Research Article

Laszlo Csirmaz*

Secret sharing and duality

https://doi.org/10.1515/jmc-2019-0045
Received Oct 02, 2019; accepted Apr 30, 2020

Abstract: Secret sharing is an important building block in cryptography. All explicit secret sharing schemes which are known to have optimal complexity are multi-linear, thus are closely related to linear codes. The dual of such a linear scheme, in the sense of duality of linear codes, gives another scheme for the dual access structure. These schemes have the same complexity, namely the largest share size relative to the secret size is the same. It is a long-standing open problem whether this fact is true in general: the complexity of any access structure is the same as the complexity of its dual. We give a partial answer to this question. An almost perfect scheme allows negligible errors, both in the recovery and in the independence. There exists an almost perfect ideal scheme on 174 participants whose complexity is strictly smaller than that of its dual.

Keywords: secret sharing; ideal access structure; matroid; duality; matroid ports, almost entropic polymatroid

AMS subject classification: 05B35, 94A15, 06D50, 94A62

1 Introduction

The complexity of a secret sharing scheme is the largest share size relative to the secret size. An access structure is ideal if it can be realized by a scheme of complexity 1. The open question that has been posed in many papers is if there exists an ideal structure whose dual is not ideal. And, more generally, if the optimal complexity of an access structure is preserved by duality. This paper gives a partial answer to these questions by using a different secret sharing model. This model allows negligible errors, both in secret recovery and in the independence; "almost" refers to this relaxed model. The construction of a secret sharing scheme whose almost complexity differs from its dual's one is a *tour de force* connecting several different pieces of earlier results. Theorems 19 and 20 state the equivalence of secret sharing conjectures and matroid representation problems using the standard and the relaxed models, respectively. The final construction in Section 4 is based on the second theorem. Settling the duality conjecture in the standard model is an interesting research work, a possible direction is indicated in the last section.

We assume familiarity with secret sharing schemes, for an overview consult [1]. A significant portion of matroid and polymatroid theory is used. The standard textbook for matroids is [21], for polymatroids see [13] and works of F. Matúš [15, 16]. Nevertheless, most of the theorems and claims are proved here – a notable exception is F. Matúš result from [17].

Following the usual practice, sets and their subsets are denoted by capital letters, their elements by lower case letters. The union sign $\cup$ is frequently omitted as well as the curly brackets around singletons. Thus asP denotes the set $\{a, s\} \cup P$. The set difference operator has lower priority than the union, thus $aA-bB$ is $(\{a\} \cup A)-(\{b\} \cup B)$.

Dedicated to the memory of Frantisek Matúš

***Corresponding Author: Laszlo Csirmaz:** Laszlo Csirmaz, Alfred Renyi Institute of Mathematics, Budapest, Hungary; Email: csirmaz@renyi.hu

The paper is organized as follows. Section 2 introduces polymatroids, secret sharing, complexity measures, duality, and concludes with conjectures on the complexity of dual structures. Section 3 presents two questions on matroid representability and proves that they are equivalent to the conjectures. Section 4 gives a detailed account of Tarik Kaced's result on almost entropic matroids [10], completing the tour. Some open problems are listed in Section 5. Two proofs are postponed to the Appendix: the first is on matroid circuits used in Claim 5, the second is the the MMRV entropy inequality used in the proof of Theorem 21.

2 Preliminaries

2.1 Polymatroids

A *polymatroid* $\mathcal{M} = (f, M)$ is a non-negative, monotone and submodular function f defined on the collection of non-empty subsets of the finite set M. Here M is the *ground set*, and f is the *rank function*. If f takes non-negative integer values only, then $\mathcal{M}$ is *integer*; an integer polymatroid is a *matroid* if the rank of singletons are either zero or one. Polymatroids can be identified to vectors in the $(2^{|M|}-1)$-dimensional Euclidean space where the coordinates are indexed by subsets of M. The collection of polymatroids with ground set M is a full-dimensional pointed polyhedral cone denoted by Γ_M, see [23].

For a discrete random variable ξ its information content is measured by the Shannon entropy $\mathbf{H}(\xi)$, see [23]. Let $\xi = \langle \xi_i : i \in M \rangle$ be a collection of discrete random variables with some joint distribution. For a subset $A \subseteq M$, the subcollection $\langle \xi_i : i \in A \rangle$ is denoted by ξ_A. The *conditional entropy* of random variables ξ_A and ξ_B is $\mathbf{H}(\xi_A|\xi_B) = \mathbf{H}(\xi_{A\cup B}) - \mathbf{H}(\xi_B)$ with value between zero an $\mathbf{H}(\xi_A)$. The value is zero if and only if ξ_A is determined completely by ξ_B, and equals $\mathbf{H}(\xi_A)$ if and only if the random variables ξ_A and ξ_B are independent.

As observed by Fujishige [7], the function $A \mapsto \mathbf{H}(\xi_A)$ is a rank function of a polymatroid which we denote by $\mathcal{M}_\xi$. The polymatroid $\mathcal{M}$ is *entropic* if it can be got this way. The collection of entropic polymatroids on the ground set M is $\Gamma^*_M \subseteq \Gamma_M$. For $|M| \geq 3$ the set Γ^*_M is not closed (in the usual Euclidean topology). Polymatroids in the closure of Γ^*_M are called *almost entropic*, or just *aent*. Aent polymatroids form a full-dimensional convex cone, and every internal point of this cone is entropic [17]. For $|M| \geq 4$ there is a polymatroid in Γ_M with a positive distance from the aent cone [23]; and the aent cone is not polyhedral [18].

By an abuse of notation, we say that $\mathcal{M}$ is an *entropic matroid* if $\mathcal{M}$ is a matroid and for some positive real number λ the polymatroid $\lambda\mathcal{M}$ is entropic.

The singleton $e \in M$ in the polymatroid (f, M) is a *loop* if it has rank zero. In terms of entropic polymatroid being a loop means that the variable ξ_e is deterministic: takes a single value with probability 1. If not mentioned otherwise, polymatroids in this paper have no loops.

With an eye on entropic polymatroids, disjoint subsets A, B of the ground set M are called *independent* if $f(AB) = f(A)+f(B)$. If A and B are independent, $A' \subseteq A$, $B' \subseteq B$, then A' and B' are independent as well – this follows from the submodularity of the rank function. The single subset A is *independent* if any two disjoint subsets of A are independent. In other words, A is independent iff

$$f(A) = \sum \{f(i) : i \in A\}.$$

A *base* is a maximal independent subset which contains no loops; a *circuit* is a minimal dependent subset. In a loopless polymatroid every independent set can be extended to a base, and every dependent set contains a circuit. In the case when $\mathcal{M}$ is a matroid every base has the same number of elements, and this number equals the rank of the ground set M. Moreover every subset $A \subseteq M$ contains an independent set of size $f(A)$, and every subsets $A \subseteq M$ with rank $f(A) < |A|$ contains a circuit, see [21].

The polymatroid (f, M) is *connected* if for every partition of M into two non-empty sets A and B we have $f(A) + f(B) > f(M)$, that is, A and B are *not* independent. Connected polymatroids have no loops. Indeed, if $i \in M$ is a loop then $f(M) = f(M{-}i)$, thus the partition $M = \{i\} \cup (M{-}i)$ contradicts the connectedness.

For an element $i \in M$, the *private info of* i is $f(M) - f(M{-}i)$, as this is the amount of information which only i and nobody else in M has. If i has no private information, then we say that the polymatroid is *tight at* i.

Tightening at i means that i is stripped off its private info resulting in the function $f{\downarrow}i$ defined as

$$f{\downarrow}i : A \mapsto \begin{cases} f(A) & \text{if } i \notin A \\ f(A) - \big(f(M) - f(M{-}i)\big) & \text{if } i \in A. \end{cases}$$

Of course, $(f{\downarrow}i, M)$ is a polymatroid tight at i. If $\mathcal{M} = (f, M)$ is tight at every $i \in M$ then $\mathcal{M}$ is *tight*. $\mathcal{M}{\downarrow}$ is the polymatroid got from $\mathcal{M}$ after tightening at every element of its ground set (the result is independent of the order the elements are taken). Clearly, $\mathcal{M}$ is tight if and only if $\mathcal{M} = \mathcal{M}{\downarrow}$. If $\mathcal{M}$ is almost entropic then $\mathcal{M}{\downarrow}$ is almost entropic; this is a result of F. Matúš [20, Lemma 3]. In particular, the tight part of an entropic polymatroid is guaranteed to be almost entropic, but it is not necessarily entropic. A notable exception is the case of matroids: a matroid $\mathcal{M}$ is entropic if and only if $\mathcal{M}{\downarrow}$ is entropic. It is so as if i is not tight, then $1 = f(M) - f(M{-}i) \le f(i) \le 1$ thus i is independent from all subsets of $M{-}i$, thus the random variable representing i can be discarded.

2.2 Secret sharing

In a perfect secret sharing scheme there is a *secret*, and each participant from the finite set P receives a *share* such that certain subsets of participants can recover the secret from their joint shares, while other subsets – based on the value of their shares – should have no information on the secret. Subsets who can recover the secret are *qualified*, the qualified subsets form the *access structure* $\mathcal{A} \subseteq 2^P$. Sets not in $\mathcal{A}$ are called *forbidden* or *unqualified*. An access structure is clearly upward closed. To avoid exceptional cases, $\mathcal{A}$ is assumed to be non-empty (thus all participants together can recover the secret), and the empty set not to be in $\mathcal{A}$ (there must be a secret at all).

The participant $i \in P$ is *important* if there is an unqualified subset such that when i joins this subset, it becomes qualified. If i is not important, then it can join or leave any subset without affecting its status. Consequently the share of an unimportant participant does not play any role, unimportant participants can be discarded. The access structure $\mathcal{A}$ is *connected* if every participant is important. This terminology comes from the relationship between access structures and polymatroids realizing them, see Claims 4 and 5 below. In the rest of the paper, if not mentioned otherwise, access structures are assumed to be connected.

There are several definitions of what perfect secret sharing schemes are. The following definition is considered to be the most general one encompassing all other natural notions [1]. P is the set of participants and $s \notin P$ denotes the secret. A *distribution scheme* is a collection of discrete random variables $\xi = \langle \xi_i : i \in sP \rangle$ with some joint distribution. The value of ξ_s is the *secret*, while the value of ξ_i is the *share* of participant $i \in P$. The secret must be non-trivial, namely it must take at least two different values with positive probability.

The distribution scheme ξ *realizes* an access structure if a) the collection of shares of a qualified subset determine the secret, and b) the collection of shares of an unqualified subset is independent of the secret. Let $\mathcal{M}_\xi = (f, sP)$ be the entropic polymatroid associated with ξ. Shares of the subset $A \subseteq P$ determine the secret iff $\mathbf{H}(\xi_s|\xi_A) = 0$, which translates to $f(sA) = f(A)$. The same collection is independent of the secret if $\mathbf{H}(\xi_s|\xi_A) = \mathbf{H}(\xi_s)$, which translates to $f(sA) = f(A) + f(s)$. This justifies the following definition.

Definition (realizing an access structure)**.** The polymatroid $\mathcal{M} = (f, sP)$ *realizes the access structure* $\mathcal{A} \subseteq 2^P$ if a) $A \in \mathcal{A}$ if and only if $f(sA) = f(A)$, and b) $A \notin \mathcal{A}$ if and only if $f(sA) = f(A) + f(s)$. Polymatroids realizing an access structure are called *secret sharing polymatroids*.

The entropic polymatroid $\mathcal{M}_\xi$ realizes the access structure $\mathcal{A}$ if and only if ξ is a distribution scheme realizing $\mathcal{A}$. Indeed, if ξ is a distribution scheme then $f(s) = \mathbf{H}(\xi_s)$ is positive, thus one cannot have $f(sA) = f(A)$ and $f(sA) = f(A) + f(s)$ at the same time. Conversely, if $\mathcal{M}_\xi$ realizes $\mathcal{A}$, then $f(s) > 0$ (otherwise both $f(As) = f(A)$ and $f(As) = f(A) + f(s)$ hold simultaneously), thus the secret is not trivial. Other conditions follow easily.

The proof of the following well-known fact illustrates the ease of reasoning when using polymatroids rather than using entropies directly.

Claim 1. *Suppose $\mathcal{M}$ realizes $\mathcal{A}$. Then $f(i) \geq f(s)$ for every important participant $i \in P$.*

Proof. As $i \in P$ is important, there is an unqualified subset $A \subseteq P$ (A can be empty) such that iA is qualified. Then $f(sA) = f(A) + f(s)$, and $f(siA) = f(iA)$. Using that $f(i) + f(sA) \geq f(siA)$ and $f(iA) \geq f(A)$ (submodularity and monotonicity) one gets

$$f(i) \geq f(siA) - f(sA) = f(iA) - \big(f(A) - f(s)\big) \geq f(s),$$

which proves the claim. □

All participants together can always determine the secret, thus $f(sP) = f(P)$. This means that the secret has no private info. The private info of the participants does not help at all.

Claim 2. *The polymatroid $\mathcal{M}$ realizes $\mathcal{A}$ if and only if $\mathcal{M}{\downarrow}$ realizes $\mathcal{A}$.*

Proof. As observed above, the secret is tight, so let $i \in P$ and $\mathcal{M}{\downarrow}i = (f^*, sP)$ be the polymatroid after taking away the private info of i. For every $A \subseteq P$, either i is in both A and sA, or i is in none of them, thus

$$f^*(sA) - f^*(A) = f(sA) - f(A).$$

This means that if one of $\mathcal{M}$ or $\mathcal{M}{\downarrow}i$ realizes $\mathcal{A}$, then the other does the same. the claim follows after tightening at each participant. □

Given an access structure it would be tempting to consider tight polymatroids only among those which realize it. But, as was mentioned at the end of Section 2.1, there is no guarantee that the tight part of an entropic polymatroid is also entropic.

Corollary 3. *Suppose $\mathcal{A}$ is connected, and $\mathcal{M}$ realizes $\mathcal{A}$. If $f(i) = f(s)$ then $i \in P$ is tight.*

Proof. By Claim 2 $\mathcal{M}{\downarrow}i = (f^*, sP)$ also realizes $\mathcal{A}$. As $i \in P$ is important, Claim 1 gives $f^*(i) \geq f(s)$. Now $f^*(i) \leq f(i) = f(s)$, thus $f^*(i) = f(i)$ showing that i is tight. □

According to Claim 4 below, a polymatroid realizing a connected access structure must be connected. The converse is not true in general. In the special case when the polymatroid is a matroid the converse follows from some standard properties of matroid circuits [21].

Claim 4. *Suppose the polymatroid $\mathcal{M}$ realizes the access structure $\mathcal{A}$. If the access structure is connected, then $\mathcal{M}$ is connected.*

Proof. Assume, by contradiction, that $\mathcal{M} = (h, sP)$ is not connected, which means $sA \cup B, B \neq \emptyset$ is a partition of the ground set sP and $h(sAB) = h(sA) + h(B)$. In other words, sA and B are independent, consequently subsets of sA and B are independent as well. Let $b \in B$ and assume $A'B'$ is not qualified while $A'bB'$ is qualified with $A' \subseteq A$ and $B' \subseteq B - b$. Then $h(sA'B') = h(A'B') + h(s)$, from where

$$h(sA') + h(B') = h(sA'B') = h(A'B') + h(s) = h(A') + h(B') + h(s).$$

On the other hand, $h(sA'bB') = h(A'bB')$, which gives

$$h(sA') + h(bB') = h(sA'bB') = h(A'bB') = h(A') + h(bB').$$

From the first line $h(sA') = h(A') + h(s)$, while from the second $h(sA') = h(A')$, a contradiction. □

Claim 5. *Suppose $\mathcal{M}$ is a matroid which realizes the access structure $\mathcal{A}$. If $\mathcal{M}$ is connected then so is the access structure $\mathcal{A}$.*

Proof. Using matroid terminology, A is *dependent* if $h(A) < |A|$, and A is a *circuit* if it is a minimal dependent set. If C is a circuit, then $h(C) = |C| - 1$ and for each $i \in C$, $h(C{-}i) = |C| - 1$. A circuit *connects* two points if it contains both of them.

Let the ground set of the matroid be sP and pick some $a \in P$. To show that a is important it is enough to find a circuit C connecting a and s. Indeed, let $A = C{-}s$, then $a \in A$ and $h(sA) = h(C) = h(C{-}s) = h(A)$, thus A is qualified. C is minimal dependent, thus $sA{-}a = C{-}a$ is independent, and then $h(sA{-}a) = h(s) + h(A{-}a)$ which means $A{-}a$ is not qualified.

To finish the proof it suffices to quote the following result from matroid theory [21, Proposition 4.1.4]: *a matroid is connected if and only if any two points can be connected by a circuit*. For a quick proof see the Appendix. □

2.3 Complexity

Distribution schemes realizing an access structure scale up: taking n independent copies of the scheme all entropies are multiplied by n and the composite scheme still realizes the same access structure. Similarly, whether a polymatroid realizes an access structure or not is invariant for multiplying the polymatroid by any positive constant. When defining the efficiency one has to take into account this scalability. The usual way is to measure everything in multiples of the secret size. For example, if $\mathcal{M} = (f, sP)$ is a secret sharing polymatroid, then the *relative share size* of participant $i \in P$ is $f(i)/f(s)$, and the (worst case) *complexity of* $\mathcal{M}$ is

$$\sigma(\mathcal{M}) = \max\left\{\frac{f(i)}{f(s)} \,:\, i \in P\right\},$$

Other complexity measures, not considered here, include average relative size, and the scaled total randomness. If $\mathcal{M}$ realizes the connected access structure $\mathcal{A}$, then $\sigma(\mathcal{M}) \geq 1$ by Claim 1. Access structures where this lower bound is attained are called *ideal*.

Definition (ideal and almost ideal structures)**.** The access structure $\mathcal{A}$ is *ideal* if it can be realized by an entropic polymatroid with complexity 1. The access structure $\mathcal{A}$ is *almost ideal* if it can be realized by an almost entropic polymatroid with complexity 1.

In general, the usual definition of the complexity of an access structure is the infimum of the complexity of all secret sharing schemes realizing it:

$$\sigma(\mathcal{A}) = \inf\left\{\sigma(\mathcal{M}) \,:\, \mathcal{M} \text{ is entropic and realizes } \mathcal{A}\right\}.$$

Interestingly, there is a non-ideal (according to our definition) access structure with complexity 1, see [2, Section 6], thus the infimum here is not necessarily taken. The cone of almost entropic polymatroids is closed, see [17] or [23], thus an access structure with complexity 1 is almost ideal. It is an interesting open question whether the converse is true. When approximating an aent polymatroid by an entropic one, the only guarantee is that the rank functions differ by a small (negligible) amount. This means that qualified subsets can recover the secret with "overwhelming probability" only (as $\mathbf{H}(s|A)$ is not necessarily zero, only negligible), and unqualified subsets might get information on the secret (as $\mathbf{H}(s|A)$ can be strictly smaller than $\mathbf{H}(s)$), but this information is negligible. This relaxation is investigated under the name *probabilistic secret sharing* see, e.g., [5] and [11]. The question is can we patch these imperfections by adding a small amount of entropy to the secret? For secret recovery the answer is *yes*, see [11]; for independence the author tends to believe that the answer is *no*.

Next to $\sigma(\mathcal{A})$ other complexity measures can be defined by considering other polymatroid classes. Realizing $\mathcal{A}$ by an entropic polymatroid is the same as realizing it by a distribution scheme. Realizing by an almost entropic polymatroids instead means that one relaxes the strict requirements of recoverability and independence "up to a negligible amount". Linearly representable polymatroids are important from both practical and theoretical point of view. Such polymatroids arise from linear error correcting codes [9], they are studied

extensively and typically provide concise, efficient and low complexity schemes. We consider the following polymatroid classes, listed in decreasing order:

a) all polymatroids,
b) almost entropic polymatroids,
c) entropic polymatroids,
d) (conic hull of) linearly representable polymatroids.

Every access structure can be realized by a linearly representable polymatroid, thus every class gives a complexity notion on access structures. For classes a), c) and d) they are denoted by κ, σ, and λ [22]. For class b) we use $\bar{\sigma}$ to indicate that we are considering the closure of entropic polymatroids. The earlier definition of $\sigma(\mathcal{A})$ is the same as given here.

$$\begin{aligned}
\kappa(\mathcal{A}) &= \inf\{\,\sigma(\mathcal{M}) : \mathcal{M} \text{ realizes } \mathcal{A}\},\\
\bar{\sigma}(\mathcal{A}) &= \inf\{\,\sigma(\mathcal{M}) : \mathcal{M} \text{ is aent and realizes } \mathcal{A}\},\\
\sigma(\mathcal{A}) &= \inf\{\,\sigma(\mathcal{M}) : \mathcal{M} \text{ is entropic and realizes } \mathcal{A}\},\\
\lambda(\mathcal{A}) &= \inf\{\,\sigma(\mathcal{M}) : \mathcal{M} \text{ is linear and realizes } \mathcal{A}\}.
\end{aligned}$$

For the same access structure these values increase (as less and less polymatroids are considered). Each pair of these measures is known to be separated except for σ and $\bar{\sigma}$, see [1, 22].

2.4 Duals

Let P be the set of participants, and $\mathcal{A} \subseteq 2^P$ be an access structure. The qualified subsets in the *dual access structure* $\mathcal{A}^\perp$ are the complements of unqualified subsets of $\mathcal{A}$:

$$\mathcal{A}^\perp = \{A \subseteq P : P\text{–}A \notin \mathcal{A}\}.$$

Clearly, the dual of $\mathcal{A}^\perp$ is $\mathcal{A}$; $\emptyset \notin \mathcal{A}^\perp$ and $P \in \mathcal{A}^\perp$ as these are true for $\mathcal{A}$.

Claim 6. *$\mathcal{A}$ is connected if and only if $\mathcal{A}^\perp$ is connected.*

Proof. Suppose $\mathcal{A}$ is connected, we show that $\mathcal{A}^\perp$ is connected. The other direction follows from $(\mathcal{A}^\perp)^\perp = \mathcal{A}$. Let $a \in P$, and $A \subset P$ unqualified in $\mathcal{A}$ such that $aA \in \mathcal{A}$. Such an A exists as $\mathcal{A}$ is connected. Then $a \in P\text{–}A$, $P\text{–}A$ is qualified in $\mathcal{A}^\perp$ and $(P\text{–}A)\text{–}a$ is not qualified in $\mathcal{A}^\perp$, as required. □

Let $\mathcal{M} = (f, M)$ be a polymatroid. Define the discrete measure μ on subsets of M by $\mu(i) = f(i)$. As the measure is additive, for every subset $A \subseteq M$ we have

$$\mu(A) = \sum\{f(i) : i \in A\}.$$

The *dual of the polymatroid* $\mathcal{M}$ is $\mathcal{M}^\perp = (f^\perp, M)$ where the function $f^\perp$ is defined for subsets of M as

$$f^\perp : A \mapsto f(M\text{–}A) + \mu(A) - f(M).$$

By submodularity, $f^\perp$ is non-negative; submodularity holds by an easy inspection, thus $\mathcal{M}^\perp$ is a polymatroid. If $\mathcal{M}$ is integer-valued then so is $\mathcal{M}^\perp$; moreover if $\mathcal{M}$ is a matroid (the rank of a singleton is zero or one), then so is the dual.

Claim 7. a) *$\mathcal{M}$ is connected if and only if $\mathcal{M}^\perp$ is connected.* b) *$\mathcal{M}$ realizes the access structure $\mathcal{A}$ if and only if $\mathcal{M}^\perp$ realizes $\mathcal{A}^\perp$.*

Proof. a) Suppose $A \cup B$ is a partition of M, then $\mu(A) + \mu(B) = \mu(M)$. By the definition of $f^\perp$ we have

$$f^\perp(A) + f^\perp(B) - f^\perp(M) = f(B) + f(A) - f(M).$$

If one of them is positive, then the other is positive, as required.

b) Let $M = sP$, $A \subseteq P$, then $\mu(sA) - \mu(A) = \mu(s) = f(s)$, thus

$$\big(f^\perp(sA) - f^\perp(A)\big) + \big(f(sP{-}A) - f(P{-}A)\big) = f(s).$$

If $\mathcal{M}$ realizes $\mathcal{A}$, then $f(sP{-}A) - f(P{-}A)$ is either zero or $f(s)$ depending on whether $P{-}A \in \mathcal{A}$ or not. Consequently $f^\perp(sA) - f^\perp(A)$ is either zero of $f(s)$ depending on whether $P{-}A \notin \mathcal{A}$ or not. Thus $f^\perp$ realizes $\mathcal{A}^\perp$. The converse is similar. □

The dual polymatroid $\mathcal{M}^\perp$ is always tight as

$$f^\perp(M{-}i) = f(i) + \mu(M{-}i) - f(M) = \mu(M) - f(M) = f^\perp(M).$$

Consequently the dual of $\mathcal{M}^\perp$ is also tight, and if $\mathcal{M}$ was not tight, the dual of $\mathcal{M}^\perp$ cannot be the same as $\mathcal{M}$. However, if $\mathcal{M}$ is tight, then it equals $\mathcal{M}^{\perp\perp}$, in particular $\mathcal{M}^{\perp\perp\perp} = \mathcal{M}^\perp$ always true.

Claim 8. a) *Suppose $\mathcal{M}$ is tight. Then $\mathcal{M}^{\perp\perp} = \mathcal{M}$, moreover $\mathcal{M}$ and $\mathcal{M}^\perp$ have the same value on singletons.* b) *For every polymatroid $\mathcal{M}$, $\mathcal{M}^{\perp\perp} = \mathcal{M}{\downarrow}$.*

Proof. a) We start with the second claim. By the assumption, $f(M) = f(M{-}i)$,

$$f^\perp(i) = f(M{-}i) + \mu(i) - f(M) = \mu(i) = f(i),$$

as claimed. It means that $\mu^\perp(A) = \mu(A)$, and then

$$f^\perp(M{-}A) = f(A) + \mu(M{-}A) - f(M),$$
$$f^\perp(M) = \mu(M) - f(M),$$

thus

$$f^{\perp\perp}(A) = f^\perp(M{-}A) + \mu^\perp(A) - f^\perp(M) = f(A) + \mu(M{-}A) + \mu(A) - \mu(M) = f(A),$$

proving $\mathcal{M}^{\perp\perp} = \mathcal{M}$.

b) It is enough to show that the dual of $\mathcal{M}$ and the dual of $\mathcal{M}{\downarrow}$ are the same, from here the claim follows by a). In $\mathcal{M}{\downarrow}i$ the rank of every set containing $i \in M$ decreases by the same amount. In the expression

$$f(M{-}A) + \mu(A) - f(M)$$

this amount is added once in the first two terms, and subtracted once in the last term, thus it cancels. □

2.5 Factor and principal extension

Let $\mathcal{M} = (h, M)$ be a polymatroid. Partitions of the ground set M can be considered as equivalence classes of an equivalence relation on M. Let $\cong$ be an equivalence relation on M, $N = M/\cong$ be the set of equivalence classes, and $\varphi : M \to N$ be the map which assigns to each element its equivalence class. The *factor of* $\mathcal{M}$ *by* $\cong$, denoted as $\mathcal{M}/\cong$, is the pair (g, N) where g assigns the value $g : A \mapsto h(\varphi^{-1}(A))$ to subsets of N (that is, union of complete equivalence classes). It is clear that $\mathcal{M}/\cong$ is a polymatroid.

Let $a \in M$, and $\alpha \geq 0$ be a real number. The *principal extension* $\mathcal{M}_{a,\alpha}$ is a one-point extension of $\mathcal{M}$ defined on the set $M \cup \{a'\}$ assigning the value

$$h : a'A \mapsto \min\{h(A) + \alpha, h(aA)\}$$

to new subsets. It is a routine to check that the principal extension is a polymatroid [13]. Principal extension of an almost entropic polymatroid is almost entropic. This is an immediate consequence of (and actually, is equivalent to) a result of F. Matúš [17, Theorem 2], see also [20, Lemma 3]. We state this result without proof.

Theorem 9 (F. Matúš). *If the polymatroid $\mathcal{M}$ is almost entropic, then so is the principal extension $\mathcal{M}_{a,\alpha}$.* □

Matúš' proof guarantees the extension to be only almost entropic even if $\mathcal{M}$ is entropic. In fact, there is an entropic polymatroid where some principal extension is not entropic.

Principal extensions can be used to "split atoms" of a polymatroid, which, in turn, will be used to prove that integer polymatroids are factors of matroids. Let us see the details. In what follows $\mathcal{M} = (h, M)$ is a polymatroid.

Lemma 10. *Let $a \in M$, and α_1, α_2 be non-negative numbers whose sum is $h(a)$. There is a polymatroid $\mathcal{M}' = (h', a_1a_2 \cup M{-}a)$ such that $h'(a_i) = \alpha_i$, and $\mathcal{M}$ is a factor of $\mathcal{M}'$ collapsing a_1 and a_2 to a. Moreover, $\mathcal{M}$ is almost entropic if and only if so is $\mathcal{M}'$.*

Proof. Let $\mathcal{M}'$ be the principal extension $\mathcal{M}_{a,\alpha_1}$ adding the new point a_1, so that $M' = a_1 \cup M$; then let $\mathcal{M}''$ be the principal extension $\mathcal{M}'_{a,\alpha_2}$ adding the new point a_2. Then for each $A \subseteq M{-}a$ we have

$$\begin{aligned} h''(A) &= h(A), \\ h''(a_1A) &= \min\{h(A) + \alpha_1, h(aA)\}, \\ h''(a_2A) &= \min\{h(A) + \alpha_2, h(aA)\}, \\ h''(a_1a_2A) &= \min\{h(A) + \alpha_1 + \alpha_2, h(aA)\}. \end{aligned}$$

As $h(A) + \alpha_1 + \alpha_2 = h(A) + h(a) \geq h(aA)$, we have $h''(a_1a_2A) = h(aA)$. This shows that $\mathcal{M}''$ restricted to the ground set $a_1a_1 \cup M{-}a$ is the required splitting. If $\mathcal{M}$ is aent, then both $\mathcal{M}'$ and $\mathcal{M}''$ are aent by Theorem 9. A restriction and a factor of an aent polymatroid is trivially aent, proving the last claim. □

Lemma 11. *Let $\mathcal{M} = (f, aN)$ be tight, and suppose $\mathcal{N} = (g, a_1a_2N)$ splits a in $\mathcal{M}$ as $g(a_i) = \alpha_i$. Then $\mathcal{N}^\perp$ splits a in $\mathcal{M}^\perp$ in the same way.*

Proof. Let $A \subseteq N$, then $g(A) = f(A)$ and $g(a_1a_2A) = f(aA)$. Calculating $g^\perp(A)$ one gets

$$\begin{aligned} g^\perp(A) &= g(a_1a_2N{-}A) + \mu(A) - g(a_1a_2N) = \\ &= f(aN{-}A) + \mu(A) - f(aN) = f^\perp(A), \end{aligned}$$

and similarly $g^\perp(a_1a_2A) = f^\perp(aA)$. Finally,

$$\begin{aligned} g^\perp(a_1A) &= g(a_1a_2N{-}a_1A) + \mu(a_1A) - g(a_1a_2N) \\ &= g(a_2N{-}A) + \mu(a_1) + \mu(A) - f(aN) \\ &= \min\{f(N{-}A) + \alpha_2, f(aN{-}A)\} + \alpha_1 + \mu(A) - f(aN) \\ &= \min\{f(N{-}A) + \mu(aA) - f(aN), f(aN{-}A) + \mu(A) - f(aN) + \alpha_1\} \\ &= \min\{f^\perp(aA), f^\perp(A) + \alpha_1\}, \end{aligned}$$

thus $\mathcal{N}^\perp$ splits a as claimed as $f^\perp(a) = f(a) = \alpha_1 + \alpha_2$ using that $\mathcal{M}$ is tight. □

Factors of a matroid are integer polymatroids. Helgason's theorem [8] says that the converse is true: every integer polymatroid is a factor of some matroid. We need the following strengthening of this result.

Theorem 12. *For each integer polymatroid $\mathcal{M}$ there is a matroid $\varphi(\mathcal{M})$ such that* a) *$\mathcal{M}$ is a factor of $\varphi(\mathcal{M})$,* b) *$\mathcal{M}$ is aent if and only if $\varphi(\mathcal{M})$ is aent,* c) *if $\mathcal{M}$ is tight, then $\varphi(\mathcal{M}^\perp)$ is the dual of $\varphi(\mathcal{M})$.*

Proof. Let $\mathcal{M}$ be an integer polymatroid. The matroid $\varphi(\mathcal{M})$ is generated by a series of splitting. If all singletons have rank zero or one, then $\mathcal{M}$ is a matroid, and we are done. Otherwise some $a \in M$ has rank $h(a) > 1$. Using Lemma 10 split a into two with ranks 1 and $h(a) - 1$. All ranks in the split polymatroid $\mathcal{M}'$ remain integer, and by Lemma 10 $\mathcal{M}'$ is aent if and only if $\mathcal{M}$ is aent. Continue this way to get the matroid $\varphi(\mathcal{M})$. Clearly $\mathcal{M}$ is a factor of $\varphi(\mathcal{M})$, and c) holds by Lemma 11. □

2.6 The duality conjecture

Fix the connected access structure $\mathcal{A} \subset 2^P$ and consider all polymatroids on the ground set sP which realize $\mathcal{A}$. We are interested in $\kappa(\mathcal{A})$, the minimal complexity of these polymatroids. By Claim 2 the search can be restricted to tight polymatroids. Suppose the infimum is attained by a tight polymatroid $\mathcal{M}$. (It is attained as polymatroids form a closed set.) Claim 8 a) implies that $\mathcal{M}$ and $\mathcal{M}^\perp$ have the same complexity. According to Claim 7 b) $\mathcal{M}^\perp$ realizes $\mathcal{A}^\perp$, thus $\kappa(\mathcal{A}^\perp) \le \kappa(\mathcal{A})$. Applying the same reasoning to the dual structure we get $\kappa(\mathcal{A}^{\perp\perp}) \le \kappa(\mathcal{A}^\perp)$. As $\mathcal{A}^{\perp\perp}$ and $\mathcal{A}$ are the same, we have

Claim 13. *For every access structure we have* $\kappa(\mathcal{A}) = \kappa(A^\perp)$. □

Every access structure can be realized by some linearly representable polymatroid, the complexity measure $\lambda(\mathcal{A})$ defines the infimum of the complexity of such representations. It is well-known that the conic hull of linearly representable polymatroids is a closed subset of the entropic polymatroids, and it is closed for taking duals. Therefore it is also closed for tightening by Claim 8 b). The corresponding complexity measure is $\lambda(\mathcal{A})$, and the same reasoning as above gives

Claim 14. *For every access structure we have* $\lambda(\mathcal{A}) = \lambda(\mathcal{A}^\perp)$. □

Every explicitly defined access structure $\mathcal{A}$ with known exact complexity value $\sigma(\mathcal{A})$ satisfies $\lambda(\mathcal{A}) = \sigma(\mathcal{A}) = \kappa(\mathcal{A})$ – consequently the same is true for the dual structure, and then $\sigma(\mathcal{A}) = \sigma(\mathcal{A}^\perp)$. It is a long-standing open problem whether the statement similar to Claims 13 and 14 holds for the entropic complexity σ.

Conjecture 1 (complexity of dual structure)**.** *For every access structure we have* $\sigma(\mathcal{A}) = \sigma(\mathcal{A}^\perp)$.

The conjecture is probably not true, but even the particular case when $\mathcal{A}$ is an ideal access structure resisted all efforts. Recall, that $\mathcal{A}$ is ideal if it can be realized by an ideal entropic polymatroid, or, equivalently, by an ideal distribution scheme.

Conjecture 2 (dual of ideal structure)**.** *The dual of an ideal access structure is ideal.*

Refuting the second conjecture does not necessarily refutes Conjecture 1 as the dual might be non-ideal while having complexity 1. In Section 3 we prove that Conjecture 2 is equivalent to a question about matroid representability. Using results of that section, and a construction by Tarik Kaced [10] the duality question for almost ideal schemes is settled.

3 Ideal structures and matroids

First we give a self-contained proof of a somewhat extended result of Blakley and Kabatianski [3, 19], which, in turn, extends a result of Brickell and Davenport [4] connecting ideal access structures and matroids. Using this connection we present a statement about matroid representability which is equivalent to Conjecture 2.

Fix the connected access structure $A \subset 2^P$ and suppose the polymatroid $\mathcal{M} = (f, sP)$ realizes it. Assume furthermore that $\mathcal{M}$ has complexity 1, that is, the rank of all singletons equals $f(s)$. The following lemmas establish some structural properties of $\mathcal{M}$. In the lemmas A is a subset of P, $a \in P$, and s denotes the secret.

Lemma 15. *Suppose* $A \in \mathcal{A}$ *and* $A{-}a \notin \mathcal{A}$. *Then* $f(A) - f(A{-}a) = f(s)$.

Proof. By submodularity of the rank function f, we have

$$f(a) \ge f(A) - f(A{-}a) = f(sA) - \big(f(sA{-}a) - f(s)\big) = \big(f(sA) - f(sA{-}a)\big) + f(s) \ge f(s).$$

As $f(a) = f(s)$, the conclusion follows. □

Lemma 16. *Let $a \in A' \subseteq A$, Suppose $A-a$ and A' are qualified and $A'-a$ is not. Then $f(A) = f(A-a)$.*

Proof. For qualified subsets $f(sA') = f(A')$, etc., for the unqualified subset $f(sA'-a) = f(A'-a) + f(s)$. Thus

$$f(A) - f(A-a) = f(sA) - f(sA-a) \le f(sA') - f(sA'-a) = \big(f(A') - f(A'-a)\big) - f(s) = 0,$$

where the inequality follows from submodularity and the last equality from Lemma 15. Thus $0 \le f(A) - f(A-a) \le 0$, proving the claim. □

Lemma 17. *Suppose $f(A) - f(A-a) = f(s)$, and $a \in A' \subseteq A$. Then $f(A') - f(A'-a) = f(s)$.*

Proof. By submodularity, $f(A)-f(A-a) \le f(A')-f(A'-a) \le f(a)$. As both sides equal $f(s)$, the claim follows. □

Theorem 18 (Blakley–Kabatianski)**.** *Let $\mathcal{A} \subset 2^P$ be a connected access structure and $\mathcal{M} = (f, sP)$ be a polymatroid realizing $\mathcal{A}$ such that $f(a) = f(s) = 1$ for all $a \in P$. Then $\mathcal{M}$ is a matroid which is uniquely determined by the access structure.*

Proof. All singletons have rank 1, thus $\mathcal{M}$ is a matroid if all ranks are integer. The basic idea is to show that for any subset A of the ground set sP one can find an element a of A such that $f(A) - f(A-a)$ is either zero or one. The additional claim that $\mathcal{M}$ is uniquely determined by $\mathcal{A}$ follows from the fact that for the chosen element $a \in A$ the value of $f(A) - f(A-a)$ depends only on the access structure, and not on the particular realization.

If the subset contains the secret s, then $f(sA) - f(A)$ is either zero or $f(s) = 1$ depending on whether $A \in \mathcal{A}$ or $A \notin \mathcal{A}$, which settles this case. So assume $A \subseteq P$.

When A is qualified, then there are two cases. If $A-a$ is not qualified for some $a \in A$, then Lemma 15 gives that this difference is $f(s) = 1$. If all $A-a$ is qualified, then pick a minimal qualified $A' \subseteq A$ and use Lemma 16 with any $a \in A'$.

Thus assume A is unqualified. As $\mathcal{A}$ is connected, there is an unqualified subset B such that AB is qualified (pick any element of A and let B show that this element is important). Choose such an unqualified B such that the set $B-A$ has minimal cardinality, and within this constrain $A \cap B$ has maximal cardinality. Then $AB-k$ is unqualified for any $k \in B-A$ (as otherwise $B-A$ is not minimal), and aB is qualified for any $a \in A-B$ (as otherwise $A \cap B$ is not maximal). Fix $a \in A-B$. With any $k \in B-A$ we have that AB is qualified, $AB-k$ is not. Lemma 15 gives $f(AB) - f(AB-k) = 1$, and by Lemma 17, $f(A') - f(A'-k) = 1$ for all $k \in A' \subseteq AB$. By induction this gives both $f(AB)-f(A) = |A-B|$ and $f(AB-a)-f(A-a) = |A-B|$. Therefore $f(A)-f(A-a) = f(AB)-f(AB-a)$. Now AB is qualified. If $AB-a$ is unqualified, then by Lemma 15 this difference is $f(s) = 1$. If $AB-a$ is qualified, then $f(AB) = f(AB-a)$ using Lemma 16 with $A' = aB$. □

The main result of this section is the equivalence of a statement about matroid representability and Conjecture 2. Recall that $\mathcal{M}$ is an *entropic matroid* if for some positive λ the polymatroid $\lambda\mathcal{M}$ is entropic.

Theorem 19. *The following statements are equivalent.*

a) *The dual of every ideal access structure is ideal.*

b) *The dual of every entropic matroid is entropic.*

Proof. Let us first make some simplifying assumptions. In a) the access structure can be assumed to be connected: simply forget about the unimportant participants, they will be unimportant in the dual structure. In b) the matroid can be assumed to be tight and connected. This is so as the matroids $\mathcal{M}$ and $\mathcal{M}{\downarrow}$ are entropic at the same time: if i has a non-zero private info, then i is completely independent of the rest of the matroid. Furthermore, if $\mathcal{M}$ is not connected, then it is an independent sum of the connected components, and then $\mathcal{M}^\perp$ is the sum of the duals of the components.

The reduction from entropic matroids to tight entropic matroids was discussed briefly at the end of Section 2.1. In the proof of Theorem 20 we need a similar reduction for almost entropic matroids which is provided by Matúš' theorem, see [20].

a) $\to$ b) As remarked above, we may assume that the entropic matroid $\mathcal{M}$ is tight and connected. Pick any element of its ground set and name it s, the remaining elements are in P. Since $\mathcal{M}$ is connected, it has no loops, thus $f(s) = 1$. Define the access structure $\mathcal{A} \subset 2^P$ by

$$\mathcal{A} = \{A \subseteq P : f(sA) = f(A)\}.$$

Clearly $\mathcal{M}$ realizes this access structure, consequently $\mathcal{A}$ is ideal, and by Claim 5 it is also connected. By Claim 7 b), the dual matroid $\mathcal{M}^\perp$ realizes $\mathcal{A}^\perp$.

As $\mathcal{A}$ is a connected ideal structure, assumption a) says that $\mathcal{A}^\perp$ is ideal. Let $\mathcal{M}'$ be the scaled entropic polymatroid which realizes $\mathcal{A}^\perp$ with $f'(s) = f'(a) = 1$. As $\mathcal{A}^\perp$ is connected by Claim 6, conditions of Theorem 18 hold. Consequently $\mathcal{M}'$ is the unique matroid realizing $\mathcal{A}^\perp$. As $\mathcal{M}^\perp$ also realizes the same access structure, $\mathcal{M}'$ and $\mathcal{M}^\perp$ are the same matroids. Now $\mathcal{M}'$ is a scaled version of an entropic polymatroid, thus $\mathcal{M}' = \mathcal{M}^\perp$ is an entropic matroid, as was required.

b) $\to$ a) Let $\mathcal{A}$ be an ideal connected access structure realized by the entropic polymatroid $\mathcal{M}^\star$. As $\mathcal{A}$ is connected and ideal, we have $f^\star(i) = f^\star(s) > 0$ for all participants $i \in P$. Let $\lambda = 1/f^\star(s)$ and $\mathcal{M} = \lambda\mathcal{M}^\star$. Then $\mathcal{M}$ also realizes $\mathcal{A}$ and $f(i) = f(s) = 1$ for all $i \in P$. By Corollary 3 $\mathcal{M}$ is tight, and by Theorem 18 $\mathcal{M}$ is a matroid. As $\mathcal{A}$ is connected, by Claim 4 $\mathcal{M}$ is connected. Consequently $\mathcal{M}$ is a tight, connected, entropic matroid which realizes the access structure $\mathcal{A}$. By assumption b) $\mathcal{M}^\perp$ is an entropic matroid, realizes $\mathcal{A}^\perp$ by Claim 7 b); finally by Claim 8 a) $\mathcal{M}^\perp$ and $\mathcal{M}$ have the same value on singletons. Thus $\lambda^\perp\mathcal{M}^\perp$ is an entropic polymatroid for some positive $\lambda^\perp$, realizes $\mathcal{A}^\perp$, and has complexity $\sigma(\mathcal{M}^\perp) = \sigma(\mathcal{M}) = 1$. Therefore $\mathcal{A}^\perp$ is ideal. □

Almost entropic polymatroids form a closed cone, which means that positive multiples of an aent polymatroid are aent. Consequently the definition of almost entropic matroids does not require scaling as was the case for entropic matroids. The matroid $\mathcal{M}$ is *almost entropic* if it is almost entropic as a polymatroid. Repeating the proof above word by word while replacing "ideal" by "almost ideal" and "entropic" by "almost entropic" everywhere one gets the following theorem.

Theorem 20. *The following statements are equivalent.*
a) *The dual of every almost ideal access structure is almost ideal.*
b) *The dual of every almost entropic matroid is almost entropic.* □

4 Duals of almost entropic matroids

We have almost all the pieces together to prove the main result:

Theorem 21. *There is an almost ideal access structure whose dual is not almost ideal.*

By Theorem 20 we need to exhibit an almost entropic matroid whose dual is not almost entropic. The existence of such a matroid was proved by Tarik Kaced [10, Theorem 2], this section is a detailed account of that result. The proof starts with the construction of an entropic polymatroid whose dual is not entropic. Using a continuity argument and linear scaling, one gets an integer polymatroid with the same properties. Theorem 12 established a connection between integer polymatroids and matroids which preserves duality and almost entropicity. To complete the tour apply this theorem to get the required matroid. Now let us see the details.

Finding an entropic polymatroid whose dual is not entropic was a long-standing open problem. The example below is due to Kaced [10]. The polymatroid is specified by a distribution on five binary random variables. To show that its dual is not entropic, Kaced used a 5-variable non-Shannon type information inequality, see [14, 16]. Such an inequality is a closed halfspace in the $(2^{|M|} - 1)$-dimensional space which a) contains all entropic points on its non-negative side (consequently all aent points as well), and b) cuts into the polymatroid cone Γ_M. Entropy inequalities are typically written using abbreviations originating in information theory. For

disjoint subsets A, B, C we write

$$h(A|B) = h(AB) - h(B),$$
$$h(A, B) = h(A) + f(B) - h(AB),$$
$$h(A, B \mid C) = h(AC) + h(BC) - h(ABC) - h(C),$$

corresponding to conditional entropy, mutual information, and conditional mutual information, respectively. In any polymatroid these expressions are always non-negative. The MMRV inequality written for the singletons of the five-element set $\{abcde\}$ is

$$\big(h(a, b|c) + h(b, c|a) + h(c, a|b)\big) + \big(h(b, c|d) + h(b, c|e) + h(d, e) - h(b, c)\big) \geq 0. \tag{1}$$

For a short proof that this inequality holds for aent polymatroids see the Appendix.

Claim 22. *There is a tight, integer and aent polymatroid whose dual is not aent.*

Proof. The distribution on five random variables $\xi_a, \ldots, \xi_e$ is specified in Table 1. Each of the variables takes either zero or one, there are only eight combinations with positive probability. The associated polymatroid $\mathcal{M}_\xi$ is entropic, the left hand side of (1) evaluates to 0.108494. The dual $\mathcal{M}_\xi^\perp$ is not aent as the left hand side of (1) is -0.0715364.

Table 1: Distribution on five variables

ξ_a	ξ_b	ξ_c	ξ_d	ξ_e	Prob
0	0	0	0	0	0.077
0	0	1	1	0	0.182
0	1	0	0	1	0.182
0	1	1	0	0	0.077
1	0	0	0	0	0.105
1	0	1	0	0	0.136
1	1	0	0	0	0.136
1	1	1	0	0	0.105

The duality operation is continuous, thus duals of the polymatroids in a small neighborhood of $\mathcal{M}_\xi$ are still violating the MMRV inequality. The entropic polymatroid $\mathcal{M}_\xi$ is on the boundary of the aent cone (for example, d and e have no private info), but there is another polymatroid $\mathcal{M}'$ arbitrarily close to $\mathcal{M}_\xi$ *inside* that cone. By [17] interior points of the aent cone are entropic. Take $\mathcal{M}''$ very close to $\mathcal{M}'$ such that all coordinates rational. Let n be the smallest common denominator of the fractions in the coordinates. Coordinates in $n\mathcal{M}''$ are integer. The dual of $n\mathcal{M}''$ violates the MMRV as the dual of $\mathcal{M}''$ violates it, and the left hand side of (1) also multiplies by n. Finally, $n\mathcal{M}''$ is entropic: to realize it take n independent copies of the random variables realizing $\mathcal{M}''$. The tight part of $n\mathcal{M}''$ is integer and almost entropic, its dual is the same as the dual of $n\mathcal{M}''$ by Claim 8 b), proving the claim.

Using the distribution ξ above, such an integer polymatroid can be constructed directly. For a subset $A \subseteq M$ define the the polymatroid r_A as

$$\mathsf{r}_A : I \mapsto \begin{cases} 1 & \text{if } A \cap I \neq \emptyset\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

Clearly, $\lambda \mathsf{r}_A$ is entropic for every positive λ. As A runs over all non-empty subsets of M these polymatroids are linearly independent and span a full-dimensional subcone of $\Gamma_M^\star$ consisting of entropic polymatroids only

[17]. The idea is that take a multiple of $\mathcal{M}_\xi$ (which is almost entropic), and use some linear combination of r_A's to round up the coordinates to integer values. This idea works. The polymatroid

$$\begin{aligned}\mathcal{M} = {} & 50.03\mathcal{M}_\xi + 0.3819594(\mathsf{r}_{abd} + \mathsf{r}_{acd} + \mathsf{r}_{abe} + \mathsf{r}_{ace}) + \\ & 0.1741526(\mathsf{r}_b + \mathsf{r}_c) + 0.0067674\mathsf{r}_{bc} + 0.5112645\mathsf{r}_{abc} + \\ & 0.6235703(\mathsf{r}_{bd} + \mathsf{r}_{cd} + \mathsf{r}_{be} + \mathsf{r}_{ce}) + 0.0270848(\mathsf{r}_{bcd} + \mathsf{r}_{bce}) + \\ & 0.1012390\mathsf{r}_a + 0.4887355(\mathsf{r}_{ab} + \mathsf{r}_{ac}) + 0.3314441(\mathsf{r}_{ad} + \mathsf{r}_{ae}) + \\ & 0.3356126(\mathsf{r}_{abcd} + \mathsf{r}_{abce}) + 0.4877698\mathsf{r}_{bcde} + 0.5648560\mathsf{r}_{abcde}\end{aligned}$$

is clearly entropic, and it is integer. This is so as the coefficients in this formula are the solutions of a system of linear equations yielding exact values. Table 2 shows the coordinates of $51\mathcal{M}_\xi$ (left column), the integer entropic polymatroid $\mathcal{M}$ (middle column), and the tightening of $\mathcal{M}$ (right column). The value of the MMRV inequality for the dual of $\mathcal{M}$ is -1, thus $\mathcal{M}^\perp$ is not almost entropic. As $\mathcal{M}^\perp = (\mathcal{M}{\downarrow})^\perp$, the tight part of $\mathcal{M}$ is a tight, integer, aent polymatroid whose dual is not aent. □

Table 2: An integer entropic polymatroid

a	49.983219	55	37
b	50.030000	55	31
c	50.030000	55	31
d	34.242173	38	38
e	34.242173	38	38
ab	100.013219	107	65
ac	100.013219	107	65
ad	74.221223	81	63
ae	74.221223	81	63
bc	97.356052	105	57
bd	73.693026	80	56
be	73.693026	80	56
cd	73.693026	80	56
ce	73.693026	80	56
de	65.536972	72	72

abc	146.591925	155	89
abd	111.389648	119	77
acd	111.389648	119	77
abe	111.389648	119	77
ace	111.389648	119	77
ade	90.946998	99	81
bde	97.356052	105	81
cde	97.356052	105	81
bcd	113.024608	121	73
bce	113.024608	121	73
$abcd$	146.591925	155	89
$abce$	146.591925	155	89
$abde$	122.766078	131	89
$acde$	122.766078	131	89
$bcde$	128.693164	137	89
$abcde$	146.591925	155	89

Let the tight integer polymatroid provided by Claim 22 be $\mathcal{N}$, and consider the matroid $\varphi(\mathcal{N})$ provided by Theorem 12. As $\mathcal{N}$ is aent, $\varphi(\mathcal{N})$ is almost entropic; $\mathcal{N}^\perp$ is not aent, thus $\varphi(\mathcal{N}^\perp)$ is not aent. Consequently the matroid $\varphi(\mathcal{N})$ is aent and its dual, $\varphi(\mathcal{N}^\perp)$, is not aent either – completing the proof of Theorem 21.

Using the tight almost-entropic polymatroid of Table 2 the construction in the proof of Theorem 19 gives an almost-ideal access structure on 174 participants (as the corresponding aent matroid has $f(a)+f(b)+f(c)+f(d)+f(e) = 175$ atoms, one of them is the secret, others are the participants) whose dual is not almost-ideal. It is left to the interested reader to describe the qualified subsets for different choices of the secret.

According to Theorem 20, to construct a counterexample to Conjecture 2 we need an entropic matroid whose dual is not entropic. Entropic matroids (and their multiples) are always on the boundary of the aent cone; the boundary has an intricate and complicated structure. There seems to be no other way to show that a matroid is entropic than giving the probability distribution explicitly. But it is not clear how to guarantee $\mathbf{H}(\xi_A)/\mathbf{H}(\xi_s)$ to be an integer. No entropic matroid is known which is not a multiple of a linearly representable polymatroid. Finding such a matroid would be very interesting.

5 Conclusion and open problems

An almost ideal secret sharing scheme on 174 participants was constructed explicitly whose dual structure is not almost ideal. It was done by putting together several pieces of earlier works. The intricate connection between ideal secret sharing schemes and matroids was observed by Brickell and Davenport [4]. This connection is expressed in Theorem 18 extending a result of Blakley and Kabatiansky [3]; the presented proof is an adoption of the one from [19]. Entropic and almost entropic polymatroids have been studied intensively by Frantisek Matúš [15–18, 20]; his insight of the structure of the entropic region was indispensable to this paper. And, of course, we were using the surprising result of Tarik Kaced [10] who settled an old conjecture by constructing an entropic polymatroid whose dual is not entropic. These results allowed us to solve the duality problem of ideal secret sharing schemes – is the dual of an ideal structure is ideal? – in a model slightly differing from the standard one, namely secret recovery and secret independence is required only "up to a negligible factor". This model has been studied earlier under the name of "probabilistic secret sharing", see [5, 11, 24]. The original problem remained unsolved.

Problem 1. *Is the dual of an ideal structure is ideal?*

A substantial obstacle attacking this problem was mentioned at the end of the previous section: every known entropic matroid is linearly representable.

Problem 2. *Find an entropic matroid which is not linear.*

A promising approach seems to be using subgroup representation for the matroid [6]. It requires substantial knowledge of the subgroup structure of non-commutative finite groups.

It is an interesting question how restrictive the probabilistic model is. If an access structure has complexity 1, then it is almost ideal (while not necessarily ideal [2]); this follows from the fact that the aent polymatroids form a closed cone [17]. The following problem asks about the converse of this implication.

Problem 3. *Does every almost ideal access structure have complexity 1?*

The question is equivalent to whether $\bar{\sigma}(\mathcal{A}) = 1$ implies $\sigma(\mathcal{A}) = 1$. As mentioned at the end of Section 2.3, $\bar{\sigma}$ and σ are not known to be separated.

Problem 4. *Is there an access structure $\mathcal{A}$ with $\bar{\sigma}(\mathcal{A})$ strictly smaller than $\sigma(\mathcal{A})$?*

This problem was raised in Section 2.3: can the imperfections allowed by the probabilistic model be patched by adding some small entropy to the secret and / or shares? This question has been considered by Kaced in [11], but remained unsolved.

Acknowledgement: The author would like to thank the encouragement and fruitful discussion at the Prague Stochastics Conference, 2019. He is particularly indebted to Oriol Farrás and Carles Padró. Special thanks to Gabor Tardos for figuring out the subtleties of Claim 5.

The research reported in this paper was supported by GACR project number 19-04579S, and partially by the Lendület program of the HAS.

References

[1] A. Beimel (2011), Secret-sharing schemes: a survey, in: *IWCC 2011, volume 6639 of LNCS*, Springer, 2011, pp 11-46

[2] A. Beimel, N. Livne (2006) On matroids and non-ideal secret sharing In: Halevi S., Rabin T. (eds) *Theory of Cryptography, volume 3876 of LNCS*, Springer, Berlin, Heidelberg pp 482-501

[3] G. Blakley, G. Kabatianski (1995), On general perfect secret sharing schemes, in: *LNCS 963, Advances in Cryptology, Proceedings of Crypto'95*, Springer 1995, pp. 367–371
[4] E. F. Brickell, D. M. Davenport (1991) On the classification of ideal secret sharing schemes, *J. of Cryptology*, vol 4 (73) pp 123-134
[5] P. D'Arco, R. De Prisco. A. De Santis, A. Pérez del Pozo, U. Vaccaro (2018), Probabilistic Secret Sharing, in: *43rd International Symposium on Mathematical Foundations of Computer Science, MFCS 2018*, Leibniz International Proceedings in Informatics, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Vol 117, pp 64:1–64:16
[6] T. H. chan, R. W. Yeung (2002), On a relation between information inequalities and group theory, *IEEE Tran. Information Theory* **57** pp 6364-6378
[7] S. Fujishige (1978), Polymatroidal dependence structure of a set of random variables. *Information and Control* **39** 55–72.
[8] T. Helgason (1974) Aspects of the theory of hypermatroids, In: Berge C., Ray-Chaudhuri D. (eds) *Hypergraph Seminar*, Lecture Notes in Mathematics, vol 411. Springer, Berlin, Heidelberg
[9] W. C. Huffman and V. Pless (2003), *Fundamentals of error correcting codes*, Cambridge University Press, 2003
[10] T. Kaced (2018), Information Inequalities are Not Closed Under Polymatroid Duality, *IEEE Transactions on Information Theory*, 64, pp 4379–4381
[11] T. Kaced (2011), Almost-perfect secret sharing, *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, pp 1603-1607
[12] J. Katz, Y. Lindell (2007), *Introduction to modern cryptography*, Chapman & Hall/CRC
[13] L. Lovász (1982), Submodular functions and convexity. *Mathematical Programming – The State of the Art* (A. Bachem, M. Grötchel and B. Korte, eds.), Springer-Verlag, Berlin, 234–257.
[14] K. Makarichev, Y. Makarichev, A. Romashchenko, N. Vereshchagin (2002), A new class of non-Shannon type inequalities for entropies. *Communications in Information and Systems*, vol 2, pp 147–166
[15] F. Matúš (1994), Probabilistic conditional independence structures and matroid theory: background. *Int. Journal of General Systems* **22** 185–196.
[16] F. Matúš (2007), Adhesivity of polymatroids, *Discrete Mathematics* **307** pp. 2464–2477
[17] F. Matúš (2007), Two constructions on limits of entropy functions. *IEEE Transactions on Information Theory* 53, pp 320-330.
[18] F. Matúš (2007), Infinitely many information inequalities. *Proceedings IEEE ISIT 2007*, Nice, France, pp 41–44.
[19] F. Matúš (2012), Polymatroids and polyquantoids. in: *Proceedings of WUPES'2012* (eds. J. Vejnarová and T. Kroupa) Mariánské Lázně, Prague, Czech Republic, pp 126-136.
[20] F. Matúš, L. Csirmaz (2016), Entropy region and convolution, *IEEE Trans. Inf. Theory* **62** 6007–6018
[21] J.G. Oxley (1992) *Matroid Theory*, Oxford Science Publications. The Calrendon Press, Oxford University Press, New York
[22] C. Padró (2012), Lecture notes in secret sharing, *Cryptology ePrint archive*, report 2012/674
[23] R. W. Yeung (2002), *A First Course in Information Theory*, Kluwer Academic/Plenum Publishers, New York.
[24] Y. Yu, M Wang (2011), A probabilistic secret sharing scheme for a compartmented access structure. *In: International Conference on Information and Communications Security*, pp 136-142. Springer, Berlin, Heidelberg,

Appendix

Theorem 23. *A matroid is connected if and only if any two points can be connected by a circuit.*

Proof. Let $\mathcal{M} = (h, M)$ be a matroid. Using matroid terminology, A is *dependent* if $h(A) < |A|$, and A is a *circuit* if it is a minimal dependent set. Every dependent set contains a circuit. Points x and y are *connected*, written as $a \approx b$, if there is a circuit containing both of them. First we prove that $\approx$ is an equivalence relation: if $x \approx z$ and $z \approx y$ then $x \approx y$. This is done in three steps. In claims a), b), c), C_1 and C_2 are different circuits.

a) *Suppose $z \in C_1 \cap C_2$. There is a circuit $E \subseteq C_1 \cup C_2$ which avoids z* (exchange property of circuits):
Proof. As C_1, C_2 are different circuits, $h(C_i) = |C_i| - 1$ and $h(C_1 \cap C_2) = |C_1 \cap C_2|$ as $C_1 \cap C_2$ is a proper subset of a circuit. Using submodularity for C_1 and C_2,

$$\begin{aligned} h(C_1 \cup C_2) &\le h(C_1) + h(C_2) - h(C_1 \cap C_2) \\ &= |C_1| + |C_2| - h(C_1 \cap C_2) - 2 \\ &= |C_1| + |C_2| - |C_1 \cap C_2| - 2 \\ &= |C_1 \cup C_2| - 2. \end{aligned}$$

Consequently $h(C_1C_2{-}z) \le |C_1C_2{-}z| - 1$, which means that $C_1C_2{-}z$ is dependent, thus contains a circuit.

b) *Let $x \in C_1{-}C_2$, and $z \in C_1 \cap C_2$. There is a circuit in $C_1 \cup C_2$ which contains x and avoids z.*

Proof. By induction on $|C_1 \cup C_2|$. By a) there is a circuit $E \subset C_1 \cup C_2$ which avoids z. Then $E \cap (C_2 - C_1)$ is not empty, as E is dependent while $E \cap C_1$, as a proper subset of C_1, is independent. If $x \in E$ then we are done. If $x \notin E$, then pick $z' \in E \cap (C_2 - C_1)$. By a) there is circuit $F \subset E \cup C_2$ which avoids z'. Use induction on C_1 and F.

c) *Let $x \in C_1 - C_2$, $y \in C_2 - C_1$, and $C_1 \cap C_2 = \emptyset$. There is a circuit $E \subseteq C_1 \cup C_2$ which contains x and y.*
Proof. By induction on $|C_1 \cup C_2|$. Let $z \in C_1 \cap C_2$. By b) there is a circuit $E \subset C_1 \cup C_2$ which contains x and avoids z. If $y \in E$, then we are done. If $y \notin E$, then pick $z' \in E \cap (C_2 - C_1)$. By b) there is a circuit $F \subset E \cup C_2$ such that $y \in F$ and $z' \notin F$. Use induction on C_1 and F.

This proves that $\approx$ is an equivalence relation. Any two points of the matroid are connected by a circuit if and only if there is only a single equivalence class for $\approx$. First assume that the matroid is connected, and by contradiction that A is a proper equivalence class of $\approx$. Consider the partition $A \cup B$ where B is the complement of A. Choose the independent sets $A' \subseteq A$ and $B' \subseteq B$ such that $h(A) = |A'|$ and $h(B) = |B'|$. As A and B are not independent, $h(A' \cup B') \le h(A \cup B) < h(A) + h(B) = h(A') + h(B') = |A'| + |B'|$, thus $A' \cup B'$ contains a circuit E. But E must intersect both A' and B' (as A' and B' are independent), contradicting that elements from $A' \subseteq A$ and from $B' \subseteq B$ are not connected.

Conversely, if the matroid is not connected, say the elements of the partition $A \cup B$ are independent, then no circuit can intersect both A and B. Indeed, first the independence of A and B implies $h(E) = h(E \cap A) + h(E \cap B)$ for all subsets $E \subseteq M$. Second, assume the circuit E intersects both A and B. Then $E \cap A$ and $E \cap B$ are independent (as proper subsets of E), and then

$$h(E) = h(E \cap A) + h(E \cap B) = |E \cap A| + |E \cap B| = |E|,$$

a contradicting that E is dependent. □

Theorem 24. *If $\xi = \langle \xi_a, \dots, \xi_e \rangle$ is a distribution on five elements, then the polymatroid $\mathcal{M}_\xi$ satisfies the* MMRV *inequality*

$$\big(h(a,b|c) + h(b,c|a) + h(c,a|b)\big) + \big(h(b,c|d) + h(b,c|e) + h(d,e) - h(b,c)\big) \ge 0, \tag{2}$$

written as $\mathsf{MMRV}(\mathcal{M}_\xi) \ge 0$.

Proof. Observe first that in *any* polymatroid $\mathcal{M} = (h, M)$ the inequality

$$\mathsf{MMRV}(\mathcal{M}) + 3h(a, de|bc) \ge 0$$

always holds. This is so as expanding $\mathsf{MMRV}(\mathcal{M}) + 3h(a, de|bc)$ as a linear combination of rank values, and expanding the clearly non-negative sum below, the results are the same:

$$h(a,d|b) + h(a,d|c) + h(a,e|b) + h(a,e|c) + h(b,c|ad) + h(b,c|ae) + h(a,bc|de) + h(d,e|a) + h(a,e|bcd) + h(a,d|bce).$$

The MMRV inequality (2) has been grouped into two parts. The first part depends only on ranks of subsets of abc, and the second part depends only on subsets of $bcde$. In other words, the value of the first (and second) part depends only on the marginal distribution ξ_{abc} and ξ_{bcde}, respectively. Σ denotes the collection of all distributions $\eta = \langle \eta_a, \dots, \eta_e \rangle$ where each of these five variables takes the same values as the corresponding variable does in ξ but with arbitrary joint probability. Consider the optimization problem of maximizing the entropy of $\eta \in \Sigma$ under the constraints that certain marginal distributions are fixed:

$$\max_\eta \{\mathbf{H}(\eta) : \eta \in \Sigma, \eta_{abc} = \xi_{abc}, \eta_{bcde} = \xi_{bcde}\}.$$

As $\mathbf{H}(\eta)$ is a strictly convex function of the probabilities, this is a convex optimization problem with linear constraints, consequently it has a single unique optimal solution $\eta^* \in \Sigma$. Considering the distribution with the maximal entropy is often referred to as the *maximum entropy principle*. As the marginals on abc and $bcde$ of ξ and η^* are the same, $\mathsf{MMRV}(\mathcal{M}_\xi) = \mathsf{MMRV}(\mathcal{M}_{\eta^*})$. The extremal distribution η^* has the additional

property that $\eta^\star_a$ and $\eta^\star_{de}$ are independent given $\eta^\star_{bc}$. This is so, as fixing the value of $\eta^\star_{bc}$, one can redefine the distribution while keeping the probabilities on abc and on $bcde$ fixed such that a and de becomes independent. This would increase the total entropy, thus a and de must be independent – giving the claimed conditional independence. Consequently the polymatroid $\mathcal{M}_{\eta^\star}$ satisfies additionally $h^\star(a, de|bc) = 0$, and then $\mathsf{MMRV}(\mathcal{M}_{\eta^\star}) \geq 0$, proving the theorem. □