On products of linear error correcting codes

Mirandola, D.

STELLINGEN

behorende bij het proefschrift
On Products of Linear Error Correcting Codes
van Diego Mirandola

All codes involved in the following propositions are linear.

1. From combinatorial arguments involving quadratic forms, it follows that the probability that a random code of length n and dimension k fills the whole space is exponentially close to 1 in the difference $k(k+1)/2 - n$, if this difference is at least linear in k.

   Consequently, random codes are not suitable for applications which involve multiplicative properties. (Main Theorem 3.1.2)

2. If a code C of length n satisfies

   $$d_{\min}(C^2) = n - 2\dim C + 2 \geq 2$$

   then, from coding-theoretic analogues of the classical theorems of Kneser and Vosper from additive combinatorics, it follows that C is either a Reed-Solomon code or a direct sum of self-dual codes. (Theorem 4.1.2)

3. An MDS code C of length n and dimension smaller than $(n-1)/2$ is Reed-Solomon if and only if

   $$\dim C^2 = 2\dim C - 1.$$

   This result, together with other consequent results concerning error correcting pairs and code-based secret sharing, supports the idea that certain classes of combinatorial objects assume rich structures when on the boundaries of the parameter space. (Corollary 4.3.6)

4. Using combinatorial arguments in the space of symmetric tensors, it can be shown that there exist "exotic" multiplicative linear secret sharing schemes whose privacy is good but whose product reconstruction function is necessarily non linear. (Main Theorem 5.1.3)

5. If no multiplicative property is required, a secret sharing scheme can be based on a random code.

6. We say that a code is *good* if both its dimension and its minimum distance have positive rate. The existence of good codes whose dual is also good is well-known from classical algebraic coding theory. Recently, it has been proved that there exist good binary codes whose square is also good. However, it is an open problem whether there exist good binary codes whose dual and whose square are *simultaneously* good.

7. A Mathematician Said Who
   Can Quote Me a Theorem that's True?
   For the ones that I Know
   Are Simply not So,
   When the Characteristic is Two!
   (attributed to T. Y. Lam)

   In characteristic 2, the theory of quadratic forms dramatically differs from all other cases. The first peculiarity is that in this case the radical of a quadratic form is not necessarily trivial: if we consider for instance the quadratic form defined by $Q(x) = x^2$ for all $x \in \mathbb{F}_2$, we notice that its associated bilinear form is identically 0, hence the radical equals the whole space, yet Q does not vanish at $x = 1$.

8. Three players are each given a hat, which is either red or blue, and they can see each other but cannot communicate; each player can either guess the colour of his hat or pass and the players have to answer simultaneously; the three players win if at least one or them guesses correctly and none guess incorrectly, and they lose otherwise.

   The knowledge of the theory of error correcting codes gives the best chance of winning this game. Remarkably, increasing the number of players increases the winning rate.