Yet More Projective Curves over $\mathbb{F}_2$

Chris Lomont

CONTENTS

2000 AMS Subject Classification: Primary 14H45; Secondary 11T71, 94B

Keywords: Error correcting codes, low genus curves, curves over finite fields

All plane curves of degree less than 7 with coefficients in $\mathbb{F}_2$ are examined for curves with a large number of $\mathbb{F}_q$ rational points on their smooth model, for $q = 2^m, m = 3, 4, ..., 11$. Known lower bounds are improved, and new curves are found meeting or close to Serre's, Lauter's, and Ihara's upper bounds for the maximal number of $\mathbb{F}_q$ rational points on a curve of genus g.

1. INTRODUCTION

Let $\mathbb{F}_q$ denote the finite field with q elements. All absolutely irreducible homogeneous polynomials $f \in \mathbb{F}_2[x, y, z]$ of degree less than 7 are examined for those with a large number of $\mathbb{F}_q$ rational points, $q = 2^m, m = 3, 4, 5, ..., 11$, extending the results in [Moreno et al. 95]. A brute force search obtained all rational points for each polynomial of a given degree. The resulting list of polynomials with many rational points, perhaps with singularities, were then studied to determine if resolving singularities would add more rational points on the smooth model. The result is an exhaustive search of all curves resulting from desingularizing a homogeneous polynomial of degree less than 7 in $\mathbb{F}_2[x, y, z]$.

In this paper, first known bounds on the maximal number of $\mathbb{F}_q$ rational points of a genus g curve are recalled, along with some theorems that speed up the computations. Then the computation is described in some detail. A listing of the best found polynomials is given for each genus, so that one can check the claimed number of rational points on each curve. Finally the new lower bounds are listed in a table for each $\mathbb{F}_q$ and genus combination.

2. GENUS BOUNDS AND IRREDUCIBILITY TESTS

Let $f \in \mathbb{F}_2[x, y, z]$ be an absolutely irreducible homogeneous polynomial; f defines a projective plane curve C. Let $\tilde{C}$ be the smooth model, and g its genus. Some bounds on the genus can be deduced from knowing the number of $\mathbb{F}_q$ rational points in the plane and the number of singularities in the plane. $N_q(g)$ is the

maximum number of $\mathbb{F}_q$-rational points on a curve of genus g. Serre's bound [Serre 83] on $N_q(g)$ is

$$|N_q(g) - (q+1)| \leq g\lfloor 2\sqrt{q}\rfloor$$

where $\lfloor\alpha\rfloor$ is the integral part of α. This gives

$$N_q(g) \leq (q+1) + g\lfloor 2\sqrt{q}\rfloor;$$

so if there is an integer g_0 such that

$$q + 1 + g_0\lfloor 2\sqrt{q}\rfloor < p,$$

where p is the point count on the particular curve C in question, then $g_0 < g$. If the number of singularities is r, and the degree of the polynomial f is d, then

$$g \leq \frac{(d-1)(d-2)}{2} - r.$$

To get an estimate of the total number of points possible on the smooth model $\tilde{C}$ resulting from blowing up singularities, the following estimate was used.

Theorem 2.1. *Let $C \subseteq \mathbb{P}^2$ be a plane curve of degree d with singularities $P_1, P_2, ..., P_r$, with multiplicities $m_1, m_2, ..., m_r$, for $r \geq 2$. Then $\sum_{i=1}^{r} m_i \leq \lfloor \frac{d}{2}\rfloor r + 1$ if d is odd, and $\sum_{i=1}^{r} m_i \leq \lfloor \frac{d}{2}\rfloor r$ if d is even.*

So the number of points obtained from blowing up singularities is bounded above by $\lfloor \frac{d}{2}\rfloor r + 1$.

Proof: By Bezout's theorem, a line through any 2 singularities P_i and P_j implies $m_i + m_j \leq d$. Thus at most one singularity can have multiplicity $> d/2$, and the result follows. □

More details on resolution of curve singularities can be found in [Hartshore 77] and [Walker 62].

To test for absolute irreducibility the following was used [Ragot 98]:

Definition 2.2. Let k be a field. The polynomial $f \in k[x_1, x_2, ..., x_n]$ has a **simple solution** at a point $P \in k^n$ if $f \in I(P) \setminus I(P)^2$, with $I(P)$ being the ideal of polynomials vanishing at P.

Theorem 2.3. *If $f \in k[x_1, x_2, ..., x_n]$ is irreducible over the perfect field k and has a simple solution in k^n, then f is absolutely irreducible.*

Proof: Since f is irreducible over k, its absolutely irreducible factors are conjugate over k. If $P \in k^n$ is a root of one of the factors, it must be a root of the others. But P only vanishes to order 1, thus f has one factor, and is absolutely irreducible. □

The number of $\mathbb{F}_q$ points on a plane curve can be computed directly by brute force, as can lower bounds on the number of singularities, and then the above inequalities can be used to obtain bounds on the genus. Given a polynomial f, the number of rational points computed on it, and the number of singularities found, upper and lower bounds on the possible genus are obtained. This speeds up the search by removing curves that have uninteresting combinations of genus and rational point count early in the computation.

3. COMPUTATION

3.1 Storing Polynomials Compactly

All $\mathbb{F}_q$ rational points were found on each homogeneous polynomial of degree ≤ 5 in $\mathbb{F}_2[x, y, z]$, for $q = 2^m, m = 3, 4, ..., 11$. Due to the the time requred, degree 6 homogeneous polynomials were examined only for $m = 3, 4, ..., 9$.

The most time consuming part was counting the number of $\mathbb{F}_q$-rational points on each plane curve. This was done with a C program using exhaustive search. Several ideas were used to reduce the complexity at each stage. Degree 6 computations will be described; the other degrees are similar. The code was checked for correctness by comparing the degree ≤ 5 results with [Moreno et al. 95], and in the process a few curves were found that were previously overlooked.

First, each homogeneous polynomial can be represented uniquely by a 32-bit integer, using each bit to signify the presence of a certain monomial in the polynomial. In degree 6, there are $\binom{6+2}{2} = 28$ different monomials of the form $x^i y^j z^k$ with $i + j + k = 6$ and $0 \leq i, j, k$. Each bit from 0 to 27 denotes the presence of a monomial, and the mapping $\alpha : \{\textit{homogeneous degree } 6\ f \in \mathbb{F}_2[x, y, z]\} \to \{1, 2, ..., 2^{28} - 1\}$ thus defined is a bijection. Thus each homogeneous polynomial $f \in \mathbb{F}_2[x, y, z]$ of degree 6 corresponds to a unique integer between 1 and $2^{28} - 1 \approx 268$ million.

3.2 Reducing Computation Time

To reduce the number of polynomials searched, equivalent ones under the action of $GL_3(\mathbb{F}_2)$ on the variables x, y, z were removed. To fit the entire degree-6 computation in memory, a bit table of 32 megabytes of RAM was used, with the position of each bit representing the number of a polynomial using the above bijection. All bits were set to 1, denoting all polynomials are still in the search space. Then the orbit of each polynomial under $GL_3(\mathbb{F}_2)$ was removed from the bit table, and the

polynomial in each orbit requiring the least computation to evaluate was written to a data file. Since the size of $GL_3(\mathbb{F}_2)$ is 168, this was expected to give approximately a 168-fold decrease in the number of curves needing to be searched (not exactly 168 since some polynomials are invariant under some automorphisms). By using the representative of each orbit requiring the least work to evaluate, the search time was reduced significantly (see below). This trimmed the 268 million degree-6 polynomials down to 1.6 million. Also, clearly reducible polynomials, such as those with all even exponents or divisible by a variable, were removed at this point. At each stage, data was saved to prevent having to rerun any step.

Because of speed considerations, table lookup was used to find solutions, so in each orbit the polynomial needing the fewest number of lookups was selected. By choosing the representative with the fewest number of lookups as opposed, for example, to the polynomial with the lowest value of $\alpha(f)$ defined above, 12 million lookups were removed from polynomials of degree 6, resulting in over 3 trillion operations removed during rational point counting.

3.3 Timing

After the C program computes all the $\mathbb{F}_q$-rational points, the points were tested for singularities (a singularity will add an additional $\mathbb{F}_q$ rational point only if it comes from resolving a $\mathbb{F}_q$ rational singularity). The computation up to this point took about 80 hours of computer time on a Pentium III 800 MHZ. Using the bounds above on the genus and possible ranges for number of $\mathbb{F}_q$ rational points on the smooth model, the program searched all curves for those with a large number of possible $\mathbb{F}_q$ rational points for each genus and field combination, and all such curves were written out to be examined. If the genus of one of these curves was not forced to be unique using the bounds, the program KANT [Kant 00] was used to compute the genus, and this data was incorporated into the C program, and another pass was run. Due to the large number of degree-6 curves, and the length of time to compute the genus of all of them, not all degree-6 curves of genus ≤ 5 were identified. All curves of degree 6, genus ≥ 6 were identified. The C program also found simple points over $\mathbb{F}_2$ to apply the irreducibility theorem above, and then Maple V [Maple 00] was used to test for irreducibility since it has multivariable factoring algorithms over finite fields. For 12 curves of degree 6, there were no simple $\mathbb{F}_2$ points, so $\mathbb{F}_4$ simple points were used. For 2 of these curves there were no such simple $\mathbb{F}_4$ points, so $\mathbb{F}_8$ simple points were used. This turned out to suffice to check absolute irreducibility of all polynomials in this paper. The C program also found the singularity types of the $\mathbb{F}_2$ singularities for visual inspection to see if there were clearly more rational points on the smooth model. The package of [Haché and Le Brigand 95] was not available to do a more detailed singularity analysis, thus some of the bounds below may be improved by looking for rational points over a wider class of singularities than the $\mathbb{F}_2$ singularities considered here.

The final C code can be found at [Lomont 00].

4. Computational Results

For each field and genus combination, polynomials are listed that result in the largest found number of rational points on the smooth model of the curve. For fields $\mathbb{F}_q$, $q = 2^m, m = 3, 4, .., 11$, all homogeneous polynomials in $\mathbb{F}_2[x, y, z]$ of degree ≤ 5 were searched. For $m = 3, 4, ...9$, the search was extended to include all degree-6 homogeneous polynomials in $\mathbb{F}_2[x, y, z]$. For genus and field combinations not listed here, see [Moreno et al. 95].

Remark 4.1. The four polynomials found in [Moreno et al. 95] of degree 4, genus 3, with 113 rational points over $\mathbb{F}_{64}$, are only 2 distinct polynomials modulo the action of $GL_3(\mathbb{F}_2)$ on the variables x, y, z.

4.1 $\mathbb{F}_8$

A curve of genus 3 with the maximal number of smooth points, 24, is the Klein Quartic

$$x^3\,y + y^3\,z + x\,z^3.$$

A genus 5 curve with 28 planar smooth points is

$$x^6 + x^5\,y + x^3\,y^3 + y^6 + y^5\,z + y^4\,z^2 + \left(x^3 + x\,y^2 + y^3\right) z^3 + \left(x^2 + x\,y\right)\, z^4 + x\,z^5.$$

Note: A reviewer remarked that a genus 5 curve is known with 29 points [van der Geer and van der Vlugt 03].

A genus 6 curve, with 33 planar smooth points is

$$x^4\,y^2 + x^3\,y^3 + x\,y^5 + x\,y^4\,z + y^4\,z^2 + \left(x^2 + y^2\right)\, z^4 + y\,z^5.$$

A curve of genus 7 with 33 smooth planar points is

$$x^6 + x^5y + x^4y^2 + x^3y^3 + y^6 + y^5z + \left(x^2\,y^2 + xy^3 + y^4\right) z^2 + \left(x^2\,y + x\,y^2\right)\, z^3 + \left(x^2 + x\,y + y^2\right)\, z^4.$$

A genus 8 curve with 33 smooth planar points is

$$x^5\,y + x^2\,y^4 + x\,y^5 + y^6 + \left(x^4\,y + x^2\,y^3\right)\, z + x^3\,y\,z^2 + \left(x^3 + x\,y^2\right)\, z^3 + x\,y\,z^4 + y\,z^5.$$

Two curves of genus 9, each with 33 smooth planar points:

$$f_1 = x^5\,y + x^4\,y^2 + x^2\,y^4 + \left(x^3\,y^2 + x^2\,y^3\right)\,z + x^4\,z^2 + \left(x\,y^2 + y^3\right)\,z^3 + x^2\,z^4 + x\,z^5 + z^6.$$

$$f_2 = x^6 + x^4\,y^2 + x^3\,y^3 + x^2\,y^4 + x^3\,y^2\,z + \left(x^4 + x^3\,y + x\,y^3\right)\,z^2 + y^3\,z^3 + (x+y)\,z^5 + z^6.$$

Five curves of genus 10 with 35 smooth points in the plane:

$$f_1 = x^5\,y + x^2\,y^4 + y^6 + \left(x^3\,y^2 + x\,y^4 + y^5\right)\,z + y^4\,z^2 + \left(x^2\,y + x\,y^2\right)\,z^3 + \left(x^2 + y^2\right)\,z^4 + x\,z^5.$$

$$f_2 = x^5\,y + x^4\,y^2 + x^3\,y^3 + x\,y^5 + y^6 + x^2\,y^3\,z + \left(x^4 + x^2\,y^2 + x\,y^3\right)\,z^2 + x^3\,z^3 + y^2\,z^4 + x\,z^5 + z^6.$$

$$f_3 = x^5\,y + x^4\,y^2 + x^2\,y^4 + \left(x^4\,y + y^5\right)\,z + \left(x^4 + x\,y^3\right)\,z^2 + x^3\,z^3 + \left(x^2 + y^2\right)\,z^4 + y\,z^5 + z^6.$$

$$f_4 = x^5\,y + x^3\,y^3 + x^2\,y^4 + \left(x^5 + x^2\,y^3 + y^5\right)\,z + \left(x^2\,y + y^3\right)\,z^3 + x^2\,z^4 + (x+y)\,z^5 + z^6.$$

$$f_5 = x^4\,y^2 + x^2\,y^4 + x\,y^5 + x^5\,z + x\,y^3\,z^2 + \left(x^3 + x^2\,y\right)\,z^3 + \left(x^2 + y^2\right)\,z^4 + x\,z^5.$$

4.2 $\mathbb{F}_{16}$

One genus 6 curve, a Hermitian curve, with the maximal number of smooth points, 65, was found (it is known to be the unique such curve up to isomorphism):

$$x^5 + y^5 + z^5.$$

Two genus 7 curves each with 57 smooth points in the plane:

$$f_1 = x^4\,y^2 + x\,y^5 + y^6 + \left(x^2\,y^3 + x\,y^4 + y^5\right)\,z + \left(x^2 + x\,y\right)\,z^4 + y\,z^5.$$

$$f_2 = x^4\,y^2 + x^2\,y^4 + y^6 + \left(x^2\,y^3 + x\,y^4\right)\,z + \left(x^2 + x\,y\right)\,z^4 + y\,z^5.$$

A curve with genus 8 with 57 smooth plane points is

$$x^6 + x^3\,y^3 + x^2\,y^4 + x^4\,y\,z + x^2\,y^2\,z^2 + \left(x^3 + x^2\,y\right)\,z^3 + (x+y)\,z^5.$$

There are two curves of genus 9 with 57 smooth plane points, each receiving two points from blowups: f_1 from the singularity $(1:1:1)$ of type u^2+uv+v^2 which splits over $\mathbb{F}_{16}$, and f_2 from the singularity $(0:1:1)$ of type uv. Thus $N_{16}(9) \geq 59$.

$$f_1 = x^5\,y + x^3\,y^3 + x\,y^5 + \left(x^5 + y^5\right)\,z + x^2\,y^2\,z^2 + \left(x^3 + y^3\right)\,z^3 + (x+y)\,z^5.$$

$$f_2 = x^6 + x^5\,y + x^2\,y^4 + y^5\,z + x^2\,y^2\,z^2 + x\,y^2\,z^3 + \left(x^2 + x\,y\right)\,z^4 + y\,z^5.$$

The two curves of genus 10 each with 59 plane smooth points are:

$$f_1 = x^5\,y + y^6 + \left(x^2\,y^3 + y^5\right)\,z + \left(x^4 + x^3\,y + x\,y^3\right)\,z^2 + x\,y^2\,z^3 + (x+y)\,z^5 + z^6.$$

$$f_2 = x^5\,y + y^6 + \left(x^4\,y + x\,y^4 + y^5\right)\,z + \left(x^4 + x\,y^3\right)\,z^2 + \left(x^3 + x\,y^2\right)\,z^3 + y^2\,z^4 + z^6.$$

4.3 $\mathbb{F}_{32}$

Three curves with genus 4 and 71 smooth points on the plane curve are:

$$f_1 = x^4\,y + x\,y^4 + y^5 + x\,y^3\,z + \left(x\,y^2 + y^3\right)\,z^2 + x^2\,z^3 + x\,z^4 + z^5.$$

$$f_2 = x^6 + x^3\,y^3 + y^6 + \left(x^4\,y + y^5\right)\,z + \left(x^3\,y + x^2\,y^2\right)\,z^2 + \left(x^3 + x^2\,y + y^3\right)\,z^3 + x^2\,z^4 + y\,z^5 + z^6.$$

$$f_3 = x^6 + x^3\,y^3 + y^6 + \left(x^5 + x^3\,y^2 + x^2\,y^3\right)\,z + y^4\,z^2 + \left(x^3 + y^3\right)\,z^3 + y^2\,z^4 + x\,z^5 + z^6.$$

A curve with 82 smooth points in the plane and genus 5 is

$$x^6 + x^3\,y^3 + x^2\,y^4 + y^6 + x^5\,z + x^3\,y\,z^2 + \left(x^3 + x\,y^2 + y^3\right)\,z^3 + x^2\,z^4 + y\,z^5.$$

A genus 6 curve with 82 planar smooth points and 2 points above the singularity $(1:0:1)$ of type uv (thus $N_{32}(6) \geq 84$) is

$$x^6 + y^6 + \left(x^4\,y + x^3\,y^2 + x\,y^4\right)\,z + x\,y^2\,z^3 + \left(x^2 + x\,y + y^2\right)\,z^4.$$

Two genus 7 curves each with 92 planar smooth points are

$$f_1 = x^3\,y^3 + y^6 + \left(x^5 + x^3\,y^2\right)\,z + \left(x^4 + y^4\right)\,z^2 + \left(x^3 + y^3\right)\,z^3 + y^2\,z^4 + x\,z^5 + z^6.$$

$$f_2 = x^6 + y^6 + \left(x^5 + y^5\right)\,z + y^4\,z^2 + \left(x^3 + y^3\right)\,z^3 + x^2\,z^4 + (x+y)\,z^5.$$

A curve with 93 planar smooth points, genus 8, is

$$x\,y^5 + y^6 + \left(x^5 + x^4\,y\right)\,z + y^4\,z^2 + \left(x^3 + y^3\right)\,z^3 + y^2\,z^4 + y\,z^5.$$

A genus 9 curve with 93 smooth planar points:

$$x^4\,y^2 + x^3\,y^3 + \left(x^5 + x^3\,y^2 + x\,y^4 + y^5\right)\,z + x^2\,y^2\,z^2 + \left(x^3 + y^3\right)\,z^3 + x^2\,z^4 + z^6.$$

Genus 10 with 103 smooth planar points:

$$x^6 + x^3\,y^3 + x\,y^5 + \left(x^2\,y^2 + x\,y^3\right)\,z^2 + \left(x^3 + x\,y^2 + y^3\right)\,z^3 + x\,y\,z^4 + (x+y)\,z^5.$$

4.4 $\mathbb{F}_{64}$

One curve had genus 4 and 118 smooth planar points:

$$x^3\,y^2 + y^5 + y^4\,z + y^2\,z^3 + z^5.$$

Two curves of genus 6 had 160 smooth planar points (which is one less than the bound of 161):

$$\begin{aligned} f_1 &= x^4\,y^2 + x^2\,y^4 + x\,y^5 + y^5\,z + y^3\,z^3 + y\,z^5 + z^6. \\ f_2 &= x^6 + x^5\,z + \left(x^4 + y^4\right)\,z^2 + x^3\,z^3 + y^2\,z^4 + y\,z^5. \end{aligned}$$

Genus 7, 153 planar smooth points:

$$x^2\,y^4 + x\,y^5 + y^6 + \left(x^3\,y^2 + x\,y^4 + y^5\right)\,z + x\,y^3\,z^2 + x^2\,z^4 + x\,z^5 + z^6.$$

Three curves had genus 8 and 159 plane smooth points, the last two of which have no rational points over $\mathbb{F}_2$:

$$\begin{aligned} f_1 &= x^3\,y^3 + y^6 + \left(x^4\,y + x\,y^4\right)\,z + \left(x^3 + y^3\right)\,z^3 + x\,y\,z^4. \\ f_2 &= x^6 + x^5\,y + x^3\,y^3 + x\,y^5 + y^6 + \left(x^3\,y^2 + y^5\right)\,z + x^3\,y\,z^2 + \left(x^2\,y + y^3\right)\,z^3 + y^2\,z^4 + x\,z^5 + z^6. \\ f_3 &= x^6 + x^4\,y^2 + x^3\,y^3 + x^2\,y^4 + y^6 + \left(x^4 + x^2\,y^2 + y^4\right)\,z^2 + \left(x^3 + y^3\right)\,z^3 + \left(x^2 + y^2\right)\,z^4 + z^6. \end{aligned}$$

There are 166 plane smooth points on this curve of genus 9:

$$x^6 + x^3\,y^3 + \left(x^4\,y + x^2\,y^3\right)\,z + \left(x^3\,y + x\,y^3 + y^4\right)\,z^2 + x^2\,z^4 + y\,z^5.$$

Four genus 10 curves each had 171 points on their smooth model:

$$\begin{aligned} f_1 &= x^6 + y^6 + \left(x^4\,y + x^2\,y^3 + x\,y^4\right)\,z + x^3\,y\,z^2 + x\,y^2\,z^3 + x\,y\,z^4 + z^6. \\ f_2 &= x^6 + x^5\,y + x^4\,y^2 + x^3\,y^3 + x^2\,y^4 + x\,y^5 + y^6 + \left(x^4\,y + x\,y^4\right)\,z + \left(x^2\,y + x\,y^2\right)\,z^3 + z^6. \\ f_3 &= x^6 + x^3\,y^3 + y^6 + \left(x^4\,y + x\,y^4\right)\,z + \left(x^3 + y^3\right)\,z^3 + z^6. \\ f_4 &= x^6 + x^3\,y^3 + x\,y^5 + x^3\,y^2\,z + \left(x^4 + x^3\,y + y^4\right)\,z^2 + y^2\,z^4 + x\,z^5 + z^6. \end{aligned}$$

4.5 $\mathbb{F}_{128}$

There is one degree 6 plane curve with a genus 3 smooth model, with 183 smooth plane points, and another point coming from the singularity $(0:0:1)$ of type $(u+v)(u^2+uv+v^2)$, which matches [Moreno et al. 95]. The curve is

$$x^6 + x^5\,y + x^4\,y^2 + x^3\,y^3 + x^2\,y^4 + \left(x^5 + x^4\,y\right)\,z + y^4\,z^2 + \left(x^3 + y^3\right)\,z^3.$$

A curve of genus 4 with 215 planar smooth points (2 less than the maximum possible) is

$$x^2\,y^3 + x\,y^4 + x^4\,z + x\,y^2\,z^2 + x\,y\,z^3 + (x+y)\,z^4.$$

There are two curves of genus 6 with 240 planar smooth points, receiving 3 points each from singularities. f_1 has type $uv(u+v)$ at $(0:1:0)$ and f_2 has type $(u+v)(u^2+uv+v^2)$ at $(0:1:0)$ and type uv at $(1:0:0)$. Thus $N_{128}(6) \geq 243$.

$$\begin{aligned} f_1 &= x^4\,y^2 + \left(x^5 + x^4\,y + x^2\,y^3\right)\,z + \left(x^2\,y^2 + x\,y^3\right)\,z^2 + \left(x^2 + x\,y + y^2\right)\,z^4. \\ f_2 &= x^3\,y^3 + x^4\,y\,z + \left(x^4 + x^3\,y\right)\,z^2 + \left(x^3 + x^2\,y + y^3\right)\,z^3 + z^6. \end{aligned}$$

Two genus 7 curves with 248 smooth planar points:

$$\begin{aligned} f_1 &= x^3\,y^3 + x\,y^5 + y^6 + x^3\,y^2\,z + y^4\,z^2 + x^3\,z^3 + \left(x^2 + y^2\right)\,z^4 + (x+y)\,z^5. \\ f_2 &= x^5\,y + x^4\,y^2 + x^2\,y^4 + \left(x^3\,y^2 + x^2\,y^3\right)\,z + x^4\,z^2 + x\,y^2\,z^3 + z^6. \end{aligned}$$

A curve with 266 planar smooth points, genus 8, and no $\mathbb{F}_2$ rational points is

$$x^6 + x^3\,y^3 + x^2\,y^4 + x\,y^5 + y^6 + \left(x^5 + y^5\right)\,z + \left(x^2\,y^2 + y^4\right)\,z^2 + \left(x^3 + y^3\right)\,z^3 + x\,z^5 + z^6.$$

There are 269 smooth plane points on the curves of genus 9 given by

$$f_1 = x^4\,y^2 + x\,y^5 + \left(x^4 + y^4\right)\,z^2 + \left(x^3 + y^3\right)\,z^3 + x\,y\,z^4 + x\,z^5 + z^6.$$
$$f_2 = x^6 + x^3\,y^3 + x^2\,y^4 + y^6 + \left(x\,y^4 + y^5\right)\,z + x^2\,y^2\,z^2 + \left(x^2 + x\,y + y^2\right)\,z^4.$$

The smooth curve of genus 10 with 276 $\mathbb{F}_{128}$ rational points is

$$x^6+y^6+x^2\,y^3\,z+\left(x^4 + x^3\,y + y^4\right)\,z^2+x^3\,z^3+x^2\,z^4+x\,z^5.$$

4.6 $\mathbb{F}_{256}$

A genus 3 curve not listed in [Moreno et al. 95] with 350 smooth planar points is given by

$$x^5+x\,y^4+y^5+\left(x^2\,y^2 + y^4\right)\,z+\left(x^2\,y + x\,y^2\right)\,z^2+x\,z^4+z^5.$$

A curve with 399 smooth plane points and genus 5 is

$$x^6 + x^4\,y^2 + x^5\,z + \left(x^2\,y^2 + y^4\right)\,z^2 + \left(x^2\,y + x\,y^2\right)\,z^3 + x^2\,z^4 + y\,z^5.$$

A genus 6 curve with 416 smooth plane points is

$$x^4\,y + x^3\,y^2 + y^4\,z + \left(x^3 + y^3\right)\,z^2 + \left(x^2 + x\,y\right)\,z^3 + z^5.$$

One point from the singularity $(1:0:0)$ of type uv^2 is added to the 442 smooth plane points on a curve of genus 7 given by

$$x^3\,y^3+x^2\,y^4+y^5\,z+x^3\,y\,z^2+\left(x\,y^2 + y^3\right)\,z^3+y^2\,z^4+z^6.$$

A curve of genus 8 with one point less than the Serre bound has 512 smooth plane points and is given by

$$x^4\,y^2 + y^5\,z + x\,z^5.$$

Two curves of genus 9, each with 474 smooth points and 2 points from singularities of type $u^2 + uv + v^2$, which factor over $\mathbb{F}_{256}$, at points $(0:1:1)$ and $(1:1:0)$ respectively (so $N_{256}(9) \geq 476$) are

$$f_1 = x^5\,y + x^3\,y^3 + x^2\,y^4 + x\,y^5 + y^4\,z^2 + x^3\,z^3 + y^2\,z^4 + x\,z^5.$$
$$f_2 = x^6 + y^6 + \left(x^5 + y^5\right)\,z + x^4\,z^2 + \left(x^2\,y + x\,y^2\right)\,z^3 + x\,z^5 + z^6.$$

Two smooth curves of genus 10 have 537 smooth plane points:

$$f_1 = x^6 + x\,y^5 + x^4\,y\,z + x^2\,y^2\,z^2 + y^3\,z^3 + x\,z^5.$$
$$f_2 = x^6 + x^5\,y + x^3\,y^3 + x\,y^5 + y^6 + \left(x^5 + y^5\right)\,z + x^2\,y^2\,z^2 + x\,y\,z^4 + z^6.$$

4.7 $\mathbb{F}_{512}$

Four curves overlooked in [Moreno et al. 95] of genus 4 have 663 plane smooth points. They are

$$f_1 = x^4\,y + x\,y^4 + \left(x^3\,y + y^4\right)\,z + \left(x\,y + y^2\right)\,z^3 + z^5.$$
$$f_2 = x^4\,y + x\,y^4 + y^5 + \left(x\,y^3 + y^4\right)\,z + \left(x\,y^2 + y^3\right)\,z^2 + x^2\,z^3 + x\,z^4.$$
$$f_3 = x^4\,y + x^2\,y^3 + y^5 + \left(x^2\,y^2 + x\,y^3 + y^4\right)\,z + \left(x^3 + y^3\right)\,z^2 + z^5.$$
$$f_4 = x^5 + y^5 + \left(x^4 + x^3\,y + y^4\right)\,z + \left(x\,y^2 + y^3\right)\,z^2 + z^5.$$

A genus 6 curve with 766 smooth plane points and one more point from the singularity $(1:0:0)$ of type $(u+v)(u^2+uv+v^2)$ (so $N_{512}(6) \geq 767$) is

$$x^3\,y^3 + y^6 + \left(x\,y^4 + y^5\right)\,z + \left(x^2\,y^2 + y^4\right)\,z^2 + x^3\,z^3 + x\,y\,z^4 + (x+y)\,z^5.$$

There are 786 smooth plane points and 1 point from the singularity $(1:0:0)$ of type uv^2 on the genus 7 curve

$$x^2\,y^4 + y^6 + x^3\,y^2\,z + \left(x^3 + x\,y^2\right)\,z^3 + x\,y\,z^4 + y\,z^5.$$

A curve of genus 8 with 813 plane smooth points is

$$x^2\,y^4 + y^6 + \left(x^5 + x^2\,y^3\right)\,z + \left(x^3\,y + x\,y^3 + y^4\right)\,z^2 + \left(x^3 + x^2\,y\right)\,z^3 + x\,z^5.$$

A genus 9 curve with 837 smooth plane points is

$$x^6 + x^4\,y^2 + \left(x\,y^4 + y^5\right)\,z + x^2\,y^2\,z^2 + \left(x^2\,y + x\,y^2\right)\,z^3 + x\,y\,z^4 + x\,z^5 + z^6.$$

A smooth genus 10 plane curve with 845 plane points is

$$x^5\,y + x^4\,y^2 + x^2\,y^4 + y^6 + \left(x^2\,y^3 + y^5\right)\,z + \left(x^3\,y + y^4\right)\,z^2 + x^2\,z^4 + (x+y)\,z^5.$$

4.8 $\mathbb{F}_{1024}$

A genus 3 curve with 1211 smooth plane points is

$$x^3\,y + y^3\,z + y\,z^3 + z^4.$$

Three genus 4 curves have 1273 smooth plane points:

$$f_1 = x^3\,y^2 + y^5 + x^2\,y\,z^2 + y^2\,z^3 + x\,z^4.$$
$$f_2 = x^4\,y + x^2\,y^3 + y^5 + \left(x^2\,y^2 + y^4\right)\,z + \left(x^3 + y^3\right)\,z^2 + x\,z^4.$$
$$f_3 = x^5 + x^3\,y^2 + x^2\,y^3 + y^5 + y^4\,z + x\,y^2\,z^2 + x^2\,z^3.$$

F_q	best 3	bound 3	best 4	bound 4	best 5	bound 5	best 6	bound 6
8	24[1]	24	25[2]	25[4]	28	30[4]	33	35 [3]
16	38[1]	41	45[2]	45[4]	45[2]	53[4]	65	65
32	63[2]	65[3]	71	74[4]	82	85[4]	84	96[4]
64	113[2]	113	118	129	130[2]	145	160	161
128	184[2]	195	215	215[4]	227[2]	239	243	258[4]
256	350[2]	353	381[2]	385	399	417	416	449
512	640[2]	648	663	693	724[2]	738	767	783
1024	1211	1217	1273	1281	1345	1345	1383	1409
2048	2294	2319	2380	2409	2422	2499	2556	2589
F_q	best 7	bound 7	best 8	bound 8	best 9	bound 9	best 10	bound 10
8	33	38 [4]	33	42[4]	33	45[4]	35	49[4]
16	57	69[4]	57	75[4]	59	81[5]	59	87[5]
32	92	107[4]	93	118[4]	93	128[4]	103	139[4]
64	153	177	159	193	166	209	171	225
128	248	283	266	302[4]	269	322[4]	276	349
256	443	481	512	513	476	545	537	577
512	787	828	813	873	837	918	845	963

[1]= [Serre 83] [2] = [Moreno et al. 95] [3] = [Lauter 01] [4] = [Howe and Lauter 02] [5] = [Ihara 81]

TABLE 1. Summary of results.

A curve with 1343 smooth plane points, genus 5, and 2 points coming from the singularity $(1:0:0)$ of type uv (and thus attaining the maximum possible 1345) is

$$x^3\,y^2 + y^5 + x^3\,y\,z + y^3\,z^2 + z^5.$$

A genus 6 curve with 1383 smooth plane points is

$$x^4\,y + x\,y^4 + y^5 + x^2\,y^2\,z + x\,y\,z^3 + z^5.$$

4.9 $\mathbb{F}_{2048}$

Two genus 3 curves with 2293 smooth plane points, and one more coming from the singularity $(0:1:0)$ of type $(u+v)(u^2+uv+v^2)$ on each curve are

$$f_1 = x^4\,y + x^3\,y^2 + x^3\,y\,z + y^2\,z^3 + (x+y)\,z^4.$$
$$f_2 = x^4\,y + x^3\,y^2 + x^3\,y\,z + x^3\,z^2 + y^2\,z^3 + y\,z^4.$$

Three curves with 2380 smooth plane points and genus 4 are

$$\begin{aligned} f_1 &= x^5 + y^5 + x^3\,y\,z + y^2\,z^3 + x\,z^4. \\ f_2 &= x^5 + x^4\,y + \left(x\,y^3 + y^4\right)\,z + x^3\,z^2 \\ &\quad + \left(x^2 + y^2\right)\,z^3 + z^5. \\ f_3 &= x^5 + x^2\,y^3 + x\,y^4 + x^4\,z + x^3\,z^2 \\ &\quad + \left(x^2 + x\,y + y^2\right)\,z^3 + x\,z^4 + z^5. \end{aligned}$$

A genus 5 curve with 2422 smooth plane points is

$$x^4\,y + x^3\,y^2 + y^5 + x\,y^2\,z^2 + \left(x^2 + x\,y + y^2\right)\,z^3.$$

Finally, a genus 6 curve with 2556 planar smooth points is

$$x^4\,y + x^2\,y^3 + x\,y^4 + y^5 + \left(x^3\,y + y^4\right)\,z + x^2\,z^3 + y\,z^4.$$

4.10 Tallies

The columns headed "bound" give the Serre [Serre 83] bound, unless marked [Ihara 81] as Ihara or [Lauter 01] as Lauter. The columns headed "best" give the lower bounds for $N_q(g)$ found above; bounds marked [Moreno et al. 95] and [Serre 83] are from those previous papers. Note in particular the reduction from the Serre [Serre 83] upper bounds using [Ihara 81] and [Lauter 01] has made several known curves closer to or already optimal. After this paper was initially written in 2000, improved bounds were published in [Howe and Lauter 02] and incorporated in this table. These new bounds made the $q = 128, g = 4$ curve optimal.

5. CONCLUSIONS

Previously known results are [Moreno et al. 95] and [Serre 83]. The bounds in this paper could possibly be strengthened by analyzing the singularities in more detail, resulting in more known $\mathbb{F}_q$ rational points on the smooth models of the curves. Also all genus ≤ 5 curves from the degree 6 polynomials were not identified. More work could be done to compute exact parameters for these curves.

6. COMMENTS

The techniques used here make a search over degree 7 plane curves feasible on a supercomputer, and quite possibly on a home PC. The desingularized curves can be used to construct algebraic-geometric Goppa codes [Pretzel 98], [Tsfasman 91]. For example, using the genus 5 curve over $\mathbb{F}_{1024}$ with 1345 rational points, linear codes with parameters $[n, k-4, n-k]$ can be constructed for $10 \leq n \leq 1344$ and $8 < k < n$ over $\mathbb{F}_{1024}$. Similarly, using the genus 6 $\mathbb{F}_{64}$ curve with 160 points, $[n, k-5, n-k]$-linear codes can be constructed for $12 \leq n \leq 159$ and $10 < k < n$, and the $\mathbb{F}_{256}$ curve of genus 8 with 512 rational points gives $[n, k-7, n-k]$-linear codes for $16 \leq n \leq 511$ and $14 < k < n$ (see, for example, [Pretzel 98]).

ACKNOWLEDGMENTS

Thanks to the reviewer for numerous suggestions on layout and a few corrections.

REFERENCES

[Haché and Le Brigand 95] G. Haché and D. Le Brigand. "Effective Construction of Algebraic-Geometric Codes." *IEEE Transactions on Information Theory* 41 (1995), 1615–1628.

[Hartshore 77] R. Hartshorne. *Algebraic Geometry,* GTM 52. New York: Springer-Verlag, 1977.

[Howe and Lauter 02] E. Howe and K. Lauter. Available from World Wide Web: (http://arxiv.org/abs/math.NT/0207101), 2002.

[Ihara 81] Y. Ihara. "Some Remarks on the Number of Rational Points of Algebraic Curves over Finite Fields." *J. Fac. Sci. Tokyo* 28 (1981), 721–724.

[Kant 00] KANT. Available from World Wide Web: (http://www.math.tu-berlin.de/algebra), 2000.

[Lauter 01] K. Lauter. "Geometric Methods for Improving the Upper Bounds of the Number of Rational Points on Algebraic Curves over Finite Fields." *Journal of Algebraic Geometry* 10 (2001), 19–36.

[Lomont 00] C. Lomont. Available from World Wide Web: (www.math.purdue.edu/∼clomont/Math/Papers/2000/PolySolver.zip), 2000.

[Maple 00] MAPLE. Available from World Wide Web: (www.maplesoft.com), 2000.

[Moreno et al. 95] O. Moreno, D. Zinoviev, and V. Zinoviev. "On Several New Projective Curves Over F_2 of Genus 3, 4, and 5." *IEEE Transactions on Information Theory* 41 (1995), 1643–1648.

[Pretzel 98] O. Pretzel. *Codes and Algebraic Curves.* Oxford: Oxford Science Publications, Clarendon Press, 1998.

[Ragot 98] J. Ragot. Available from World Wide Web: (http://pauillac.inria.fr/algo/seminars/sem97-98/ragot.html), 1998.

[Serre 83] J.-P. Serre. "Nombres de points des courbes algebriques sur F_q." *Seminaire de Theorie des Nombres de Bordeux* 22 (1983), 1–8.

[Tsfasman 91] M. A. Tsfafman and S. G. Vlăduţ. *Algebraic-Geometric Codes.* Dordrecht/Boston/London: Kluwer, 1991.

[van der Geer and van der Vlugt 03] Tables. Available from World Wide Web: (http://www.science.uva.nl/˜geer/), 2003.

[Walker 62] R. Walker, *Algebraic Curves.* New York: Dover Publications, 1962.

Chris Lomont, Department of Mathematics, Purdue University, West Lafayette, IN 47907 (clomont@math.purdue.edu)

Received June 1, 2001; accepted in revised form January 9, 2002.