On the Equivalence between the Set Covering Problem and the Problem of Finding Optimal Cumulative Assignment Schemes

Qiang Li[*], Xiangxue Li[†], Dong Zheng[*], Zheng Huang[*] and Kefei Chen[*]
[*]*School of Electronic Information and Electrical Engineering,*
Shanghai Jiao Tong University, Shanghai 200240, China.
Email: {qiangl, dzheng, huang-zheng, kfchen}@sjtu.edu.cn
[†]*Department of Computer Science and Technology,*
East China Normal University, Shanghai 200241,China.
Email: xxli@cs.ecnu.edu.cn

Abstract

A cumulative assignment scheme (CAS for short) is a special type of secret sharing schemes. For any given access structure (AS), a CAS which minimizes the cardinality of the primitive share set (the average information rate, or the worst information rate) is called an optimal CAS and can be constructed via solving some binary integer programming (BIP). The problem of finding optimal CAS's for complete AS's is solved.

We consider in this paper the problem of finding optimal CAS's for incomplete AS's. The paper introduces some notions including the connected-super-forbidden-family and the lower-forbidden-family for AS's. We show that an optimal CAS can be derived from some smaller sized BIP whose variables (constraints, resp.) are based on the connected-super-forbidden-family (lower-forbidden-family, resp.) of the given AS. The paper further builds the close relationship between the problem of finding optimal CAS's and the set covering problem (SCP). We prove that the problem of finding a CAS with minimum cardinality of the primitive share set (or minimum average information rate) is equivalent to the SCP, and thus is NP-hard. Other contributions of the paper include: 1) two types of AS's are recognized so that we can construct the corresponding optimal CAS's directly; and 2) a greedy algorithm is proposed to find CAS's with smaller worst information rate.

1. Introduction

Secret sharing schemes (SSS's), introduced by Shamir [1] and Blakley [2] independently, are methods of distributing a secret among a set of participants, in such a way that each qualified subset can reconstruct the secret whereas any forbidden subset has no information about it. And the collection of qualified and forbidden subsets composes an access structure (AS) [3]. The efficiency of a SSS is measured by information rate [4]. The information rate of a perfect SSS is lower bounded by 1 [5], [6], [7], and that of an ideal one [1], [2] is exactly 1.

Ito et al. [3] show that there exist perfect SSS's named as multiple assignment schemes (MAS's) realizing any given AS. And the construction of [3] outputs a cumulative assignment scheme (CAS) [8] which is a special type of MAS's. Recently, [9], [10] propose independently a novel method to obtain optimal MAS's by integer programming (IP) [11]. For any given AS, the minimum information rate a MAS can achieve is always less than or equal to that a CAS can do [9], [10]. However, in some specific applications, e.g., visual cryptography [12], [13], only CAS's can be used as building blocks. And we focus on finding optimal CAS's in this paper. Li et al. [14] enable an optimal CAS construction by binary integer programming (BIP) [11]. Simmons et al. [8] show that among all CAS's realizing a given complete AS, the scheme [3] achieves the minimum cardinality of the primitive share set, and [14] further proves that [3] attains the minimum average and worst information rates simultaneously. And so, the problem of finding optimal CAS's for complete AS's is solved.

We consider in this paper the problem of finding optimal CAS's for incomplete AS's. The paper introduces some notions including the connected-super-forbidden-family and the lower-forbidden-family for general AS's. We show that an optimal CAS can be derived from some smaller sized BIP whose variables (constraints, resp.) are based on the connected-super-forbidden-family (lower-forbidden-family, resp.) of the given AS. The paper further builds the close relationship between the problem of finding optimal CAS's and the set covering problem (SCP) [11]. We prove that the problem of finding a CAS with minimum cardinality of the primitive share set (or minimum average information rate) is equivalent to the SCP, and thus is NP-hard [15]. Other contributions of the paper include: 1) two types of AS's are recognized so that we can construct the corresponding optimal CAS's directly; and 2) a greedy algorithm is proposed to find CAS's with smaller worst information rate.

The remainder of the paper is organized as follows. Basic definitions and related work are reviewed in section 2. Section 3 first introduces some notions including the connected-super-forbidden-family and the lower-forbidden-family, then shows that the size of the BIP problems for optimal CAS's can be cut down, builds the close relationship between the problem of finding optimal CAS's and the SCP, lastly proves that finding CAS's with minimum cardinality of the primitive share set (or minimum average information rate) is NP-hard. We show two types of AS's whose optimal CAS's can be directly given in section 4. We propose in section 5 a greedy algorithm to find CAS's with smaller worst information rate. Conclusions are drawn in section 6.

2. Preliminaries

Throughout this paper, $P = \{p_1, p_2, \cdots, p_n\}$ is the set of n participants. I, J are the set $I = \{1, 2, \cdots, n\}$, $J = \{1, 2, \cdots, 2^n - 1\}$. For $j \in J$, we denote $j_i, i \in I$ as the unique integers satisfying $j = \sum_{i=1}^{n} j_i 2^{i-1}, j_i \in \{0, 1\}$, and $P_j = \{p_i \in P : j_i = 1, i \in I\}$, $w(j, S) = \sum_{p_i \in S} j_i$, $w_j = w(j, P)$.

An access structure [3] $\mathcal{A} = \{\mathcal{Q}, \mathcal{F}\}$ contains two families of subsets of P, the qualified family $\mathcal{Q}$ and the forbidden family $\mathcal{F}$, and is monotone in the sense that $\mathcal{Q} \cap \mathcal{F} = \emptyset$ and $\forall S \subseteq T \subseteq P : S \in \mathcal{Q} \Rightarrow T \in \mathcal{Q}, T \in \mathcal{F} \Rightarrow S \in \mathcal{F}$. $\mathcal{A}$ is complete if $\mathcal{Q} \cup \mathcal{F} = 2^P$. The minimal qualified family $\mathcal{Q}^-$ and the maximal forbidden family $\mathcal{F}_+$ of $\mathcal{A}$ are defined as (1).

$$\begin{cases} \mathcal{Q}^- = \{Q \in \mathcal{Q} : \forall p \in Q, Q - \{p\} \notin \mathcal{Q}\} \\ \mathcal{F}_+ = \{F \in \mathcal{F} : \forall p \in P - F, F \cup \{p\} \notin \mathcal{F}\} \end{cases} \tag{1}$$

For a SSS Π, if each $S \subseteq P$ is either qualified or forbidden, then Π is perfect. When we say Π realizes $\mathcal{A}$, it means that each subset $Q \in \mathcal{Q}$ is qualified whereas any subset $F \in \mathcal{F}$ is forbidden. A (k, n)-threshold scheme [1], [2] is a SSS with $|P| = n$, $\mathcal{Q} = \{Q \subseteq P : |Q| \geq k\}$ and $\mathcal{F} = \{F \subseteq P : |F| \leq k - 1\}$. And a (n, n)-threshold scheme is also named as an unanimous consent scheme of rank n [5].

Let K be the set of the secret, $K_\Pi(p)$ be the set of all possible shares given to $p \in P$. Denote $H(K), H(K_\Pi(p))$ as the entropies of K and of $K_\Pi(p)$ respectively. Then the information rate of p in Π is $\rho_\Pi(p) = H(K_\Pi(p))/H(K)$, the average information rate $\bar{\rho}_\Pi$ and the worst information rate ρ_Π of Π are $\bar{\rho}_\Pi = \sum_{p \in P} \rho_\Pi(p)/|P|$ and $\rho_\Pi = \max\{\rho_\Pi(p) : p \in P\}$ respectively [4]. For a perfect SSS Π, if $\rho_\Pi(p) = 1, p \in P$ then Π is ideal [1], [2], [5].

In a multiple assignment scheme Π [3], there is a map $\psi_\Pi : P \mapsto 2^{\Omega_\Pi}$ assigning a subset of Ω_Π to each participant, where Ω_Π is the primitive share set of an ideal (k_Π, m_Π)-threshold scheme. Thus $\rho_\Pi(p) = |\psi_\Pi(p)|, p \in P$ and Π realizes $\mathcal{A}$ if and only if (2) holds true [3].

$$\begin{cases} \forall Q \in \mathcal{Q}^- : |\bigcup_{p \in Q} \psi_\Pi(p)| \geq k_\Pi \\ \forall F \in \mathcal{F}_+ : |\bigcup_{p \in F} \psi_\Pi(p)| \leq k_\Pi - 1 \end{cases} \tag{2}$$

For a MAS Π, there is a collection of nonnegative integers $X_\Pi = \{x_\Pi(j) = |\Omega_\Pi(j)| : j \in J\}$, where $\Omega_\Pi(j) = \bigcap_{j_i=1, i\in I} \psi_\Pi(p_i), j \in J$. On the other hand, for any given collection of nonnegative integers $X = \{x_j : j \in J\}$, there exists a MAS Π satisfying $|\Omega_\Pi(j)| = x_j, j \in J$. Since (2), (3) hold true for each MAS Π realizing the given $\mathcal{A}$, a MAS which minimizes the cardinality of the primitive share set (the average information rate, or the worst information rate) can be obtained by solving the corresponding IP problem [9], [10].

$$\begin{cases} \forall i \in I : \rho_\Pi(p_i) = |\psi_\Pi(p_i)| = \sum_{j_i=1, j\in J} x_\Pi(j) \\ m_\Pi = \sum_{j\in J} x_\Pi(j) \\ \bar{\rho}_\Pi = \sum_{i\in I} \rho_\Pi(p_i)/|P| = \sum_{j\in J} w_j x_\Pi(j)/n \\ \rho_\Pi = max\{\rho_\Pi(p_i) : i \in I\} \\ \forall S \subseteq P : |\bigcup_{p\in S} \psi_\Pi(p)| = \sum_{w(j,S)\geq 1, j\in J} x_\Pi(j) \end{cases} \tag{3}$$

A MAS Π is also called a cumulative assignment scheme [8] if $k_\Pi = m_\Pi$, i.e, Ω_Π is the primitive share set of an ideal unanimous consent scheme. Denote $J' = \{j \in J : \forall Q \in \mathcal{Q}^-, w(j,Q) \geq 1\}$, then a CAS Π realizes $\mathcal{A}$ if and only if (4) holds true [14]. And there exists an optimal CAS Π satisfying $x_\Pi(j) \in \{0,1\}, j \in J'$, i.e., an optimal CAS realizing $\mathcal{A}$ can be derived from BIP [14].

$$\begin{cases} \forall j \in J - J' : x_\Pi(j) = 0 \\ \forall F \in \mathcal{F}_+ : \sum_{w(j,F)=0, j\in J'} x_\Pi(j) \geq 1 \end{cases} \tag{4}$$

3. On the Equivalence between the SCP and the Problem of Finding Optimal CAS's

As [14] points out, a CAS which minimizes the cardinality of the primitive share set (the average information rate, or the worst information rate) can be obtained via solving some BIP problem. In this section, we will show that such a scheme can be found from an even smaller sized BIP problem. And there is a close relationship between the problem of finding optimal CAS's and the set covering problem [11]. We will prove that finding a CAS with minimum cardinality of the primitive share set (or minimum average information rate) is equivalent to the SCP, and thus is NP-hard [15].

3.1. Definitions

Definition 1: Given $\mathcal{A}$ and a CAS Π realizing $\mathcal{A}$, if there is no CAS Π' realizing $\mathcal{A}$ such that $m_{\Pi'} < m_\Pi$ ($\bar{\rho}_{\Pi'} < \bar{\rho}_\Pi$, or $\rho_{\Pi'} < \rho_\Pi$), then Π is a CAS *realizing $\mathcal{A}$ with minimum cardinality of the primitive* *share set* (*minimum average information rate*, or *minimum worst information rate*), and we briefly call Π an *optimal* CAS for simplicity.

Definition 2: For $\mathcal{A}=\{\mathcal{Q},\mathcal{F}\}$, as the monotone property holds true, we define the *lower-qualified-family* $\mathcal{Q}_-$, the *super-forbidden-family* $\mathcal{F}^+$, and the *connected-super-forbidden-family* $\mathcal{F}^*$ of $\mathcal{A}$ as (5). As a contrast, we rename the minimal qualified family $\mathcal{Q}^-$ (maximal forbidden family $\mathcal{F}_+$, resp.) as the *super-qualified-family* (*lower-forbidden-family*, resp.) of $\mathcal{A}$.

$$\begin{cases} \mathcal{Q}_- = \{Q \notin \mathcal{F} : \forall p \in Q, Q-\{p\} \in \mathcal{F}\} \\ \mathcal{F}^+ = \{F \notin \mathcal{Q} : \forall p \in P-F, F\cup\{p\} \in \mathcal{Q}\} \\ \mathcal{F}^* = \{F^+ \in \mathcal{F}^+ : \exists F_+ \in \mathcal{F}_+, F_+ \subseteq F^+\} \end{cases} \tag{5}$$

Here is an example to help understand these notions. Let $\mathcal{A}$ be the AS with $\mathcal{Q}=\{Q\subseteq P:|Q|\geq 5\},\mathcal{F}=\{F\subseteq P:|F|\leq 2\}$, then the corresponding families are $\mathcal{Q}^-=\{Q\subseteq P:|Q|=5\},\mathcal{Q}_-=\{Q\subseteq P:|Q|=3\},\mathcal{F}^+=\mathcal{F}^*=\{F\subseteq P:|F|=4\}$ and $\mathcal{F}_+=\{F\subseteq P:|F|=2\}$.

From the definitions, one can check the correctness of the following claims.

Remark 1: For a complete AS $\mathcal{A}$, it must hold that $\mathcal{Q}^-=\mathcal{Q}_-,\mathcal{F}^+=\mathcal{F}^*=\mathcal{F}_+$.

Remark 2: If $F_+\in\mathcal{F}_+$, then there exists $F^+\in\mathcal{F}^+$ satisfying $F_+\subseteq F^+$.

Remark 3: $\mathcal{F}^*\subseteq\mathcal{F}^+$ and there exist AS's such that $\mathcal{F}^*\neq\mathcal{F}^+$. For example, let $P=\{p_1,p_2,p_3,p_4,p_5\}$, $\mathcal{Q}=\{Q\subseteq P:|Q|\geq 4\}$ and $\mathcal{F}_+=\{\{p_1,p_2\},\{p_3,p_4\},\{p_1,p_5\}\}$, then $\{p_2,p_3,p_5\}\in\mathcal{F}^+-\mathcal{F}^*$.

3.2. Cutting Down the Size of the BIP problems for Optimal CAS's

For any given $\mathcal{A}$, an optimal CAS can be derived from a BIP problem with $|J'|$ binaries and $|\mathcal{F}_+|$ constraints [14]. Next, we will show that such a CAS can be obtained via solving an even smaller sized BIP problem with $|\mathcal{F}^*|$ binaries and $|\mathcal{F}_+|$ constraints, whose variables (constraints, resp.) are based on the connected-super-forbidden-family (lower-forbidden-family, resp.) of $\mathcal{A}$.

Lemma 1: Let Π be a CAS realizing $\mathcal{A}$ with the collection of $X_\Pi=\{x_\Pi(j):j\in J\}$. If there exists an index $\bar{j}\in J$ such that $x_\Pi(\bar{j})\geq 1, P-P_{\bar{j}}\notin\mathcal{F}^*$, then there is another CAS Π' realizing $\mathcal{A}$ which is better than Π in the sense that $m_{\Pi'}\leq m_\Pi$, $\bar{\rho}_{\Pi'}<\bar{\rho}_\Pi$, $\rho_{\Pi'}\leq\rho_\Pi$ and $\rho_{\Pi'}(p)\leq\rho_\Pi(p),p\in P$.

Proof: Since $\mathcal{F}^*\subseteq\mathcal{F}^+$ and $P-P_{\bar{j}}\notin\mathcal{F}^*$, it follows that either $P-P_{\bar{j}}\in\mathcal{F}^+-\mathcal{F}^*$ or $P-P_{\bar{j}}\notin\mathcal{F}^+$ holds true. If $P-P_{\bar{j}}\in\mathcal{F}^+-\mathcal{F}^*$, then $\forall F\in\mathcal{F}_+, F\nsubseteq P-P_{\bar{j}}$, thus $F\cap P_{\bar{j}}\neq\emptyset$, i.e, $w(\bar{j},F)\geq 1$. Let Π' be a CAS with $x_{\Pi'}(\bar{j})=0,x_{\Pi'}(j)=x_\Pi(j),j\in J-\{\bar{j}\}$. As $w(\bar{j},F)\geq 1$ and Π realizes $\mathcal{A}$, from (4) we have $\sum_{w(j,F)=0,j\in J'}x_{\Pi'}(j)=\sum_{w(j,F)=0,j\in J'}x_\Pi(j)\geq 1$, and so Π' realizes $\mathcal{A}$ too. From (3), Π' is a candidate, and we finish the proof for this case.

Now assume that $P-P_{\bar{j}} \notin \mathcal{F}^{+}$, then there exists $S \subseteq P$ satisfying $S \subsetneq P_{\bar{j}}, P-S \in \mathcal{F}^{+}$. Let $S_0 = P_{\bar{j}}$, as $x_{\Pi}(\bar{j}) \geq 1$ and Π realizes $\mathcal{A}$, we have $P - S_0 \notin \mathcal{Q}$ because the primitive shares in the nonempty set $\Omega_{\Pi}(\bar{j})$ are not held by any participant in $P - S_0$. Since $P - S_0 \notin \mathcal{Q}, P - S_0 \notin \mathcal{F}^{+}$, there exists $p_{i_1} \in P-(P-S_0) = S_0$ such that $(P-S_0) \cup \{p_{i_1}\} = P-(S_0-\{p_{i_1}\}) \notin \mathcal{Q}$. Let $S_1 = S_0 - \{p_{i_1}\} \subsetneq S_0 = P_{\bar{j}}$, if $P-S_1 \in \mathcal{F}^{+}$, then $S = S_1$ is a good choice. Otherwise, from the fact that $P-S_1 \notin \mathcal{Q}, P-S_1 \notin \mathcal{F}^{+}$, there exists $p_{i_2} \in P-(P-S_1) = S_1$ satisfying $(P-S_1) \cup \{p_{i_2}\} = P-(S_1-\{p_{i_2}\}) \notin \mathcal{Q}$. Let $S_2 = S_1 - \{p_{i_2}\} \subsetneq S_1 \subsetneq P_{\bar{j}}$, if $P-S_2 \in \mathcal{F}^{+}$, then $S = S_2$ is a candidate. Otherwise, we can continue the process and get such a S because $|P_{\bar{j}}|$ is finite.

Denote $\tilde{j} \in J$ as the index such that $P_{\tilde{j}} = S$ and let Π' be a CAS satisfying (6).

$$x_{\Pi'}(\bar{j}) = 0, x_{\Pi'}(\tilde{j}) = 1, x_{\Pi'}(j) = x_{\Pi}(j), j \in J - \{\bar{j}, \tilde{j}\} \tag{6}$$

Then from (3) we have $m_{\Pi} - m_{\Pi'} = \delta_0$ and

$$\rho_{\Pi}(p_i) - \rho_{\Pi'}(p_i) = \begin{cases} \delta_0 & p_i \in P_{\tilde{j}} \\ \delta_1 & p_i \in P_{\bar{j}} - P_{\tilde{j}} \\ 0 & p_i \in P - P_{\bar{j}} \end{cases}$$

where $\delta_0 = (x_{\Pi}(\bar{j}) - x_{\Pi'}(\bar{j})) + (x_{\Pi}(\tilde{j}) - x_{\Pi'}(\tilde{j})) \geq 0$, $\delta_1 = (x_{\Pi}(\bar{j}) - x_{\Pi'}(\bar{j})) > 0$. And it follows that $m_{\Pi'} \leq m_{\Pi}$, $\bar{\rho}_{\Pi'} < \bar{\rho}_{\Pi}$, $\rho_{\Pi'} \leq \rho_{\Pi}$ and $\rho_{\Pi'}(p) \leq \rho_{\Pi}(p), p \in P$. Thus, if Π' does realize $\mathcal{A}$, i.e, the nonnegative integers of (6) satisfy condition (4), then the proof is complete.

As Π realizes $\mathcal{A}$, from (4) we have $x_{\Pi}(j) = 0, j \in J - J'$. Thus, if $\tilde{j} \in J'$, then $x_{\Pi'}(j) = 0, j \in J - J'$. And $\tilde{j} \in J'$ does hold. In fact, if $P - P_j \in \mathcal{F}^{+}$ then $j \in J'$. Otherwise, there exists $Q \in \mathcal{Q}^{-}$ with $w(j, Q) = 0$, which means that $P_j \cap Q = \emptyset$, i.e, $Q \subseteq P - P_j$. From the monotone property, $P - P_j \in \mathcal{Q}$ holds true, which is contrary to the fact of $P - P_j \in \mathcal{F}^{+}$.

Let $F \in \mathcal{F}_{+}$. If $w(\tilde{j}, F) = 0$ then $\sum_{w(j,F)=0, j \in J'} x_{\Pi'}(j) \geq x_{\Pi'}(\tilde{j}) = 1$. Otherwise, it holds that $P_{\tilde{j}} \cap F \neq \emptyset$ because $w(\tilde{j}, F) \geq 1$, together with the fact of $P_{\tilde{j}} = S \subsetneq P_{\bar{j}}$, we have $P_{\bar{j}} \cap F \neq \emptyset$, i.e, $w(\bar{j}, F) \geq 1$, and so, $\sum_{w(j,F)=0, j \in J'} x_{\Pi'}(j) = \sum_{w(j,F)=0, j \in J'} x_{\Pi}(j) \geq 1$. □

With Lemma 1, we have Theorem 1 as a conclusion.

Theorem 1: Denote $J^{*} = \{j \in J : P - P_j \in \mathcal{F}^{*}\} \subseteq J'$, then a CAS realizing $\mathcal{A}$ with minimum cardinality of the primitive share set (minimum average information rate, or minimum worst information rate) can be found in schemes satisfying (7). Moreover, each CAS satisfying (7) does realize $\mathcal{A}$.

$$\begin{cases} \forall j \in J - J^{*} : x_{\Pi}(j) = 0 \\ \forall j \in J^{*} : x_{\Pi}(j) \in \{0, 1\} \\ \forall F \in \mathcal{F}_{+} : \sum_{w(j,F)=0, j \in J^{*}} x_{\Pi}(j) \geq 1 \end{cases} \tag{7}$$

3.3. Optimal CAS's and the SCP

In this paragraph, we first give a brief introduction to the set covering problem [11] (one of the famous Karp's 21 NP-complete problems [15]), then show the relationship between the problem of finding optimal CAS's and the SCP, and finally arrive at Theorem 2, the main contribution of this paper.

Theorem 2: The problem of finding a CAS with minimum cardinality of the primitive share set (or minimum average information rate) is equivalent to the SCP, and thus is NP-hard.

Here is a brief introduction to the SCP.

Definition 3: [11] In a set covering system $\{U, \mathcal{V}, C\}$, there are a set U (called the universe), a family $\mathcal{V}$ of nonempty subsets of U such that $\bigcup_{V\in\mathcal{V}} V = U$ and a positive number set $C = \{c_V : V \in \mathcal{V}\}$ (called the cost set). A subset $\mathcal{V}'$ of $\mathcal{V}$ is called a cover of U if $\bigcup_{V\in\mathcal{V}'} V = U$, the cost of this cover is $\sum_{V\in\mathcal{V}'} c_V$. The set covering problem is to find a cover with minimum cost.

We call two set covering systems $\{U, \mathcal{V}, C\}$ and $\{U', \mathcal{V}', C'\}$ are isomorphic if there exist two bijective maps $f : U \mapsto U'$ and $g : \mathcal{V} \mapsto \mathcal{V}'$ such that $\forall V \in \mathcal{V}, g(V) = \{f(u) : u \in V\}$ and $\forall V_1, V_2 \in \mathcal{V}, c_{V_1}/c_{V_2} = c'_{g(V_1)}/c'_{g(V_2)}$.

There is a close relationship between the problem of find optimal CAS's and the SCP.

Definition 4: Given $\mathcal{A}$, the universe $U_{\mathcal{A}}$ and the family $\mathcal{V}_{\mathcal{A}}$ of subset of $U_{\mathcal{A}}$ are defined as $U_{\mathcal{A}} = \{u_{F_+} : F_+ \in \mathcal{F}_+\}$, $V_{F^*} = \{u_{F_+} \in U_{\mathcal{A}} : F_+ \subseteq F^*\} \neq \emptyset, F^* \in \mathcal{F}^*$ and $\mathcal{V}_{\mathcal{A}} = \{V_{F^*} : F^* \in \mathcal{F}^*\}$. For $\bar{J} \subseteq J^*$, let $\mathcal{V}(\bar{J}) = \{V_{F^*} \in \mathcal{V}_{\mathcal{A}} : F^* = P - P_j, j \in \bar{J}\}$ and $\Pi(\bar{J})$ be a CAS satisfying (8).

$$x_{\Pi}(j) = \begin{cases} 1 & j \in \bar{J} \\ 0 & j \in J - \bar{J} \end{cases} \tag{8}$$

Since $\bigcup_{V_{F^*}\in\mathcal{V}_{\mathcal{A}}} V_{F^*} = U_{\mathcal{A}}$ and $w(j, F) = 0 \Leftrightarrow P_j \cap F = \emptyset \Leftrightarrow F \subseteq P - P_j$, we have

Theorem 3: $\Pi(\bar{J})$ is a CAS satisfying (7) if and only if $\mathcal{V}(\bar{J})$ is a cover of $U_{\mathcal{A}}$.

Theorem 4: The problem of finding a CAS realizing $\mathcal{A}$ with minimum cardinality of the primitive share set can be done by solving the SCP of $\{U_{\mathcal{A}}, \mathcal{V}_{\mathcal{A}}, C\}$ where $C = \{c_V = 1 : V \in \mathcal{V}_{\mathcal{A}}\}$.

Theorem 5: The problem of finding a CAS realizing $\mathcal{A}$ with minimum average information rate can be solved by the SCP of $\{U_{\mathcal{A}}, \mathcal{V}_{\mathcal{A}}, C_{\mathcal{A}}\}$ where $C_{\mathcal{A}} = \{c_{V_{F^*}} = |P - F^*| = n - |F^*| : F^* \in \mathcal{F}^*\}$.

By now, we know that there is a set covering system $\{U_{\mathcal{A}}, \mathcal{V}_{\mathcal{A}}, C_{\mathcal{A}}\}$ corresponding to any given $\mathcal{A}$. Moreover, we have Theorem 6 on the reverse. And Theorem 2 is a corollary of Theorem 4, 5 and 6.

Theorem 6: Let $\{U, \mathcal{V}, C\}$ be a set covering system where C is a collection of positive rational numbers, then there exists an access structure $\mathcal{A}$ such that $\{U_{\mathcal{A}}, \mathcal{V}_{\mathcal{A}}, C_{\mathcal{A}}\}$ is isomorphic to $\{U, \mathcal{V}, C\}$.

Proof: We will prove Theorem 6 by constructing such an access structure. Suppose $U = \{1, 2, \cdots, |U|\}$, $\mathcal{V} = \{V_1, V_2, \cdots, V_{|\mathcal{V}|}\}$. And more, without loss of generality, suppose $c_V, V \in \mathcal{V}$ are coprime positive integers. Let d, l, s be positive integers satisfying $l \geq max\{((d|U|+|\mathcal{V}|)-(d|V|+1))/c_V : V \in \mathcal{V}\}$ and $s \geq max\{lc_V+(d|V|+1)-(d|U|+|\mathcal{V}|) : V \in \mathcal{V}\}$, denote $s_V = (d|U|+|\mathcal{V}|+s)-(d|V|+1)-lc_V, V \in \mathcal{V}$, then it follows that $0 \leq s_V \leq s$ and $(d|U|+|\mathcal{V}|+s)-(d|V|+1+s_V) = lc_V$. Now set

$$\begin{cases} n = d|U| + |\mathcal{V}| + s \\ P = \{p_1, \cdots, p_n\} \\ P(u) = \{p_{d(u-1)+1}, p_{d(u-1)+2}, \cdots, p_{du}\}, u \in U \\ P(V_i) = (\bigcup_{u \in V_i} P(u)) \cup \{p_{d|U|+i}\} \cup (\bigcup_{j=1}^{s_{V_i}} \{p_{d|U|+|\mathcal{V}|+j}\}) \end{cases}$$

then $\forall V \in \mathcal{V}, \forall u \in U$, we have

$$\begin{cases} |P(V)| = d|V| + 1 + s_V \\ |P - P(V)| = lc_V \\ P(u) \subseteq P(V) \Leftrightarrow u \in V \\ \forall u' \in U, u' \neq u : P(u) \nsubseteq P(u'); P(u') \nsubseteq P(u) \\ \forall V' \in \mathcal{V}, V' \neq V : P(V) \nsubseteq P(V'), P(V') \nsubseteq P(V) \end{cases}$$

Let $\mathcal{A}$ be the following AS,

$$\begin{cases} \mathcal{F} = \{F \subseteq P : \exists u \in U, F \subseteq P(u)\} \\ \mathcal{Q} = \{Q \subseteq P : \forall V \in \mathcal{V}, Q \nsubseteq P(V); \exists u \in U, P(u) \subseteq Q\} \end{cases}$$

then $\mathcal{A}$ is monotone, the corresponding $\mathcal{F}_+, \mathcal{F}^*$ of $\mathcal{A}$ are

$$\begin{cases} \mathcal{F}_+ = \{P(1), P(2), \cdots, P(|U|)\} \\ \mathcal{F}^* = \{P(V_1), P(V_2), \cdots, P(V_{|\mathcal{V}|})\} \end{cases}$$

and $\{U_\mathcal{A}, \mathcal{V}_\mathcal{A}, C_\mathcal{A}\}$ is isomorphic to $\{U, \mathcal{V}, C\}$. □

4. Optimal CAS's for Two Types of AS's

In this section, we will discuss two types of AS's whose optimal CAS's can be directly derived.

Let $\{U, \mathcal{V}, C\}$ be a set covering system, denote $\mathcal{V}(u) = \{V \in \mathcal{V} : u \in V\}, u \in U$, $U^* = \{u \in U : |\mathcal{V}(u)| = 1\}$ and $\mathcal{V}^* = \bigcup_{u \in U^*} \mathcal{V}(u)$. Then $\mathcal{V}^* \subseteq \mathcal{V}'$ holds true for every cover $\mathcal{V}'$ of U. And so we have

Theorem 7: If $\bigcup_{V \in \mathcal{V}_\mathcal{A}^*} V = U_\mathcal{A}$, then the CAS Π satisfying (9) attains the minimum m_Π, $\bar{\rho}_\Pi$, ρ_Π and $\rho_\Pi(p), p \in P$ simultaneously.

$$x_\Pi(j) = \begin{cases} 1 & P - P_j = F^*, V_{F^*} \in \mathcal{V}_\mathcal{A}^* \\ 0 & \text{others} \end{cases} \tag{9}$$

For every complete AS $\mathcal{A}$, since $\mathcal{F}^+ = \mathcal{F}^* = \mathcal{F}_+$ holds true, from Theorem 7 it holds that the CAS Π satisfying (9) is an optimal CAS. A careful observation will say that Π is just the one proposed in [3]. And we should like to notice that such a conclusion has been drawn in [14].

Next, we will introduce another type of AS's whose optimal CAS's can be obtained directly.

For simplicity, we denote $\text{AS}(b,t,n), b < t \leq n$ as the AS with $|P| = n$, $\mathcal{Q} = \{Q \subseteq P : |Q| \geq t\}$ and $\mathcal{F} = \{F \subseteq P : |F| \leq b\}$. Let Π be a CAS realizing $\text{AS}(b,t,n)$, then $m_\Pi \geq b+1$. Otherwise, by selecting just one participant in subset $\{p \in P : s \in \psi_\Pi(p)\}$ for each $s \in \Omega_\Pi$, a subset S is collected. Now S is a qualified subset with $|S| \leq m_\Pi \leq b$ because S contains all primitive shares.

Let Π' be a CAS realizing $\text{AS}(b,t,n)$ with minimum average information rate. From Theorem 1, we can further assume (7) holds true for Π'. From (3) we have $\bar{\rho}_\Pi \geq \bar{\rho}_{\Pi'} = \sum_{j \in J^*} w_j x_{\Pi'}(j)/n = (n+1-t)m_{\Pi'}/n \geq (n+1-t)(b+1)/n$.

If $(n+1-t)(b+1) \leq n$, then we can divide P into $b+2$ pieces, in each of the first $b+1$ pieces, there are exactly $n+1-t$ participants, and the last one contains all the left $n-(n+1-t)(b+1)$ participants. By constructing an ideal unanimous consent scheme with primitive share set $\Omega = \{s_1, \cdots, s_{b+1}\}$, and assigning $s_l, 1 \leq l \leq b+1$ to all participants in the l-th piece, we get a CAS Π. Now $m_\Pi = b+1, \bar{\rho}_\Pi = (n+1-t)(b+1)/n, \rho_\Pi = 1$. And Π realizes $\text{AS}(b,t,n)$. Thus, Π is an optimal CAS achieves the minimum m_Π, $\bar{\rho}_\Pi$, and ρ_Π at the same time.

As a special example, an optimal CAS for $\text{AS}(b,n,n)$ can be obtained directly.

5. A Greedy Algorithm to Find CAS's with smaller worst information rate

For a general incomplete AS $\mathcal{A}$, as mentioned in Section 3, we can construct an optimal CAS by solving the corresponding BIP problem. Moreover, a CAS with minimum cardinality of the primitive share set or minimum average information rate can be derived from the corresponding SCP, and all techniques for the SCP (e.g., [16], [17], [18], [19], [20], [21], [22]) work for these two cases.

We do not know whether the problem of finding CAS's with minimum worst information rate is NP-hard (although we believe it is NP-hard, we can not prove this until now). And we will propose here a greedy algorithm to find CAS's with smaller worst information rate. At each stage of this algorithm, a preferred subset is chosen.

To describe our algorithm, for $\mathcal{V}' \subseteq \mathcal{V}_\mathcal{A}$, we denote some notations as (10). And there are four rules be applied to giving the preference for the next stage. Among these rules, higher ones are prior to lower ones, i.e, if Rule(l) gives the preference then Rule$(l+1)$ is omitted. The ideal behind Rule(1) is to delay the increase of $\rho(\mathcal{V}')$, the purpose of Rule(2) is to expedite the covering, and Rule(3) tries to suspend the growth of the potential of $\rho(\mathcal{V}')$ measured by $f(F, \mathcal{V}')$.

$$\begin{cases} \rho(p, \mathcal{V}') = |\{V_{F^*} \in \mathcal{V}' : p \notin F^*\}|, p \in P \\ n(p, \mathcal{V}') = |\{q \in P : \rho(q, \mathcal{V}') < \rho(p, \mathcal{V}')\}|, p \in P \\ f(F, \mathcal{V}') = \sum_{p \in P-F} 2^{n(p, \mathcal{V}')}, F \subseteq P \\ \rho(\mathcal{V}') = max\{\rho(p, \mathcal{V}') : p \in P\} \\ U(\mathcal{V}') = \bigcup_{V \in \mathcal{V}'} V \\ L(\mathcal{V}') = \{V \in \mathcal{V}_{\mathcal{A}} : V \nsubseteq U(\mathcal{V}')\} \end{cases} \tag{10}$$

Let $V_{F_1}, V_{F_2} \in L(\mathcal{V}')$, then the rules are listed as below.

Rule(1): If $\rho(\mathcal{V}' \cup \{V_{F_1}\}) < \rho(\mathcal{V}' \cup \{V_{F_2}\})$, then V_{F_1} is better.

Rule(2): If $|V_{F_1} - U(\mathcal{V}')| > |V_{F_2} - U(\mathcal{V}')|$, then discard V_{F_2}.

Rule(3): If $f(F_1, \mathcal{V}') < f(F_2, \mathcal{V}')$, then we prefer to V_{F_1}.

Rule(4): Suppose $P_{j_1} = P - F_1, P_{j_2} = P - F_2$, choose V_{F_1} if $j_1 < j_2$.

Algorithm: Finding CAS's with smaller worst information rate

```
S0  Set $\mathcal{V}' = \mathcal{V}_{\mathcal{A}}^*$;
S1  If $L(\mathcal{V}') = \emptyset$ then stop, and $\mathcal{V}'$ is the corresponding cover. Otherwise, find the preferred subset
    $V \in L(\mathcal{V}')$ according to Rule(1)-Rule(4), replace $\mathcal{V}'$ with $\mathcal{V}' \cup \{V\}$ and process to S2;
S2  If there is $W \in \mathcal{V}' - (\mathcal{V}_{\mathcal{A}}^* \cup \{V\})$ satisfying $W \subseteq U(\mathcal{V}' - \{W\})$, go to S3; else process to S1;
S3  Replace $\mathcal{V}'$ with $\mathcal{V}' - \{W\}$ and process to S2;
```

6. Conclusion

We consider in this paper the problem of finding optimal CAS's for incomplete AS's. The paper introduces some notions including the connected-super-forbidden-family and the lower-forbidden-family for AS's. We show that an optimal CAS can be derived from some smaller sized BIP whose variables (constraints, resp.) are based on the connected-super-forbidden-family (lower-forbidden-family, resp.) of the given AS. The paper further builds the close relationship between the problem of finding optimal CAS's and the SCP. We prove that the problem of finding a CAS with minimum cardinality of the primitive share set (or minimum average information rate) is equivalent to the SCP, and thus is NP-hard.

Other contributions of the paper include: 1) two types of AS's are recognized so that we can construct the corresponding optimal CAS's directly; and 2) a greedy algorithm is proposed to find CAS's with smaller worst information rate. We do not know whether the problem of finding CAS's with minimum worst information rate is NP-hard, and leave it as an open problem.

Acknowledgment

The authors appreciate the supports from the National Natural Science Foundation of China under Grant Nos. 61070249, 60970111, 61133014 and 60803146.

References

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612–613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the 1979 AFIPS National Computer Conference*, vol. 48, 1979, pp. 313–317.

[3] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," in *IEEE Globecom*, 1987, pp. 99–102.

[4] E. F. Brickell and D. R. Stinson, "Some improved bounds on the information rate of perfect secret sharing schemes," *Journal of Cryptology*, vol. 5, pp. 153–166, 1992.

[5] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," *IEEE Transactions on Information Theory*, vol. 29, pp. 35–41, 1983.

[6] R. M. Capocelli, A. D. Santis, L. Gargano, and U. Vaccaro, "On the size of shares for secret sharing schemes," *Journal of Cryptology*, vol. 6, no. 3, pp. 157–167, 1993.

[7] L. Csirmaz, "The size of a share must be large," *Journal of Cryptology*, vol. 10, pp. 223–231, 1997.

[8] G. J. Simmons, W. A. Jackson, and K. M. Martin, "The geometry of shared secret schemes," *Bulletin of the Institute of Combinatorics and its Applications*, vol. 1, pp. 71–88, 1991.

[9] Q. Li, H. Yan, and K. F. Chen, “A new method of using (k,n)-threshold scheme to realize any access structure, (in chinese),” *Journal of Shanghai Jiaotong University*, vol. 38, no. 1, pp. 103–106, 2004.

[10] M. Iwamoto, H. Yamamoto, and H. Ogawa, “Optimal multiple assignments based on integer programming in secret sharing schemes,” in *Proc. ISIT ’04*, 2004, pp. 16–16.

[11] R. S. Garfinkel and G. L. Nemhauser, *Integer Programming*. John Wiley & Sons, New York, 1972.

[12] M. Naor and A. Shamir, “Visual cryptography,” in *Proc. EUROCRYPT ’94*, 1995, pp. 1–12.

[13] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Visual cryptography for general access structures,” *Information and Computation*, vol. 129, pp. 86–106, 1996.

[14] Q. Li, X. X. Li, D. Zheng, and K. F. Chen, “Optimal multiple assignments with (m,m)-scheme for general access structures,” Cryptology ePrint Archive, Report 2012/007, 2012.

[15] R. M. Karp, “Reducibility among combinatorial problems,” *Complexity of Computer Computations*, vol. 40, no. 4, pp. 85–103, 1972.

[16] M. L. Fisher and P. Kedia, “Optimal solution of set covering/partitioning problems using dual heuristics,” *Management Science*, vol. 36, no. 6, pp. 674–688, 1990.

[17] J. E. Beasley and K. Jornsten, “Enhancing an algorithm for set covering problems,” *European Journal of Operational Research*, vol. 58, pp. 293–300, 1992.

[18] E. Balas and M. C. Carrera, “A dynamic subgradient-based branch-and-bound procedure for set covering,” *Operations Research*, vol. 44, no. 6, pp. 875–890, 1996.

[19] D. S. Johnson, “Approximation algorithms for combinatorial problems,” in *Proc. STOC ’73*, 1973, pp. 38–49.

[20] V. Chvatal, “A greedy heuristic for the set-covering problem,” *Mathematics of Operations Research*, vol. 4, no. 3, pp. 233–235, 1979.

[21] J. E. Beasley and P. C. Chu, “A genetic algorithm for the set covering problem,” *European Journal of Operational Research*, vol. 94, pp. 392–404, 1996.

[22] A. Caprara, M. Fischetti, and P. Toth, “A heuristic method for the set covering problem,” *Operations Research*, vol. 47, no. 5, pp. 730–743, 1999.