u, respectively. Without loss of generality, assume that $v_1, v_2, \ldots, v_{n_u}$ are the vertices which are incident to vertex u. The constraint

$$\max_v \{\alpha_{u\vec{v}} | u\vec{v} \in E(\vec{G})\} + \sum_v \alpha_{v\vec{u}} \leq 1$$

can be converted to n_u inequalities

$$\begin{aligned} &\alpha_{\overrightarrow{uv_1}} + \sum_v \alpha_{\vec{vu}} \leq 1, \\ &\alpha_{\overrightarrow{uv_2}} + \sum_v \alpha_{\vec{vu}} \leq 1, \\ &\vdots \\ &\alpha_{\overrightarrow{uv_{n_u}}} + \sum_v \alpha_{\vec{vu}} \leq 1. \end{aligned}$$

Since StarDC associates each undirected $u\bar{v}$ of G with two opposite vectors $u\vec{v}$ and $v\vec{u}$, we have

$$\sum_{\forall u \in V(G)} n_u = 2|E|$$

inequalities for $\max_v \{\alpha_{u\vec{v}} | u\vec{v} \in E(\vec{G})\} + \sum_v \alpha_{v\vec{u}} \leq 1 \ \forall u \in V(G)$.

We have

$$\begin{aligned} &N_v = 2|E| + 1 = O(|V|^2), \\ &N_c = |E| + 2|E| = 3|E| = O(|V|^2). \end{aligned} \tag{5.19}$$

Thus, the time complexity is

$$\begin{aligned} &O(((N_c + N_v)N_v^2 + (N_c + N_v)^{1.5}N_v)L) \\ &= O((|V|^2(|V|^2)^2 + (|V|^2)^{1.5}|V|^2)L) = O(|V|^6 L). \end{aligned} \tag{5.20}$$

We consider the complexity of stage two in StarDC. In the worst case, for each vertex of access structure, there is a $K_{1,|V|-1}$ with $|V|-1$ different coefficients on every vector in the $K_{1,|V|-1}$. Each $K_{1,|V|-1}$ could be split into at most $|V|-1$ different star schemes. The sorting of $|V|-1$ coefficients requires $O(|V|\log|V|)$ operations. Therefore, the splitting of a $K_{1,|V|-1}$ needs at most $O(|V|\log|V|)$ operations. Since there are at most $|V|$ centers, the worst case time complexity of stage two in StarDC is

$$(|V|\log|V|)|V| = O(|V|^2\log|V|). \tag{5.21}$$

Thus, by (5.20) and (5.21), the worst case time complexity of StarDC is

$$O(|V|^2\log|V|) + O(|V|^6 L) = O(|V|^6 L). \tag{5.22}$$

6. Conclusion. StarDC exploits a different way to avoid the predicament of listing all feasible schemes of the linear programming problem in the Stinson method. Significantly, StarDC makes possible the automatic distribution of decomposition construction. In addition, StarDC can also be applied to other generalized decompositions, such as (λ,γ)-decomposition and weighted decomposition, because these generalized decompositions are also challenged with finding the suitable subgraphs (ideal or with high information rate schemes) for a given graph. The information rate from StarDC is the same as that from the Stinson method with star schemes. StarDC improves the time complexity for the decomposition of the access structure with star schemes in the Stinson method from exponential time complexity $O(2^{3|V|}L)$ to polynomial time complexity $O(|V|^6 L)$, where $|V|$ is the number of vertices in the graph that represents the access structure and L is defined as the number of bits needed to encode the linear programming problem.

REFERENCES

[1] A. Beimel, T. Tassa, and E. Weinreb, *Characterizing ideal weighted threshold secret sharing*, SIAM J. Discrete Math., 22 (2008), pp. 360–397.

[2] J. C. Benaloh and J. Leichter, *Generalized secret sharing and monotone functions*, in Proceedings of Advances in Cryptology—CRYPTO'88, Lecture Notes in Comput. Sci. 403, Springer-Verlag, London, 1988, pp. 27–35.

[3] B. Blakley, G. R. Blakley, A. H. Chan, and J. L. Massey, *Threshold schemes with disenrollment*, in Advances in Cryptology—CRYPTO'92, Proceedings of the 12th Annual International Cryptology Conference, Santa Barbara, CA, 1992, Lecture Notes in Comput. Sci. 740, Springer-Verlag, London, 1992, pp. 540–548.

[4] G. R. Blakley, *Safeguarding cryptographic keys*, in Proceedings of the American Federation of Information Processing Societies Records (AFIPS1979) National Computer Conference, Vol. 48, 1979, pp. 313–317.

[5] C. Blundo, A. De Santis, R. De Simone, and U. Vaccaro, *Tight bounds on the information rate of secret sharing schemes*, Des., Codes Cryptogr., 11 (1997), pp. 107–122.

[6] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro, *Graph decompositions and secret sharing schemes*, J. Cryptology, 8 (1995), pp. 39–64.

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

[8] E. F. Brickell and D. R. Stinson, *Some improved bounds on the information rate of perfect secret sharing schemes*, J. Cryptology, 5 (1992), pp. 153–166.

[9] G. Di Crescenzo and C. Galdi, *Hypergraph decomposition and secret sharing*, Discrete Appl. Math., 157 (2009), pp. 928–946.

[10] L. Csirmaz and P. Ligeti, *On an infinite family of graphs with information ratio* $2-1/k$, Computing, 85 (2009), pp. 127–136.

[11] M. Ito, A. Saito, and T. Nishizeki, *Secret sharing scheme realizing general access structure*, in Proceedings of IEEE Global Communications (Globecom'87), Tokyo, 1987, pp. 99–102.

[12] M. Ito, A. Saito, and T. Nishizeki, *Multiple assignment scheme for sharing secret*, J. Cryptology, 6 (1993), pp. 15–20.
[13] W.-A. Jackson and K. M. Martin, *Perfect secret sharing schemes on five participants*, Des. Codes Cryptogr., 9 (1996), pp. 233–250.
[14] N. Karmarkar, *A new polynomial time algorithm for linear programming*, Combinatorica, 4 (1984), pp. 373–395.
[15] L. G. Khachian, *A polynomial algorithm in linear programming*, Soviet Math. Dokl., 20 (1979), pp. 191–194.
[16] M. Li and R. Poovendran, *Disenrollment with perfect forward secrecy in threshold schemes*, IEEE Trans. Inform. Theory, 52 (2006), pp. 1676–1682.
[17] M. Liu, L. Xiao, and Z. Zhang, *Multiplicative linear secret sharing schemes based on connectivity of graphs*, IEEE Trans. Inform. Theory, 53 (2007), pp. 3973–3978.
[18] J. Marti-Farre and C. Padro, *Secret sharing schemes with three or four minimal qualified subsets*, Des. Codes Cryptogr., 34 (2005), pp. 17–34.
[19] R. J. McEliece and D. V. Sarwate, *On sharing secrets and Reed-Solomon codes*, Commun. ACM, 24 (1981), pp. 583–584.
[20] C. Padro and G. Saez, *Secret sharing schemes with bipartite access structure*, IEEE Trans. Inform. Theory, 46 (2000), pp. 2596–2604.
[21] C. Padro and G. Saez, *Lower bounds on the information rate of secret sharing schemes with homogeneous access structure*, Inform. Process. Lett., 83 (2002), pp. 345–351.
[22] A. Shamir, *How to share a secret*, Commun. ACM, 22 (1979), pp. 612–613.
[23] R. Steinfeld, J. Pieprzyk, and H. Wang, *Lattice-based threshold changeability for standard Shamir secret-sharing schemes*, IEEE Trans. Inform. Theory, 53 (2007), pp. 2542–2559.
[24] D. R. Stinson, *An explication of secret sharing schemes*, Des. Codes Cryptogr., 2 (1992), pp. 357–390.
[25] D. R. Stinson, *Decomposition constructions for secret sharing schemes*, IEEE Trans. Inform. Theory, 40 (1994), pp. 118–125.
[26] H. M. Sun and B. L. Chen, *Weighted decomposition construction for perfect secret sharing schemes*, Comput. Math. Appl., 43 (2002), pp. 877–887.
[27] H. M. Sun and S. P. Shieh, *Recursive constructions for perfect secret sharing schemes*, Comput. Math. Appl., 37 (1999), pp. 87–96.
[28] P. M. Vaidya, *An algorithm for linear programming which requires* $o(((m+n)n^2+(m+n)^{1.5}n)l)$ *arithmetic operations*, in Proceedings of the Nineteenth Annual ACM Conference on Theory of Computing, 1987, pp. 29–38.
[29] M. van Dijk, *On the information rate of perfect secret sharing schemes*, Des. Codes Cryptogr., 6 (1995), pp. 143–169.
[30] M. van Dijk, W.-A. Jackson, and K. M. Martin, *A general decomposition construction for incomplete secret sharing schemes*, Des. Codes Cryptogr., 15 (1998), pp. 301–321.
[31] M. van Dijk, T. Kevenaar, G.-J. Schrijen, and P. Tuyls, *Improved constructions of secret sharing schemes by applying* (λ,ω)*-decompositions*, Inform. Process. Lett., 99 (2006), pp. 154–157.
[32] J. Yuan and C. Ding, *Secret sharing schemes from three classes of linear codes*, IEEE Trans. Inform. Theory, 52 (2006), pp. 206–212.