A Construction of Curves over Finite Fields

Luciane Quoos
Universidade Federal do Rio de Janeiro, Brazil
e-mail: luciane@im.ufrj.br

The interest on curves over finite fields with many rational points was renewed after Goppa's construction of linear codes with good parameters from such curves (see [Go]).

A celebrated theorem of A. Weil says: Let $\mathcal{X}$ be a nonsingular, projective, geometrically irreducible algebraic curve of genus g defined over a finite field $_q$, then the number $N := \#\mathcal{X}(\ _q)$ of $_q$-rational points of $\mathcal{X}$ satisfies:

$$|N - (q+1)| \leq 2g\sqrt{q}.$$

We introduce (see [G-Q]) an effective method for the construction of curves over finite fields with many rational points. The method is motivated by a recent paper of van der Geer and van der Vlugt [G-V].

For a polynomial $g(x) \in \ _\ell[x]$ of degree bigger or equal to ℓ, we define the *associated reduced polynomial* $R(g(x))$ as the polynomial of degree $\leq (\ell - 1)$ obtained from $g(x)$ by operating on its monomials as follows:

- $R(x^j) = x^j, \quad \forall\ j \leq \ell - 1.$
- $R(x^{\ell+j}) = R(x^{1+j}), \quad \forall\ j \geq 0.$

Note that by the definition of the operator R, we have for an element $\alpha \in \ _\ell$:

$$g(x)(\alpha) = R(g(x))(\alpha).$$

and, in particular, the quocient $g(x)(\alpha)/R(g(x))(\alpha)$ is equal to one for almost all elements in $_\ell$.

In the next theorem we write $\ell = q^n$ and we denote by $\overline{\ }_q$ the algebraic closure of $_q$. For the proof of the theorem we refer to the theory of Kummer extensions of function fields over finite fields in [S].

Theorem : Let $f(x) \in \ _q\ [x]$ be a separable polynomial and let q^j be a power of the characteristic such that $q^j \cdot (\deg f) \geq q^n$. Suppose that the reduced polynomial $R(f(x)^q\ )$ is also separable and that the curve $\mathcal{X}$ given by

$$y^m = \frac{f(x)^q}{R(f(x)^q\ )}, \quad m \text{ a divisor of } (q^n - 1),$$

is absolutely irreducible.

Then the genus g and the number N of rational points of the curve $\mathcal{X}$ over $_q$ satisfy:

$$2g = (\delta + \delta' - 2c - 2)(m-1) + c(m-d) + (m-d') \text{ and } N \geq (q^n - c_1) \cdot m,$$

where $\delta = \deg f(x)$, $\delta' = deg(R(f(x)^q))$, $d = gcd(m, q^j - 1)$, $d' = gcd(m, q^j \cdot \delta - \delta')$ and moreover $c_1 \leq c$ are given by

$$c_1 = \#\{\alpha \in \ _q \mid f(x)(\alpha) = 0\}$$

and

$$c = \#\{\alpha \in \overline{\ }_q \mid f(x)(\alpha) = R(f(x)^q)(\alpha) = 0\}.$$

We illustrate the theorem with an example.

Example : Consider the curve over $_{q^2}$ given by

$$y^m = \frac{(x^{q+1} + x + 1)^q}{x^{q+1} + x^q + 1}, \qquad \text{with } m \text{ a divisor of } (q^2 - 1).$$

By applying the preceeding theorem and comparing the values obtained with the values in the tables [Ge-Vl] and [Sh], we get:

New record				**Complete the table**				**Meet the record**			
Finite Field	m	g	N	Finite Field	m	g	N	Finite Field	m	g	N
$_9$	8	17	74	$_{25}$	6	25	156	$_4$	3	4	15
				$_{25}$	8	35	208	$_{16}$	3	4	45
								$_{16}$	15	40	225
								$_9$	2	2	20

References

[G-Q] A. Garcia and L. Quoos, *A Construction of Curves over Finite Fields* , to appear in Acta Arithmetica.

[G-V] G. van der Geer and M. van der Vlugt, *Kummer Covers with Many Points*, math. AG/9909037.

[Ge-Vl] G. van der Geer and M. van der Vlugt, *Tables of Curves with Many Points*, available at http://www.wins.uva.nl/~geer .

[Go] V.D. Goppa, *Codes on Algebraic Curves*, Sov. Math. Dokl. 24 (1981), 170–172.

[Sh] V. Shabat, *Tables of curves with many points*, available at http://www.turing.wins.uva.nl/~shabat/tables.html .

[S] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.