J. Timmis, C. Eckert // 4th International Conference on Artifical Immune Systems (ICARIS): Proceedings / Eds.: C. Jacob et al., Banff, Alberta, Canada, August, 14–17, 2005. – Berlin : Springer-Verlag, 2005. – P. 262–275.

10. *De Castro L. N.* The clonal selection algorithm with engineering applications / L. N. de Castro, F. J. von Zuben // Genetic and Evolutionary Computation Conference (GECCO'00) : proceedings, Las Vegas, July 2000. – California : Morgan Kaufmann Publishers, 2000. – P. 36–37.
11. *Stibor T.* On the Use of Hyperspheres in Artificial Immune Systems as Antibody Recognition Regions / T. Stibor, J. Timmis, C. Eckert // 5th International Conference on Artifical Immune Systems (ICARIS): Proceedings / Eds.: H. Bersini, J. Carneiro, Oeiras, September 4–6, 2006. – New York : Springer-Verlag, 2006. – P. 215–228.
12. *Verleysen M.* Learning high-dimensional data / M. Verleysen // Limitations and future trends in neural computation. – 2003. – Vol. 186. – P. 141–162.
13. *Jensen R.* Computational Intelligence and Feature Selection: Rough and Fuzzy Approaches / R. Jensen, Q. Shen. – UK : IEEE Press and Wiley & Sons, 2008. – P. 340.
14. *Ji Z.* V-Detector: An Efficient Negative Selection Algorithm with «Probably Adequate» Detector Coverage / Z. Ji, D. Dasgupta // Information Sciences. – 2009. – Vol. 179. – P. 1390–1406.
15. *Buhlmann P.* Analysing Bagging / P. Buhlmann, B. Yu // The Annals of Statistics. – 2002. – Vol. 30. – P. 927–961.

Надійшла 29.03.2010

Зайцев С. О., Субботін С. О.

МЕТОДИ ТА МОДЕЛІ АВТОМАТИЧНОЇ КЛАСИФІКАЦІЇ ОБ'ЄКТІВ ЗА ОЗНАКАМИ НА ОСНОВІ ІМУНОКОМП'ЮТИНГУ

Проведено аналіз основних моделей штучної імунної системи. Експериментально оцінено роботу різних видів детекторів у вирішенні задачі автоматичної класифікації сільськогосподарських рослин за результатами дистанційного зондування. Запропоновано метод класифікації рослин на основі моделей імунокомп'ютингу, що дозволяє проводити навчання на екземплярах лише одного класу та забезпечує необхідний рівень точності розпізнавання.

Ключові слова: штучна імунна система, негативна селекція, Hypercell.

Zaitsev S. A., Subbotin S. A.

METHODS AND MODELS OF AUTOMATED OBJECTS CLASSIFICATION BY FEATURES BASED ON IMMUNOCOMPUTING

Basic artificial immunity models have been analyzed. Experiments were carried out and various detectors were estimated by solving the problem of plants recognition on remote sensing results. The method based on the immunocomputing principles was proposed. It allows to perform learning procedure using single class exemplars and ensures necessary recognition accuracy.

Key words: artificial immune system, negative selection, Hypercell.

УДК 681.3.06

Халимов Г. З.

Канд. техн. наук, доцент Харьковского национального университета радиоэлектроники

ОЦЕНКА ЧИСЛА РЕШЕНИЙ УРАВНЕНИЯ ГУРВИЦА В КОНЕЧНОМ ПОЛЕ

Представлены результаты по оценкам числа решений уравнения Гурвица в конечном поле и практический алгоритм нахождения решений.

Ключевые слова: кривая Гурвица.

ВВЕДЕНИЕ

Алгеброгеометрический подход при решении ряда задач в кодировании и криптографии связывается с полем рациональных функций на многообразиях, которые во многих случаях определяются точками алгебраических кривых. Можно отметить, например, традиционные исследования по эллиптическим кривым в криптографии цифровой подписи или по кривым Эрмита, Сузуки для задач универсального хеширования и помехоустойчивого кодирования. Кривые Гурвица относятся к классу замечательных кривых с большим числом точек.

Основные результаты по кривым Гурвица представлены в работах F. Torres [1, 2], P. Carbonne, T. Henocq в [3], R. Pellikan, P. Beelen [4, 5] и автора статьи [6, 7]. В работе [1] введено определение обобщенных кривых Гурвица и установлен морфизм между обобщенными кривыми Гурвица и Ферма. Здесь же определены условия максимальности для обычных кривых Гурвица и обобщенных кривых при ограничении на выбор показателей степени кривой. Связь между кривыми Гурвица и Ферма представлена P. Carbonne, T. Henocq в [3]. В работе [4] предложена техника построения кривых на основе формального полинома и определен класс кривых Гурвица, как обобщение квартики Клейна. В работе [5] представлены соотношения для рода кривой. Некоторые оценки числа решений кривой Гурвица для про-

извольного конечного поля представлены в [6]. Теорема о существовании нетривиальных кривых Гурвица и правила построения нетривиальных кривых также получены в [6]. Впервые получена максимальная кривая Гурвица с третьим значением рода для максимальных кривых в [7].

Целью статьи является нахождение оценок для числа решений уравнения Гурвица в конечном поле. В разделе 1 приводятся определения и основные результаты по кривым Гурвица. В разделе 2 получены оценки числа точек для кривых Гурвица в конечном поле. В разделе 3 представлен практический алгоритм вычисления числа точек кривой Гурвица.

1. ОПРЕДЕЛЕНИЕ И ОСНОВНЫЕ РЕЗУЛЬТАТЫ ПО КРИВЫМ ГУРВИЦА В КОНЕЧНОМ ПОЛЕ

Кривые Гурвица H_n определяются выражением

$$X^nY + Y^nZ + XZ^n = 0 \qquad (1)$$

и имеют частные производные вида

$$F_X = nX^{n-1}Y + Z^n,\ F_Y = nY^{n-1}Z + Z^n,$$
$$F_Z = nZ^{n-1}X + Y^n. \qquad (2)$$

Несингулярность кривых Гурвица над F_q определяется условиями вида:

1) n и q должны быть взаимно простыми;

2) $\gcd(n^2 - n + 1, q) = 1$.

Для вычисления рода кривой Гурвица H_n используем выражение рода для кривой вида

$$X^a + X^bY^c + Y^d = 0. \qquad (3)$$

В работе [4] (замечание 43) доказывается, что для несингулярной модели кривой (2) справедливо

$$g \le 1 + \frac{1}{2}\{|ac + bd - ad| - \gcd(a - b, c) -$$
$$- \gcd(b, c - d) - \gcd(a, d)\}. \qquad (4)$$

Если характеристика поля F_q не делит $\gcd(a - b, c)$, $\gcd(b, c - d)$, $\gcd(a, d)$ и $ac + bd - ad$, тогда справедливо равенство. В силу соотношения (4) для кривой Гурвица H_n выражение для рода имеет следующий вид

$$g = \frac{n^2 - n}{2}. \qquad (5)$$

Существует обобщение кривых Гурвица $H_{n,l}$, которое имеет вид

$$X^nY^l + Y^nZ^l + X^lZ^n = 0, \qquad (6)$$

где $n \ge l \ge 2$, $\Delta(n, l) = n^2 - nl + l^2 \ge 2$ и частные производные

$$F_X = nX^{n-1}Y^l + lX^{l-1}Z^n;\ F_Y = nY^{n-1}Z^l + lX^nY^{l-1};$$
$$F_Z = nZ^{n-1}X^l + lY^nZ^{l-1}. \qquad (7)$$

Несингулярность кривых Гурвица $H_{n,l}$ над F_q определяется условием [1]:

$$(\Delta(n, l), char(F_q)) = 1. \qquad (8)$$

Род кривой $H_{n,l}$, как следует из (4) и отмечается в [5], равен

$$g = \frac{n^2 - nl + l^2 + 2 - 3\gcd(n, l)}{2}. \qquad (9)$$

Справедливо следующее утверждение.

Утверждение 1. В простом поле F_q все кривые Гурвица H_n являются несингулярными.

Доказательство следует из того, что всегда выполняются условия: $\gcd(n, q) = 1$ и $\gcd(n^2 - n + 1, q) = 1$.

2. ОЦЕНКИ ЧИСЛА ТОЧЕК ДЛЯ КРИВЫХ ГУРВИЦА В КОНЕЧНОМ ПОЛЕ

Ниже рассмотрим основные свойства кривых Гурвица для случая произвольного конечного поля F_q, прежде всего оценки для числа точек кривых.

Следующая теорема определяет число решений кривой Гурвица для произвольного конечного поля.

Теорема 1. Пусть кривая $X^nY^l + Y^nZ^l + X^lZ^n = 0$ определена над конечным полем F_q и является несингулярной. Пусть $\gcd(n, l, q - 1) = c > 1$ и $\gcd(n^2 - nl + l^2, c(q - 1)) = c^2d$, тогда имеем следующую оценку для числа точек кривой Гурвица:

$$N = tc^2d + 3, \qquad (10)$$

где $0 \le t \le q - 1$.

Доказательство. Решения для кривой $X^nY^l + Y^nZ^l + X^lZ^n = 0$ есть точки проективного пространства P^2: $(\gamma:\zeta:1)$, $\gamma, \zeta \in F_q$ и $\gamma \ne 0$, $\zeta \ne 0$, удовлетворяющие уравнению

$$\gamma^n\zeta^l + \zeta^n + \gamma^l = 0. \qquad (11)$$

Выражение (11) сократим на $\gamma^l \ne 0$

$$\gamma^{n-1}\zeta^l + \zeta^n\gamma^{-l} + 1 = 0. \qquad (12)$$

Пусть $\gamma = \beta^i$, $\zeta = \beta^j$, где β – образующий элемент поля F_q, тогда

$$\beta^{i(n-l)+jl} + \beta^{-il+jn} + 1 = 0. \qquad (13)$$

Равенство (13) относительно неизвестных i и j имеет решения, если

$$\begin{cases} i(n-l)+jl \equiv a(\mathrm{mod}(q-1)); \\ -il+jn \equiv b(\mathrm{mod}(q-1)); \\ \beta^a+\beta^b+1 = 0. \end{cases} \quad (14)$$

Система тождественных уравнений (14) первой степени относительно неизвестных i и j для значений a и b, удовлетворяющих условию $\beta^a+\beta^b+1=0$, имеет следующие решения.

Пусть $\gcd(n, l, q-1) = c > 1$, тогда левые и правые части уравнений системы (14) можно сократить на значение c:

$$\begin{cases} \frac{i(n-l)}{c}+j\frac{l}{c} \equiv \frac{a}{c}\left(\mathrm{mod}\frac{(q-1)}{c}\right); \\ -i\frac{l}{c}+j\frac{n}{c} \equiv \frac{b}{c}\left(\mathrm{mod}\frac{(q-1)}{c}\right). \end{cases} \quad (15)$$

Выразим неизвестные i и j значения в уравнениях системы (15). После элементарных преобразований система тождественных уравнений преобразуется к системе линейных уравнений

$$\begin{cases} i\frac{(n^2-nl+l^2)}{c^2} = \frac{an-bl}{c^2}+\frac{k_1n-k_2l}{c}\frac{(q-1)}{c}; \\ j\frac{(n^2-nl+l^2)}{c^2} = \frac{al+b(n-l)}{c^2}+\frac{k_1l+k_2(n-l)}{c}\frac{(q-1)}{c}. \end{cases} \quad (16)$$

Множество коэффициентов k_1 и k_2 определяют все решения для i и j при зафиксированных значениях a и b. Так как c делит n и l, систему линейных уравнений (16) преобразуем к системе тождественных уравнений по модулю $(q-1)c$:

$$\begin{cases} i(n^2-nl+l^2) \equiv an-bl(\mathrm{mod}(c(q-1))); \\ j(n^2-nl+l^2) \equiv al+b(n-l)(\mathrm{mod}(c(q-1))). \end{cases} \quad (17)$$

Пусть $\gcd(n^2-nl+l^2, c(q-1)) = c^2d$, тогда для зафиксированных значений a и b, удовлетворяющих уравнению $\beta^a+\beta^b+1=0$ и условию делимости $an-bl$ и $al+b(n-1)$ на c^2d, получим c^2d решений. Пусть число пар степеней a и b, удовлетворяющих условию делимости, равно t. С учетом особых точек (1:0:0), (0:1:0), (0:0:1), число точек кривой $H_{n,l}$ будет равно $N = tc^2d + 3$.

Частные результаты по кривым Гурвица представлены следствиями 1–4.

Следствие 1. Если $\gcd(n^2-nl+l^2, q-1) = 1$ и $\gcd(n, l) = 1$, тогда число точек несингулярной кривой Гурвица $H_{n,l}$ будет равно

$$N = q + 2. \quad (18)$$

Действительно, если $\gcd(n^2-nl+l^2, q-1) = 1$, а степени n и l не имеют общих сомножителей, тогда при зафиксированных значениях a и b уравнения (7) имеют единственное решение. Общее число пар степеней a и b, удовлетворяющих условию $\beta^a+\beta^b+1=0$, равно $q-1$. С учетом особых точек (1:0:0), (0:1:0), (0:0:1), число точек кривой $H_{n,l}$ будет равно $N = q + 2$.

Данный случай описывает кривые Гурвица $H_{n,l}$ с тривиальным числом точек, равным $q+2$, и родом $g = \frac{n^2-nl+l^2-1}{2}$.

Следствие 2. Если $\gcd(n^2-nl+l^2, q-1) = 1$ и $\gcd(n, l) = c$, тогда число точек несингулярной кривой Гурвица $H_{n,l}$ будет равно

$$N = tc^2 + 3. \quad (19)$$

Так как $\gcd(n, l) = c$ и $\gcd(n^2-nl+l^2, q-1) = 1$, тогда $\gcd(n^2-nl+l^2, c(q-1)) = c^2$.

Для зафиксированных значений a и b уравнения (15) имеют c^2 решений, если a и b делятся на c. Пусть число пар степеней a и b, удовлетворяющих условию делимости, равно t. Тогда число точек кривой $H_{n,l}$ будет равно $N = tc^2 + 3$.

В данном случае род кривых Гурвица $H_{n,l}$ равен $g = \frac{n^2-nl+l^2+2-3c}{2} = \frac{c(c\delta-3)}{2}+1$, где $\delta = \frac{n^2-nl+l^2}{c^2} > 1$.

Замечание 1. Если $\gcd(n^2-nl+l^2, q-1) = 1$ и $\gcd(n, l) = c$, тогда кривая Гурвица $H_{n,l}$ покрывается кривой Ферма Fr_c $X^c+Y^c+Z^c=0$, рода $g = \frac{(c-1)(c-2)}{2}$. Следует это из оценок для числа точек кривых. Род кривых Ферма Fr_c меньше рода кривых Гурвица $H_{n,l}$ данного типа.

Следствие 3. Пусть $\gcd(n^2-nl+l^2, q-1) = d$ и $\gcd(n, l) = 1$, тогда число точек несингулярной кривой Гурвица $H_{n,l}$ будет равно

$$N = td + 3. \quad (20)$$

Пусть $\gcd(n^2-nl+l^2, q-1) = d$ и $\gcd(n, l) = 1$. Для фиксированных значений a и b уравнения (5) имеют d решений, если $an-bl$ и $al+b(n-l)$ делятся на d. Пусть число пар степеней a и b, удовлетворяющих условию делимости, равно t. Тогда число точек кривой $H_{n,l}$ будет равно $N = td + 3$.

Данный случай кривых является наиболее интересным. Докажем следующие полезные леммы.

Лемма 1. Пусть $n > 0$ есть целое число и $\Delta(n, l) = n^2 - n + 1$ имеет простые делители $d > 3$. Тогда $d \equiv 1 \bmod 6$.

Пусть d – простое число есть делитель $\Delta(n, l)$. Тогда

$$n^2 - n + 1 \equiv 0 \bmod d. \quad (21)$$

Применим модульную операцию к членам суммы $\Delta(n, l)$. С учетом подстановки $n \equiv n_d \bmod d$ получим

$$n_d^2 - n_d + 1 \equiv 0 \bmod d. \quad (22)$$

Вычисления по модулю простого числа можно свести к вычислениям в конечном поле F_{d_i}. Пусть α – образующий элемент поля и пусть $n_d = \alpha^s$, тогда имеем уравнение

$$\alpha^{2s} - \alpha^s + 1 = 0. \quad (23)$$

Так как $\alpha^{\frac{d-1}{2}} = -1$, получим

$$\alpha^{2s} + \alpha^{\frac{d-1}{2}}\alpha^s + 1 = 0. \quad (24)$$

Трехчлен (24) с единицей равен нулю, если его элементы образуют мультипликативную подгруппу третьего порядка 1, β, β^2. Здесь $\beta = \alpha^{2s}$, $\beta^2 = \alpha^{\frac{d-1}{2}+s}$. Получим решение относительно параметра $s = \frac{d-1}{6}$. Таким образом, каждый делитель $\Delta(n, l)$, если он больше 3, имеет свойство $d_i \equiv 1 \bmod 6$.

Лемма 2. Пусть $n > 1$ есть целое число и $\Delta(n, l) = n^2 - n + 1$. Тогда одним из делителей $\Delta(n, l)$ может быть простой делитель, равный 3.

Действительно, пусть $d = 3$ есть делитель $\Delta(n, l)$. Тогда с учетом подстановки $n \equiv n_d \bmod 3$ получим

$$n_d^2 - n_d + 1 \equiv 0 \bmod 3. \quad (25)$$

Решение уравнения (25) возможно только в случае, если $n_d^2 = 1$ и $n_d = 2$. Из уравнения (24) следует, что $s = 1$ и $\alpha^2 + \alpha^1\alpha^1 + 1 = 0$ справедливо для подгруппы второго порядка.

Лемма 3. Пусть $n > 0$ есть целое число и $\Delta(n, l) = n^2 - n + 1$ имеет степенные делители d^e, $d > 3$ и $d \equiv 1 \bmod 6$.

Пусть d^e – делитель $\Delta(n, l)$. Тогда

$$n^2 - n + 1 \equiv 0 \bmod d^e. \quad (26)$$

Применим модульную операцию к членам суммы $\Delta(n, l)$. С учетом подстановки $n \equiv n_d \bmod d^e$ получим

$$n_d^2 - n_d + 1 \equiv 0 \bmod d^e. \quad (27)$$

Вычисления по модулю d^e можно свести к вычислениям в кольце целых чисел F_{d^e}, порядка $p = d^e - d^{e-1}$. Пусть α – образующий элемент кольца и пусть $n_d = \alpha^s$, тогда имеем уравнение

$$\alpha^{2s} - \alpha^s + 1 = 0. \quad (28)$$

Так как $\alpha^{\frac{p}{2}} = -1$, получим

$$\alpha^{2s} + \alpha^{\frac{p}{2}}\alpha^s + 1 = 0. \quad (29)$$

Трехчлен (29) с единицей равен нулю, если его элементы образуют мультипликативную подгруппу третьего порядка 1, β, β^2. Здесь $\beta = \alpha^{2s}$, $\beta^2 = \alpha^{\frac{p}{2}+s}$. Получим решение относительно параметра $s = \frac{p}{6}$. По условию $p \equiv 0 \bmod 6$, в силу того, что $d \equiv 1 \bmod 6$, в разложении $\Delta(n, l)$ делитель d^e может иметь место. ◊

Обобщение полученных результатов на случай, когда $l \neq 1$ в параметре $\Delta(n, l) = n^2 - nl + l^2$, представлено в лемме 4.

Лемма 4. Пусть $n, l > 0$ есть целые взаимно простые числа, $\gcd(n, l) = 1$ и $\Delta(n, l) = n^2 - nl + l^2$. Тогда одним из делителей $\Delta(n, l)$ может быть простой делитель, равный 3, простые делители $d > 3$ со свойством $d \equiv 1 \bmod 6$, а также степенные делители d^e, $d > 3$ и $d \equiv 1 \bmod 6$.

Пусть d – есть делитель $\Delta(n, l)$. Рассмотрим выражение

$$n^2 - nl + l^2 \equiv 0 \bmod d. \quad (30)$$

Применим модульную операцию к членам суммы $\Delta(n, l)$. С учетом подстановки $n \equiv n_d \bmod d$, $l \equiv l_d \bmod d$ получим

$$n_d^2 - n_d l_d + l_d^2 \equiv 0 \bmod d. \quad (31)$$

Вычисления по модулю числа d можно свести к вычислениям в конечном поле F_{d_i}. Пусть α – образующий элемент поля и пусть $n_d = \alpha^s$, $l_d = \alpha^t$, тогда имеем уравнение

$$\alpha^{2s} - \alpha^s\alpha^t + \alpha^{2t} = 0. \quad (32)$$

Сделаем замену переменных $I = s - t$. После преобразований с учетом $\alpha^{\frac{d-1}{2}} = -1$ получим

$$\alpha^{2t}(\alpha^{2i} + \alpha^{d-1_2}\alpha^i + 1) = 0. \quad (33)$$

Таблица 1. Уравнения кривых Гурвица и оценки для числа точек и рода в конечном поле F_q

Уравнение кривой Гурвица	Свойства кривой	Число точек кривой N	Род кривой g
$X^nY + Y^nZ + XZ^n$	$\gcd(n^2 - n + 1, q - 1) = 1$	$q + 2$	$n(n-1)/2$
$X^nY^l + Y^nZ^l + X^lZ^n$	$\gcd(n^2 - nl + 1^2, q - 1) = 1$; $\gcd(n, l) = 1$	$q + 2$	$(n^2 - nl + l^2 - 1)/2$
$X^nY^l + Y^nZ^l + X^lZ^n$	$\gcd(n^2 - nl + 1^2, q - 1) = 1$; $\gcd(n, l) = c$	$tc^2 + 3$	$(n^2 - nl + l^2 + 2 - 3c)/2$
$X^nY + Y^nZ + XZ^n$	$\gcd(n^2 - n + 1, q - 1) = d$	$td + 3$	$n(n-1)/2$
$X^nY^l + Y^nZ^l + X^lZ^n$	$\gcd(n^2 - nl + 1^2, q - 1) = d$; $\gcd(n, l) = 1$	$td + 3$	$(n^2 - nl + l^2 - 1)/2$
$X^nY^l + Y^nZ^l + X^lZ^n$	$\gcd(n^2 - nl + 1^2, c(q-1)) = c^2d$; $\gcd(n, l, (q-1)) = c > 1$	$tc^2d + 3$	$(n^2 - nl + l^2 + 2 - 3c)/2$

Трехчлен в выражении (33) с единицей равен нулю, если его элементы образуют мультипликативную подгруппу третьего порядка 1, b, β^2. Выполнение условий существования мультипликативной подгруппы третьего порядка определяются в леммах $1 \div 3$, и свойства делителей $\Delta(n, l)$ переносятся на данную лемму.

Параметр $\Delta(n, l) = n^2 - nl + l^2$ имеет следующие свойства:

1. $$\Delta(n, l) = \Delta(l, n). \qquad (34)$$

2. $$\Delta(n, l) = \Delta(n, n - l). \qquad (35)$$

3. Если $\gcd(n, l) = 1$ и $p > n > 1$ является делителем $\Delta(n, l)$, тогда

$$\Delta(n, l) = \Delta(p - n, p - l). \qquad (36)$$

4. Если $\gcd(n, l) = 1$ и p является делителем $\Delta(n, l)$, тогда $\Delta(n', l')$ будет иметь делители не выше $p > n > l$, где $n \equiv n' \bmod p$, $l \equiv l' \bmod p$.

5. $$\Delta(cn, cl) = c^2\Delta(n, l). \qquad (37)$$

Рассмотрим доказательство свойства 4. Так как $n', l' < p$, возьмем верхнюю оценку $n' = l' = p$. Получим $\Delta(n', l') = p^2 - pp + p^2 = p^2$. Отсюда следует, что один делитель p, другие не больше чем p.

Доказательства свойств 1–3, 5 простые.

Основные результаты по оценкам для числа точек и рода для кривых Гурвица представлены в табл. 1.

В табл. 1 представлено все многообразие кривых Гурвица, которое вытекает из результатов теоремы 1.

3. ПРАКТИЧЕСКИЙ АЛГОРИТМ ВЫЧИСЛЕНИЯ ЧИСЛА ТОЧЕК КРИВОЙ ГУРВИЦА

В соответствии с теоремой 1, практический алгоритм вычисления числа точек кривой Гурвица включает следующие шаги:

1. Для заданной кривой $X^nY^l + Y^nZ^l + X^lZ^n = 0$ в конечном поле F_q вычисляем параметр $\Delta(n, l) = n^2 - nl + l^2$ и определяем по результатам вычислений $\gcd(n, l, q - 1)$ и $\gcd(n^2 - nl + l^2, q - 1)$, к какому множеству кривых Гурвица относится кривая по классификации, представленной в табл. 1, и по какой оценке определяется число точек.

2. Для конечного поля F_q с элементами β^i подсчитываем число пар степеней a и b образующего элемента β мультипликативной группы порядка $q - 1$, которые удовлетворяют уравнению $\beta^a + \beta^b + 1 = 0$ и условию делимости $an - bl$ и $al + b(n - l)$ на $\Delta(n, l)$. В результате получим t пар. С учетом особых точек (1:0:0), (0:1:0), (0:0:1) вычисляем значение для числа точек кривой Гурвица $N = t\Delta(n, l) + 3$.

ВЫВОДЫ

1. Оценки для числа точек кривых Гурвица, представленные теоремой 1, являются новыми, и при доказательстве теоремы 1 используется конструктивный алгоритм вычисления числа точек кривой Гурвица в конечном поле.

2. Сложность вычислений практического алгоритма определяется размерностью конечного поля, что существенно меньше перебора всех решений по точкам проективного пространства.

СПИСОК ЛИТЕРАТУРЫ

1. *Torres F.* Plan maximal curves / Torres F // Acta Arithmetic. – 2001. – Vol. 98, No. 2. – P. 165–179.
2. *Cossidente A.* Curves of large genus covered by the Hermitian curve / Cossidente A., Korchm'aros G. and Torres F. // Commutative Algebra. – 2000. – Vol. 28, No. 10. – P. 4707–4728.
3. *Carbonne P.* Decomposition de la Jacobienne sur les corps finis / Carbonne P., Henocq T. // Bulletin Polish Academy of Sciences Mathematics. – 1994. – Vol. 42, No. 3. – P. 207–215.
4. *Pellikan R.* The Klein quartic, the Fano plan and curves representing design / Pellikan R. // In Codes, Curves and

Signals: Common Threads in Communications. – Dordrecht : Kluwer Academy Publication, 1998. – P. 9–20.
5. *Beelen P.* The Newton polygon of plane curves with many rational points / Beelen P. and Pellikan R. // Designs, Codes and Cryptography. – 2000. – No. 21. – P. 41–67.
6. *Халимов Г. З.* Оценка параметров кривых Гурвица для целей универсального хеширования / Халимов Г. З. // Сборник трудов I Международной научно-технической конференции «Компьютерные науки и технологии» (Белгород, Россия, 8–10 октября 2009). – 2009. – Ч. 2. – С. 118–121.
7. *Халимов Г. З.* Максимальные кривые Гурвица для целей универсального хеширования/ Халимов Г. З. // Материалы XI Международной научно-практической конференции «Информационная безопасность» (Таганрог, Россия, 23–25 июня 2010), ТТИ ЮФУ. – 2010. – Ч. 3. – С. 144–146.

Надійшла 12.04.2010

Халімов Г. З.

ОЦІНКА ЧИСЛА РІШЕНЬ РІВНЯННЯ ГУРВИЦА В КІНЦЕВОМУ ПОЛІ

Представлено результати по оцінках числа рішень рівняння Гурвица в кінцевому полі та практичний алгоритм знаходження рішень.

Ключові слова: крива Гурвица.

Khalimov G. Z.

ESTIMATE OF HURVITZ EQUATION SOLUTIONS NUMBER IN FINITE FIELD

The author presents the results of estimation of Hurvitz equation solutions number in finite field and practical algorithm of solutions finding.

Key words: Hurvitz curve.