МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Приложение

№4 Сентябрь 2011

Свидетельство о регистрации: ПИ №ФС 77-33762
от 16 октября 2008 г.

ТЕЗИСЫ ДОКЛАДОВ

X Сибирской научной школы-семинара с международным участием
«Компьютерная безопасность и криптография» — SIBECRYPT'11
(Томск, ТГУ, 5–10 сентября 2011 г.)

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

СОДЕРЖАНИЕ

Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Секция 2

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

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. *Тарасников 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., Pottonen 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. *Потапов 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; $X^{\geqslant n}$ — 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) $L \cup R = \{w : w \in L \text{ или } w \in R\}$;

2) $L \overset{n}{\circ} R = \{w_1 \overset{n}{\circ} w_2 : w_1 \in L \text{ и } w_2 \in R\}$;

3) $L^{\overset{n}{+}} = \bigcup\limits_{i=1}^{\infty} L^i$, где $L^1 = L$; $L^{i+1} = L^i \overset{n}{\circ} L$ для всех $i \geqslant 1$.

Рассмотрим семейство алгебр $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$. В случае, когда $n = 0$, операция $\overset{n}{\circ}$ совпадает с операцией конкатенации, а рассматриваемая алгебра является алгеброй регулярных языков.

Регулярные выражения в алгебре $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$ определим следующим образом:

1) $\varnothing$ является регулярным выражением и представляет язык $L(\varnothing) = \varnothing$;
2) x является регулярным выражением и представляет язык $L(x) = \{x\}$ для всех $x \in \bigcup\limits_{0 \leqslant i \leqslant n+1} X^i$;
3) если R и Q — регулярные выражения, представляющие языки $L(R)$ и $L(Q)$ соответственно, то выражения $(R \overset{n}{\circ} Q)$, $(R \cup Q)$, $(R^{\overset{n}{+}})$ также являются регулярными, причем $L(R \overset{n}{\circ} Q) = L(R) \overset{n}{\circ} L(Q)$, $L(R \cup Q) = L(R) \cup L(Q)$, $L(R^{\overset{n}{+}}) = (L(R))^{\overset{n}{+}}$.

Графом с отмеченными дугами (вершинами) назовем четверку $G = (Q, E, X, \mu)$, где Q — конечное множество вершин; $E \subseteq Q \times Q$ — множество дуг; X — конечное множество отметок дуг; $\mu : E \to X$ ($\mu : Q \to X$) — функция отметок дуг (вершин). Отметкой пути будем называть последовательность отметок входящих в этот путь дуг (вершин).

Пусть $I \subseteq Q$ — множество начальных вершин графа G с отмеченными дугами или с отмеченными вершинами, $F \subseteq Q$ — множество финальных вершин. Отметки всех путей в графе G, начальные вершины которых принадлежат множеству I, а конечные — множеству F, назовем языком, допускаемым графом G, и обозначим $L(G)$.

Теорема 1. Язык $L \subseteq X^*$ допустим в графе с отмеченными дугами (вершинами) тогда и только тогда, когда он описывается регулярным выражением любой алгебры из семейства $(2^{X^*}, \overset{n}{\circ}, \cup, \overset{n}{+}, \varnothing)$.

Эта теорема в некотором смысле аналогична широко известной теореме Клини для конечных автоматов. В случае, когда $n = 0$ и рассматриваются только графы с отмеченными дугами, теорема 1 совпадает с теоремой Клини. На основе доказательства теоремы разработаны методы анализа и синтеза языков, представимых в отмеченных графах.

ЛИТЕРАТУРА

1. *Капитонова Ю. В., Летичевский А. А.* Математическая теория проектирования вычислительных систем. М.: Наука, 1988.
2. *Anderson J.* Automata Theory with Modern Applications. Cambridge: Cambridge University Press, 2006.

УДК 519.7

ГИПОТЕЗЫ О ЧИСЛЕ БЕНТ-ФУНКЦИЙ[1]

Н. Н. Токарева

Проблема определения числа всех *бент-функций* — булевых функций от четного числа переменных, максимально удаленных от множества аффинных функций, — яв-

[1]Исследование выполнено при поддержке РФФИ (проекты №09-01-00528, 10-01-00424, 11-01-00997) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт №02.740.11.0429).