# Maximal Curves Covered by the Hermitian Curve

Carmen Rovi and Milagros Izquierdo

*Matematiska Institutionen, Linköpings Universitet, SE-58183 Linköping. Sweden.*

**Abstract**

By implementing the methods given in [2] and [3] we have been able to define new lower bounds for 77 entries in the tables of curves with many rational points given in http: //wins.uva.nl/˜geer. In fact, as the curves found are maximal, these entries no longer need a bound and they can be given by a unique entry, since the exact value of $N_q(g)$ is now known.

*Keywords:*
Rational Points, Maximal Curve, Finite Field, Genus

## 1. Introduction

After Goppa's construction of algebraic geometric codes in 1980, a new interest arose in the study of curves over finite fields. For the applications to coding theory and cryptography it is specially important to have the explicit equations for curves with many rational points (see [11], [12]). Curves that attain the maximum possible number of rational points are called maximal curves, and they attain the Hasse-Weil upper bound,

$$N_q(g) \leq q + 1 + [2g\sqrt{q}]$$

where $q$ is the order of the finite field and $g$ is the genus of the curve.

In their article "Tables of Curves with Many Points", Gerhard van der Geer and Marcel van der Vlugt present several tables giving the best bounds for the number of rational points on curves over finite fields of genera up to 50.

The tables were initially constructed for curves over finite fields $\mathbb{F}_q$ where $q = 2^m$ with $1 \leq m \leq 7$, and $q = 3^m$ with $1 \leq m \leq 4$. Afterwards they have been extended to consider finite fields of characteristic up to 97. The genera

of the curves under consideration is $g \leq 50$. Regularly updated tables can be found at

http: //wins.uva.nl/~geer

The entries of the table give the value of $N_q(g)$, that is, the number of rational places of the corresponding curve.

When the entry consists of a unique number, it represents the exact value for $N_q(g)$.

Some entries are given as ranges since the exact value for $N_q(g)$ is not known. In this case the smaller number means that there exist curves for the corresponding $\mathbb{F}_q$ and genus $g$ with at least that number of rational points, and the bigger number is given by the best upper bound for $N_q(g)$.

Finally, there are some missing entries in the tables. The reason for these missing entries is that if for a given $\mathbb{F}_q$ and a genus $g$, a curve is known to have at least a number $a$ of rational points, but the upper bounds of rational points are much bigger, then the curve is discarded. Such a curve cannot be considered to have many rational points since the upper bound tells us that it could have many more rational points.

## 2. Maximal curves over $\mathbb{F}_{\ell^2}$ covered by the Hermitian Curve

In [9] a list of different methods used for the construction of curves with many points is given. In his article "Curves over Finite Fields Attaining the Hasse-Weil Upper Bound", Arnaldo García concentrates upon maximal curves and considers the determination of the possible genera of these curves (see also [1], [7]). A. García also goes further to determine explicit equations for maximal curves; i.e. curves which attain the Hasse-Weil upper bound.

The crucial point is provided by Serre who has shown that a curve over $\mathbb{F}_{\ell^2}$ covered by a maximal curve also over $\mathbb{F}_{\ell^2}$ is itself maximal. (A. García [2] and Serre [6])

The Hermitian curve,

$$y^\ell + y = x^{\ell+1} \text{ over } \bar{\mathbb{F}}_{\ell^2}(x, y)$$

is a maximal curve and the genus of this curve is given by

$$g = \frac{1}{2}\ell(\ell - 1)$$

The Hermitian curve is in fact the unique maximal curve over $\mathbb{F}_{\ell^2}$ with genus $g = \ell(\ell - 1)/2$.

As stated by Arnaldo García in [2], there is no known example of a maximal curve which cannot be covered by the Hermitian curve. But it is not yet known whether all maximal curves are in fact covered by Hermitian curves.

As shown in [2] and [3] we can find explicit equations of curves over $\mathbb{F}_{\ell^2}$ covered by the Hermitian curve also over $\mathbb{F}_{\ell^2}$.

The curve over $\mathbb{F}_{\ell^2}$

$$y^\ell + y = x^m, \text{ where } m \text{ is a divisor of } (\ell + 1)$$

is covered by the Hermitian curve $y^\ell + y = x^{\ell+1}$ over $\mathbb{F}_{\ell^2}$. So $y^\ell + y = x^m$ with $m|(\ell + 1)$ is maximal. Nevertheless, this curve does not have maximum genus.

The genus of this curve is given by

$$g = \frac{1}{2}(m - 1)(\ell - 1)$$

Using this idea we can find explicit equations for maximal curves providing new entries which are listed in TABLE 1.

In [3] it is shown that

$$z^n = t(t + 1)^{\ell-1}, \quad \text{with } n \text{ a divisor of } (\ell^2 - 1)$$

is the equation of a maximal curve over $\mathbb{F}_{\ell^2}$ with genus given by

$$g = (n - \delta)/2, \text{ where } \delta = gcd(n, \ell - 1)$$

From this idea we have been able to find the new entries listed in TABLE 2.

## 3. Results

Following the arguments given in [2] and [3] we can find several new entries for the tables in http: //wins.uva.nl/˜geer. Unlike other methods for constructing curves with many rational points like the ones presented in [10] or [8], the ideas presented in [2] and [3] work for relatively large orders of the finite field, since they keep the genera within bounds. Thus, we have found explicit curves over $\mathbb{F}_q$, where $q$ is a square, which are covered by the Hermitian curve, also over $\mathbb{F}_q$. These curves are maximal by [2] and hence they provide a unique entry for the tables, since the maximum number of rational points for the corresponding genus and order of finite field is attained. Some of the entries in Table 1 are given in [5]

TABLE 1

| **Explicit Curve** | **Finite Field** $\mathbb{F}_q$ | **Genus** $g$ | **Number of Rational Points** $N_q(g)$ |
|---|---|---|---|
| $y^5 + y = x^3$ | $q = 5^2$ | $g = 4$ | $N_q(g) = 66$ |
| $y^5 + y = x^6$ | $q = 5^2$ | $g = 10$ | $N_q(g) = 126$ |
| $y^{25} + y = x^2$ | $q = 5^4$ | $g = 12$ | $N_q(g) = 1226$ |
| $y^7 + y = x^4$ | $q = 7^2$ | $g = 9$ | $N_q(g) = 176$ |
| $y^7 + y = x^8$ | $q = 7^2$ | $g = 21$ | $N_q(g) = 344$ |
| $y^{49} + y = x^2$ | $q = 7^4$ | $g = 24$ | $N_q(g) = 4754$ |
| $y^{11} + y = x^2$ | $q = 11^2$ | $g = 5$ | $N_q(g) = 232$ |
| $y^{11} + y = x^3$ | $q = 11^2$ | $g = 10$ | $N_q(g) = 342$ |
| $y^{11} + y = x^4$ | $q = 11^2$ | $g = 15$ | $N_q(g) = 452$ |
| $y^{11} + y = x^6$ | $q = 11^2$ | $g = 25$ | $N_q(g) = 672$ |
| $y^{13} + y = x^2$ | $q = 13^2$ | $g = 6$ | $N_q(g) = 326$ |
| $y^{13} + y = x^7$ | $q = 13^2$ | $g = 36$ | $N_q(g) = 1106$ |
| $y^{17} + y = x^2$ | $q = 17^2$ | $g = 8$ | $N_q(g) = 562$ |
| $y^{17} + y = x^3$ | $q = 17^2$ | $g = 16$ | $N_q(g) = 834$ |
| $y^{17} + y = x^6$ | $q = 17^2$ | $g = 40$ | $N_q(g) = 1650$ |
| $y^{19} + y = x^2$ | $q = 19^2$ | $g = 9$ | $N_q(g) = 704$ |
| $y^{19} + y = x^4$ | $q = 19^2$ | $g = 27$ | $N_q(g) = 1388$ |
| $y^{19} + y = x^5$ | $q = 19^2$ | $g = 36$ | $N_q(g) = 1730$ |

TABLE 2

| **Explicit Curve** | **Finite Field $\mathbb{F}_q$** | **Genus $g$** | **Number of Rational Points $N_q(g)$** |
|---|---|---|---|
| $z^{16} = t(t+1)^{24}$ | $q = 5^4$ | $g = 4$ | $N_q(g) = 826$ |
| $z^{48} = t(t+1)^{24}$ | $q = 5^4$ | $g = 6$ | $g = 12$ $N_q(g) = 926$ $N = 1226$ |
| $z^{52} = t(t+1)^{24}$ | $q = 5^4$ | $g = 18$ | $g = 24$ $N_q(g) = 1526$ $N = 1826$ |
| $z^{13} = t(t+1)^{24}$ | $q = 5^4$ | $g = 24$ | $g = 6$ $N_q(g) = 1826$ $N = 926$ |
| $z^{104} = t(t+1)^{24}$ | $q = 5^4$ | $g = 36$ | $g = 48$ $N_q(g) = 2426$ $N = 3026$ |
| $z^{26} = t(t+1)^{24}$ | $q = 5^4$ | $g = 48$ | $g = 12$ $N_q(g) = 3026$ $N = 1226$ |
| $z^{10} = t(t+1)^{48}$ | $q = 7^4$ | $g = 4$ | $N_q(g) = 2794$ |
| $z^{15} = t(t+1)^{48}$ | $q = 7^4$ | $g = 6$ | $N_q(g) = 2990$ |
| $z^{32} = t(t+1)^{48}$ | $q = 7^4$ | $g = 8$ | $N_q(g) = 3186$ |
| $z^{30} = t(t+1)^{48}$ | $q = 7^4$ | $g = 12$ | $N_q(g) = 3578$ |
| $z^{40} = t(t+1)^{48}$ | $q = 7^4$ | $g = 16$ | $N_q(g) = 3970$ |
| $z^{80} = t(t+1)^{48}$ | $q = 7^4$ | $g = 32$ | $N_q(g) = 5538$ |
| $z^{75} = t(t+1)^{48}$ | $q = 7^4$ | $g = 36$ | $N_q(g) = 5930$ |
| $z^{120} = t(t+1)^{48}$ | $q = 7^4$ | $g = 48$ | $N_q(g) = 7106$ |
| $z^{24} = t(t+1)^{10}$ | $q = 11^2$ | $g = 11$ | $N_q(g) = 364$ |
| $z^{16} = t(t+1)^{120}$ | $q = 11^4$ | $g = 4$ | $N_q(g) = 15610$ |
| $z^{48} = t(t+1)^{120}$ | $q = 11^4$ | $g = 12$ | $N_q(g) = 17546$ |
| $z^{80} = t(t+1)^{120}$ | $q = 11^4$ | $g = 20$ | $N_q(g) = 19482$ |
| $z^{61} = t(t+1)^{120}$ | $q = 11^4$ | $g = 30$ | $N_q(g) = 21902$ |
| $z^{21} = t(t+1)^{12}$ | $q = 13^2$ | $g = 9$ | $N_q(g) = 404$ |
| $z^{28} = t(t+1)^{12}$ | $q = 13^2$ | $g = 12$ | $N_q(g) = 482$ |
| $z^{42} = t(t+1)^{12}$ | $q = 13^2$ | $g = 18$ | $N_q(g) = 638$ |
| $z^{56} = t(t+1)^{12}$ | $q = 13^2$ | $g = 24$ | $g = 26$ $N_q(g) = 794$ $N = 846$ |
| $z^{16} = t(t+1)^{168}$ | $q = 13^4$ | $g = 4$ | $N_q(g) = 29914$ |
| $z^{15} = t(t+1)^{168}$ | $q = 13^4$ | $g = 6$ | $N_q(g) = 30590$ |
| $z^{20} = t(t+1)^{168}$ | $q = 13^4$ | $g = 8$ | $N_q(g) = 31266$ |
| $z^{48} = t(t+1)^{168}$ | $q = 13^4$ | $g = 12$ | $N_q(g) = 32618$ |
| $z^{35} = t(t+1)^{168}$ | $q = 13^4$ | $g = 14$ | $N_q(g) = 33294$ |
| $z^{40} = t(t+1)^{168}$ | $q = 13^4$ | $g = 16$ | $N_q(g) = 33970$ |
| $z^{60} = t(t+1)^{168}$ | $q = 13^4$ | $g = 24$ | $N_q(g) = 36674$ |
| $z^{112} = t(t+1)^{168}$ | $q = 13^4$ | $g = 28$ | $N_q(g) = 38026$ |

| **Explicit Curve** | **Finite Field $\mathbb{F}_q$** | **Genus $g$** | **Number of Rational Points $N_q(g)$** |
|---|---|---|---|
| $z^{68} = t(t+1)^{168}$ | $q = 13^4$ | $g = 32$ | $N_q(g) = 39378$ |
| $z^{80} = t(t+1)^{168}$ | $q = 13^4$ | $g = 36$ | $N_q(g) = 40730$ |
| $z^{105} = t(t+1)^{168}$ | $q = 13^4$ | $g = 42$ | $N_q(g) = 42758$ |
| $z^{120} = t(t+1)^{168}$ | $q = 13^4$ | $g = 48$ | $N_q(g) = 44786$ |
| $z^{12} = t(t+1)^{16}$ | $q = 17^2$ | $g = 4$ | $N_q(g) = 426$ |
| $z^{72} = t(t+1)^{16}$ | $q = 17^2$ | $g = 32$ | $N_q(g) = 1378$ |
| $z^{10} = t(t+1)^{288}$ | $q = 17^4$ | $g = 4$ | $N_q(g) = 85834$ |
| $z^{15} = t(t+1)^{288}$ | $q = 17^4$ | $g = 6$ | $N_q(g) = 86990$ |
| $z^{20} = t(t+1)^{288}$ | $q = 17^4$ | $g = 8$ | $N_q(g) = 88146$ |
| $z^{30} = t(t+1)^{288}$ | $q = 17^4$ | $g = 12$ | $N_q(g) = 90458$ |
| $z^{29} = t(t+1)^{288}$ | $q = 17^4$ | $g = 14$ | $N_q(g) = 91614$ |
| $z^{64} = t(t+1)^{288}$ | $q = 17^4$ | $g = 16$ | $N_q(g) = 92770$ |
| $z^{45} = t(t+1)^{288}$ | $q = 17^4$ | $g = 18$ | $N_q(g) = 93926$ |
| $z^{60} = t(t+1)^{288}$ | $q = 17^4$ | $g = 24$ | $N_q(g) = 97394$ |
| $z^{58} = t(t+1)^{288}$ | $q = 17^4$ | $g = 28$ | $N_q(g) = 99706$ |
| $z^{80} = t(t+1)^{288}$ | $q = 17^4$ | $g = 32$ | $N_q(g) = 102018$ |
| $z^{90} = t(t+1)^{288}$ | $q = 17^4$ | $g = 36$ | $N_q(g) = 104330$ |
| $z^{87} = t(t+1)^{288}$ | $q = 17^4$ | $g = 42$ | $N_q(g) = 107798$ |
| $z^{192} = t(t+1)^{288}$ | $q = 17^4$ | $g = 48$ | $N_q(g) = 111266$ |
| $z^{10} = t(t+1)^{18}$ | $q = 19^2$ | $g = 4$ | $N_q(g) = 514$ |
| $z^{15} = t(t+1)^{18}$ | $q = 19^2$ | $g = 6$ | $N_q(g) = 590$ |
| $z^{30} = t(t+1)^{18}$ | $q = 19^2$ | $g = 12$ | $N_q(g) = 818$ |
| $z^{45} = t(t+1)^{18}$ | $q = 19^2$ | $g = 18$ | $N_q(g) = 1046$ |
| $z^{40} = t(t+1)^{18}$ | $q = 19^2$ | $g = 19$ | $N_q(g) = 1084$ |
| $z^{16} = t(t+1)^{360}$ | $q = 19^4$ | $g = 4$ | $N_q(g) = 133210$ |
| $z^{48} = t(t+1)^{360}$ | $q = 19^4$ | $g = 12$ | $N_q(g) = 138986$ |
| $z^{80} = t(t+1)^{360}$ | $q = 19^4$ | $g = 20$ | $N_q(g) = 144762$ |
| $z^{144} = t(t+1)^{360}$ | $q = 19^4$ | $g = 36$ | $N_q(g) = 156314$ |

## References


[1] R.Fuhrmann, F. Torres *The Genus of Curves over Finite Fields with many Rational Points*, Manuscripta Math., 89, 103-106, 1996.

[2] A. García *Curves over Finite Fields Attaining the Hasse-Weil Upper Bound*, Progress in Mathematical Physics, Birkhäuser-Verlag, Basel, v. 202, p. 199-205, 2001.

[3] A. García, H. Stichtenoth and C.P.Xing *On Subfields of the Hermitian Function Field*, Compositio Math., 120, 137-170, 2000.

[4] J. W. P. Hirschfeld, G. Korchmáros and F. Torres *Algebraic Curves over a Finite Field*, Princeton Series in Applied Mathematics, 2008.

[5] C. Rovi, *Algebraic Curves over Finite Fields. Master's Thesis*, Linköping University, Sweden. Available at http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-56761, 2010.

[6] J.-P. Serre *Sur le Nombre de Points Rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math., 296, 397-402, 1983.

[7] H. Stichtenoth, C.P. Xing *The Genus of maximal Function Fields over Finite Fields*, Manuscripta Math., 86, 217-224, 1995.

[8] G. van der Geer and M. van der Vlugt, *Constructing curves over finite fields with many points by solving linear equations*, Applications of Curves over Finite Fields (M.D. Fried, ed.), Contemporary Math., Vol. 245, pp. 41-47, American Math. Society, Providence, RI, 1999.

[9] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, Math. Comp. 69, 797-810, 2000.

[10] G. van der Geer and M. van der Vlugt, *Kummer covers with many points*, Finite Fields Appl. 6, 327-341, 2000.

[11] H. van Lint and G. van der Geer, *Introduction to coding theory and algebraic geometry*, Birkhäuser, Basel, Boston, Berlin, 1988.

[12] J. L. Walker, *Codes and Curves*, AMS in the IAS/Park City Mathematical Subseries of the Student Mathematical Series.