

## CASTLE CURVES AND CODES

**Fernando Torres**

IMECC/UNICAMP, Brasil

ftorres@ime.unicamp.br

Algebraic Geometry (AG) Codes were introduced by Goppa around 1980, and since then, there have been quantitative and qualitative advances in Coding Theory. The game is to find families of curves having a reasonable easy handling from which codes with excellent parameters could be constructed. For instance, we single out the following type of curves. A nonsingular, projective, geometrically irreducible pointed curve  $(\mathcal{X}, P)$  over the finite field  $\mathbb{F}$  of order  $q$  is called *Castle* if  $\#\mathcal{X}(\mathbb{F})$  attains the Lewittes bound, namely  $1 + q\rho$ , where  $\rho$  is the multiplicity of the Weierstrass semigroup  $H(P)$  at  $P$  with  $H(P)$  being symmetric. For instance, Deligne-Lusztig curves (Hermitian, Suzuki, Ree curves) are outstanding examples of such curves; as a matter of fact, many well-known examples of AG codes arise from Castle curves.

Moreover, Euclidian and Hermitian self-orthogonality properties on AG codes based on Castle curves are often easy to describe and handle; thus one can apply the CSS method in order to produce good quantum codes.

*Joint work with Carlos Munuera (Universidad de Valladolid, España) and Wanderson Tenório (IMECC/UNICAMP, Brasil).*