DIMACS Technical Report 2001-35
October 2001

Secret Sharing and Hypergraph Decomposition

by

Giovanni Di Crescenzo[1] Clemente Galdi[2]

[1]Telcordia Technologies Inc., 445 South Street Morristown, New Jersey 07960, USA. DIMACS permanent member. email: giovanni@research.telcordia.com.
[2]Dipartimento di Informatica ed Applicazioni, Universitá di Salerno, 84081 Baronissi (SA), ITALY. email: clegal@unisa.it. Work done while visiting Telcordia Technologies. The visit of the author to Telcordia Technologies has been partially supported by DIMACS under grant NSF CCR 99-06105.

ABSTRACT

A secret sharing scheme is a protocol by which a dealer distributes a secret among a set of participants in such a way that only qualified sets of them can reconstruct the value of the secret whereas any non-qualified subset of participants obtain no information at all about the value of the secret. Secret sharing schemes have always played a very important role in the construction of higher level cryptographic primitives and protocols.

In this paper we investigate the construction of efficient secret sharing schemes by using a technique called *hypergraph decomposition*, extending in a non-trivial way the previously studied graph decomposition technique.

The application of this technique allows us to obtain secret sharing schemes for particular and large classes of access structures (such as hyperpaths, hypercycles, hyperstar and hypertrees) with dramatically improved efficiency over previous results. Specifically, in all cases, schemes obtained using previous techniques generate shares of exponential blowup in size, while for ours the blowup is always polynomial, in some cases even constant. Our schemes are also complemented by bounds on the blowup that are essentially tight.

In the course of the formulation of the hypergraph decomposition technique, we also obtain an elementary characterization of the ideal access structures among the hyperstar, which is of independent interest.

1 Introduction

A secret sharing scheme is a pair of efficient algorithms: a distribution algorithm and a reconstruction algorithm, run by a dealer and some parties. The distribution algorithm is executed by a dealer who, given a secret, computes some shares of it and gives them to the parties. The reconstruction algorithm is executed by a qualified subset of parties who, by putting together their own shares, can therefore reconstruct the secret. A secret sharing scheme satisfies the additional property that any non-qualified subset of participants does not obtain any information about the secret. The set of qualified subsets of parties is also called "access structure". The notion of secret sharing was introduced by Blackley [2] and Shamir [11], who considered the important case in which the set of qualified subsets of participants is the set of all subsets of size at least k, for some integer k.

Since their introduction, secret sharing schemes have been widely employed in the construction of more elaborated cryptographic primitives and several types of cryptographic protocols. Being so often employed, central research questions in this area are both the construction of efficient secret sharing schemes for several classes of access structures, and finding bounds on the possible efficiency that any such scheme can achieve for a certain access structure. The efficiency measures studied in the literature, and the ones that we will also consider in this paper, are related to the size of the largest distributed share (typically called "information rate", for its analogy with a so-called coding theory notion), or the sum of the distributed shares (typically called "average information rate"). The importance of these parameters is clear since they are directly related to the storage complexity, the communication complexity and the amount of secret information of the scheme. In the construction of efficient sharing schemes and in the search of bounds on such efficiency, the literature has paid special attention to the so-called "ideal" access structures; namely, access structures for which there exists a secret sharing scheme where the share distributed to each participant has the same size as the secret. (Note that this is well-known to be the best efficiency that one can achieve.) Further studied topics along these lines are: The classification of all access structures according to whether they are ideal or not, and the investigation of the efficiency of non-ideal access structures using ideal ones, using elegant techniques such as "graph decomposition".

In this paper we elaborate along this research direction by studying a non-trivial extension of the graph decomposition technique, which we call "hypergraph decomposition"; by applying this technique so to obtain secret sharing schemes that are dramatically more efficient than what previously known; and by finding novel and elementary characterization of ideal access structures within a large class of them.

Previous results. Secret sharing schemes have been proposed, for instance, in [11, 2] for threshold structures, in [12] for all graph-based access structures, in [1] for all monotone circuits, in [10] for all access structures. Lower bounds on the size of shares for all secret sharing schemes have been proposed, for instance, in [7, 3, 4] for certain graph-based access structures, and in [13, 9, 15] for other classes of access structures. A characterization of ideal access structures in terms of weighted matroids has been presented in [6]. The *graph* *decomposition* technique [12, 5] consists of decomposing a graph into smaller graphs whose union covers the original graph and representing ideal access structure. (We note that graphs can be associated to access structures containing subsets of size at most 2.)

Our results. Extending the above graph decomposition, we define *hypergraph decomposition*, a technique consisting of decomposing an hypergraph into smaller hypergraphs whose union covers the original hypergraph and representing ideal access structures. A secret sharing scheme for the original hypergraph can then be obtained by composing the schemes for the smaller ones. We note that since each access structure can be represented as an hypergraph, our technique potentially can be applied to any access structure (even those containing subsets of size larger than 2). Applying this technique requires (a) finding small hypergraphs which represent access structure and (b) finding the optimal decomposition of the input hypergraph into such smaller ones. As for (a), we consider simple structures such as hyperstars, and find a new and elementary condition that characterizes whether a given hyperstar is ideal or not. We prove (b) to be an NP-complete problem for general hypergraphs, but we note that it can be solved efficiently for special types of hypergraphs. We then move on to study special classes of access structures to which the hypergraph decomposition technique can be successfully applied. Specifically, we study hyperpaths, hypercycles, hyperstars and hypertrees (all generalizing their graph-based counterpart) and obtain efficient secret sharing schemes for these structures. We note that the share size blowup of these schemes is either a constant or a small polynomial, while it turns out to be exponentially small when applying previous techniques [10]. For all these special classes of access structure, we also present upper bounds on the size of shares, which either meet or almost meet the performance of the previously given secret sharing schemes.

Organization of the paper. In Section 2 we give all definitions of interest for the rest of the paper. In Section 3 we present the hypergraph decomposition technique along with some results concerning the application of this technique. In Section 4 we show the characterization of ideal hyperstar. In Sections 5 and 6 we apply the hypergraph decomposition technique to obtain secret sharing schemes for hyperpaths, hypercycles, hypertrees and hyperstars, and we also present lower bounds on the information rate and average information rate of these access structures.

2 Definitions and Preliminaries

In this section we review some basic definition and notations that will be used through the paper. Suppose $\mathcal{P}$ be a set of participants. We denote by $\mathcal{A}$ the set of subsets of players which we desire to be able to reconstruct the secret, thus $\mathcal{A} \subseteq 2^{\mathcal{P}}$. Each set in $\mathcal{A}$ is said to be an *authorized set* while each set not in $\mathcal{A}$ is called a *forbidden set*. We define the family of *minimal sets* as $\delta^{-}A = \{A \in \mathcal{A} : A \not\subset A', \forall A' \in \mathcal{A}\}$. The set $\mathcal{A}$ is called the *access structure* and $\delta^{-}\mathcal{A}$ is said to be its basis. We will deal only with access structures that are *monotone*, i.e., they satisfy the following property: If $B \in \mathcal{A}$ and $B \subseteq C \subseteq \mathcal{P}$ then $C \in \mathcal{A}$. Thus, in order to describe an access structure it is sufficient to describe its basis. Analogously, let

$\mathcal{B} = 2^{\mathcal{P}} \setminus \mathcal{A}$ be the family of forbidden sets. We can define the family of *maximal* forbidden sets as $\delta^{+}\mathcal{B} = \{B \in \mathcal{B} : B \not\supset B', \forall B' \in \mathcal{B}\}$.

Let $\mathcal{S}$ be a set of size q containing all the possible secrets to be shared. For every participant $P \in \mathcal{P}$ let us denote by S_P a set of size s_P containing all the possible information given to P be a secret sharing scheme. The elements in S_P are called shares. We will denote by P both the player in the access structure and the shares assigned to him. Suppose a *dealer* $D \notin \mathcal{P}$ wants to share a secret $s \in \mathcal{S}$ among the participants in $\mathcal{P}$. For each player in $P \in \mathcal{P}$ he selects one element in S_P and gives it to P. A secret sharing scheme is said to be *perfect* (with respect to the access structure $\mathcal{A}$) if the following conditions holds:

1 Any set $A \in \mathcal{A}$ of participants who pool their shares together can recover the secret s.
2 Any set $A \notin \mathcal{A}$ of participants who pool their share together obtain no information on s.

Notice that the security of the value s is to be intended in an information-theoretic sense. These two conditions can be expressed in a more compact form using the Shannon's entropy function (see [8] for a complete covering) as follows:

1 $H(S|A) = 0, \forall A \in \mathcal{A}$
2 $H(S|A) = H(S), \forall A \notin \mathcal{A}$

We will use two values for measuring the efficiency of a secret sharing schemes, the *information rate* and the *average information rate* we define shortly. Both these indices depends on the amount of information distributed to the participant. More formally, the information rate is defined as:

$$\rho = \frac{\log q}{\log \max\{s_P : P \in \mathcal{P}\}}$$

It is easy to see that in any perfect secret sharing scheme, $q \leq \max\{s_P : P \in \mathcal{P}\}$ and thus $\rho \leq 1$. A secret sharing scheme in which $\rho = 1$ is said to be *ideal*. An access structure having an ideal secret sharing scheme is also called ideal. Notice that as the (maximum) amount of information distributed to the players increases, the information rate decreases. Thus the closer the information rate is to one, the better the secret sharing scheme is.

The information rate considers only the "maximum size" among the share distributed to the players. Sometimes it could be more preferable to consider the average size of the share distributed by the secret sharing scheme. The *average information rate* is defined as:

$$\tilde{\rho} = \frac{|\mathcal{P}| \log q}{\sum_{P \in \mathcal{P}} \log s_P}$$

Since, in any perfect secret sharing scheme, for any $P \in \mathcal{P}$, $s_P \leq q$ it is immediate that $\tilde{\rho} \leq 1$. Moreover it is not hard to see that $\tilde{\rho} \geq \rho$.

Definition 1 (Hypergraphs) *A hypergraph H is a pair (V, E) where V is a non-empty set of vertices and $E = \{E_1, \ldots, E_m\} \subseteq 2^V$ is a set of hyperedges. The hypergraph is said to be connected if for any two vertices $u, v \in V$ there exists a hyperpath from u to v in H. More formally there exists a sequence $E_{i_1}, \ldots, E_{i_s}$ such that $u \in E_{i_1}$, $E_{i_j} \cap E_{i_{j+1}} \neq \emptyset$ for each $j = 1, \ldots, s-1$, and $v \in E_{i_s}$.*

Each access structure, $\mathcal{A} \subseteq 2^{\mathcal{P}}$, can be represented as a hypergraph $H = (\mathcal{P}, \mathcal{A})$ by letting each player being a vertex and each authorized set being represented as an hyperedge in the hypergraph.

Definition 2 (Induced Sub-Hypergraph) *Let $H = (V, E)$ be a hypergraph and let $W \subseteq V$. The hypergraph H' induced by W is defined as $H' = (V', E')$ where $E' = \{e \in E | e \cap W \neq \emptyset\}$ and $V' = \cup_{e \in E'} e$*

Let I be a set of hyperedges. We say that the region determined by the hyperedges in I is the set of vertices that belong to all the hyperedges in I and does not belong to any other hyperedge in the hypergraph. More formally:

Definition 3 (Region) *Let $H = (V, E)$ be a hypergraph. A set $R \subseteq V$ is said to be a region of H if and only if: there exists $I \subseteq E$ such that $R = \texttt{Region}(I) = (\cap_{E_i \in I} E_i) \setminus \cup_{E_i \in (E \setminus I)} E_i$. We will say that the hyperedges in I determine the region R. Moreover we say that R is an i-region if $|I| = i$.*

Definition 4 (Remove) *Let $H = (V, E)$ be a hypergraph and let R be one of its region. We define $\texttt{Remove}(H, R)$ to be hypergraph $H' = (V', E')$ where $V' = V \setminus R$ and $E' = \{E_i' = E_i \cap V'$ for any $E_i \in E\}$.*

Notice that, for any subset $W \subseteq \mathcal{P}$, the sub-hypergraph induced by W represents a minimal sub-access structure containing all the vertices in W. On the other hand it is important to notice that $\texttt{Remove}(H, R)$ is no longer a substructure of H. Indeed some forbidden sets with for H could be authorized sets for $\texttt{Remove}(H, R)$. It is immediate that the following holds:

Theorem 1 *Let $H = (V, E)$ be a hypergraph, $W \subseteq V$ and let H_W be the sub-hypergraph induced by W. Then $\rho(H) \leq \rho(H_W)$.*

We will extensively use some classes of hypergraph that we are going to define formally. These hypergraphs are a natural generalization of graphs like stars, paths and cycles.

Definition 5 (Hyperstar) *A Hypergraph $H = (V, E)$ is said to be a hyperstar if $A = \bigcap_{E_i \in E} E_i \neq \emptyset$. We will call A the center of the hyperstar.*

Definition 6 (HyperPath) *A hypergraph $H = (V, E)$, with $E = \{E_1, \ldots, E_m\}$ is said to be a hyperpath, if there exists an permutation $\pi : \{0, \ldots, m-1\} \to \{0, \ldots, m-1\}$ such that such that:*

- $E_{\pi(i)} \cap E_{\pi(i+1)} \neq \emptyset$ *for any* $i = 1, \ldots, m-1$
- $E_{\pi(i)} \cap E_{\pi(j)=\emptyset}$ *if* $j \notin \{i-1, i, i+1\}$ *and* $2 \leq i \leq m-1$.

Definition 7 (HyperCycle) *A hypergraph* $H = (V, E)$*, with* $E = \{E_0, \ldots, E_{m-1}\}$ *is said to be a hypercycle, if there exists an permutation* $\pi : \{0, \ldots, m-1\} \to \{0, \ldots, m-1\}$ *such that such that:*

- $E_{\pi(i)} \cap E_{\pi(i+1 \bmod m)} \neq \emptyset$
- $E_{\pi(i)} \cap E_{\pi(j)=\emptyset}$ *if* $j \notin \{i-1 \bmod m, i, i+1 \bmod m\}$.

We will denote by P_m the hyperpath with m hyperedges and by C_m the hypercycle with m hyperedges.

3 Hypergraph Decomposition

In this section we describe the technique of hypergraph decomposition. This technique is a generalization of graph decomposition studied in [5, 12]. Given an access structure $\mathcal{A}$, we can construct a secret sharing for it as follows. We first represent $\mathcal{A}$ as an hypergraph H. Then we decompose the hypergraph in smaller sub-hypergraphs $H_1, \ldots, H_k$ for which efficient (and possibly ideal) secret sharing schemes are known and such that all the edges in H belong to at least one of the H_i. In particular we will try to decompose hypergraphs into *ideal* hyperstars. Thus each participant will receive a certain number of shares by means of each sub-structure H_i. The secret sharing for H is thus obtained as a "union" of the secret sharing of all the H_i's. Indeed since all the hyperedges in H are covered by the decomposition, each authorized set will be able to reconstruct the secret. On the other hand, the security of the secret sharing scheme for H is guaranteed by the security of the secret sharing schemes for the H_i's and by the fact that these schemes are independent. Notice that the performance of the secret sharing scheme not only depends on the performance of the decomposition of $\mathcal{A}$, but also on "how" the sub-structure combine together.

We now define formally a hypergraph decomposition:

Definition 8 (Hypergraph Decomposition) *Let* $H = (V, E)$ *be a hypergraph and let* $\Delta = \{H_1, \ldots, H_k\}$ *be a set of sub-hypergraphs of* H*. The sequence* Δ *is said to be a decomposition of* H *if and only if each hyperedge in* H *belongs to at least one* H_i*. The decomposition is said to be ideal if the access structure represented each* H_i *is ideal. A decomposition* $\Delta = \{H_1, \ldots, H_k\}$ *of* H *is said to be a hyperstar decomposition of* H *if all the subhypergraphs* H_i *are hyperstars.*

We are now ready to give a generalization of some Theorems from [5]. The first theorems allows to evaluate the information rate and the average information rate that can be achieved by a secret sharing scheme for an access structure $\mathcal{A}$ having a decomposition of the hypergraph representing $\mathcal{A}$.

The second theorem states that, having a number of distinct decompositions of a hypergraph, it is possible to construct secret sharing schemes that improve the average information rate w.r.t. the algorithm that use a single hypergraph decomposition.

Theorem 2 (Hypergraph Decomposition Construction) *Suppose $H = (V, E)$ is a hypergraph and $\Delta = \{H_1, \ldots, H_k\}$ be an ideal decomposition of H. For $1 \leq i \leq k$, denote by $\{B_{i1}, \ldots, B_{ij_i}\}$ the set of all regions in H_i and $t_i = \max\{|B_{i1}|, \ldots, |B_{ij_i}|\}$ and let $t = \max\{t_i : 1 \leq i \leq k\}$. For every vertex v define: $R_v = |\{i : v \in H_i\}|$ and $R = \max\{R_v : v \in V\}|$. Then for $\rho = 1/R$ and $\widetilde{\rho} = |V| / \sum_{v \in V} R_v$ there exists a perfect secret sharing for H with information rate ρ (resp. average information rate $\widetilde{\rho}$) for a secret selected by a set of size q, for any prime power $q \geq t$*[1].

Theorem 3 (Multiple Hypergraph Decomposition Construction) *Suppose $H = (V, E)$ is a hypergraph and for $1 \leq j \leq \ell$ let $\Delta_j = \{H_{j1}, \ldots, H_{jk_j}\}$ be an ideal decomposition of H. For $1 \leq j \leq \ell$ and $1 \leq i \leq k_j$, denote by $\{B_{ji1}, \ldots, B_{jir_{ij}}\}$ the set of all regions in H_{ji} and $t_{ji=} \max\{|B_{ji1}|, \ldots, |B_{jir_{ji}}|\}$ and let $t = \max\{t_{ji} : 1 \leq j \leq \ell, 1 \leq i \leq k_j\}$. For every vertex v define: $R_{jv} = |\{i : v \in H_{ji}\}|$ and $R_v = \sum_{j=1}^{\ell} R_{jv}$ $R = \max\{R_v : v \in V\}|$. Then for $\rho = \ell/R$ there exists a perfect secret sharing for H with information rate ρ for a secret selected by a set of size q, for any prime power $q \geq t$.*

The proof of these theorem is an extension of the proofs of the cited theorems. In order to apply the hypergraph decomposition construction to a certain class of access structures, we have to solve the following two main problems.

- Define classes of ideal hypergraph-based access structures for which it is possible to construct in polynomial time an ideal secret sharing scheme.
- Represent the class of access structures given as a class of hypergraphs and find in polynomial time the optimal decomposition of these hypergraphs using only the ideal structures previously defined.

4 Hyperstars

In this section we give a complete characterization of the hyperstars having an ideal secret sharing scheme. We will begin by characterizing hyperstars with three hyperedges and we will then extend this result to hyperstars with any number of hyperedges. We will show that it is possible in polynomial time to decide whether a given hyperstar represents an ideal access structure on not. This gives a new (and more elementary than [6]) characterization of ideal structures within this specific class of structures.

We further give an algorithm that, on input an access structure $\mathcal{A}$ representable as an ideal hyperstar, realizes an ideal secret sharing scheme for it.

[1] Roughly speaking, the reason for which q must be greater or equal to t is the following: The secret is often written as the sum of two shares. Each share is eventually assigned to a unique region and we use a threshold scheme to share this value among the players in that region. Thus we need that the field from which the secret is chosen must be as large as the biggest region in the hypergraph. This remark applies to the following theorem as well.

4.1 Hyperstar with 3-edges

In this section we completely characterize hyperstars with three hyperedges. In particular we shall show a necessary and sufficient condition for the existence of an ideal secret sharing scheme for the access structure such hypergraph represents.

Let $H = (V, E)$ be a hyperstar and $E = (E_1, E_2, E_3)$. By Definition 2, there exists a non-empty 3-region, say $A = E_1 \cap E_2 \cap E_3$. One of the following two cases can arise:

1 There exists at most one 2-region, i.e a pair $\{i, j\}$, with $i \neq j$, such that $(E_i \cap E_j) \setminus A \neq \emptyset$;
2 There exist at least two 2-regions, i.e., there exists at least two pairs $\{i_1, j_1\} \neq \{i_2, j_2\}$, with $i_l \neq j_l$, such that $(E_{i_l} \cap E_{j_l}) \setminus A \neq \emptyset$, for $l = 1, 2$.

We shall show that ideal secret sharing schemes exists only for cases 1 while, for case 2, we prove that it is not possible to construct such a scheme. We shall show the following:

Theorem 4 *Let H be a hyperstar with 3 hyperedges. There exists an ideal secret sharing scheme for H if and only if H contains at most one 2-region.*

We split the proof of this theorem in the following lemmas. The first lemma gives the algorithm for the ideal secret sharing scheme for an ideal hyperstar with 3 hyperedges. The idea of the algorithm is the following: Let A be the center of the hyperstar and let s be the secret to be shared. We write $s = s_1 + s_2$ and we share s_1 among the players in A, and s_2 using the access structure $\texttt{Remove}(H, A)$. Of course, if H is an ideal access structure, so must be $\texttt{Remove}(H, A)$.

Lemma 5 *Let H be a hyperstar with 3 hyperedges. If H contains at most one 2-region then there exists an ideal secret sharing scheme for H.*

Proof. We can have the following cases:

- H contains no 2-regions. Since H does not contain any 2-region, each of its vertex either belongs to the center of the hyperstar or belongs to exactly one hyperedge. Thus the access structure described by H can be written as $\mathcal{A} = \{AB_1, AB_2, AB_3\}$ where B_1, B_2, B_3 constitute a partition of $\mathcal{P} \setminus A$. To share a secret s with this access structure, we write $s = s_1 + s_2$ and use an $(|A|, |A|)$-threshold scheme to share s_1 among all the players in A. We have to share s_2 according to the access structure $\texttt{Remove}(\mathcal{A}, A) = \{B_1, B_2, B_3\}$. Since B_i and B_j are disjoint, for any $i \neq j$, for any $j = 1, 2, 3$, we will share s_2 among the players in B_j using an independent $(|B_j|, |B_j|)$-threshold scheme. Since the threshold schemes are ideal and since independent schemes are applied to disjoint sets of players, the resulting scheme is ideal.
- H contains exactly one 2-region. This case is shown in Figure 1(a). The access structure can be written as $\mathcal{A} = \{ABD, ABE, AC\}$. In this case we write $s = s_1 + s_2$ and share s_1 among the players in A using a $(|A|, |A|)$-threshold scheme. At this point we share s_2 using this new access structure $\mathcal{B} = \{BD, BE, C\}$. Notice that the hypergraph

representing $\mathcal{B}$ is not connected. Thus we use a $(|C|, |C|)$-threshold scheme to share s_2 among the players in C. We then write $s_2 = s_3 + s_4$ and share s_3 among the players in B and s_4 among the players of $\texttt{Remove}(\mathcal{B}, B) = \{D, E\}$. But, since D and E are disjoint, we can share s_4 among the player in D using a $(|D|, |D|)$-threshold scheme and among the player in E using a $(|E|, |E|)$-threshold scheme

■

Notice that this lemma actually shows an ideal secret sharing scheme for a simple structure like the 3-edges hyperstar. The performance of this scheme improves on the result presented in [10]. Indeed, for this access structure, while the algorithm presented in this paper distributes to all each player exactly one share, the scheme presented in [10] distributes to some player a quadratic number of shares. For a more detailed description please refer to Appendix A.

In order to show that an access structure cannot be ideal, we need to prove that for any secret sharing scheme, there exists some player in the structure that receives a share whose size is strictly greater than the share size.

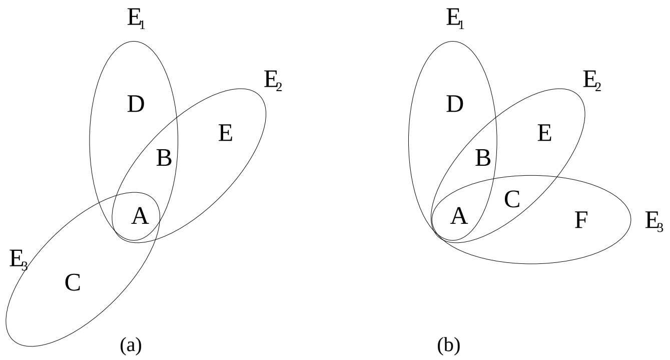

Figure 1: Hyperstar with 3 hyperedges with (a) with one 2-region and (b) with two 2-regions

The proof of the following lemmas are reported here mainly for self-containment.

Lemma 6 ([7]) *Let $\mathcal{A}$ be an access structure for a secret S and let X and Y such that $Y \notin \mathcal{A}$ and $X \cup Y \in \mathcal{A}$. Then $H(X|Y) = H(S) + H(X|YS)$*

Proof. Consider the mutual information:

$$\begin{aligned} I(X;S|Y) &= H(X|Y) - H(X|SY) \\ &= H(S|Y) - H(S|XY) \end{aligned}$$

We can thus write:

$$\begin{aligned} H(X|Y) &= H(S|Y) - H(S|XY) + H(X|SY) \\ &= H(S|Y) + H(X|SY) \end{aligned}$$

Where $H(S|XY) = 0$ since $X \cup Y \in \mathcal{A}$. ■

Lemma 7 ([7]) *Let $\mathcal{A}$ be an access structure for a secret S and let X and Y such $X \cup Y \notin \mathcal{A}$ then $H(X|Y) = H(X|YS)$*

Proof. Since $X \cup Y \notin \mathcal{A}$, $H(S|Y) = H(S|XY) = H(S)$. Thus $I(X; S|Y) = H(X|Y) - H(X|SY) = H(S|Y) - H(S|XY) = 0$ ■

Lemma 8 *Let $H = (V, E)$ be a hyperstar with three hyperedges. If H contains at least two 2-regions, B_1 and B_2, then for any $P_i \in B_1$ and for any $P_j \in B_2$, it holds that $H(P_i) + H(P_j) \geq 3H(S)$.*

Proof.

Since $H = (V, \{E_1, E_2, E_3\})$ is a hyperstar with three hyperedges, there exists a non-empty 3-region A that is common to all the hyperedges. Moreover, by hypothesis, there are at least two 2-regions. Assume that there are exactly two 2-regions are defined by the pairs (E_1, E_2) and (E_2, E_3) (see Figure 1(b)). The access structure can thus be written as $\mathcal{A} = \{ABD, ABCE, ACF\}$, where $A = E_1 \cap E_2 \cap E_3$, $B = (E_1 \cap E_2) \setminus A$ and $C = (E_2 \cap E_3) \setminus A$, and D, E, F are disjoint subsets of $\mathcal{P} \setminus A \cup B \cup C$. Notice that, since A, B, C are regions in H, they must be disjoint subsets of $\mathcal{P}$. Let us write $B = \{P_1, \ldots, P_b\}$ and $C = \{P_{b+1}, \ldots, P_c\}$ and $B' = B \setminus \{P_b\}$ and $C' = C \setminus \{P_c\}$.

$$
\begin{aligned}
H(S) &\leq H(P_c|ADEFB'C') \text{ (by Lemma 6)} \\
&\leq H(P_c|ADEB'C') \\
&= H(P_c|ADEB'C'S) \text{ (by Lemma 7)} \\
&\leq H(P_bP_c|ADEB'C'S) \\
&= H(P_b|ADEB'C'S) + H(P_c|ADEB'C'SP_b) \\
&\leq H(P_b|ADB'S) + H(P_c|AEBC'S) \\
&= H(P_b|ADB') - H(S) + H(P_c|AEBC') - H(S) \text{ (by Lemma 6)} \\
&\leq H(P_b) + H(P_c) - 2H(S).
\end{aligned}
$$

Using similar arguments it is possible to prove the same result also when H contains three 2-regions. Since a three-edge hypergraph cannot have more than three 2-region, the proof is completed. ■

At this point we can derive immediately the same bounds for hyperpaths and hypercycles of length three. Indeed, a hyperpath with three hyperedges can be seen as a hyperstar with three hyperedges and two 2-regions in which the center is empty. Similarly, a hypercycle can be seen as a hyperstar with three hyperedges, three 2-region and and "empty" center. From this observation we can derive the following:

Corollary 9 *Let H be a hyperpath with 3 hyperedges and let B_1, B_2 its 2-regions. Then, for any $P_i \in B_1$ and $P_j \in B_2$ it holds that: $H(P_i) + H(P_j) \geq 3H(S)$.*

Corollary 10 *Let H be a hypercycle with 3 hyperedges and let B_1, B_2, B_3 its 2-regions. Then, for any $P_i \in B_r$ and $P_j \in B_s$ it holds that: $H(P_i) + H(P_j) \geq 3H(S)$.*

Given these results on non-ideal connected hypergraphs with three hyperedges we can derive a lower bound on the numbers of share distributed to the players by any secret sharing scheme for these class of hypergraphs.

Corollary 11 *Let $H = (V, E)$ be a connected hypergraph with three hyperedges and at least two 2-regions. Denote by B_1, B_2, B_3 the 2-regions of H and by $w_i = |B_i|$ It holds that:*

$$\sum_{v \in V} H(X_v) \geq \mid V \mid H(S) + \min\{w_1, w_2, w_3\} H(S)$$

Proof. W.l.o.g. assume that $w_1 = \min\{w_1, w_2, w_3\}$. By Lemma 8 and Corollary 9, for any $P_i \in B_1$ and any $P_j \in B_2$, it holds that $H(P_i) + H(P_j) \geq 3H(S)$. We can write $B_1 = \{P_1 \ldots, P_{w_1}\}$ and $B_2 = \{P_{w_1+1} \ldots, P_{w_1+w_2}\}$. Thus:

$$\begin{aligned}
\sum_{i \in V} H(P_i) &= \sum_{i \in V \setminus \{B_1 \cup B_2\}} H(P_i) + \sum_{i \in B_1 \cup B_2} H(P_i) \\
&= \sum_{i \in V \setminus \{B_1 \cup B_2\}} H(P_i) + \sum_{i=1}^{w_1} (H(P_i) + H(P_{w_1+i})) + \sum_{i=w_1+1}^{w_2} H(P_{w_1+i}) \\
&\geq \sum_{v \in V \setminus \{B_1 \cup B_2\}} H(S) + 3 \sum_{i=1}^{w_1} H(S) + \sum_{i=w_1+1}^{w_2} H(S) \\
&\geq \sum_{v \in V \setminus \{B_1 \cup B_2\}} H(S) + \sum_{v \in B_1} H(S) + \sum_{v \in B_2} H(S) + \sum_{i=1}^{w_1} H(S) \\
&= \sum_{i \in V} H(S) + w_1 H(S)
\end{aligned}$$

■

Theorem 12 *Let $H = (V, E)$ be a hyperstar with three hyperedges and at least two 2-regions. Let B_1, B_2, B_3 the 2-regions of H and denote by $w_i = |B_i|$. It holds that:*

$$\tilde{\rho}\,(H) \leq \frac{|V|}{|V| + \min\{w_1, w_2, w_3\}}$$

Proof. By definition, $\tilde{\rho}\,(H) = \frac{|V| H(S)}{\sum_{v \in V} H(P_v)}$. But by Corollary 11,

$$\begin{aligned}
\sum_{v \in V} H(P_v) &\geq \mid V \mid H(S) + \min\{w_1, w_2, w_3\} H(S) \\
&= (|V| + \min\{w_1, w_2, w_3\}) H(S)
\end{aligned}$$

from which the theorem follows. ■

4.2 Hyperstars with n hyperedges

In the previous section we have shown a necessary and sufficient condition for a three-edges hyperstar to have an ideal secret sharing scheme. In this section we will present a generalization of this condition to the case on n-edges hyperstars.

The key idea of the generalization is the fact that if a hyperstar H contains a non-ideal sub-hypergraph, than H itself cannot be ideal. On the other hand we need an algorithm that, given an ideal hyperstar, distributes to each player a share of the same size of the secret. We start by proving the condition under which a hyperstar is not ideal.

Lemma 13 *Let $H = (V, E)$ be a hyperstar with $|V| = n$, $E = (E_1, \ldots, E_m)$ and let $B_1, \ldots, B_p$ be the set of all regions in H. Denote by $I_j \subseteq E$ the set of hyperedges determining B_j. If there exists two non-empty sets I_{j_1} and I_{j_2} such that $I_{j_1} \cap I_{j_2} \neq \emptyset$, $I_{j_1} \setminus I_{j_2} \neq \emptyset$ and $I_{j_2} \setminus I_{j_1} \neq \emptyset$, then there exist two players P_i and P_j such that $H(P_i) + H(P_j) \geq 3H(S)$.*

Proof. Assume w.l.o.g. that $j_1 = 1$ and $j_2 = 2$. By hypothesis there exists three hyperedges E_i, E_j, E_k such that:

1 $E_i \in I_1 \cap I_2$
2 $E_j \in I_1$ and $E_j \notin I_2$,
3 $E_k \notin I_1$ and $E_j \in I_2$,

Since H is a hyperstar, $E_i \cap E_j \cap E_k \neq \emptyset$, thus these three hyperedges constitute a 3-edge hyperstar with two non-empty regions constituted by the pair (E_i, E_j) and (E_i, E_k). Thus the lemma follows by by Theorem 1 and by Theorem 4. ∎

We shall now show that if the condition of the previous lemma does not hold, there exists an ideal secret sharing scheme for the hypergraph H. Let us write formally the statement of the lemma.

Lemma 14 *Let $H = (V, E)$ be a hyperstar with $|V| = n$, $E = (E_1, \ldots, E_m)$ and let $B_0, \ldots B_p$ be the set of all regions in H with B_0 being the center of H. Denote by $I_j \subseteq E$ the set of hyperedges determining B_j. If for each pair of sets I_{j_1} and I_{j_2} it holds that either $I_{j_1} \cap I_{j_2} = \emptyset$ or $I_{j_1} \subseteq I_{j_2}$ (or $I_{j_2} \subseteq I_{j_1}$), then* `Remove`$(H, B_0)$ *is the union of disjoint ideal hyperstars.*

Proof. Since H is a hyperstar and since the center of the H, B_0, is induced by all the hyperedges in H, $I_0 = E$. Consider the hypergraph H' =`Remove`(H, B_0) and consider the set B' of regions in H'. It is immediate that $B' = \{B_1, \ldots B_p\}$, i.e. the regions in H' are all the regions of H but B_0 that has been removed from H. It follows that, for any $j = 1, \ldots, p$ it is possible to create a 1-to-1 mapping between the set of hyperedges I_j determining the region B_j and the set of hyperedges I'_j determining the region B'_j. More precisely, if $I_j = \{E_{j_1}, \ldots, E_{j_k}\}$, then $I'_j = \{E'_{j_1}, \ldots, E'_{j_k}\}$. Notice that since the removal of vertices from the hyperedges does not affect the properties of the sets determining the regions. In other words:

$$I_{j_1} \cap I_{j_2} = \emptyset \implies I'_{j_1} \cap I'_{j_2} = \emptyset \quad (1)$$

$$I_{j_1} \subseteq I_{j_2} \implies I'_{j_1} \subseteq I'_{j_2} \quad (2)$$

Consider now $I'_{max} \subseteq I'$ be the set of *maximal* sets in I', i.e. $I'_j \in I'$ if and only if there exists no $I'_p \in I'$ such that $I'_j \subseteq I'_p$. Assume w.l.o.g. $I'_{max} = \{I'_1, \ldots, I'_q\}$ with $q \leq p$. By Equation 2, each elemente in I' is either in I'_{max}, i.e. is maximal, or is contained in a maximal element. Moreover, by Equation 1, the elements in I'_{max} are disjoint thus each hyperedge of H' belongs to exactly one set $I_j \in I'_{max}$.

Thus, for any $I'_j \in I'_{max}$, the hyperedges in I'_j share a common region, namely $\texttt{Region}(I_j)$. Moreover, for any $I'_{j_1}, I'_{j_2} \in I'_{max}$, the set of hyperedges contained in I'_{j_1} is disjoint from the hyperedges in I'_{j_2}. ■

This Lemma immediately suggests an algorithm that allows to construct an ideal secret sharing scheme for an ideal hyperstar. Roughly speaking, given an ideal hyperstar H, the algorithm applies a `Remove` operation on the center B_0 of H obtaining a set of disjoint (ideal) hyperstars. We write s as $s_1 + s_2$, and share s_1 among the players in the center using a $(|B_0|, |B_0|)$-threshold scheme, and s_2 among the remaining players of H. Since the hypergraph graph obtained is the union of a set of disjoint ideal hyperstars, we can apply recursively the same algorithm to each of these hyperstars with secret s_2.

However, there are two algorithmic issues to take into account when dealing with this algorithm. The first one is partitioning the players into disjoint regions. In Appendix B we show that this task can be accomplished in polynomial time in the number of hyperedges and the number of players. A second problem is an algorithm to verify that a given hyperstar is ideal. But, given the decomposition in regions of the hyperstar, this problem can be easily solved in polynomial time.

5 Average Information Rate

In this section we will give some bounds on the average information rate for general access structures. We will first show that finding the optimal hyperstar decomposition of a general hypergraph is an NP-Hard task. We will then present efficient secret sharing schemes for some classes of hypergraphs, namely hyperpaths, hypercycles and hypertrees. The improvement of our solution with respect to previoustly known secret sharing schemes is in some cases exponential. We also present the upper bounds on the average information rate for these classes of hypergraph.

5.1 NP-Hardness of Optimal Decomposition

As mentioned above, a crucial step towards constructing a secret sharing scheme for a general access structure is to find a decomposition of the hypergraph into ideal sub-hypergraphs. We first notice that, given a hypergraph $H = (V, E)$ and one of its ideal hyperstar-decomposition

$\Delta = \{H_1, \ldots, H_k\}$, with $H_i = (V_i, E_i)$ the average information obtained by applying the decomposition construction is $\widetilde{\rho}\,(H) = |V|/(\sum_{v \in V} R_v) = |V|/(\sum_{i=1}^{k} |V_i|)$. Thus in order to maximize the quantity $\widetilde{\rho}\,(H)$, we need to minimize $\sum_{i=1}^{k} |V_i|$.

Theorem 15 *Let $H = (V, E)$ be a hypergraph. Finding the ideal hyperstar decomposition $\Delta = (H_1, \ldots, H_k)$ where $H_i = (V_i, E_i)$ that minimizes the value $\sum_{i=1}^{k} |V_i|$ is NP-Hard.*

Proof. Let H is a 2-regular hypergraph, i.e., H is actually a graph, then H_i will be a star-graph, thus $|V(H_i)| = 1 + |E(H_i)|$. Recall that any access structure described by hyperstar graph is ideal. Thus solving the problem of finding the minimal hyperstar decomposition in this case is equivalent to find the minimal star-decomposition on graphs that, in turn, authors in [5] proved to be equivalent to finding the minimum vertex cover. ∎

5.2 Lower Bounds on the Average Information Rate

In this section we present some lower bounds on the average information rate for some classes of hypergraphs. Notice that a lower bound on the average information rate is obtained by giving an *upper* bound on the total size of the shares distributed by a secret sharing scheme. Thus in order to obtain a lower bound on the average information rate we need to present and analyze algorithms for secret sharing schemes on given structures.

5.2.1 The case of hyperpaths

In this section we give an algorithm for finding the optimal hyperstar decomposition of a particular class of hypergraphs: the hyperpaths.

Let P_m be a hyperpath and let $(E_1 \ldots, E_m)$ be its hyperedges. Let us denote $A_1, \ldots, A_m$ and $B_1, \ldots, B_{m-1}$ be, respectively, its 1 and 2-regions. We can write $E_1 = A_1B_1$, $E_i = B_{i-1}A_iB_i$ and $E_m = B_{m-1}A_m$. We notice that the hyperstar partitioning of the hyperpath can be represented simply by the set of centers of the hyperstars. Indeed choosing A_i as center of a hyperstar will result in a hyperstar with one edge, namely, $B_{i-1}A_iB_i$. On the other hand, choosing an hyperstar with center B_i will always result in a hyperstar with two hyperedges. It is immediate that, in any minimal hyperstar decomposition $\Delta = \{H_1, \ldots, H_k\}$, each hyperedge in the hypergraphs belongs to exactly one H_i. As a result of this, all the players that belong to one hyperedge (i.e., all the players in A_i for any i) will receive exactly one share. On the other hand, the vertices with degree two (i.e., all the players in B_i for any i), could receive either one or two shares. The following lemmas will characterize the sets of 2-regions belonging to the optimal hyperstar decomposition.

We will denote by $Cost(\Delta)$ the number of shares distributed by the algorithms, i.e., $Cost(\Delta) = \sum_{i=1}^{k} |V_i|$, where V_i denotes the set of vertices of the hypergraph H_i. Moreover, we will denote by $w_i = |B_i|$, i.e., the number of vertices in the region B_i.

Lemma 16 *In any minimum cost hyperstar decomposition Δ, there exists no i such that $\{B_{i-1}, A_i\} \subseteq \Delta$ or $\{A_i, B_i\} \subseteq \Delta$.*

Proof. By the way of contradiction assume that $\{A_i, B_i\} \subseteq \Delta$. We notice that the hyperedge $E_i = B_{i-1}, A_i, B_i$ belongs to two hyperstars in the decomposition, namely the one with center A_i and the one with center B_i. Thus if we remove the former by the hyperstar partitioning we still obtain a hyperstar partitioning of the hypergraph with smaller cost. ■

Lemma 17 *In any minimum cost hyperstar decomposition Δ, there exists no i such that $\{B_i, B_{i+1}\} \subseteq \Delta$.*

Proof.

Assume such i exists and consider the subparh $...A_{i-1}B_{i-1}A_iB_iA_{i+1}B_{i+1}A_{i+2}B_{i+2}...$

The cost of the hyperstar decomposition Δ can be computed as: $Cost(\Delta) = 2w_{i-1} + 2w_i + 2w_{i+1} + 2w_{i+2} + Cost(\Delta \setminus \{B_{i-1}, B_i\})$

Since $B_i \in \Delta$ and $B_{i+1} \in \Delta$, players in B_i receives 2 shares it receives one share from its hyperstar and one share because it is a part of the hyperstar with center B_{i+1}. Similar arguments apply for the players in B_{i+1}.

On the other hand, consider $\Delta' = \Delta \cup \{A_i\} \setminus \{B_i\}$. If Δ is a hyperstar partition of H so is Δ'. Indeed, removing B_i from Δ will result in a "partial" decomposition of H in which the hyperedge $E_i = B_{i-1}A_iB_i$ does not belong to any hyperstar (the hyperedge E_{i+1} still belongs to the hyperstar with center B_{i+1}).

Thus by adding A_i we ensure that all the hyperedges in H are covered by at least one star. Moreover,

$Cost(\Delta') = 2w_{i-1} + 2w_i + w_{i+1} + 2w_{i+2} + Cost(\Delta \setminus \{B_{i-1}, B_i\}) < Cost(\Delta)$ ■

Notice that Lemma 16 and Lemma 17 implies that in any optimal hyperstar decomposition, any player in B_i will receive one share if and only if B_i is the center of a hyperstar. Indeed, if this is not the case, B_i is the region defined by the hyperedges E_i and E_{i+1} thus all the players in B_i will receive one share from the hyperstar to which E_i belongs to and another share from the hyperstar to which E_{i+1} belongs to.

Since, for any i, all the players in A_i receive exactly one share, we can thus restate the problem of hyperstar decomposition as the problem of finding the subsets of 2-regions that will be the centers of stars. Once we have found this set, we can simply add to the hyperstar decomposition all the hyperedges that do not belong to any hyperstar, i.e., add to the Δ all the A_i's that do not belong to any hyperstar.

Before giving the algorithm we need this technical lemma.

Lemma 18 *In any minimum cost hyperstar decomposition Δ for P_m, $\{B_{i-1}, B_i, B_{i+1}\} \cap \Delta \neq \emptyset$, for any i.*

Proof.

Assume that there exists i such that $\{B_{i-1}, B_i, B_{i+1}\} \cap \Delta = \emptyset$. The cost of this solution is:

$$\begin{aligned}
Cost(\Delta) &= 2w_{i-1} + 2w_{i-1} + 2w_{i-1} + Cost(\Delta \setminus \{B_{i-1}, B_i, B_{i+1}\}) \\
&\geq 2w_{i-1} + w_{i-1} + 2w_{i-1} + Cost(\Delta \setminus \{B_{i-1}, B_i, B_{i+1}\}) \\
&= Cost(\Delta')
\end{aligned}$$

where $\Delta' = \Delta \cup \{B_i\}$. Thus Δ is not a minimum cost decomposition for P_m.

■

Lemma 17 actually states that in any optimal star decomposition there are no two adjacent 2-regions. On the other hand, Lemma 18 states that for any triple of consecutive 2-regions, at least one belongs to the optimal star decomposition. Thus the cost of the optimal hyperstar decomposition Δ is given by:

$$Cost(\Delta) = Opt(P_m, (w_1, \ldots, w_{m-1})) + |U|$$

where $U \subseteq V$ is the set of vertices in V that have degree one or, in other words, that belong to a 1-region, and $Opt(P_m, (w_1, \ldots, w_{m-1}))$ is defined as:

$$Opt(P_m, (w_1, \ldots, w_{m-1})) = \min \begin{cases} w_m + 2w_{m-1} + Opt(P_{m-2}, (w_1, \ldots, w_{m-3})) \\ 2w_m + w_{m-1} + 2w_{m-2} + Opt(P_{m-3}, (w_1, \ldots, w_{m-4})) \end{cases} \tag{3}$$

Notice that the solution presented can be computed in time linear in m by means of dynamic programming techniques. Since we are considering only the 2-regions of the hyperpath, the algorithm that implements this recurrence could possibly return a set of 2-regions that is not hyperstar decomposition for the hyperpath. Indeed there could be some hyperedges that do not belong to any H_i. Lemma 18 also states that all the edges that are not covered by a partial partitioning are isolated. In other words, the solution computed by recurrence 3 does not contains any subpath of length 2 that is not covered. As stated before, the optimal hyperstar partitioning is computed by adding to the computed partial partitioning all the hyperedges that do not belong to it.

We notice that our scheme improves exponentially on the average information rate w.r.t. the algorithm presented in [10]. Please refer to Appendix C for further details.

5.2.2 The case of hypercycles

Given the results in the previous section, we can write the following:

$$Opt(C_m, (w_1, \ldots, w_m)) = \min \begin{cases} 2w_m + Opt(P_{m-1}, (w_1, \ldots, w_{m-1})) \text{ If } B_1 \text{ or } B_{m-1} \in \Delta \\ w_m + Opt(P_{m-1}, (w_1, \ldots, w_{m-1})) \text{ If } B_1 \text{ and } B_{m-1} \notin \Delta \\ w_m + 2w_{m-1} + 2w_1 + Opt(P_{m-2}, (w_2, \ldots, w_{m-2})) \end{cases}$$

5.2.3 The case of hypertrees

A hypertree can be defined as a connected hypergraph with no hypercycles. We will consider a particular class of hypertrees. More precisely, Each hyperedge is incident to at most two hyperstars. We will assume that the connections between the hyperedges are by means of ideal hyperstars whose center have maximum degree d.

Given such a hypertree H we can construct a graph T as follows: Consider all the hyperstars contained in $H = (H_1, \ldots, H_k)$. For each hyperstar H_i add a vertex to the T.

Two vertices in T are connected if and only if the two corresponding hyperstars in H share a region. Since each hyperedge is incident to at most two hyperstars and since the original graph has no hypercycle, it is immediate by construction that the graph T is actually a tree. We associate to each vertex v_i in T a weight w_i that is the number of vertices in the hyperstar associated to v_i with degree greater than one. Moreover there exists a 1-to-1 mapping among the hyperedges in H and the edges in T.

At this point we compute the minimum weighted vertex cover VC of the tree. The computed set VC naturally induces a hyperstar partitioning of the hypergraph H. Since we assumed the connection between the hyperedges to be ideal hyperstar, the partitioning is actually an ideal partitioning.

We use this ideal partitioning as a basis for a secret sharing scheme. We are left to analyze the performances of this algorithm.

Lemma 19 *Let H be a hypertree and let Δ be the hyperstar decomposition obtained as described above. Let $\delta_i = \max_{j \in adj(i)}\{|w_i - w_j|\}$, $\delta_{max} = \max_{1 \le i \le k} \delta_i$ and let us denote by U the set of vertices in H with degree 1. The total number of shares distributed by the algorithm is $(Cost(\Delta) + |U|)$, where $Cost$ is defined as the number of shares distributed to the players with degree greater than one and can be computed as:*

$$Cost(\Delta) = \sum_{v_i \in VC} [(d_i + 1)w_i] + |VC| d_{max} \delta_{max}$$

Proof. Let us denote by d_i the degree of the vertex v_i in T.

$$\begin{aligned}
Cost(\Delta) &\le \sum_{v_i \in VC} w_i + \sum_{v_i \notin VC} d_i w_i \\
&\le \sum_{v_i \in VC} \left[w_i + \sum_{v_j \in adj(v_i)} \frac{1}{d_j} w_j \right] \\
&\le \sum_{v_i \in VC} \left[w_i + \sum_{v_j \in adj(v_i)} w_j \right] \\
&\le \sum_{v_i \in VC} [w_i + d_i(w_i + \delta_i)] \\
&\le \sum_{v_i \in VC} [(d_i + 1)w_i] + |VC| d_{max} \delta_{max}
\end{aligned}$$

■

5.3 Upper Bounds on the Average Information Rate

In this section we consider the problem of computing an upper bound on the average information rate for a given access structure.

Given a hypergraph H, we construct a new hypergraph H' we call the *foundation* of H. The idea is to construct a hypergraph that contains all the vertices that will receive a share whose size is strictly greater than the size of the secret. More formally we have:

Definition 9 (Foundation) *Let $H = (V, E)$ be a hypergraph. The foundation of H is a hypergraph $H' = (V', E')$ constructed as follows:*

For any hyperedge $E_i \in E$, $E_i \in E'$ if and only if there exist two hyperedges E_j, E_k such that:

- $E_i \cap E_j \neq \emptyset$ *and* $E_i \cap E_k \neq \emptyset$
- $E_i \cap E_j \not\subseteq E_k$ *and* $E_i \cap E_k \not\subseteq E_j$

Moreover, $V' = \cup_{E_i \in E'} E_i$.

Consider a hyperedge E_i in the foundation hypergraph of H. We denote by $N(E_i)$ the set of hyperedges incident to E_i and satisfying the conditions of Definition 9. Moreover, for each E_i in the foundation hypergraph, there exists at least two regions, say $B_{i,1} = E_i \cap E_j$ and $B_{j,2} = E_i \cap E_k$ with $E_j, E_k \in N(E_i)$. By Lemma 8, some of the players in these regions will receive shares whose size is strictly greater than the size of the secret. Two possible cases can arise:

- $E_i \cap E_j \cap E_k = \emptyset$. In this case, the three hyperedges form a hyperpath of length three that, by Corollary 9, is not ideal.
- $E_i \cap E_j \cap E_k \neq \emptyset$. In this case the three hyperedges form a hyperstar with three hyperedges and two 2-regions that, by Lemma 8 is not ideal.

Given a hypergraph H, we consider the following linear programming problem $\mathcal{A}(\mathcal{H})$.

$$
\begin{array}{lrcl}
\textit{Minimize} & C & = & \sum_{v \in V} a_v \\
 & a_v & \geq & 0, v \in V \\
 & a_v + a_w & \geq & 1, \forall E_i \in E', \forall E_j, E_k \in N(E_i), \forall v \in E_i \cap E_j, w \in E_i \cap E_k, j \neq k
\end{array}
$$

Theorem 20 *Let $H = (V, E)$ be a hypergraph with foundation H'. Let C^* the optimal solution for the problem $\mathcal{A}(H)$. Then:*

$$\tilde{\rho}^* (H) \leq \frac{|V|}{C^* + |V|}.$$

Proof. Consider any secret sharing scheme realizing the access structure described by the hypergraph H. For every vertex $v \in V$ define:

$$a_v = \frac{\log s_v}{\log q} - 1$$

Since $\log s_v \geq \log q$, it holds that $a_v \geq 0$ for any $v \in V$. Moreover, if E_i is a hyperedge in H', there must exist $E_j, E_k \in E$ such that condition 1 of Definition 9 is satisfied. But by Lemma 8 the hypergraph composed by the hyperedges E_i, E_j, E_k is not ideal and for any

$v \in E_i \cap E_j$ and for any $w \in E_i \cap E_k$, it holds that $\log s_v + \log s_w \geq 3 \log q$ or, equivalently, $a_v + a_w \geq 1$.

This means that any secret sharing scheme is associated to an admissible solution for the problem $\mathcal{A}(H)$. Hence

$$C^* \leq \sum_{v \in V} a_v$$

where C^* defines the optimal solution for the problem $\mathcal{A}(H)$. It follows that:

$$C^* \leq \frac{\sum_{v \in V} \log s_v}{\log q} - |V|$$

But we have that:

$$\begin{aligned} \tilde{\rho}\,(H) &= \frac{|V| \log q}{\sum_{v \in V} \log s_v} \\ &\leq \frac{|V|}{C^* + |V|} \end{aligned}$$

■

Theorem 20 defines an upper bound on the average information rate for general access structures. In the next sections we are going to give specific upper bounds for particular class of access structures, namely the one that can be represented by an "hypergraph" generalization of paths, cycles and trees.

Before going on, we are going to prove a result that will be used in the rest of this section. For any hyperedge $E_j \in E'$ in the foundation hypergraph there are at least two *non-ideal regions* we call $B_{j,1}$ and $B_{j,2}$ with weight $w_{B_{j,1}} = |B_{j,1}|$ and $w_{Bj,2} = |B_{j,2}|$ respectively. Denote by $w_j = \min\{w_{B_{j,1}}, w_{B_{j,2}}\}$, $w_{min} = \min\{w_{B_{j,1}}, w_{B_{j,2}} | j = 1, \ldots |E'|\}$, and $w_{max} = \max\{w_{B_{j,1}}, w_{B_{j,2}} | j = 1, \ldots |E'|\}$.

Theorem 21 *Let H be a hypergraph and let $H' = (V', E')$ be its foundation. If the vertices in V' have degree at most d than:*

$$C^* \geq \frac{w_{min}}{w_{max}} \frac{|E'|}{d}$$

Proof.

Using the second constraint of the problem $\mathcal{A}(\mathcal{H})$, we can write:

$$\sum_{j=1}^{|E'|} 1 \leq \sum_{j=1}^{|E'|} (a_{x_j} + a_{y_j})$$

Where $a_{x_j} \in B_{j,1}$ and $a_{y_j} \in B_{j,2}$. From this inequality follows:

$$
\begin{aligned}
w_{min}|E'| &\leq \sum_{j=1}^{|E'|} w_j && (4)\\
&\leq \sum_{j=1}^{|E'|} w_j(a_{x_j} + a_{y_j}) && (5)\\
&\leq dw_{max}\sum_{j=1}^{n} a_i && (6)\\
&\leq dw_{max}C^* && (7)
\end{aligned}
$$

From which the lemma follows. ■

From this theorem we it is possible to derive some interesting results on some classes of hypergraphs.

HyperCycles The first class of hypergraphs we are going to consider is the class of hypercycles. It is not hard to see that the foundation hypergraph of C_m is the C_m itself. Moreover, the non-ideal regions in C_m are exactly all its 2-regions. Since C_m has maximum degree 2, by Theorem 21 we can obtain the following:

Corollary 22 *Let $C_m = (V, E)$ be a hypercycle, let $B_1, \ldots, B_m$ be its 2-regions and let $w_i =| B_i |$ for $i = 1, \ldots, m$. The it holds that:*

$$\tilde{\rho} \leq \frac{|V|}{r\frac{m}{2} + |V|}$$

where $r = \min_{1\leq j\leq m} w_j / \max_{1\leq j\leq m} w_j$

HyperPaths The next bound we are going to show is the upper bound on the average information rate for hyperpaths. It is not hard to see that the foundation hypergraph of a hyperpath P_m is isomorphic to P_{m-2}. More precisely, given a hyperpath P_m, its foundation hypergraph is obtained by removing the first and the last hyperedge in the hyperpath. Indeed all the other hyperedges in the hyperpath will be the middle-hyperedge of some subpaths of length 3.

Corollary 23 *Let $P_m = (V, E)$ be a hyperpath, and let P_{m-2} be its foundation hypergraph. Moreover let $B_1, \ldots, B_{m-2}$ be the 2-regions of P_{m-2} and let $w_i =| B_i |$ for $i = 1, \ldots, m-2$. The it holds that:*

$$\tilde{\rho} \leq \frac{|V|}{r\frac{m-2}{2} + |V|}$$

where $r = \min_{1\leq j\leq m-2} w_j / \max_{1\leq j\leq m-2} w_j$

Hypertrees Let H be a hypertree with at least four hyperedges. The foundation hypergraph of a hypertree contains at least all the internal vertices of the tree.

Corollary 24 *Let H be a hypertree with maximum degree d and let H' be its foundation. It holds that*

$$C^* \geq \frac{w_{min}}{w_{max}} \frac{|E'|}{d}$$

6 Optimal Information Rate

In this section we present a general lower bound on the information rate based on the multiple hypergraph decomposition. We shall show that using this technique it is possible to construct optimal secret sharing schemes for some classes of hypergraph w.r.t. the information rate. Even in this case, we can achieve exponential improvement w.r.t. known secret sharing schemes. For a hypergraph H define

$\rho^*(H) = \sup\{\rho :$ there exists a perfect secret sharing scheme for H with information rate $\rho\}$

Note that the definition requires that a perfect secret sharing schemes exists only for *some* values of q, not for *all*.

We are interested in the best information rate we can obtain by multiple hypergraph decomposition. To this aim we define $\rho^*_C(H)$ to be this optimal information rate. It is immediate that $\rho^*_C(H) \leq \rho^*(H)$. We first generalize a result in [5] that allows to compute the value of $\rho^*_C(H)$.

Let $H = (V, E)$ be an hypergraph and assume $\Delta_j = \{H_{j1}, \ldots, H_{jk_j}\}$, with $1, 2$ be two hypergraph decomposition of H. We can define a partial order on the Δ_j's as follows: Let $R_{jv} = |\{i : v \in H_{ji}\}|$. We say that $\Delta_i \leq \Delta_j$ if and only if $R_{iv} \leq R_{jv}$ for any $v \in V$. Define a hypergraph decomposition Δ_i to be *minimal* if there does not exists Δ_j such that $\Delta_j \leq \Delta_i$ and $\Delta_j \neq \Delta_j$. Now assume that $\Delta_j = \{H_{j1}, \ldots, H_{jk_j}\}$, with $j = 1, \ldots, L$ be a complete enumeration of all minimal hypergraph decomposition of H and for every vertex $v \in V$ and for any $j = 1, \ldots, L$ define $R_{jv} = |\{i : v \in H_{ji}\}|$. Consider the following optimization problem $\mathcal{I}(H)$

$$\begin{array}{lrcl} Minimize & R & = & \max\{\sum_{j=1}^{L} a_j R_{jv} : v \in V\} \\ & a_j & \geq & 0, 1 \leq j \leq L \\ & \sum_{j=1}^{L} a_j & = & 1 \end{array}$$

The proof of the following theorem is a straightforward extension of the corresponding theorem in [5].

Theorem 25 *Let R^* be the optimal solution to $\mathcal{I}(H)$. Then $\rho^*_C(H) = 1/R^*$.*

Theorem 26 *Let $P_3(V, \{E_1, E_2, E_3\})$ be the hyperpath with three hyperedges. Then $\rho^*(P_3) =$* $2/3$.

Proof.

Let B_1 and B_2 the two 2-regions of P_3. By Corollary 9, for any $x \in B_1$ and any $y \in B_2$, it holds that $H(x) + H(y) \geq 3H(S)$. Thus either $H(x) \geq 3H(S)/2$ or $H(y) \geq 3H(S)/2$. Thus $\max_{x \in V} H(x) \geq 3H(S)/2$ and

$$\rho^*(P_3) \leq \frac{H(S)}{\max_{x \in V}\{H(x)\}} \leq \frac{2}{3}$$

We need to show that $\rho^*(P_3) \geq 2/3$. Let us denote by A_1, A_2, A_3 and by B_1, B_2 respectively the 1 and the 2-regions of P_3. We can write $E_1 = A_1, B_1$, $E_2 = B_1, A_2, B_2$ and $E_3 = B_2, A_3$. Consider the decomposition construction induced by the sets $\{B_1, A_3\}$ and $\{A_1, B_3\}$. Given these decompositions we can apply the multiple decomposition construction obtaining $R_v = 2$ for any $v \in A_1 \cup A_2 \cup A_3$ and $R_v = 3$ for any $v \in B_1 \cup B_2$ and thus, by Theorem 3, $\rho^*(P_3) \geq 2/3$. ∎

For the sake of self containment, we next recall some results on graph-based structures presented in [5]. For these theorems, P_n represents a path with n edges and C_n represents a cycle with m edges.

Theorem 4.5 [5] If $n \geq 3$, then $\rho^*(P_n) = 2/3$.

Theorem 4.6 [5] If $n \geq 3$, then $\rho^*(C_{2n}) = 2/3$.

Theorem 4.7 [5] If $n \geq 3$, then $\rho^*_C(C_{2n+1}) = (2n+1)/(3n+2)$.

Theorem 27 *Let P_m be the hyperpath with m hyperedges. Then $\rho^*(P_m) = 2/3$.*

Proof.

By Theorem 1 and Theorem 26 $\rho^*(P_m) \leq 2/3$. Let us denote by $E_1, \ldots, E_m$ the hyperedges in P_m. We can rewrite the hyperedges of the hyperpath as $E_i = B_{i-1}A_iB_i$, for any $i = 2, \ldots, m-1$, $E_1 = A_1, B_1$ and $E_m = B_{m-1}A_m$ where A_i and B_i represents respectively the 1 and 2-regions of P_m. Starting from P_m we construct a path $P'_m = (V', E')$ defined as follows: $V' = \{a_1, b_1 \ldots, b_{m-1}, a_m\}$ and $E' = \{(a_1, b_1), (b_1, b_2), \ldots, (b_{m-2}, b_{m-1}), (b_{m-1}, a_m)\}$. Notice that P'_m is a path with m edges, and thus, by Theorem 4.5 in [5], for any m, there exists a secret sharing scheme for P'_m with information rate $2/3$.

Assume $\Delta' = \{x_1, \ldots, x_k\} \subseteq V'$. We construct a new set $\Delta = \{X_1, \ldots, X_k\}$ where $X_i = B_j$ iff $x_i = b_j$ and $X_i = A_j$ iff $x_i = a_j$. It is immediate that if Δ' is a star decomposition for P'_m, then Δ is a hyperstar decomposition for P_m. Notice that the two decompositions induce secret sharing schemes with the same information rate. ∎

Theorem 28 *Let C_m be the hypercycle with $m \geq 3$ hyperedges. Then if m is even $\rho^*(C_m) = 2/3$ otherwise $\rho^*_C(C_m) = (2n+1)/(3n+2)$*

Proof. From Theorem 1 $\rho^*(C_m) \geq 2/3$. Let us denote by $B_0, \ldots, B_{m-1}$ the set of 2-regions of C_m. We construct a graph $C'_m = (V', E')$ as follows: $V' = \{b_0, \ldots, b_{m-1}\}$ and $E' = \{(b_i, b_{i+1 \bmod m}), i = 0, \ldots, m-1\}$. Notice that C'_m is a cycle graph with m vertices. The theorem follows by Theorems 4.6 and 4.7 in [5] and using similar argument of Theorem 27. ∎

Theorem 29 *Let H be a non-ideal hyperstar with three hyperedges. It holds that $\rho^*(H) = 2/3$.*

Proof.

To prove that $\rho^*(H) \leq 2/3$ we use similar argument of Theorem 26.

To prove $\rho^*(H) \geq 2/3$ we consider the following secret sharing scheme for a secrets s. We write $s = s_1 + s_2$. At this point we decompose the hypergraph H as the center A of H and $\texttt{Remove}(H, A)$ and share s_1 among the players in A using a $(|A|, |A|)$-threshold schemes. Recall that, since H is non-ideal hyperstar, than H must contain at least two 2-regions. Here two possible cases can arise:

- H contains two 2-regions. The hypergraph $\texttt{Remove}(H, A)$ is a hyperpath with three hyperedges and thus, as shown in Theorem 26, $\rho^*(\texttt{Remove}(H, A) = 2/3$.
- H contains three 2-regions. The hypergraph $\texttt{Remove}(H, A)$ is a hypercycle with three hyperedges and thus, as shown in Theorem 28, $\rho^*(\texttt{Remove}(H, A) = 2/3$.

The theorem follows since $\rho^* \geq \min\{\rho^*(A), \rho^*(\texttt{Remove}(H, A))\}$. ∎

Corollary 30 *Let H be a non-ideal hyperstar with m hyperedges then $\rho^*(H) \leq 2/3$.*

References

[1] J. Benaloh and J. Leichter, *Generalized secret sharing and monotone functions*, in Advances in Cryptology – CRYPTO '88, S. Goldwasser, ed., Lecture Notes in Computer Science 403 (1989), 27-35.

[2] G. R. Blakley, *Safeguarding cryptographic keys*, in Proceedings of the National Computer Conference, 1979, American Federation of Information Processing Societies Proceedings 48 (1979), 313-317.

[3] C. Blundo, A. De Santis, R. De Simone, and U. Vaccaro, *Tight Bounds on the Information Rate of Secret Sharing Schemes*, Design, Codes, and Cryptography, vol. 11, 1997, pp. 107–122.

[4] C. Blundo, A. De Santis, L. Gargano and U. Vaccaro, *On the Information Rate of Secret Sharing Schemes,* in Theoretical Computer Science, vol. 154, pp. 283–306, 1996.

[5] C. Blundo, A. De Santis, D. R. Stinson, U. Vaccaro, *Graph Decomposition and Secret Sharing Schemes*, Journal of Cryptology, Vol. 8 (1995), pp. 39-64.

[6] E. F. Brickell, D.M. Davenport, *On the Classification of Ideal Secret Sharing Schemes*, Journal of Cryptology, Vol. 4 (1991), pp. 123-134.

[7] R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro, *On the Size of Shares for Secret Sharing Schemes*, Journal of Cryptology, vol. 6, n. 3, pp. 157-169, 1993.

[8] T.M. Cover and J.A. Thomas, *Elements of Information Theory*, John Wiley & Sons, Singapore, 1991.

[9] L. Csirmaz, *The Size of a Share Must be Large,* Journal of Cryptology, Vol. **10**, n. 4, pp. 223–231, 1997.

[10] M. Ito, A. Saito and T. Nishizeki, *Secret sharing scheme realizing general access structure*, in Proceedings of the IEEE Global Telecommunications Conference, Globecom '87, IEEE Press, 1987, 99-102.

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

[12] D. R. Stinson, *Decomposition Constructions for Secret Sharing Schemes*, IEEE Transactions on Information Theory, vol. 40, 1994.

[13] D. R. Stinson, *An Explication of Secret Sharing Schemes*, Design, Codes and Cryptography, Vol. **2**, pp. 357–390, 1992.

[14] D. R. Stinson, *Bibliography on Secret Sharing Schemes*, http://cacr.math.uwaterloo.ca/~stinson/ssbib.html, October 13, 1998.

[15] M. van Dijk, *On the Information Rate of Perfect Secret Sharing Schemes,* in Design, Codes and Cryptography, vol. 6, pp. 143–169, 1995.

A Comparing Performances on Hyperstar

As an example of the improvement of the performance of the secret sharing schemes w.r.t. the algorithm presented in [10], let us consider the hypergraph in Figure 1 (a), i.e., a hyperstar with three edges and one 2-region. For the sake of simplicity, let us assume that all the regions in the hyperstar have cardinality k.

In the proof of Lemma 5, we have presented an ideal secret sharing scheme for this hypergraph, i.e., a secret sharing scheme in which each player receives one share of the same size of the secret. This also means that the information rate and the average information rate are both equal to one.

Let us analyze the performances of the secret sharing scheme presented in [10] on the same access structure. The protocol presented in [10] requires to construct the family $\delta^+\mathcal{B}$ of maximal forbidden sets for the access structure. We notice that, for this access structure, $\delta^+\mathcal{B} = \{B_1, \ldots, B_t\}$ can be written as $\{D_1, D_2, D_3\}$ where $D_1 = \{V \setminus \{x\} : \forall x \in A\}$, $D_2 = \{V \setminus \{x, y\} : \forall x \in B, y \in C\}$, and $D_3 = \{V \setminus \{x, y, z\} : \forall x \in C, y \in D\ z \in E\}$. Indeed, for example, all the sets in D_1 are maximal (since they contain all but one vertices in the hypergraph), distinct and forbidden since each authorized set must include all the vertices in A. Notice that $|D_1| = k$, $|D_2| = k^2$, $|D_3| = k^3$ and thus $|\delta^+\mathcal{B}| = t = k^3 + k^2 + k$.

At this point a (t, t) threshold scheme is used to obtain t shares, $s_1, \ldots, s_t$, one for each set in $\delta^+\mathcal{B}$. The share s_i will be given to all the players that do *not* belong to B_i. Thus, this protocol assignes to each player a number of shares that is equal to the number of maximal forbidden set to which it does *not* belongs to.

The correctness of this protocol has been stated in [10]. In order to analyze the performances of this scheme, let us fix a player $x_1 \in A$. This player will receive exactly one share since it belongs to all but one the sets in $\delta^+\mathcal{B}$, namely it does not belong to the set $V \setminus \{x_1\} \in D_1$. Thus all the players in A will receive exactly one share. Let us now fix a player $x_2 \in B$. This player will receive k shares. Indeed x_2 belongs to all the sets in D_1 and D_3, and it does not belong to k sets in D_2, namely all the sets $V\{x_2, y\}$ for any $y \in C$. Using similar arguments, it is possible to show that all the players in $D \cup E$ receive k^2 shares and all the players in C will receive $k^2 + k$ shares. Thus the information rate achieved by this scheme is $\rho = 1/(k^2 + k)$ and the average information rate is $5/(3k^2 + 2k + 1)$.

B Partitioning the Hypergraph in Regions

The first step towards constructing an ideal secret sharing scheme for an ideal hyperstar is partitioning the hypergraph into regions. Here we present an algorithm to accomplish this task that runs in time $O(mn + n \log n)$, where m and n are the number of hyperedges and the number of vertices, respectively, in the hypergraph. number The algorithm works as follows:

Algorithm `Region-Partition`(H)
Input: Hypergraph $H = (V, E), V = \{P_1, \ldots, P_n\}, E = \{E_1, \ldots, E_m\}$

1 For each P_i construct $List_i$ containing the list of hyperedges P_i belongs to. We assume $List_i$ to be an ordered sub-sequence of $(1, \ldots, m)$.
2 Sort the set $\{List_1, \ldots, List_n\}$ obtaining an ordered list L.
3 Remove from L all the elements that appear more than once.
4 Output L

Let us briefly explain the idea of the algorithm. By definition, a region a determined by a set of determining edges. Thus two vertices P_i and P_j will belong to the same region if and only if $List_i = List_j$. Thus the set of all regions in the hypergraph will be the set of all (different) lists generated in the first step. The first step in the algorithm can be executed in time $O(mn)$ since each hyperedge may contain $O(n)$ vertices. The second step consists of sorting a list containing n elements. Finally, since the list L is ordered, the last step takes time $O(n)$. Thus the algorithm $Region - Partition$ runs in time $O(mn + n \log n)$.

Theorem 31 *Given an ideal hyperstar $H = (V, E)$, where $|V| = n$ and $E = (E_1, \ldots, E_m)$, and a secret s, there exists an algorithm that implements an ideal secret sharing for s according to H that runs in time $O(mn + n \log n)$.*

C Comparing Performances on Hyperpath

As a second example of the improvement of the performance of the secret sharing schemes w.r.t. the algorithm presented in [10], let us consider the case of a hyperpath $P_m = (V, E)$ with m edges. For the sake of simplicity, let us rewrite the hyperedges as follows: $E_1 = A_1A_2$, $E_i = A_{2i-2}A_{2i-1}A_{2i}$ and $E_m = A_{2m-2}A_{2m-1}$, where A_i is either a 1-region of the hyperpath (if i is odd) or a 2-region (if i is even). Moreover let us assume that all the regions have cardinality k.

It is not hard to see that, the algorithm presented in Section 5.2.1 allows to obtain an average information rate $\widetilde{\rho} \simeq 4/5$ for this particular hypergraph. On the other hand, Theorem 27 shows that it is possible, using the multiple hypergraph decomposition, to obtain an information rate $\rho = 2/3$

Let us analyze the performance of the algorithm presented in [10] on the described hyperpath. Let us denote by T_n the size of the family of maximal forbidden sets over a path with n regions, i.e. $T_n = |\delta^+\mathcal{B}$. First notice that T_2 is the number of maximal forbidden sets over one hyperedge composed by two regions. Thus $T_2 = 2k$ since the number of maximal forbidden sets for a $(2k, 2k)$ threshold scheme is $2k$. We will first compute T_3 that is the size of δ^+B for an hyperpath with 2 edges whose regions have size k. We can write $E_1 = A_1A_2$ and $E_2 = A_2A_3$. We can write $\delta^+B = \{D_1, D_2\}$, where $D_1 = \{V \setminus \{x\} : \forall x \in A_2\}$, $D_2 = \{V \setminus \{x, y\} : \forall x \in A_1, y \in A_3\}$. Thus $T_3 = k^2 + k$.

We are now ready to compute T_n. Fix any maximal forbidden set X. Since X is forbidden than, for each hyperedge in the hyperpath, there must be at least one vertex that does not belong to X. On the other hand, since X is maximal, it must include possibly all but one vertices from all the hyperedges. Consider now, the regions A_n, A_{n-1} and A_{n-2} and, w.l.o.g., assume n is odd, i.e, A_n is a 1-region. Similar arguments apply if n is even. The family of all maximal forbidden set on $A_1 \dots A_n$ is composed by:

- All the sets containing all but one the vertices in A_n, all the vertices in A_{n-1} and all the maximal forbidden sets in $A_1, \dots, A_{n-2}$. Since A_n is 1-region, removing from a forbidden set X a vertex from A_n allows us to include in it all the other vertices in the (only) hyperedge A_n belongs to, i.e., $A_{n-1}A_n$.

- All the sets containing all the vertices in A_n, all but one the vertices in A_{n-1}, all the vertices in A_{n-2} and all the maximal forbidden sets in $A_1, \dots, A_{n-3}$. Since A_{n-1} is a 2-region, removing from a forbidden set X a vertex in A_{n-2} will allow us to include in it all the other vertices in the two hyperedges A_{n-1} belongs to, i.e., $A_{n-1}A_n$ and $A_{n-3}A_{n-2}A_{n-1}$.

The number of maximal forbidden set can thus be computed as $T_n = kT_{n-2} + kT_{n-4}$ that is exponential in the number of hyperedges of the hyperpath. Recall that in order to share the secret, the protocol presented in [10] requires to use a (t, t) threshold scheme where $t = |\delta^+\mathcal{B}|$. This means that the number of shares to be distributed among the players in exponential in the number of hyperedges. Since total number of players is $k(2m - 1)$ this means that both the information rate and the average information rate are exponentially small.