Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 11 de abril de 2023, 16:00 horas (GMT+1)

Stabilizer quantum codes

Helena Martín-Cruz
Universitat Jaume I[1]

The existence of polynomial time algorithms for prime factorization and discrete logarithms on quantum computers is a clear example that illustrates the importance of quantum computing [4]. Quantum error-correcting codes are essential for this type of computation since they protect quantum information from decoherence and quantum noise. Many of the known quantum error-correcting codes are stabilizer codes. A *stabilizer code* $\mathcal{C} \neq \{0\}$ is the common eigenspace (with respect to the eigenvalue 1) of a commutative subgroup of the error group generated by a suitable error basis on the space $\mathbb{C}^{q^n}$, where $\mathbb{C}$ denotes the complex field, q is a prime power and n is a positive integer. A main advantage of stabilizer quantum error-correcting codes is that they can be constructed from self-orthogonal classical linear codes [3].

Quantum error-correcting codes with good parameters can be constructed from evaluation codes by evaluating polynomials at the roots of the polynomial trace $\mathrm{tr}_{2n}(X) = X + X^q + \cdots + X^{q^{2n-1}} \in \mathbb{F}_{q^{2n}}[X]$ [1] . In this talk, we propose to evaluate polynomials at the roots of trace-depending polynomials $a + \mathrm{tr}_{2n}(h(X))$, where $a \in \mathbb{F}_{q^{2n}}$ and $h(X) \in \mathbb{F}_{q^{2n}}[X]$, and show that this procedure gives rise to stabilizer quantum error-correcting codes with a wider range of lengths than in [1] and with excellent parameters. Namely, we are able to provide new binary records according to [2] and non-binary codes improving the ones available in the literature.

Referencias

[1] C. Galindo, F. Hernando, D. Ruano. *Classical and quantum evaluation codes at the trace roots.* IEEE Trans. Inform. Theory. **65(4)** (2019) 2593-2602.

[2] M. Grassl. Bounds on the minimum distance of linear codes (accessed on 29/06/2022) http://www.codetables.de

[3] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli. *Nonbinary stabilizer codes over finite fields.* IEEE Trans. Inform. Theory. **52(11)** (2006) 4892-4914.

[4] P. W. Shor. *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* In Proc. 35th Ann. Symp. Found. Comp. Sc., IEEE Comp. Soc. Press. (1994) 124-134.

[1]Instituto Universitario de Matemáticas y Aplicaciones de Castellón
Universitat Jaume I
Spain
martinh@uji.es