УДК 512.62

# ПЕРЕСТАНОВОЧНЫЕ МНОГОЧЛЕНЫ МАЛОЙ ДЛИНЫ НАД ПРОСТЫМИ КОНЕЧНЫМИ ПОЛЯМИ

***М. А. Рыбалкин***[a, 1], *аспирант*
[a]*Санкт-Петербургское отделение Математического института им. В. А. Стеклова РАН, Санкт-Петербург, РФ*

***Постановка проблемы:*** *перестановочным многочленом над конечным полем называется многочлен, реализующий перестановку элементов конечного поля. В настоящее время не известно эффективных критериев для определения перестановочных многочленов над конечными полями даже для многочленов малой длины, состоящих из нескольких мономов. Для построения таких критериев нами была поставлена задача о построении таблиц перестановочных многочленов, зависимости в которых можно использовать для нахождения новых серий перестановочных многочленов, а также для построения эффективных критериев таких многочленов.* ***Методы:*** *реализация алгоритма перебора на C++, численные эксперименты в системе компьютерной алгебры Sage, вычисление порядков групп перестановок в системе компьютерной алгебры GAP.* ***Результаты:*** *разработан метод перечисления перестановочных многочленов, работающий для многочленов малой длины, на основе которого были вычислены таблицы перестановочных пятичленов для простых конечных полей характеристики до 100. Полученные таблицы пятичленов были сравнены с таблицами перестановочных четырехчленов, трехчленов и двучленов над конечными полями из предыдущих работ. Исследование общих зависимостей и сравнение с предыдущей гипотезой о классификации многочленов меньшей длины позволили сформулировать гипотезу об общей классификации перестановочных многочленов с не более чем пятью членами. Также было проведено исследование статистических свойств случайных перестановок, соответствующих случайному выбору равнораспределенных случайных перестановочных многочленов с фиксированным количеством мономов. Было показано, что получающееся распределение на перестановках уже не является равномерно распределенным.* ***Практическая значимость:*** *сформулированные гипотезы о классификации перестановочных многочленов малой длины являются шагом к построению полной доказанной классификации перестановочных многочленов, а также могут быть использованы при построении криптографических протоколов с открытым ключом на основе перестановочных многочленов.*

***Ключевые слова*** *— перестановочные многочлены, конечные поля, криптография с открытым ключом.*

## Введение

Пусть $p$ — просто число и $q = p^n$. Многочлен $f(x)$ называется перестановочным многочленом над конечным полем $GF(q)$, если соответствующее ему отображение задает перестановку элементов множества $GF(q)$. Перестановочный многочлен можно использовать как полиномиальную форму перестановки. Исследование перестановочных многочленов началось с работ Эрмита и Диксона [1, 2]. Перестановочные многочлены могут представлять собой краткую форму нетривиальных перестановок над конечными полями, и в связи с этим в настоящее время наблюдается повышение интереса к перестановочным многочленам из-за их потенциальных приложений в криптографии, теории кодирования и комбинаторике. Над конечным полем $GF(q)$ существует $q!$ перестановок, и каждую такую перестановку задает единственный перестановочный многочлен степени, меньшей $q$, который может быть получен как интерполяционный многочлен. Интерес представляют задачи о характеризации перестановок, которые бы соответствовали многочленам с небольшим количеством членов: двучленам, трехчленам, четырехчленам и пятичленам. Иногда такие многочлены называются малочленами. Их важным обобщением являются многочлены с низкой алгоритмической сложностью вычисления. Также очень интересной является задача об исследовании полиномиальной формы перестановок определенного вида, например транспозиций и инволюций.

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, нахождение критериев перестановочных двучленов и трехчленов, вопрос о возможности и эффективности использования перестановочных многочленов в криптографии.

В данной работе исследуются перестановочные многочлены малой длины, а именно двучлены, трехчлены, четырехчлены и пятичлены. 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 длины, а также проведен анализ его результатов. На основе данного анализа мы выдвинули гипотезу о классификации перестановочных пятичленов над простыми конечными полями.

[1] Научный руководитель — кандидат физико-математических наук, старший научный сотрудник лаборатории теории представлений и динамических систем Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российской академии наук *Н. Н. Васильев*.

## Связь между перестановочными многочленами и перестановками

### Группы, порождаемые перестановочными двучленами

Каждой перестановке элементов конечного поля можно сопоставить перестановочный многочлен, задающий данную перестановку. Тогда композиции многочленов будет соответствовать умножение перестановок, а значит можно рассматривать группы, образованные перестановочными многочленами разных классов. В 1953 г. было доказано [5] в общем случае, что вся группа перестановок $S_q$ конечного поля $GF(q)$ порождается линейными многочленами и многочленом $x^{q-2}$. Нами были исследованы перестановочные двучлены над конечными полями [6], и для некоторых конечных полей мы обнаружили, что перестановочные двучлены порождают всю группу $S_{q-1}$ перестановок, оставляющих элемент 0 неподвижным. Обозначим через $G(q)$ группу, порожденную перестановочными двучленами. Факт об изоморфизме $S_{q-1}$ и $G(q)$ может быть обобщен и сформулирован в виде гипотезы 1.

*Гипотеза 1.* Существует бесконечное количество конечных полей $GF(q)$, для которых симметрическая группа $S_{q-1}$ перестановок, оставляющих элемент 0 неподвижным, порождается перестановками, задаваемыми перестановочными двучленами $ax^n + bx^m$.

Экспериментально данная гипотеза бала нами проверена для следующих порядков конечных полей: 31, 61, 64, 211, 256, 421, 841, 1024, 1331, 1849, 2521, 2809, 3125, 3481, 3721, 4096, 4489, 4621. Можно отметить, что среди данной последовательности есть все элементы вида $4^n$, $n > 2$. В недавней работе [7] был доказан частный случай гипотезы 1 для случая конечных полей $GF(p^2)$ в следующем виде.

*Теорема 2* ([7], *частный случай гипотезы*). Существует бесконечно много простых чисел $p$, для которых группа $G(p^2)$ изоморфна $S_{p^2-1}$. В частности:

$$\liminf_{N\to\infty} \frac{\text{количество } p : G(p^2) \cong S_{p^2-1}}{\text{количество простых } p < N} \geq \frac{1}{96}.$$

Вопрос о справедливости гипотезы 1 для случая простых конечных полей остается открытым.

### Инволюции

Интересным вопросом является характеризация перестановочных многочленов, задающих инволюции, т. е. перестановок, обратными к которым являются они сами. Нами были рассмотрены два вида перестановочных двучленов, задающих инволюции. Критерии таких многочленов представлены в виде теорем 3 и 4, доказательство которых может быть получено проверкой условия $f(x) = x \bmod x^p - x$.

*Теорема 3* (*класс 1*). Перестановочный многочлен $ax\left(b + x^{\frac{p-1}{2}}\right)$ над простым конечным полем $GF(p)$ задает инволюцию тогда и только тогда, когда $a^2(b^2 - 1) = 1$ и $\chi(b + 1) = \chi(b - 1) = \chi(a)$, где $\chi$ — квадратичный характер.

*Теорема 4* (*класс 2*). Перестановочный многочлен $ax^{\frac{p-3}{2}}\left(b + x^{\frac{p-1}{2}}\right)$ над простым конечным полем $GF(p)$ задает инволюцию тогда и только тогда, когда $\chi(b^2 - 1) = -1$ и $\chi(b + 1) = \chi(a)$.

Количество перестановочных двучленов указанных классов над простым конечным полем $GF(p)$ равно $\frac{p-3}{2}$ и $\frac{p-1}{2}\frac{p-3}{2}$ соответственно. Можно показать, что если $\frac{p-1}{2}$ является простым числом, то не существует других классов перестановочных двучленов, задающих инволюции. Вопрос о полной классификации перестановочных многочленов, задающих инволюции, представляет большой интерес и будет рассмотрен в следующих работах.

## Перечисление перестановочных многочленов малой длины

Нормированный многочлен с фиксированным количеством членов описывается его степенями и всеми коэффициентами за исключением старшего.

Например, 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 $x^{n1} + c_2x^{n2} + c_3x^{n3} + c_4x^{n4}$ является перестановочным. Множество перестановочных многочленов над любым конечным полем $GF(q)$ бесконечно, так как к любому перестановочному многочлену можно добавить $x^q - x$. Поэтому достаточно перечислять многочлены степени, меньшей $q$. Они представляют все полиномиальные перестановки над $GF(q)$. 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 существенно 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 эквивалентных многочленов будем называть представительными многочленами.

По аналогии с алгоритмом перечисления перестановочных двучленов [6] можно показать, что достаточно 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) $n_1 \geq \gcd(n_i, q - 1)$ для $i = 2, 3, 4$.

Для дальнейшего использования обозначим через $NoneqDeg(q)$ множество показателей степеней ($n_1$, $n_2$, $n_3$, $n_4$), удовлетворяющих приведенными выше условиями.

Одним из основных инструментов для проверки критерия перестановочного многочлена общего вида является критерий Эрмита.

*Теорема 5* (*критерий Эрмита*). Пусть $p$ — характеристика поля $GF(q)$. Тогда многочлен $f \in GF(q)[x]$ является перестановочным многочленом тогда и только тогда, когда:

1) для любого $i$ от 1 до $q - 2$ и $i \neq 0 \bmod p$ результат приведения $f^i$ по модулю $x^q - x$ имеет степень меньше $q - 1$;

2) многочлен $f$ имеет ровно один корень в $GF(q)$.

Критерий Эрмита позволяет доказывать, что какой-то многочлен не является перестановочным, так как для этого достаточно 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 $N$, то он заменяется на неизвестное значение $\varepsilon$. При этом вводится тождество, что умножение любого многочлена $f$ на неизвестное значение $\varepsilon$ также дает неизвестное значение $\varepsilon$, что можно записать как $f\varepsilon = \varepsilon$.

Через $Truncate_N(f)$ обозначим функцию, которая заменяет коэффициенты многочлена $f$ на $\varepsilon$, если длина такого коэффициента больше $N$. Тогда получение условий из критерия Эрмита можно записать в виде следующего алгоритма:

**Вход:** $f$ — многочлен с неизвестными коэффициентами

**Выход:** условия в критерии Эрмита длины меньше $N$

**function** $TruncatedHermite_N(f)$
$f' := f$
$Conditions := \varnothing$
**for all** $i = 2..q - 2$ **do**
$f' := Truncate_N(f' f \bmod x^q - x)$
$c := Coef(f', x^{q-1})$
**if** $i \neq 0 \bmod p$, $c \neq 0$, $c \neq \varepsilon$ **then**
$Conditions := Conditions \cup \{c\}$
**end for**
**return** $Conditions$
**end function**

Для конкретных показателей степеней ($n_1, n_2, n_3, n_4$) алгоритм для вычисления $TruncatedHermite_N(f)$ позволяет получить из критерия Эрмита условия, длина которых не превосходит $N$. Если множество таких условий оказалось пустым или состоящим только из одного-двух элементов, это значит, что 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 имеют 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 $GF(331)$.

Итоговый алгоритм перечисления перестановочных четырехчленов можно записать в следующем виде:

**Вход:** $q$ — порядок конечного поля

**Выход:** перестановочные четырехчлены вида $x^{n_1} + c_2x^{n_2} + c_3x^{n_3} + c_4x^{n_4}$

**for all** ($n_1$, $n_2$, $n_3$, $n_4$) **in** $NoneqDeg(q)$ **do**
$HermiteConditions :=$
$:= TruncatedHermite_N(x^{n_1} + c_2x^{n_2} + c_3x^{n_3} + c_4x^{n_4})$
**for all** ($c_2$, $c_3$, $c_4$) **in** Solve($HermiteConditions$)
$f := x^{n_1} + c_2x^{n_2} + c_3x^{n_3} + c_4x^{n_4}$
**if** $f$ — перестановочный многочлен
**yield** $f$
end for
**end for**

Алгоритм для перечисления трехчленов и пятичленов аналогичен данному алгоритму. На практике данный алгоритм применим для перечисления перестановочных многочленов, содержащих до пяти членов, т. е. двучленов, трехчленов, четырехчленов и пятичленов. Этот алгоритм позволил перечислить все перестановочные пятичлены для простых конечных полей $GF(p)$, $p < 100$,

■ ***Таблица 1.*** Примеры перестановочных малочленов

| Перестановочный многочлен | Конечное поле |
|---|---|
| $x + 61x^{45}$ | $GF(67)$ |
| $x + 122x^{114}$ | $GF(227)$ |
| $x^3 + 154x^{263}$ | $GF(313)$ |
| $x^4 + 194x^{241}$ | $GF(317)$ |
| $x + 143x^{174}$ | $GF(347)$ |
| $x + x^2 + 44x^3$ | $GF(131)$ |
| $x + 6x^{39} + 49x^{77}$ | $GF(229)$ |
| $x^3 + 20x^{210} + 200x^{256}$ | $GF(277)$ |
| $x + 194x^{142} + 257x^{189}$ | $GF(283)$ |
| $x + x^2 + 24x^4 + 33x^5$ | $GF(53)$ |
| $x + x^4 + 66x^{34} + x^{37}$ | $GF(67)$ |
| $x^2 + 8x^{15} + 53x^{28} + 11x^{54}$ | $GF(79)$ |
| $x + x^{40} + 82x^{42} + x^{81}$ | $GF(83)$ |
| $x + 2x^3 + 46x^5 + 40x^7 + 9x^9$ | $GF(59)$ |
| $x^4 + 4x^{16} + 12x^{25} + 47x^{28} + 9x^{52}$ | $GF(61)$ |

все четырехчлены при $p < 500$ и все трехчлены для простых конечных полей $GF(p)$, $p < 5000$. Примеры некоторых перечисленных многочленов приведены в табл. 1. Результаты перечислений и гипотезы о свойствах перестановочных малочленов приводятся в следующих разделах.

## Анализ серий и классификация перестановочных многочленов

Любой многочлен над конечным полем $GF(q)$ может быть представлен в виде $x^r f\left(x^{\frac{q-1}{d}}\right)$, где значение параметра $d$ является важной характеристикой. Такое представление является интересным при $d > 1$. Так, проверка перестановочного многочлена может быть осуществлена за $O(d^2)$ операций [8, 9], а многочлен, соответствующий обратному отображению, также может быть найден за $O(d^2)$ операций [10]. При фиксированном $d$ класс таких многочленов замкнут относительно операции композиции, и в работе [8] исследуется размер порождаемой группы. В работе [11] доказывается, что для перестановочных двучленов над простыми конечными полями $GF(p)$ значение $d$ ограничено снизу значением $\sqrt{p}$, а также выдвигается гипотеза о том, что $d < 2\log p$. При выполнении этой гипотезы за полиномиальное время могут быть эффективно реализованы следующие операции с перестановочными двучленами над конечными полями:

1) проверка того, что двучлен является перестановочным;

2) построение случайных перестановочных двучленов;

3) нахождение многочлена, соответствующего обратному отображению.

Из работы [11] следует, что все множество перестановочных двучленов принадлежит одному классу вида $x^r f\left(x^{\frac{p-1}{d}}\right)$, где $d < 2\log p$ в предположении справедливости гипотезы о классификации. В нашей предыдущей работе [12] была предложена гипотеза о классификации, которая показывает, что для трехчленов и четырехчленов большинство многочленов принадлежит аналогичному классу, но в дополнение для трехчленов появляется еще один класс, а для четырехчленов появляются два класса. Экспериментальные результаты данной работы показывают, что классификация для пятичленов также аналогична классификации для четырехчленов.

Сравнение классификаций для перестановочных двучленов, трехчленов и четырехчленов и пятичленов приведено в табл. 2. Класс 1 содержит все многочлены вида $x^r f\left(x^{\frac{p-1}{d}}\right)$, свойства которых были описаны выше.

Неравенство в ограничении на $d$ не является строгим, но позволяет сравнить соответствующее значение для многочленов разной длины. Из таблицы видно, что с увеличением длины многочлена значение $d$ также увеличивается. Класс 2 представляет собой композицию монома и многочлена малой степени. При этом прослеживается зависимость между степенью такого многочлена: она ограничена значением $2n - 1$, где $n$ — длина многочлена.

■ ***Таблица 2.*** Классификация перестановочных многочленов

| Тип | Класс 1 $x^r f\left(x^{\frac{p-1}{d}}\right)$ | Класс 2 $f\left(x^r\right)$ | Специальный класс |
|---|---|---|---|
| Двучлены | $d < 2\log p$ | — | — |
| Трехчлены | $d < 4\log p$ | $\deg f \le 5$ | — |
| Четырехчлены | $d < 6\log p$ | $\deg f \le 7$ | Серия Эрмита [12] |
| Пятичлены | $d < 8\log p$ | $\deg f \le 9$ | Новый класс |

■ ***Таблица 3.*** Примеры перестановочных пятичленов, попадающих в классы 1 и 2

| Перестановочный пятичлен | Конечное поле |
|---|---|
| $x + 6x^3 - 9x^{21} + 6x^{22} + 13x^{23}$ | $GF(41)$ |
| $x + 2x^3 - x^5 + 6x^{28} - 21x^{30}$ | $GF(53)$ |
| $x + x^7 + x^{29} - x^{45} + x^{51}$ | $GF(67)$ |
| $x + x^7 + x^{23} + x^{45} - x^{51}$ | $GF(67)$ |
| $x + x^{21} + x^{23} - x^{43} + x^{45}$ | $GF(67)$ |

■ ***Таблица 4.*** Среднее значение нормированной длины наибольшего цикла

| $p$ | Двучлены | Трехчлены | Четырехчлены | Пятичлены |
|---|---|---|---|---|
| 29 | 0,366 | 0,394 | 0,434 | 0,479 |
| 31 | 0,350 | 0,365 | 0,440 | 0,478 |
| 43 | 0,259 | 0,356 | 0,435 | 0,491 |
| 53 | 0,240 | 0,306 | 0,307 | 0,432 |

Классификация перестановочных четырехчленов [14] содержит класс, названный серией Эрмита ввиду того, что он был приведен в работе Эрмита [1] в качестве примера нетривиального перестановочного многочлена:

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

Экспериментальные результаты по перестановочным пятичленам также содержат небольшое число многочленов, не принадлежащих классу 1 и 2 и похожих на многочлены из серии Эрмита, но вычислительная сложность перечисления не позволила нам получить достаточное количество таких многочленов, чтобы можно было обобщить их форму. Несколько таких многочленов приведены в табл. 3. Обобщение данного класса будет сделано в следующих работах.

Анализ результатов перечисления показывает, что большинство перестановочных многочленов малой длины принадлежит первому классу, т. е. представимо в виде $x^r f\left(x^{\frac{p-1}{d}}\right)$ с малым значением параметра $d$.

## 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 [13–15]. В работе [6] показано, что перестановочные двучлены не подходят на роль обобщения криптографического протокола RSA ввиду свойств степеней мономов. При этом вопрос об использовании более сложных многочленов остается открытым.

Разбиение перестановочных многочленов по количеству мономов естественным образом соответствует мере случайности задаваемых перестановок: перестановочные многочлены длины $q$ задают все перестановки над конечным полем $GF(q)$, 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 исследовать получаемые алгоритмы алгебраическими методами. При этом возникает вопрос, насколько такие перестановки могут быть отличимы от случайных перестановок, и для этого можно исследовать различные статистики. Нами была исследована максимальная длина цикла, соответствующая двучленам, трехчленам, четырехчленам и пятичленам, нормированная на длину перестановки. Для случайной перестановки данная статистика равна постоянной Голомба — Дикмана $\lambda \approx 0{,}6243$ [16]. Соответствующие значения для перестановочных многочленов над некоторыми конечными полями приведены в табл. 4.

Экспериментальные результаты, приведенные в табл. 4, показывают, что перестановочные многочлены малой длины задают перестановки, статистические свойства которых значительно отличаются от случайных перестановок с равномерным распределением. Вопрос об асимптотическом поведении данных характеристик для перестановочных многочленов остается открытым.

## Заключение

В представляемой работе описывается алгоритм перечисления и исследуются свойства перестановочных многочленов малой длины над простыми конечными полями. Об общих свойствах таких перестановочных многочленов малой длины известно очень мало, поэтому для нахождения таких свойств нами были применены компьютерные эксперименты по полному перечислению таких многочленов. Задача перечисления является алгоритмически сложной ввиду огромного пространства поиска параметров многочлена, и для перечисления нами были разработаны различные методы по сокращению этого пространства поиска.

Анализ результатов компьютерного перечисления позволил сформулировать гипотезы

о классификации перестановочных многочленов, состоящих не более чем из пяти членов. Эта классификация является расширением аналогичной классификации перестановочных двучленов, в которую были добавлены два новых класса. Также на основе проведенных компьютерных вычислений можно сделать наблюдение о том, что все множество перестановочных пятичленов может быть разбито на три класса. Вопрос о доказательстве полноты и корректности этой классификации будет предметом обсуждения в последующих работах.

## Литература


1. **Hermite C.** Sur Les Fonctions de Sept Lettres // C. R. Acad. Sci. Paris. 1905. P. 750–757.
2. **Dickson L. E.** The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group // Annals of Mathematics. 1896. Vol. 11. N 1/6. P. 161–183.
3. **Lidl R., Mullen G. L.** When Does a Polynomial over a Finite Field Permute the Elements of the Field? // The American Mathematical Monthly. 1988. Vol. 95. P. 243–246.
4. **Lidl R., Mullen G. L.** When Does a Polynomial over a Finite Field Permute the Elements of the Field? II // The American Mathematical Monthly. 1993. Vol. 100. P. 71–74.
5. **Carlitz L.** Permutations in a Finite Field // Proc. of the American Mathematical Society. 1953. Vol. 4. P. 538.
6. **Vasilev N., Rybalkin M.** Permutation Binomials and their Groups // J. of Mathematical Sciences. 2011. Vol. 179. P. 679–689.
7. **Zieve M. E.** Permutation Groups Generated by Binomials // ArXiv e-prints. Dec. 2013. http://arxiv.org/pdf/1312.2649.pdf (дата обращения: 13.01.2014).
8. **Wan D., Lidl R.** Permutation Polynomials of the Form $x^r f(x^{(q-1)/d})$ and their Group Structure // Monatshefte fur Mathematik. 1991. Vol. 112. N 2. P. 149–163.
9. **Zieve M. E.** On Some Permutation Polynomials over Fq of the Form $x^r h(x^{(q-1)/d})$ // Proc. of the American Mathematical Society. 2009. Vol. 137. N 7. P. 2209–2216.
10. **Wang Q.** On Inverse Permutation Polynomials // Finite Fields and Their Applications. 2009. Vol. 15. N 2. P. 207–213.
11. **Masuda A. M., Zieve M. E.** Permutation Binomials over Finite Fields // Transactions of the American Mathematical Society. 2009. Vol. 361. N 8. P. 4169–4180.
12. **Рыбалкин М.** Классификация перестановочных многочленов малой длины над простыми конечными полями // Записки научных семинаров ПОМИ. 2014. № 421. С. 152–165.
13. **Singh R. P., Sarma B. K., Saikia A.** Public Key Cryptography Using Permutation p-polynomials over Finite Fields // IACR Cryptology ePrint Archive. 2009. http://eprint.iacr.org/2009/208 (дата обращения: 23.04.2014).
14. **Castagnos G., Vergnaud D.** Trapdoor Permutation Polynomials of Z/nZ and Public Key Cryptosystems // Lecture Notes in Computer Science. 2007. Vol. 4779. P. 333–350.
15. **Lidl R., Muller W. B.** Permutation Polynomials in RSA-cryptosystems //Proc. of Conf. «Advances in Cryptology» (CRYPTO 83), Santa Barbara, California, 1983. P. 293–301.
16. **Finch S. R.** Mathematical Constants//Encyclopedia of Mathematics and its Applications. 2003. Vol. 94. P. 284–286.


UDC 512.62

**Permutation Polynomials of Small Length over Prime Finite Fields**

Rybalkin M. A.[a], Post-Graduate Student, rybalkin@pdmi.ras.ru
[a]Saint-Petersburg Department of the Steklov Mathematical Institute of RAS, Saint-Petersburg, Russian Federation

**Purpose:** A permutation polynomial over a finite field is a polynomial inducing a permutation of finite field elements. At present, there are no known efficient criteria for permutation polynomials even with a small number of monomials. The purpose of this work was to generate tables of permutation polynomials, to study these tables in order to find new series of permutation polynomials, and to propose and prove some hypotheses about permutation polynomials. **Methods:** C++ algorithm implementation, numeric experiments in the Sage computer algebra system, computation of permutation group orders in the GAP computer algebra system. **Results:** A permutation polynomials enumeration algorithm was developed which works for polynomials of small length. Using it, tables of permutation quintics were built for prime finite fields up to order 100. These tables were compared with the tables for permutation quadrinomials, trinomials and binomials obtained in our previous works. To formulate a hypothesis on permutation polynomials classification, we studied dependencies between polynomials in the obtained tables. We also studied the statistical properties of random permutations generated by random permutation polynomials with a fixed number of monomials using uniform distribution. It was shown that the obtained distribution is not uniform. **Practical relevance:** The stated hypotheses on the classification of small-length permutation polynomials lead towards their complete proved classification. These hypotheses can also be used for constructing public-key cryptographic protocols based on permutation polynomials.

**Keywords** — Permutation Polynomials, Finite Fields, Public Key Cryptography.

**References**

1. Hermite C. Sur Les Fonctions de Sept Lettres. *C. R. Acad. Sci.*, Paris, 1905, pp. 750–757.
2. Dickson L. E. The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group. *Annals of Mathematics*, 1896, vol. 11, no. 1/6, pp. 161–183.
3. Lidl R., Mullen G. L. When Does a Polynomial over a Finite Field Permute the Elements of the Field? *The American Mathematical Monthly*, 1988, vol. 95, pp. 243–246.
4. Lidl R., Mullen G. L. When Does a Polynomial over a Finite Field Permute the Elements of the Field? II. *The American Mathematical Monthly*, 1993, vol. 100, pp. 71–74.
5. Carlitz L. Permutations in a Finite Field. *Proc. of the American Mathematical Society*, 1953, vol. 4, p. 538.
6. Vasilev N., Rybalkin M. Permutation Binomials and their Groups. *Journal of Mathematical Sciences*, 2011, vol. 179, pp. 679–689.
7. Zieve M. E. Permutation Groups Generated by Binomials. *ArXiv e-prints*, 2013. Available at: http://arxiv.org/pdf/1312.2649.pdf (accessed 13 January 2014).
8. Wan D., Lidl R. Permutation Polynomials of the Form $x^r f(x^{(q-1)/d})$ and their Group Structure. *Monatshefte fur Mathematik*, 1991, vol. 112, no. 2, pp. 149–163.
9. Zieve M. E. On Some Permutation Polynomials over Fq of the Form $x^r h(x^{(q-1)/d})$. *Proc. of the American Mathematical Society*, 2009, vol. 137, no. 7, pp. 2209–2216.
10. Wang Q. On Inverse Permutation Polynomials. *Finite Fields and Their Applications*, 2009, vol. 15, no. 2, pp. 207–213.
11. Masuda A. M., Zieve M. E. Permutation Binomials over Finite Fields. *Transactions of the American Mathematical Society*, 2009, vol. 361, no. 8, pp. 4169–4180.
12. Rybalkin M. Classification of Permutation Trinomials and Quadrinomials over Prime Fields. *Zapiski nauchnykh seminarov POMI*, 2014, vol. 200, no. 6, pp. 734–741 (In Russian).
13. Singh R. P., Sarma B. K., Saikia A. Public Key Cryptography Using Permutation p-polynomials over Finite Fields. *IACR Cryptology ePrint Archive*, 2009. Available at: http://eprint.iacr.org/2009/208 (accessed 24 April 2014).
14. Castagnos G., Vergnaud D. Trapdoor Permutation Polynomials of Z/nZ and Public Key Cryptosystems. *Lecture Notes in Computer Science*, 2007, vol. 4779, pp. 333–350.
15. Lidl R., Muller W. B. Permutation Polynomials in RSA-cryptosystems. *Proc. of Conf. "Advances in Cryptology" (CRYPTO 83)*, Santa Barbara, California, 1983, pp. 293–301.
16. Finch S. R. Mathematical Constants. *Encyclopedia of Mathematics and its Applications*, 2003, vol. 94, pp. 284–286.

## ПАМЯТКА ДЛЯ АВТОРОВ

*Поступающие в редакцию статьи проходят обязательное рецензирование.*

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию. Рукописи не возвращаются.

*Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.*