# Algebraic curves with many rational points over finite fields

Maria Montanucci
Technical University of Denmark

Joint work with: Daniele Bartoli, Peter Beelen, Massimo Giulietti, Leonardo Landi, Vincenzo Pallozzi Lavorante, Luciane Quoos, Guilherme Tizziotti, Fernando Torres, Lara Vicino, Giovanni Zini.

**Abstract**

Algebraic curves over a finite field $\mathbb{F}_q$ and their function fields have been a source of great fascination for number theorists and geometers alike, ever since the seminal work of Hasse and Weil in the 1930s and 1940s. Many important and fruitful ideas have arisen out of this area, where number theory and algebraic geometry meet. For a long time, the study of algebraic curves and their function fields was the province of pure mathematicians. But then, in a series of three papers in the period 1977-1982, Goppa found important applications of algebraic curves over finite fields to coding theory.

The key point of Goppa's construction is that the code parameters are essentially expressed in terms of arithmetic and geometric features of the curve, such as the number $N_q$ of $\mathbb{F}_q$-rational points and the genus $g$.

Goppa codes with good parameters are constructed from curves with large $N_q$ with respect to their genus $g$. Given a smooth projective, algebraic curve of genus $g$ over $\mathbb{F}_q$, an upper bound for $N_q$ is a corollary to the celebrated Hasse-Weil Theorem,

$$N_q \leq q + 1 + 2g\sqrt{q}.$$

Curves attaining this bound are called $\mathbb{F}_q$-maximal. The Hermitian curve $\mathcal{H}$, that is, the plane projective curve with equation

$$X^{\sqrt{q}+1} + Y^{\sqrt{q}+1} + Z^{\sqrt{q}+1} = 0,$$

is a key example of an $\mathbb{F}_q$-maximal curve, as it is the unique curve, up to isomorphism, attaining the maximum possible genus $\sqrt{q}(\sqrt{q}-1)/2$ of an $\mathbb{F}_q$-maximal curve. Other important examples of maximal curves are the Suzuki and the Ree curves. It is a result commonly attributed to Serre that any curve which is $\mathbb{F}_q$-covered by an $\mathbb{F}_q$-maximal curve is still $\mathbb{F}_q$-maximal. In particular, quotient curves of $\mathbb{F}_q$-maximal curves are $\mathbb{F}_q$-maximal. Many examples of $\mathbb{F}_q$-maximal curves have been constructed as quotient curves $\mathcal{X}/G$ of the Hermitian/Ree/Suzuki curve $\mathcal{X}$ under the action of subgroups $G$ of the full automorphism group of $\mathcal{X}$. It is a challenging problem to construct maximal curves that cannot be obtained in this way for some $G$.

In this talk, we will describe our main contributions to both the theory of maximal curves over finite fields and to applications of algebraic curves with many points in coding theory.

In particular, the following three topics will be discussed:

1. Construction of maximal curves;
2. Weierstrass semigroups and points on maximal curves;
3. Algebraic curves with many rational points and coding theory.