4. Micciancio D., Voulgaris P. Faster exponential time algorithms for the shortest vector problem // Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms. Society for Industrial and Applied Mathematics. — 2010. — P. 1468–1480.

5. Nielsen M. A., Chuang I. L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2010.

DOI: 10.20948/dms-2022-79

О МОЩНОСТИ ОБРАЗА ПРАВИЛЬНЫХ СЕМЕЙСТВ БУЛЕВЫХ ФУНКЦИЙ

А. В. Галатенко, В. А. Носов, А. Е. Панкратьев, К. Д. Царегородцев (Москва)

Конечные квазигруппы являются перспективной структурой для реализации различных криптографических примитивов [1, 2]. Табличное задание квазигрупповой операции требует квадатичного от порядка квазигруппы объема памяти; как следствие, при использовании квазигрупп большого порядка становится актуальной задача минимизации пространственной сложности. Одно из возможных решений — переход от табличного задания операции к функциональному. В. А. Носовым была предложена конструкция, основанная на правильных семействах функций и позволяющая задавать большие параметрические семества квазигрупп большого порядка [3]. В работе [4] были анонсированы результаты о мощности множества квазигрупп, порождаемых заданным правильным семейством. Оказалось, что эта мощность оценивается снизу с помощью функции от мощности образа правильного семейства. В нашей работе представлен ряд результатов о мощности образа правильных семейств булевых функций.

Определение. Пусть $n \in \mathbb{N}$. Семейство $(g_1, \ldots, g_n)$ булевых функций арности n называется правильным, если для любой пары различных входных наборов $\alpha = (a_1, \ldots, a_n)$ и $\beta = (b_1, \ldots, b_n)$ найдется индекс i, $1 \leq i \leq n$, такой что $a_i \neq b_i$, но $g_i(\alpha) = g_i(\beta)$.

Очевидно, что если все g_i являются константами, семейство правильное. Менее тривиальными примерами являются треугольные семейства, в которых с точностью до согласованной перенумерации функций и аргументов каждая функция может зависеть только от переменных с меньшими номерами (заметим, что по крайней мере одна из функций треугольного семейства является константой), и ортогональные семейства, в которых одноименная переменная фиктивна для каждой функции и для любых $1 \leq i < j \leq n$ выполнено тождество $g_i \cdot g_j \equiv 0$.

Определение. Конечной квазигруппой называется пара (Q, f), где Q — конечное множество, а $f\colon Q \times Q \to Q$ обратима по каждой переменной.

Пусть $|Q| = 2^n$ для некоторого $n \in \mathbb{N}$. Тогда без ограничения общности можно считать, что элементами Q являются двоичные вектора длины n, а функция f представляется в виде $(f_1, \ldots, f_n)$, где f_i — булевы функции от $2n$ переменных $x_1, \ldots, x_n, y_1, \ldots, y_n$. Дополнительно предположим, что функция f имеет вид

$$\begin{array}{rcl} f_1 & = & x_1 \oplus y_1 \oplus g_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \\ f_2 & = & x_2 \oplus y_2 \oplus g_2(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \\ & \vdots & \\ f_n & = & x_n \oplus y_n \oplus g_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)). \end{array} \qquad (*)$$

Здесь $\oplus$ означает сложение по модулю 2, $g_1, \ldots, g_n$ — булевы функции арности n, $\pi_1, \ldots, \pi_n$ — булевы функции арности 2. Связь правильных семейств и квазигрупп устанавливает следующая теорема.

Теорема ([5]). *Соотношения* $(*)$ *задают квазигрупповую операцию для любых функций* $\pi_1, \ldots, \pi_n$ *тогда и только тогда, когда семейство* $(g_1, \ldots, g_n)$ *правильное.*

Из теоремы следует, что одно правильное семейство порядка n порождает 16^n квазигрупп. Некоторые из этих квазигрупп могут совпадать; в частности, если семейство $(g_1, \ldots, g_n)$ состоит только из констант, совпадают все порождаемые квазигруппы. Оказывается, что мощность множества квазигрупп, порождаемых подстановкой всевозможных функций $\pi_1, \ldots, \pi_n$ в соотношения $(*)$, оценивается снизу с помощью функции от мощности образа семейства $(g_1, \ldots, g_n)$.

Теорема. *Пусть* $(g_1, \ldots, g_n)$ *— правильное семейство, вектор-функция* $(g_1, \ldots, g_n)$ *принимает ровно* M *различных значений. Тогда соотношения* $(*)$ *порождают не менее* M^4 *попарно различных квазигрупп.*

Существуют примеры правильных семейств, для которых приведенная оценка является точной.

В. В. Пухкой в своей дипломной работе установил следующий факт.

Теорема. *Пусть* $(g_1, \ldots, g_n)$ *— правильное семейство, образ которого имеет мощность* M*. Тогда* M *удовлетворяет соотношению* $1 \leq M \leq 2^{n-1}$*, и для любого* M *из указанного диапазона существует правильное семейство, мощность образа которого равна* M*.*

Несложно показать, что утверждение теоремы остается верным при замене всех правильных семейств треугольными. При переходе к ортогональным семействам мощность образа, а следовательно и нижняя оценка мощности множества порождаемых квазигрупп резко падает. Действительно, из определения ортогонального семейства вытекает, что в образе могут содержаться только наборы веса ≤ 1. Число таких наборов равно $n + 1$, то есть мощность образа принадлежит множеству $\{1, \ldots, n + 1\}$.

Мы проанализировали число правильных семейств небольшого порядка, имеющих заданные мощности образа. Получились следующие результаты:

- при $n = 2$ четыре семейства имеют мощность образа, равную 1, оставшиеся 8 семейств принимают по два значения;
- при $n = 3$ мощности представлены в следующей таблице:

M	1	2	3	4
число семейств	8	192	384	160

- при $n = 4$ мощности представлены в следующих таблицах:

M	1	2	3	4
число семейств	16	8864	199296	1101960

M	5	6	7	8
число семейств	2062848	1594368	514048	57344

В дальнейшем планируется найти новые примеры правильных семейств, мощность образа которых близка к максимальной, а также обобщить результаты на логики более высокой значности и d-квазигруппы.

Список литературы

1. Shcherbacov V. A. Quasigroups in cryptology // Computer Science Journal of Moldova. — 2009. — Vol. 17, no. 2(50). — P. 193–228.

2. Chauhan D., Gupta I., Verma R. Quasigroups and their applications in cryptography // Cryptologia. — 2021. — Vol. 45, no. 3. — P. 227–265.

3. Galatenko A. V., Nosov V. A., Pankratiev A. E. Latin squares over quasigroups // Lobachevskii Journal of Mathematics. — 2020. — Vol. 41, no. 2. — P. 194–203.

4. Галатенко А. В., Носов В. А., Панкратьев А. Е., Чаплыгина С. С. О числе n-квазигрупп, порождаемых правильным семейством функций // Материалы XXI Международной конференции "Алгебра, теория чисел, дискретная геометрия и многомасштабное моделирование: современные проблемы, приложения и проблемы истории", посвященной 85-летию со дня рождения А. А. Карацубы (17–21 мая 2022 г.). — Тула, 2022. — С. 149–152.

5. Носов В. А. Построение классов латинских квадратов в булевой базе данных // Интеллектуальные системы. — 1999. — Т. 4, вып. 3–4. — С. 307–320.

DOI: 10.20948/dms-2022-80

О СЛОЖНОСТИ ВЫЧИСЛЕНИЙ В ПОЛЯХ $GF(3^n)$

С. Б. Гашков (Москва)

Через L обозначаем сложность вычисления в поле $GF(3)$, измеренную в количестве операций умножения, обозначаемых M, и в количестве операций сложения-вычитания, обозначаемых A. В случае операций над полем $GF(9)$ с базисом $\{1, i\}, i^2 = -1$, сложность, измеренную в операциях над полем $GF(3)$, обозначаем L_C. Сложность умножения многочленов $\deg < n$ над полем $GF(3)$ обозначаем как $M(n)$, а в случае коэффициентов из $GF(9)$ как $M_C(n)$. Для сложности умножения по модулю $x^n \pm 1$ вместо $L(fg \pmod{x^n - 1})$ пишем $L(n)$, вместо $L_C(fg \pmod{x^n - 1})$ — $LC(n)$, вместо $L(fg \pmod{x^n + 1})$ — $L_1(n)$, вместо $L_C(fg \pmod{x^n + 1})$ — $LC_1(n)$.

Для оценки битовой сложности умножения и сложения в поле $GF(3)$ представляем 0 как $(0, 0)$, 1 как $(0, 1)$ и -1 как $(1, 1)$, тогда $A = A(GF(3)) \le 7; M = M(GF(3)) \le 4$. Используя модификацию метода Шенхаге, можно доказать, что

$$LC_1(2) \le 8M + 16A; LC(2) \le 8M + 16A;$$