

которая берётся из множества $W_{w,r}$ всех таких нетривиальных систем и фиксирована. Максимальная группа подстановок, сохраняющая данную систему импримитивности $W \in W_{w,r}$, есть группа сплетения $IG_W = (S_w \wr S_r, W)$ в её импримитивном действии. Близость между подстановками $g, h \in S_n$ измеряется расстоянием Хемминга $\chi(g, h)$.

В работе рассматриваются два параметра:

- порядок W -примитивности, то есть число

$$\chi_W(g) = \min \{ \chi(g, h) : h \in IG_W \};$$

- порядок (w, r) -примитивности, то есть число

$$\chi_{(w,r)}(g) = \min \{ \chi(g, h) : h \in IG_W, W \in W_{w,r} \}.$$

Если соответствующие параметры больше нуля, то подстановку g будем называть W -примитивной, (w, r) -примитивной; в противном случае — W -импримитивной, (w, r) -импримитивной. При рассмотрении W -примитивности каждой подстановке ставится в соответствие матрица, характеризующая удалённость данной подстановки от группы IG_W . Через коэффициенты данной матрицы получено выражение для $\chi_W(g)$. Описаны классы максимально W -примитивных подстановок, являющихся «бент-подстановками» относительно системы импримитивности. Приведены оценки числа таких подстановок.

Порядок (w, r) -примитивности подстановки $g \in S(X)$ определяется только её цикловой структурой, то есть является функцией на классах сопряжённых элементов в группе $S(X)$. Перечислены цикловые структуры подстановок из множества $IG_{(w,r)} = \bigcup_{W \in W_{(w,r)}} IG_W$. Поскольку множество $IG_{(w,r)}$ является объединением классов сопряжённых элементов группы $S(X)$, то цикловая структура элемента g однозначно характеризует его принадлежность множеству $IG_{(w,r)}$. В целом задача нахождения порядка (w, r) -примитивности оказалась сложнее. Получены порядки (w, r) -примитивности при чётном n в крайних случаях $w = 2$ и $r = 2$.

Исходя из общего подхода, получены порядки (w, r) -примитивности для s -боксов криптосистем AES, ARIA, Whirlpool, MISTY1, Camellia, FOX.

УДК 519.14

О СОВЕРШЕННЫХ 2-РАСКРАСКАХ q -ЗНАЧНОГО ГИПЕРКУБА¹

В. Н. Потапов

Обозначим через Z_q множество $\{0, \dots, q-1\}$. Декартово произведение Z_q^n называется q -значным n -мерным кубом (гиперкубом). Функция $f : Z_q^n \rightarrow Z_q$ называется *корреляционно-иммунной порядка $n - t$* , если мощность пересечения грани размерности t с множеством $f^{-1}(a)$ зависит только от $a \in Z_q$. Через $\text{cor}(f)$ будем обозначать максимальный порядок корреляционной иммунности. *Плотностью* булевозначной функции χ^S будем называть отношение $\rho(S) = |S|/q^n$. Если $\rho(S) = 1/2$, то булевозначную корреляционно-иммунную функцию χ^S называют *уравновешенной*.

¹Работа выполнена при поддержке РФФИ (проекты №10-01-00424, 10-01-00616) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт №02.740.11.0429).

Расстоянием Хэмминга $d(x, y)$ между вершинами $x = (x_1, x_2, \dots, x_n)$ и $y = (y_1, y_2, \dots, y_n)$ называется число позиций, в которых наборы x и y различаются. Определим величину $A(S)$ как среднее число вершин из $S \subseteq Z_q^n$, которые находятся на расстоянии 1 от вершины из дополнения $Z_q^n \setminus S$, т.е. $A(S) = \frac{1}{q^n - |S|} \sum_{x \notin S} |\{y \in S : d(x, y) = 1\}|$.

Отображение $\text{col} : Z_q^n \rightarrow \{0, \dots, k\}$ называется *совершенной раскраской* с матрицей параметров $M = \{m_{ij}\}$, если для любых i и j , для каждой вершины цвета i число соседей цвета j равняется m_{ij} . В дальнейшем рассматриваются только раскраски в два цвета (2-раскраски). Будем считать, что $\{0, 1\}$ — множество цветов. В этом случае булевозначная функция col является характеристической функцией множества вершин цвета 1.

Совершенный код (исправляющий одну ошибку) $C \subset Z_q^n$ можно рассматривать как множество единиц совершенной 2-раскраски с матрицей параметров $M = \begin{pmatrix} n(q-1)-1 & 1 \\ n(q-1) & 0 \end{pmatrix}$. Если число q является степенью простого числа, то раскраска с такими параметрами существует только при $n = (q^j - 1)/(q - 1)$. При $q = 2$ список известных параметров совершенных 2-раскрасок имеется в [1, 2].

Известно (см., например, [3, 4]), что совершенная раскраска булева n -куба с матрицей параметров $\begin{pmatrix} n-b & b \\ c & n-c \end{pmatrix}$ является корреляционно-иммунной функцией порядка $(b+c)/2 - 1$, т.е. из регулярной распределённости вершин некоторого множества по шарам радиуса 1 следует равномерное распределение вершин этого множества по граням. Весьма интересным представляется выяснение возможности обратного следствия.

В [5] доказано, что если для некоторого множества $S \subset Z_2^n$ величины $\text{cor}(\chi^S)$ и $\rho(S)$ совпадают с соответствующими параметрами для совершенного кода, то множество S является совершенным кодом. В [3] установлено, что неуравновешенная булева функция $f = \chi^S$ ($S \subset Z_2^n$) удовлетворяет неравенству $\text{cor}(f) \leq 2n/3 - 1$. Кроме того, в случае равенства $\text{cor}(f) = 2n/3 - 1$ функция f является совершенной раскраской. Подобным образом, если для множества $S \subset Z_2^n$ неравенство Биербрауэра — Фридмана (см. [6, 7]) превращается в равенство $\rho(S) = 1 - \frac{n}{2(\text{cor}(f) + 1)}$, то функция χ^S является совершенной 2-раскраской [8].

Оказывается, имеет место следующий критерий.

Теорема 1.

- Для каждой булевозначной функции $f = \chi^S$, где $S \subset Z_q^n$, справедливо неравенство $\rho(S)q(\text{cor}(f) + 1) \leq A(S)$.
- Булевозначная функция $f = \chi^S$ является совершенной 2-раскраской тогда и только тогда, когда $\rho(S)q(\text{cor}(f) + 1) = A(S)$.

Таким образом, равномерное распределение вершин множества по граням гиперкуба при экстремальных условиях на плотность множества влечёт регулярное распределение вершин множества по шарам. Более того, любая совершенная 2-раскраска получается как максимально равномерно распределённая по граням булевозначная функция при некоторых дополнительных односторонних ограничениях на размещение её единиц. При доказательстве теоремы использовались методы, развитые в [7].

ЛИТЕРАТУРА

1. *Fon-Der-Flaass D. G.* Perfect 2-colorings of a hypercube // *Siber. Math. J.* 2007. V. 48. No. 4. P. 740–745.
2. *Фон-Дер-Флаасс Д. Г.* Совершенные 2-раскраски 12-мерного куба, достигающие границы корреляционной иммунности // *Сибирские электронные математические известия.* 2007. Т. 4. С. 292–295.
3. *Fon-Der-Flaass D. G.* A bound of correlation immunity // *Siber. Electron. Math. Rep.* 2007. V. 4. P. 133–135.
4. *Таранников Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях // *Математические вопросы кибернетики.* Вып. 11. М.: Физматлит, 2002. С. 91–148.
5. *Ostergard P. R. J., Pottanen O., and Phelps K. T.* The perfect binary one-error-correcting codes of length 15: Part II-Properties // *IEEE Trans. Inform. Theory.* 2010. V. 56. P. 2571–2582.
6. *Friedman J.* On the bit extraction problem // *Proc. 33rd IEEE Symposium on Foundations of Computer Science.* 1992. P. 314–319.
7. *Bierbrauer J.* Bounds on orthogonal arrays and resilient functions // *J. Combinat. Designs.* 1995. V. 3. P. 179–183.
8. *Потанов В. Н.* О совершенных раскрасках булева n -куба и корреляционно-иммунных функциях малой плотности // *Сибирские электронные математические известия.* 2010. Т. 7. С. 372–382.

УДК 519.6

АЛГЕБРЫ ЯЗЫКОВ,
АССОЦИИРОВАННЫЕ С ОТМЕЧЕННЫМИ ГРАФАМИ

Е. А. Пряничникова

В теории конечных автоматов одним из важнейших результатов является теорема Клини, в которой утверждается, что класс языков, распознаваемых конечными автоматами, совпадает с классом рациональных языков, представимых регулярными выражениями алгебры Клини [1].

В данной работе определяется понятие языка, допустимого в отмеченном графе, вводится система операций на формальных языках, которая, в частности, может использоваться в биологии, генетике, а также ДНК-вычислениях [2], и понятие регулярных выражений для этой системы операций.

Исследованы основные свойства семейства алгебр языков, допустимых в отмеченных графах; доказано, что язык допустим в отмеченном графе тогда и только тогда, когда он описывается регулярным выражением во введенной системе операций; разработаны методы анализа и синтеза языков, ассоциированных с отмеченными графами.

Пусть X — конечный алфавит; X^* — множество всех слов конечной длины в алфавите X ; X^n — множество всех слов длины n в алфавите X ; $X^{\geq n}$ — множество всех слов конечной длины в алфавите X , длина которых больше или равна n .

Определим на множестве X^* частичную бинарную операцию $\overset{n}{\circ}$ склеивания двух слов с параметром n следующим образом: для всех $w_1, w_2 \in X^*$

$$w_1 \overset{n}{\circ} w_2 = \begin{cases} xyz, & \text{если } w_1 = xy, w_2 = yz, y \in X^n; \\ \text{не определено} & \text{в противном случае.} \end{cases}$$

Введем на языках $L, R \subseteq X^*$ следующие операции:

- 1) $L \cup R = \{w : w \in L \text{ или } w \in R\};$