The dealer's random bits in perfect secret sharing schemes

László Csirmaz*

Mathematical Institute of the Hungarian Academy of Sciences
Reáltanoda u. 13-15, Budapest, Hungary, H-1053

Abstract

A secret sharing scheme permits a secret to be shared among participants of an n-element group in such a way that only qualified subsets of participants can recover the secret. If any non-qualified subset has absolutely no information on the secret, then the scheme is called *perfect*. The *share* in a scheme is the information what a participant must remember. It was known that in any perfect secret sharing scheme realizing a certain collection of qualified sets over n participant, at least one participant must use at least $O(n/\log n)$ random bits for each bit in the secret. Here we present a collection of qualified sets so that the total number of random bits used by all the participants, i.e. the *dealer's random bits* is at least $O(n^2/\log n)$ for each bit in the secret.

Key words. Secret sharing, perfect secret sharing schemes, polymatroid structures, information theory.

1 Introduction

An important issue in secret sharing systems is the size of the shares distributed among the participants which has received considerable attention in the last few years, see e.g. [16], [5], [6], [9], etc. The reason is practical on one hand: the more information must be kept secret the less secure the system is since human being are not too good at remembering even medium size random data. On the other hand the problem is theoretically intriguing, too. All the known general constructions which work for arbitrary access structures assigns exponentially large shares. For a long time even it was not known whether the size of the shares should tend to infinity. The first results in this direction were [7] and [9] where an almost linear lower bound was given. In [9] the question for access

*This research was supported by OTKA grant no. 1911

structures based on graphs was settled: here the lower and upper bounds agree. For other access structures still there is a gap, and as it was remarked in [7], any better lower bound would yield an affirmative answer to a long standing question in information theory: are there more (linear) inequalities among the joint entropies of random variables which are not consequences of the known ones [8]?

In this paper we construct an access structure on which any perfect secret sharing scheme must use $n/4 \log n$ random bits for each secret bit *on average* for each participant, i.e. total $n^2/4 \log n$ bits. The construction in [7] gave an access structure where *some* (in fact, at least $\log n$) participant must use $O(n/\log n)$ random bits.

The paper is arranged as follows. First we give some definitions, and cite notions and facts from information theory which we shall use. Then we present the construction and prove that it is good. Finally we outline a conjecture about the entropy function.

2 Prerequisites

In this section we review the technical concepts both from information theory and from secret sharing which will be used in this paper. For a more complete treatment of information theory the reader is referred to [8]; its application to secret sharing is explained in [5].

2.1 Information Theoretic Notions

Given a probability distribution $\{p(x)\}_{x \in X}$ in a finite set X, define the *entropy* of X as

$$H(X) = -\sum_{x \in X} p(x) \log_2 p(x).$$

The entropy $H(X)$ is a measure of the average information content of the elements in X. By definition, the entropy is always non-negative.

Given two sets X and Y and a joint probability distribution $\{p(x,y)\}_{x \in X, y \in Y}$ on the Cartesian product of X and Y, the *conditional entropy* $H(X|Y)$ of X assuming Y is defined as

$$H(X|Y) = \sum_{y \in Y} p(y) H(X|Y = y), \tag{1}$$

where "$X|Y = y$" is the probability distribution got from p by fixing the value $y \in Y$. The conditional entropy can also given in the form

$$H(X|Y) = H(XY) - H(Y) \tag{2}$$

where Y is the marginal distribution. From definition (1) it is easy to see that $H(X|Y) \geq 0$.

The *mutual information* between X and Y is defined by

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$$
$$= H(X) + H(Y) - H(XY)$$

and is always non-negative: $I(X;Y) \geq 0$. This inequality expresses the intuitive fact that the knowledge of Y, on average, can only decrease the uncertainty one has on X.

Similarly to the conditional entropy, the *conditional mutual information* between X and Y given Z is defined as

$$I(X;Y|Z) = H(X|Z) - H(X|YZ)$$
$$= H(XZ) + H(YZ) - H(XYZ) - H(Z), \tag{3}$$

and is also non-negative: $I(X;Y|Z) \geq 0$. In fact, the only known (linear) inequalities for the entropy function are $H(X) \geq 0$, $H(X|Y) \geq 0$ and $I(x;Y|Z) \geq 0$ and their algebraic consequences. One of the open questions in information theory is to find more, or to show that there are none. We shall say more about it in the last section.

2.2 Secret Sharing Schemes

In the following individuals will be denoted by small letters: a, b, x, y, etc., sets (groups) of individuals by capital letters A, B, X, Y, etc., finally collection of groups by script letters $\mathcal{A}$, $\mathcal{B}$. We use P to denote the set of *participants* who will share the secret.

An *access structure* on an n-element set P of participants is a collection $\mathcal{A}$ of subsets of P: exactly the qualified groups are collected into $\mathcal{A}$. We shell denote a group simply by listing its members, so x denotes both a member of P and the group which consists solely of x.

A *secret sharing scheme* permits a secret to be shared among n participants in such a way that only qualified subsets of them can recover the secret. Secret sharing schemes satisfying the additional property that unqualified subsets can gain absolutely no information about the secret are called *perfect* as opposed to schemes where unqualified groups may have some information on the secret.

A natural property of access structures is *monotonicity*, i.e. $A \in \mathcal{A}$ and $A \subseteq B \subseteq P$ implies that $B \in \mathcal{A}$. This property expresses the fact that if any subset can recover the secret, then the whole group can also recover the secret. Also, a natural requirement is that the empty set should not be in $\mathcal{A}$, i.e. there must be some secret at all. Thus we may concentrate on *minimal* qualified subsets, no members of which can be dismissed without changing the subset into an unqualified one. We say that the access structure is *generated* by its minimal elements,

Let P be the set of participants, $\mathcal{A}$ be an access structure, and S be the set of possible secrets. A *secret sharing scheme*, given a secret $s \in S$, assigns to

each member $x \in p$ a random *share* from some domain. The shares are thus random variables with some disjoint distribution determined by the value of the secret s. Thus a scheme can be regarded as a collection of random variables, one for the secret, and one for each $x \in P$. The scheme determines the joint distribution of these $n+1$ random variables. For $x \in P$ the x's share, which is (the value of) a random variable, will also be denoted by x. For a subset $A \subseteq P$ of participants, A also denotes the joint (marginal) distribution of the shares assigned to the participants in A.

Following [5] we call the scheme *perfect* if the following hold:

1. Any qualified subset can reconstruct the secret, that is, the shares got by the participants in A determine uniquely the secret. This means $H(s|A) = 0$ for all $A \in \mathcal{A}$.

2. Any non qualified subset has absolutely no information on the secret, i.e. s and the shares got by members of A are statistically independent: knowing the shares in A, the conditional distribution of s is exactly the same as its a priori distribution. Translated to information theoretic notions this gives $H(s|A) = H(s)$ for all $A \notin \mathcal{A}$.

By the above description the entropy of the secret, $H(s)$ can be considered as the *length* of the secret. Any lower bound on the entropy of $x \in P$ gives immediately a lower bound on the size of x's share, and any lower bound on any subset $X \subseteq P$ of participants gives a lower bound on the *total* amount of random bits the dealer must have when distributing the shares among the participants.

2.3 Polymatroid structure

Let Q be any finite set, and $\mathcal{B} = 2^Q$ be the collection of the subsets of Q. Let $f : \mathcal{B} \to \mathbf{R}$ be a function assigning real numbers to subsets of Q and suppose f satisfies the following conditions:

(i) $f(A) \geq 0$ for all $A \subseteq Q$, $f(\emptyset) = 0$,

(ii) f is monotone, i.e. if $A \subseteq B \subseteq Q$ then $f(A) \leq f(B)$,

(iii) f is submodular, i.e. if A and B are different subsets of Q then $f(A) + f(B) \geq f(A \cap B) + f(A \cup B)$.

The system (Q, f) is called *polymatroid*. If, in addition, f takes only integer values and $f(x) \leq 1$ for one-element subsets, then the system is a *matroid*.

S. Fujishige in [10] observed that having a finite collection of random variables, we will get a polymatroid by assigning the entropy to each subset. The proof of the following proposition can also be found in [14].

Proposition 2.1 *By defining $f(A) = H(A)/H(s)$ for each $A \subseteq P \cup \{s\}$ we get a polymatroid.*

In our case the random variable s, the "secret" plays a special role. By our extra assumptions on the conditional entropies containing s we can calculate the value of $f(As)$ from $f(A)$ for any $A \subseteq P$, see [5, 14].

Proposition 2.2 *The secret sharing scheme is perfect if and only if for any $A \subseteq P$ we have*

if $A \in \mathcal{A}$ then $f(As) = f(A)$;

if $A \notin \mathcal{A}$ then $f(As) = f(A) + 1$.

Now let us consider the function f defined in Proposition 2.1 restricted to the subsets of P. From this restriction we can calculate easily the whole function; and since the extension is also a polymatroid, the restriction will satisfy some additional inequalities.

Proposition 2.3 *The function f defined in Proposition 2.1 satisfies the following additional inequalities:*

(i) *if $A \subseteq B$, $A \notin \mathcal{A}$ and $B \in \mathcal{A}$ then $f(B) \geq f(A) + 1$;*

(ii) *if $A \in \mathcal{A}$, $B \in \mathcal{A}$ but $A \cap B \notin \mathcal{A}$ then $f(A)+f(B) \geq f(A \cap B)+f(A \cup B)+1$.*

The method can be outlined as follows. We define an access structure on the n-element set P, an $A \subseteq P$, and show that for *any* polymatroid (P, f) satisfying (i) and (ii) above we have $f(A) \geq n^2/4 \log n$. By the discussion at the beginning of this section this implies that for any perfect secret sharing scheme $H(A)/H(s) \geq n^2/4 \log n$. This means that members of A has to remember $n/4 \log n$ bits for every secret bit on the average, and also that the dealer must use at least $n^2/4 \log n$ random bits for each secret bit for distributing the shares to the members of $\mathcal{A}$.

3 The construction

The first lemma expresses a trivial fact about qualified and unqualified subsets.

Lemma 3.1 *Let $A_1, \ldots, A_k$, and $B_1, \ldots, B_\ell$ be subsets of P. There exists an access structure $\mathcal{A}$ on P for which all A_i are qualified and all B_j are unqualified if and only if no B_j is a subset of any A_i.*

The next lemma is also the main lemma in [7]. Let $k > 1$ and $t < 2^k - 1$; X be a k-element set, $X_0 = X$, $X_1, \ldots, X_{2^k-1} = \emptyset$ all the subsets of X in such an order that if $i < j$ then $X_i \not\subseteq X_j$. (Reverse order, for example, by the size of the subsets.) Let $b_1, \ldots, b_t$ be individuals, not in X, and $B_0 = \emptyset$, $B_1 = \{b_1\}$, in general $B_j = \{b_1, \ldots, b_j\}$ for $j \leq t$.

Lemma 3.2 *Let $\mathcal{A}$ be an access structure on P, (P, f) be a polymatroid satisfying* (i) *and* (ii) *of Proposition 2.3; $Y \subseteq P$, X_j and B_j as above. Suppose that for each $j \leq t$, $Y \cup B_j \cup X_j \in \mathcal{A}$ and $Y \cup B_j \cup X_{j+1} \notin \mathcal{A}$. Then*

$$f(X \cup Y) - f(Y) \geq t + 1.$$

Proof. Observe that $Y \cup B_j \notin \mathcal{A}$ since it has a superset not in $\mathcal{A}$, and $Y \cup B_j \cup X \in \mathcal{A}$ since it has a subset in $\mathcal{A}$. Thus (i) of Proposition 2.3 gives immediately

$$f(Y \cup B_j \cup X) - f(Y \cup B_j) \geq 1. \tag{4}$$

Similarly, for each $0 \leq j < t$, (ii) of Proposition 2.3 gives

$$f(Y \cup B_{j+1} \cup X_{j+1}) + f(Y \cup B_j \cup X) \geq f(Y \cup B_j \cup X_{j+1}) + f(Y \cup B_{j+1} \cup X) + 1.$$

The submodular inequality applied to $Y \cup B_{j+1}$ and $Y \cup B_j \cup X_{j+1}$ yields

$$f(Y \cup B_{j+1}) + f(Y \cup B_j \cup X_{j+1}) \geq f(Y \cup B_j) + f(Y \cup B_{j+1} \cup X_{j+1}).$$

Adding up the last two inequalities, after rearranging we get

$$\big[f(Y \cup B_j \cup X) - f(Y \cup B_j)\big] - \big[f(Y \cup B_{j+1} \cup X) - f(Y \cup B_{j+1})\big] \geq 1. \tag{5}$$

This holds for $j = 0, \ldots, j = t - 1$. Since $B_0 = \emptyset$, adding (5) for all of these values to (4) gives the claim of the lemma. ∎

Theorem 3.3 *Let $k > 1$, $t < 2^k - 1$, $s \geq 1$. There is an access structure $\mathcal{A}$ on an $n = t + sk + \lceil \log_2 s \rceil$ element set P so that for any polymatroid (P, f) satisfying the conditions of Proposition 2.3, $f(P) \geq s(t + 1)$.*

Proof. Let $B_t = \{b_1, \ldots, b_t\}$; have $X^{(i)}$ exactly k elements for $1 \leq i \leq s$, finally let Z be a $\lceil \log_2 s \rceil$ element set, and Z_1, Z_2, …, Z_s be subsets of Z such that if $i < j$ then $Z_i \not\subseteq Z_j$. The set of participants P will be just the union of the disjoint sets B_t, $X^{(i)}$ and Z, obviously $|P| = n$. Let moreover $W^{(1)} = \emptyset$, $W^{(2)} = X^{(1)}$, $W^{(3)} = X^{(1)} \cup X^{(2)}$, …, $W^{(s+1)} = X^{(1)} \cup \ldots \cup X^{(s)}$, and $Y^{(i)} = Z_i \cup W^{(i)}$ for $1 \leq i \leq s + 1$.

Applying Lemma 3.2 to the sets $Y^{(i)}$, B_1, …, B_t, and $X^{(i)}$ we get

$$f(X^{(i)} \cup Y^{(i)}) - f(Y^{(i)}) \geq t + 1,$$

i.e.

$$f(Z_i \cup W^{(i+1)}) - f(Z_i \cup W^{(i)}) \geq t + 1.$$

The submodularity applied to $W^{(i+1)}$ and $Z_i \cup W^{(i)}$ gives

$$\big[f(W^{(i+1)}) - f(W^{(i)})\big] - \big[f(Z_i \cup W^{(i+1)}) - f(Z_i \cup W^{(i)})\big] \geq 0,$$

from where we get

$$f(W^{(i+1)}) - f(W^{(i)}) \geq t + 1.$$

Since $f(W^{(1)}) = f(\emptyset) = 0$ and $f(P) \geq f(W^{(s+1)})$ the claim of the theorem follows. We still have to check that there is an access structure so that conditions of Lemma 3.2 hold. Let the subsets of $X^{(i)}$ be $X_j^{(i)}$ as in the lemma; picking any i and j we must have $Y^{(i)} \cup B_j \cup X_j^{(i)} \in \mathcal{A}$, and $Y^{(k)} \cup B_\ell \cup X_{\ell+1}^{(k)} \notin \mathcal{A}$. By our observation 3.1 such an access structure exists if for no two different pairs (i, j) and (k, ℓ)

$$Y^{(i)} \cup B_j \cup X_j^{(i)} \subseteq Y^{(k)} \cup B_\ell \cup X_{\ell+1}^{(k)}.$$

Suppose on the contrary that this is the case. Replacing Y's with their definitions this means

$$Z_i \cup W^{(i)} \cup X_j^{(i)} \cup B_j \subseteq Z_k \cup W^{(k)} \cup X_{\ell+1}^{(k)} \cup B_\ell.$$

Since Z, B, and $W^{(s+1)}$ are pairwise disjoint, this inclusion means that $Z_i \subseteq Z_k$, $W^{(i)} \subseteq W^{(k)} \cup X_{\ell+1}^{(k)}$, and $B_j \subseteq B_\ell$. Now, if $i < k$ then by the choice of the Z's, $Z_i \not\subseteq Z_k$, and if $i > k$ then $W^{(i)}$ is a proper superset (and not a subset) of $W^{(k)} \cup X_{\ell+1}^{(k)}$. Therefore we must have $i = k$. Similarly, if $j < \ell + 1$ then $X_j^{(i)}$ is not a subset of $X_{\ell+1}^{(k)} = X_{\ell+1}^{(i)}$, finally if $j \geq \ell + 1$ then B_j is a proper superset of B_ℓ. No cases left, the claim is proved. ∎

To get the result announced in the Introduction, choose $k = \log(n/2)$, $t = n/2$, and $s = n/(2 \log n)$, this gives $f(P) \geq n^2/(4 \log n)$, as claimed. The following table summarizes the best values for k, t and s, and the coefficient λ so that $f = n^2/\lambda_n \log_2 n$. It is not hard to see that λ_n converges to 4 as n tends to infinity.

n	f	λ_n	t	s	k
3	2	2.839184	1	1	2
4	2	4.000000	1	1	3
5	3	3.588971	2	1	3
10	8	3.762875	3	2	3
20	24	3.856304	11	2	4
30	52	3.527222	12	4	4
50	116	3.818617	28	4	5
100	400	3.762875	49	8	6
200	1386	3.775585	98	14	7
400	4900	3.777603	195	25	8
800	17556	3.780103	398	44	9
1600	63520	3.786435	793	80	10
3200	231710	3.795407	1597	145	11
6400	851200	3.805825	3199	266	12

4 Conclusion

There are several general methods for generating shares, see [2, 16]. These usually work well on "structured" access structures, but assign exponentially large shares on the worst case. We have constructed an access structure on an n-element group so that in any perfect secret sharing scheme the dealer must use at least $n^2/4 \log n$ random bits for each bit in the secret. This shows that any method must assign almost linear shares on the average in some cases.

Karchmer and Wigderson in [13] showed that there is a strong connection between the so-called (monotone) span programs and certain secret sharing schemes. Thus our result also gives immediately a lower bound for the size of span programs. Beimel, Gál, and Paterson in [1] gave general lower bounds for the size of span programs, which implies that for some access structure on n participants, if the scheme is of Karchmer–Wigderson type the dealer must use at least $c \cdot n^2$ random bits for each secret bit.

Given any, say random, access structure $\mathcal{A}$ on a set P of n participants, all perfect secret sharing schemes can be generated as follows.

(i) devise a polymatroid (P, f) satisfying the conditions of Proposition 2.2, and then

(ii) *realize* f by assigning random variables to each participant so that for each $A \subseteq P$, $f(A) = \lambda \cdot H(A)$ for some constant λ.

The total number of random bits used by the dealer will then be $\lambda H(P)$.

The lower bound proved in the present paper comes from (i). We showed that for a particular access structure every feasible polymatroid must satisfy $f(P) \geq O(n^2/\log n)$. We cannot push it higher since for any access structure there exists a polymatroid with $f(P) \leq n^2$. Thus we have to concentrate on (ii) and consider only *representable* polymatroids. Unfortunately very little is known along this line. For $n \leq 3$ all polymatroids are representable. For $n = 4$ F. Matuš in [15] gives a non representable polymatroid. In fact, he proves that if $P = \{a, b, c, d\}$ and (P, f) is a polymatroid then

$$f(ac) + f(bc) + f(ad) + f(bd) + f(cd) - f(c) - f(d) - f(acd) - f(bcd) - f(ab) \geq -\frac{1}{4} f(abcd),$$

and for representable polymatroids equality holds only if $f(abcd) = 0$. There are polymatroids for which equality holds here, thus they are not representable. It is interesting to note that the left hand side also appears in matroid theory: it cannot be negative for matroids representable over fields [11]. For those more familiar with the entropy function the above inequality can be written as

$$I(a; b) + I(c; d|a) + I(c; d|b) - I(c; d) \geq -\frac{1}{4} H(abcd),$$

and is the consequence of the usual entropy inequalities. We conjecture that for representable polymatroids (i.e. for random variables) the constant 1/4 can be replaced by a much smaller value. Showing that it holds with any value less than 1/4 would also give a new linear inequality for the entropy thus settling an important open problem of information theory.

Conjecture 4.1 *If a, b, c, and d are random variables, then*

$$I(a;b) + I(c;d|a) + I(c;d|b) - I(c;d) \geq -0.09876...H(abcd),$$

and equality attained, for example, if all variables take only 0-1 values, $c = \min(a,b)$, $d = \max(a,b)$, and

$$\begin{aligned} \text{Prob}(a=0,b=0) &= \text{Prob}(a=1,b=1), \\ \text{Prob}(a=0,b=1) &= \text{Prob}(a=1,b=0). \end{aligned}$$

References

[1] A. Beimel, A. Gál, M. Paterson, Lower bounds for monotone span programs, Preprint, 1994

[2] G. R. Blakley and C. Meadows, Security of Ramp Schemes, *Proceeding of Crypto'84 – Advances in Cryptology,* Lecture Notes in Computer Science, Vol 196, G. R. Blakley and D. Chaum, eds. Springer-Verlag, Berlin, 1985, pp. 411-431.

[3] C. Blundo, A. De Santis, L. Gargano, U. Vaccaro, On the Information Rate of Secret Sharing Schemes, in *Advances in Cryptology – CRYPTO '92*, Lecture Notes in Computer Science, Vol 740, E. Brickell ed, Springer-Verlag, Berlin, 1993, pp. 149-169.

[4] C. Blundo, A. De Santis, A. G. Gaggia, U. Vaccaro, New Bounds on the Information Rate of Secret Sharing Schemes, Preprint, 1993

[5] R. M. Capocelli, A. De Santis, U. Vaccaro, On the Size of Shares for Secret Sharing Schemes, *Journal of Cryptology*, Vol 6(1993) pp. 157-167.

[6] M. Carpentieri, A. De Santis, U. Vaccaro, Size of Shares and Probability of Cheating in Threshold Schemes, *Proceeding of Eurocrypt'93.*

[7] L. Csirmaz, The size of a share must be large, *Journal of Cryptology*, to appear

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

[9] M. van Dijk, On the Information Rate of Perfect Secret Sharing Schemes, Preprint, 1994

[10] S. Fujishige, Polymatroid dependence structure of a set of random variables, *Information and Control* 39(1978) pp. 55-72.

[11] A. W. Ingleton, Conditions for representability and transversality of matroids, *Proceeding of Fr. Br. Conf* Springer Lecture Notes 211(1970), pp. 62-67

[12] M. Ito, A. Saito, T. Nishizeki, Multiple Assignment Scheme for Sharing Secret *Journal of Cryptology*, Vol 6(1993) pp. 15-20.

[13] M. Karchmer and A. Wigderson, On span programs in: *Proceedings of the 8th annual structure in complexity theory* (1993) pp. 102-111

[14] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, S. Tsujii, Nonperfect Secret Sharing Schemes and Matroids, *Proceedings of Eurocrypt'93*.

[15] F. Matuš, Ascending and descending conditional independence relations, *Transactions of the 11th Prague Conference on Information Theory* Academia, Prague, Vol B, pp. 181-200

[16] G. J. Simmons, An Introduction to Shared Secret and/or Shared Control Schemes and Their Application, *Contemporary Cryptology, IEEE Press* pp. 441-497, 1991.