Hierarchity of multipartite access structures

Summary of doctoral thesis

Renata Kawa

A notion of a secret sharing scheme was introduced independently by Blakley and Shamir in 1979. An idea, which is a basis of a secret sharing scheme, is dividing information, called a secret, into pieces that are sent to participants. It is crucial that only some sets of participants are able to recover the secret. These sets are called authorised. A family of authorised sets is called an access structure. It is also important that sets of participants, which are not in the access structure, cannot reconstruct the secret.

The participants, which take part in a secret sharing scheme, do not have to be equivalent to each other, but they belong to the different hierarchies. It is natural that the secret sharing scheme should take into consideration a position of a participant in a hierarchy. An access structure, in which participants are divided into disjoint blocks of people having the same position in a hierarchy, is called a hierarchical access structure.

The hierarchical access structures were first considered by Shamir. They concerned a hierarchy which corresponds to a linear order in a set of blocks. Such access structures are called strict hierarchical access structures. Another family of access structures found in the literature are compartmented access structures, which means that they concern a hierarchy that corresponds to an antilinear order in a set of blocks.

In the first chapter we present basic definitions and facts about secret sharing schemes and access structures. We also study properties of connected and ideal secret sharing schemes. In particular, we show a connection between numbers of elements in independent sets and maximal unauthorised sets of a secret sharing scheme.

Next chapter is dedicated to matroids and polymatroids, since there exists a strong connection between these notions and secret sharing schemes and access structures. We focus mainly on access structures which are determined by uniform polymatroids, hence, among other things, we show a characterization of uniform polymatroids by non-increasing sequences of non-negative integers. What is more, we specify a sufficient and necessary condition for a uniform polymatroid to be a boolean polymatroid.

In the third chapter we present a definition of a hierarchical access structure which generalises notions of strict hierarchical access structures and compartmented access structures. We also introduce a vector representation of sets of participants invented by Farràs, Martí-Farré and Padró. Moreover, we look closer at the history of strict hierarchical access structures and compartmented access structures. Finally, we give a negative answer for a question posed by Tassa.

The fourth chapter is devoted to constructing hierarchical access structures with use of uniform polymatroids, particularly access structures which are neither strict hierarchical nor compartmented. We examine a hierarchy in a family of blocks which are determined by constructed access structures. We also study a connectivity and ideality of obtained access structures. In addition to this, we prove (using boolean uniform polymatroids), that there exist hierarchical access structures, which are neither strict hierarchical nor compartmented, but they are ports of some representable matroids.

The last chapter is slightly different than the previous chapters. Farràs and Padró showed how to compare two sets of participants in strict hierarchical access structure using their vector representations. In this chapter we generalise this results for an arbitrary hierarchical access structure. In order to do that, we use a method that refers to a transportation problem from the area of operational research.