On the impossibility of graph secret sharing

László Csirmaz*

Abstract

A *perfect secret sharing scheme* based on a graph G is a randomized distribution of a secret among the vertices of the graph so that the secret can be recovered from the information assigned to vertices at the endpoints of any edge, while the total information assigned to an independent set of vertices is independent (in statistical sense) of the secret itself.

The efficiency of a scheme is measured by the amount of information the most heavily loaded vertex receives divided by the amount of information in the secret itself. The (worst case) *information ratio* of G is the infimum of this number. We calculate the best lower bound on the information ratio for an infinite family of graphs the celebrated entropy method can give.

We argue that all existing constructions for secret sharing schemes are special cases of the generalized vector space construction. We give direct constructions of this type for the first two members of the family, and show that for the other members no construction exists which would match the bound yielded by the entropy method.

1 Introduction

Secret sharing has been investigated in several papers [1, 2, 5, 7, 14, 16, 17, 18, 22] as well as schemes based on graphs [4, 6, 8, 9, 12, 13] just to mention a few. Subsets of the participants are split into *qualified* and *unqualified* ones. A qualified subset can recover the secret, while the total information an unqualified subset has should be (statistically) independent of it. When the scheme is based on a graph, then the participants are the vertices of the graph, and a collection of vertices is qualified if it contains an edge.

The most important property of a scheme is its *efficiency*, namely how many bits the most heavily loaded participant must remember for each bit in the secret. The (worst case) *information ratio* of a graph G is the infimum of the efficiency of all schemes based on G. In the literature the inverse of this number is used and called the *information rate of* G in resemblance to the coding efficiency on noisy channels.

Determining the information ratio for a simple graph could be a very difficult problem cf. [9, 12, 13]. Nevertheless, the ratio was determined exactly for several infinite families of graphs in the above references. Interestingly, all these ratios are of the form $2 - 1/k$ or $k/2$ for some positive integer k, and it is an open problem to find a graph with ratio different from these values. In this paper we investigate another infinity family of graphs. We establish the best lower bound the entropy method can give, and show that present-day techniques cannot reach this bound. We formulate an open problem and some conjectures as well.

1.1 Basic notions

In the paper we use the standard techniques and notions, see [4, 6, 8]. For the sake of the reader we briefly repeat some of the definitions.

Let G be a graph. A *secret sharing scheme on* G is a collection of random variables ξ_v for all vertices v in G, plus the special random variable ξ_s. The value of this latter one is the *secret*, that of the others are the *shares*. The random variables form a joint distribution. The *dealer* draws

*Central European University, Budapest

from this distribution, and sends the value ξ_v to the *participant* $v \in G$, while keeps the value of ξ_s secret.

The secret sharing scheme is *perfect* if whenever v, w is an edge in G then ξ_v and ξ_w together determine the secret uniquely; while if A is an independent set of vertices (i.e. no edge exist between vertices in A), then the collection $\{\xi_v : v \in A\}$ is statistically independent from ξ_s, i.e. the totality of shares this collection has provides zero information about the secret.

Using the usual (Shannon) entropy [11], A determines B iff the entropy of A and AB are the same, while A and B are statistically independent iff the entropy of AB is the sum of the entropies of A and B. (Here and in the sequel we write AB in place of $A \cup B$.) The Shannon entropy of A, denoted as $\mathbf{H}(A)$, is roughly the number of independent bits necessary to encode the value of A. Applying this notion to the secret sharing we see that the *size of the share* assigned to the participant $v \in G$ is the entropy of ξ_v, and the size of the secret is $\mathbf{H}(\xi_s)$. Thus the *information ratio* of the graph G is

$$R(G) = \inf\left\{\frac{\max_{v\in G}\mathbf{H}(\xi_v)}{\mathbf{H}(\xi_s)}\right\}, \tag{1}$$

where the infimum is taken over all perfect schemes on G.

1.2 Proving a lower bound

Let the distribution $\{\xi_s, \xi_v\}$ be any perfect secret sharing scheme on G. Consider the real-valued function f which assigns the value

$$f(A) = \frac{\mathbf{H}(\{\xi_v : v \in A\})}{\mathbf{H}(\xi_s)} \tag{2}$$

to the subset A of the vertices. Using standard properties of the entropy function [11, 20, 24], this f has certain properties, namely

(a)	$f(A) \ge 0$, $f(\emptyset) = 0$	positivity,
(b)	$f(B) \ge f(A)$ when $B \supseteq A$	monotonicity,
(c)	$f(A) + f(B) \ge f(A \cup B) + f(A \cap B)$	submodularity.

Furthermore, $\mathbf{H}(\xi_s \cup \{\xi_v : v \in A\})$ is equal to $\mathbf{H}(\{\xi_v : v \in A\})$ if A determines the secret, i.e. when A contains an edge; and is equal to the sum of $\mathbf{H}(\xi_s)$ and $\mathbf{H}(\{\xi_v : v \in A\})$ when A is independent. This observation leads us to

(d) $f(B) \ge f(A) + 1$
when $B \subseteq A$, A is independent and B is not

(e) $f(A) + f(B) \ge f(A \cup B) + f(A \cap B) + 1$
when $A \cap B$ are independent but A, B are not.

Properties (d) and (e) are called *strict monotonicity* and *strict submodularity*, respectively.

Unfortunately properties (a)–(e) do not characterize the real-valued functions which can be got from perfect secret sharing schemes. They satisfy further *non Shannon-type* inequalities [24] as well, and no complete characterization is known up to now [20]. Even for the case of four (dependent) random variables we do not have a complete description of the 15 dimensional cone spanned by the entropies of the different subsets of the variables [20].

Now we can describe the celebrated *entropy method* [4, 6, 8]. Take any real-valued function f which satisfies properties (a)–(e) above (and maybe further inequalities which are always true for the entropy function). Suppose we show for some real number r that for all of such functions f, $\max_{v\in G} f(v) \ge r$. Then the *information ratio* $R(G)$ of G defined in (1) is at least r.

Observe that properties (a)–(e) are linear inequalities (and, in fact, all further known properties of the entropy are), thus determining the best lower bound is, in fact, an LP problem [10]. The only problem is that both the number of variables and the number of constrains grow exponentially with the size of the graph, which makes the LP problem unsolvable even for relatively small graphs. We remark for the interested reader that the system of conditions given by (a)–(e) is overdetermined. Even after reducing the conditions [20], the system remains ill-posed which makes further complications.

1.3 Proving an upper bound

Typically upper bounds come easily: one has to find an appropriate scheme which realizes the given bound. There are constructions based on some algebraic structure (mainly vector spaces over finite fields) [1, 13, 12, 21], or on geometry (finite projective geometry) [3]. The celebrated, and incredibly effective construction of Stintson [22] can be used to build a scheme from other smaller schemes. van Dijk and al [13] used a slightly different method where the intermediate schemes are not necessarily perfect. Nevertheless, all presently known constructions [1, 5, 17] (even the ones arising from van Dijk's construction or from span programs) are special cases of the following general one.

Let $\mathbb{F}$ be a vector space (sometimes a weaker structure, such as a module suffices), and assign (non-trivial) linear subspaces of $\mathbb{F}$ both to the participants and the secret: let L_v be the subspace assigned to $v \in G$ and L_s be the subspace assigned to the secret. These subspaces should have the following property: if vw is an edge in G, then the linear span of L_v and L_w should contain (as a subspace) L_s. If, on the other hand, $\{v_1, \ldots, v_k\}$ is an independent set (this is always the case when $k = 1$), then the intersection of the linear span of $\{L_{v_1}, \ldots, L_{v_k}\}$ and L_s must be trivial, i.e. the single element subspace $\{0\}$.

The dealer chooses an element from $\mathbb{F}$ uniformly (here we must assume that $\mathbb{F}$ is finite). The *secret*, i.e. the value of ξ_s is the orthogonal projection of this random element on L_s. The *share* of participant $v \in G$ is the orthogonal projection of the dealer's element on L_v.

Now, if vw is an edge, then using elementary linear algebra, the secret can be expressed as an appropriate linear combination of the shares. On the other hand, if $\{v_1, \ldots, v_k\}$ is an independent subset of vertices, then the linear span of $\{L_{v_1}, \ldots, L_{v_k}\}$ and the subspace L_s intersect in the zero vector, thus projection on the first one gives no information at all on the value of projection on the other. (This is the second point where the finiteness of $\mathbb{F}$ plays a crucial role.)

The amount of information (i.e. entropy) in the secret is proportional to the dimension of L_s, and the information v gets is proportional to $\dim(L_v)$. Thus the *ratio* of this construction is

$$\frac{\max_{v \in G} \dim(L_v)}{\dim(L_s)}.$$

The total randomness the dealer needs to produce the shares is proportional to the dimension of the whole vector space $\mathbb{F}$.

Looking at this construction more carefully, the function f defined in (2) takes the same value as the ratio of the dimensions of the corresponding subspaces:

$$f(A) = \frac{\mathbf{H}(\{\xi_v : v \in A\})}{\mathbf{H}(\xi_s)} = \frac{\dim(\langle L_v : v \in A \rangle)}{\dim(L_s)}$$

Linear subspaces of a vector space form a matroid [23]. However not all matroids can be represented this way. Matroids arising from linear subspaces satisfy the so-called *Ingleton inequality* [15], which not all matroids, and not all functions arising from entropy, do:

$$\text{(f)} \quad \begin{aligned} &f(AC) + f(AD) + f(BC) + f(BD) + f(CD) \geq \\ &\quad f(C) + f(D) + f(ACD) + f(BCD) + f(AB) \ . \end{aligned} \tag{3}$$

In particular, this inequality is not a consequence of the inequalities (a)–(e) discussed above, but it always holds for all existing secret sharing constructions.

2 The graph family

One of the smallest graphs where no exact information ratio was known for a long time [12] is the following. It has six vertices, v_1, v_2, v_3, and w_1, w_2, w_3. The first three vertices form a triangle, furthermore only v_i and w_i are connected.

Using the entropy method sketched in section 1.2, an LP package was used to get the optimal bound for this graph, which turned out to be 7/4. There is an easy construction with ratio 2 using Stinson's decomposition method [22], but the exact value was not known for some time. The first published construction with ratio 7/4 can be found in [13]. This graph is clearly an element of the following infinite family of graphs:

Let G_n have vertices $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$. The edges are v_iv_j for each pair i and j, furthermore only v_i and w_i are connected. That is, G_n is a complete graph on n vertices and each vertex is connected to an extra vertex from an independent set of size n. The above graph is G_3, while G_2 is the path of length 4 (a complete graph on 2 vertices, plus two additional vertices). The information ratio of G_2 is 3/2 [4], while that of G_3 is 7/4. Using an LP package we found that the entropy method yields the lower bound 15/8 for G_4. This data supported the conjecture that the ratio of G_n is at least $(2^n - 1)/2^{n-1} = 2 - 1/2^{n-1}$. In section 3 we show that indeed this is the case, and, furthermore, this is the best value what the entropy method can give.

In section 4 we give a novel construction for G_3 which matches the lower bound, finally in section 5 we show that there exists no similar construction which would work for G_4, and, consequently, for other graphs in this family. In the last section we discuss the intuition that no vector-space construction can exist in general for this graph family. We also list some open problems.

3 Lower bound for G_n

Let G_n be the graph defined above. Among its $2n$ vertices $v_1, \ldots, v_n$ form a complete graph, while the vertex w_i is connected to v_i only. The set of vertices $\{v_1, \ldots, v_n\}$ is denoted by V, while set of the other is denoted by W, where W is an independent set (i.e. it contains no edges).

As explained in section 1.2, let f be a real function assigning non-negative values to subsets of vertices so that f satisfies properties (a)–(e) listed there. Our goal is to give the best possible lower estimate for $\max_{v \in V \cup W} f(v)$. We start with a lemma. As customary, we leave out the $\{\}$ and $\cup$ signs, and write, e.g., vX for the set $\{v\} \cup X$.

Lemma 1 *Let X be a subset of W, $w \in W - X$, $a, b \in V$ so that a is not connected to any vertex in $X \cup \{w\}$, while b is connected to w. Then*

$$f(aX) - f(X) + f(bX) - f(X) \geq f(awX) - f(wX) + 2.$$

Proof Observe that awX is independent, while $abwX$ is not. Thus property (d) gives

$$f(abwX) \geq f(awX) + 1.$$

As bX is independent, abX and bwX are not, the strict submodularity property (e) gives the first line below. Other lines are instances of the submodularity property (b):

$$\begin{aligned} f(abX) + f(bwX) &\geq f(bX) + f(abwX) + 1 \\ f(aX) + f(bX) &\geq f(abX) + f(X) \\ f(wX) + f(bX) &\geq f(X) + f(bwX) \end{aligned}$$

Adding up these inequalities we get the claim of the lemma. □

Using the lemma with X as the empty set we get

$$f(v_2) + f(v_1) \geq f(v_2w_1) - f(w_1) + 2,$$

and similarly

$$f(v_3) + f(v_1) \geq f(v_3w_1) - f(w_1) + 2.$$

Adding these up and using the lemma again with $X = \{w_1\}$ we have

$$f(v_3) + f(v_2) + 2f(v_1) \geq f(v_3w_2w_1) - f(w_2w_1) + 2 \cdot 2 + 2.$$

Similar reasoning gives

$$f(v_4) + f(v_2) + 2f(v_1) \geq f(v_4w_2w_1) - f(w_2w_1) + 2 \cdot 2 + 2,$$

or, one can argue, the conditions are invariant under swapping v_3 and v_4 and w_3 and w_4 (and keeping all other vertices fixed), thus all results are also invariant for this variable change. Applying the lemma again we arrive at

$$f(v_4) + f(v_3) + 2f(v_2) + 4f(v_1) \geq f(v_4w_3w_2w_1) - f(w_3w_2w_1) + 2 \cdot 2^2 + 2 \cdot 2 + 2.$$

Here we can replace v_4 by v_5, and continue the same way until there are no more vertices in V:

$$\begin{aligned} f(v_n) + f(v_{n-1}) + 2f(v_{n-2}) + 2^2f(v_{n-3}) + \ldots + 2^{n-3}f(v_2) + 2^{n-2}f(v_1) \geq \\ \geq f(v_nw_{n-1}\ldots w_2w_1) - f(w_{n-1}\ldots w_2w_1) + 2(2^{n-1} - 1). \end{aligned}$$

Let $Y = \{w_{n-1}, \ldots, w_2, w_1\}$, then

$$f(v_nY) - f(Y) \geq f(v_nw_nY) - f(w_nY) \geq 1.$$

Here the first inequality is an equivalent form of submodularity (c), while the second one is the strict monotonicity property (d). Consequently

$$f(v_n) + f(v_{n-1}) + 2f(v_{n-2}) + \ldots + 2^{n-2}f(v_1) \geq 2^n - 1.$$

By symmetry the same inequality is valid for all circular shifts of the vertices. There are n such instances all together, adding them up each $f(v_i)$ will have coefficient

$$1 + 1 + 2 + 4 + \ldots + 2^{n-2} = 2^{n-1},$$

consequently the sum is

$$2^{n-1}\big(f(v_1) + f(v_2) + \ldots + f(v_n)\big) \geq n(2^n - 1). \tag{4}$$

Therefore not all of the values $f(v_i)$ can be smaller than $(2^n - 1)/2^{n-1} = 2 - 2^{-n+1}$. That is, we have proved the following

Theorem 2 *The ratio of the graph G_n is at least $2 - 2^{-n+1}$.* □

In section 5 we shall need the following result which can be proved analogously.

Lemma 3 *Suppose $n \geq 4$. For some $3 \leq k \leq n$ we have*

$$f(v_kw_2w_1) - f(w_2w_1) \geq 2 - 2^{-n+3}.$$

Proof Let us denote the value $f(v_kw_2w_1) - f(w_2w_1)$ by a_k. As in the previous proof, Lemma 1 gives

$$a_4 + a_3 \geq f(v_4w_3w_2w_1) - f(w_3w_2w_1) + 2,$$

and also

$$a_5 + a_3 \geq f(v_5w_3w_2w_1) - f(w_3w_2w_1) + 2.$$

Adding these up and applying the lemma again we get

$$a_5 + a_4 + 2a_3 \geq f(v_5w_4w_3w_2w_1) - f(w_4w_3w_2w_1) + 2\cdot 2 + 2.$$

Continuing as above, we get

$$\begin{aligned} & a_n + a_{n-1} + 2a_{n-2} + \ldots + 2^{n-5}a_4 + 2^{n-4}a_3 \geq \\ & \quad \geq f(v_nw_{n-1}\ldots w_2w_1) - f(w_{n-1}\ldots w_2w_1) + 2^{n-2} - 2 \geq \\ & \quad \geq 1 + 2^{n-2} - 2 = 2^{n-2} - 1. \end{aligned}$$

Making a cyclic shift of the vertices v_k, …, v_3, we get

$$a_3 + a_n + 2a_{n-1} + \ldots + 2^{n-5}a_5 + 2^{n-4}a_4 \geq 2^{n-2} - 1.$$

Adding up all of these $n-2$ inequalities,

$$2^{n-3}\big(a_n + a_{n-1} + \ldots + a_3\big) \geq (n-2)\big(2^{n-2} - 1\big)$$

from where the claim of the lemma follows. □

The lower bound in Theorem 2 is the best possible one what the entropy method sketched in section 1.2 can give. To show it we present a function f with properties (a)–(e) which, in addition, satisfies $f(v) \leq 2 - 2^{-n+1}$ for all vertices v in the graph. In fact, we'll have equality for vertices in V, while $f(w) = 1$ for vertices of degree one.

This function f should be defined for all subsets of the vertices. Let the set of vertices of G_n be $V \cup W$. With each $A \subseteq V \cup W$ we associate three non-negative integers i_A, j_A and k_A as follows. A contains exactly j_A pairs v_iw_i where v_i and w_i are connected, $v_i \in V$ and $w_i \in W$. Apart from these vertices there are i_A vertices of A in V, and k_A vertices of A in W.

Now $|A| = i_A + 2j_A + k_A$, and A is independent iff $i_A \leq 1$ and $j_A = 0$. Let furthermore $\ell_A = i_A + j_A + k_A$, obviously $\ell_A \leq n$. Define the function f on all subsets of the vertices as follows:

$$f(A) = \begin{cases} \ell_A & \text{if } i_A + j_A = 0, \\ \ell_A + 1 - 2^{-n+\ell_A} & \text{if } i_A + j_A > 0 \text{ and } A \text{ is independent}, \\ \ell_A + 2 - 2^{-n+\ell_A} & \text{otherwise.} \end{cases} \tag{5}$$

It is a tedious but otherwise trivial task to check that indeed this f satisfies properties (a)–(e) for all subsets of the vertices. When $A = \{v\}$ and v is a V, then $i_A = 1$, $j_A = k_A = 0$, thus $\ell_A = 1$ and $f(v) = 1 + 1 - 2^{-n+1}$. Similarly, if $A = \{w\}$ with $w \in W$ then $i_A = j_A = 0$, $k_A = 1$, thus $f(w) = 1$ (first case of the definition in (5)).

4 A novel construction

In this section we give a construction which matches the corresponding lower bound for the graphs G_2 and G_3, and show how to generalize it for arbitrary n to yield the upper bound 2.

Our construction follows the idea outlined in section 1.3. Namely, we start with a high-dimensional vector space $\mathbb{F}$, and assign linear subspaces to the vertices *and* the secret so that

- if v and w are connected, then the linear span of the subspaces L_v and L_w contain the subspace L_s assigned to the secret, and
- whenever $\{v_1, \ldots, v_k\}$ is an independent set then the linear span of $\{L_{v_1}, \ldots, L_{v_k}\}$ intersects L_s in the null space $\{0\}$.

Having such subspaces, we can construct a perfect secret sharing scheme with ratio

$$\frac{\max_{v\in G}\dim(L_v)}{\dim(L_s)}.$$

In our case the graph G_n has vertices v_i and w_i for $1 \le i \le n$, where $V = \{v_1, \ldots, v_n\}$ is a complete graph, while $\{w_1 \ldots, w_n\}$ is empty (i.e. independent). $\mathbb{F}$ will have dimension $d(n+1)$, and all subspaces will be given as the linear span of certain vectors.

Each element in $\mathbb{F}$ is a vector with $d(n+1)$ coordinates. We split these coordinates into $n+1$ groups of coordinates d each. We define k vectors from $\mathbb{F}$ as a sequence of $n+1$ matrices each of size $k \times d$. As usually, $I = I_d$ is the unit $d \times d$ matrix: it has 1 in the diagonal elements and zero elsewhere.

The *secret* is assigned the subspace spanned by the d vectors of the form $I, \ldots, I, I$:

$$L_s = (I, \ldots, I, I)$$

where we have exactly $n+1$ unit matrices here. As these vectors are linearly independent, the dimension of L_s is d.

Vertices in the independent set $\{w_1, \ldots, w_n\}$ will be assigned a subspace generated by the d vectors

$$L_{w_i} = (0, \ldots, 0, I, 0, \ldots, 0, 0)$$

where the only I block is at the i-th position. Here $\dim(L_{w_i}) = d$ again, and the linear span of all subspaces L_{w_i} contain those vectors where all coordinates in the last, $(n+1)$-st block are zero. As any non-trivial linear combination of L_s has non-zero coordinate in each block, consequently

$$\langle L_{w_1}, \ldots, L_{w_n}\rangle \cap L_s = \{0\},$$

thus satisfying the second requirement for the independent set W.

Next we assign linear spaces to the remaining vertices v_i. These subspaces should satisfy the following requirements:

1. the span of L_{v_i} and L_{w_i} must contain L_s,
2. the span of L_{v_i} with $\{L_{w_j} : j \ne i\}$ should avoid L_s, finally
3. the span of two different L_{v_i} and L_{v_j} should contain L_s again.

To satisfy the first condition we include in L_{v_i} the vectors

$$(I, \ldots, I, 0, I, \ldots, I, I)$$

where only the i-th block is zero. The sum of the j-th vector from L_{w_i} and the j-th vector from L_{v_i} gives the generating elements of L_s, i.e. the linear span of L_{v_i} and L_{v_i} contains L_s as required.

To satisfy the second condition, we stipulate that all vectors in L_{v_i} should have zero coordinate in the i-th block. Then the linear span of L_{v_i} with all other L_{w_j}'s with $j \ne i$ has zero coordinate in this block, consequently contains only the all zero element from L_s.

The difficulty comes with the third condition. First, we show how to add d further vectors to each L_{v_i} to satisfy it. Then we show how to reduce the number of added vectors when $n = 2$ or $n = 3$.

Let M_1, M_2, …, M_n be $d \times d$ matrices so that $M_i - M_j$ has full rank whenever $i \ne j$. This is the case, for example, when we choose $M_i = \lambda_i I$ for different constants λ_i. We add to the generating set of L_{v_i} the vectors

$$(M_i - M_0, M_i - M_1, \ldots, M_i - M_{i-1}, 0, M_i - M_{i+1}, \ldots, M_i - M_n, M_i)\,.$$

As the i-th block is all zero, the second condition holds. To check that the third condition holds as well, observe that the difference of the latter d vectors assigned to v_i and v_j is

$$(M_i - M_j, M_i - M_j, \ldots, M_i - M_j, M_i - M_j)\,,$$

and since $M_i - M_j$ has full rank, the linear span of these vectors contain the generating vectors of L_s as well.

In this construction each L_{v_i} is generated by $2d$ linearly independent vectors, thus $\dim(L_{v_i}) = 2d$, while $\dim(L_s) = d$, which shows that it has ratio 2.

To reduce the dimension of L_{v_i} we look at the first d generating vectors more carefully:

$$(I, \dots, I, 0, I, \dots, I, I)\,.$$

The linear span of L_{v_i} and L_{v_j} must contain all vectors in the generating set of L_s, i.e. the vectors

$$(I, \dots, I, I, I, \dots, I, I)\,,$$

which happens iff it contains the vectors

$$(0, \dots, 0, I, 0, \dots, 0, 0)$$

where the only I occurs at the i-th position. Now the linear span of L_{v_i} and L_{v_j} definitely contains

$$(0, \dots, 0, I, 0, \dots, 0, -I, 0, \dots, 0, 0)$$

where I is at the i-th block, and $-I$ is at the j-th block. Then it also contains the vectors of the form

$$(0, \dots, 0, \mathbf{x}, 0, \dots, 0, -\mathbf{x}, 0, \dots, 0, 0)$$

for an arbitrary d-dimensional vector $\mathbf{x}$, which means that in the linear span we can move the content of the i-th block into the j-th block, effectively zeroing all elements in one of the block. We shall use this observation to reduce the dimension of L_{v_i}.

4.1 The case of $n = 2$

When $n = 2$ we will choose $d = 2$ and the linearly independent 2-dimensional vectors $\mathbf{x}$ and $\mathbf{y}$. The vectors which span the subspaces L_{v_1} and L_{v_2}, respectively, are

$$\begin{array}{lccccr}
(& 0,0, & 0,1, & 0,1 &) \\
(& 0,0, & 1,0, & 1,0 &) \\
(& 0,0, & \mathbf{x}, & 0,0 &)
\end{array}
\qquad
\begin{array}{lccccr}
(& 0,1, & 0,0, & 0,1 &) \\
(& 1,0, & 0,0, & 1,0 &) \\
(& \mathbf{y}, & 0,0, & 0,0 &)
\end{array}$$

It is clear that both spaces have dimension 3, moreover their linear span contains the vectors $(I, -I, 0)$ and $(0, \mathbf{x}, 0)$, thus also the vector $(\mathbf{x}, 0, 0)$ as explained above. This together the vector $(\mathbf{y}, 0, 0)$ from v_2' set gives all vectors in the linear span of $(I, 0, 0)$, as was required.

4.2 The case of $n = 3$

In this case we choose $d = 4$ and six 4-dimensional vectors $\mathbf{x}_1$, …, $\mathbf{x}_6$ such that any four of them has full rank. The subspaces assigned to v_1, v_2 and v_3 are generated by seven vectors as follows:

$$\begin{array}{lccccr}
(& 0 & I & I & I &) \\
(& 0 & \mathbf{x}_2 & 0 & 0 &) \\
(& 0 & 0 & \mathbf{x}_4 & 0 &) \\
(& 0 & \mathbf{x}_5 & \mathbf{x}_6 & 0 &)
\end{array}
\qquad
\begin{array}{lccccr}
(& I & 0 & I & I &) \\
(& \mathbf{x}_1 & 0 & 0 & 0 &) \\
(& \mathbf{x}_3 & 0 & \mathbf{x}_4 & 0 &) \\
(& 0 & 0 & \mathbf{x}_6 & 0 &)
\end{array}
\qquad
\begin{array}{lccccr}
(& I & I & 0 & I &) \\
(& \mathbf{x}_1 & \mathbf{x}_2 & 0 & 0 &) \\
(& \mathbf{x}_3 & 0 & 0 & 0 &) \\
(& 0 & \mathbf{x}_5 & 0 & 0 &)
\end{array}$$

This construction has ratio 7/4, and it works indeed. For example, in the linear span of $L_{v_1} \cup L_{v_2}$ we have the four vectors $(\mathbf{x}_1, 0, 0, 0)$, $(0, \mathbf{x}_2, 0, 0)$, $(\mathbf{x}_3, 0, 0, 0)$ and $(0, \mathbf{x}_5, 0, 0)$. Indeed the first two are explicitly given, the third and fourth ones can be got as the difference of one-one vectors from the assigned subspaces:

$$\begin{aligned}
(\mathbf{x}_3, 0, 0, 0) &= (\mathbf{x}_3, 0, \mathbf{x}_4, 0) - (0, 0, \mathbf{x}_4, 0) \\
(0, \mathbf{x}_5, 0, 0) &= (0, \mathbf{x}_5, \mathbf{x}_6, 0) - (0, 0, \mathbf{x}_6, 0)
\end{aligned}$$

As $(I, -I, 0, 0)$ is also in the span, so is $(\mathbf{x}_2, -\mathbf{x}_2, 0, 0)$ and then $(\mathbf{x}_2, -\mathbf{x}_2, 0, 0) + (0, \mathbf{x}_2, 0, 0) = (\mathbf{x}_2, 0, 0, 0)$ is there as well. Consequently all vectors $(\mathbf{x}_1, 0, 0, 0)$, $(\mathbf{x}_2, 0, 0, 0)$, $(\mathbf{x}_3, 0, 0, 0)$ and $(\mathbf{x}_5, 0, 0, 0)$ are in the linear span of $L_{v_1} \cup L_{v_2}$, thus there are all vectors of the form $(I, 0, 0, 0)$, as was required.

5 Impossibility of tight vector space construction

The *Ingleton inequality* (f) cited in section 1.3 holds for all representable matroids, and, in general, for all secret sharing schemes based on the general construction outlined in sections 1.3 and 4, see [15] . For the sake of the reader we repeat the inequality here:

$$\text{(f)} \quad f(AC) + f(AD) + f(BC) + f(BD) + f(CD) \geq \\ f(C) + f(D) + f(ACD) + f(BCD) + f(AB)\ .$$

Using this inequality we can check that the bound $2-2^{-n+1}$ got in Theorem 2 in *not* achievable by a vector space construction for $n \geq 4$. Should such a construction exist, the extremal point of the LP problem given in (5) would satisfy the Ingleton inequality (f) as well, which it does not. Apply (f) with the following cast:

$$A = v_2w_1, \quad B = v_3w_1, \quad C = v_1w_1, \quad D = w_1w_4$$

where, as usual, $v_i \in V$, $w_i \in W$ and v_i and w_i are connected. The left hand side value of (f) is

$$(4 - 2^{-n+2}) + (4 - 2^{-n+3}) + (4 - 2^{-n+2}) + (4 - 2^{-n+3}) + (4 - 2^{-n+2}) = \\ = 20 - 14 \cdot 2^{-n+1},$$

which is computed from values given in (5), while the value of the right hand side of (f) is

$$(3 - 2^{-n+1}) + 2 + (5 - 2^{-n+3}) + (5 - 2^{-n+3}) + (5 - 2^{-n+3}) = \\ = 20 - 13 \cdot 2^{-n+1}.$$

Consequently the value of the left hand side of (f) does *not* exceed that of the right hand side, i.e. the Ingleton inequality does not hold for this case.

Unfortunately we are not done. Equation (5) gives a feasible solution of the LP problem defined by all conditions in (a)–(e), and by the result in section 3 the solution (5) is on the boundary. Showing that this point does not satisfy a particular instance of the Ingleton inequality does not necessarily mean that another extremal solution wouldn't do it. So we prove the following stronger statement:

Theorem 4 *Let $n \geq 4$ and suppose the perfect secret sharing scheme on G_n is based on a vector space construction. Then the ratio is at least $2 - 2^{-n+1} + 0.2 \cdot 2^{-n+1}$, i.e. exceeds the lower bound of Theorem 2 by $0.2 \cdot 2^{-n+1}$.*

Proof Let f be any real valued function satisfying conditions (a)–(e) *and* all instances of the Ingleton inequality (f) where the subsets might contain the secret as well. We show that in this case $f(v) \geq 2 - 0.8 \cdot 2^{-n+1}$ for some vertex v which proves the Theorem.

As in section 3 the vertices of G_n are denoted by v_i, w_i for $1 \leq i \leq n$ so that v_i and w_i are connected, the subset $\{v_1, \ldots, v_n\}$ is a complete graph, while $\{w_1, \ldots, w_n\}$ is empty.

By Lemma 3 we may assume that

$$f(v_3w_2w_1) - f(w_2w_1) \geq 2 - 2^{-n+3} \tag{6}$$

by relabeling the vertices if necessary. Let moreover $v_\circ$, $w_\circ$ be the vertices v_4, w_4, respectively.

Claim 5 $f(v_1v_\circ) + f(w_1w_\circ) \geq f(v_1w_1w_\circ) + 2.$

Proof The claim follows from the following sequence of inequalities:

$$\begin{aligned} f(v_1v_\circ) &\overset{(1)}{\geq} f(v_1v_\circ) + \big(f(v_\circ w_\circ) - f(v_\circ) - f(w_\circ)\big) \geq \\ &\overset{(2)}{\geq} f(v_1v_\circ) + \big(f(v_1v_\circ w_\circ) - f(v_1v_\circ) + 1\big) - f(w_\circ) = \\ &= f(v_1v_\circ w_\circ) - f(w_\circ) + 1 \geq \\ &\overset{(3)}{\geq} \big(f(v_1w_\circ) + 1\big) - f(w_\circ) + 1 \geq \\ &\overset{(4)}{\geq} f(v_1w_1v_\circ) - f(w_1w_\circ) + 2. \end{aligned}$$

Here (1) follows from the submodular property $f(v_\circ) + f(w_\circ) \geq f(v_\circ w_\circ)$; (2) is the strict submodularity as both $v_1v_\circ$ and $v_\circ w_\circ$ are edges; (3) is strict monotonicity using that $v_1v_\circ$ is and edge and $v_1w_\circ$ is empty, finally (4) is the submodularity. □

Claim 6 $f(v_3v_2w_1) - f(w_1) \geq 4 - 2^{-n+3}$.

Proof Similarly as before, this is a consequence of the following sequence of inequalities:

$$\begin{aligned} & f(v_3v_2w_1) - f(w_1) = \\ &= \big(f(v_3v_2w_1) - f(v_2w_1)\big) + \big(f(v_2w_1) - f(w_1)\big) \geq \\ &\overset{(1)}{\geq} \big(f(v_3v_2w_2w_1) - f(v_2w_2w_1) + 1\big) + \big(f(v_2w_2w_1) - f(w_2w_1)\big) = \\ &= f(v_3v_2w_2w_1) - f(w_2w_1) + 1 = \\ &= \big(f(v_3v_2w_2w_1) - f(v_3w_2w_1)\big) + \big(f(v_3w_2w_1) - f(w_2w_1)\big) + 1 \geq \\ &\overset{(2)}{\geq} 1 + \big(2 - 2^{-n+3}\big) + 1. \end{aligned}$$

At (1) we applied strict submodularity and submodularity, while (2) follows from the choice of the indices of the vertices (cf. (6)), and from the strict monotonicity. □

Turning to the proof of the Theorem, we shall use a single instance of the Ingleton inequality (f) for the same case as at the beginning of this section, namely

$$A = v_2w_1, \quad B = v_3w_1, \quad C = v_1w_4, \quad D = w_1w_4,$$

and then (f) becomes

$$\begin{aligned} & f(v_2v_1w_1) + f(v_2w_1w_\circ) + f(v_3v_1w_1) + f(v_3w_1w_\circ) + f(v_1w_1w_\circ) \geq \\ & \quad \geq f(v_1w_1) + f(w_1w_\circ) + f(v_2v_1w_1w_\circ) + f(v_3v_1w_1w_\circ) + f(v_3v_2w_1). \end{aligned}$$

We continue with a series of inequalities which will be added to this one:

$$\begin{aligned} f(v_2v_1w_1w_\circ) &\overset{(1)}{\geq} f(v_2w_1w_\circ) + 1 \\ f(v_3v_1w_1w_\circ) &\overset{(1)}{\geq} f(v_3w_1w_\circ) + 1 \\ f(v_1w_1) + f(v_2v_1) &\overset{(2)}{\geq} f(v_1) + f(v_2v_1w_1) + 1 \\ f(v_1w_1) + f(v_3v_1) &\overset{(2)}{\geq} f(v_1) + f(v_3v_1w_1) + 1 \\ f(v_1) + f(w_1) &\geq f(v_1w_1) \\ f(v_1v_\circ) + f(w_1w_\circ) &\overset{(3)}{\geq} f(v_1w_1w_\circ) + 2 \\ f(v_3v_2w_1) &\overset{(4)}{\geq} f(w_1) + 4 - 2^{-n+3} \end{aligned}$$

Here (1) is strict monotonicity, (2) is strict submodularity, (3) comes from Claim 5, and (4) comes from Claim 6. The sum is

$$f(v_2v_1) + f(v_3v_1) + f(v_1v_\circ) \geq f(v_1) + 10 - 2^{-n+3}.$$

From here, using that $f(v_iv_j) \geq f(v_i) + f(v_j)$, we arrive at

$$2f(v_1) + f(v_2) + f(v_3) + f(v_\circ) \geq 10 - 2^{-n+3} = 10 - 4 \cdot 2^{-n+1}.$$

It means that not all of the values $f(v_1)$, $f(v_2)$, $f(v_3)$, $f(v_\circ)$ can be below $2 - 0.8 \cdot 2^{-n+1}$, proving the Theorem. □

6 Conclusion

We defined an sequence of graphs G_n, and considered perfect secret sharing schemes based on them. We established the best lower bound on the efficiency of the schemes the entropy method can give, and matched that lower bound for G_2 and G_3 by a novel construction. We also proved in Theorem 4 that no similar construction exists for other members of the family: any secret sharing scheme for G_n based on linear construction must have a strictly larger rate than the entropy method gives.

As all presently known constructions are based on some linear coding, they are subject to our result. Without breakthrough new results we cannot hope for a construction, even for G_4, which would match the lower bound $2 - 2^{-n+1}$.

Problem 7 *Show that $R(G_4) > 2 - 2^{-n+1}$, i.e. there is no perfect secret sharing scheme on G_4 which would match the entropy bound.*

There are further, non-Shannon type inequalities, cf. [24], which the function f in section 1.2 must satisfy beyond (a)–(e) enlisted there. The extremal point found in (5) satisfies these extra inequalities as well, thus they do not help in solving Problem 7 as they did in [1].

In section 4 we showed how to construct a scheme with ratio 2 for arbitrary n. Our result in Theorem 4 indicates, that any vector space construction must have higher ratio than the absolutely minimum given by the entropy method. This ratio, however, is still below 2, but we were unable to construct any such scheme in general. It is not hard to see that the scheme must follow the pattern outlined there, namely subspaces assigned to the 1-degree vertices can be assumed to be pairwise orthogonal, have similar connection to the secret subspace, and subspaces assigned to other vertices must follow similar pattern as well.

Also, if the ratio is below 2 then it is exponentially close to 2, which means that the vector space dimension must also be exponential (in n). But this contradicts to the intuition that we do not need more dimensions than the number of minimal qualified subsets multiplied by the dimension of the secret, which is definitely below n^3.

Problem 8 *Find a perfect secret sharing scheme on G_n, $n \geq 4$ with ratio strictly below 2, or show that no such a scheme exists.*

References

[1] A. Beimel, N. Livne, C. Padró: Matroids can be far from ideal secret sharing, *Proceedings of TCC'08*, LNCS **4948** (2008), pp. 194–212

[2] A. Beimel, N. Livne: On matroids and non-ideal secret sharing, In: Proc. of the third Theory of Cryptography Conference, Lecture Notes in Computer Science, Vol 3876(2006) pp. 482–501

[3] G. R. Blakley: Safeguarding cryptographic keys, *Proc.NCC AFIPS 1979*, pp. 313–317

[4] C. Blundo, A. De Santis, R. D. Simone, U. Vaccaro: Tight Bounds on the Information Rate of Secret Sharing Schemes, *Designs, Codes and Cryptography*, Vol 11(1997) pp. 107–110

[5] E. F. Brickell: Some ideal secret sharing schemes, *Journal of Combin. Math. and Combin. Computation*, Vol 6 (1989), pp 105–113

[6] R. M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro: On the size of shares of secret sharing schemes, *Journal of Cryptology*, vol 6(1993), pp. 157–168

[7] B. Chor, E. Kushilevitz: Secret sharing over infinite domains, *Journal of Cryptology*, Vol 6(1993) pp. 87–96

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

[9] L. Csirmaz: Secret sharing schemes on graphs, *Studia Mathematica Hungarica*, vol 44(2007) pp. 297–306 – available as IACR preprint `http://eprint.iacr.org/2005/059`

[10] L. Csirmaz, P. Ligeti: On an infinite families of graphs with information ratio $2-1/k$, Special Issue of Computing on the occasion CECC'08 to appear

[11] I. Csiszár and J. Körner: *Information Theory. Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1981.

[12] M. van Dijk: On the information rate of perfect secret sharing schemes, *Designs, Codes and Cryptography*, Vol 12(1997) pp. 143–169

[13] M. van Dijk, T. Kevenaar, G. Schrijen, P. Tuyls: Improved constructions of secret sharing schemes by applying (λ,ω)-decompositions, *Inf. Process. Lett.* vol 99(4), 2006, pp.154–157

[14] O. Ferràs, J. Martì-Farré, C. Padró: Ideal Multipartite Secret Sharing Schemes, Preprint (2006) `http://www-ma4.upc.edu/~cpadro/papers/mltprtt.pdd`

[15] A. W. Ingleton: Conditions for representability and transversability of matroids, in *Proc. Fr. Br. Conf 1970* pp 62–27, Springer-Verlag, 1971

[16] W. Jakson, K. M. Martin: Perfect secret sharing schemes on five participants, *Designs, Codes and Cryptography*, Vol 9(1996) pp. 233-250

[17] M. Karchmer, A. Widgerson: On span programs, In *Proc. of the 8th IEEE Trans on Information Theory* vol 29(1993) pp 102-111

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

[19] F. Matus: Matroid representations by partitions, *Discrete Mathematics*, vol 203(1999) pp. 169–194

[20] F. Matus: Adhesivity of polymatroids, *Discrete Mathematics*, Vol 307(2007) 21, pp 2464–2477

[21] A. Shamir: How to share a secret, *Communications of the ACM*, vol 22(1979), pp. 612–613

[22] D. R. Stinson: Decomposition constructions for secret sharing schemes, *IEEE Trans. Inform. Theory* IT-40 (1994) pp 118–125.

[23] D. J. A. Welsh: *Matroid theory*, Academic Press, London (1976).

[24] Z. Zhang, R. W. Yeung: On characterization of entropy function via information inequalities, *IEEE Trans. Inform. Theory* Vol 44, 1998, pp 1440–1452