F-sequences, Hamiltonian cycles in the hypercube and hard problems

Ph. D. Candidate: **Israel Buitrón-Dámaso**
Advisors: **Guillermo Morales-Luna, Feliú Salgols-Troncoso**

September 28, 2018

We review the progress made in the thesis work uptodate. The initial proposal presented in the doctoral research protocol was focused on the study of authentication protocols, namely zero-knowledge proofs (ZKP's), based on hard problems of graph theory. However, this approach was modified. The analysis of the originally considered graph problem showed us the infeasibility for its practical application in cryptographic protocols, so the study was refocused into the area of formal graph theory. Each hypercube is a Hamiltonian graph and the number of Hamiltonian cycles has a doubly-exponential growth. Any Hamiltonian cycle in the hypercube is described by a sequence whose entries are the indexes of the basic directions traversed according to the cycle. These number sequences are called f-sequences (f-seqs). Through elementary transformations, e.g. sequence rotation, sequence reflexion, and some others, the f-seqs are classified into equivalence classes. We have defined a canonical representative of each such class. There is a huge number of cycle classes in the hypercube. Gray's Code is the minimal-lexicographic f-seq and it is particularly interesting due to several properties. Among the representative f-seqs, we have introduced several transformations. For each such transformation we have built a particular trajectory graph: the nodes are the representative f-seqs and the edges result form the transformation, a node and its transformed node form an edge. When considering several transformations, we may consider the (edge) union of the corresponding trajectory graphs. The se are doubly-exponential huge graphs. We will describe several transformations: the clover, the inverted clover, the mushroom and the inverted mushroom. Several problems arise, e.g. which are the minimal transformation sets that produce connected trajectory graphs, for a given transformation, which is the number of connected components in the trajectory graph. We have designed several algorithms for efficient application of transformations and to answer several decision problems, as well as to generate uniformly random representative f-seqs in order to check connectivity and reachability problems, in both versions: decision and search. We have built a C library which implements those algorithms. The library is of the kind GNU build system compatible, which allows an easy installation and function usage and makes it portable.