I Encuentro Matemático del Caribe

Noviembre 18 - 19, 2019

Universidad Tecnológica de Bolívar, Cartagena de Indias - Colombia

Quaternary Goppa codes from binary Goppa codes and generalization

Eddie Arrieta Arrieta y Heeralal Janwa (advisor).*

Resumen

We give, what we call, an amalgamated construction from binary codes to Quaternary codes that are linear if self-amalgamated and are Quaternary additive in general.
We construct a Quaternary Goppa code by an amalgamation of two binary classical Goppa codes of the same length and we determine its parameters. We also generalize this construction to Goppa codes over arbitrary finite field $\mathbb{F}_q$, see [2].
We generalize our amalgamated construction taking two different codes, and then one can apply these codes for quantum error-correction. Also, the resulting codes are potentially good for post-quantum cryptosystems.

Palabras & frases claves: Amalgamated code, Cryptosystem, Finite field, Goppa code, Quaternary

1. Introducción

We study non-binary Goppa codes. We have that for a binary Goppa code, $C = \Gamma(L, g(x))$, where $g(x) \in \mathbb{F}_{2^m}[x]$ is a separable polynomial of degree t, the minimum weight of C has a lower bound given by $2t+1$, see [5]. Given a binary Goppa code C, we construct a non-binary code with the same length, dimension and minimum weight of C, which we call amalgamated code. We show that the amalgamated code contains the subfield subcode of C and contains another subset which is additive over $\mathbb{F}_4$ and linear over $\mathbb{F}_2$.

*University of Puerto Rico, e-mail: eddie.arrieta@upr.edu, heeralal.janwa@upr.edu

Really, we generalize the same construction in two way: First we take any linear code, C, over $\mathbb{F}_q$ and we obtain a linear code over $\mathbb{F}_{q^2}$.
Second taking any two linear codes over $\mathbb{F}_q$ and we obtain an additive code over $\mathbb{F}_{q^2}$ and linear over $\mathbb{F}_q$.

1.1. Examples.

We observe that if C_0 is a $[2^{m-1},\ m,\ 2^{m-2}]$ binary linear code and C_1 is a $[2^{m-1}, 1\ 2^{m-1}]$ binary repetition code, then $C_0 \hat{+} C_1$ is an additive Quaternary code which is a binary linear code with parameters $[2^m,\ m+1,\ 2^{m-1}]$.

Referencias

[1] N. Koblitz, A Curse in Number Theory and Cryptography, 2*nd. ed., Spring-Verlag,* (1994)

[2] R. Lidl, H. Niederreiter Introduction to finite fields and their applications Revised edition. ed., Cambridge University Press, 194

[3] F.J. MacWilliams, N.J.A. Sloane The Theory of Error-Correcting Codes, *North-Holland Publishing Company,* 1978

[4] R.J. McEliece A public-Key Cryptosystem Based On Algebraic Coding Theory, *Communication Systems Research Section. January and February* 1978.

[5] R.J. McEliece The Theory of Information and Coding, *Encyclopedia of Mathematics and its Applications. Vol 3.* 19977.

[5] W. W. Peterson, E. J. Weldon Error-Correcting Codes, 2*nd. ed., The Massachusetts Institute of Technology,* (1971).

[7] W. Trappe, L. C. Washington, Introduction to Cryptography with Coding Theory, 2*nd. ed., Pearson Prentice Hall,* (2006).