

ТЕОРІЯ ТА МЕТОДИ ОБРОБЛЕННЯ СИГНАЛІВ

УДК 519.711/.72 (045)

А. Я. Белецкий, д-р техн. наук, проф.,
Д. А. Стеценко**ПОРЯДОК АБЕЛЕВЫХ ЦИКЛИЧЕСКИХ ГРУПП, ПОРОЖДАЕМЫХ
ОБОБЩЕННЫМИ ПРЕОБРАЗОВАНИЯМИ ГРЕЯ**

Институт электроники и систем управления НАУ, e-mail: abelnau@ukr.net

Получены оценки периода цикла L_n квадратных невырожденных $(0, 1)$ -матриц n -го порядка, порождаемых составными преобразованиями Грея $G = 1g$. Показано, что этот период определяется соотношением $L_n = 2^m - 1$, где $m \leq n$, за исключением ограниченного набора n , образующих подмножество артефактов.

Ключевые слова: группа, преобразования Грея, образующая матрица.

Введение и постановка задачи. Пусть \mathbf{M}_n есть квадратная невырожденная матрица n -го порядка, компонентами которой являются числа 0, 1. Совокупность степеней \mathbf{M}_n^k , $k \geq 0$, этой матрицы над кольцом вычетов по mod 2 образует абелеву циклическую группу порядка L_n , в которой \mathbf{M}_n^0 совпадает с единичной матрицей n -го порядка. Оценка порядка циклической группы, порождаемой степенями матриц \mathbf{M}_n , относится к чрезвычайно сложным задачам и остается нерешенной до настоящего времени. Вместе с тем, для ряда приложений знание L_n является насущно необходимым. Приведем пример из криптографии.

В статье [1] авторы предлагают строить блочные шифры на основе обратимых над полем $GF(2)$ матриц двух элементов 0 и 1. Если \mathbf{X}, \mathbf{Y} – двоичные векторы, представляющие соответственно открытый и зашифрованный текст, а \mathbf{M} – шифрующая матрица n -го порядка, то шифрование задается уравнением $\mathbf{Y} = \mathbf{X} \cdot \mathbf{M}$. Расшифрование осуществляется обратным преобразованием $\mathbf{X} = \mathbf{Y} \cdot \mathbf{M}^{-1}$. Ключом шифрования является матрица \mathbf{M} .

Для установления сеансовых ключей авторы предлагают использовать протокол Диффи–Хеллмана [2] в циклической группе двоичных матриц \mathbf{M} , причем \mathbf{M} считается общедоступной. В процессе выполнения протокола обмена данными абонент A вырабатывает случайный показатель x , вычисляет матрицу \mathbf{M}^x , которую посылает пользователю B . В свою очередь пользователь B вырабатывает случайный показатель y , вычисляет матрицу \mathbf{M}^y и посылает ее пользователю A . Затем оба пользователя возводят полученные матрицы в свои степени и получают общую матрицу $\mathbf{M}^{xy} = \mathbf{M}^{yx}$. По мнению авторов, количество невырожденных матриц при рекомендованном порядке $n = 100$ достаточно велико. На этом основании утверждается, что вычисление ключа имеет переборную сложность.

К сожалению, это не всегда так, в чем мы убедимся в дальнейшем. Основная проблема использования приведенного выше алгоритма шифрования состоит в том, что порядок L_n циклической группы, порождаемой матрицей \mathbf{M} , с ростом n не является гарантированно большим. Причиной такого явления оказывается нелинейный характер зависимости порядка группы L_n от размера n матрицы \mathbf{M} . При некоторых значениях L_n , которые априори нам неизвестны, мы вполне можем столкнуться с ситуацией, когда вычет произведения случайных чисел x и y по mod L_n оказывается не таким уж и большим числом. И как следствие, предполагаемая «переборная сложность» может оказаться совсем «несложной», допуская «лобовую атаку» на ключ шифрования.

В данной работе решается задача синтеза невырожденных квадратных матриц n -го порядка \mathbf{M}_n с компонентами, принадлежащими $GF(2)$, и оценки порядка L_n циклической группы, порождаемой степенями матрицы \mathbf{M}_n в кольце вычетов по mod 2.

Синтез невырожденных двоичных матриц. В основу синтеза матриц \mathbf{M}_n положим достаточно хорошо разработанный одним из соавторов данной статьи алгоритм формирования матриц преобразования, отвечающих обобщенным (составным) кодам Грея (КГ) [3]. В дальнейшем будем рассматривать исключительно лишь матричные формы КГ с элементами 0 и 1, т. е. двоичные матрицы.

Составным кодом Грея (СКГ) называется код \mathbf{G} , образованный произведением простых (элементарных) КГ. Полное множество (группа) простых КГ включает шесть кодов. В их число входят так называемые инварианты преобразования Грея (ПГ), а также операторы прямого и обратного как лево-, так и правостороннего ПГ. Перечисленным элементарным операторам (кодам) Грея поставим в соответствие символьные обозначения \mathbf{g}_i , $i = \overline{0, 5}$. Для простоты обозначения вместо символов кодов будем писать их цифровые индексы.

К инвариантам ПГ относятся оператор \mathbf{g}_0 , представляющий собой единичную матрицу n -го порядка, и оператор инверсной перестановки \mathbf{g}_1 , матричная форма которого (для $n = 4$) имеет вид:

$$1 = \mathbf{g}_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Приведем (также для порядка $n = 4$) матричные формы простых операторов Грея, отвечающих прямому \mathbf{g}_2 и обратному \mathbf{g}_3 левостороннему КГ:

$$2 = \mathbf{g}_2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}; \quad 3 = \mathbf{g}_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Операторы правосторонних ПГ (прямого \mathbf{g}_4 и обратного \mathbf{g}_5) образуются транспонированием соответствующих операторов левосторонних ПГ, т. е. $\mathbf{g}_4 = \mathbf{g}_2^T$ и $\mathbf{g}_5 = \mathbf{g}_3^T$.

Аналитически СКГ можно представить соотношением

$$\mathbf{G} = \prod_{j=1}^k \mathbf{g}_j, \quad (1)$$

где \mathbf{g}_j – простой КГ, выбираемый из полной группы $\{\overline{\mathbf{g}_0, \mathbf{g}_5}\}$, а k – порядок СКГ.

Естественно, что вычисления в соотношении (1), как и всюду далее, необходимо выполнять в кольце вычетов по mod 2.

Как простые, так и составные КГ обладают рядом замечательных свойств. Во-первых, отвечающие им матрицы преобразования являются невырожденными и в силу этого оказываются обратимыми. И, во-вторых, поскольку любой КГ является образующим

элементом абелевой циклической группы, то существуют достаточно простые алгоритмы обращения СКГ.

Подтвердим последнее утверждение на простом примере. Пусть $n = 4$ и $\mathbf{G} = 4251$. Выбранному СКГ отвечает матрица преобразования

$$\mathbf{G} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}. \quad (2)$$

Пусть, кроме того, задана степень $k = 2$ матрицы G . Согласно матрице (2) имеем

$$\mathbf{G}^2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}. \quad (3)$$

В общем случае для вычисления обратной матрицы k -й степени образующего элемента \mathbf{G} циклической группы L -го порядка можно воспользоваться, по крайней мере, тремя вариантами. Поскольку $\mathbf{G}^L \equiv \mathbf{E}$, тогда имеем:

Вариант 1. $\overline{\mathbf{G}^k} = \mathbf{G}^{L-k}$;

Вариант 2. $\overline{\mathbf{G}^k} = \mathbf{G}^k \cdot \mathbf{G}^{L-2k}$.

Порядок циклической группы L , порождаемой элементом \mathbf{G} в матрице (2), равен семи. Это означает, что $\mathbf{G}^7 = \mathbf{E}$. Каждый из приведенных выше вариантов оценок обратной матрицы приводит к одинаковому результату

$$\overline{\mathbf{G}^2} = \mathbf{G}^5 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}. \quad (4)$$

Корректность выражения (4) легко проверить, перемножив матрицы прямого (3) и обратного (4) преобразований. Получим единичную матрицу, как и должно быть.

Можно воспользоваться еще одним (третьим, но далеко не последним) вариантом обращения СКГ. Он состоит из двух этапов. На первом этапе символическая запись кода переписывается в обратном порядке. На втором этапе каждый простой КГ заменяется соответствующим ему обратным кодом. Например, если $\mathbf{G} = 24135$, то $\overline{\mathbf{G}} = 42153$. В самом деле,

$$\mathbf{G} \cdot \overline{\mathbf{G}} = 24135 \cdot 42153 = \mathbf{E}. \quad (5)$$

В конструкции (5) симметрично относительно знака умножения находятся взаимно обратные простые коды (две пары таких кодов выделены связующими линиями), произведение которых равно единичной матрице. И, следовательно, полное произведение множителей в средней части выражения (5) также равно \mathbf{E} , что и подтверждает корректность определения обратного СКГ по третьему варианту.

Период цикла составных кодов Грея $1g$. Как показали результаты компьютерных расчетов, одними из наиболее приемлемых для криптографических приложений являются матрицы, отвечающие СКГ типа $1g$, где $g = \overline{2,5}$ – простые операторы Грея. Замечательная особенность таких матриц состоит в том, что порядок L_n циклических групп, порождаемых

операторами $1g$, за небольшим исключением (названных нами артефактом) определяется соотношением:

$$L_n = 2^m - 1, \quad m \leq n, \quad (6)$$

где n - порядок матрицы.

Обратим внимание на то, что при $m = n$ длина последовательности элементов группы $1g$ совпадает с максимальной длиной ненулевых элементов расширенного поля Галуа $GF(2^n)$ или так называемой m -последовательностью.

Оценки L_n , полученные прямыми компьютерными вычислениями, приведены в табл. 1.

Таблица 1

Порядок циклических групп, отвечающих СКГ $G = 1g$

n	L_n	n	L_n	n	L_n	n	L_n
1	$2^1 - 1$	9	$2^9 - 1$	17	$2^{12} - 1$	25	$2^8 - 1$
2	$2^2 - 1$	10	$2^6 - 1$	18	87381	26	$2^{26} - 1$
3	$2^3 - 1$	11	$2^{11} - 1$	19	$2^{12} - 1$	27	$2^{20} - 1$
4	$2^3 - 1$	12	$2^{10} - 1$	20	$2^{10} - 1$	28	$2^9 - 1$
5	$2^5 - 1$	13	$2^9 - 1$	21	$2^7 - 1$	29	$2^{29} - 1$
6	$2^6 - 1$	14	$2^{14} - 1$	22	$2^{12} - 1$	30	$2^{30} - 1$
7	$2^4 - 1$	15	$2^5 - 1$	23	$2^{23} - 1$	31	$2^6 - 1$
8	$2^4 - 1$	16	$2^5 - 1$	24	$2^{21} - 1$	32	$2^6 - 1$

Из анализа данных, представленных в табл. 1, приходим к таким выводам.

Во-первых, подтверждается форма оценки L_n , заданная соотношением (6). Исключение (артефакт) проявляется лишь в точке $n = 18$, в которой

$$L_{18} = 87381_{10} = 10101010101010101_2 = (2^{18} - 1)/3. \quad (7)$$

Во-вторых, существуют такие значения порядка n (в табл. 1 они выделены затенением), для которых элементы групп, порожденные степенями матриц M_n , составляют последовательность максимальной длины, равную $2^n - 1$.

И, наконец, в-третьих. Для каждой смежной пары значений $(n, n+1)$, расположенных на границе изменения разрядности r (т. е. на границе перехода от r к $(r+1)$ -битным числам), оценки L_n и L_{n+1} совпадают. Такими парами в табл. 1 являются смежные числа (3, 4), (7, 8), (15, 16) и (31, 32). Аналитически порядок циклических групп указанных пар смежных значений n можно представить выражением

$$L_{2^r-1} = L_{2^r} = 2^{r+1} - 1, \quad r \geq 2.$$

Отметим, что для получения значения L_{30} потребовалось порядка 80 часов работы компьютера средней производительности. Естественно, что прямые вычисления периода L_n для $n \geq 33$ становятся не только расточительными, но и физически не реализуемыми, по

крайней мере, для значений n (априорно неизвестных), которые порождают m -последовательности. Выход из создавшейся ситуации состоит в использовании степенных свойств значений L_n . Структурная схема алгоритма оценки L_n для СКГ $G=13$, опирающегося на отмеченные особенности периода циклической группы, показана на рис. 1.

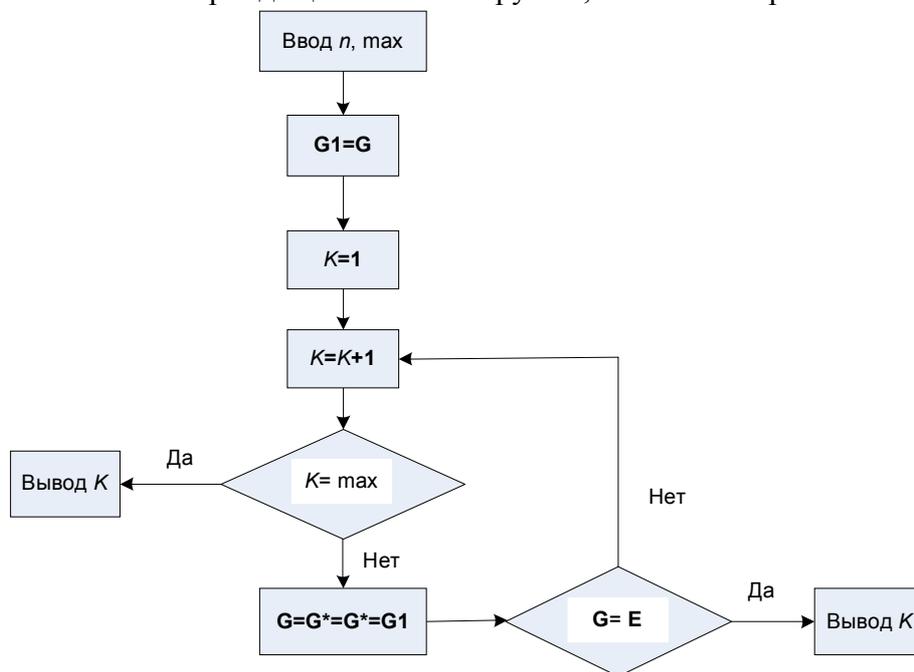


Рис. 1. Алгоритм вычисления степенных значений периода цикла СКГ $G=13$

В данном алгоритме параметр K является показателем степени двойки в оценке (6).

Все значения порядков n (в интервале от 33 до 256) матриц M_n , степени которых формируют n -последовательности, т. е. $L_n = 2^n - 1$, сведены в табл. 2.

Таблица 2

Порядки n матриц M_n , формирующих n -последовательности

33	35	39	41	51	53	65	69	74	81	83	86	89
90	95	99	105	113	119	135	146	155	158	173	179	183
189	191	209	210	221	230	231	233	239	243	245	251	254

Программа вычислений, отвечающая алгоритму, представленному на рис. 1, не в состоянии обнаруживать артефакты. Да она и не предназначена для решения таких задач. Будучи инициализирована значением $n=18$, программа выдаст значение $L_{18} = 2^{18} - 1$, что, согласно табл. 1, не соответствует действительности. Попробуем разобраться более подробно с отмеченным «недоразумением».

Двоичный эквивалент десятичного числа $2^{18} - 1$ представляет собой последовательность из 18 единиц, т. е.

$$(2^{18} - 1)_{10} = 111111111111111111_2. \quad (8)$$

Умножим двоичное значение L_{18} , взяв его из выражения (7), на 3 (также в двоичном представлении, равном 11), получим

На анализируемом интервале выявлен единственный артефакт A_2 в точке $n = 101$. Совмещение артефактов A_1 и A_2 в одном значении n легко объяснимо. Нетрудно убедиться в том, что умножив A_2 на 101_2 , приходим к артефакту A_1 . Артефактов более высокой степени на интервале $n = 33 - 256$ не установлено.

Выводы. Целесообразность применения в криптографии матриц, отвечающих составным кодам Грея, объясняется рядом замечательных свойств, которыми они обладают. Во-первых, матрицы СКГ любого порядка чрезвычайно просто сгенерировать. Во-вторых, такие матрицы являются гарантированно невырожденными. В-третьих, для них легко вычисляются обратные матрицы. И, наконец, отметим еще одну особенность. Как установлено на основании компьютерного моделирования, для произвольных порядков n матриц существуют такие СКГ, которые доставляют соответствующим матрицам свойство n -полноты. Это свойство проявляется в том, что порядок циклических групп, формируемых этими матрицами, достигает максимального значения, равного $2^n - 1$.

Список литературы

1. *Ерош И. Л.* Адресная передача сообщений с использованием матриц над полем GF(2). / Ерош И. Л., Скуратов В. В. // Проблемы информационной безопасности. Компьютерные системы. – 2004. – №1. – С. 72 – 78.
2. *Венбо Мао.* Современная криптография: теория и практика. – М.: Издат. дом «Вильямс», 2005. – 768 с.
3. *Белецкий А. Я.* Комбинаторика кодов Грея. – К.: Издат. компания «КВЦ», 2003. – 506 с.
4. *Белецкий А. Я.* Преобразования Грея / А. Я. Белецкий, А. А. Белецкий, Е. А. Белецкий: монография: в 2 т. – К.: Книж. изд-во НАУ, 2007. – 644 с.

А. Я. Білецький, Д. А. Стеценко

Порядок абелевих циклічних груп, що породжуються узагальненими перетвореннями Грея

Отримано оцінки періоду циклу невідроджених квадратних $(0, 1)$ -матриць n -го порядку, що породжуються складеними перетвореннями Грея $\mathbf{G} = \mathbf{1g}$. Показано, що цей період визначається співвідношенням $L_n = 2^m - 1$, де $m \leq n$, за винятком обмеженого набору n , що створює підмножину артефактів.

A. J. Beletsky, D. A. Stecenko

The order of abelian cyclic groups generated by the generalized transformations of Gray

Estimates of the period of the cycle square nondegenerate $(0, 1)$ -matrices of order raised by the constituent transformations of Gray $\mathbf{G} = \mathbf{1g}$. It is shown that this period is given by $L_n = 2^m - 1$, where $m \leq n$, with the exception of a limited set n of forming a subset of the artifacts.