accepted to *Proceedings of the AMS* June 28, 2017

Algebraic matroids are almost entropic[*]

František Matúš [†]

Abstract. Algebraic matroids capture properties of the algebraic dependence among elements of extension fields. Almost entropic matroids have the rank functions arbitrarily well approximated by the entropies of subvectors of random vectors. The former class of matroids is included in the latter. A key argument in the proof is the Lang-Weil bound on the number of points in algebraic varieties.

Let $\mathsf{M} = (N, r)$ be a matroid with a finite ground set N and rank function r, see [13].

Let $\mathbb{G}$ be a field. The matroid M is *algebraic* over $\mathbb{G}$ if there exist an extension field $\mathbb{H}$ of $\mathbb{G}$ and $e_i \in \mathbb{H}$ for $i \in N$ such that $r(I) = \deg_{\mathrm{tr}/\mathbb{G}} \mathbb{G}(e_i \colon i \in I)$ for $I \subseteq N$. Here, $\deg_{\mathrm{tr}/\mathbb{G}}$ denotes the transcendence degree over $\mathbb{G}$ and $\mathbb{G}(e_i \colon i \in I)$ the smallest subfield of $\mathbb{H}$ that contains $\mathbb{G}$ and $\{e_i \colon i \in I\}$. Thus, $I \subseteq N$ is an independent set of M, $r(I) = |I|$, if and only if e_i, $i \in I$, are algebraically independent over $\mathbb{G}$. This means that a nonzero polynomial with indeterminates x_i, $i \in I$, and coefficients in $\mathbb{G}$ cannot vanish when substituting e_i for x_i.

For random variables ξ_i, $i \in N$, that take only finitely many values, the mapping that assigns to $I \subseteq N$ the Shannon entropy of $(\xi_i \colon i \in I)$ is a polymatroidal rank function [4]. The polymatroids constructed in this way are called *entropic*. Their rank functions exhaust the entropy region [11]. A polymatroid (N, g) with rank function g is *almost entropic*, or asymptotically entropic [9], if there exists a sequence of entropic polymatroids (N, h_n) such that $h_n \to g$ pointwise, thus if g belongs to the closure of the entropy region. This defines in particular the almost entropic matroids.

Theorem 1. *Every algebraic matroid is almost entropic.*

Proof. Let M be a matroid that is algebraically representable over $\mathbb{G}$ by $e_i \in \mathbb{H}$, $i \in N$. There is no loss of generality in assuming that $\mathbb{H}$ is algebraically closed, $\mathbb{H} = \overline{\mathbb{H}}$.

[*] AMS 2010 Mathematics Subject Classification. Primary 05B35, 94A17; secondary 12F20, 11G25.

Key words and phrases. Matroid, polymatroid, matroid representations, algebraic matroid, almost entropic matroid, partition representable matroid, ideal secret sharing, entropy region.

[†] 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 (`matus@utia.cas.cz`).

In the first part of the proof, let the characteristic of $\mathbb{G}$ be positive. If $\mathbb{G}$ is infinite then M is algebraically representable over the prime field of $\mathbb{G}$ by [7]. Thus, it suffices to assume that $\mathbb{G}$ is finite.

The following form of the Lang-Weil bound [6], estimating the number of points of a variety, is needed in the sequel. Let $\mathbb{G}$ be finite field, $\overline{\mathbb{G}}$ its algebraic closure and $\boldsymbol{V} \subseteq \overline{\mathbb{G}}^{\,d}$ an affine algebraic variety defined by a set of polynomials with coefficients in $\mathbb{G}$. The variety decomposes into irreducible components over $\overline{\mathbb{G}}$. Every component has a dimension, which is the transcendence degree of its coordinate ring over $\overline{\mathbb{G}}$. Let $c_{\boldsymbol{V}}$ denote the number of those components that have the maximal dimension, which is by definition the dimension $\dim \boldsymbol{V}$ of $\boldsymbol{V}$. Every component is defined by a finite set of polynomials with coefficients in $\overline{\mathbb{G}}$. Let $\mathbb{A} \subseteq \overline{\mathbb{G}}$ denote the finite set of all coefficients in these polynomials. The smallest subfield of $\overline{\mathbb{G}}$ that contains $\mathbb{G}$ and $\mathbb{A}$ is denoted by $\mathbb{G}_{\boldsymbol{V}}$. It is a finite extension of $\mathbb{G}$. The Lang-Weil inequality implies that if $\mathbb{F}$ is a finite field extending $\mathbb{G}_{\boldsymbol{V}}$ then the number of points in the variety $\boldsymbol{V} \cap \mathbb{F}^d$ is approximately $c_{\boldsymbol{V}} \cdot |\mathbb{F}|^{\dim \boldsymbol{V}}$ in the sense that there exists a constant $\kappa_{\boldsymbol{V}} > 0$ not depending on $\mathbb{F}$ such that

$$\left| \frac{|\boldsymbol{V} \cap \mathbb{F}^d|}{|\mathbb{F}|^{\dim \boldsymbol{V}}} - c_{\boldsymbol{V}} \right| \leqslant \frac{\kappa_{\boldsymbol{V}}}{\sqrt{|\mathbb{F}|}} \,. \tag{1}$$

For more sophisticated bounds see [2]. The reader may like to consult Corollary 4 of the blog[‡] by T. Tao, however, in the above formulation, $c_{\boldsymbol{V}}$ does not depend on $\mathbb{F}$.

The polynomials from the ring $\mathbb{G}[x_i\colon i \in N]$ that vanish when substituting e_i, $i \in N$, form a radical ideal $\boldsymbol{I}_{\mathbb{G}}$. Given a base I of the matroid M, if a polynomial from $\boldsymbol{I}_{\mathbb{G}}$ contains only the indeterminates x_i, $i \in I$, then it is zero. Given a circuit C of M, the collection $(e_i\colon i \in C)$ is algebraically dependent but $(e_i\colon i \in C \setminus j)$ is algebraically independent for any $j \in C$. Hence, there exists a nonzero polynomial p_C from $\boldsymbol{I}_{\mathbb{G}}$ that contains each of the indeterminates x_c, $c \in C$, and none of the remaining ones. Let $\mathcal{P}$ denote the set of the polynomials p_C for C running over the circuits of M. The polynomials from $\mathcal{P}$ define an affine algebraic variety in $\overline{\mathbb{G}}^{\,N}$ that will be denoted by $\boldsymbol{V}_{\mathcal{P}}$.

The variety $\boldsymbol{V}_{\mathcal{P}} \subseteq \overline{\mathbb{G}}^{\,d}$ has the dimension $r(N)$. In fact, the algebraic dependence in $\mathbb{H}$ is the same over $\mathbb{G}$ and $\overline{\mathbb{G}}$, see Remark 3. For a base $I \subseteq N$, the elements e_i, $i \in I$, are algebraically independent over $\overline{\mathbb{G}}$ and every $j \in N \setminus I$ is algebraically dependent on them over $\mathbb{G}$. Hence, the quotient ring of $\boldsymbol{V}_{\mathcal{P}}$ has the transcendence dimension $|I| = r(N)$.

It follows from the above formulation of the Lang-Weil bound and (1) that there exist a finite extension field $\mathbb{G}_{\boldsymbol{V}_{\mathcal{P}}}$ of $\mathbb{G}$ and constants $c_{\boldsymbol{V}_{\mathcal{P}}} \geqslant 1$ and $\kappa_{\boldsymbol{V}_{\mathcal{P}}} > 0$ such that for every finite extension field $\mathbb{F}$ of $\mathbb{G}_{\boldsymbol{V}_{\mathcal{P}}}$

$$\left| \frac{|\boldsymbol{V}_{\mathcal{P}} \cap \mathbb{F}^N|}{|\mathbb{F}|^{r(N)}} - c_{\boldsymbol{V}_{\mathcal{P}}} \right| \leqslant \frac{\kappa_{\boldsymbol{V}_{\mathcal{P}}}}{\sqrt{|\mathbb{F}|}} \,. \tag{2}$$

The index $\mathcal{P}$ at $\boldsymbol{V}_{\mathcal{P}}$ is omitted in the sequel.

[‡] https://terrytao.wordpress.com/2012/08/31/the-lang-weil-bound/

The ineq. (2) implies that $\boldsymbol{V}\cap\mathbb{F}^N$ is nonempty if the cardinality of $\mathbb{F}$ is large. In such a case, let $P_{\mathbb{F}}$ be the probability measure on $\mathbb{F}^N$ that sits and is uniform on $\boldsymbol{V}\cap\mathbb{F}^N$. In other words, the probability of each point of the variety is the same and the points outside the variety have the probability zero. For the coordinate projection $\pi_I\colon \mathbb{F}^N\to\mathbb{F}^I$, $I\subseteq N$, the image of $P_{\mathbb{F}}$ under π_I, thus a marginal probability measure on $\mathbb{F}^I$, is denoted by $P^I_{\mathbb{F}}$. The projections π_i, $i\in N$, turn into random variables, having the joint distribution $P_{\mathbb{F}}$. They give rise to the entropic polymatroid $(\mathsf{H}(P^I_{\mathbb{F}}))_{I\subseteq N}$ where H stands for the Shannon entropy. Then, the polymatroid $(\mathsf{H}(P^I_{\mathbb{F}})/\ln|\mathbb{F}|)_{I\subseteq N}$ is almost entropic using that the closure of the entropy region is convex [12, Remark 2]. It remains to prove that this point can be arbitrarily close to $(r(I))_{I\subseteq N}$ when the cardinality of the field $\mathbb{F}$ is large enough.

For $I\subseteq N$ and $y_I\in\pi_I(\boldsymbol{V}\cap\mathbb{F}^N)\subseteq\mathbb{F}^I$ let $\pi^{-1}_{I,\mathbb{F}}(y_I)$ denote the fibre consisting of those $z\in\boldsymbol{V}\cap\mathbb{F}^N$ that project to y_I, thus $\pi_I(z)=y_I$. The entropy of the marginal $P^I_{\mathbb{F}}$ can be written as

$$\mathsf{H}(P^I_{\mathbb{F}}) = -\sum_{y_I\in\pi_I(\boldsymbol{V}\cap\mathbb{F}^N)} \frac{|\pi^{-1}_{I,\mathbb{F}}(y_I)|}{|\boldsymbol{V}\cap\mathbb{F}^N|}\ln\frac{|\pi^{-1}_{I,\mathbb{F}}(y_I)|}{|\boldsymbol{V}\cap\mathbb{F}^N|}\,,\qquad I\subseteq N\,. \tag{3}$$

Let $I\subseteq N$ be a base of M, $j\in N\setminus I$ and $C=\gamma(j,I)$ be the fundamental circuit of j w.r.t. I. The polynomial p_C contains a term with a positive power of the indeterminate x_j, having a nonzero coefficient. Let $d_{j,C}\geqslant 1$ be the largest power of x_j in such a term. The product of $d_{j,\gamma(j,I)}$ over $j\in N\setminus I$ is denoted by D_I. It follows that each fibre $\pi^{-1}_{I,\mathbb{F}}(y_I)$ has at most D_I elements. Let D^* denote the maximum of D_I over the bases I of M. This number does not depend on the choice of $\mathbb{F}$. Hence, if a finite field $\mathbb{F}$ extends $\mathbb{G}_{\boldsymbol{V}}$ and its cardinality is large enough then

$$\mathsf{H}(P^I_{\mathbb{F}}) \geqslant -\ln\frac{D^*}{|\boldsymbol{V}\cap\mathbb{F}^N|} \geqslant -\ln D^* + \ln\Big[c_{\boldsymbol{V}}-\tfrac{\kappa_{\boldsymbol{V}}}{\sqrt{|\mathbb{F}|}}\Big] + r(N)\ln|\mathbb{F}|\,,\qquad I\subseteq N \text{ base},$$

estimating the ratio under logarithm in (3) and using (2). In turn, as $r(N)=|I|$,

$$\frac{\mathsf{H}(P^I_{\mathbb{F}})}{\ln|\mathbb{F}|}-|I| \geqslant -\frac{\ln D^*}{\ln|\mathbb{F}|}+\frac{\ln[1-\kappa_{\boldsymbol{V}}/\sqrt{|\mathbb{F}|}\,]}{\ln|\mathbb{F}|}\,,\qquad I\subseteq N \text{ base}.$$

By submodularity of entropy, $\mathsf{H}(P^I_{\mathbb{F}})\leqslant\mathsf{H}(P^J_{\mathbb{F}})+\mathsf{H}(P^{I\setminus J}_{\mathbb{F}})$, $J\subseteq I$. The last term is at most $|I\setminus J|\ln|\mathbb{F}|$. Therefore, dividing by $\ln|\mathbb{F}|$ and subtracting $|I|$, as $r(J)=|J|$,

$$0\geqslant\frac{\mathsf{H}(P^J_{\mathbb{F}})}{\ln|\mathbb{F}|}-r(J)\geqslant -\frac{\ln D^*}{\ln|\mathbb{F}|}+\frac{\ln[1-\kappa_{\boldsymbol{V}}/\sqrt{|\mathbb{F}|}\,]}{\ln|\mathbb{F}|}\,,\qquad J\subseteq N \text{ independent}. \tag{4}$$

The strategy is to prove similar bounds for circuits C which together with (4) imply bounds for any subset K of N. For a circuit C in M, $j\in C$ and $J=C\setminus j$, using (3) with $I=C$ and $I=J$,

$$\mathsf{H}(P^C_{\mathbb{F}})=\mathsf{H}(P^J_{\mathbb{F}})-\sum_{y_C\in\pi_C(\boldsymbol{V}\cap\mathbb{F}^N)}\frac{|\pi^{-1}_{C,\mathbb{F}}(y_C)|}{|\boldsymbol{V}\cap\mathbb{F}^N|}\ln\Big[\frac{|\pi^{-1}_{C,\mathbb{F}}(y_C)|}{|\boldsymbol{V}\cap\mathbb{F}^N|}\Big/\frac{|\pi^{-1}_{J,\mathbb{F}}(\pi^C_J(y_C))|}{|\boldsymbol{V}\cap\mathbb{F}^N|}\Big]$$

where $\pi^C_J\colon\mathbb{F}^C\to\mathbb{F}^J$ is the coordinate projector. For $y_J\in\pi_J(\boldsymbol{V}\cap\mathbb{F}^N)$, the mapping

$$y_j\mapsto|\pi^{-1}_{C,\mathbb{F}}(y_j,y_J)|/|\pi^{-1}_{J,\mathbb{F}}(y_J)|\,,\quad y_j\in\mathbb{F}\,,$$

takes at most $d_{j,C}$ nonzero values. It defines a conditional probability measure whose entropy is at most $\ln d_{j,C}$. Hence, summing in the above sum first over y_j,

$$\mathsf{H}(P_{\mathbb{F}}^{C}) \leqslant \mathsf{H}(P_{\mathbb{F}}^{J}) + \ln d_{j,C} \leqslant |J| \ln |\mathbb{F}| + \ln D^* \,.$$

By $r(C)=|J|$, $\mathsf{H}(P_{\mathbb{F}}^{C}) \geqslant \mathsf{H}(P_{\mathbb{F}}^{J})$ and (4),

$$\frac{\ln D^*}{\ln|\mathbb{F}|} \geqslant \frac{\mathsf{H}(P_{\mathbb{F}}^{C})}{\ln|\mathbb{F}|} - r(C) \geqslant -\frac{\ln D^*}{\ln|\mathbb{F}|} + \frac{\ln[1-\kappa_{\boldsymbol{V}}/\sqrt{|\mathbb{F}|}\,]}{\ln|\mathbb{F}|}\,, \qquad C \subseteq N \text{ circuit}\,. \tag{5}$$

For arbitrary $K \subseteq N$ let J be a maximal independent subset of K, and for $k \in K \setminus J$ let $\gamma(k,J)$ be the unique circuit contained in $k \cup J$. Abbreviating $\mathsf{H}(P_{\mathbb{F}}^{K})$ to $h(K)$, by submodularity of entropy,

$$\textstyle\sum_{k\in K\setminus J} \big[h(\gamma(k,J)) - h(\gamma(k,J)\setminus k)\big] \geqslant \sum_{k\in K\setminus J} \big[h(k\cup J) - h(J)\big] \geqslant h(K) - h(J)\,.$$

The inequalities are combined with (5), applied to the circuits $\gamma(k,J)$, and (4), applied to the independent sets $\gamma(k,J)\setminus k$,

$$|K\setminus J|\cdot\Big[2\,\frac{\ln D^*}{\ln|\mathbb{F}|} - \frac{\ln[1-\kappa_{\boldsymbol{V}}/\sqrt{|\mathbb{F}|}\,]}{\ln|\mathbb{F}|}\Big] \geqslant \Big[\frac{\mathsf{H}(P_{\mathbb{F}}^{K})}{\ln|\mathbb{F}|} - r(K)\Big] - \Big[\frac{\mathsf{H}(P_{\mathbb{F}}^{J})}{\ln|\mathbb{F}|} - r(J)\Big] \geqslant 0\,, \quad K \subseteq N\,,$$

using also that $r(\gamma(k,J))) = r(\gamma(k,J)\setminus k)$ and $r(K) = r(J)$. It follows by (4) that the almost entropic point $(\mathsf{H}(P_{\mathbb{F}}^{K})/\ln|\mathbb{F}|)_{K\subseteq N}$ can be arbitrarily close to $(r(K))_{K\subseteq N}$ when the cardinality of $\mathbb{F}$, extending $\mathbb{G}_{\boldsymbol{V}}$, is sufficiently large.

In the second part of the proof, the characteristic of $\mathbb{G}$ is zero. Then, M is linear over $\mathbb{G}(T)$ where T is a finite set of transcendentals over $\mathbb{G}$ [13, Proposition 6.7.11]. In turn, M is linear over a finite field $\mathbb{F}$ [13, Proposition 6.8.2]. Hence, M is algebraic over $\mathbb{F}$ [13, Proposition 6.7.10]. By the first part of the proof, it is almost entropic. □

The assertion of Theorem 1 settles [12, Conjecture 2]. Since there exists a multilinear matroid that is not algebraic [1] the implication of Theorem 1 cannot be reversed, knowing that the multilinear matroids are partition representable, see Remark 2, and hence almost entropic. Relations between several classes of matroids are summarized in [12, Figure 1].

The Vámos matroid is not algebraic [5]. The assertion follows alternatively from Theorem 1 and the fact that it is not almost entropic. Namely, the almost entropic matroids are selfadhesive [10] whence they satisfy Zhang-Yeung inequality, violated by the Vámos matroid. However, the algebraic matroids are selfadhesive directly by [12, Lemma 14].

Remark 1. An interesting special case in the above proof is when the polynomials from $\mathcal{P}$ are linear. Each variety $\boldsymbol{V}_{\mathcal{P}} \cap \mathbb{F}^N$ becomes a linear space over $\mathbb{F}$. The probability measure $P_{\mathbb{F}}$ on the space has all marginals sitting on linear spaces and uniform. Then, the entropies of the marginals are integer multiples of $\ln|\mathbb{F}|$. It follows from the proof that the entropic point $(\mathsf{H}(P_{\mathbb{F}}^{K}))_{K\subseteq N}$ is equal to $(r(K)\cdot\ln|\mathbb{F}|)_{K\subseteq N}$, provided $\mathbb{F}$ is large enough and extends $\mathbb{G}_{\boldsymbol{V}_{\mathcal{P}}}$. No limiting with the size of the field $\mathbb{F}$ is needed.

Remark 2. The situation when an entropic point is a multiple of a matroidal rank function corresponds to a matroid representation by partitions, or to an ideal secret sharing scheme from cryptography. A matroid $\mathsf{M} = (N, r)$ is partition representable of the degree $d \geqslant 2$

if there exist a set of the cardinality $d^{r(N)}$ and its partitions π_i, $i \in N$, such that the meet-partition $\wedge_{i \in I} \pi_i$ has $d^{r(I)}$ blocks of the same size, $I \subseteq N$, see [8]. In Remark 1, the set is $\boldsymbol{V}_{\mathcal{P}} \cap \mathbb{F}^N$ and the blocks of the i-th partition are the fibers of the i-th coordinate projection of $\mathbb{F}^N$.

Remark 3. To see that the algebraic dependence (a.d.) is the same over $\mathbb{G}$ and $\overline{\mathbb{G}}$, let $t \in \mathbb{H}$ be a.d. on a finite set $T \subseteq \mathbb{H}$ over $\overline{\mathbb{G}}$. Thus, a nonzero polynomial q in an indeterminate y with coefficients in $\overline{\mathbb{G}}[T]$ vanishes when substituting t for y. However, q is also a polynomial with coefficients from $\mathbb{G}[T \cup B]$ for a finite set $B \subseteq \overline{\mathbb{G}}$. Then t is a.d. on $T \cup B$ over $\mathbb{G}$. The elements of B are a.d. on the finite set $\mathbb{G}$ over $\mathbb{G}$. Hence, the elements of $T \cup B$ are a.d. on $T \cup \mathbb{G}$ over $\mathbb{G}$. It follows that t is a.d. on $T \cup \mathbb{G}$ over $\mathbb{G}$ [13, Lemma 6.7.5] which implies that t is a.d. on T over $\mathbb{G}$.

Sampling of points on algebraic varieties, thus from the distribution $P_{\mathbb{F}}$, is studied in [3] in connection to problems in NP.

Acknowledgement

This is to thank John Voight and Bernd Sturmfels for discussions related to the Lang-Weil bound. This work was supported by Grant Agency of the Czech Republic under Grant 16-12010S.

References

[1] A. Ben-Efraim (2016) Secret-sharing matroids need not be algebraic. *Discrete Math.* **339** 2136–2145.

[2] A. Cafure and G. Materab (2006) Improved explicit estimates on the number of solutions of equations over a finite field. *Finite Fields and Their Applications* **12** 155–185.

[3] M. Cheraghchi and A. Shokrollahi (2009) Almost-uniform sampling of points on high-dimensional algebraic varieties. *Symposium on Theoretical Aspects of Computer Science* (Freiburg), 277–288. (arXiv:0902.1254 [cs.DS])

[4] S. Fujishige (1978) Polymatroidal dependence structure of a set of random variables. *Information and Control* **39** 55–72.

[5] A.W. Ingleton and R.A. Main (1975) Non-algebraic matroids exist. *Bulletin of the London Mathematical Society* **7** 144–146.

[6] S. Lang and A. Weil (1954) Number of Points of Varieties in Finite Fields *American J. of Mathematics* **76** 819–827.

[7] B. Lindström (1987) A reduction of algebraic representations of matroids. *Proceedings of AMS* **100** 388–389.

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

[9] F. Matúš (2007) Two constructions on limits of entropy functions. *IEEE Trans. Inform. Theory* **53** 320–330.

[10] F. Matúš (2007) Adhesivity of polymatroids. *Discrete Mathematics* **307** 2464–2477.

[11] F. Matúš and L. Csirmaz (2016) Entropy region and convolution. *IEEE Trans. Inform. Theory* **62** 6007–6018.

[12] F. Matúš (2017) Classes of matroids closed under the minors and principal extensions. (to appear in *Combinatorica,* Springer-Verlag, 20pp, DOI: 10.1007/s00493-016-3534-y)

[13] J.G. Oxley (2011) *Matroid Theory.* (Second Edition) Oxford Graduate Texts in Mathematics **21** Oxford University Press, Oxford.