COMBINATORICS OF SECRET SHARING

CARLES PADRÓ

Abstract. In this survey talk, the main connections between secret sharing and matroid theory (including polymatroids) are discussed.

Secret sharing was independently introduced in 1979 by Shamir [11] and Blakley [1] as a method to safeguard sensitive information. A secret sharing scheme is a code with a randomized encoding function. Every code word consists of the *secret value* and the *shares* for the *players*. Only the *qualified* sets of players, which form the *access structure*, can recover the secret value from their shares. A secret sharing scheme can be seen as well as a collection of random variables, and, as pointed out by Fujishige [6], their joint Shannon entropies determine a monotone and submodular set function, that is, a *polymatroid.* In the optimal case of a perfect, ideal secret sharing scheme, in which each share has the same size as the secret value, Brickell and Davenport [2] proved that the scheme defines a *matroid* and its access structure is a *port* of that matroid. Linear representations of matroids and polymatroids provide *linear* secret sharing schemes, which are efficient and specially useful in some applications. In general, the matroids and polymatroids determined by secret sharing schemes are *entropic.*

Minimize the size of the shares is a capital problem in secret sharing. Shannon inequalities, which are equivalent to polymatroid axioms, provided the first known lower bounds. Specifically, the first lower bound far from 1 [3] and Csirmaz's [4] lower bound, the best of the currently known ones for the general case. Combined with Seymour's [10] forbidden minor characterization of matroid ports, Shannon inequalities imply a lower bound for all access structures that are not matroid ports [7]. All those lower bounds can be derived from linear programming problems. A recent refinement [5] of that technique improved the lower bounds for a number of access structures on small sets of players.

From the aforementioned developments in secret sharing and other topics in information theory, other classes of matroids beyond the linear and algebraic ones have received a considerable amount of attention. Namely, the *entropic* and *almost entropic* matroids, and the *folded linear* matroids. Remarkable ideas and techniques on entropic matroids were given by Matúš [8], who recently proved that algebraic matroids are almost entropic [9].

References

[1] G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings* 48 (1979) 313–317. https://doi.org/10.1109/MARK.1979.8817296

[2] E.F. Brickell, D.M. Davenport. On the Classification of Ideal Secret Sharing Schemes. *J. Cryptology* 4 (1991) 123–134. https://doi.org/10.1007/BF00196772

[3] R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro. On the Size of Shares for Secret Sharing Schemes. *J. Cryptology* 6 (1993) 157–167. https://doi.org/10.1007/BF00198463

[4] L. Csirmaz. The size of a share must be large. *J. Cryptology* 10 (1997) 223–231. https://doi.org/10.1007/BFb0053420

[5] O. Farràs, T. Kaced, S. Martín, C. Padró. Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing. *IEEE Trans. Inf. Theory* 66(11) (2020) 7088–7100. http://dx.doi.org/10.1109/TIT.2020.3005706

[6] S. Fujishige. Polymatroidal Dependence Structure of a Set of Random Variables. *Information and Control* 39 (1978) 55–72. https://doi.org/10.1016/S0019-9958(78)91063-X

[7] J. Martí-Farré, C. Padró. On secret sharing schemes, matroids and polymatroids. *J. Math. Cryptol.* 4 (2010) 95—120. https://doi.org/10.1515_jmc.2010.004

[8] F. Matúš. Matroid representations by partitions. *Discrete Mathematics* 203 (1999) 169–194. https://doi.org/10.1016/S0012-365X(99)00004-7

[9] F. Matúš. Algebraic matroids are almost entropic. To appear in *Proceedings of the AMS.*

[10] P.D. Seymour. A forbidden minor characterization of matroid ports. *Quart. J. Math. Oxford Ser.* 27 (1976) 407–413. https://doi.org/10.1093/qmath/27.4.407

[11] A. Shamir. How to share a secret. *Commun. of the ACM* 22 (1979) 612–613. https://doi.org/10.1145/359168.359176

Carles Padró; Universitat Politècnica de Catalunya, Barcelona
Email address: carles.padro@upc.edu