Limitations on arithmetic codices

This project is about the concept of arithmetic codices which has very interesting applications in cryptography and other areas.

Let K be a field and let S be an (unital, commutative, associative) algebra over K of finite dimension (as a vector space over K) k. Let $n > 0$ be an integer. Consider a K-vector subspace $C \subseteq S \times K^n$. We say a vector $\mathbf{v} \in K^n$ is a "representation" of $x \in S$ (with respect to C) if $(x, \mathbf{v}) \in C$. We require that C is such that every element in S has at least one representation and no vector in K^n may represent two different elements.

Now we look at representations restricted to subsets of the coordinates. We say that C is t-disconnected if, given any subset of t coordinates of a representation we have no information (in a precisely defined mathematical way) about which is the represented element.

On the other hand, we say that C is $(2, n)$-reconstructing if the coordinate-wise product of representations of two elements uniquely determines the product (in S) of these elements. This can be generalized to (d, r)-reconstruction, where we consider products of representations of d elements and where the property still holds if we are given any set of $r \leq n$ coordinates of the product instead of all the n coordinates.

An (n, t, d, r)-codex C for S (over K), where $1 \leq t < r \leq n$, is then a K-vector subspace $C \subseteq S \times K^n$ such that C is t-disconnected and (d, r)-reconstructing.

The description of a codex above can be formalized in a number of equivalent ways. One such formulation appeared in [1] for the case $K = \mathbb{F}_q$, the finite field of q elements and $S = \mathbb{F}_q^k$, under the name of arithmetic secret sharing scheme. But this notion can also be defined in terms of multilinear algebra.

Arithmetic codices have very interesting applications in cryptography, specifically in the area of secret sharing, secure multiparty computation and two party computation (zero knowledge proofs, oblivious transfer from noisy channels...) and other areas of mathematics such as the complexity of multiplications in extension fields. There are several existing results concerning constructions of arithmetic codices for algebras over finite fields $K = \mathbb{F}_q$. Especially interesting is the case of asymptotically good constructions. Here the precise meaning of "asymptotically good" varies depending on each application but we mean that q is fixed, n is unbounded while some of the remaining parameters depend linearly on n. The known asymptotically good constructions for the most interesting applications make use of results from algebraic geometry.

But the other side of the coin is the problem of determining for which parameters no arithmetic codex exists. The known results here use tools which are more elementary in nature. Currently, there is still a large gap between those parameters for which there are known constructions and those for which it is known that no codices exist.

This project concentrates on this latter question of limitations of arithmetic codices. Using some basic results of coding theory, such as the Plotkin bound (which one can find in any book on error correcting codes, such as [2]), combined with some other elementary ideas, we can obtain a series of results that rule out the existence of (n, t, d, r)-codices for some values of n, t, r, d, q and k (the dimension of S). The project would involve that the student gets familiarized with the definitions above and with basic definitions and results about code theory and understand how these are used to prove some of these limitations on the parameters of codices. Furthermore, there are many combinations of the several known basic tools which still remain unexplored and which the student can try to investigate.

Supervisor: Ignacio Cascudo

References

[1] I. Cascudo, R. Cramer and C. Xing. The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing. *Advances in Cryptology: CRYPTO 2011.* Springer Verlag LNCS, Volume 6841/2011, 685-705, 2011.

[2] V. Pless and W. C. Huffman. Fundamentals of Error-Correcting Codes. Cambridge University Press, 2003.