

Порождение правильных семейств функций

А. В. Галатенко¹, В. А. Носов², А. Е. Панкратьев³,
В. М. Староверов⁴

В работе показано, что задача проверки правильности семейства функций при компактном задании входа является coNP-полной, а также предложены процедуры для порождения множества всех правильных семейств заданного порядка и равномерного распределения на этом множестве.

Ключевые слова: правильные семейства функций, цепи Маркова

1. Введение

Задача порождения семейств квазигрупп, обладающих заданными свойствами, актуальна для криптографических приложений. В криптосистеме с открытым ключом из работы [1] для генерации ключей требуются два семейства многомерных квадратичных квазигрупп порядка 32 , каждое из которых должно иметь мощность не ниже 2^{20} . В. А. Носов предложил породить большие семейства квазигрупп большого порядка с помощью правильных семейств функций [2]. В работе [3] авторы рассмотрели методы для явного порождения больших семейств многомерных квадратичных квазигрупп с заданным значением квадратичности с помощью правильных семейств булевых функций. Для переноса результатов на логики большей значности возникла задача поиска правильных семейств специального вида. Для булева случая известны утверждения

¹ *Галатенко Алексей Владимирович* — старший научный сотрудник каф. MaTIS мех.-мат. ф-та МГУ, e-mail: agalat@msu.ru.

Galatenko Alexei Vladimirovich — senior researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, MaTIS chair

² *Носов Валентин Александрович* — ведущий научный сотрудник каф. MaTIS мех.-мат. ф-та МГУ, e-mail: vnosov40@mail.ru.

Nosov Valentin Aleksandrovich — leading researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, MaTIS chair

³ *Панкратьев Антон Евгеньевич* — доцент каф. MaTIS мех.-мат. ф-та МГУ, e-mail: apankrat@intsys.msu.ru.

Pankratiev Anton Evgenievich — associate professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, MaTIS chair

⁴ *Староверов Владимир Михайлович* — доцент каф. выч. мат. мех.-мат. ф-та МГУ, e-mail: staroverovvl@imscs.msu.ru.

Staroverov Vladimir Mikhailovich — associate professor, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Computational Mathematics

о трудности задачи распознавания правильности (coNP-полнота в случае задания функций схемами [4]) и о скорости роста числа правильных семейств: если $T(n)$ — число правильных семейств булевых функций порядка n , то, как показано в [5], существует положительная константа A , такая что $n^{A2^n} \leq T(n)$. Эти утверждения удалось перенести на случай k -значной логики при $k \geq 3$. Мы также предлагаем алгоритм для построения всех правильных семейств функций k -значной логики порядка n при условии, что получены все правильные семейства порядка $n - 1$ (из неравенства на $T(n)$ следует, что алгоритм допускает практическое применение при небольших значениях n), и МСМС-процедуру для порождения равномерного распределения на множестве всех правильных семейств заданного порядка в логике значности $k \geq 3$ (случай $k = 2$ рассмотрен в работах [6]).

2. Основные понятия и результаты

Пусть $E_k = \{0, 1, \dots, k - 1\}$, P_k^n — множество всех функций k -значной логики от n переменных.

Определение 1. Семейство (f_1, \dots, f_n) , где $n \in \mathbb{N}$, $f_1, \dots, f_n \in P_k^n$, называется правильным, если для любых $\alpha, \beta \in E_k^n$, $\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n)$, $\alpha \neq \beta$, найдется индекс i , $1 \leq i \leq n$, такой что $\alpha_i \neq \beta_i$, но $f_i(\alpha) = f_i(\beta)$.

Очевидным примером правильного семейства является набор константных функций.

Заметим, что правильные семейства булевых функций порядка n могут быть естественным образом инъективно вложены в множество правильных семейств k -значной логики того же порядка. Для этого достаточно рассмотреть функцию $\mu: E_k \rightarrow E_2$, такую что $\mu(x) = 0$ если и только если $x = 0$, и отобразить булево семейство (f_1, \dots, f_n) в семейство (g_1, \dots, g_n) функций k -значной логики, определяемых соотношением $g_i(x_1, \dots, x_n) = f_i(\mu(x_1), \dots, \mu(x_n))$.

Из приведенной конструкции вытекают следующие утверждения.

Теорема 1. Задача проверки, является ли семейство функций k -значной логики, заданное схемой в конечном функционально полном базисе, правильным, coNP-полна.

Теорема 2. Пусть $T_k(n)$ — число правильных семейств функций k -значной логики порядка n , Тогда $T_k(n) > T(n) \geq n^{A2^n}$.

Пусть $F = (f_1, \dots, f_n)$ — правильное семейство функций k -значной логики, $1 \leq i \leq n$, α — последовательность элементов E_k . Рассмотрим преобразование $\text{Switch}(F, i, \alpha)$, возвращающее семейство $F' =$

$(f_1, \dots, f_{i-1}, f'_i, f_{i+1}, \dots, f_n)$, где f'_i определяется следующим образом. По семействам F_j , полученным из F фиксацией $x_i = j$ и отбрасыванием i ой функции, строим граф с множеством вершин E_k^{n-1} с помощью процедуры, описанной в работе [7]. Затем выделяем компоненты связности графа в некотором порядке (например, лексикографическом). Компоненте связности номер m ставим в соответствие m ую компоненту набора α . Пусть $(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n)$ — вершина из компоненты связности номер m , $a \in E_k$. Полагаем $f'_i(a_1, \dots, a_{i-1}, a, a_{i+1}, \dots, a_n) = \alpha_m$.

Рассмотрим следующую процедуру. Всевозможными способами выбираем набор (G_0, \dots, G_{k-1}) правильных семейств порядка n . Определяем функции f_1, \dots, f_n с помощью соотношения $f_i(x_1, \dots, x_n, x_{n+1}) = \bigvee_{j=0}^{k-1} (I_{x_{n+1}}(j) \wedge g_i^j(x_1, \dots, x_n))$, где g_i^j — функция номер i семейства G_j . Полагаем $f_{n+1} \equiv 0$ и выдаем на выход $\text{Switch}((f_1, \dots, f_{n+1}), n+1, \alpha)$ для всевозможных α .

Теорема 3. *Описанная процедура порождает все правильные семейства порядка $n+1$ в k -значной логике.*

Для генерации равномерного распределения на множестве правильных семейств заданного порядка можно воспользоваться цепью Маркова, порожденную следующим методом. Стартуем с правильного семейства, все функции которого есть тождественный 0. На каждом шаге случайно равновероятно выбираем i и α и применяем преобразование Switch к текущему семейству.

Теорема 4. *Множество состояний указанной цепи Маркова совпадает с множеством всех правильных семейств заданного порядка k -значной логики. При числе итераций, стремящемся к бесконечности, имеется сходимость к равномерному распределению на множестве состояний.*

Экспоненциальная по n сложность преобразования является ожидаемой — проверка правильности является сложной задачей.

Список литературы

- [1] Gligoroski D., Markovski S., Knapskog S. J., “Public key block cipher based on multivariate quadratic quasigroups”, Cryptology ePrint Archive, Report 2008/320, 2008, 22 pp.
- [2] Носов В. А., “Построение классов латинских квадратов в булевой базе данных”, *Интеллектуальные системы*, 4:3–4 (1999), 307–320.
- [3] Галатенко А. В., Носов В. А., Панкратьев А. Е., “Порождение квадратных квазигрупп с помощью правильных семейств булевых функций”, *Фундаментальная и прикладная математика*, 23:2 (2020), 57–73.

- [4] Gärtner B., Thomas A., “The complexity of recognizing unique sink orientations”, *Leibniz International Proceedings in Informatics*, **30** (2015), 341–353.
- [5] Matousek J., “The number of unique-sink orientations of the hypercube”, *Combinatorica*, **26** (2006), 91–99.
- [6] Schurr I., *Unique sink orientations of cubes*, Doctoral thesis, ETH Zurich, 2004, 171 с.
- [7] Галатенко А. В., Носов В. А., Панкратьев А. Е., “Об одном алгоритме построения правильных семейств функций”, Материалы XVIII Международной конференции «Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории», 2020, 142–146

Generation of proper families of functions

Galatenko A.V., Nosov V.A., Pankratiev A.E., Staroverov V.M.

We show that the problem of deciding properness of a family of functions specified by a circuit is coNP-complete, and propose procedures for generation of all proper families of a given order and of uniform distribution on the set of proper families.

Keywords: proper families of functions, Markov chains

References

- [1] Gligoroski D., Markovski S., Knapskog S. J., “Public key block cipher based on multivariate quadratic quasigroups”, Cryptology ePrint Archive, Report 2008/320, 2008, 22 pp.
- [2] Nosov V. A., “Construction of classes of Latin squares in Boolean databases”, *Intelligent Systems*, **4:3–4** (1999), 307–320 (In Russian)
- [3] Galatenko A. V., Nosov V. A., Pankratiev A. E., “Generation of multivariate quadratic quasigroups using proper families of Boolean functions”, *Fundamental and Applied Mathematics*, **23:2** (2020), 57–73 (In Russian)
- [4] Gärtner B., Thomas A., “The complexity of recognizing unique sink orientations”, *Leibniz International Proceedings in Informatics*, **30** (2015), 341–353
- [5] Matousek J., “The number of unique-sink orientations of the hypercube”, *Combinatorica*, **26** (2006), 91–99
- [6] Schurr I., *Unique sink orientations of cubes*, Doctoral thesis, ETH Zurich, 2004, 171 pp.
- [7] Galatenko A. V., Nosov V. A., Pankratiev A. E., “An algorithm for construction of proper families of functions”, Proc. 18th Int. Conf. “Algebra, number theory and discrete geometry: modern problems, applications and problems of history“, 2020, 142–146 (In Russian)