

Curves with Many Points

Rohit Ghosh

Department of Mathematics, University of Texas, Austin, TX 78712, USA ^{*†}

May 12, 2006

In this essay we describe an elementary method to construct curves over \mathbb{F}_q with many points. This construction is due to Gerard Van Der Geer and Marcel Van Der Vlugt. The Authors consider fibre products C_F over a base curve C of Artin-Schreier extensions $C_f \rightarrow C$ defined by the function field extensions $\mathbb{F}_q(C_f) = \mathbb{F}_q(C)(y)$ where $y^p - y = f$ and f belongs to a suitable \mathbb{F}_p -vector space of $K = \mathbb{F}_q(C)$.

Let us define the Artin-Schreier operator ρ acting on our field by $\rho : h \rightarrow h^p - h$. We should note that $\rho y = f$ and $\rho y = f + \rho h$ define birationally isomorphic coverings. Hence the isomorphism class of the covering C_f depends only on the class $f + \rho K \in K/\rho K$. We want to exclude classes where $\rho y = f$ gives a constant field extension of K . We state the following theorem.

Theorem 1. *If $f \in K - (pK + \mathbb{F}_q)$, then the equation $\rho y = f$ defines a Artin-Schreier (A-S) covering of C .*

We would like to compute the number of rational points and the genus for a A-S covering For any place Q of C and $f \in K$ we define the reduced evaluation of f at Q by

$$v_Q^*(f) := \sup\{v_Q(f + \rho h) | h \in K\}.$$

The following two theorems give us information about the genus and the number of rational points of a A-S extension.

Theorem 2. *Let $\pi : C_f \rightarrow C$ be an A-S given by $\rho y = f$. This covering is ramified precisely at the places Q of C at which $v_Q^*(f) < 0$; let Q' denote the unique place of C_f lying over Q . Then the ramification divisor is given by*

$$R_f = \sum_{Q: v_Q^*(f) < 0} (p-1)(-v_Q^*(f) + 1)Q'.$$

The genus of C_f can be determined using Hurwitz formula:

$$2g(C_f) - 2 = p(2g(C) - 2) + \deg R_f.$$

^{*}E-mail address: rghosh@math.utexas.edu

[†]URL: www.ma.utexas.edu/users/rghosh

Theorem 3. *Let $\pi : C_f \rightarrow C$ be an A-S given by $\rho y = f$, and take a rational point $Q \in C(\mathbb{F}_q)$. Then the number of rational points of C_f lying over Q is equal to*

$$\begin{aligned} &1, \text{ if } v_Q^*(f) < 0 \\ &p, \text{ if } v_Q^*(f) \geq 0 \text{ and } \text{Tr}(f + \rho K)(Q) = 0 \\ &0, \text{ if } v_Q^*(f) \geq 0 \text{ and } \text{Tr}(f + \rho K)(Q) \neq 0. \end{aligned}$$

Since all rational points of C_f lie above rational points of C , this theorem allows us to compute the number of rational points on C_f .

For function fields the fibre product is a curve corresponding to the function field defined as the compositum of the respective field extensions of the field of functions on the base curve in a fixed algebraic closure. Suppose we are given A-S coverings

$$\rho y_1 = f_1, \dots, \rho y_r = f_r$$

of the curve C . If we assume that the fibre product of these coverings is absolutely irreducible then it is curve whose corresponding function field is $K(y_1, \dots, y_r)$. For $\lambda_i \in \mathbb{F}_p$ this function field also contains $y = \sum \lambda_i y_i$, satisfying the equation $\rho y = \sum \lambda_i f_i$. So f_i 's may be replaced with their nondegenerate \mathbb{F}_p -linear combinations and the fibre product is determined by \mathbb{F}_p -vector space $V = \langle f_1, \dots, f_r \rangle \subset K$.

Theorem 4. *If the \mathbb{F}_p -vector space $V \subset K$ has a zero intersection with $\mathbb{F}_q + \rho K$, then for any basis $\{f_1, f_2, \dots, f_r\}$ of V , the equations $\rho y_1 = f_1, \dots, \rho y_r = f_r$ define a Galois covering of C , with Galois Group $(\mathbb{Z}/p\mathbb{Z})^r$.*

A-S theory tells us that the converse to this theorem is also true. Let C_V be the A-S corresponding to $V \subset K$. For a fixed point Q of C , denote $V_Q = \{f \in V \mid v_Q^*(f) \geq 0\}$ and $V'_Q = \{f \in V \mid \text{Tr}(f + \rho K)(Q) = 0\}$. Then both these spaces are \mathbb{F}_p -subspaces of K . Let r_Q and r'_Q denote their respective dimensions. We have either $r'_Q = r_Q$ and $r'_Q = r_Q - 1$.

Theorem 5. *If $V_Q \neq V'_Q$, then there are no rational points of C_V over Q . Otherwise, the number of rational points of C_V which lie above Q is p^{r_Q} .*

Let S be the set of rational points Q of C such that Q is completely split i.e. $V_Q = V'_Q$ then

$$\#C_V(\mathbb{F}_q) = \sum_{Q \in S} p^{r_Q}$$

We would now like to compute the genus of C_V . Let as before C_f be the covering of the curve C defined by the equation $\rho y = f$. Further let τ_V, τ_f and τ be the traces of the Frobenius acting on the Jacobians of C_V, C_f and C respectively. For $\lambda \in \mathbb{F}_p^*$ we have $C_f \cong C_{\lambda f}$ and so $\tau_f = \tau_{\lambda f}$. Let $\mathbb{P}(V)$ be the complete set

of representatives of $V - \{0\}$ modulo equivalence, where two elements f and f' are equivalent if $f' = \lambda f$ for $\lambda \in \mathbb{F}_p^*$. The following theorem relates τ_V , τ_f and τ .

Theorem 6.

$$\tau_V = \tau + \sum_{f \in \mathbb{P}(V)} \tau_f - \tau$$

Let us denote by P_f the Prym variety of the covering $C_f \rightarrow C$. Then the trace of Frobenius on P_f is equal to $\tau_f - \tau$. We define

$$J := \text{Jac}(C) \times \prod_{f \in \mathbb{P}(V)} P_f.$$

By theorem 6 we have trace of Frobenius on J is the same as the trace of Frobenius on $\text{Jac}(C_V)$. Proceeding similarly we can prove the same result for Frobenius morphism relative to a finite extension of \mathbb{F}_q . Thus the traces of all powers of the Frobenius morphism on J and $\text{Jac}(C_V)$ are equal. But the theorem of Tate claims that this is only possible when these varieties are \mathbb{F}_q -isogenous. We now obtain the genus of C_V from the following theorem we just proved.

Theorem 7. *There is an isogeny relation*

$$\text{Jac}(C_V) \sim \text{Jac}(C) \times \prod_{f \in \mathbb{P}(V)} P_f.$$

In particular $g(C_V) = g(C) + \sum_{f \in \mathbb{P}(V)} (g(C_f) - g(C))$.

References

- [1] Farkas G, Class notes M390C Abelian Varieties.
- [2] Geer G.V.D , Vlugt M.V.D, Constructing Curves over Finite Fields with Many Points.
- [3] Shabat V. , Curves with Many Points , Ph.D thesis, University of Amsterdam, 2002.