Proceedings of WUPES 2012, Sept. 12–15, Mariánské Lázně, Czech Republic, 126–136.

Polymatroids and polyquantoids*

František Matúš

Institute of Information Theory and Automation
Academy of Sciences of the Czech Republic
matus@utia.cas.cz

Abstract

When studying entropy functions of multivariate probability distributions, polymatroids and matroids emerge. Entropy functions of pure multiparty quantum states give rise to analogous notions, called here polyquantoids and quantoids. Polymatroids and polyquantoids are related via linear mappings and duality. Quantum secret sharing schemes that are ideal are described by selfdual matroids. Expansions of integer polyquantoids to quantoids are studied and linked to that of polymatroids.

1 Introduction

A polymatroid (N, h) consists of a finite ground set N and rank function h on the subsets of N that is normalized $h(\emptyset) = 0$, nondecreasing $h(I) \leqslant h(J)$, $I \subseteq J$, and submodular $h(I)+h(J) \geqslant h(I\cup J)+h(I\cap J)$, $I, J \subseteq N$. A polymatroid is entropic if there exists a probability measure P on a finite set $\prod_{i\in N} X_i$ such that $h(I)$ equals Shannon entropy of the marginal of P to $\prod_{i\in I} X_i$, for all $I \subseteq N$. This means that h equals the entropy function of P. These functions always induce polymatroids.

In this work, a ***polyquantoid*** is introduced as a pair (N, e) with a rank function e on the subsets of N that is normalized, complementary $e(I) = e(N \setminus I)$, $I \subseteq N$, and submodular. A polyquantoid is entropic if there exists a quantum state ρ on a complex Hilbert space $\bigotimes_{i\in N} H_i$ of finite dimension such that $e(I)$ equals von Neumann entropy of the reduction of ρ to $\bigotimes_{i\in I} H_i$, for all $I \subseteq N$. This means that e equals the entropy function on ρ. These functions always induce polyquantoids, by properties of von Neumann entropy.

A polymatroid/polyquantoid is integer if all values of its rank function are integer numbers. An integer polymatroid whose values on singletons equal zero or one is called matroid. Let *quantoid* be defined as an integer polyquantoid with this property.

This contribution studies interplay between polymatroids, polyquantoids, matroids, quantoids and secret sharing schemes, both classical and quantum. In Section 2, duality of set functions is worked out. Section 3 introduces mutually inverse linear mappings that provide a one-to-one correspondence between tight selfdual polymatroids and polyquantoids, see Theorem 1. This correspondence can serve as a tool for comparing problems on classical and quantum entropy functions.

In Section 4, secret sharing schemes are lifted to the level of polymatroids/polyquantoids. Theorem 2 recalls that the ideal sharing in polymatroids is governed by matroids. This result is translated to polyquantoids in Theorem 3 that describes the ideal quantum sharing via those quantoids that correspond to tight selfdual matroids.

Section 5 departs from the notion of expansions of integer polymatroids to matroids. An analogous construction for integer polyquantoids is introduced to provide expansions of polyquantoids to quantoids, see Theorem 4. Thus, the quantoids play a role of matroids in quantum settings. In Section 6, remarks and discussion of related material and literature are collected.

This work was supported by Grant Agency the Czech Republic under Grant 201/08/0539.

2 Duality

For set functions h with a ground set N, the following definition

$$h'(I) \triangleq h(N \setminus I) + h(\emptyset) - h(N) + \sum_{i \in I} \big[h(i) - h(\emptyset) + h(N) - h(N \setminus i)\big]\,, \quad I \subseteq N\,,$$

gives rise to a duality mapping $h \mapsto h'$. A function h is *selfdual* if $h' = h$. The functions that are complementary, as in polyquantoids, are selfdual.

Let us say that a set function h is *tight* if $h(N \setminus i) = h(N)$ for all $i \in N$. If h is normalized and tight then the definition of duality simplifies to

$$h'(I) = h(N \setminus I) - h(N) + \sum_{i \in I} h(i)\,, \quad I \subseteq N\,.$$

Lemma 1. *For any function h on the subsets of N,*
(i) $h'(\emptyset) = h(\emptyset)$,
(ii) $h'(i) = h(i)$ for $i \in N$,
(iii) $h'(N) - h'(N \setminus i) = h(N) - h(N \setminus i)$ for $i \in N$,
(iv) $h'' = h$,
(v) h is submodular if and only if h' is so,
(vi) if h is normalized, submodular and $h(N) \geqslant h(N \setminus i)$, $i \in N$, then h' is nondecreasing.

Proof. First two assertions follow directly from the definition. For $K \subseteq J$ the equality

$$h'(J) - h'(K) = h(N \setminus J) - h(N \setminus K) + \sum_{i \in J \setminus K} \big[h(i) - h(\emptyset) + h(N) - h(N \setminus i)\big]$$

implies *(iii)*. Choosing $K = N \setminus I$ and $J = N$, it rewrites to

$$h(I) = h'(N \setminus I) + h(\emptyset) - h'(N) + \sum_{i \in I} \big[h(i) - h(\emptyset) + h(N) - h(N \setminus i)\big]\,, \qquad I \subseteq N\,.$$

By *(i)*, *(ii)* and *(iii)*, the right-hand side equals $h''(I)$ which proves *(iv)*. If h is submodular then $I \mapsto h(N \setminus I)$ is so whence h' is submodular. Then, the equivalence *(v)* holds by *(iv)*. If h is normalized and $h(N) \geqslant h(N \setminus i)$, $i \in N$, then for $J \supseteq K$

$$h'(J) - h'(K) \geqslant h(N \setminus J) - h(N \setminus K) + \sum_{i \in J \setminus K} h(i)\,.$$

If h is also submodular then the right-hand side is nonnegative whence *(vi)* holds. □

Corollary 1. *The duality mapping restricts to an involution on the (tight) polymatroids.*

3 Tight selfdual polymatroids and polyquantoids

Let h and e be set functions with the ground set N. The linear mappings $e \mapsto e^\wedge$ and $h \mapsto h^\vee$ introduced here by

$$e^\wedge(I) \triangleq e(I) + \sum_{i \in I} e(i) \quad \text{and} \quad h^\vee(I) \triangleq h(I) - \tfrac{1}{2} \sum_{i \in I} h(i)\,, \quad I \subseteq N\,,$$

are mutually inverse, $(e^\wedge)^\vee = e$ and $(h^\vee)^\wedge = h$. They provide a natural link between the polymatroids and polyquantoids.

Theorem 1. *The mappings $e \mapsto e^\wedge$ and $h \mapsto h^\vee$ restrict to mutually inverse bijections between the polyquantoids and the tight selfdual polymatroids.*

Proof. Let (N, e) be a polyquantoid. Since e is normalized $e^\wedge(\emptyset) = 0$. The submodularity of e is equivalent to that of $e^\wedge$, and implies $e(N \setminus I) \leqslant e(N \setminus J) + \sum_{i \in J \setminus I} e(i)$ for $I \subseteq J \subseteq N$. By complementarity, $e(I) \leqslant e(J) + \sum_{i \in J \setminus I} e(i)$, and thus $e^\wedge(I) \leqslant e^\wedge(J)$. Therefore, $(N, e^\wedge)$ is a polymatroid. Since e is normalized and complementary

$$e^\wedge(N) = \sum_{j \in N} e(j) = e(N \setminus i) + \sum_{j \in N \setminus i} e(j) = e^\wedge(N \setminus i)\,, \quad i \in N\,,$$

thus $e^\wedge$ is tight. For $I \subseteq N$ it follows that

$$\begin{aligned}(e^\wedge)'(I) &= e^\wedge(N \setminus I) - e^\wedge(N) + \sum_{i \in I} e^\wedge(i) \\ &= \Big[e(N \setminus I) + \sum_{i \in N \setminus I} e(i)\Big] - \sum_{i \in N} e(i) + 2 \sum_{i \in I} e(i) = e^\wedge(I)\,,\end{aligned}$$

thus $e^\wedge$ is selfdual.

Let (N, h) be a tight selfdual polymatroid. Since h is normalized $h^\vee(\emptyset) = 0$. Since h is tight and selfdual $h(I) = h(N \setminus I) - h(N) + \sum_{i \in I} h(i)$, $I \subseteq N$. Then, $h(N)$ is equal to $\frac{1}{2} \sum_{i \in N} h(i)$. It follows that

$$h^\vee(N \setminus I) = \Big[h(I) - h(N) + \sum_{i \in N \setminus I} h(i)\Big] - \tfrac{1}{2} \sum_{i \in N \setminus I} h(i) = h^\vee(I)\,, \quad I \subseteq N\,,$$

thus $h^\vee$ is complementary. The submodularity of h implies that of $h^\vee$. Therefore, $(N, h^\vee)$ is a polyquantoid. □

Remark 1. The above proof provides also arguments for the assertion that the mappings $e \mapsto e^\wedge$ and $h \mapsto h^\vee$ restrict to mutually inverse bijections between the class of normalized complementary functions and the class of normalized tight selfdual functions, dropping submodularity in Theorem 1.

Corollary 2. *The mappings $e \mapsto e^\wedge$ and $h \mapsto h^\vee$ induce mutually inverse bijections between the integer polyquantoids and the integer tight selfdual polymatroids whose values on all singletons are even.*

Corollary 3. *The mappings $e \mapsto e^\wedge$ and $h \mapsto h^\vee$ induce mutually inverse bijections between the quantoids and the integer tight selfdual polymatroids whose values on all singletons equal zero or two.*

4 Ideal secret sharing

Given a polymatroid (N, h), an element $\mathit{0}$ of N is *perfect* if $h(\mathit{0} \cup I) - h(I)$ equals $h(\mathit{0})$ or zero, for all $I \subseteq N \setminus \mathit{0}$. In the latter case, I is *authorized* for $\mathit{0}$. By submodularity,

$$h(\mathit{0} \cup I) - h(I) \geqslant h(\mathit{0} \cup J) - h(J)\,, \qquad I \subseteq J \subseteq N \setminus \mathit{0}\,.$$

Hence, $h(\mathit{0} \cup I) - h(I) = 0$ implies $0 \geqslant h(\mathit{0} \cup J) - h(J)$, and $h(\mathit{0} \cup J) - h(J) = h(\mathit{0})$ implies $h(\mathit{0} \cup I) - h(I) \geqslant h(\mathit{0})$. The two inequalities are tight as h is a polymatroid. Thus, the family of authorized sets for $\mathit{0}$ is closed to supersets and the family of sets $I \subseteq N \setminus \mathit{0}$ with $h(\mathit{0} \cup I) - h(I)$ equal to $h(\mathit{0})$ is closed to subsets. This is referred to as heredity. If $\mathit{0}$ is perfect and $h(\mathit{0}) > 0$ then the two families are disjoint and cover all subsets of $N \setminus \mathit{0}$, which is referred to as dichotomy.

In a polymatroid (N, h) with a perfect element $\mathit{0} \in N$, an element $i \in N \setminus \mathit{0}$ is *essential* for $\mathit{0}$ if it belongs to some set I that is authorized for $\mathit{0}$ and $h(\mathit{0} \cup I \setminus i) - h(I \setminus i) = h(\mathit{0})$. As a consequence,

$$h(i) \geqslant h(I) - h(I \setminus i) = h(\mathit{0} \cup I) - h(I \setminus i) \geqslant h(\mathit{0} \cup I \setminus i) - h(I \setminus i) = h(\mathit{0})\,,$$

since h is submodular and nondecreasing. A perfect element $\mathit{0}$ in a polymatroid (N, h) is *ideal* if each $i \in N \setminus \mathit{0}$ is essential for $\mathit{0}$ and $h(i) = h(\mathit{0})$.

For example, in any matroid (N, r) each element is perfect. Given $\mathit{0} \in N$, a set $I \subseteq N \setminus \mathit{0}$ is authorized for $\mathit{0}$ if and only if a circuit contained in $\mathit{0} \cup I$ contains $\mathit{0}$. If $r(\mathit{0}) = 0$, thus $\mathit{0}$ is a loop, then all $i \in N \setminus \mathit{0}$

are essential for $\mathit{0}$. Hence, $\mathit{0}$ is ideal if only if $r(N) = 0$. Otherwise, when $r(\mathit{0}) = 1$, i is essential for $\mathit{0}$ if and only if there exists a circuit of the matroid containing $\mathit{0}$ and i. Therefore, $\mathit{0}$ is ideal if only if the matroid is connected. Each element of any connected matroid is ideal.

When restricting to the entropic polymatroids, the above notions correspond to the information-theoretical secret sharing schemes.

The following assertion claims that existence of an ideal element implies matroidal structure. It follows from an existing result, see Section 6, but a self-contained proof is presented for convenience.

Theorem 2. *If a polymatroid (N, h) has an ideal element then there exists a matroid (N, r) and $t > 0$ such that $h = t\, r$.*

Proof. Let $\mathit{0} \in N$ be an ideal element of the polymatroid. If $h(\mathit{0}) = 0$ then $h(i) = 0$ for all $i \in N$ whence (N, h) is a matroid and the assertion holds with any $t > 0$. Let $h(\mathit{0}) > 0$.

The idea is to prove that 'if $L \subseteq N$ is nonempty then there exists $\ell \in L$ such that $h(L) - h(L \setminus \ell)$ equals $h(\mathit{0})$ or zero'. This implication and an induction argument on the cardinality of L show that all values of h are multiples of $h(\mathit{0})$. As a consequence, h equals a matroid rank function multiplied by $t = h(\mathit{0}) > 0$.

If $L \subseteq N$ contains $\mathit{0}$ the implication holds with $\ell = \mathit{0}$ because $\mathit{0}$ is perfect.

If $L \subseteq N \setminus \mathit{0}$ is authorized, $h(\mathit{0} \cup L) = h(L)$, then $h(\mathit{0} \cup I) = h(\mathit{0}) + h(I)$ for some $I \subseteq L$, e.g. $I = \emptyset$. Such a set I is chosen to be inclusion maximal. By dichotomy, $I \subsetneq L$. Let $\ell \in L \setminus I$. Since I is maximal and $\mathit{0}$ perfect, $\ell \cup I$ is authorized, $h(\mathit{0} \cup \ell \cup I) = h(\ell \cup I)$. This and submodularity imply

$$h(\mathit{0} \cup L \setminus \ell) + h(\mathit{0} \cup \ell \cup I) \geqslant h(\mathit{0} \cup L) + h(\mathit{0} \cup I) = h(\mathit{0} \cup L) + h(\mathit{0}) + h(I)\,,$$
$$h(\ell) + h(I) \geqslant h(\ell \cup I) = h(\mathit{0} \cup \ell \cup I)\,.$$

As $\mathit{0}$ is ideal, $h(\mathit{0}) = h(\ell)$, and it follows by adding that $h(\mathit{0} \cup L \setminus \ell) \geqslant h(\mathit{0} \cup L)$. Thus, $h(\mathit{0} \cup L \setminus \ell) = h(\mathit{0} \cup L) = h(L)$ because h is nondecreasing and L authorized. This implies that $h(L) - h(L \setminus \ell)$ equals $h(\mathit{0} \cup L \setminus \ell) - h(L \setminus \ell)$ which is zero or $h(\mathit{0})$ by perfectness of $\mathit{0}$. Hence, the implication holds for every L authorized.

By dichotomy, it remains to consider a nonempty subset L of $N \setminus \mathit{0}$ such that $h(\mathit{0} \cup L)$ equals $h(\mathit{0}) + h(L)$. Since $\mathit{0}$ is ideal, any $\ell \in N \setminus \mathit{0}$ is essential for $\mathit{0}$. Taking some $\ell \in L$ there exists an authorized set K, $h(\mathit{0} \cup K) = h(K)$, such that $\ell \in K$ and $h(\mathit{0} \cup K \setminus \ell)$ equals $h(\mathit{0}) + h(K \setminus \ell)$. Such a set K is chosen to obtain the cardinality of $K \setminus L$ minimal. By dichotomy, K is not contained in L. For every $k \in K \setminus L$ the minimality implies that the set $L \cup K \setminus k$, containing the chosen ℓ, is not authorized. In turn, since h is submodular, $L \cup K$ authorized and h nondecreasing

$$h(k) + h(L \cup K \setminus k) \geqslant h(L \cup K) = h(\mathit{0} \cup L \cup K) \geqslant h(\mathit{0} \cup L \cup K \setminus k) = h(\mathit{0}) + h(L \cup K \setminus k)\,.$$

The above two inequalities are tight because $h(\mathit{0}) = h(k)$, using that $\mathit{0}$ is ideal. Therefore, $h(L \cup K) = h(k) + h(L \cup K \setminus k)$ for $k \in K \setminus L$. By induction,

$$h(I \cup (K \setminus L)) = h(I) + \sum_{k \in K \setminus L} h(k)\,, \qquad I \subseteq L\,.$$

This implies that $h(L) - h(L \setminus \ell)$ equals $h(L \cup K) - h((L \cup K) \setminus \ell)$. The previous part of the proof is applied to the authorized set K in the role of L and the non-authorized set $K \setminus \ell$ in the role of I to conclude that $h(\mathit{0} \cup K \setminus \ell) = h(\mathit{0} \cup K)$. This implies that $h(\mathit{0} \cup (L \cup K) \setminus \ell)$ equals $h(\mathit{0} \cup L \cup K)$ which coincides with $h(L \cup K)$ because $L \cup K$ is authorized. Hence, $h(L) - h(L \setminus \ell)$ equals $h(\mathit{0} \cup (L \cup K) \setminus \ell) - h((L \cup K) \setminus \ell)$ which is zero or $h(\mathit{0})$ by perfectness of $\mathit{0}$. Thus, the implication holds for all nonempty $L \subseteq N \setminus \mathit{0}$. □

Given a polyquantoid (N, e), an element $\mathit{0}$ of N is *perfect* if $e(\mathit{0} \cup I) - e(I)$ equals $e(\mathit{0})$ or $-e(\mathit{0})$, for all $I \subseteq N \setminus \mathit{0}$. In the latter case, I is *authorized* for $\mathit{0}$. The definition of perfectness does not change when requiring that $e^\wedge(\mathit{0} \cup I) - e^\wedge(I)$ equals $e^\wedge(\mathit{0})$ or zero. Thus, $\mathit{0}$ is perfect in (N, e) if and only if it is perfect in the polymatroid $(N, e^\wedge)$. Therefore, supersets of authorized sets are authorized and the equality $e(\mathit{0} \cup I) - e(I) = e(\mathit{0})$ with $I \subseteq N \setminus \mathit{0}$ is inherited by the subsets of I. The dichotomy takes place whenever $e(\mathit{0}) > 0$.

In a polyquantoid (N, e) with a perfect element $\mathit{0} \in N$, an element $i \in N \setminus \mathit{0}$ is *essential* for $\mathit{0}$ if there exists a set I which authorized for $\mathit{0}$, contains i and $e(\mathit{0} \cup I \setminus i) - e(I \setminus i) = e(\mathit{0})$. This is equivalent to saying that $i \in N \setminus \mathit{0}$ is *essential* for $\mathit{0}$ in the polymatroid $(N, e^\wedge)$. Hence, $e(i) \geqslant e(\mathit{0})$ once i is essential for $\mathit{0}$ in (N, e). A perfect element $\mathit{0}$ in a polyquantoid (N, e) is *ideal* if each $i \in N \setminus \mathit{0}$ is essential for $\mathit{0}$ and $e(i) = e(\mathit{0})$.

Theorem 3. *If a polyquantoid (N, e) has an ideal element then there exists a tight selfdual matroid (N, r) and $t > 0$ such that $e = t\, r^\vee$.*

Proof. If $\mathit{0} \in N$ is ideal in the polyquantoid then $\mathit{0}$ is ideal in $(N, e^\wedge)$ which is a tight selfdual polymatroid by Theorem 1. Theorem 2 implies that $e^\wedge = t\, r$ for $t > 0$ and a matroid rank function r. Hence, r is tight, selfdual, and $e = (e^\wedge)^\vee = (t\, r)^\vee = t\, r^\vee$. □

As a consequence, if $\mathit{0}$ is an ideal element of a polyquantoid then $I \subseteq N \setminus \mathit{0}$ is authorized for $\mathit{0}$ if and only if $\mathit{0} \in C \subseteq \mathit{0} \cup I$ for some circuit C of the tight selfdual matroid that is assigned to the polyquantoid in Theorem 3.

5 Expansions

A set function h with a ground set N *expands* to a set function $h^\#$ with a ground set $N^\#$ if there exists a mapping ϕ on N ranging in the family of subsets of $N^\#$ such that $h^\#(\bigcup_{i \in I} \phi(i))$ equals $h(I)$ for all $I \subseteq N$.

Each integer polymatroid (N, h) can be expanded to a matroid as follows. Let ϕ map $i \in N$ to a set $\phi(i)$ of cardinality $h(i)$ such that these sets are pairwise disjoint. Writing $\phi(I) = \bigcup_{i \in I} \phi(i)$, $I \subseteq N$, the construction

$$h_\phi \colon K \mapsto \min_{J \subseteq N} \left[\, h(J) + |K \setminus \phi(J)| \,\right], \qquad K \subseteq \phi(N)\,,$$

defines a matroid $(\phi(N), h_\phi)$ called a *free expansion* of (N, h). The value $h_\phi(K)$ depends on K only through the cardinalities of the sets $\phi(i) \cap K$, $i \in N$. The minimization can be equivalently over the sets that satisfy

$$\{i \in N \colon \phi(i) \cap K \neq \emptyset\} \supseteq J \supseteq \{i \in N \colon \emptyset \neq \phi(i) \subseteq K\}$$

since h is nondecreasing and submodular. Such sets J are termed to be *adapted* to K. Hence, $h_\phi(\phi(I))$ equals $h(I)$ for all $I \subseteq N$, using that $\{i \in I \colon \phi(i) \neq \emptyset\}$ is the unique adapted set to $\phi(I)$, and thus h expands to h_ϕ.

For any integer polyquantoid (N, e), an analogous construction is introduced as follows. Let ψ map $i \in N$ to a set $\psi(i)$ of cardinality $e(i)$ such that these sets are pairwise disjoint, $\psi(I) = \bigcup_{i \in I} \psi(i)$, $I \subseteq N$, and

$$e_\psi \colon K \mapsto \min_{J \subseteq N} \left[\, e(J) + |K \vartriangle \psi(J)| \,\right], \qquad K \subseteq \psi(N)\,.$$

Let $(\psi(N), e_\psi)$ be called a *free expansion* of (N, e). The minimization can be equivalently over the sets adapted to K, using that e is normalized, complementary and submodular. Therefore, $e_\psi(\psi(I)) = e(I)$, $I \subseteq N$, thus e expands to e_ψ indeed.

The following assertion shows that from the viewpoint of expansions, quantoids are for polyquantoids what matroids are to polymatroids.

Theorem 4. *Any free expansion of an integer polyquantoid is a quantoid.*

Proof. Let (N, e) be an integer polyquantoid and ψ a mapping as above. By definition, $e_\psi(K) = |K|$ if $K \subseteq \psi(i)$ for some $i \in N$. In particular, e_ψ is normalized and its values on singletons equal one.

For $J \subseteq N$ adapted to $K \subseteq \psi(N)$, the set $J' = \{i \in N \setminus J \colon \psi(i) \neq \emptyset\}$ is adapted to $\psi(N) \setminus K$ and

$$e(J) + |K \vartriangle \psi(J)| = e(J') + \big|(\psi(N) \setminus K) \vartriangle (\psi(J'))\big|$$

using $e(J) = e(N \setminus J) = e(J')$. Moreover, $J \mapsto J'$ is a bijection between the families of those sets that are adapted to K, resp. to $\psi(N) \setminus K$. It follows by minimization that $e_\psi(K)$ equals $e_\psi(\psi(N) \setminus K)$, thus e_ψ is complementary.

To prove that e_ψ is submodular, let $K, L \subseteq \psi(N)$ and

$$e_\psi(K) = e(I) + |K \vartriangle \psi(I)| \quad \text{and} \quad e_\psi(L) = e(J) + |L \vartriangle \psi(J)|$$

where I is adapted to K and J is adapted to L. As $e(I) + e(J) \geqslant e(I \cup J) + e(I \cap J)$ and

$$|K \vartriangle \psi(I)| + |L \vartriangle \psi(J)| = |(K \cup L) \vartriangle \psi(I \cup J)| + |(K \cap L) \vartriangle \psi(I \cap J)|$$

the submodularity of e_ψ follows. □

In the remaining part of this section, expansions of polymatroids and polyquantoids are compared by means of the mappings $e \mapsto e^\wedge$ and $h \mapsto h^\vee$.

Let (N, h) be an integer polymatroid with $h(i)$ even for all $i \in N$ and $(\phi(N), h_\phi)$ its free expansion. Then, each set $\phi(i)$ can be partitioned into two-element blocks $m = \{k, \ell\}$ having $k, \ell \in \phi(i)$ different. Let $\phi^*(i)$ denote the set of all blocks in such a partition, $\phi^*(I) = \bigcup_{i \in I} \phi^*(i)$, $I \subseteq N$, and

$$h_{\phi^*}(M) \triangleq h_\phi(\textstyle\bigcup M) = \min_{J \subseteq N} \left[h(J) + |\bigcup M \setminus \phi(J)| \right], \qquad M \subseteq \phi^*(N).$$

This defines a polymatroid $(\phi^*(N), h_{\phi^*})$ called here 2-*factor* of $(\phi(N), h_\phi)$. By definitions, (N, h) expands to $(\phi^*(N), h_{\phi^*})$ which in turn expands to $(\phi(N), h_\phi)$.

The following assertion indicates a correspondence between the free expansions of polymatroids and polyquantoids.

Lemma 2. *If (N, e) is an integer polyquantoid, $h = e^\wedge$, $(\phi(N), h_\phi)$ a free expansion of (N, h) and $(\phi^*(N), h_{\phi^*})$ its 2-factor then $(\phi^*(N), (h_{\phi^*})^\vee)$ is a free expansion of (N, e).*

Proof. For $M \subseteq \phi^*(N)$

$$(h_{\phi^*})^\vee(M) = h_{\phi^*}(M) - \tfrac{1}{2} \sum_{m \in M} h_{\phi^*}(\{m\}) = h_\phi(\textstyle\bigcup M) - |M|$$

using that $h_{\phi^*}(\{m\}) = h_\phi(m) = 2$. Since $e(j) = h(j)/2 = |\phi^*(j)|$ for $j \in N$, if $J \subseteq N$ then $h(J) = e(J) + |\phi^*(J)|$. Then, by the definition of polymatroid expansions,

$$(h_{\phi^*})^\vee(M) = \min_{J \subseteq N} \left[e(J) + |\phi^*(J)| + |\textstyle\bigcup M \setminus \phi(J)| \right] - |M|$$

Here, $|\bigcup M \setminus \phi(J)| = 2|M \setminus \phi^*(J)|$. Since $|\phi^*(J)| + |M \setminus \phi^*(J)| - |M|$ equals $|\phi^*(J) \setminus M|$ it follows from definition of polyquantoid expansions that $(h_{\phi^*})^\vee$ coincides with e_{ϕ^*}. □

In the above lemma, the integer polymatroid $h = e^\wedge$ is tight and selfdual, by Theorem 1. The following two lemmas imply that the expansion h_ϕ and its 2-factor h_{ϕ^*} have the same properties. Hence, Theorem 4 can be proved alternatively by combining Theorem 1 with Lemmas 2, 3 and 4. This argument is more involved but illustrates the interplay between the two kinds of expansions.

Lemma 3. *If an integer polymatroid is tight and selfdual then so are its free expansions.*

Proof. Let (N, h) be an integer polymatroid and ϕ a mapping with $|\phi(i)| = h(i)$, $i \in N$, as above. For $k \in \phi(N)$ there exists unique $i \in N$ such that $k \in \phi(i)$. Assuming that h is tight $h_\phi(\phi(N \setminus i)) = h(N \setminus i) = h(N) = h_\phi(\phi(N))$. This implies $h_\phi(\phi(N) \setminus k) = h_\phi(\phi(N))$ whence h_ϕ is tight.

By definition, $h_\phi(K) = |K|$ if $K \subseteq \phi(i)$ for some $i \in N$. Hence, assuming that h is tight and selfdual, for a set $J \subseteq N$ adapted to $K \subseteq \phi(N)$,

$$\begin{aligned} h(J) + |K \setminus \phi(J)| &= h(N \setminus J) - h(N) + |\phi(J)| + |K \setminus \phi(J)| \\ &= h(N \setminus J) - h_\phi(\phi(N)) + |K| + \big|(\phi(N) \setminus K) \setminus (\phi(N \setminus J))\big| . \end{aligned}$$

Minimizing over the adapted sets, it follows that $h_\phi(K) \geqslant h_\phi(\phi(N) \setminus K) - h_\phi(\phi(N)) + |K|$. Since J is adapted to K if and only if $J' = \{i \in N \setminus J \colon \phi(i) \neq \emptyset\}$ is adapted to $\phi(N) \setminus K$ this inequality is tight. Thus, h_ϕ is selfdual. □

Lemma 4. *If an integer polymatroid is tight, selfdual and takes even values on all singletons then all 2-factors of its free expansions are tight and selfdual.*

Proof. Let (N,h) satisfy the assumptions. Keeping the notation of the proof of Lemma 3, for $m\in\phi^*(N)$ there exists unique $i\in N$ such that $m\subseteq\phi(i)$. Since h is tight $h_\phi(\phi(N\setminus i))$ equals $h_\phi(\phi(N))$. Hence,

$$h_{\phi^*}(\phi^*(N)\setminus\{m\})=h_\phi(\phi(N)\setminus m)\geqslant h_\phi(\phi(N\setminus i))=h_\phi(\phi(N))=h_{\phi^*}(\phi^*(N))$$

In turn, h_{ϕ^*} is tight.

By Lemma 3, $(\phi(N),h_\phi)$ is selfdual. Hence, for $M\subseteq\phi^*(N)$

$$\begin{aligned}(h_{\phi^*})'(M)&=h_{\phi^*}(\phi^*(N)\setminus M)-h_{\phi^*}(\phi^*(N))+\sum_{m\in M}h_{\phi^*}(\{m\})\\&=h_\phi(\phi(N)\setminus\bigcup M)-h_\phi(\phi(N))+\sum_{k\in\bigcup M}h_\phi(k)=h_\phi(\bigcup M)=h_{\phi^*}(M)\end{aligned}$$

using that $h_{\phi^*}(\{m\})=2=h_\phi(k)+h_\phi(\ell)$ where $m=\{k,\ell\}$. □

6 Discussion

The polymatroids [10, 5, 14] have been studied for decades and history of the matroid theory [16] is even longer. The duality defined in Section 2 is in general different from known ones, as those in [14, 16, 20], since it conserves values on singletons, see Lemma 1*(ii)*. For matroids without loops and coloops, the duality coincides with the usual one [16, 2.1.9]. Functions called above selfdual are in literature also termed identically selfdual. Tightness is a notion suitable for this work but not used elsewhere. A matroid is tight if and only if it has no coloop.

The problem which polymatroid is entropic is of interest for information-theoretical approaches to networks and cryptography, and beyond, for references see e.g. [21, 11, 12]. Its quantum version, asking which polyquantoid is entropic, has also attracted considerable attention [17, 9, 3].

Ideal secret sharing schemes were investigated first in a combinatorial setting [2]. Theorem 2 is a consequence of [1, Theorem 2], building on [2, Theorem 1]. The presented proof is based on the approach of [1]. Quantum secret sharing schemes go back to [4, 7, 6]. Ideal sharing and matroids were discussed recently in [18, 19]. Theorem 3 solves a question related to [18, Fig. 2]. It implies that the access structure of any ideal quantum secret sharing scheme must be generated by circuits of a tight selfdual matroid.

Free expansions were proposed independently by several researchers, see [8, 13, 15]. If an entropic integer polymatroid expands to a matroid then the latter is the limit of entropic polymatroids [12, Theorem 4]. The quantum analogue of this assertion is open.

Acknowledgement

The author wants to express sincere thanks to Mary Beth Ruskai and Andreas Winter for numerous inspiring discussions and kind hospitality during visits. Discussions with Oriol Farràs Ventura on quantum secret sharing are acknowledged.

References

[1] G.R. Blakley and G.A. Kabatianski (1997) Generalized ideal secret-sharing schemes and matroids. *Problems of Inf. Transmission* **33** 277–284.

[2] E.F. Brickell and D.M. Davenport (1991) On the classification of ideal secret-sharing schemes. *J. Cryptology* **4** 123–134.

[3] J. Cadney, N. Linden and A. Winter (2012) Infinitely many constrained inequalities for the von Neumann entropy. *IEEE Trans. Inf. Th.* **58** 3657–3663.

[4] R. Cleve, D. Gottesman and H.-K. Lo (1999) How to share a quantum secret. *Ph. Review Letters* **83** 648–651.

[5] S. Fujishige (1991) *Submodular Functions and Optimization.* North-Holland, Amsterdam.

[6] D. Gottesman (2000) Theory of quantum secret sharing. *Phys. Rev. A* **61** 042311.

[7] M. Hillery, V. Bužek and A. Berthiaume (1999) Quantum secret sharing. *Phys. Rev. A* **59** 1829–1834.

[8] T. Helgason (1974) Aspects of the theory of hypermatroids. In: *Hypergraph Seminar* (C. Berge and D.K. Ray-Chaudhuri, eds.), Lecture Notes in Mathematics **411**, Springer-Verlag, Berlin, 191–214.

[9] N. Linden and A. Winter (2005) A new inequality for the von Neumann entropy. *Commun. Math. Phys.* **259** 129–138.

[10] L. Lovász (1982) Submodular functions and convexity. In: *Mathematical Programming – The State of the Art* (A. Bachem, M. Grötchel and B. Korte, eds.), Springer-Verlag, Berlin, 234–257.

[11] F. Matúš (2007) Infinitely many information inequalities. *Proceedings ISIT 2007*, Nice, France, 41–44.

[12] F. Matúš (2007) Two constructions on limits of entropy functions. *IEEE Trans. Inf. Th.* **53** 320–330.

[13] C.J.H. McDiarmid (1975) Rado's theorem for polymatroids. *Math. Proc. Cambridge Phil. Soc.* **78** 263–281.

[14] H. Narayan (1997) *Submodular Functions and Electrical Networks.* Elsevier, Amsterdam.

[15] H.Q. Nguyen (1978) Semimodular functions and combinatorial geometries. *Trans. AMS* **238** 355–383.

[16] J.G. Oxley (1992) *Matroid Theory.* Oxford University Press, Oxford, New York, Tokyo.

[17] N. Pippenger (2003) The inequalities of quantum information theory. *IEEE Trans. Inf. Th.* **49** 773–789.

[18] P. Sarvepalli and R. Raussendorf (2010) Matroids and quantum-secret-sharing schemes. *Physical Review A* **81** 052333.

[19] P. Sarvepalli (2011) Quantum codes and symplectic matroids. (arXiv:1104.1171v1 [quant-ph])

[20] G. Whittle (1992) Duality in polymatroids and set functions. *Combinatorics, Probability and Computing* **1** 275–280.

[21] Z. Zhang and R.W. Yeung (1998) On characterization of entropy function via information inequalities. *IEEE Trans. Inf. Th.* **44** 1440–1452.