On products of linear error correcting codes

Mirandola, D.

Summary

The product CD of two codes C and D is defined to be the span of all elements of the form xy, where x is in C, y is in D and the product is computed componentwise. The square C^2 of a code C is naturally defined as the product of C with itself. These notions, throughout the last forty years, have appeared in many different fields, such as cryptography, complexity theory, additive combinatorics and cryptanalysis. We show three main results on such products and discuss applications to cryptography. Our methods are typically algebraic-combinatorial in nature, though sometimes probabilistic techniques will be involved.

Our first purpose is to answer the following question: does the square of a code "typically" fill the whole space? We give a positive answer, for codes of dimension k and length roughly $k^2/2$ or smaller. Moreover, the convergence speed is exponential if the difference $k(k+1)/2 - n$ is at least linear in k. The proof uses random coding and combinatorial arguments, together with algebraic tools involving the precise computation of the number of quadratic forms of a given rank, and the number of their zeros. As a consequence of this work, it is impossible to rely on random codes in situations where properties of the code square are required, as it will be the full space, hence trivial, with high probability. This impacts for instance secret sharing: it is known that linear, non-multiplicative secret sharing schemes with optimal privacy and reconstruction parameters can be constructed using random codes; however, due to our results, such schemes will most likely not be arithmetic.

Our second result characterizes Product-MDS pairs of linear codes, i.e. pairs of codes C, D whose product under coordinatewise multiplication has maximum possible minimum distance as a function of the code length and the dimensions $\dim C, \dim D$. We prove in particular, for $C = D$, that if the square of the code C has minimum distance at least 2, and (C, C) is a Product-MDS pair, then either C is a generalized Reed-Solomon code, or C is a direct sum of self-dual codes. The proof is based on new coding-theory analogues of classical theorems of additive combinatorics, namely Kneser's and Vosper's Theorems. More

recently, these techniques have been used to prove that, among all t-strongly multiplicative secret sharing schemes on n players, only Shamir's scheme can achieve the optimal $t = (n-1)/3$.

Finally, we focus on a foundational question which is novel to the best of our knowledge. Multiplicative linear secret sharing is a fundamental notion in the area of secure multiparty computation and, since recently, in the area of two-party cryptography as well. In a nutshell, this notion guarantees that "the product of two secrets is obtained as a linear function of the vector consisting of the coordinatewise product of two respective share-vectors". Suppose we abandon the linearity condition and instead require that this product is obtained by some, not-necessarily-linear "product reconstruction function". Is the resulting notion equivalent to multiplicative linear secret sharing? We show the (perhaps somewhat counter-intuitive) result that this relaxed notion is strictly more general. Concretely, fix a finite field as the base field over which linear secret sharing is considered. Then we show there exists an (exotic) linear secret sharing scheme with an unbounded number of players n such that it has t-privacy with $t = \Omega(n)$ and such that it does admit a product reconstruction function, yet this function is necessarily nonlinear. In addition, we determine the minimum number of players for which those exotic schemes exist. Our proof is based on combinatorial arguments involving quadratic forms. It extends to similar separation results for important variations, such as strongly multiplicative secret sharing.