Journal of Algebraic Systems
Vol. 6, No. 1, (2018), pp 1-12

MAXIMAL PRYM VARIETY AND MAXIMAL MORPHISM

M. FARHADI*

ABSTRACT. We investigated maximal Prym varieties on finite fields by attaining their upper bounds on the number of rational points. This concept gave us a motivation for defining a generalized definition of maximal curves i.e., maximal morphisms. By MAGMA, we give some non-trivial examples of maximal morphisms that results in non-trivial examples of maximal Prym varieties.

1. INTRODUCTION

The problem of counting the number of rational points of algebraic varieties defined over finite fields absorbs the attention of many researchers, because of their various applications in other branches of science and technology, such as Information Theory, Coding Theory, Cryptography and Physics.

A. Lesfari in [7] had shown the application of Prym varieties. The Kirchhoff's equation that describes the motion of a solid body can be modeled by genus two hyperelliptic functions.

Many papers have published about this important thought of point counting [4, 5, 9, 10, 13, 14]. Our goal is to study the number of rational points of Prym varieties. This concept has studied recently by M. Perret in [8].

Let $\pi : D \mapsto C$ be a covering of smooth algebraic irreducible projective curves defined over a field k of zero or odd character then the

MSC(2010): Primary 14Q05; Secondary 14H40.
Keywords: Prym Variety, maximal curve, maximal morphism.
Received: 17 July 2017, Accepted: 15 November 2017.
*Corresponding author.

Jacobian J_C of C is isogenous to a sub-abelian variety of the Jacobian J_D of D. If, moreover, we suppose that π has degree 2 then the non-trivial involution σ of this covering σ induces an involution σ^* on J_D.

Definition 1.1. The Prym variety $\mathrm{Pr} = \mathrm{Pr}_\pi$ associated to the unramified double covering $\pi : D \mapsto C$ of a curve C of genus $g \geq 2$ is defined as $\mathrm{Pr} := \mathrm{Im}(\sigma^* - id)$. It is an abelian subvariety of J_D of dimension $g-1$ isogenous to a direct factor of J_C in J_D.

Suppose henceforth that k is the finite field $\mathbb{F}_q$ with q elements, Pr is an abelian variety of dimension $g-1$. There is following important question:
When does Prym variety defined over finite fields reache its upper bound on the number of rational points?

This paper contains contributions of defining maximal morphisms and some results about this concept that is a generalization of maximal curves. After, we have found some non-trivial examples of maximal morphisms. This new concept is useful for obtaining examples of maximal Prym varieties.

The remainder of this paper is organized as follows: Section 2 describes the previous literature related to the problem. Suitable definitions to formulate the new concept, maximal morphisms, are presented in Section 3, which is followed in Section 4 by some non-trivial examples that calculated by MAGMA. Section 5 provides some final conclusions.

2. Related works

The following result of Weil formulates the bounds for the number of rational points of an algebraic variety defined over a finite field (see, [14]).

Theorem 2.1 (Weil, 1948)**.** *Let A be an abelian variety of dimension d defined over $\mathbb{F}_q$. Then, there exists $\theta_1, \ldots, \theta_d \in \mathbb{R}/(2\pi\mathbb{Z})$ such that for any $n \geq 1$ the number of rational points of A over $\mathbb{F}_{q^n}$, is given by*

(i) card $A(\mathbb{F}_{q^n}) = \prod_{i=1}^{d} \left(q^n + 1 - 2\sqrt{q^n}\cos\theta_i\right)$ *in particular,*

(ii) $\left(q + 1 - 2\sqrt{q}\right)^d \leq \text{card } A(\mathbb{F}_q) \leq \left(q + 1 + 2\sqrt{q}\right)^d$,

(iii) *If in addition, A is the Jacobian of a curve C of genus g, then $d = g$ and the θ_i are also related to the J_C, then the number of* *rational points of C over $\mathbb{F}_{q^n}$, is given by*

$$\text{card } C(\mathbb{F}_{q^n}) = q^n + 1 - 2\sqrt{q^n}\Big(\sum_{i=1}^{g} \cos n\theta_i\Big).$$

The second part of Theorem 2.1 for the Prym variety Pr_π of a double unramified cover π of a curve C of genus g reads

$$\big(g+1-2\sqrt{q}\big)^{g-1} \leq \text{card}\,\mathrm{Pr}(\mathbb{F}_q) \leq \big(g+1+2\sqrt{q}\big)^{g-1}. \tag{2.1}$$

These upper and lower bounds in (2.1) are the "best possible", in the sense that both can be reached. Indeed, it is known that an elliptic curve is a Prym variety. Now, suppose that E is so that it reaches the upper (resp., lower) bound of Weil's inequality, such an elliptic curve exists if q is square [8], then E reaches the upper (resp., lower) bound of (2.1). The existence of such an elliptic curve E, proves also the second part of (Theorem 2.1) for the Jacobian variety J_C of a curve C,

$$\big(q+1-2\sqrt{q}\big)^{g} \leq \text{card } J_C(\mathbb{F}_q) \leq \big(q+1+2\sqrt{q}\big)^{g}, \tag{2.2}$$

is also best possible at least for $g = 1$. Several sharper lower and upper bounds for Jacobian were also given in the literature, for instance:

Theorem 2.2 (G. Lachaud, M. Martin-Dechamps [6])**.** *Let J_C be the Jacobian variety of a genus g of a curve C defined over $\mathbb{F}_q$ and* card $C(\mathbb{F}_q)$ *be the number of rational points of C. Then*

$$\big(\sqrt{q}-1\big)^2 \frac{\big(q^{g-1}-1\big)\big(\text{card } C(\mathbb{F}_q)+q-1\big)}{g(q-1)} \leq \text{card } J_C(\mathbb{F}_q). \tag{2.3}$$

If C admits a map of degree n onto the projective line, then one has also

$$\text{card } J_C(\mathbb{F}_q) \leq \frac{e}{q}\big(2g\sqrt{e}\big)^{n-1} q^g. \tag{2.4}$$

In [8], Marc Perret presented some bounds for Prym variety. Let C be an algebraic curve and the number of $\mathbb{F}_q$–rational points of C denoted by card $C(\mathbb{F}_q)$.

Theorem 2.3. *Let C be an absolutely irreducible projective smooth algebraic curve defined over the finite field k of the odd characteristic with q elements. Let also g be the genus of C and $\pi : D \mapsto C$ be an unramified covering of degree 2. Then,*

(i)

$$\Big(\frac{\sqrt{q}+1}{\sqrt{q}-1}\Big)\Big(\frac{\text{card } D(\mathbb{F}_q) - \text{card } C(\mathbb{F}_q)}{(2\sqrt{q})} - 2\delta\Big)(q-1)^{g-1} \leq \text{card}\,\mathrm{Pr}(\mathbb{F}_q)$$

with

$$\delta = \begin{cases} 1 & \textit{if } \frac{\text{card } D(\mathbb{F}_q) - \text{card } C(\mathbb{F}_q)}{2\sqrt{q}} \in \mathbb{Z}; \\ 0 & \textit{otherwise.} \end{cases}$$

(ii)

$$\text{card}\,\text{Pr}(\mathbb{F}_q) \leq \Big(q + 1\frac{\text{card } D(\mathbb{F}_q) - \text{card } C(\mathbb{F}_q)}{g-1}\Big)^{g-1}.$$

Remark 2.4. Let X be a curve with genus g defined over $\mathbb{F}_q$. There is a formal series over X relative to $\mathbb{F}_q$ called *Zêta Function*:

$$Z_{X,q}(t) := \exp\Big(\sum_{i=1}^{\infty} \frac{\text{card } X(\mathbb{F}_{q^i})}{i} t^i\Big). \tag{2.5}$$

There exists a polynomial of degree $2g$ with integer coefficients, such that

$$Z_{X,q}(t) = \frac{P(t)}{(1-t)(1-q^t)}. \tag{2.6}$$

Remark 2.5. [12]

(i) Let

$$P(t) = \sum_{i=0}^{2g} a_i t^i, \tag{2.7}$$

then $a_0 = 1$, $a_{2g} = q^g$ and $a_{2g-i} = q^{g-i} a_i$ for $i = 0, \dots, g$.

(ii) Let

$$h(t) = h_{X,q}(t) := t^{2g} P(t^{-1}). \tag{2.8}$$

Then, the $2g$ roots (counted with multiplicity) $\alpha_1, \dots, \alpha_{2g}$ of $h(t)$ can be arranged such that $\alpha_j \alpha_{g+j} = q$ for $j = 1, \dots, g$. Note that, $a_1 = -\sum_{j=1}^{2g} \alpha_j$.

Now, let J_X be the Jacobian of X. According to Theorem 2.1, we know that $h(t)$ is exactly the characteristic polynomial of Fr J_X on the Tate module, where Fr is the Frobenius endomorphism (relative to $\mathbb{F}_q$).

Now, let C and D be two curves and $\pi : D \mapsto C$ a unramified double covering. We know that the Prym variety Pr_π is a direct factor of J_C in J_D.

Theorem 2.6 (Y. Aubry, M. Perret [1])**.** *Let $\pi : D \mapsto C$ be a finite morphism between two reduced algebraic smooth absolutely irreducible projective curves D and C defined over a finite field k. Then, the numerator of the zeta function of C divides that of D in $\mathbb{Z}[t]$.*

Proof. For any prime ℓ different to the characteristic of $\mathbb{F}_q$, we consider the $\mathbb{Q}_\ell$–vector space $T_\ell(J_C) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ of dimension $2g_C$, where $T_\ell(J_X)$ is the Tate module of Jacobian J_C of C. The numerator $h_{C,q}(t)$ of the zeta function of C is the reciprocal characteristic polynomial of Frobenius endomorphism on $T_\ell(J_C) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. The function

$$\pi^* : J_C \longrightarrow J_D,$$

which is induced by π on Jacobian, is of the finite kernel, and sends every point of ℓ^n–torsion of J_C on points of ℓ^n–torsion of J_D. So, we have a morphism injective of $\mathbb{Q}_\ell$–vector spaces

$$\pi^* \otimes 1 : T_\ell(J_C) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \longrightarrow T_\ell(J_D) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

The Frobenius morphism in $T_\ell(J_D) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a stable subspace of the Frobenius morphism in $T_\ell(J_C) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Therefore, the characteristic polynomial of $T_\ell(J_C)$ divides the characteristic polynomial of $T_\ell(J_D)$ in $\mathbb{Q}[t]$, and hence in $\mathbb{Z}[t]$, since $h_C, h_D \in \mathbb{Z}[t]$. Thus, we conclude that $h_C(t)$ divides $h_D(t)$. □

3. Relative maximal morphisms

In this section, we give the definition of maximal morphism, which generalizes the concept of famous maximal curve.

A. Weil [14], had shown that the number of $\mathbb{F}_q$-rational points of the curve C of genus g satisfies

$$q + 1 - 2g\sqrt{q} \leq \text{card } C(\mathbb{F}_q) \leq 1 + q + 2g\sqrt{q}.$$

J. P. Serre [9, 10], improved Weil's upper bound. If q is not square, then

$$\text{card } C(\mathbb{F}_q) \leq q + 1 + g[2\sqrt{g}].$$

A curve is called *Weil* (*Serre*) *maximal* if it gets the Weil (Serre) upper bound of $\mathbb{F}_q$-rational points. Many works have published about maximal curves and related concepts [4, 5, 9, 10, 13, 14].

Corollary 3.1. *If $\pi : D \mapsto C$ is a surjective morphism between irreducible smooth projective algebraic curves on a finite field $\mathbb{F}_q$, then*

$$\left|\text{card } D(\mathbb{F}_q) - \text{card } C(\mathbb{F}_q)\right| \leq 2\big(g_D - g_C\big)\sqrt{q}.$$

Proof. According to Theorem 2.6, all eigenvalues of Frobenius endomorphism on $T_\ell(J_D)$ with multiplicity, contains that of Frobenius endomorphism on $T_\ell(J_C)$. We then apply Theorem 2.1 (iii), and the result follows. □

Proposition 3.2. *If $\pi : D \mapsto C$ is a surjective morphism between irreducible smooth projective algebraic curves on a finite field, then*

$$\left|\text{card } D(\mathbb{F}_q) - \text{card } C(\mathbb{F}_q)\right| \leq \left(g_D - g_C\right)\left[2\sqrt{q}\right].$$

Proof. Let $A \subset \mathbb{C}$ be the set of algebraic integers, i.e., a complex number α is in A if and only if α satisfies in equation $\alpha^m + b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0 = 0$ for coefficients $b_i \in \mathbb{Z}$. It is an elementary fact of algebraic number theory that

$$A \text{ is subring of } \mathbb{C}, \text{ and } A \cap \mathbb{Q} = \mathbb{Z}. \tag{3.1}$$

We consider the L-polynomial $L_D(t) = \prod_{i=1}^{2g_D}(1 - \alpha_i t)$ and $L_C(t) = \prod_{i=1}^{2g_C}(1-\beta_i t)$. Complex numbers $\alpha_1, \ldots, \alpha_{2g_D}$ are the algebraic integers with $|\alpha_i| = q^{1/2}$ (Theorems V.2.1 and V.1.15 of [12]). They can be arranged so that $(\alpha_1, \ldots, \alpha_{2g_C}, \alpha_{2g_C+1}, \ldots, \alpha_{2g_D}) = (\beta_1, \ldots, \beta_{2g_C}, \beta_{2g_C+1}, \ldots, \beta_{2g_D})$ and $\alpha_i\alpha_{g_D+i} = q$. Therefore,

$$\overline{\alpha_i} = \alpha_{g+i} = q/\alpha_i \text{ for } 1 \leq i \leq g_D.$$

(We denote by $\overline{\alpha}$ the complex conjugate of α.) Let

$$\gamma_i := \alpha_i + \overline{\alpha_i} + \left[2q^{1/2}\right] + 1$$

and

$$\delta_i := -(\alpha_i + \overline{\alpha_i}) + \left[2q^{1/2}\right] + 1.$$

According to (3.1), γ_i and δ_i are algebraic integers and since $|\alpha_i| = q^{1/2}$, they satisfy

$$\gamma_i > 0, \;\; \delta_i > 0. \tag{3.2}$$

Let $\prod_{i=1}^{2g_D}(t - \alpha_i) = L_D^{\perp}(t) \in Z(t)$, $\prod_{i=1}^{2g_C}(t - \beta_i) = L_C^{\perp}(t) \in Z(t)$ and $L_D^{\perp}(t) = L_C^{\perp}(t)\prod_{i=1}^{2g_D-2g_C}(t - \alpha_i)$. Any extension

$$\sigma : \mathbb{Q}(\alpha_1, \ldots, \alpha_{2g_D-2g_C}) \to \mathbb{C},$$

permute $\alpha_1, \ldots, \alpha_{2g_D-2g_C}$, since $\prod_{i=1}^{2g_D-2g_C}(t-\alpha_i) \in Z(t)$. On the other hand, if $\sigma(\alpha_i) = \alpha_j$ then,

$$\sigma(\overline{\alpha_i}) = \sigma(q/\alpha_i) = q/\sigma(\alpha_i) = \overline{\sigma(\alpha_i)} = \overline{\alpha_j}.$$

Therefore, σ acts as a permutation over the sets $\{\gamma_1, \ldots, \gamma_{g_D-g_C}\}$ and $\{\delta_1, \ldots, \delta_{g_D-g_C}\}$. Define

$$\gamma := \prod_{i=1}^{g_D-g_C} \gamma_i \text{ and } \delta := \prod_{i=1}^{g_D-g_C} \delta_i.$$

Then, γ and Δ are algebraic integers invariants in all extensions of $Q(\alpha_1, \ldots, \alpha_{2g_D-2g_C})$ in C. Therefore, $\gamma, \delta \in \mathbb{Q} \bigcap A = \mathbb{Z}$. With (3.2), $\gamma > 0$ and $\delta > 0$, and hence

$$\prod_{i=1}^{g_D-g_C} \gamma_i \geq 1 \text{ and } \prod_{i=1}^{g_D-g_C} \delta_i \geq 1.$$

The well-known inequality between arithmetic and geometry gives

$$\frac{1}{(g_D-g_C)} \sum_{i=1}^{g_D-g_C} \gamma_i \geq \Big(\prod_{i=1}^{g_D-g_C} \gamma_i \Big)^{1/(g_D-g_C)} \geq 1.$$

Therefore,

$$\begin{aligned} g_D - g_C &\leq \Big(\sum_{i=1}^{g_D-g_C} \big(\alpha_i + \overline{\alpha_i}\big) \Big) + (g_D-g_C)\big[2q^{1/2}\big] + g_D - g_C \\ &= \sum_{i=1}^{2g_D-2g_C} \alpha_i + (g_D-g_C)\big[2q^{1/2}\big] + g_D - g_C. \end{aligned}$$

By observing that $\sum_{i=1}^{2g_D-2g_C} \alpha_i = N$, we get

$$N \leq (g_D-g_C)\big[2q^{1/2}\big].$$

In the same way, inequality

$$\frac{1}{(g_D-g_C)} \sum_{i=1}^{g_D-g_C} \delta_i \geq \Big(\prod_{i=1}^{g_D-g_C} \delta_i \Big)^{1/(g_D-g_C)} \geq 1,$$

gives

$$N \geq -(g_D-g_C)\big[2q^{1/2}\big].$$

□

Remark 3.3. Since Pr has dimension $g-1$, we already saw in the Theorem 2.1 that

$$\big(q+1-2\sqrt{q}\big)^{g-1} \leq \operatorname{card} \Pr(\mathbb{F}_q) \leq \big(q+1+2\sqrt{q}\big)^{g-1}.$$

On the other hand, we know card $J_C(\mathbb{F}_q) = \prod_{\omega \in Spec\mathbb{F}(C)}(1-\omega)$ and $|\omega| = 2\sqrt{q}$ for all $\omega \in Spec\mathbb{F}(C)$. So,

$$-2(g-1)\sqrt{q} \leq \text{card } D(\mathbb{F}_q) - \text{card } C(\mathbb{F}_q) \leq 2(g-1)\sqrt{q}.$$

Hence, our bounds in theorem are dependent to card $D(\mathbb{F}_q)-$card $C(\mathbb{F}_q)$ and are always "better" than Weil's one (in the sense that, for instance, our upper bound is smaller than Weil's one).

Hence, if card $D(\mathbb{F}_q)$ − card $C(\mathbb{F}_q)$ reaches the upper bound, then $\Pr(\mathbb{F}_q)$ will have the maximal number of rational points if Prym variety is in the Jacobian form.

Definition 3.4. A Prym variety $\Pr_\pi$ is maximal if it attains the upper bound of the number of rational points, where π is a double unramified covering between two curves.

Remark 3.5. We know $\Pr_\pi$ is an abelian subvariety of J_D. Historically, Prym varieties were considered interesting exclusivity, because they give examples of principally polarized abelian varieties that are not Jacobian varieties. However, if $\dim(\Pr_\pi) \leq 2$, then $\Pr_\pi$ generally is a Jacobian variety (see, [3]).

Definition 3.6. Let $\pi : D \mapsto C$ is a double unramified covering and C, D are two smooth, irreducible curves. We say π is a Weil maximal morphism on $\mathbb{F}_q$ if card $D(\mathbb{F}_q)$ − card $C(\mathbb{F}_q) = 2(g-1)\sqrt{q}$. Similarly, we can define Serre maximal morphism (optimal maximal morphism).

Definition 3.7. Let $\pi : D \mapsto C$ be a unbranched double covering between two smooth, projective, irreducible curves. We say that π is a *Serre-maximal morphism* over $\mathbb{F}_q$, if

$$\text{card } D(\mathbb{F}_q) - \text{card } C(\mathbb{F}_q) = (g-1)\left[2\sqrt{q}\right].$$

Proposition 3.8. *Let* $\Pr_\pi \cong Jac(E)$. *If* π *is a Weil maximal morphism, then* $\Pr_\pi$ *is also Weil maximal.*

Proof. We know that $\Pr_\pi$ is a direct factor of J_C in J_D and the number of eigenvalues of $\mathrm{Fr}_{\Pr_\pi}$ is exactly $2(g-1)$. Hence, $\Pr_\pi$ is maximal if and only if each proper value ω_i verifies $\omega_i = -\sqrt{q}$. This property is equivalent to the maximality of π. □

Theorem 3.9. *Suppose that* $\Pr_\pi \cong Jac(F)$ *for a curve* F. *Then, the following assertions are equivalent:*

(i) π *is Weil-maximal;*
(ii) $\Pr_\pi$ *is Weil-maximal;*
(iii) F *is Weil-maximal.*

Proof. (i)⇔(ii): We know that $\Pr_\pi$ is a direct factor of J_C in J_D and the number of eigenvalues of $\mathrm{Fr}_{\Pr_\pi}$ with multiplicity is exactly $2(g-1)$. Therefore, $\Pr_\pi$ is maximal if and only if each proper value ω_i verifies $\omega_i = -\sqrt{q}$. This property is equivalent to the maximality of π.
(ii)⇔(iii): In fact, we must prove also $\mathrm{Jac}(F)$ is maximal if and only if F is maximal. Thanks to Theorem (i), (iii) we have $\theta_i = \pi$ for all i. □

Theorem 3.10. *Suppose that* $\mathrm{Pr}_\pi \cong Jac(F)$ *for a curve* F. *Then, the following assertions are equivalent:*

(i) π *is Serre-maximal;*
(ii) F *is Serre-maximal.*

Proof. (i)$\Rightarrow$(ii): π is Serre maximal if $\left|\mathrm{Tr}_{\mathrm{Fr}_{\mathrm{Pr}_\pi}}\right| = (g-1)\left[2\sqrt{q}\right]$. But $\mathrm{Pr}_\pi \cong \mathrm{Jac}(F)$, so $\left|\mathrm{Tr}_{\mathrm{Fr}_{\mathrm{Jac}_F}}\right| = (g-1)\left[2\sqrt{q}\right]$. With [9, Theorem 1], we have equality if and only if the characteristic polynomial of $\mathrm{Fr}_{\mathrm{Pr}_\pi}$ is equal to $\left(X^2 \pm mX + q\right)^{g-1}$, where $m = \left[2\sqrt{q}\right]$. Then every eigenvalue of Tate matrix $\mathrm{Fr}_{\mathrm{Jac}_F}$ is equal to $[\sqrt{q}]$.
(ii)$\Rightarrow$(i): If F is Serre maximal, then $\left|\mathrm{Tr}_{\mathrm{Fr}_{\mathrm{Jac}_F}}\right| = (g-1)\left[2\sqrt{q}\right]$. But we know that $\mathrm{Pr}_\pi \cong \mathrm{Jac}(F)$ and $\left|\mathrm{Tr}_{\mathrm{Fr}_{\mathrm{Pr}_\pi}}\right| = (g-1)\left[2\sqrt{q}\right]$, then π is Serre maximale. ☐

Proposition 3.11. *If D is a Weil maximal curve, then C is Weil maximal and every double covering $\pi : D \mapsto C$ is Weil maximal.*

Proof. With the maximality of D, we know that all eigenvalues of $T_\ell(J_D)$ are equal to $-\sqrt{q}$. Then, using Theorem 3.9, we get the desired result. ☐

Remark 3.12. The Proposition 3.11 will be correct if we replace Weil maximal morphism with *Serre maximal morphism* or optimal morphism.

Remark 3.13. If C or D is a maximal curve, then any unramified double covering $\pi : D \mapsto C$ is maximal morphism. Hence, this case gives the trivial examples of maximal morphisms.

4. Some non-trivial examples

Are there some non-trivial maximal morphisms or equivalently maximal Prym varieties in Jacobian form?

In this section, we try to give some non-trivial explicit examples by the result of [3], and by MAGMA [2] (a software package designed to solve the computationally hard problem in algebra, ...).

In fact, with [3] in characteristic zero, we have some cases that Prym varieties are isomorph with Jacobian varieties. In fact, [3] gives examples of isomorphisms of Prym varieties that are Jacobian varieties.

Let C be the double covering of $\mathbb{P}^1$. Then, C has an affine model

$$C : y^2 = f(x),$$

where $f \in k[x]$ is a square-free polynomial of degree $2g_C+2$. According to *Kummer's theory*, for any factorization $f = F_1F_2$, with $F_1, F_2 \in k[x]$

of an even degree, we have a curve D which is given by the affine model:

$$\begin{tikzcd}
 & D \arrow[dl, "\pi_1"'] \arrow[d, "\pi"] \arrow[dr, "\pi_2"] & \\
F_1 \arrow[dr, "x"'] & C \arrow[d, "x"] & F_2 \arrow[dl, "x"] \\
 & \mathbb{P}^1 &
\end{tikzcd}$$

$$\begin{cases} y_1^2 = F_1(x) \\ y_2^2 = F_2(x), \end{cases} \tag{4.1}$$

and a unramified morphism of degree 2

$$\pi : D \mapsto C$$
$$(x, y_1, y_2) \mapsto (x, y_1 y_2) = (x, y).$$

Consider two curves

$$F_1 : y_1^2 = F_1(x)$$
and
$$F_2 : y_2^2 = F_2(x),$$

with the obvious projections $\pi_1 : D \to F_1$ and $\pi_2 : D \to F_2$.

Proposition 4.1. [3] *Let C, D, F_1, F_2, π, π_1, π_2 be as defined above. Then,*

$$\pi_1^* \times \pi_2^* : Jac(F_1) \times Jac(F_2) \to Prym(D/C),$$

is an isomorphism of abelian varieties.

Remark 4.2. By letting $\deg F_1(x) = 2$ in Proposition 4.1, we have $F_1 : y_1^2 = F_1(x)$ is of genus 0. Then, $F_1 \cong P_1$, and therefore

$$Jac(F_1) \times Jac(F_2) \cong Jac(F_2) \cong \mathrm{Prym}(D/C).$$

Remark 4.3. Consider the affine forms of curves C, D and F. Suppose that $C : y^2 = Q(x)R(x)$, where $\deg(Q) = 2$, $\deg(R) = 6$ and $D : y_1^2 = Q(x)$ and $y_2^2 = R(x), F : y^2 = R(x)$. Consider $\pi : D \mapsto C$ is double unramified covering then $\mathrm{Pr}_\pi \cong \mathrm{Jac}(F)$, so for obtaining nontrivial examples of maximal morphisms we have to find some examples such that D, C are not maximal curves. However, F is a maximal curve with MAGMA, we can attain some examples of nontrivial morphisms. Now, we give an example that we calculated with MAGMA.

Consider the field $\mathbb{F}_{81}$ and let $R(x) = x^6 + x^5 + x^4 + x^3 + 2x^2 + 2x + \alpha^{50}$ and $Q(x) = x^2 + x + \alpha$, where α is a primitive element of $\mathbb{F}_{81}$. The following table, prepared with MAGMA, give us some nontrivial examples of maximal morphism (and hence maximal Prym variety).

q	81
C	$y^2 = x^8 + 2x^7 + \alpha^{77}x^6 + \alpha^{77}x^5 + \alpha x^4 + \alpha^{28}x^3 + \alpha^{12}x^2 + \alpha^{53}x + \alpha^{51}$
D	$y_1^2 = x^2 + x + \alpha,\ y_2^2 = x^6 + x^5 + x^4 + x^3 + 2x^2 + 2x + \alpha^{50}$
F	$y^2 = x^6 + x^5 + x^4 + x^3 + 2x^2 + 2x + \alpha^{50}$
q	81
C	$y^2 = x^8 + 2x^7 + \alpha^{70}x^6 + \alpha^{70}x^5 + \alpha^{10}x^4 + \alpha^{20}x^3 + \alpha^{70}x^2 + \alpha^{10}x + \alpha^{60}$
D	$y_1^2 = x^2 + x + \alpha,\ y_2^2 = x^6 + x^5 + x^4 + x^3 + 2x^2 + 2x + \alpha^{50}$
F	$y^2 = x^6 + x^5 + x^4 + x^3 + 2x^2 + 2x + \alpha^{50}$

5. Conclusion

Finding non-trivial examples of maximal Prym variety, grants us the motivation for defining a new concept which we call maximal morphism, that is a generalization of maximal curves.

Acknowledgments

I would like to thank Marc Perret "my Ph.D. thesis supervisor", for all of the discussions on Prym varieties and my student, Hamideh Baypoor for her helps in preparing the paper.

References

1. Y. Aubry, and M. Perret, Divisibility of zeta functions of curves in a covering, *Arkiv der Math.* **82** (2004), 205–213.
2. W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.* **24** (1997), 235–265.
3. N. Bruin, The arithmetic of Prym varieties in genus 3, *Compos. Math.* **144** (2008), 317–338.
4. M. Farhadi, Les morphismes relativement maximaux et les codes de Goppa, Unpublished doctoral thesis. Universite de Toulouse, Toulouse, France, 2007.
5. A. Kazemifard, A. R. Naghipour and S. Tafazolian, A Note on Superspecial and Maximal Curves, *Bull. Iran. Math. Soc.*, **39(3)** (2013), 405–413.
6. G. Lachaud, and M.Martin-Deschamps, Nombre de points des jacobienne sur un corps fini, *Acta Arith Math. LVI.* **56(4)** (1990), 320–329.
7. A. Lesfari, Prym varieties and applications. *J. Geometry Physics*, **58(9)** (2008), 1063–1079.
8. M. Perret, On the number of points of Prym varieties over finite fields, *Glasg. Math. J.*, **48** (2006), 275–280.

9. J. P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C. R. Acad. Sci. Paris*, **Série I** (1983), 397–402.
10. J. P. Serre, Rational points on curves over finite fields, unpublished notes by F. Q. Gouvéa of lectures at Harvard University, 1985.
11. I. R. Shafarevich, *Basic Algebraic Geometry 1 varieties in projective space*, Spriger-Verlag, Berlin, 1994.
12. H. Stichtenoth, *Algebraic function fields and codes*, Springer Verlag, Berlin, 1993.
13. K. O. Stohr, and J. F. Voloch, Weierstrass points and curves over finite fields. *Proc. London Math. Soc.*, **52** (1986), 1–19.
14. A. Weil, *Courbes algebrique et variétés abélienne*, Hermann, Paris, 1978.

Majid Farhadi
School of Mathematics and Computer Science, University of Damghan, Damghan, Iran.
Email: `farhadi@du.ac.ir`

Journal of Algebraic Systems

Maximal Prym variety and maximal morphism

M. Farhadi

چندگوناهای پرایم ماکسیمال و مرفیسم‌های ماکسیمال

مجید فرهادی
دانشکده ریاضی دانشگاه دامغان، ایران، دامغان

ما چندگوناهای پرایم ماکسیمال را از این منظر که کران بالای تعداد نقاط گویا روی میدان‌های متناهی را بگیرد، بررسی کردیم. این مفهوم، انگیزه تعریف مرفیسم‌های ماکسیمال تعمیم مفهوم خم‌های ماکسیمال را می‌دهد. با کمک ماگما، مثال‌هایی نابدیهی از مرفیسم‌های ماکسیمال ارائه کرده‌ایم که مثال‌های نابدیهی از چندگوناهای پرایم ماکسیمال را نتیجه می‌دهد.

کلمات کلیدی: چندگونای پرایم، خم ماکسیمال، مرفیسم ماکسیمال.