Weighted Hierarchical Simple Games

Tatyana Gvozdeva
Supervisor: Arkadii Slinko

Abstract

In many situations cooperating agents have different status with respect to the activity. In the theory of simple games developed by (Neumann & Morgenstern, 1944) seniority of players is modeled by giving them different weights. Such situation, for example, arise in context of corporate voting when different shareholders have different number of shares. The access structure in secret sharing scheme (Simmons, 1990; Stinson, 1992) can also be modeled by a simple game but in this theory a different approach in defining seniority is often used. To this end (Simmons, 1990) introduced the concept of a hierarchical access structure. Such access structure stipulates that agents are partitioned into m levels and a sequence of thresholds $k_1 < k_2 < \ldots < k_m$ is set such that a coalition is authorised if it has either k_1 agents of the first level or k_2 agents of the first two levels or k_3 agents of the first three levels etc. Consider, for example, the situation of a money transfer from one bank to another. If the sum to be transferred is sufficiently large this transaction must be authorised by three senior tellers or two vice-presidents. However, two senior tellers and a vice-president can also authorise the transaction. These hierarchical structures are called *disjunctive* since only one of the m conditions must be satisfied for a coalition to be authorised. If all conditions must be satisfied, the hierarchical access structure is called *conjunctive*.

It was shown that these two approaches are seldom equivalent since hierarchical access structures are seldom weighted. Both (Beimel, Tassa, & Weinreb, 2008) and (Farràs & Padró, 2010) characterised weighted disjunctive hierarchical access structures as a part of their characterisation of weighted ideal access structures. They showed that beyond two levels disjunctive hierarchical structures are normally non-weighted. This is extremely interesting from game-theoretic point of view since we now have a natural class of non-weighted access structures and hence simple games. However, the proof of this characterisation in both papers was indirect. They used the fact that hierarchical access structures are ideal and well-known relation between ideal secret sharing schemes and matroids Conjunctive hierarchical access structures introduced in (Tassa, 2007) have got much less attention. We will use the game-theory methods and terminology and will be talking about hierarchical games, not access structures.

We will show the duality between disjunctive and conjunctive hierarchical games. We introduce a canonical representation theorem for both. We give an idea of a short combinatorial proof of the Beimel-Tassa-Weinreb characterisation theorem of weighted disjunctive hierarchical games. By duality we get similar theorems for conjunctive hierarchical games.

This is a join work with Ali Hameed and Arkadii Slinko

References

Beimel, A., Tassa, T., & Weinreb, E. (2008). Characterizing ideal weighted threshold secret sharing. *SIAM Journal on Discrete Mathematics*, *22*(1), 360-397.

Farràs, O., & Padró, C. (2010). Ideal hierarchical secret sharing schemes. In D. Micciancio (Ed.), *Theory of cryptography* (Vol. 5978, p. 219-236). Springer Berlin / Heidelberg.

Neumann, J. von, & Morgenstern, O. (1944). *Theory of games and economic behavior*. Princeton University Press.

Simmons, G. J. (1990). How to (really) share a secret. In *Proceedings of the 8th annual international cryptology conference on advances in cryptology* (pp. 390–448). London, UK: Springer-Verlag.

Stinson, D. R. (1992). An explication of secret sharing schemes. *Des. Codes Cryptography*, *2*, 357–390.

Tassa, T. (2007). Hierarchical threshold secret sharing. *J. Cryptol.*, *20*, 237–264.