известного результата о представлении произвольной перестановки в виде произведения транспозиций.

Элементарные и перестановочные сети являются примерами простейших биективных сетей и, как показывает следующая теорема, этих примитивов достаточно для реализации произвольной биективной сети постоянной ширины.

Теорема 1. Сеть Σ постоянной ширины является биективной для некоторого множества Ω, $|\Omega| \geqslant 2$, в том и только в том случае, когда она эквивалентна произведению

$$\Pi_L \cdot \Sigma_{L,1} \cdot \ldots \cdot \Sigma_{L,t} \text{ (или } \Sigma_{R,1} \cdot \ldots \cdot \Sigma_{R,t} \cdot \Pi_R),$$

где Π_L (Π_R) — перестановочная сеть; $\Sigma_{L,1}, \ldots, \Sigma_{L,t}$ ($\Sigma_{R,1}, \ldots, \Sigma_{R,t}$) — элементарные сети. При этом длина произведения равна количеству вершин сети Σ со степенью захода 2 и соответственно не зависит от выбора представления.

Следствие 1. Если сеть Σ постоянной ширины является биективной для некоторого множества Ω, $|\Omega| \geqslant 2$, то сеть Σ является биективной для всех множеств.

Указанные в теореме 1 представления биективной сети Σ в виде произведения элементарных сетей будем называть *каноническими представлениями* сети Σ. Количество вершин сети Σ со степенью захода 2 будем называть *весом* сети Σ и обозначать $\|\Sigma\|$.

Биективную сеть Σ будем называть *транзитивной для множества* Ω, если множество отображений $\{\Sigma^F : F \in \mathcal{Q}(\Omega)\}$ является транзитивным. Основным результатом работы можно считать разработанный автором аппарат разметки сетей, который позволяет проверить транзитивность произвольной биективной сети, а при отрицательном ответе определить особенности строения сети, противоречащие транзитивности. С помощью этого аппарата, например, доказывается следующая теорема.

Теорема 2. Если биективная сеть Σ постоянной ширины является транзитивной для некоторого множества Ω, $|\Omega| \geqslant \|\Sigma\|$, то сеть Σ является транзитивной для любого множества, мощность которого строго больше чем $\|\Sigma\|$.

Стоит отметить, что аппарат разметки позволяет сформулировать и обосновать алгоритм модификации канонического представления произвольной биективной сети Σ постоянной ширины n. В результате применения алгоритма получается биективная сеть $\widehat{\Sigma}$ веса $\|\widehat{\Sigma}\| \leqslant \|\Sigma\| + 4n$, которая является транзитивной для большей части множеств.

Теорема 3. Модификация $\widehat{\Sigma}$ произвольной сети Σ является транзитивной для любого множества, мощность которого строго больше чем $\|\widehat{\Sigma}\|$.

Автор благодарит профессора А. В. Черемушкину за постановку задачи и внимание к проводимым исследованиям.

UDC 512.772.7 DOI 10.17223/2226308X/10/11

HYPERELLIPTIC CURVES, CARTIER — MANIN MATRICES AND LEGENDRE POLYNOMIALS

S. A. Novoselov

We investigate the hyperelliptic curves of the form $C_1 : y^2 = x^{2g+1} + ax^{g+1} + bx$ and $C_2 : y^2 = x^{2g+2} + ax^{g+1} + b$ over the finite field $\mathbb{F}_q$, $q = p^n$, $p > 2$. We transform these curves to the form $C_{1,\rho} : y^2 = x^{2g+1} - 2\rho x^{g+1} + x$ and $C_{2,\rho} : y^2 = x^{2g+2} - 2\rho x^{g+1} + 1$ and

prove that the coefficients of corresponding Cartier — Manin matrices are Legendre polynomials. As a consequence, the matrices are centrosymmetric and, therefore, it's enough to compute a half of coefficients to compute the matrix. Moreover, they are equivalent to block-diagonal matrices under transformation of the form $S^{(p)}WS^{-1}$. In the case of $\gcd(p, g) = 1$, the matrices are monomial, and we prove that characteristic polynomial of the Frobenius endomorphism $\chi(\lambda) \pmod p$ can be found in factored form in terms of Legendre polynomials by using permutation attached to the monomial matrix. As an application of our results, we list all the possible polynomials $\chi(\lambda) \pmod p$ for the case of $\gcd(p, g) = 1$, $g \in \{1, \ldots, 7\}$ and the curve C_1 is over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$.

Keywords: *hyperelliptic curve cryptography, Cartier — Manin matrix, Legendre polynomials.*

Let $\mathbb{F}_q$ be a finite field, $q = p^n$, $p > 2$. A hyperelliptic curve of genus g over $\mathbb{F}_q$ is a nonsingular curve, given by equation

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

where $f \in \mathbb{F}_q[x]$, f — monic, $\deg f = 2g + 1$ or $\deg f = 2g + 2$.

Hyperelliptic curves were first proposed for use in cryptography by Koblitz [1]. Every hyperelliptic curve has an associated group — its Jacobian $J_C(\mathbb{F}_q)$, where all computations take place. For applications in cryptography it is required to compute the order of $J_C(\mathbb{F}_q)$, which is equivalent to computing of the characteristic polynomial of the Frobenius endomorphism $\chi(\lambda)$ of the J_C.

Let $f(x)^{(p-1)/2} = \sum\limits_{i=0}^{(\deg f)(p-1)/2} c_i x^i$. Then the Cartier — Manin matrix of the hyperelliptic curve C is a matrix $W = (w_{i,j}) = (c_{ip-j})$ of the size $g \times g$.

Manin [2] showed that the characteristic polynomial of the matrix W is connected with the polynomial $\chi(\lambda)$ in the following way. Let $W_p = W \cdot W^{(p)} \cdot \ldots \cdot W^{(p^{n-1})}$, where $W^{(p^k)} = (w_{i,j}^{p^k})$, then

$$\chi(\lambda) \equiv (-1)^g \lambda^g |W_p - \lambda I_g| \pmod p.$$

If the polynomial $\chi(\lambda) \bmod p$ is known, we can use Hasse — Weil bound in combination with other methods to recover the polynomial $\chi(\lambda)$.

The Cartier — Manin matrices in general can be computed by optimized algorithms from [3, 4]. In our work we show that for specific curves we only need to compute a half of elements to find all matrix. Moreover, in the case of $\gcd(p, g) = 1$ we can find all the possible variants of the polynomial $\chi(\lambda) \bmod p$ in explicit form in terms of Legendre polynomials.

In this work we study hyperelliptic curves of the form

$$C_1 : y^2 = x^{2g+1} + ax^{g+1} + bx \quad \text{and} \quad C_2 : y^2 = x^{2g+2} + ax^{g+1} + b.$$

These curves are isomorphic to curves

$$C_{1,\rho} : y^2 = x^{2g+1} - 2\rho x^{g+1} + x \quad \text{and} \quad C_{2,\rho} : y^2 = x^{2g+2} - 2\rho x^{g+1} + 1$$

over the field $K = \mathbb{F}_q[\sqrt{b}]$. Therefore, we can restrict discussion to the case of $C_{1,\rho}, C_{2,\rho}$ and our results for polynomials $\chi(\lambda)$ holds over $\mathbb{F}_q$ if b is square and over $\mathbb{F}_{q^2}$ if b is not square in $\mathbb{F}_q$. These forms of curves are generalizations of Jacobi quartics [5].

The curves C_1, C_2 were first studied by Miller and Lubin [6], who proved that the Cartier — Manin matrices of these curves are generalized permutation (monomial) matrices. For

$g = 1$ these curves are elliptic curves. It is known that number of points of elliptic curves is congruent to Legendre polynomials [5, 7]. In this work we generalize this to the $g > 1$ case. We prove first that coefficients of the Cartier — Manin matrix of $C_{1,\rho}$ are either zeroes or Legendre polynomials.

Theorem 1. Let $W = (w_{i,j})$ be a Cartier — Manin matrix of the curve $C_{1,\rho}$. Then

1) $w_{i,j} = 0$, if $ip - j \not\equiv (p-1)/2 \pmod{g}$;
2) $w_{i,j} \equiv P_{(ip-j)/g-(p-1)/(2g)}(\rho) \pmod{p}$, otherwise.

Then using properties of Legendre polynomials [8] we get result.

Theorem 2. The Cartier — Manin matrix of the curve $C_{1,\rho}$ is centrosymmetric in $\mathbb{F}_q$.

Therefore, it's sufficient to compute a half of coefficients for computation of this matrix.

The Cartier — Manin matrix W of any hyperelliptic curve is defined upto transformation of the form $S^{(p)}WS^{-1}$, where S is non-singular [9]. Since centrosymmetic matrices are orthogonally similar to block-diagonal matrices, we can prove theorem.

Theorem 3. The Cartier — Manin matrix W of $C_{1,\rho}$ is equivalent to a block-diagonal matrix via transformation of the form $S^{(p)}WS^{-1}$.

Analogous results can be proved for the curve $C_{2,\rho}$.

Theorem 4. Let $W = (w_{i,j})$ be a Cartier — Manin matrix of $C_{2,\rho}$. Then

1) $w_{i,j} = 0$, if $ip \not\equiv j \pmod{g+1}$;
2) $w_{i,j} \equiv P_{(ip-j)/(g+1)}(\rho) \pmod{g+1}$;
3) W is a centrosymmetric matrix in $\mathbb{F}_q$;
4) W is equivalent to block-diagonal matrix via transformation of the form $S^{(p)}WS^{-1}$.

In the case of $\gcd(p, g) = 1$ the Cartier — Manin matrix of the curve $C_{1,\rho}$ is monomial and we get an explicit formula for $\chi(\lambda) \bmod p$.

Theorem 5. Let the curve $C_{1,\rho}$ is defined over the finite field $\mathbb{F}_q$, $q = p^n$, $\gcd(p, g) = 1$ and W be a Cartier — Manin matrix of $C_{1,\rho}$. Then W is a monomial matrix with a permutation σ, such that $\sigma(i) \equiv ip - (p-1)/2 \pmod{g}$ and W_p is a monomial matrix with permutation σ^n, $\sigma^n(i) \equiv ip^n - (p^n - 1)/2 \pmod{g}$. If $W_p = (w'_{i,j})$ and $\sigma^n = \sigma_1\sigma_2 \dots \sigma_m$ is a decomposition of σ^n into disjoint cycles, then

$$\chi(\lambda) \equiv \lambda^g \prod_{j=1}^{m} \left(\lambda^{|\sigma_j|} - \prod_{k=1}^{|\sigma_j|} w'_{\sigma_{j,k},\sigma_{j,k+1}} \right) \pmod{p},$$

where $\sigma_{j,k} = j_k$ for $\sigma_j = (j_1, \dots, j_{|\sigma_j|})$.

Coefficients $w'_{i,j}$ of W_p can be computed by using formula:

$$W_p = (w'_{i,j}) = \left(w^{p^{n-1}}_{\sigma^{n-1}(i),j} \prod_{k=0}^{n-2} w^{p^k}_{\sigma^k(i),\sigma^{k+1}(i)} \right).$$

As application of our methods we found all the possible variants of polynomials $\chi(\lambda) \bmod p$ for the case of $\gcd(g, p) = 1$, $p > 2$, and the curve C_1 over fields $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$.

REFERENCES

1. *Koblitz N.* Hyperelliptic cryptosystems. J. Cryptology, 1989, vol. 1, no. 3, pp. 139–150.
2. *Manin Y. I.* O matritse Khasse — Vitta algebraicheskoy krivoy [The Hasse — Witt matrix of an algebraic curve]. Izv. Akad. Nauk USSR, Ser. Mat., 1961, vol. 25, no. 1, pp. 153–172. (in Russian)
3. *Bostan A., Gaudry P., and Schost; E.* Linear recurrences with polynomial coefficients and application to integer factorization and Cartier — Manin operator. SIAM J. Comput., 2007, vol. 36, no. 6, pp. 1777–1806.
4. *Harvey D. and Sutherland A. V.* Hasse — Witt matrices of hyperelliptic curves in average polynomial time. LMS J. Comput. Math., 2014, vol. 17, no. A, pp. 257–273.
5. *Yui N.* Jacobi quartics, Legendre polynomials and formal groups. Lecture Notes in Mathematics, 1988, vol. 1326, pp. 182–215.
6. *Miller L.* The Hasse — Witt matrix of special projective varieties. Pacific J. Math., 1972, vol. 43, no. 2, pp. 443–455.
7. *Brillhart J. and Morton P.* Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial. J. Number Theory, 2004, vol. 106, no. 1, pp. 79–111.
8. *Carlitz L.* Congruence properties of the polynomials of Hermite, Laguerre and Legendre. Mathematische Zeitschrift, 1953, vol. 59, pp. 474–483.
9. *Yui N.* On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. J. Algebra, 1978, vol. 52, no. 2, pp. 378–410.