Записки научных
семинаров ПОМИ
Том 421, 2014 г.

М. А. Рыбалкин

КЛАССИФИКАЦИЯ ПЕРЕСТАНОВОЧНЫХ МНОГОЧЛЕНОВ МАЛОЙ ДЛИНЫ НАД ПРОСТЫМИ КОНЕЧНЫМИ ПОЛЯМИ

Введение

Пусть p – просто число и $q = p^n$. Многочлен $f(x)$ называется перестановочным многочленом над полем $\mathbb{F}_q$, если соответствующее ему отображение задает биекцию множества $\mathbb{F}_q$. Изучение перестановочных многочленов началось с работ Эрмита и Диксона [1, 2]. В настоящее время наблюдается повышение интереса к перестановочным многочленов в связи с их потенциальными приложениями в криптографии, теории кодирования и комбинаторике. Над конечным полем $\mathbb{F}_q$ существует $q!$ перестановок и каждую такую перестановку задает единственный перестановочный многочлен степени меньшей q, который может быть получен как интерполяционный многочлен. Интерес представляет обратная задача по нахождению многочленов, которые бы задавали перестановки над конечными полями, а также задача по исследованию свойства перестановок, соответствующих определенным классам перестановочным многочленов.

Теория перестановочных многочленов содержит большое число открытых вопросов и гипотез [3, 4]: вопрос об эффективном критерии различных классов перестановочных многочленов, сложность нахождения обратной перестановки, нахождение новых серий перестановочных многочленов, нахождении критериев перестановочных двучленов и трехчленов.

В данной работе исследуются перестановочные многочлены малой длины, а именно двучлены, трехчлены и четырехчлены. Такие многочлены могут быть использованы в качестве компактного представления нетривиальных перестановок и при этом имеют эффективную процедуру вычисления значений ввиду малой длины. Нами был разработан метод по перечислению перестановочных многочленов малой

Ключевые слова: классификация перестановочных многочленов, перестановочные двучлены, перестановочные трехчлены, перестановочные четырехчлены.

длины, анализ результатов перечисления которого позволил построить гипотезу о классификации перестановочных трехчленов и четырехчленов над простыми конечными полями.

§1. Алгоритм перечисления перестановочных многочленов малой длины

В общем случае для перечисления всех перестановочных четырехчленов требуется найти множество наборов $(n_1, n_2, n_3, n_4, c_2, c_3, c_4)$ таких, что многочлен $x^{n_1} + c_2 x^{n_2} + c_3 x^{n_3} + c_4 x^{n_4}$ является перестановочным. Множество перестановочных многочленов над любым конечным полем $\mathbb{F}_q$ бесконечно, т.к. к любому перестановочному многочлену можно добавить $x^q - x$. Поэтому достаточного перечислять многочлены степени меньшей q. Для сокращения пространства поиска нами используется тот факт, что композиция перестановочных многочленов также является перестановочным многочленом. Если рассмотреть всевозможные подстановки перестановочных одночленов x^k, можно ввести ограничения на перебираемые значения $(n_1, n_2, n_3, n_4, c_2, c_3, c_4)$ и значительно сократить пространство поиска. Так, например, если мы нашли перестановочный многочлен, то из процесса перечисления можно исключить все многочлены, получаемые из данного подстановками перестановочных одночленов x^k с последующим приведением по модулю $x^q - x$. Представителей из класса эквивалетных многочленов будем называть представительными многочленами.

По аналогии с алгоритмом перечисления перестановочных двучленов [5] можно показать, что достаточного проверять показатели степеней (n_1, n_2, n_3, n_4) удовлетворяющие следующим свойствам:

(1) $n_1 < n_2 < n_3 < n_4$
(2) $\gcd(n_1, n_2, n_3, n_4) = 1$
(3) $n_1 \mid q - 1$
(4) $n_1 \geqslant \gcd(n_i, q-1)$, для $i = 2, 3, 4$.

Обозначим через $NoneqDeg_q$ множество показатели степеней (n_1, n_2, n_3, n_4) удовлетворяющих приведенными выше условиями.

Одним из основным инструментом для проверки критерия перестановочного многочлена общего вида является критерий Эрмита:

Теорема 1 (Критерий Эрмита)**.** *Пусть p — характеристика поля $\mathbb{F}_q$. Тогда многочлен $f \in \mathbb{F}_q[x]$ является перестановочным многочленом тогда и только тогда, когда:*

(1) *Для любого* i *от* 1 *до* $q-2$ *и* $i \not\equiv 0 \bmod p$, *результат приведения* f^i *по модулю* $x^q - x$ *имеет степень меньше* $q-1$.
(2) *Многочлен* f *имеет ровно один корень в* $\mathbb{F}_q$.

Критерий Эрмита позволяет доказывать, что какой-то многочлен не является перестановочным, т.к. для этого достаточного привести значение i такое, что $\deg(f^i \bmod x^q - x) = q - 1$. Вместе с тем, если показатели степеней мономов фиксированы, а неизвестны только коэффициенты при этих мономах, критерий Эрмита позволяет получить систему полиномиальных уравнений, соответствующих коэффициенту при мономе x^{q-1} в многочлене $f^i \bmod x^q - x$ для всех i от 1 до $q-2$. На практике же такие коэффициенты, как многочлены от коэффициентов c_2, c_3, c_4, могут быть очень большими и для многих многочленов длина коэффициента начинает экспоненциально расти вместе с ростом i, что не позволяет использовать критерий Эрмита напрямую. Поэтому с вычислительной точки зрения имеет смысл проверять коэффициент при x^{p-1} только в том случае, если длина этого коэффициента мала. Для нахождения коэффициентов малой длины в данной работе предлагается вычислять усеченные степени $f^i \bmod x^q - x$, где все длины коэффициентов меньше наперед заданного ограничения N. Если длина какого-то коэффициента становится больше чем N, то он заменяется на неизвестное значение ε. При этом вводится тождество, что для любого многочлена f, $f\varepsilon = \varepsilon$, которое отражает тот факт, что умножение любого многочлена на неизвестный многочлен дает также неизвестный многочлен. Через $Trancate_N(f)$ обозначим функцию, которая заменяет коэффициенты многочлена $f(x)$ на ε, если длина такого коэффициента больше N. Тогда получение условий из критерия Эрмита можно записать в виде следующего алгоритма, приведенного на рисунке 1.

Для конкретных показателей степеней (n_1, n_2, n_3, n_4) алгоритм $Trancate_N(f)$ позволяет получить условия из критерия Эрмита, длина которых не превосходит N. Если множество таких условий оказалось пустым или состоящим только из 1-2 элементов, то значит выражения в критерии Эрмита имеют большую длину, и для их получения можно просто увеличить N. На практике нами использовалось начальное значение $N = 5$ с последующим увеличением до 60. Существуют многочлены, для которых все условия Эрмита умеют большую длину, но которые не являются перестановочными многочленами ни для

каких значений параметров. Примером такого многочлена является $x + c_2x^2 + c_3x^{166} + c_4x^{167}$ над $\mathbb{F}_{331}$.

Вход: f — многочлен с неизвестными коэффициентами
Выход: условия в критерии Эрмита, длины меньше N

```
1.  function TrancatedHermite_N f
2.  f' := f
3.  Conditions := ∅
4.  for all i ∈ [2..q − 2]
5.     f' := Trancate_N(f'f mod x^q − x)
6.     c := Coef(f', x^{q−1})
7.     if i ≢ 0 mod p, c ≠ 0, c ≠ ε then
8.        Conditions := Conditions ∪ {c}
9.     end for
10.    return Conditions
11.  end function
```

Рис. 1. Функция получения усеченных условий из критерия Эрмита

Итоговый алгоритм перечисления перестановочных четырехчленов приведен на рисунке 2. Алгоритм для перечисления трехчленов полностью аналогичен данному алгоритму.

Вход: q — порядок конечного поля
Выход: перестановочные четырехчлены вида $x^{n_1}+c_2x^{n_2}+c_3x^{n_3}+c_4x^{n_4}$

```
1. for all (n_1, n_2, n_3, n_4) ∈ NoneqDeg_q
2.    HermiteConditions := TrancatedHermite_N(x^{n_1} + c_2x^{n_2} + c_3x^{n_3} +
c_4x^{n_4})
3.    for all (c_2, c_3, c_4) ∈ Solve(HermiteConditions)
4.       f := x^{n_1} + c_2x^{n_2} + c_3x^{n_3} + c_4x^{n_4}
5.       if f перестановочный многочлен
6.          yield f
7.    end for
8. end for
```

Рис. 2. Алгоритм перечисления перестановочных четырехчленов.

Перестановочный многочлен	Конечное поле
$x + 61x^{45}$	$\mathbb{F}_{67}$
$x + 122x^{114}$	$\mathbb{F}_{227}$
$x^3 + 154x^{263}$	$\mathbb{F}_{313}$
$x^4 + 194x^{241}$	$\mathbb{F}_{317}$
$x + 143x^{174}$	$\mathbb{F}_{347}$
$x + x^2 + 44x^3$	$\mathbb{F}_{131}$
$x + 6x^{39} + 49x^{77}$	$\mathbb{F}_{229}$
$x^3 + 20x^{210} + 200x^{256}$	$\mathbb{F}_{277}$
$x + 194x^{142} + 257x^{189}$	$\mathbb{F}_{283}$
$x + x^2 + 24x^4 + 33x^5$	$\mathbb{F}_{53}$
$x + x^4 + 66x^{34} + x^{37}$	$\mathbb{F}_{67}$
$x^2 + 8x^{15} + 53x^{28} + 11x^{54}$	$\mathbb{F}_{79}$
$x + x^{40} + 82x^{42} + x^{81}$	$\mathbb{F}_{83}$

Таблица 1. Примеры перестановочных многочленов

На практике данный алгоритм применим для перечисления перестановочных двучленов, трехчленов и четырехчленов. Этот алгоритм позволил перечислить все перестановочные четырехчлены для простых конечных полей $\mathbb{F}_p, p < 500$, и все трехчлены для простых конечных полей $\mathbb{F}_p, p < 5000$. Примеры некоторых перечисленных многочленов приведены на таблице 1. Результаты перечислений и гипотезы о свойствах перестановочных трехчленов и четырехчленов проводятся в следующих разделах.

§2. Анализ серий и классификация перестановочных многочленов

Любой многочлен над конечным полем $\mathbb{F}_q$ может быть представлен в виде $x^r f(x^{\frac{q-1}{d}})$, где значение параметра d является важной характеристикой. Такое представление является интересным при $d > 1$. Так в работах [6, 7] показано, что проверка перестановочного многочлена может быть осуществлена за $O(d^2)$ операций, а в работе [8] показано, что многочлен, соответствующий обратному отображению, также может быть найдет за $O(d^2)$ операций. При фиксированном d класс таких многочленов замкнут относительно операции композиции, и в

работе [6] исследуется размер порождаемой группы. В работе [9] доказывается, что для перестановочных двучленов над простыми конечными полями $\mathbb{F}_p$ значение d ограничено снизу значением $\sqrt{p}$, а также выдвигается гипотеза о том, что $d < 2\log p$. При выполнении этой гипотезы все операции с перестановочными двучленами над конечными полями могут быть реализованы эффективно за полиномиальное время:

- проверка того, что двучлен является перестановочным.
- построение случайных перестановочных двучленов.
- нахождение многочлена, соответствующего обратному отображению.

Главным результатов данной статьи является классификация перестановочных трехчленов и четырехчленов над простыми конечными полями, полученная путем анализа результатов перечисления перестановочных многочленов. Из работы [9] следует, что все множество перестановочных двучленов принадлежит одному классу вида $x^r f(x^{\frac{q-1}{d}})$, где $d < 2\log p$ (в предположении справедливости гипотезы). Оказывается, что для трехчленов и четырехчленов большинство многочленов принадлежит аналогичному классу, но в дополнение для трехчленов появляется еще один класс, а для четырехчленов появляется 2 класса.

Обнаруженная классификация для трехчленов может быть сформулирована в виде следующей гипотезы:

Гипотеза 2. *Любой перестановочный трехчлен $ax^n + bx^m + cx^k$ над простым конечным полем $\mathbb{F}_p$ принадлежит одному из следующих классов:*

- **Класс 1:** *Класс перестановочных трехчленов вида $x^r f(x^{\frac{p-1}{d}})$, где $d < 4\log p$.*
- **Класс 2:** *Класс перестановочных трехчленов вида $f(x^r)$, $\deg f \leqslant 5$.*

В работе Диксона [2] приводится классификация всех перестановочных многочленов, степень которых ограничена значением 5. Из этой классификации можно показать, что при $p > 10$ в гипотезе 2 во втором классе многочлен $f(x)$ может иметь только два вида:

(1) $x^3 + 3\beta x^2 + 3\beta^2 x = (x+\beta)^3 - \beta^3$, если $\gcd(p-1, 3) = 1$.
(2) $x^5 - 5\beta x^3 + 5\beta^2 x = D_5(x, \beta)$, если $\gcd(p^2-1, 5) = 1$, где $D_5(x, \beta)$ — многочлен Диксона

Гипотеза 2 предсказывает, что других классов перестановочных трехчленов над простыми конечными полями не существует, и вопрос о полноте данной классификации является открытым.

Для четырехчленов появляется еще один класс, и общая гипотеза о классификации может быть сформулирована в следующей виде:

Гипотеза 3. *Любой перестановочный трехчлен* $ax^n + bx^m + cx^k + ex^m$ *над простым конечным полем* $\mathbb{F}_p, p > 23$ *принадлежит одному из следующих классов:*

- **Класс 1:** *Класс перестановочных четырехчленов вида* $x^r f(x^{\frac{p-1}{d}})$, *где* $d < 6 \log p$.
- **Класс 2:** *Класс перестановочных четырехчленов вида* $f(x^r)$, $\deg f \leqslant 7$.
- **Класс 3:** *Класс перестановочных многочленов вида* $ax^r \left(x^{\frac{p-1}{2}} + 1\right) + bx^m \left(x^{\frac{p-1}{2}} - 1\right)$.

Класс 3 приводится в качестве примера перестановочного многочлена в работе Эрмита [1], и в дальнейшем будем называть этот класс серией Эрмита. Можно показать, что две следующие леммы задают необходимые и достаточные условия на параметры данной серии:

Лемма 4. *Пусть* $p \equiv 1 \bmod 4$. *Тогда многочлен*

$$ax^r \left(x^{\frac{p-1}{2}} + 1\right) + bx^m \left(x^{\frac{p-1}{2}} - 1\right)$$

является перестановочным многочленом над конечным полем $\mathbb{F}_p$ *тогда и только тогда, когда* $gcd(r, p-1) = 1$, $gcd(m, p-1) = 1$ *и* ab *является квадратичным вычетом.*

Лемма 5. *Пусть* $p \equiv 3 \bmod 4$. *Многочлен*

$$ax^r \left(x^{\frac{p-1}{2}} + 1\right) + bx^m \left(x^{\frac{p-1}{2}} - 1\right)$$

является перестановочным многочленом над конечным полем $\mathbb{F}_p$ *тогда и только тогда, когда* $gcd(r, p-1) \in \{1, 2\}$ *и выполнено одно их двух условий*

(1) $gcd(m, p-1) = 1$ *и* ab *не является квадратичным вычетом.*
(2) $gcd(m, p-1) = 2$ *и* ab *является квадратичным вычетом.*

В гипотезе 3 среди всех перечисленных четырехчленов при $p \leqslant 23$ было найдено два исключения со следующими представительными многочленами:

(1) Несколько многочленов с мономами $\{x^{15}, x^{14}, x^{10}, x\}$ над $\mathbb{F}_{19}$, например, $x^{15} + 9x^{14} + 5x^{10} + 9x$.
(2) $x^{16} + 7x^{10} + 3x^4 + 3x$ над $\mathbb{F}_{23}$.

Классификация Диксона содержит условия на перестановочные многочлены степеней до 5, и поэтому для четырехчленов степени 5 можно доказать явный критерий перестановочного многочлена. Вопрос о продолжении классификации Диксона на многочлены больших степеней, в т.ч. на многочлены степени 6 и 7, является открытым.

Лемма 6. *Пусть $f(x) = x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x$ — перестановочных четырехчлен степени 5 над простым полем $\mathbb{F}_p, p > 13$. Тогда:*

(1) $\gcd(p^2 - 1, 5) = 1$
(2) *либо $c_2 = 0$, либо $c_3 = 0$*
(3) *существует значение $b \in \mathbb{F}_p^*$ такое, что многочлен $f(x)$ может быть представлен в виде:*
   (a) $f(x) = x^5 + 15bx^4 + 60b^2x^3 - 225b^4x$, *если* $c_2 = 0$.
   (b) $f(x) = x^5 + 5bx^4 - 20b^3x^2 - 5b^4x$, *если* $c_3 = 0$.

Доказательство. При $p > 13$ классификация Диксона показывает, что все перестановочные многочлены степени 5 получится линейной подставкой и линейным преобразованием многочлена Диксона, а именно $g(x) = dD_5(cx + b, a) + e$, где $D_5(x, \beta) = x^5 - 5\beta x^3 + 5\beta^2 x$ — многочлен Диксона. Значение e можно всегда выбрать противоположным свободному члены, поэтому можно считать, что $g(x)$ не содержит свободного члена. Классификация Диксона также показывается, что $\gcd(p^2 - 1, 5) = 1$.

Выражение $g(x) = dD_5(cx + b, a) + e$ без свободного члена равно

$$c^5dx^5 + 5bc^4dx^4 - 5(a - 2b^2)c^3dx^3 - 5b(3a - 2b^2)c^2dx^2 + 5(b^4 - 3ab^2 + a^2)cdx \tag{1}$$

Условие нормировки дает ограничение $c^5d = 1$.

Многочлен 1 задаёт четырехчлен, если $b \neq 0$ и один из коэффициентов при x, x^2 или x^3 равен 0. Коэффициент при x не может быть равным нулю, т.к. $b^4 - 3ab^2 + a^2$ неприводим над $\mathbb{F}_p$, если $\gcd(p^2 - 1, 5) = 1$ ввиду того, что 5 не является квадратичным вычетом.

Приравнивание коэффициентов отдельно при x^2 и при x^3 с необходимой линейной заменой приводит к доказательству леммы. □

Класс	**Двучлены**	**Трехчлены**	**Четырехчлены**
$x^r f(x^{\frac{p-1}{d}})$	$d < 2\log p$	$d < 4\log p$	$d < 6\log p$
$f(x^r)$	-	$\deg f \leqslant 5$	$\deg f \leqslant 7$
Серия Эрмита	-	-	$ax^r\left(x^{\frac{p-1}{2}+1}\right)+bx^m\left(x^{\frac{p-1}{2}-1}\right)$

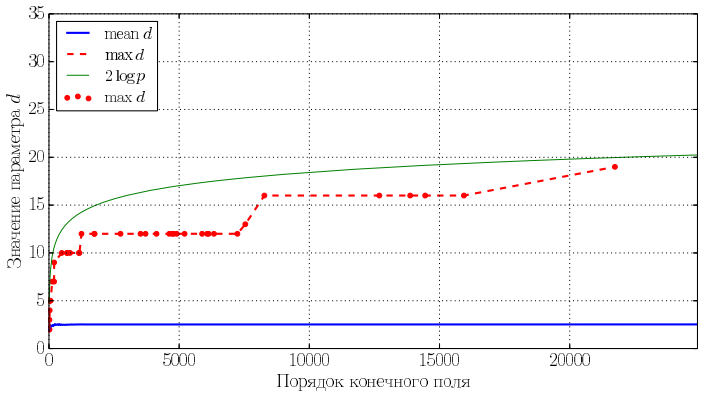
Таблица 2. Классификация перестановочных многочленов

Таблица 2 содержит сравнение классификаций для перестановочных двучленов, трехчленов и четырехчленов. Анализ результатов перечисления показывает, что большинство перестановочных трехчлены и четырехчлены принадлежат первому классу, т.е. представимы в виде $x^r f(x^{\frac{p-1}{d}})$ с малым значении параметра d. Так среди перечисленных результатов для трехчленов доля таких многочленов большое 96.7%, а для четырехчленов их доля около 73.5%, в то время как доля четырехчленов в серии Эрмита около 25%.

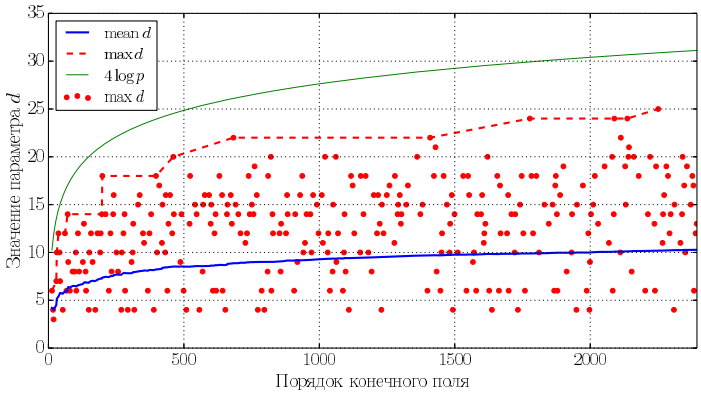
§3. Перестановочные многочлены в форме $x^r f(x^{\frac{p-1}{d}})$

Перестановочные многочлены в форме $x^r f(x^{\frac{p-1}{d}})$ при малых значениях d образуют важный класс перестановочных многочленов. Операции с такими многочленами осуществляются за полиномиальное время от параметра d. Результаты экспериментов показывают, что большинство перестановочных многочленов малой длины могут быть записаны в такой форме. В работе [9] доказывается, что для перестановочных двучленов $d < \sqrt{p}$, и выдвигается гипотеза о том, что $d < 2\log p$. Зависимость максимального значения параметра d от порядка простого поля приведена на рисунке 3. Т.к. параметр d является делителем $p-1$, то максимальное значение d сильно зависит от разложения $p-1$ на множители. Вместе с тем эксперименты показывают, что максимальное значение d ограничено логарифмической функцией от d. На основании оценок для двучленов, трехчленов и четырехчленов можно предположить следующую неформальную гипотезу 7 о значении d для перестановочных многочленов ограниченной длины.

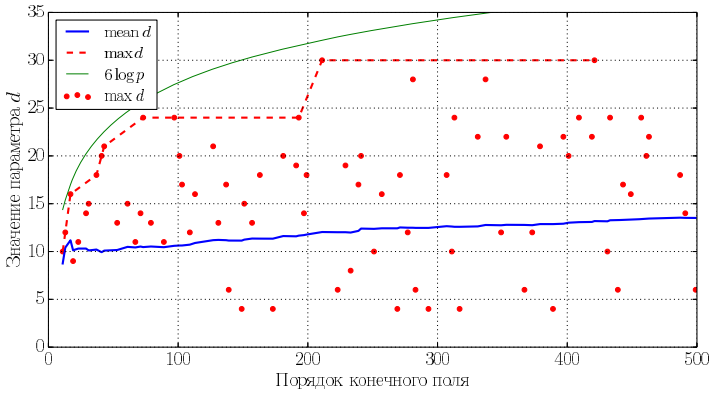
Гипотеза 7. *Существенная часть перестановочных многочленов длины k над конечным полем $\mathbb{F}_p$ может быть представлена в виде $x^r f(x^{\frac{p-1}{d}})$, где $d < 2(k-1)\log p$.*



Двучлены



Трехчлены



Четырехчлены

Рис. 3. Сравнение скорости роста максимального значения d и его оценки. На рисунке 3 промежуточные максимальные значения d опущены.

§4. Исследование статистических свойств перестановочных многочленов

Одним из основных приложений теории перестановочных многочленов может стать криптография с открытым ключом, в которой перестановочный многочлен будет использоваться в качестве функции шифрования. Данный вопрос поднимался в нескольких работах [10–12]. В работе [5] показано, что перестановочные двучлены не походят на эту роль обобщения криптографического протокола RSA ввиду свойств степеней мономов. При этом вопрос об использовании более сложных многочленов остается открытым.

p	**Двучлены**	**Трехчлены**
11	0.476	0.573
13	0.427	0.470
17	0.470	0.493
19	0.525	0.371
23	0.411	0.514
29	0.366	0.394
31	0.350	0.365
...	...	...
73	0.340	0.321
79	0.182	0.241
83	0.302	0.530
...	...	...
269	0.228	0.240
271	0.327	0.258
277	0.245	0.274
281	0.161	0.234
283	0.307	0.336

Таблица 3. Среднее значение нормированной длины наибольшего цикла. Для равномерно распределенной случайной перестановки данное значение равно постоянной Голомба – Дикмана $\lambda = 0.6243\ldots$.

Разбиение перестановочных многочленов по количеству мономов естественным образом соответствует мере случайности соответствующих перестановок: перестановочные многочлены длины q задают все

перестановки над конечным полем $\mathbb{F}_p$, в то время как перестановочные одночлены x^k задают перестановки с простой структурой циклов, которые не могут считаться случайными. Но многочлены меньшей длины могут быть вычислены за меньшее время. Использование перестановок, заданных перестановочными многочленами малой длины, позволяет эффективно вычислять данные перестановки, а также позволяет исследовать получаемые алгоритмы алгебраическими методами. При этом возникает вопрос о том, насколько такие перестановки могут быть отличимы от случайных перестановок, и для этого можно исследовать различные статистики. Нами были исследованы максимальная длина цикла и среднее количество циклов для перестановок, соответствующих двучленам, трехчленам и четырехчленном, нормированная на длину перестановки. Для равномерно распределенной случайной перестановки данная статистика равна постоянной Голомба – Дикмана $\lambda = 0.6243...$ [13]. Соответствующие значения для перестановочных многочленов над некоторыми конечными полями приведены в таблице 3.

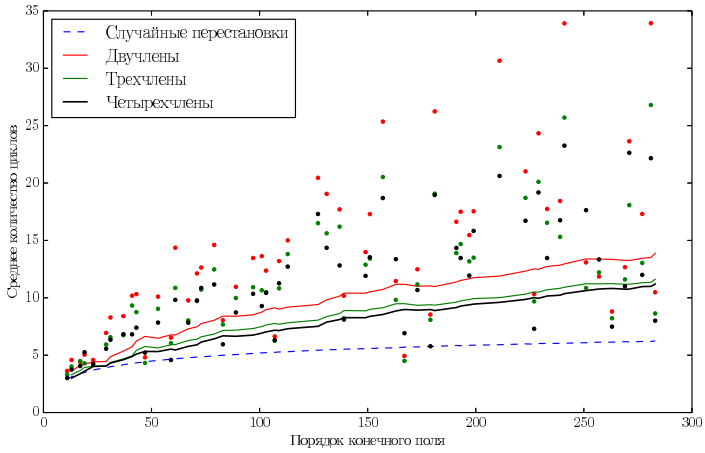


Рис. 4. Среднее число циклов в перестановках, соответствующих перестановочным двучленам, трехчленам и четырехчленам.

На рисунке 4 приведено среднее число циклов в перестановках, соответствующих перестановочным многочленам. Для Сравнения на этом же графике приведено соответствующее значение для равномерно распределенной случайной перестановки.

Экспериментальные результаты, приведенные в таблице 3 и на графике 4, показывают, что перестановочные многочлены малой длины задают перестановки, статистические свойства которых значительно отличаются от равномерно распределенных случайных перестановок. Вопрос об асимптотическом поведении данных характеристик для перестановочных многочленов остается открытым.

Заключение

В работе были исследованы свойства перестановочных многочленов малой длины над простыми конечными полями. В литературе не упоминается об общих свойствах перестановочных трехчленов и четырехчленов, и поэтому для нахождения таких свойства нами были применены компьютерные эксперименты по перечислению таких многочленов. Задача перечисления является вычислительно сложной ввиду огромного пространства поиска параметров многочлена, и различные подходы по сокращению этого пространства поиска обсуждаются в первой части данной статьи.

Анализ результатов алгоритма перечисления позвонил построить классификацию для перестановочных трехчленов и четырехчленов над простыми конечными полями. Эта классификация является расширением классификации перестановочных двучленов, в которую были добавлены два новых класса. Одним из основных результатов данной статьи является гипотеза о том, что все множество перестановочных трехчленов может быть разбито на два класса, а множество четырехчленов - на три. Вопрос о доказательстве корректности данной классификации является открытым.

Литература

1. C. Hermite, *Sur les fonctions de sept lettres* 1905.
2. L. E. Dickson, *The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group.* — Ann. Math. **11** (1896), 161–183.
3. R. Lidl, G. L. Mullen, *When Does a Polynomial over a Finite Field Permute the Elements of the Field?* — The American Mathematical Monthly **95**, no. 3 (1988), 243.

4. R. Lidl, G. L. Mullen, *When Does a Polynomial over a Finite Field Permute the Elements of the Field?, II* The American Mathematical Monthly **100**, no. 1 (1993), 71.
5. N. Vasilev, M. Rybalkin, *Permutation binomials and their groups.* — J. Math. Sci. **179** (2011), 679–689; 10.1007/s10958-011-0618-x.
6. D. Wan, R. Lidl, *Permutation polynomials of the form $x^r f(x^{\frac{q-1}{d}})$ and their group structure.* — Monatshefte für Mathematik **112**, no. 2 (1991), 149–163.
7. M. E. Zieve, *On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$.* — /arxiv.org/abs/0707.1110.
8. Qiang Wang, *On inverse permutation polynomials.* — Finite Fields and Their Applications bf15, no. 2 (2009), 207–213.
9. A. M. Masuda, M. E. Zieve, *Permutation binomials over finite fields.* — Trans. Amer. Math. Soc. (2007).
10. R. P. Singh, B. K. Sarma, A. Saikia, *Public key cryptography using permutation p-polynomials over fields.* — IACR Cryptology ePrint Archive (2009), 208.
11. G. Castagnos, D. Vergnaud, *Trapdoor permutation polynomials of $\mathbf{Z}/n\mathbf{Z}$ and public key cryptosystems.* — In: Information Security, 10th International Conference, ISC 2007, Lect. Notes Comput. Sci. **4779**, Springer, 2007, pp. 333–350.
12. R. Lidl, and W. B. Müller, *Permutation polynomials in RSA-cryptosystems.* — In: Advances in cryptology (Santa Barbara, Calif., 1983), Plenum, New York (1984), pp. 293–310.
13. S. R. Finch, *Mathematical Constants.* Encyclopedia of mathematics and its applications **94** (2003).

Rybalkin M. A. Classification of permutation fewnomials over simple finite fields.

We present a method for permutation trinomials and quadrinomials enumeration based on various symmetries and algebraic properties for search space reduction. Using this method, we enumerated all permutation trinomials and quadrinomials for the prime finite fields with orders up to 3000 and 500 respectively. Based on the enumeration results, we stated a hypothesis about permutation polynomials classification over prime finite fields. We evaluated randomness of such permutations.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН, Фонтанка 27,
191023 С.-Петербург, Россия

Поступило 17 декабря 2013 г.

E-mail: rybalkin@pdmi.ras.ru