On the construction of high dimensional affine codes whose square code has designed minimum distance

Ignacio García-Marco[1], Irene Márquez-Corbella[1] and Diego Ruano[2]

[1]Universidad de La Laguna and [2]Universidad de Valladolid

iggarcia@ull.es, imarquec@ull.es, diego.ruano@uva.es

Abstract. Given a linear code C, we define its square code C^{*2} as the span of all component-wise products of two elements of C. Our purpose with this work is to answer the following question: which families of affine codes have simultaneously high dimension and high minimum distance of C^{*2}? This work is a tribute to the work of Pellikaan whose contributions to the notion of component-wise products of codes are beyond question. Indeed, he introduced this notion in coding theory for decoding in the 90's.

Component-wise products of linear codes have been used to decode linear codes and to attack some variants of the McEliece cryptosystem, but it has also been used for secure multiparty computation that studies the case where a group of persons, each holding an input for a function, wants to compute the output of the function, without having each individual reveal his or her input to the other parties. Multi-party computation is possible from secret sharing schemes, and hence from coding theory. One of the best known protocols is MiniMac, which uses a linear binary code C, which should prevent cheating. The probability that a cheating player is caught depends on the minimum distance of the square of a linear code, denoted by $d(C^{*2})$, meaning that a high distance on the square will give a higher security. Simultaneously, it would be beneficial to have a high dimension on the code C to reduce the communication cost. Additionally, if the minimum distance of the dual of C and $d(C^{*2}) \geq t+2$, then C can be used to construct a t-strongly multiplicative secret sharing scheme (SSS). Such a SSS is enough to construct an information theoretic secure secret sharing scheme if at most t players are corrupted. These applications show the importance of finding linear codes, where both the code itself and the square has good parameters. Or maybe, to be more specific, that $\dim(C)$, $d(C^{\perp})$, and $d(C^{*2})$ are simultaneously high relative to the length of the codes.

Given $A \subset \mathbb{N}^n$, the affine code C_A is the image of the morphism that evaluates the polynomials in $\mathbb{F}_q[A] = \mathbb{F}_q[\mathbf{x}^\alpha \,|\, \alpha \in A]$ in all the points of $\mathbb{F}_q^n$. Given $d \in \mathbb{Z}^+$, in this work we propose a method to obtain an affine code C satisfying that $d(C^{*2}) \geq d$ and such that $\dim(C)$ is considerably high. Our method receives as input a value $d \in \mathbb{Z}^+$ and starts by considering an affine code C_B such that $d(C_B) \geq d$, say for example, a hyperbolic code with minimum distance at least d. Then, by means of convexity arguments, we build a set $A \subset \mathbb{N}^m$ such that the Minkowski sum $A + A$ is contained in B. The latter condition implies that $d(C_A^{*2}) \geq d(B) \geq d$. Remarkably, in many cases our approach builds a code C such that $d(C^{*2}) \geq d$ and $\dim(C) \geq \dim(D)$ for any code D from the family of weighted Reed-Muller and hyperbolic codes satisfying that $d(D^{*2}) \geq d$.

Partially funded by the Spanish Ministry of Economy/FEDER: grants MTM2015-65764-C3-2-P, MTM2015-69138-REDT, MTM2016-78881-P, MTM2016-80659-P and RYC-2016-20208 (AEI/FSE/UE).