Two constructions on limits of entropy functions

František Matúš

***Abstract*— The correspondence between the subvectors of a random vector and their Shannon entropies gives rise to an entropy function. Limits of the entropy functions are closed to convolutions with modular polymatroids, and when integer-valued also to free expansions. The problem of description of the limits of entropy functions is reduced to those limits that correspond to matroids. Related results on entropy functions are reviewed with regard to polymatroid and matroid theories, and perfect and ideal secret sharing.**

***Index Terms*— Almost affine code, coloring, entropy function, equipartition, ideal secret sharing, information rate, information inequalities, matroid, partition representation, polymatroid.**

I. Introduction

THE *entropy function* of a random vector $(\xi_i)_{i\in N}$ maps the subsets I of an index set N into the Shannon entropies $H(\xi_I)$ of the subvectors $\xi_I = (\xi_i)_{i\in I}$. Restricting attention to the vectors that are indexed by finite sets and take finite number of values, an entropy function is considered for a point of the Euclidean space $\mathbb{R}^{\mathcal{P}(N)}$ where $\mathcal{P}(N)$ is the power set of N. This work focuses on the set $\boldsymbol{H}_N^{\mathsf{ent}}$ of all such entropy functions and the set $cl(\boldsymbol{H}_N^{\mathsf{ent}})$ of their limits in the topology of this space.

By properties of the Shannon entropy, an entropy function g is normalized, $g(\emptyset) = 0$, nondecreasing, $g(I) \leqslant g(J)$ for $I \subseteq J \subseteq N$, and submodular, $g(I)+g(J) \geqslant g(I\cup J)+g(I\cap J)$ for $I, J \subseteq N$. Thus, the pair (N, g) is a *polymatroid* with the ground set N and rank function g [30], [17], [44]. Recall that a *matroid* is an integer-valued polymatroid (N, r) with the rank function bounded by the cardinality, $r(I) \leqslant |I|$ for $I \subseteq N$ [54], [48].

The polymatroids with the same finite ground set N can be represented as points of the polyhedral cone $\boldsymbol{H}_N$ in $\mathbb{R}^{\mathcal{P}(N)}$ defined by the linear inequalities expressing the normality, nondecreasingness and submodularity. Thus, $\boldsymbol{H}_N^{\mathsf{ent}} \subseteq \boldsymbol{H}_N$, and polymatroids provide a natural geometrical framework for entropy functions and their limits. In this framework, not distinguishing between polymatroids and their rank functions, let us call a polymatroid *entropic* if it equals the entropy function of a random vector taking a finite number of values, thus belongs to $\boldsymbol{H}_N^{\mathsf{ent}}$, and *asymptotically entropic* if it equals the pointwise limit of a sequence of entropic polymatroids, thus belongs to $cl(\boldsymbol{H}_N^{\mathsf{ent}})$.

It is well known that the entropic polymatroids are closed to sums, Lemma 1, and that $cl(\boldsymbol{H}_N^{\mathsf{ent}})$ is a convex cone [57, Theorem 1], see also Lemma 4 and Remark 1 in Section II. Therefore, the notion of asymptotically entropic polymatroid does not depend on the choice of the base of logarithms occuring in Shannon entropies, which are fixed here as the natural ones, whereas this does not hold for the notions of entropy function and entropic polymatroid.

Existing investigations of the set $\boldsymbol{H}_N^{\mathsf{ent}}$ have been motivated by numerous appearances of the entropy functions in problems of the information theory and multivariate analysis. This set and its closure are very closely related to the information theoretical inequalities, see Subsection IV-A, that are widely used for proving converse coding theorems. For introductory material underlying and an overview of information inequalities and entropy functions we refer the reader to [55]. A particular application in multiuser communication networks is reported in [55, Sections 15.4 and 15.5] where inner and outer bounds to the region of achievable source rate tuples are formulated directly in terms of $\boldsymbol{H}_N^{\mathsf{ent}}$ and its closure. Further applications include bounds on information rates of perfect secret-sharing schemes, expressible in terms of $\boldsymbol{H}_N^{\mathsf{ent}}$ and its approximation by selfadhesive polymatroids, and inference on conditional independences within variables of a random vector, see [40, Section 4].

The following theorem implies that the difference between the convex cone $cl(\boldsymbol{H}_N^{\mathsf{ent}})$ and its subset $\boldsymbol{H}_N^{\mathsf{ent}}$ is only on a boundary. By Lemmas 2 and 3 in Section II, $\boldsymbol{H}_N^{\mathsf{ent}}$ contains a polyhedral cone of the dimension $2^{|N|} - 1$, and thus has a nonempty interior in the topology of the linear space of normalized functions, which have the value $g(\emptyset)$ fixed to 0. This relative interior is denoted in the sequel by *ri*.

Theorem 1: $ri(cl(\boldsymbol{H}_N^{\mathsf{ent}})) \subseteq \boldsymbol{H}_N^{\mathsf{ent}}$

A proof is presented in Section II, not depending on the previously known fact that the set $cl(\boldsymbol{H}_N^{\mathsf{ent}})$ is convex.

The *convolution* $g * h$ of two polymatroids g, h with the same ground set N is defined by

$$g * h\ (I) = \min_{J\subseteq I} \left[\, g(J) + h(I \setminus J) \,\right], \qquad I \subseteq N\,.$$

It is a polymatroid whenever h is *modular*, $h(I) = \sum_{i\in I} h(i)$ for $I \subseteq N$ [30, Theorem 2.5].

Theorem 2: The cone $cl(\boldsymbol{H}_N^{\mathsf{ent}})$ is closed to the convolutions with modular polymatroids.

The proof of this theorem, presented in Section II, is based on the following technical result.

Theorem 3: Let a random variable ξ and a random vector $\eta = (\eta_\gamma)_{\gamma\in\Gamma}$ indexed by a finite set Γ range in finite sets. For i.i.d. copies $(\xi^1, \eta^1) \ldots (\xi^n, \eta^n)$ of the vector (ξ, η) let $\xi^{1.n}$ denote the vector $(\xi^1, \ldots, \xi^n)$ of n copies of ξ and $\eta_\Upsilon^{1.n}$ the vector $(\eta_\Upsilon^1, \ldots, \eta_\Upsilon^n)$ of n copies of $\eta_\Upsilon = (\eta_\gamma)_{\gamma\in\Upsilon}$, $\Upsilon \subseteq \Gamma$. Then, for $\alpha \geqslant 0$ there exists a sequence $(\phi_n)_{n\geqslant 1}$ of random variables such that ϕ_n is a function of $\xi^{1.n}$ and for all $\Upsilon \subseteq \Gamma$

$$\lim_{n\to\infty} \tfrac{1}{n}\, H(\phi_n, \eta_\Upsilon^{1.n}) = \min\left\{\alpha + H(\eta_\Upsilon), H(\xi, \eta_\Upsilon)\right\}.$$

Manuscript received February 6, 2006; revised June 7, 2006. This work was supported by Grant Agency of Academy of Sciences of the Czech Republic under the grants A1075104 and IAA100750603.

F. Matúš is with Institute of Information Theory and Automation, Academy of Sciences of the Czech Republic, Pod vodárenskou věží 4, 182 08 Prague, Czech Republic (e-mail: matus@utia.cas.cz).

A self-contained proof of Theorem 3 is presented in Section III. It is based on asymptotic equipartitions and Lemma 6, a technical improvement of [1, Lemma 3.1, p. 230] by Ahlswede and Csiszár, which has been known as a crucial building stone in Shannon secrecy. The equipartitions, including conditional ones, are elaborated in detail in the Appendix since they are defined in a slightly different way than known in literature and no reference to such an approach seems to be available.

Theorem 3 and convolutions are related to Slepian-Wolf theorem in the first two remarks of Section V.

If (M,h) is a polymatroid and a mapping $\varphi\colon N\to\mathcal{P}(M)$ is extended naturally to $\mathcal{P}(N)$ by $\varphi(I)=\cup_{i\in I}\varphi(i)$ for $I\subseteq N$, then $I\mapsto h(\varphi(I))$ is obviously the rank function of a polymatroid with the ground set N. When $\varphi(N)=M$ the latter polymatroid is called the *image* of the former under φ and is denoted by $(N,h\varphi)$. In addition, if the sets $\varphi(i)$, $i\in N$, are pairwise disjoint then the image under φ is referred to as a *factor*. It is a remarkable fact that each integer-valued polymatroid (N,g) is a factor of a matroid [22], [43], [46]. Such a factorization can be explicitly constructed as follows. Consider a set M of the cardinality $\sum_{i\in N} g(i)$ and any mapping $\varphi\colon N\to\mathcal{P}(M)$ such that $\varphi(i)$ has the cardinality $g(i)$, $i\in N$, and these sets are pairwise disjoint. Then, the *free expansion* of g by φ is defined by

$$K\mapsto \min_{I\subseteq N}\left[\,g(I)+|K\setminus\varphi(I)|\,\right],\qquad K\subseteq M\,.$$

It is a matroid on M that factors to g under φ [46, Proposition 1.3.9, p. 366]. The following assertion is proved in Section II by invoking Theorem 2 and expressing any free expansion as a convolution with a modular matroid.

Theorem 4: The class of integer-valued asymptotically entropic polymatroids is closed to the free expansions.

Theorem 4 is the main ingredient in proving that divisions by positive integers of the factors of asymptotically entropic matroids are dense in $cl(\boldsymbol{H}_N^{\mathsf{ent}})$, which is formulated more precisely as follows.

Theorem 5: For any asymptotically entropic polymatroid (N,h) there exists a sequence of positive integers t_n, a sequence of asymptotically entropic matroids (M_n,r_n) and a sequence of mappings $\varphi_n\colon N\to\mathcal{P}(M_n)$ each one with $\varphi_n(i)$, $i\in N$, pairwise disjoint and $\varphi_n(N)=M_n$ such that $\lim_{n\to\infty}\frac{1}{t_n}\,r_n\,\varphi_n=h$.

This result reduces the problem of description of the cones $cl(\boldsymbol{H}_N^{\mathsf{ent}})$ to the problem of description of the asymptotically entropic matroids. Another countable dense subset of $cl(\boldsymbol{H}_N^{\mathsf{ent}})$ was constructed by means of families of finite subgroups in [9] and is discussed in Remark 11 of Section IV.

Sections II and III are devoted to proofs, the latter entirely to that of Theorem 3 without relying on the former. Section IV discusses existing related literature, previous investigations of entropy functions, multiples of matroids that are entropic, asymptotically entropic matroids, and outlines connections to perfect and ideal secret-sharing schemes and to almost affine codes. In Subsection IV-F, relying on above theorems, special asymptotically entropic matroid and polymatroid are constructed that cannot be approximated by linear structures. Section V collects further remarks.

II. Proofs

This section contains proofs of all theorems but Theorem 3.

Lemma 1: The set $\boldsymbol{H}_N^{\mathsf{ent}}$ is closed to the sums.

Proof: Making two random vectors $(\xi_i)_{i\in N}$ and $(\eta_i)_{i\in N}$ independent, the sum of their entropy functions equals the entropy function of the vector $((\xi_i,\eta_i))_{i\in N}$. □

Corollary 1: The set $cl(\boldsymbol{H}_N^{\mathsf{ent}})$ is closed to the sums.

Let $J\subseteq N$, r_J denote the matroid given by

$$I\mapsto\min\{1,|I\cap J|\}\,,\qquad I\subseteq N\,,$$

and $\boldsymbol{H}_N^{\mathsf{imo}}$ the polyhedral cone spanned by these matroids; this notation is explained in Remark 9 of Section V.

Lemma 2: $\boldsymbol{H}_N^{\mathsf{imo}}\subseteq\boldsymbol{H}_N^{\mathsf{ent}}$

Proof: The nonnegative multiples of r_J, $J\subseteq N$, are obviously entropic and their sums are entropic by Lemma 1. □

The following assertion was mentioned in the proof of [39, Lemma 2], dealing with the Boolean polymatroids, which are the linear combinations of the matroids r_J with nonnegative integer coefficients.

Lemma 3: The family $\{r_J\colon\emptyset\neq J\subseteq N\}$ is a base of the space of normalized functions.

Proof: Let $\mathbb{A}$ be the linear transform on $\mathbb{R}^{\mathcal{P}(N)}$ given by

$$\mathbb{A}g(K)=\sum_{I\subseteq K}(-1)^{|K-I|}\left[g(N)-g(N-I)\right],\qquad K\subseteq N\,.$$

For $J\neq\emptyset$ an elementary computation shows that $\mathbb{A}r_J(K)$ is equal to 1 for $K=J$ and to 0 otherwise. Hence, the family maps to a family of $\ell=2^{|N|}-1$ linearly independent normalized functions, and therefore itself consists of ℓ linearly independent functions. □

Proof of Theorem 1: By Lemma 3, if $\epsilon>0$ then the set B_ϵ of polymatroids $\sum\alpha_J\,r_J$ with $0<\alpha_J<\epsilon$, $\emptyset\neq J\subseteq N$, is open in the space of normalized functions and the shifts of these sets provide a base for the topology of this space. Hence, if g belongs to the relative interior of $cl(\boldsymbol{H}_N^{\mathsf{ent}})$ then it belongs to such a shift contained in the relative interior. It follows that $g-B_\epsilon$ is a subset of the relative interior for some small $\epsilon>0$. Since $g-B_\epsilon$ is a relatively open subset of $cl(\boldsymbol{H}_N^{\mathsf{ent}})$ it contains an entropic polymatroid h. This implies that g belongs to $h+\boldsymbol{H}_N^{\mathsf{imo}}$, and thus g is entropic, by Lemmas 1 and 2. □

The following lemma presents a new property of the set $\boldsymbol{H}_N^{\mathsf{ent}}$. It is not used in this paper in its full strength only through a corollary that has been known earlier.

Lemma 4: $\alpha\boldsymbol{H}_N^{\mathsf{ent}}+\beta r_N\subseteq\boldsymbol{H}_N^{\mathsf{ent}}$ for $\alpha,\beta>0$.

Proof: Let g be the entropy function of a random vector $(\xi_i)_{i\in N}$ defined on a finite set $\varOmega$ endowed with a probability measure (pm) P. Extend $\varOmega$ by one element 0, endow $\varOmega\cup\{0\}$ with the pm P_γ, $0<\gamma<1$, given by $P_\gamma(0)=1-\gamma$ and $P_\gamma(\omega)=\gamma P(\omega)$, $\omega\in\varOmega$, and extend ξ_i to the random variable η_i on $\varOmega\cup\{0\}$ such that $\eta_i(0)$ is different from all values of ξ_i, $i\in N$. For $\emptyset\neq I\subseteq N$ the Shannon entropy of η_I is equal to $\gamma g(I)+c(\gamma)$ where $c(\gamma)=-\gamma\ln\gamma-(1-\gamma)\ln(1-\gamma)$. Thus, $\gamma g+c(\gamma)r_N$ is an entropic polymatroid. Since ng is entropic by Lemma 1, $\alpha g+c(\frac{\alpha}{n})r_N$ is entropic whenever $\alpha<n$. Taking n sufficiently large to have also $c(\frac{\alpha}{n})<\beta$, it follows that $\alpha g+\beta r_N$ is entropic, by Lemmas 1 and 2. □

Corollary 2: The set $cl(\boldsymbol{H}_N^{\mathsf{ent}})$ is closed to the nonnegative multiples.

Remark 1: Corollaries 1 and 2 are equivalent to [57, Theorem 1], asserting that $cl(\boldsymbol{H}_N^{\mathrm{ent}})$ is a closed convex cone. Actually, an idea of the proof of this result is used in the proof of Lemma 4.

Proof of Theorem 2: By continuity of the convolution, it suffices to prove that $g*h$ is asymptotically entropic whenever g is entropic and h modular. First, this is proved assuming that h satisfies $h(i)=\alpha$ and $h(j)\geqslant g(j)$, $j\in N\setminus i$, where $i\in N$ and $\alpha\geqslant 0$. In this case $g*h(I)$ is equal to the minimum of $\alpha+g(I\setminus i)$ and $g(I)$ when $I\subseteq N$ contains i and to $g(I)$ otherwise. If g is the entropy function of a random vector $(\zeta_j)_{j\in N}$ write $\xi=\zeta_i$, $\Gamma=N\setminus i$ and $\eta_\gamma=\zeta_\gamma$ for $\gamma\in\Gamma$. Applying Theorem 3 to α, ξ and $(\eta_\gamma)_{\gamma\in\Gamma}$, a function ϕ_n of $\zeta_i^{1.n}$ exists such that the entropy functions g_n of the random vectors $(\phi_n,\zeta_\Gamma^{1.n})$ satisfy $\frac{1}{n}\,g_n(I)\to g*h\,(I)$ for all $I\subseteq N$ containing i. Obviously, $\frac{1}{n}\,g_n(I)=g*h\,(I)=g(I)$, otherwise. By Corollary 2, the sequence $\frac{1}{n}\,g_n$ is contained in $cl(\boldsymbol{H}_N^{\mathrm{ent}})$, and thus its limit $g*h$ is asymptotically entropic.

Recall that convolution is an associative operation. If h is modular, $\beta\geqslant\max_{i\in N}\ h(i)$ and the elements of N are ordered as $i_1,\dots,i_t$ then $h=h_1*\ldots*h_t$ where h_s for $1\leqslant s\leqslant t$ is modular, $h_s(i_s)=h(i_s)$ and $h_s(j)=\beta$, $j\in N\setminus i_s$. If also $\beta\geqslant\max_{i\in N}\ g(i)$ then the first part of the proof applies t times to conclude that the convolutions $g*h_1$, $g*h_1*h_2$, ..., $g*h_1*\ldots*h_t=g*h$ are asymptotically entropic. □

Proof of Theorem 4: If (N,g) is a polymatroid and a mapping $\varphi\colon N\to\mathcal{P}(M)$ has pairwise disjoint $\varphi(i)$, $i\in N$, that cover M then g^φ given by

$$g^\varphi(K)=g(\{i\in N\colon \varphi(i)\cap K\neq\emptyset\})\,,\qquad K\subseteq M\,,$$

is a polymatroid with the ground set M. Denoting by $|\cdot|$ the cardinality function on $\mathcal{P}(M)$, it is not difficult to see that

$$\begin{aligned} g^\varphi*|\cdot|\,(K)&=\min_{L\subseteq K}\,[\,g(\{i\in N\colon\varphi(i)\cap L\neq\emptyset\})+|K\setminus L|\,]\\ &=\min_{I\subseteq N}\,[\,g(I)+|K\setminus\varphi(I)|\,]\,,\qquad K\subseteq M\,.\end{aligned}$$

It follows that if g is an integer-valued polymatroid then the free expansion of g by φ equals $g^\varphi*|\cdot|$. By Theorem 2, it suffices to show that g^φ is asymptotically entropic whenever g has this property. If g equals even the entropy function of a random vector $(\xi_i)_{i\in N}$ then g^φ equals the entropy function of $(\eta_k)_{k\in M}$ where $\eta_k=\xi_i$ for $k\in\varphi(i)$. This and continuity of $g\mapsto g^\varphi$ imply that if g is the limit of entropic f_n then g^φ is the limit of entropic f_n^φ. □

Remark 2: For a sequential approach to free expansions that is based on principal extensions see the proof of [30, Theorem 2.9, p. 246].

Proof of Theorem 5: The set of normalized rational-valued functions on $\mathcal{P}(N)$ is obviously dense in the space of normalized functions. Then, by an elementary topological argument, the rational-valued functions from $ri(cl(\boldsymbol{H}_N^{\mathrm{ent}}))$ are dense in this set, and thus also in its closure. This closure equals $cl(\boldsymbol{H}_N^{\mathrm{ent}})$ by convexity of this set [57, Theorem 1] and [49, Theorem 6.3]. It follows that the rational-valued functions from $ri(cl(\boldsymbol{H}_N^{\mathrm{ent}}))$ are dense in $cl(\boldsymbol{H}_N^{\mathrm{ent}})$. This and Theorem 1 imply that each function g in $cl(\boldsymbol{H}_N^{\mathrm{ent}})$ is the limit of a sequence of entropic rational-valued polymatroids f_n. Writing $f_n=\frac{1}{t_n}\,g_n$ with a positive integer t_n and integer-valued polymatroid g_n, the assertion follows from Theorem 4 applied to the polymatroids g_n, entropic by Lemma 1. □

III. Proof of Theorem 3

This section is devoted to a self-contained proof of Theorem 3. The proofs of Lemmas 7–10 and Corollary 3 are deferred to the Appendix. These auxiliary assertions are minor variations on inequalities involving probabilities of typical sequences and cardinalities of sets of such sequences. The notion of typicality considered here does not seem to be among those known in the literature [12], [55].

In this section and Appendix, the letters n and k are reserved for positive integers, and δ and ε for nonnegative real numbers. The following inequality is needed in the sequel.

Lemma 5: If real random variables $\zeta_1,\dots,\zeta_n$ are independent, bounded and centered then

$$Pr\Big(\textstyle\sum_{j=1}^n\zeta_j>\varepsilon\Big)\leqslant\exp\Big[-\frac{\varepsilon}{2t}\,\ln\Big(1+\frac{\varepsilon\,t}{s}\Big)\Big]$$

where $t>0$ dominates each variable $|\zeta_j|$ a.s. and $s>0$ dominates the sum of variances of ζ_j.

Proof: This is a consequence of [52, (5.2), p. 287] with weights equal to one, which is a one-sided version of [52, Theorem 3]. □

Remark 3: The assertion of Lemma 5 is weaker than Bennett inequality [4, (8b), p. 39], bounding the probability from above by $\exp[-\frac{s}{t^2}\,g(\frac{\varepsilon\,t}{s})]$ where $g(u)=(1+u)\ln(1+u)-u$, upon mentioning that $g(u)\geqslant\frac{u}{2}\ln(1+u)$ for $u\geqslant 0$, see also [52, p. 287].

In the sequel, the set $\{1,\dots,k\}$ is denoted by $\widehat{k}$. A k-coloring of a set is any mapping of the set into $\widehat{k}$.

Lemma 6: Let $\mathcal{Q}$ be a finite nonempty set of pm's on a finite set X, $|\mathcal{Q}|$ the cardinality of $\mathcal{Q}$ and $\|\mathcal{Q}\|_\infty=\max_{Q\in\mathcal{Q}}\|Q\|_\infty$ where $\|Q\|_\infty=\max_{x\in X}\ Q(x)$. For $k\geqslant 1$ and $\varepsilon\geqslant 0$ the proportion of those k-colorings f of X that violate

$$Q(f^{-1}(j))\leqslant\tfrac{1+\varepsilon}{k}$$

for some $Q\in\mathcal{Q}$ and $j\in\widehat{k}$ is at most

$$k\,|\mathcal{Q}|\,\exp\Big[-\frac{\varepsilon\ln(1+\varepsilon)}{2k\,\|\mathcal{Q}\|_\infty}\Big]\,.$$

In a typical application of this lemma, the above bound is close to zero so that a big majority of the k-colorings satisfies the above inequality for all $Q\in\mathcal{Q}$ and $j\in\widehat{k}$.

Proof: Let η_x, $x\in X$, be independent random variables, each one distributed uniformly on $\widehat{k}$. For $Q\in\mathcal{Q}$ and $j\in\widehat{k}$ let ζ_x be equal to $(k-1)Q(x)$ if $\eta_x=j$ and to $-Q(x)$ otherwise, $x\in X$. The random variables ζ_x, $x\in X$, satisfy the hypotheses of Lemma 5 with $t=k\|\mathcal{Q}\|_\infty>0$ and $s=t$, dominating the sum of variances $(k-1)\sum_{x\in X}Q(x)^2$, and hence

$$Pr(\textstyle\sum_{x\in X}\zeta_x>\varepsilon)\leqslant\exp\Big[-\dfrac{\varepsilon\ln(1+\varepsilon)}{2k\,\|\mathcal{Q}\|_\infty}\Big]\,.$$

This probability multiplied by the number of all k-colorings of X is equal to the number of k-colorings f that satisfy

$$\textstyle\sum_{x\in f^{-1}(j)}(k-1)Q(x)-\sum_{x\in X\setminus f^{-1}(j)}Q(x)>\varepsilon\,.$$

Therefore, for any $Q \in \mathcal{Q}$ and $j \in \widehat{k}$ the proportion of those k-colorings f of X that violate $Q(f^{-1}(j)) \leqslant \frac{1+\varepsilon}{k}$ is bounded above by the above exponential expression. Since this bound does not depend on Q and j the assertion follows. □

Remark 4: Lemma 6 is inspired by [1, Lemma 3.1, p. 230] where $\log(2N)$ must be replaced by $\log(2Nk)$, as noted in the remark following [13, Lemma B.1, p. 3059]. With this correction, [1, Lemma 3.1] asserts existence of a special k-coloring under some assumptions that express the fact that an upper bound on a proportion of k-colorings is less than one. Lemma 6 can help to weaken that assumptions but details are omitted here.

In the following two lemmas and corollary, P is a pm on a finite set A, $\mathsf{H}(P)$ its Shannon entropy based on the natural logarithm, $\mathsf{s}(P) = \{a \in A\colon P(a) > 0\}$ its support and $\bar{P}$ the minimum of $P(a)$ over $a \in \mathsf{s}(P)$. For a finite nonempty set N and $\delta \geqslant 0$ let $T^N_{P,\delta}$ be the set of $x = (x_i)_{i\in N}$ in A^N with the cardinality of $x^{-1}(a) = \{i \in N\colon x_i = a\}$ between $|N|P(a)[1 \mp \delta]$ for all $a \in A$. Note that if $x \in T^N_{P,\delta}$ then $\mathsf{s}(x)$ defined by $\{a \in A\colon x^{-1}(a) \neq \emptyset\}$ is contained in $\mathsf{s}(P)$, thus $T^N_{P,\delta} \subseteq \mathsf{s}(P)^N$. Frequently, $N = \widehat{n}$ and n is written in indices instead of N.

Lemma 7: For $x \in T^n_{P,\delta}$, $P^n(x)$ is between $e^{-n\mathsf{H}(P)[1\pm\delta]}$.

Corollary 3: $|T^n_{P,\delta}| \leqslant e^{n\mathsf{H}(P)[1+\delta]}$

Lemma 8: $P^n(T^n_{P,\delta}) \geqslant 1 - 2|A|e^{-2n\delta^2\bar{P}^2}$

From now on until the last proof of this section, let P be a pm on a finite set $A \times B$, P_B the marginal of P on B, $P_B(b) = \sum_{a\in A} P(a,b)$, and if $b \in \mathsf{s}(P_B)$ then let $P_{|b}$ be the pm on A given by $P_{|b}(a) = P(a,b)/P_B(b)$, $a \in A$. For $n \geqslant 1$ and $\delta \geqslant 0$ let

$$T^n_{P,\delta|y} = \Bigg(\prod_{b\in\mathsf{s}(y)} T^{y^{-1}(b)}_{P_{|b},\delta}\Bigg) \times \{y\}\,, \qquad y \in T^n_{P_B,\delta}\,.$$

Here, $y^{-1}(b) = \{i \in \widehat{n}\colon y_i = b\}$ for y in the form $(y_i)_{i\in\widehat{n}}$ and $\mathsf{s}(y) = \{b \in B\colon y^{-1}(b) \neq \emptyset\}$. Let $T^n_{P,\delta|B}$ denote the union of the subsets $T^n_{P,\delta|y}$ of $A^n \times B^n$ over $y \in T^n_{P_B,\delta}$ and $\mathsf{H}(P|P_B)$ the conditional entropy $\mathsf{H}(P) - \mathsf{H}(P_B)$.

Lemma 9: If $y \in T^n_{P_B,\delta}$ and $(x,y) \in T^n_{P,\delta|y}$ then

$$P^n(x,y) \leqslant e^{-n\mathsf{H}(P|P_B)[1-2\delta]} P^n_B(y)\,.$$

Lemma 10: If $y \in T^n_{P_B,\delta}$ then

$$P^n(T^n_{P,\delta|y}) \geqslant P^n_B(y)\left[1 - 2\,|A\times B|\, e^{-2n\delta^2[1-\delta]\bar{P}^2}\right].$$

Corollary 4:

$$P^n(T^n_{P,\delta|B}) \geqslant P^n_B(T^n_{P_B,\delta})\left[1 - 2\,|A\times B|\, e^{-2n\delta^2[1-\delta]\bar{P}^2}\right]$$

Lemma 11: For $n \geqslant 1$, $k \geqslant 1$, $\delta \geqslant 0$ and $\varepsilon \geqslant 0$, the proportion of those k-colorings f of A^n that violate

$$P^n\big((f^{-1}(j)\times\{y\}) \cap T^n_{P,\delta|B}\big) \leqslant \tfrac{1+\varepsilon}{k}\, P^n_B(y) \qquad (1)$$

for some $j \in \widehat{k}$ and $y \in T^n_{P_B,\delta}$ is at most

$$k \cdot e^{n\mathsf{H}(P_B)[1+\delta]} \cdot \exp\Big[- \tfrac{\varepsilon\ln(1+\varepsilon)}{2k} \cdot e^{n\mathsf{H}(P|P_B)[1-2\delta]} \cdot \min_{y\in T^n_{P_B,\delta}} \frac{P^n(T^n_{P,\delta|y})}{P^n_B(y)} \Big].$$

The proportion and its upper bound are denoted in the sequel by $\mathit{\Pi}^n_{P,\delta|B}(k,\varepsilon)$ and $\mathit{\Lambda}^n_{P,\delta|B}(k,\varepsilon)$.

Proof: If $P^n(T^n_{P,\delta|y}) = 0$ then (1) holds, having zero on the left. Thus, if $P^n(T^n_{P,\delta|B}) = 0$ then the proportion is zero and the assertion is trivial. Assuming this probability positive, let $X = A^n$ and $\mathcal{Q}$ be the nonempty set of the pm's Q_y on X indexed by $y \in T^n_{P_B,\delta}$ satisfying $P^n(T^n_{P,\delta|y}) > 0$, given by

$$Q_y(x) = \frac{P^n(x,y)}{P^n(T^n_{P,\delta|y})}$$

if $(x,y) \in T^n_{P,\delta|y}$ and $Q_y(x) = 0$ otherwise. If a k-coloring f of A^n violates (1) for some $j \in \widehat{k}$ and $y \in T^n_{P_B,\delta}$ then $P^n(T^n_{P,\delta|y})$ is positive and

$$\begin{aligned} Q_y((f^{-1}(j)) &= \frac{P^n((f^{-1}(j)\times\{y\})\cap T^n_{P,\delta|B})}{P^n(T^n_{P,\delta|y})} \\ &> \frac{1+\varepsilon}{k}\,\frac{P^n_B(y)}{P^n(T^n_{P,\delta|y})} \geqslant \frac{1+\varepsilon}{k}\,. \end{aligned}$$

It follows by Lemma 6 that

$$\mathit{\Pi}^n_{P,\delta|B}(k,\varepsilon) \leqslant k\,|\mathcal{Q}|\,\exp\Big[- \frac{\varepsilon\ln(1+\varepsilon)}{2k\,\|\mathcal{Q}\|_\infty}\Big]\,.$$

The assertion follows from $|\mathcal{Q}| \leqslant |T^n_{P_B,\delta}| \leqslant e^{n\mathsf{H}(P_B)[1+\delta]}$, obtained by Corollary 3, and

$$\|\mathcal{Q}\|_\infty \leqslant e^{-n\mathsf{H}(P|P_B)[1-2\delta]} \cdot \max_{y\in T^n_{P_B,\delta}} \frac{P^n_B(y)}{P^n(T^n_{P,\delta|y})}$$

by Lemma 9. □

The following limiting scheme describes a superexponential convergence of $\mathit{\Pi}^n_{P,\delta|B}(k,\varepsilon)$ to zero when n goes to infinity. In one of the cases, surprisingly, ε can go to ∞ so that Lemmas 6 and 11 are effective also for large ε, a feature not considered previously.

Lemma 12: For $\alpha \geqslant 0$ and $\frac{1}{2} > r > 0$, if n goes to infinity, $k = \lceil e^{n\alpha}\rceil$, $\delta = n^{-r}$ and

$$\varepsilon = \begin{cases} \sqrt{ne^{n[\alpha - \mathsf{H}(P|P_B)[1-4n^{-r}]]}}\,, & \alpha \leqslant \mathsf{H}(P|P_B)\,, \\ ke^{-n\mathsf{H}(P|P_B)[1-3n^{-r}]} - 1\,, & \text{otherwise,} \end{cases}$$

then $\frac{1}{n}\ln \mathit{\Pi}^n_{P,\delta|B}(k,\varepsilon) \to -\infty$.

Proof: If $\mathsf{H}(P|P_B) = 0$ then $\frac{\varepsilon+1}{k} \geqslant 1$, and thus the proportion $\mathit{\Pi}^n_{P,\delta|B}(k,\varepsilon)$ equals 0 for all $n \geqslant 1$. Otherwise, by Lemma 11, it suffices to prove that $\frac{1}{n}\ln \mathit{\Lambda}^n_{P,\delta|B}(k,\varepsilon)$ goes to $-\infty$. This means to examine the limit behaviour of

$$N - \tfrac{1}{2}\cdot\frac{\ln(1+\varepsilon)}{\varepsilon}\cdot\frac{\varepsilon^2}{nk}\, e^{n\mathsf{H}(P|P_B)[1-2n^{-r}]}\cdot M \qquad (2)$$

where $N = \frac{\ln k}{n} + \mathsf{H}(P_B)[1+n^{-r}]$ converges to $\alpha + \mathsf{H}(P_B)$ and M equals the minimum occurring in $\mathit{\Lambda}^n_{P,\delta|B}(k,\varepsilon)$. Since the minimization is eventually over a nonempty set by Lemma 8, implying $P^n_B(T^n_{P_B,\delta}) \to 1$, it follows from Lemma 10 that M converges to 1.

In the case $\alpha \leqslant \mathsf{H}(P|P_B)$,

$$\frac{\varepsilon^2}{nk}\cdot e^{n\mathsf{H}(P|P_B)[1-2n^{-r}]} = \frac{e^{n\alpha}}{k}\cdot e^{2\mathsf{H}(P|P_B)n^{1-r}}$$

where $\frac{e^{n\alpha}}{k} \to 1$ and, in turn, (2) converges to

$$\alpha + \mathsf{H}(P_B) - \tfrac{1}{2}\lim_{n\to\infty}\frac{\ln(1+\varepsilon)}{\varepsilon}\cdot e^{2\mathsf{H}(P|P_B)n^{1-r}}\,.$$

If $\alpha < H(P|P_B)$ then $\varepsilon \to 0$, and (2) converges to $-\infty$. If α equals $H(P|P_B)$, which is positive by assumption, then substituting $\varepsilon = \sqrt{n}e^{2H(P|P_B)n^{1-r}}$ above, exponentials cancel, and (2) converges to $-\infty$, using that $r < \frac{1}{2}$.

In the case $\alpha > H(P|P_B)$, rewrite (2) as

$$N - \tfrac{1}{2} \cdot \tfrac{\ln(1+\varepsilon)}{n} \cdot \tfrac{\varepsilon}{k}\, e^{nH(P|P_B)[1-2n^{-r}]} \cdot M \qquad (3)$$

where

$$\tfrac{\ln(1+\varepsilon)}{n} = \tfrac{\ln k}{n} - H(P|P_B)[1 - 3n^{-r}]$$

converges to $\alpha - H(P|P_B)$, and

$$\tfrac{\varepsilon}{k}\, e^{nH(P|P_B)[1-2n^{-r}]} = \tfrac{\varepsilon}{\varepsilon+1} \cdot e^{H(P|P_B)n^{1-r}}\,.$$

Since ε goes to infinity and $H(P|P_B) > 0$ the limit of (3) is again $-\infty$. $\square$

Lemma 13: If a k-coloring f of A^n satisfies (1) for $j \in \widehat{k}$ and $y \in T^n_{P_B,\delta}$ then the entropy of P^n restricted to the algebra generated by the sets $f^{-1}(j)\times\{y\}$, $j \in \widehat{k}$, $y \in B^n$, is between

$$-\ln 2 + P^n(T^n_{P,\delta|B})\Big[\ln \tfrac{k}{1+\varepsilon} + n\, H(P_B)\,[1-\delta]\Big]$$

and $\min\{\ln k + nH(P_B), nH(P)\}$.

The above entropy is denoted by $H(P^n|f)$.

Proof: Let $B_{j,y}$ be equal to $(f^{-1}(j)\times\{y\})\cap T^n_{P,\delta|B}$ and $C_{j,y}$ to $(f^{-1}(j)\times\{y\})\setminus T^n_{P,\delta|B}$. The entropy of P^n restricted to the algebra generated by $T^n_{P,\delta|B}$ and its complement is at most $\ln 2$, and hence $\ln 2 + H(P^n|f)$ is at least

$$-\sum_{j\in\widehat{k}\,,\, y\in B^n} P^n(B_{j,y})\,\ln P^n(B_{j,y}) + P^n(C_{j,y})\,\ln P^n(C_{j,y})\,.$$

The inequality holds also when the terms containing $C_{j,y}$'s are omitted which entails restriction of the summation over y to $T^n_{P_B,\delta}$. By the assumption on f, $\ln P^n(B_{j,y})$ can be bounded above by (1), and thus $H(P^n|f)$ is at least

$$-\ln 2 - \sum_{j\in\widehat{k}\,,\, y\in T^n_{P_B,\delta}} P^n(B_{j,y})\,\Big[\,\ln \tfrac{1+\varepsilon}{k} + \ln P^n_B(y)\Big]\,.$$

Here, $\ln P^n_B(y)$ is at most $-nH(P_B)[1-\delta]$ by Lemma 7, and hence the lower bound holds. The upper bound is trivial. $\square$

Corollary 5: If α, r, n, k, δ and ε are as in Lemma 12 and f_n is a k-coloring of A^n that satisfies (1) for all $j \in \widehat{k}$ and $y \in T^n_{P_B,\delta}$ eventually then

$$\lim_{n\to\infty} \tfrac{1}{n}\, H(P^n|f_n) = \min\{\alpha + H(P_B), H(P)\}\,.$$

Proof: This follows from Lemma 13, using that $\frac{1}{n}\ln\frac{k}{1+\varepsilon}$ converges to $\min\{\alpha, H(P|P_B)\}$ and $P^n(T^n_{P,\delta|B}) \to 1$, a consequence of Corollary 4 and $P^n_B(T^n_{P_B,\delta}) \to 1$. $\square$

Proof of Theorem 3: Suppose ξ ranges in a finite set A and η in a finite set $\prod_{\gamma\in\Gamma} B_\gamma$ so that the subvectors η_Υ range in the subproduct $B_\Upsilon = \prod_{\gamma\in\Upsilon} B_\gamma$. Let ${}^{\Upsilon}\!P$ be the distribution of (ξ, η_Υ) and ${}^{\Upsilon}Q$ the distribution of η_Υ. For each $\Upsilon \subseteq \Gamma$, Lemma 12 with $\delta = n^{-r}$, $k = \lceil e^{n\alpha}\rceil$ and ε_Υ depending on Υ (through $H({}^{\Upsilon}\!P|{}^{\Upsilon}Q) = H(\xi|\eta_\Upsilon)$) applies to the pm ${}^{\Upsilon}\!P$ on $A \times B_\Upsilon$ and implies that the proportion $\Pi^n_{{}^{\Upsilon}\!P,\delta|B_\gamma}(k, \varepsilon_\gamma)$ of k-colorings f_n of A^n that satisfy

$${}^{\Upsilon}\!P^n((f_n^{-1}(j)\times\{y_\Upsilon\})\cap T^n_{{}^{\Upsilon}\!P,\delta|B_\Upsilon}) \leqslant \tfrac{1+\varepsilon_\Upsilon}{k} \cdot {}^{\Upsilon}Q^n(y_\Upsilon)\,,$$
$$j \in \widehat{k}\,,\; y_\Upsilon \in T^n_{{}^{\Upsilon}Q,\delta}\,,$$

goes to one when $n \to \infty$. Therefore, a sequence f_n of $\lceil e^{n\alpha}\rceil$-colorings of A^n exists such that the above inequalities hold for all $\Upsilon \subseteq \Gamma$ and n sufficiently large. Corollary 5 implies that $\frac{1}{n}H({}^{\Upsilon}\!P^n|f_n)$ converges to $\min\{\alpha + H({}^{\Upsilon}Q), H({}^{\Upsilon}\!P)\}$, $\Upsilon \subseteq \Gamma$. Writing $\phi_n = f_n(\xi^{1.n})$ the assertion of Theorem 3 holds since obviously $H({}^{\Upsilon}\!P^n|f_n) = H(\phi_n, \eta^{1.n}_\Upsilon)$, $H({}^{\Upsilon}Q) = H(\eta_\Upsilon)$ and $H({}^{\Upsilon}\!P) = H(\xi, \eta_\Upsilon)$. $\square$

IV. Discussion

A. Previous results

Multivariate Shannon's information measures and their structural properties have been investigated by many researchers since the 1950's, for reviews see [12], [55]. Entropy functions were interpreted as polymatroids in [16], [17], where convolutions are termed reductions. This implies the containment $\boldsymbol{H}^{\mathsf{ent}}_N \subseteq \boldsymbol{H}_N$, an approximation of the sophisticated set $\boldsymbol{H}^{\mathsf{ent}}_N$ by the polyhedral cone $\boldsymbol{H}_N$. For results on the structure of this cone see [47], [30], [19], [34].

Necessary conditions for a polymatroid to be entropic result from information-theoretic inequalities. A real function Φ on $\mathbb{R}^{\mathcal{P}(N)}$ generates an *information inequality* if $\Phi(g) \geqslant 0$ is valid for any entropic polymatroid g. If the nonnegativity holds even for all polymatroids then the inequality is of *Shannon type*, and if it holds only for the entropic polymatroids g satisfying additional constraints then the inequality is *conditional*, following [56], [55], [58].

A linear information inequality amounts to nonpositivity of the scalar product $\sum_{I\subseteq N} c_I \cdot g(I)$ where $(c_I)_{I\subseteq N} = c$ is a point of $\mathbb{R}^{\mathcal{P}(N)}$. Ignoring the coordinate indexed by $\emptyset$, the linear information inequalities of Shannon type, parameterized by c, are in a one-to-one correspondence with the points of the polar cone $(\boldsymbol{H}_N)^\circ$ of $\boldsymbol{H}_N$, for this notion see [49, Section 14]. Similarly, $(\boldsymbol{H}^{\mathsf{ent}}_N)^\circ$, which equals $(cl(\boldsymbol{H}^{\mathsf{ent}}_N))^\circ$, parameterizes the set of all linear information inequalities.

First unconditional linear inequalities of the non-Shannon type were found in [59, Theorems 3 and 5], in particular

$$\begin{aligned}&3\big[g(ik) + g(il) + g(kl)\big] + g(jk) + g(jl)\\ &\quad\geqslant g(i) + 2\big[g(k) + g(l)\big] + g(ij) + 4g(ikl) + g(jkl) \qquad (4)\end{aligned}$$

holds for any asymptotically entropic polymatroid (N, g) where i, j, k, l are different singletons of N and the signs for union are omitted. Further generalizations of these inequalities appeared in [31], [58]. In [40], [42], the notion of *adhesivity* of polymatroids was introduced as a special type of amalgamation. A class of polymatroids with adhesive pairs of restrictions and a class of selfadhesive polymatroids were introduced and investigated, both containing the asymptotically entropic polymatroids. Known unconditional information inequalities were explained as consequences of these containments and a new one was found in [40], discussing also two applications in optimization problems involving entropy functions. The selfadhesive polymatroids with a four-element ground set were proved to be described exactly by (4), see [42]. Very recently new unconditional inequalities appeared in [15].

For conditional non-Shannon type inequalities see [57], [37], [41]. The tightness conditions in the known non-Shannon type information inequalities remain unclear, with exceptions of [29] working with Gaussian variables and [41]. Linear information inequalities are closely related to inequalities involving Kolmogorov complexities [20].

B. Entropic multiples of a matroid

To discuss which multiple of a matroid is entropic it is convenient to rule out two cases. First, nonnegative multiples of any matroid of the rank at most one, $r(N) \leqslant 1$, are entropic by Lemma 2. Second, the discussion reduces to connected matroids. Recall that a polymatroid (N, g) is not connected if N partitions into I and J such that $g(N) = g(I) + g(J)$, in which case g is the direct sum of its restrictions to $\mathcal{P}(I)$ and $\mathcal{P}(J)$, $g(K) = g(I \cap K) + g(J \cap K)$ for $K \subseteq N$. If this happens then it is easy to see that g is (asymptotically) entropic if and only if the two restrictions are (asymptotically) entropic.

If (N, r) is a connected matroid with $r(N) \geqslant 2$ and a multiple tr with $t > 0$ equals the entropy function of a random vector $\xi = (\xi_i)_{i \in N}$ then a unique integer $d \geqslant 2$ exists such that ξ_I takes $d^{r(I)}$ values, each with the probability $d^{-r(I)}$, for all $I \subseteq N$ [33, Theorem]. Thus, $t = \ln d$ and only such multiples of the matroid can be entropic. It follows that the vector ξ can sit on a set of cardinality $d^{r(N)}$ such that each subvector ξ_I generates an algebra of subsets of this set with $d^{r(I)}$ atoms of the same size. In other words, the problem whether $\ln d \cdot r$ is entropic reduces to existence of a vector $(\hat{\xi}_i)_{i \in N}$ of partitions of a $d^{r(N)}$-element set such that each meet-partition of $(\hat{\xi}_i)_{i \in I}$ consists of $d^{r(I)}$ blocks of the same size, for all $I \subseteq N$. In the language of [38], this means that the matroid is *partition representable* of degree d. It is not difficult to see that matroid is partition representable if and only if some of its positive multiples is entropic. Surprisingly, the problem of description of the partition representations of a matroid has not merely the combinatorial character of existence of a configuration of partitions but can be equivalently reformulated in the algebraic language of generalized quasigroup equations [38, Proposition 2.1].

Remark 5: Given a set Q of cardinality $d \geqslant 2$, a subset Ω of Q^N is an *almost affine code* [51] if the cardinality of the projection of Ω to Q^I is an integer power of d for all $I \subseteq N$. Then, a unique matroid r exists such that the power equals $d^{r(I)}$. Endowing Q^N with the pm that is concentrated and uniform on an almost affine code Ω, the coordinate projections ξ_i of Q^N to Q^i, $i \in N$, give rise to a random vector with the entropy function $\ln d \cdot r$. This assertion can be reversed, thus a subset Ω of Q^N with the above property is an almost affine code, provided $r(N) \geqslant 2$ and the matroid is connected.

C. Asymptotically entropic matroids

Theorem 5 provides a motivation to investigate the asymptotically entropic matroids, a class of matroids that seems to have been not mentioned in literature. A comparison with the classical class of linear matroids [54], [48] obtains by Remark 10 in Section V: any matroid that is linear, or has a positive multiple that is linear, has also a positive multiple that is entropic, and hence the matroid is asymptotically entropic by Corollary 2.

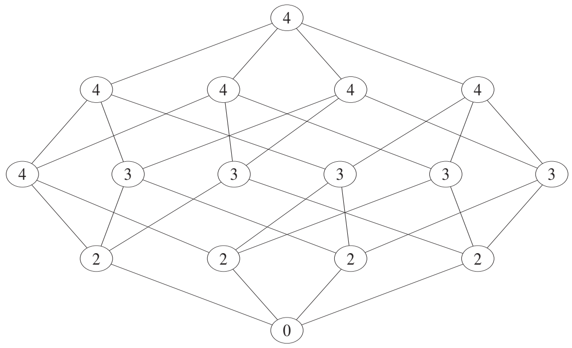

Fig. 1. A factor of Vamos matroid is not asymptotically entropic.

Not all matroids are asymptotically entropic. Vamos matroid, the well known example of a nonlinear matroid, factors to the polymatroid g from Fig. 1 that is not asymptotically entropic because it violates (4) with $g(ij) = 4$. Since factors of (asymptotically) entropic polymatroids are obviously (asymptotically) entropic it follows that Vamos matroid is not asymptotically entropic.

An asymptotically entropic matroid need not have a positive multiple that is entropic. In fact, Fano and non-Fano matroids are linear, however, always over the fields of different characteristic [54], [48], whence their direct sum is not linear. The sum is, however, asymptotically entropic because the two matroids have multiples that are entropic by Remark 10. At the same time, no positive multiple of the sum is entropic because the role of d, the degree of a partition representation, is played for Fano matroid only by powers of two and for non-Fano matroid only by odd numbers, see the proof of [38, Proposition 4.1].

D. Perfect secret sharing

Let N be a finite set with a distinguished element $\mathit{0}$ such that the cardinality of $N \setminus \mathit{0}$ is $n \geqslant 1$, and $\mathcal{A} \subseteq \mathcal{P}(N \setminus \mathit{0})$ be an *access structure* that is a filter, $I \in \mathcal{A}$ and $I \subseteq J \subseteq N \setminus \mathit{0}$ imply $J \in \mathcal{A}$, and has each $i \in N \setminus \mathit{0}$ contained in some inclusion-minimal set $I \in \mathcal{A}$. The access structure induces the following linear constraints on the polymatroids g from $\boldsymbol{H}_N$

$$\begin{aligned} g(\mathit{0} \cup I) &= g(I)\,, && I \in \mathcal{A}\,, \\ g(\mathit{0} \cup I) &= g(\mathit{0}) + g(I)\,, && I \subseteq N \setminus \mathit{0} \text{ otherwise}\,. \end{aligned}$$

In turn, these equality constraints cut a polyhedral subcone $\boldsymbol{H}_N^{\mathcal{A}}$, actually a face, of $\boldsymbol{H}_N$. A system of random variables $\xi = (\xi_i)_{i \in N}$ is called an (information-theoretical) *perfect secret-sharing scheme (sss)* for $\mathcal{A}$ if its entropy function belongs to $\boldsymbol{H}_N^{\mathcal{A}}$ and is nonzero. For interpretation and basic references on secret sharing see [18], [32]. Such schemes are mostly constructed from configurations of subspaces of a finite dimensional linear or projective space, for a recent review of geometrical approaches see [28].

The average information rate of a perfect sss extends to the nonzero polymatroids g from $\boldsymbol{H}_N^{\mathcal{A}}$ by

$$\rho(g) = \frac{g(0)}{\frac{1}{n}\sum_{i\in N\setminus 0} g(i)}\,.$$

A basic question is to determine, or at least to estimate, the supremum $\rho_{\mathcal{A}}$ of the rates $\rho(g)$ over the entropy functions g of perfect sss's for $\mathcal{A}$, actually over nonzero g in $\boldsymbol{H}_N^{\mathcal{A}} \cap \boldsymbol{H}_N^{\mathsf{ent}}$. Hence, any progress on the description of the set $\boldsymbol{H}_N^{\mathsf{ent}}$ can help to determine rates more accurately. An upper bound on $\rho_{\mathcal{A}}$ obtains when the maximization of $\rho(g)$ is considered over nonzero g in $\boldsymbol{H}_N^{\mathcal{A}} \cap \mathit{cl}(\boldsymbol{H}_N^{\mathsf{ent}})$, which motivates a study of this closed convex cone.

Remark 6: For $g \in \boldsymbol{H}_N^{\mathcal{A}}$, it is easy to see that $g(0) \leqslant g(i)$, $i \in N$, which implies $\rho_{\mathcal{A}} \leqslant 1$. A practically useful access structure should have $\rho_{\mathcal{A}}$ close to 1, however, an example with $\rho_{\mathcal{A}} \leqslant \frac{4\ln n}{n}$ is known [10, Theorem 3.3]. If the distinguished polymatroid from $\boldsymbol{H}_N^{\mathcal{A}}$ constructed in [11, Theorem 3.5] were proved to be entropic then $\rho_{\mathcal{A}}$ would be at least $\frac{1}{n}$. For many access structures, however, existing lower bounds on $\rho_{\mathcal{A}}$ are exponentially small in n and their tightness is unclear [25], [3], [32]. If $n \leqslant 5$ then the rates $\rho_{\mathcal{A}}$ are known for all but a few access structures [26].

E. Ideal secret sharing

If for some access structure $\mathcal{A}$ a polymatroid $g \in \boldsymbol{H}_N^{\mathcal{A}}$ has constant values on all singletons of N then g is a multiple of a connected matroid by [6, Theorem 2]. If additionally g is nonzero and entropic, thus equal to the entropy function of a random vector, then this vector is called *ideal sss* for $\mathcal{A}$, for references see [7], [5], [18], [45], [32]. It turns out that $I \in \mathcal{A}$ is equivalent to existence of a circuit J of the matroid satifying $0 \in J$ and $J \setminus 0 \subseteq I$. Thus, only special access structures arising from matroids are amenable to ideal secret sharing.

In the framework of ideal secret sharing, the matroids with entropic positive multiples, thus the partition representable matroids, have been called also *secret-sharing*. Hence, Subsection IV-B discusses actually the ideal secret-sharing schemes through the entropy functions. It is not generally known that some results in literature overlap. For example, Vamos matroid is not secret-sharing by [50], or by [33, Lemma 1]. The characterizations of universally ideal sss's of [2] and [18, Theorem 7] are parallel to [33, Proposition 2] describing the matroids with all $(\ln d)$-multiples entropic, $d \geqslant 2$. Properties of E-ideal schemes of [27, Section 4.2] are consequences of [33, Theorem].

F. Beyond linearity

For the non-Pappus matroid r, a textbook example of a matroid that is not linear over any field, the polymatroid $2r$ is linear over the field $\mathbb{Z}_3^2$ by [51, Example 2] and [38, p. 190]. By Remark 10, $\ln 3^2 \cdot 2r$ is entropic, and thus r is partition representable of degree 9. Since appearance of this observation in [51], a natural open problem arises whether there exists a partition representable matroid without a linear positive multiple. A candidate for such a matroid is constructed

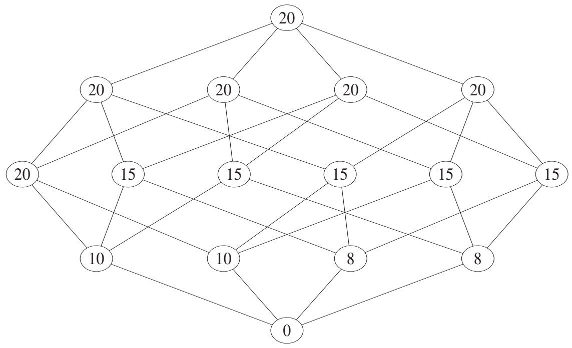

Fig. 2. The positive multiples of this asymptotically entropic polymatroid are not linear.

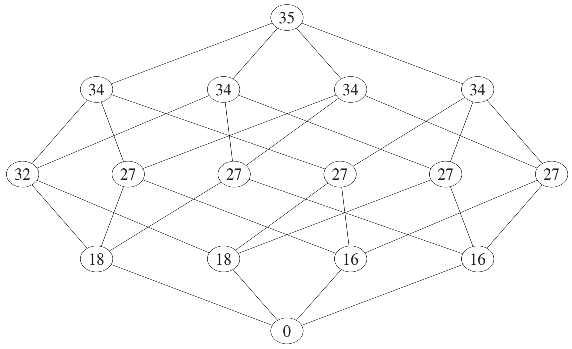

Fig. 3. The positive multiples of this polymatroid are entropic but not linear.

below as a free expansion of an integer-valued polymatroid with the positive multiples entropic but not linear.

The polymatroid of Fig. 3 has these properties.

In fact, consider $\{0,1\}$-valued random variables ξ_1 and ξ_2 that are independent and uniformly distributed, $\xi_3 = \xi_1\xi_2$ and $\xi_4 = (1-\xi_1)(1-\xi_2)$ [36, Example 1]. If g_α denotes the polymatroid given by Fig. 2 with two 8's replaced by α's then the entropy function of the vector of these variables is proportional to g_α with $\alpha = 20 - \frac{15}{2}\frac{\ln 3}{\ln 2}$. Since $\alpha > 8$ the polymatroid g_8 of Fig. 2 can be expressed as the convolution of g_α with a modular polymatroid, and is asymptotically entropic by Theorem 2. No positive multiple of g_8 is linear because of the violation of (5), see Remark 12 in Section V. However, we do not know whether a positive multiple of g_8 is entropic. By Lemmas 2 and 3, $h = \sum_{\emptyset\neq J\subseteq N} r_J$ belongs to $\mathit{ri}(\boldsymbol{H}_N^{\mathsf{ent}})$. Hence, the polymatroid $5g_8 + h$ of Fig. 3 and its positive multiples belong to $\mathit{ri}(\boldsymbol{H}_N^{\mathsf{ent}})$. By Theorem 1, they are entropic. On the other hand, no positive multiple of $5g_8 + h$ is linear since it makes (5) to fail.

By Theorem 4, a free expansion of the polymatroid of Fig. 3 is an asymptotically entropic matroid that has obviously no linear positive multiple. It remains, however, open whether this matroid has an entropic positive multiple, thus whether it is partition representable.

V. Miscellany

Remark 7: If g is the entropy function of a random vector $\xi = (\xi_i)_{i\in N}$ and h a modular polymatroid then $g * h\,(N)$

equals $g(N)$ if and only if $\sum_{i\in I} h(i) \geqslant \mathsf{H}(\xi_I|\xi_{N\setminus I})$, $I \subseteq N$. Interpreting $(h(i))_{i\in N}$ as the vector of rates, these are Slepian-Wolf inequalities of the achievable rate region for the multiple memoryless source from ξ.

Remark 8: It follows directly from the proof of Theorem 3 that each variable ϕ_n can be chosen to have the cardinality $\|\phi_n\|$ of its range bounded from above by $\lceil e^{n\alpha}\rceil$. For $\alpha \leqslant \mathsf{H}(\xi)$, this and $\frac{1}{n}\,\mathsf{H}(\phi_n) \to \alpha$ imply that $\frac{1}{n}\,\log\|\phi_n\| \to \alpha$, thus $(\phi_n)_{n\geqslant 1}$ can be viewed as a coding of the multiple memoryless source from ξ at the rate α. Hence, Theorem 3 is a relative to the achievability part of Slepian-Wolf theorem, which constructs to $\alpha > \mathsf{H}(\xi|\eta)$ and $\varepsilon > 0$ a coding $(\phi_n)_{n\geqslant 1}$ of the source from ξ at the rate α such that $\xi^{1.n}$ is eventually ε-recoverable from $(\phi_n, \eta^{1.n})$, in the sense that a decoding function of the latter differs from $\xi^{1.n}$ with a probability less than ε. This rate, decoding and probabilities of errors are disregarded in Theorem 3, focusing rather on all values of α and a generic limit relation of the sequence $(\phi_n)_{n\geqslant 1}$ to all sequences $(\eta_\Upsilon^{1.n})_{n\geqslant 1}$, $\Upsilon \subseteq \Gamma$, solely in terms of entropies.

Remark 9: The notation $\boldsymbol{H}_N^{\mathsf{imo}}$, used in Lemma 2, is motivated by the fact that this cone coincides with the images of modular polymatroids under mappings defined on N. This can be shown by modifying the proof of [39, Lemma 2] as follows. If g is the image of a modular polymatroid (M,h) under $\varphi\colon N \to \mathcal{P}(M)$ then the set $\varphi(N) = M$ is covered by the disjoint subsets $M_J = \{l \in M\colon \varphi'(l) = J\}$, $\emptyset \neq J \subseteq N$, where $\varphi'(l) = \{i \in N\colon l \in \varphi(i)\}$, $l \in M$. Hence, for $I \subseteq N$

$$\sum_{\emptyset\neq J\subseteq N} h(M_J)\, r_J(I) = \sum_{J\cap I\neq\emptyset} h(M_J) = h\Big(\bigcup_{J\cap I\neq\emptyset} M_J\Big)$$

by modularity. Here, the union consists of $l \in \varphi(N)$ satisfying $\varphi'(l) \cap I \neq \emptyset$, and thus equals $\varphi(I)$. It follows that g is the combination of r_J's with the weights $h(M_J)$. In the opposite direction, each $\alpha_J r_J$ with $\alpha_J \geqslant 0$ is obviously an image of a polymatroid with a one-element ground set. It suffices to apply the simple fact that the sum $g_1 + g_2$ of two polymatroids with the ground set N that are images of two modular polymatroids with disjoint ground sets, under two mappings φ_1 and φ_2 correspondingly, is the image of the direct sum of the modular polymatroids under $\varphi_1 \cup \varphi_2$.

Remark 10: A polymatroid (N,g) is *linear* if there exist subspaces $(E_i)_{i\in N}$ of a linear space E such that for every $I \subseteq N$ the rank of the linear envelope of $(E_i)_{i\in I}$ equals $g(I)$. Obviously, this notion concerns only the integer valued polymatroids. If a polymatroid is linear over a field then it is linear over a finite field. (In fact, for matroids this follows from [8, Proposition 7.3.4, p. 134], which combines with the fact that any polymatroid linear over a field is the factor of a matroid linear over the same field, discussed in [30, p. 246].) It is likely a piece of folklore that linearity of a polymatroid g over a finite field F implies that $\ln|F|\cdot g$ is entropic. In fact, there is no loss of generality in assuming that the linear space E is finite. Endow the dual E' of E with the uniform probability measure and define a random variable ξ_i as the factormapping of E' to the cosets of the annihilator of E_i. Elementary linear algebra arguments show that each subvector ξ_I of $(\xi_i)_{i\in N}$ takes $|F|^{g(I)}$ values with the same probabilities, thus the entropy of ξ_I equals $\ln|F|\cdot g(I)$.

Remark 11: For subgroups $(G_i)_{i\in N}$ of a finite group G and $G_I = \bigcap_{i\in I} G_i$, the function $I \mapsto \ln|G|/|G_I|$, $I \subseteq N$, is an entropic polymatroid. In fact, endowing G with the uniform pm, the polymatroid equals the entropy function of $(\xi_i)_{i\in N}$ where ξ_i is the factormapping defined on G and ranging in the set of left cosets of G_i. Note that the left cosets of G_I are the atoms of the algebra generated by ξ_I and that this subvector takes $|G|/|G_I|$ values with the same probability. It is a remarkable fact [9, Theorem 4.1] that divisions by positive integers of the entropic polymatroids that arise from subgroups of groups are dense in $\boldsymbol{H}_N^{\mathsf{ent}}$.

A proof can be sketched as follows. In approximating the entropy function of some random vector $\xi = (\xi_i)_{i\in N}$ there is no loss of generality in assuming that the vector sits on a finite set Ω endowed with the uniform pm. Consider the group G of permutations of Ω and the stabilizer G_i of the algebra generated by ξ_i, thus the subgroup of G of the permutations ρ satisfying $\xi_i\,\rho = \xi_i$. It is not difficult to see that G_I is the stabilizer of ξ_I, and hence $|G_I| = \prod_{B\in[\xi_I]} |B|!$ where $[\xi_I]$ denotes the set of atoms of the algebra generated by ξ_I. The main idea is to split each $\omega \in \Omega$ into n new elements and observe that the new symmetric group has $(n|\Omega|)!$ permutations and new stabilizers $\prod_{B\in[\xi_I]} (n|B|)!$ permutations. By the approximation $n! = \sqrt{2\pi n}\cdot n^n \cdot e^{-n+o(n)}$,

$$\ln\frac{(n|\Omega|)!}{\prod_{B\in[\xi_I]} (n|B|)!} = n|\Omega|\cdot\big[\mathsf{H}(\xi_I) + o(n)\big]\,, \qquad I \subseteq N\,.$$

Thus, upon divisions, the polymatroids arising from vectors of stabilizers converge to the entropy function of ξ when n goes to infinity.

Remark 12: Any polymatroid on the ground set N is obviously entropic if $|N| \leqslant 2$. If $|N| = 3$ then $\boldsymbol{H}_N$ is spanned by linear matroids, and thus $\mathit{cl}(\boldsymbol{H}_N^{\mathsf{ent}}) = \boldsymbol{H}_N$, see also [21], [20]. In this case, $\boldsymbol{H}_N$ contains $\boldsymbol{H}_N^{\mathsf{ent}}$ strictly. Theorem 1, Lemma 2, Lemma 4 and [41] provide known subsets of $\boldsymbol{H}_N^{\mathsf{ent}}$ and its complement, while a complete description of $\boldsymbol{H}_N^{\mathsf{ent}}$ is not yet available.

The inclusion $\mathit{cl}(\boldsymbol{H}_N^{\mathsf{ent}}) \subseteq \boldsymbol{H}_N$ is strict if $|N| = 4$, by the failure of (4) for the polymatroid of Fig. 1. In this case, the span of linear polymatroids from $\boldsymbol{H}_N$ is a proper polyhedral subcone of $\boldsymbol{H}_N$ [35], [20], [59] generated by a moderate number of linear polymatroids, or equivalently, given by the six inequalities

$$\begin{aligned} &h(ik) + h(jk) + h(il) + h(jl) + h(kl) \\ &\qquad \geqslant h(ij) + h(k) + h(l) + h(ikl) + h(jkl)\,, \end{aligned} \tag{5}$$

rewriting the necessary condition for a polymatroid to be linear by Ingleton, see [23] or [48, p. 177]. Examples of entropy functions that violate (5) are in [53], [36], [37], [59], [20].

Appendix

Proof of Lemma 7: If $x \in A^n$ and $\mathsf{s}(x)$ is a subset of $\mathsf{s}(P)$ then

$$P^n(x) = \prod_{a\in\mathsf{s}(P)} P(a)^{|x^{-1}(a)|} > 0\,.$$

This holds in particular if $x \in T^n_{P,\delta}$. In this case, using that the cardinality of $x^{-1}(a)$ is at least $nP(a)[1-\delta]$, $a \in \mathsf{s}(P)$, $\ln P^n(x)$ is at most $n[1-\delta]\sum_{a\in\mathsf{s}(P)} P(a)\ln P(a)$ and the upper bound on $P^n(x)$ follows. The lower bound obtains analogously. □

Proof of Corollary 3: Lemma 7 combines with the inequalities $1 \geqslant P^n(T^n_{P,\delta}) \geqslant |T^n_{P,\delta}| \min_{x\in T^n_{P,\delta}} P^n(x)$. □

A consequence of Hoeffding inequality [14, Theorem 8.1, p. 122] is stated explicitly.

Lemma 14: If random variables $\zeta_1,\dots,\zeta_n$ are independent and each one takes the value 1 with probability p and 0 with probability $1-p$ then

$$Pr\Big(\Big|\tfrac{1}{n}\textstyle\sum_{j=1}^n(\zeta_j-p)\Big| > \delta\Big) \leqslant 2\,e^{-2n\delta^2}\,.$$

Proof of Lemma 8: For $a \in A$ let $\zeta_1,\dots,\zeta_n$ be independent random variables that take the values 1 and 0 with probabilities $P(a)$ and $1-P(a)$, respectively. By Lemma 14, the probability of $|\frac{1}{n}\sum_{j=1}^n(\zeta_j - P(a))| > \delta P(a)$ is at most $2e^{-2n\delta^2P(a)^2}$. This probability equals the P^n-probability of the set of x in $\mathsf{s}(P)^n$ that satisfy $|\frac{1}{n}|x^{-1}(a)|-P(a)| > \delta P(a)$, thus violate one of the defining conditions of $T^n_{P,\delta}$. Hence, P^n-probability of union of these sets over $a\in A$ is at most $2|A|e^{-2n\delta^2\bar{P}^2}$, and the assertion follows. □

Proof of Lemma 9: If $y \in B^n$ and $\mathsf{s}(y)$ is contained in $\mathsf{s}(P_B)$ then $P^n_B(y) > 0$. For $x \in A^n$

$$\begin{aligned}\frac{P^n(x,y)}{P^n_B(y)} &= \prod_{i\in N} P_{|y_i}(x_i) = \prod_{b\in\mathsf{s}(y)}\ \prod_{i\in y^{-1}(b)} P_{|b}(x_i)\\ &= \prod_{b\in\mathsf{s}(y)} P_{|b}^{y^{-1}(b)}(x_{y^{-1}(b)})\end{aligned} \tag{6}$$

where $x_{y^{-1}(b)}$ denotes the projection of x to $A^{y^{-1}(b)}$. Under the assumptions on x and y, $\mathsf{s}(y)\subseteq\mathsf{s}(P_B)$ and that projection belongs to $T^{y^{-1}(b)}_{P_{|b},\delta}$. By Lemma 7, applied to $y^{-1}(b)$ and $P_{|b}$ with $b\in\mathsf{s}(y)$ in the role of $\widehat{n}$ and P,

$$\frac{P^n(x,y)}{P^n_B(y)} \leqslant \prod_{b\in\mathsf{s}(P_B)} e^{-|y^{-1}(b)|\,H(P_{|b})\,[1-\delta]}\,.$$

Here, $|y^{-1}(b)|$ is at least $nP_B(b)[1-\delta]$ because $y\in T^n_{P_B,\delta}$. Hence, for $\delta<1$

$$\frac{P^n(x,y)}{P^n_B(y)} \leqslant \exp\Big[-n\sum_{b\in\mathsf{s}(P_B)} P_B(b)\,H(P_{|b})\,[1-\delta]^2\Big]\,.$$

This implies the assertion, trivial if $\delta > \frac{1}{2}$. □

Proof of Lemma 10: By assumption, $\mathsf{s}(y)\subseteq\mathsf{s}(P_B)$. If $b\in\mathsf{s}(y)$ then

$$P_{|b}^{y^{-1}(b)}(T^{y^{-1}(b)}_{P_{|b},\delta}) \geqslant 1-2\,|A|\,\exp[-2\,|y^{-1}(b)|\,\delta^2\,\overline{P_{|b}}^{\,2}]$$

by Lemma 8. Here, $|y^{-1}(b)|\geqslant nP_B(b)[1-\delta]$ as $y\in T^n_{P_B,\delta}$. Using $\overline{P_{|b}}\,P_B(b)\geqslant\bar{P}$ and its consequence $\overline{P_{|b}}\geqslant\bar{P}$, it follows that

$$P_{|b}^{y^{-1}(b)}(T^{y^{-1}(b)}_{P_{|b},\delta}) \geqslant 1-2\,|A|\,\exp\Big[-2\,n\,\delta^2[1-\delta]\,\bar{P}^{\,2}\Big]\,.$$

This inequality and

$$\frac{P^n(T^n_{P,\delta|y})}{P^n_B(y)} = \prod_{b\in\mathsf{s}(y)} P_{|b}^{y^{-1}(b)}(T^{y^{-1}(b)}_{P_{|b},\delta})\,,$$

obtained by the summation in (6) over $x\in A^n$ satisfying $(x,y)\in T^n_{P,\delta|y}$, imply the assertion. □

ACKNOWLEDGMENT

My sincere thanks go to Imre Csiszár for numerous inspiring discussions. Being asked whether Theorem 3 might hold, he expressed a strong positive belief and draw my attention to [1, Lemma 3.1].

REFERENCES

[1] R. Ahlswede and I. Csiszár (1998) Common randomness in information theory and cryptography – Part II: CR Capacity. *IEEE Trans. Information Theory* **44** 225–240.
[2] A. Beimel and B. Chor (1994) Universally ideal secret-sharing schemes. *IEEE Trans. Information Theory* **40** 786–794. (Preliminary Version in: *CRYPTO'92 – Proc. on Advances in Cryptology*, Springer LNCS 1993, Vol. 740, 183–195.)
[3] J. Benaloh and J. Leichter (1989) Generalized secret sharing and monotone functions. In: *CRYPTO'88: – Proc. on Advances in Cryptology*, Springer LNCS 1989, Vol. 403, 27–35.
[4] G. Bennett (1962) Probability inequalities for the sum of independent random variables. *J. Amer. Statis. Assoc.* **57** 33–45.
[5] G.R. Blakley and G.A. Kabatianski (1995) General Perfect Secret Sharing Schemes. In: *CRYPTO'95: 15th Annual International Cryptology Conference*, Springer, Vol. 963, 367-371.
[6] G.R. Blakley and G.A. Kabatianski (1997) Generalized ideal secret-sharing schemes and matroids. *Problems of Information Transmission* **33** 277–284.
[7] E.F. Brickell and D.M. Davenport (1991) On the classification of ideal secret-sharing schemes. *J. Cryptology* **4** 123–134.
[8] T. Brylawski (1986) Constructions. In: *Theory of Matroids* (N. White, ed.), Cambridge University Press: Cambridge, 2127–223.
[9] T.H. Chan and R.W. Yeung (2002) On a relation between information inequalities and group theory. *IEEE Trans. Information Theory* **48** 1992–1995.
[10] L. Csirmaz (1996) The dealer's random bits in perfect secret-sharing schemes. *Studia Scient. Math. Hungarica* **32** 429–437.
[11] L. Csirmaz (1997) The size of a share must be large. *J. Cryptology* **10** 223–231.
[12] I. Csiszar and J. Körner (1981) *Information Theory: Coding Theorems for Discrete Memoryless Systems.* Academic Press, New York (Akademiai Kiadó, Budapest).
[13] I. Csiszar and P. Narayan (2004) Secrecy capacities for multiple terminals. *IEEE Trans. Information Theory* **50** 3047–3061.
[14] L. Devroye, L. Győrfi and G. Lugosi (1996) *A Probabilistic Theory of Pattern Recognition.* Springer-Verlag, New York.
[15] R. Dougherty, C. Freiling, and K. Zeger (2006) Six New Non-Shannon Information Inequalities. In: *Proc. IEEE International Symposium on Information Theory,* Seattle, Washington, 233–236.
[16] S. Fujishige (1978) Polymatroidal dependence structure of a set of random variables. *Information and Control* **39** 55–72.
[17] S. Fujishige (1991) *Submodular Functions and Optimization.* North-Holland, Amsterdam.
[18] J.Dj. Golic (1998) On matroid characterization of ideal secret sharing schemes. *Journal of Cryptology* **11** 75–86.
[19] V.P. Grishukin (1994) On the extremality of the rank function of a connected semimodular lattice. *Transactions of AMS* **158** 31-36.
[20] D. Hammer, A. Romashchenko, A. Shen, and N. Vereshchagin (2000) Inequalities for Shannon entropy and Kolmogorov complexity. *Journal of Computer and Systems Sciences* **60** 442-464.
[21] T.S. Han (1981) A uniqueness of Shannon's information distance and related nonnegativity problems. *Journal of Combinatorics, Information and System Sciences* **4** 320–331.
[22] 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.

[23] A.W. Ingleton (1971) Conditions for representability and transversality of matroids. In: *Proc. Fr. Br. Conf. 1970*, Springer Lecture Notes **211**, Springer-Verlag, Berlin, 62–67.

[24] A.W. Ingleton (1971) Representation of matroids. In: *Combinatorial Mathematics and its Applications* (D.J.A. Welsh, ed.), Academic Press, London, 149–169.

[25] M. Ito, A. Saito and T. Nishizeki (1987) Secret sharing schemes realizing general access structure. In: *Proc. IEEE Global Telecommunication Conf., Globecom'87*, 99–102.

[26] W.-A. Jackson and K.M. Martin (1996) Perfect secret sharing schemes on five participants. *Designs, Codes and Cryptography* **9** 267–286.

[27] W.-A. Jackson and K.M. Martin (1998) Combinatorial models for perfect secret-sharing schemes. *J. Comb. Math. Comb. Comput.* **28** 249–265.

[28] W.-A. Jackson, K.M. Martin and Ch.M. Keefe (2004) Geometrical contributions to secret sharing theory. *Journal of Geometry* **79** 102–133.

[29] R. Lněnička (2003) On the Tightness of the Zhang-Yeung Inequality for Gaussian Vectors. *Communications in Information and Systems* **3** 41–46.

[30] 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.

[31] K. Makarychev, Yu. Makarychev, A. Romashchenko and N. Vereshchagin (2002) A new class of non-Shannon-type inequalities for entropies. *Communications in Information and Systems* **2** 147–166.

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

[33] F. Matúš (1994) Probabilistic conditional independence structures and matroid theory: background. *Int. Journal of General Systems* **22** 185–196. (Preliminary Version in: *WUPES'91 – Proceedings of the Workshop on Uncertainty Processing in Expert Systems*, Institute of Information Theory and Automation, Prague, Czech Republic, 1991, 12pp.)

[34] F. Matúš (1994) Extreme convex set functions with many nonnegative differences. *Discrete Mathematics* **135** 177-191.

[35] F. Matúš and M. Studený (1995) Conditional independences among four random variables I. *Combinatorics, Probab. and Comput.* **4** 269–278.

[36] F. Matúš (1995) Conditional independences among four random variables II. *Combinatorics, Probab. and Comput.* **4** 407–417.

[37] F. Matúš (1999) Conditional independences among four random variables III: final conclusion. *Combinatorics, Probab. and Comput.* **8** 269–276.

[38] F. Matúš (1999) Matroid representations by partitions. *Discrete Mathematics* **203** 169–194.

[39] F. Matúš (2001) Excluded minors for Boolean polymatroids. *Discrete Mathematics* **235** 317–321.

[40] F. Matúš (2005) Inequalities for Shannon entropies and adhesivity of polymatroids. In: *Proc. 9th Canadian Workshop on Information Theory*, McGill University, Montréal, Canada, 28–31.

[41] F. Matúš (2006) Piecewise linear conditional information inequality. *IEEE Trans. Information Theory* **44** 236–238.

[42] F. Matúš (2006) Adhesivity of polymatroids. (under revision for *Discrete Mathematics*)

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

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

[45] S.-L. Ng (2003) A representation of a family of secret sharing matroids. *Designs, Codes and Cryptography* **30** 5–19.

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

[47] H.Q. Nguyen (1986) Semimodular functions. In: *Theory of Matroids* (N. White, ed.), Cambridge University Press, Cambridge, 272–297.

[48] J.G. Oxley (1992) *Matroid Theory.* Oxford University Press, Oxford.

[49] R.T. Rockafellar (1970) *Convex Analysis.* Princeton University Press, Princeton.

[50] P.D. Seymour (1992) On secret-sharing matroids. *J. Comb. Theory B* **56** 69–73.

[51] J. Simonis and A. Ashikhmin (1998) Almost affine codes. *Designs, Codes and Cryptography* **14** 179–197.

[52] S. Smale and D.-X. Zhou (2004) Shannon sampling and function reconstruction from point values. *Bulletin AMS* **41** 279–305.

[53] M. Studený (1990) personal communication

[54] D.J.A. Welsh (1976) *Matroid Theory.* Academic Press, London.

[55] R.W. Yeung (2002) *A First Course in Information Theory*. Kluwer Academic/Plenum Publishers, New York.

[56] R.W. Yeung (2001) A class of non-Shannon-type information inequalities and their applications. *Communications in Information and Systems* **1** 87–100.

[57] Z. Zhang and R.W. Yeung (1997) A non-Shannon-type conditional inequality of information quantities. *IEEE Trans. Information Theory* **43** 1982–1986.

[58] Z. Zhang (2003) On a new non-Shannon-type information inequality. *Communications in Information and Systems* **3** 47–60.

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

František Matúš received his B.S. degree in Mathematical Engineering from Faculty of Nuclear Sciences and Physical Engineering, Czech Technical University, Prague, CZ, in 1984 and CSc. degree (PhD. level in Czech Republic) in theoretical cybernetics from Czechoslovak Academy of Sciences in 1989.

Since 1985, he has been with Institute of Information Theory and Automation of Czech Academy of Sciences, Prague, CZ. During 1995-1997 he was A. von Humboldt Fellow at University of Bielefeld, Bielefeld, Germany. His research interests include Shannon theory, Information divergence geometry, Exponential families, Matroids, polymatroids and related discrete structures, Conditional independence structures and their representations, Special random sequences and arrays, de Finetti type theorems and partial exchangeability, Latin squares and quasigroups, Conditional probability spaces, Radon transform theory, also discrete, Combinatorial inequalities, Probabilistic and combinatorial methods of AI, etc.