ACACT Workshop: Open Problems

Open Problems:

Sole: Find a class of codes with a complete decoding algorithm
to implement McEliece PKC as a signature scheme.

Hoory: Is it true that of all the graphs of girth g and average
degree >= d, that the graph with the least number of vertices is
almost regular (say for example, that the minimum and maximum degrees
differ at most by one).

Hoory: The results of our paper enables one to say what is
considered to be a good girth also for irregular graphs.
Working with general graphs is easier when using probabilistic
constructions, so the question is if it is possible using
the probabilistic method to construct graphs with average degree d,
and girth g = (1+epsilon) log_{d-1}(n)
for some constant epsilon > 0.

Litsyn Problem 1: Covering radius of codes with dual distance asymptotically equal 1/2.

Statement: The dual distance of a (nonlinear) code is the first nonzero index for which the MacWilliams transform of the distance distribution vector of the code differs from zero. The covering radius is the maximal distance between a point (vector) in the ambient space and the closest point from the code.

Problem: Prove (or disprove) that the relative (to the length) covering radius tends to zero for every familiy of codes of growing length with the relative dual distance tending to 1/2.

This fact is easy for linear codes, but for nonlinear codes the best known upper bound is due to Tietavainen (see his papers in IEEE Informaion Theory and Designs, Codes and Cryptography, in 1989-1990). For linear codes this problem got much more attention - perhaps due to its relation to estimates of the girth of Cayley graphs using eigenvalues, see papers by Chung et al. For references and most recent results in this direction see
A.Ashikhmin, I.Honkala, T.Laihonen and S.Litsyn,
On relations between covering radius and dual distance,
IEEE Transactions on Information Theory,
vol.45, 6, 1999, pp. 1808--1816.

Litsyn Problem 2. Constructing codes of minimum distance which is greater than half of the length by a constant.

Statement: The best known upper bounds on the size of codes of length n and minimum distance $d=n/2-c_1$ have form $c_2 n$. However, we know only constructions of codes of sizes at most $2n+O(1)$ (from Hadamard or conference matrices), or polynomial in n sizes (e.g. duals of BCH codes) such that the minimum distance jumps to $n/2-c_3 \sqrt{n}$.

Problem: Find (or show that there is no) a construction for codes of size $c_2 n$, $c_2>2$, with minimum distance $d=n/2-c_1$.

For the best upper bounds and references see
I.Krasikov and S.Litsyn, Linear programming bounds for codes of small size, European J. of Combinatorics, vol. 18, 1997, pp.647--656.