Monotone erasure codes

Annalisa Cimatti

Abstract: Erasure codes are a critical component in reliable storage systems today, and many blockchain systems use consensus protocols that involve erasure codes to reduce their communication cost. Existing erasure codes make it easy to design systems that rely on a threshold failure assumption, meaning that at most a fixed threshold of nodes may fail, regardless of which ones. However, recent blockchain systems have departed from this simple model and use generalized failure assumptions or Byzantine quorum systems, which allow some nodes to be considered more trustworthy than others.

In this talk, we introduce monotone erasure codes, which generalize traditional codes to respect arbitrary trust assumptions characterized by a monotone access structure. We focus on the important concept of linear monotone erasure codes and provide an algorithm to construct a linear monotone erasure code for any given monotone access structure. We then examine an important class of non-threshold access structures used in the practice of cryptocurrencies, and we build an optimal monotone erasure code for these access structures.

Finally, we show how to use monotone erasure codes to obtain a communication-efficient, generalized version of the well-known asynchronous verifiable information dispersal (AVID) primitive, which is a key building block for developing efficient reliable broadcast and consensus protocols.