Appendix to "Maximal curves of genus 5 over finite fields"

Let X be a smooth, projective, absolutely irreducible curve over a finite field $\mathbf{F}_q$ of genus $g_X = 5$. Suppose that X admits an automorphism of order 5 and let G denote the group generated by it. Let E denote the quotient of X by G. The conductor-discriminant formula applied to the cyclic Galois cover $X \to E$ is

$$2g_X - 2 \;=\; 5(2g_E - 2) + \sum_{\chi} \deg(\text{conductor}(\chi)).$$

It easily implies that the genus g_E of E is 1 and that the degree of the common conductor D of the non-trivial characters χ of G is equal to 2.

By class field theory the reciprocity homomorphism

$$\theta : \mathbf{A}_E^*/K^*U_D \longrightarrow G$$

is surjective. Here K is the function field $\mathbf{F}_q(E)$ and $\mathbf{A}_E$ is the adèle ring of E. The subgroup of the idèle group $\mathbf{A}_E^*$ of unit idèles is denoted by U. The quotient group $\mathbf{A}_E^*/U$ is naturally ismorphic to the divisor group $\mathrm{Div}(E)$. Let U_D denote the subgroup of $u \in U$ for which $u \equiv 1 \pmod{D}$. There is an exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U/\mathbf{F}_q^*U_D & \longrightarrow & \mathbf{A}_E^*/K^*U_D & \longrightarrow & \mathbf{A}_E^*/K^*U & \longrightarrow & 0 \\ & & & & & & \| & & (*) \\ & & & & & & \mathrm{Pic}(E) & & \end{array}$$

Since the degree of D is 2, there are three possibilities for D. It is either a point of degree 2 or it is the sum of two degree 1 points, which may or may not be equal. The group $U/\mathbf{F}_q^*U_D$ is isomorphic to $\mathbf{F}_{q^2}^*/\mathbf{F}_q^*$, $\mathbf{F}_q^*$ or $\mathbf{F}_q$ in these cases. The orders of these groups are $q+1$, $q-1$ and q respectively.

Proposition A.1. *We have $q \not\equiv \pm 2 \pmod 5$.*

Proof. If q were congruent to $\pm 2 \pmod 5$, none of the possible orders of $U/\mathbf{F}_q^*U_D$ is divisible by 5. Therefore $U/\mathbf{F}_q^*U_D$ is in the kernel of θ. It follows that θ factors through $\mathbf{A}_E^*/K^*U = \mathrm{Pic}(E)$. But that implies that the cover $X \to E$ is unramified, which it isn't. This contradiction proves the proposition.

By Zaytsev [2, Thm. 4.13], an optimal genus 5 curve over $\mathbf{F}_q$ for which one has $[2\sqrt{q}]^2 - 4q = -19$, admits an automorphism of order 5. Therefore Proposition A.1 applies. It gives an alternative proof of Theorem 3.2 of this paper.

The next proposition regards $q = 5$. Over $\mathbf{F}_5$ there is a unique elliptic curve E' with $\#E'(\mathbf{F}_5) = 5$. The trace of its Frobenius endomorphism is 1 and the discriminant of its endomorphism ring is -19. The curve E' is given by the Weierstrass equation $y^2 = x^3 - 2x + 2$.

Proposition A.2. *If $q = 5$, then the curve E cannot be isomorphic to E'.*

Proof. If $q = 5$, the degree 2 divisor D can only be $2P$ for some $\mathbf{F}_q$-rational point P of E. In this case the order of $U/\mathbf{F}_q^* U_D$ is equal to $q = 5$. The exact sequence $(*)$ modulo fifth powers leads to the exact sequence

$$U/\mathbf{F}_5^* U_D \longrightarrow \mathbf{A}_E^*/{\mathbf{A}_E^*}^5 K^* U_D \longrightarrow \mathbf{A}_E^*/{\mathbf{A}_E^*}^5 K^* U \longrightarrow 0$$

If E were isomorphic to the elliptic curve E' given by $y^2 = x^3 - 2x + 2$, the leftmost homomorphism is zero. In other words, U is contained in the subgroup ${\mathbf{A}_E^*}^5 K^* U_D$ of $\mathbf{A}_E^*$. To see this, we first observe that the group $E(\mathbf{F}_5)$ acts transitively on itself by translations. Therefore we may take for P any of the five points in $E(\mathbf{F}_5)$. We choose $P = (1, 1)$. Then we put $Q = (2, -1)$ and let $\xi \in \mathbf{A}^*$ denote an idèle whose image in $\mathrm{Div}(E)$ is the divisor $Q - O$, where O is the point of E at infinity. It is not difficult to see that the divisor of the function

$$h = \frac{(y+1)^2(x-2)}{y - 2x - 2}$$

is equal to $5(Q - O)$. Therefore both ξ^5 and h are elements of $\mathbf{A}_E^*$ whose images in $\mathrm{Div}(E)$ are equal to $5(Q - O)$. It follows that $v = \xi^5/h$ is in U. Since $h(P) = 2$ and

$$h - 2 = \frac{(x-1)(2y + x^3 - x^2 + 2x)}{y - 2x - 2}$$

has a simple zero in P, the idèle unit v generates U/U_D. Therefore every $u \in U$ can be written as $v^k w$ for some $k \in \mathbf{Z}$ and $w \in U_D$. Since v is in ${\mathbf{A}_E^*}^5 K^*$, this proves that we indeed have $U \subset {\mathbf{A}_E^*}^5 K^* U_D$.

It follows that the natural map

$$\mathbf{A}_E^*/{\mathbf{A}_E^*}^5 K^* U_D \xrightarrow{\cong} \mathbf{A}_E^*/{\mathbf{A}_E^*}^5 K^* U$$

is an isomorphism. By class field theory, the group on the left is isomorphic to the Galois group of the maximal abelian exponent 5 extension L of K of conductor at most $D = 2P$. Note that the function field $\mathbf{F}_5(X)$ of the curve X is a subfield of L. Since $\mathbf{A}_E^*/{\mathbf{A}_E^*}^5 K^* U_D$ is isomorphic to $\mathbf{A}_E^*/{\mathbf{A}_E^*}^5 K^* U$, the extension $K \subset L$ is unramified at *all* places. Since we have $K \subset \mathbf{F}_5(X) \subset L$, the same is true for $\mathbf{F}_5(X)$. However, the cover $X \to E'$ is actually ramified and hence we obtain a contradiction.

This proves the proposition.

Corollary A.3. *When q is a power of 5, there is no optimal genus 5 curve X over $\mathbf{F}_q$ for which $[2\sqrt{q}]^2 - 4q = -19$.*

Proof. Suppose X is such an optimal curve. By Proposition 6.4 of this paper, the curve X cannot exist, except possibly when $q = 5^7$. In this case we have $[2\sqrt{q}] = 559$ and the eigenvalues of the characteristic polynomial of Frobenius are $\frac{-559+\sqrt{-19}}{2} = \phi^7$ and its complex conjugate where $\phi = \frac{1+\sqrt{-19}}{2}$. Since the ring $\mathbf{Z}[\phi]$ is generated by ϕ^7, a theorem of Serre [1, Thm. 9 of the appendix] implies that X is the base change of a genus 5 curve X' over $\mathbf{F}_5$.

By Zaytsev [2, Thm. 4.13] the automorphism group of X over $\mathbf{F}_{5^7}$ is isomorphic to the the dihedral group D_5. The Galois group of $\mathbf{F}_{5^7}$ over $\mathbf{F}_5$ acts on $\mathrm{Aut}_{\mathbf{F}_{5^7}}(X')$. Since 7 is prime to $\#\mathrm{Aut}(D_5) = 20$, this action is trivial. Therefore all automorphisms of X' are defined over $\mathbf{F}_5$. The quotient of X' by an automorphism of order 5 is isomorphic to the unique elliptic curve E' over $\mathbf{F}_5$ with five rational points. Therefore Proposition A.2 applies and we conclude that this is not possible. Therefore X cannot exist.

In view of the results in this paper, the fields $\mathbf{F}_q$ over which an optimal genus 5 curve X with $[2\sqrt{q}]^2 - 4q = -19$ may exist, necessarily satisfy $q \equiv 1 \pmod 5$. As we explained above, in these cases X is a cyclic degree 5 cover ramified over two distinct $\mathbf{F}_q$-rational points of a specific genus 1 curve E. By translating we may assume that the two points are the point O at infinity and a second point P. By Kummer theory the function field of X is of the form $\mathbf{F}_q(E)(\sqrt[5]{h})$, where $h \in \mathbf{F}_q(E)$ is a function whose divisor is $m(P-O)$ with $m = \#E(\mathbf{F}_q)$. The function h is unique up to a scalar multiple. The number of $\mathbf{F}_q$-rational points on X is equal to $2 + 5r$, where r is the number of points $Q \in E(\mathbf{F}_q) - \{P, O\}$ for which $h(Q)$ is a fifth power in $\mathbf{F}_q^*$.

A short Pari-GP program, computing the number r for each point $P \neq O$ in $E(\mathbf{F}_q)$ and each function h, showed that for $q < 10000$ there is no optimal genus 5 curve X over $\mathbf{F}_q$ with $[2\sqrt{q}]^2 - 4q = -19$. This is actually a short list of ten primes, the smallest and largest being $q = 61$ and 9511 respectively. The entire computation took less than two hours.

Bibliography.

[1] J.-P. Serre: Appendice to K. Lauter: Geometric Methods for Improving the Upper Bounds on the Number of Rational Points on Algebraic Curves over Finite Fields, *J. Alg. Geometry* **10** (2001), 19–36.

[2] A. Zaytsev: Optimal curves of low genus over finite fields, *Finite Fields and Their Applications* **37** (2016) 203–224.

René Schoof

Dipartimento di Matematica
2ª Università di Roma "Tor Vergata"
I-00133 Roma ITALY
Email: schoof@mat.uniroma2.it