# Complexity of universal access structures

László Csirmaz*

Central European University, Budapest
Rényi Institute, Budapest

**Abstract**

An important parameter in a secret sharing scheme is the number of minimal qualified sets. Given this number, the universal access structure is the richest possible structure, namely the one in which there are one or more participants in every possible Boolean combination of the minimal qualified sets. Every access structure is a substructure of the universal structure for the same number of minimal qualified subsets, thus universal access structures have the highest complexity given the number of minimal qualified sets. We show that the complexity of the universal structure with $n$ minimal qualified sets is between $n/\log_2 n$ and $n/2.7182\ldots$ asymptotically.

**Keywords:** secret sharing; complexity; entropy method; harmonic series.
**MSC numbers:** 94A62, 90C25, 05B35.

## 1 Introduction

In a secret sharing scheme the access structure defines which subsets of the participants should recover the secret – these are the *qualified subsets*. Unqualified subsets are also called *independent*. The collection of qualified subsets is determined uniquely by the *minimal* qualified sets. Suppose in an access structure we have $n$ minimal qualified sets: $A_1, \ldots, A_n$. For $\varepsilon_i = 0$ or 1 let $A_i^{\varepsilon_i}$ be $A_i$ when $\varepsilon_i = 1$, and the complement of $A_i$ when $\varepsilon_i = 0$. The access structure is *universal* if none of the $2^n$ possible intersections $\bigcap A_i^{\varepsilon_i}$ is empty. In this note $\mathcal{U}_n$ denotes a universal access structure with $n$ qualified subsets.

Universal structures with at most three minimal qualified sets were investigated in [3, 4], and for four qualified sets in [5]. For $n = 2$ and $n = 3$ the exact complexity is known: it is 1 and 3/2, respectively. For $n = 4$ it is proved in [5] that the complexity of $\mathcal{U}_4$ is between 7/4 and 11/6, the exact value is not known. This paper provides the first bounds for the compexity of $\mathcal{U}_n$ for larger values

*This research was partially supported by the "Lendület Program" of the Hungarian Academy of Sciences and by the grant NKTH OM-00289/2008

of $n$. The upper bound follows from a secret sharing scheme defined recursively for each $n$. The lower bound is a well-tailored application of the *independent sequence method* described, e.g., in [1].

## 2 Reduction

First we note that the number of participants in each class $\bigcap A_i^{\varepsilon_i}$ is irrelevant: the complexity of the scheme does not depend on the number of participants in the classes, it depends only on which classes are empty and which are not. Consequently, for each $n$, we can define a unique "general" universal access structure with $n$ minimal qualified sets. As a first step, we can evidently discard all participants who are not in any of the qualified sets as they can play no role in recovering the secret. Less trivially we can also discard those participants which are in all of the qualified sets. Details follow.

Let $\mathcal{U}_n^*$ be the *normalized* structure with $n$ minimal qualified sets $A_1$, ..., $A_n$, where the intersection $\bigcap A_i^{\varepsilon_i}$ has exactly one element when not all the $\varepsilon_i$ are equal, and is empty otherwise. In particular, the structure $\mathcal{U}_n^*$ is *connected*, no participant is in all, or none, of the minimal qualified subsets, and has exactly $2^n - 2$ participants.

**Claim 1** *The complexity of the structures $\mathcal{U}_n$ and $\mathcal{U}_n^*$ are equal: $\sigma(\mathcal{U}_n) = \sigma(\mathcal{U}_n^*)$*

**Proof** Let $\mathcal{S}$ be any scheme realizing $\mathcal{U}_n$. Pick one participant from each class $\bigcap A_i^{\varepsilon_i}$ except when all the $\varepsilon_i$'s are equal, $2^n - 2$ participants in total. Make the shares of all other participants public. This defines a scheme $\mathcal{S}^*$ realizing the access structure $\mathcal{U}_n^*$, and it is clear that the complexity of $\mathcal{S}^*$ is less than or equal to the complexity of $\mathcal{S}$. This establishes $\sigma(\mathcal{U}_n^*) \leq \sigma(\mathcal{U}_n)$.

To see the other direction, let $\mathcal{S}^*$ be a scheme realizing $\mathcal{U}_n^*$. For the sake of simplicity we assume that the secret for $\mathcal{S}^*$ is a single random bit. Define the scheme $\mathcal{S}$ for $\mathcal{U}_n$ as follows. Write the random bit $s$ as the mod 2 sum of two random independent bits $r_1$ and $s_1$:

$$s = r_1 \oplus s_1.$$

The secret for $\mathcal{S}$ will be $s$. Use any perfect ideal $k$ out of $k$ threshold scheme to distribute $r_1$ among participants in the intersection $\bigcap A_i$. That is, all participants from this set together can reconstruct $r_1$, but no proper subset of them (or any any other subset not containing all participants from $\bigcap A_i$) has any information on $r_1$. Next, distribute $s_1$ according to the scheme $\mathcal{S}^*$. Participants in the intersection $\bigcap A_i^{\varepsilon_i}$ (not all $\varepsilon_i$ are equal) will be able to recover the share what $\mathcal{S}^*$ assigns to them using again an independent realization of a perfect ideal $k$ out of $k$ threshold scheme (different $k$, of course). It is clear that qualified subsets of $\mathcal{U}_n$ can recover the secret $s$, while unqualified subsets have no information on it. The complexity of $\mathcal{S}$ is $\max\{1, \sigma(\mathcal{S}^*)\}$ (here 1 comes from distributing $r_1$) as threshold schemes have complexity 1. This establishes $\sigma(\mathcal{U}_n) \leq \sigma(\mathcal{U}_n^*)$ as required. □

**Claim 2** $\sigma(\mathcal{U}_2) = 1$.

**Proof** In $\mathcal{U}_2^*$ there are $2^2 - 2 = 2$ participants, and both of them form a one-element qualified set. Simply give the secret to both of them. □

# 3 Upper bound

In this section we define a perfect scheme realizing $\mathcal{U}_n^*$ by recursion on $n$. Using this scheme we establish an upper bound for the complexity of the universal scheme. We call participants $p$ and $q$ of $\mathcal{U}_n^*$ *equivalent* if there is a permutation $\pi$ on the full set of participants which sends $p$ to $q$ and maps all qualified subsets into qualified subsets, i.e., $\pi$ is an automorphism of the structure $\mathcal{U}_n^*$. It is easy to see that $p$ and $q$ are equivalent if and only if both of them are members of exactly the same number of minimal qualified sets. Thus there are $n-1$ equivalence classes, one for each $i = 1, \ldots, n-1$.

Suppose $\mathcal{S}_n$ realizes $\mathcal{U}_n^*$. Using the standard symmetrization technique we may assume that $\mathcal{S}_n$ is *fully symmetrical*, that is, equivalent participants receive shares of the same size. We denote by $f_n(i)$ this common size of the shares of those who are in exactly $i$ qualified subsets divided by the size of the secret. The complexity of the scheme $\mathcal{S}_n$ is then

$$\sigma(\mathcal{S}_n) = \max\{f_n(i) \,:\, 1 \le i < n\}.$$

Let us also define $f_n(0) = 0$ and $f_n(n) = 1$.

**Lemma 3** *Suppose $\mathcal{S}_n$ realizes $\mathcal{U}_n^*$ with $f_n(i)$ as defined above. Then there is a perfect scheme $\mathcal{S}_{n+1}$ realizing $\mathcal{U}_{n+1}^*$ such that*

$$n \cdot f_{n+1}(i) = (n+1-i) \cdot f_n(i) + i \cdot f_n(i-1) \quad \textit{for all} \quad 0 < i \le n. \qquad (1)$$

**Proof** We will use Stinson's decomposition technique from [7]. Given $U_{n+1}^*$ define $n+1$ access structures $\Gamma_1, \ldots, \Gamma_{n+1}$ such that the set of participants is the same, while in $\Gamma_j$ the $j$-th minimal qualified subset is left out. By the assumption and by Claim 1 above there are perfect schemes realizing $\Gamma_j$ such that participants in $i$ out of the $n$ qualified subsets of $\Gamma_j$ receive $f_n(i)$-size shares for all $0 \le i \le n$.

Now use all of these $n+1$ schemes simultaneously. Each (minimal) qualified subset of $U_{n+1}^*$ recovers exactly $n$ out of the $n+1$ distributed secrets, while an unqualified subset has no information on any of those secrets. Using Stinson's trick from [7] we can define a secret of size $n$ and $n+1$ shadows of size 1 each so that the secret can be determined by any $n$ of the shadows. Thus the composite scheme will distribute a secret of size $n$. A participant who is in exactly $i$ of the minimal qualified subsets will receive shares of size $f_n(i-1)$ from $\Gamma_j$ when $j$ is one of the minimal qualified subsets he is in ($i$ in total), and shares of size $f_n(i)$ from $\Gamma_j$ when $j$ is one of the minimal qualified subsets he is not in ($n+1-i$ in total). This establishes the claim of the lemma. □

**Lemma 4** *Suppose $f_n(0) = 0$, $f_n(n) = 1$, $f_2(1) = 1$ and for $n \geq 2$ the function $f_{n+1}$ satisfies the recursion in* (1)*. Then*

$$f_n(i) = (n-i)\big(h(n) - h(n-i)\big) \quad \textit{for all} \quad 0 \leq i < n, \tag{2}$$

*where $h(1) = 0$ and $h(n) = \sum_{0<j<n} 1/j$ otherwise.*

**Proof** When $i = 0$ then, by definition, $f_n(0) = 0$, and (2) also yields 0. (2) also gives

$$f_2(1) = h(2) - h(1) = 1 - 0 = 1.$$

Suppose (2) holds for $n \geq 2$ and $0 < i < n$. Equation (1) can be rewritten as

$$\frac{f_{n+1}(i)}{n+1-i} = \frac{n-i}{n} \cdot \frac{f_n(i)}{n-i} + \frac{i}{n} \cdot \frac{f_n(i-1)}{n+1-i} \tag{3}$$

Now $h(n+1) = h(n)+1/n$, and $h(n+1-i) = h(n-i)+1/(n-i)$. Consequently

$$h(n+1) = h(n) + \frac{1}{n} = \frac{i}{n} \cdot h(n) + \frac{n-i}{n} \cdot h(n) + \frac{1}{n},$$
$$h(n+1-i) = \frac{i}{n} \cdot h(n+1-i) + \frac{n-i}{n} \cdot \big(h(n-i) + \frac{1}{n-i}\big),$$

that is

$$h(n+1) - h(n+1-i) = \frac{n-i}{n}\big(h(n) - h(n-i)\big) + \frac{i}{n}\big(h(n) - h(n+1-i)\big).$$

This shows that the function $h(n) - h(n-i)$ satisfies the recursion (3), that is $f_n(i) = (n-i)\big(h(n) - h(n-i)\big)$ for all $n$ and $i$ by induction. □

**Theorem 5** *The complexity of $\mathcal{U}_n$ is asymptotically at most $n/e$ where $e = 2.7182\ldots$ is the Euler number.*

**Proof** By Lemma 3 there is a scheme $\mathcal{S}_n$ realizing $\mathcal{U}_n$ with complexity

$$\sigma(\mathcal{S}_n) = \max\{f_n(i) \,:\, 1 \leq i < n\}$$

where, by Lemma 4 $f_n(i) = (n-i)\big(h(n) - h(n-i)\big)$. Now

$$f_n(i+1) - f_n(i) = h(n-i) + 1 - h(n). \tag{4}$$

As $h(n-i)$ is strictly decreasing, $f_n$ increases while $h(n-i) \geq h(n) - 1$, and decreases after this value of $i$, and takes its maximum when (4) changes sign. Using the approximation $h(x) = \gamma + \log(x - 1/2) + O(x^{-2})$ from [6] where $\gamma$ is the Euler-Mascheroni constant, this happens when

$$n - i = \frac{n}{e} + \frac{e-1}{2e} + O(1/n),$$

and then the maximal value of $f_n$ taken at this $i$ is

$$f_n(i) = (n-i)\big(1 + O(1/n)\big) = \frac{n}{e} + \frac{e-1}{2e} + O(1/n).$$

From here the theorem follows. □

A more careful analysis shows that

$$\max_i f_n(i) < \frac{n}{e} + \frac{e-1}{2e} + \frac{1}{3n} < \frac{n}{e} + 0.5$$

for all $n \geq 2$ which gives a non-asymptotic estimate on the complexity of $\mathcal{S}_n$.

# 4 Lower bound

As mentioned in the Introduction, for the lower bound we use a variation of the *independent sequence method* from [1]. For a general description how the method works, see, e.g., [1, 2]. Briefly, for any subset $A$ of the participant one considers the *relative entropy* $f(A)$, which is simply the entropy of all the shares given to members of $A$ divided by the entropy of the secret. The function $f$ satisfies a certain set of linear inequalities derived from the Shannon inequalities for the entropy function. For example, $f(\emptyset) = 0$, for arbitrary subsets $A$ and $B$ of the participants

$$f(AB) \leq f(A) + f(B),$$

or, $f(B) \leq f(A)$ when $B \subseteq A$. This latter inequality is called *monotonicity*. The *strict monotonicity property* says that whenever $B$ is independent and $B \subseteq A$ is qualified then not only $f(A)$ is larger than $f(B)$, but the difference is at least one: $f(B) + 1 \leq f(A)$. As a particular case,

$$f(A) \leq f(a_1) + f(a_2) + \cdots + f(a_k) \tag{5}$$

when $A = \{a_1, \ldots, a_k\}$. Here and the in the sequel, as usual, we write $f(a)$ instead of $f(\{a\})$, and write $AB$ and $Aa$ instead of $A \cup B$ and $A \cup \{a\}$, respectively.

The *entropy method* works as follows. To prove that the complexity of an access structure is at least $\kappa$ it is enough to show that for all non-negative functions $f$ satisfying all of the above inequailities there is a participant $p$ with $f(p) \geq \kappa$.

The *independent sequence method* relies on the following lemma which we cite without proof from [2].

**Lemma 6** *Suppose $B \subseteq A$, $p$ is a participant not in $A$, and for some $B \subseteq C \subseteq A$, $C$ is independent, while $Cp = C \cup \{p\}$ is qualified. Then $f(A) - f(B) \geq f(Ap) - f(Bp) + 1$.* □

The next lemma summarizes the method itself.

**Lemma 7 (Independent sequence method)** *Supppose $A_0$ is a qualified set, $B_0$ is the empty set, and $b_1$, ..., $b_n$ are participants not in $A_0$. Let $B_i = \{b_1, \ldots, b_i\}$, and $A_i = A_0 \cup B_i$. Suppose that for all $0 \leq i < n$ there is a subset $C_i \subset A_0$ such that $B_iC_i$ is independent, while $B_{i+1}C_i = b_{i+1}B_iC_i$ is qualified. Then $f(A_0) \geq n$.*

In the usual terminology the sequence $A_0$, $A_1$, ... is *made independent* by the sequence $B_0$, $B_1$, ... from where the method got its name.

**Proof** By the monotonicity of the function $f$, $f(A_n) - f(B_n) \geq 0$ as $A_n \supseteq B_n$. By Lemma 6,

$$f(A_i) - f(B_i) \geq f(A_{i+1}) - f(B_{i+1}) + 1$$

which is shown by the set $C = B_iC_i$ and the participant $p = b_{i+1}$. Putting all of these inequalities together we get

$$f(A_0) - f(B_0) \geq n.$$

As $B_0$ is the emptyset, $f(B_0) = 0$ and the claim of the lemma follows. □

As it was remarked in the Introduction, among all access structures with $n$ minimal qualified subsets, $\mathcal{U}_n$ has the highest complexity. Consequently to show that $\mathcal{U}_n$ has complexity at least $\kappa$ it is enough to find *any* access structure with $n$ minimal qualified subsets with complexity $\geq \kappa$. This is exactly what we will do.

**Theorem 8** *For each $n \geq 2$ there is an access structure with $n$ minimal qualified subsets and complexity at least $n/(1 + \log_2 n)$.*

**Proof** Let $k \geq 1$ to be chosen later and $X$ be a set with exactly $k$ elements. Enumerate the proper subsets of $X$ in *decreasing order* as $C_0, C_1, \ldots, C_{\ell-1} = \emptyset$ where $\ell = 2^k - 1$. "Descreasing" means that sets with larger index does not have more elements; in particular $C_i \not\subset C_j$ whenever $0 \leq i < j < \ell$.

Let $b_1, \ldots, b_\ell$ be new participants not in $X$, and define $B_0 = \emptyset$, and for $1 \leq i \leq \ell$ let $B_i$ be the set $\{b_1, b_2, \ldots, b_i\}$. There will be $n \leq \ell$ minimal qualified subsets: $B_1C_0$, $B_2C_1$, $\ldots$, $B_nC_{n-1}$. These sets can indeed form a collection of minimal qualified subsets as none of them is a subset of any other. Also we remark that the sets $B_iC_i$ for $0 \leq i < n$ are *independent* as none of $B_{j+1}C_j$ is a subset of $B_iC_i$. Indeed, if $j \geq i$ then $B_{j+1}$ is not a subset of $B_i$, and if $j < i$ then $C_j$ is not a subset of $C_i$. Thus we can apply Lemma 7 with $A_0 = X$ giving

$$f(X) \geq n.$$

As $X$ has $k$ elements, say $a_1, \ldots, a_k$, applying property (5) we get

$$f(a_1) + \cdots + f(a_k) \geq f(X) \geq n,$$

meaning that some participant in this access structure has an $f$-value at least $n/k$. Thus the complexity of the structure is also at least $n/k$. Our aim is to choose $k$ as small as possible. We have only a single restriction, namely that $n$ should not exceed the value $\ell = 2^k - 1$. Thus there is always an approriate $k$ which is less than or equal to $(1 + \log_2 n)$, proving the theorem. □

As a consequence of Theorem 8 the universal structure $\mathcal{U}_n$ also has complexity at least $n/(1 + \log_2 n)$, proving that the complexity is at least $n/\log_2 n$ asymptotically.

# References


[1] C. Blundo, A. De Santis, R. De Simone, U. Vaccaro: Tight Bounds on the Information Rate of Secret Sharing Schemes, *Designs, Codes and Cryptography*, vol 11(2) (1997), pp. 107–110

[2] L. Csirmaz: An impossibility result on graph secret sharing, *Designs, Codes and Cryptography*, vol 53 (2009), pp 195–209

[3] J. Martí-Farré, C. Padró. Ideal secret sharing schemes whose minimal qualified subsets have at most three participants. *Designs, Codes and Cryptography* 52 (2009) 1-14.

[4] J. Martí-Farré, C. Padró. Secret sharing schemes with three or four minimal qualified subsets. *Designs, Codes and Cryptography* 34 (2005) 17-34.

[5] J. Martí-Farré, C. Padró, L. Vzquez. Optimal Complexity of Secret Sharing Schemes with Four Minimal Qualified Subsets. Manuscript, to appear in *Designs, Codes and Cryptography*. Available as `http://www3.ntu.edu.sg/home/carlespl/papers/sss4mqs.html`

[6] J. Sondow, E. W. Weisstein. Harmonic Number. *From MathWorld – A Wolfram Web Resource*. `http://mathworld.wolfram.com/HarmonicNumber.html`

[7] D. R. Stinson: Decomposition Constructions for Secret-Sharing Schemes *IEEE Transactions on Information Theory*, vol 40(1) (1994) pp. 118–125