№ п/п	Тип	Функция
1	1 1 1 1 1 1	100000000100001 (iter1)
2	2 2 1 1 1 1	100001000100001 (iter1)
3	2 2 2 2 1 1	100001000100101 (iter2)
4	3 2 2 1 1 1	100001001001100 (iter1) 100001001100001 (iter3)
5	3 2 2 2 2 1	100001001100101 100001000010111
6	3 3 2 2 1 1	100001001110001 (iter1) 100001000110101 (iter2)
7	3 3 2 2 2 2	011001011100001 101101001100001
8	3 3 3 1 1 1	100001010110001 (iter2)
9	3 3 3 2 2 1	100001001100111 (iter2) 100001001110101 100001001100111
10	3 3 3 3 1 1	100001010110110 (iter2) 111001100100001 (iter1) 111000000110101 (iter1)
11	3 3 3 3 2 2	110011100100101 110101001100101 111001001100101 101101001100101
12	4 2 2 2 1 1	100001101100001 (iter3)
13	4 3 2 2 2 1	100001101100101 100001100100111
14	4 3 3 2 1 1	100001101100011
15	4 3 3 2 2 2	111011000100101
16	4 3 3 3 2 1	111100001110100 (iter3)
17	4 3 3 3 3 2	110011000110111
18	4 4 3 2 2 1	100001101100111
19	4 4 3 3 1 1	100001101101110 (iter2)
20	4 4 3 3 2 2	110001011110011
21	4 4 3 3 3 1	100001100111111
22	4 4 3 3 3 3	111011001110101
23	4 4 4 3 3 2	011101001110111
24	4 4 4 4 3 1	100001101111111
25	4 4 4 4 3 3	111001100010111 110101101100111
26	5 2 2 2 2 1	100001111100001
27	5 3 3 2 2 1	100001111100101
28	5 3 3 3 2 2	110001000111111
29	5 3 3 3 3 3	110101001111110
30	5 4 3 3 2 1	100001111111100
31	5 4 4 3 2 2	110111000111101
32	5 4 4 4 3 2	111101000111111
33	5 4 4 4 4 1	100001111111111
34	5 5 3 3 3 3	111001100111111
35	5 5 4 4 3 3	111001111111011
36	5 5 5 4 4 3	111101111111110
37	5 5 5 5 5 5	111111111111111

Поясним обозначения. Конструкция iter1 означает, что к бент-функции от четырёх переменных добавляется слагаемое x_5x_6; iter2 — слагаемое $x_ix_5 \oplus x_jx_6$, где $i, j \in \in \{1, 2, 3, 4\}$; iter3 — слагаемое $x_ix_5 \oplus x_5x_6$, где $i \in \{1, 2, 3, 4\}$. Пример: АНФ функции, заданной вектором 100001101100011, имеет вид $x_1x_2 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_4x_6 \oplus \oplus x_5x_6$. Данное исследование помогает выявить общие закономерности построения бент-функций от $(n + 2)$ переменных с помощью бент-функций от n переменных.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.

УДК 519.7

СЛАБОЦЕНТРАЛЬНЫЕ КЛОНЫ И ПРОБЛЕМА ПОЛНОТЫ В НИХ[1]

Н. Г. Парватов

Проблема полноты и критериальные системы. Пусть E — конечное множество. Через P_E обозначается множество функций $f : E^n \to E$ при всевозможных целых положительных n. Классы таких функций, замкнутые операциями суперпозции и

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).

содержащие селекторные функции, называются *клонами*, а клоны, включающие множество $A \subseteq P_E$, — *A-клонами*.

Будем интересоваться *проблемой полноты в A-клоне* (иначе — проблемой A-полноты в клоне) B, состоящей в описании всех его *A-порождающих подмножеств*, порождающих его с использованием операций суперпозиции, селекторов и функций из множества A. Инструментом решения этой проблемы является *A-критериальная* система. Так называется система $\mathcal{S}$ A-клонов, собственным образом содержащихся в клоне B, если всякий A-клон, собственным образом содержащийся в клоне B, можно расширить до некоторого клона из $\mathcal{S}$. A-критериальная система $\mathcal{S}$ называется *безызбыточной*, если она не содержит пары сравнимых по включению клонов и совпадает тогда с системой $\mathcal{S}(A, B)$ всех максимальных A-клонов среди строго содержащихся в B, в остальных случаях лишь включённой в $\mathcal{S}$.

Обозначим через Π_E множество предикатов $p : E^n \to \{\text{И,Л}\}$ при всевозможных натуральных n. Неинвариантный для клона B предикат p из Π_E называется *B-предельным* [1], если всякий отличный от p предикат, полученный из него проектированием, отождествлением переменных, B-сужением (пересечением с инвариантным для B предикатом) или симметризацией (пересечением с перестановочно эквивалентным предикатом), ужé инвариантен для клона B. Обозначим через $\Lambda(A, B)$ множество инвариантных для A B-предельных предикатов и через $\tilde{\Lambda}(A, B)$ — множество клонов $B \cap \mathrm{pol}_E(p)$, где $p \in \Lambda(A, B)$. В [1] доказана

Теорема 1. Система $\tilde{\Lambda}(A, B)$ является A-критериальной для клона B. Эта система конечная, если клон B обладает конечным A-порождающим подмножеством.

Заметим, что теорема 1 не исключает возможной избыточности системы $\tilde{\Lambda}(A, B)$.

Слабоцентральные клоны. Пусть c — некоторый элемент из множества E. Предикат p из Π_E назовём *c-слабоцентральным*, если в любом удовлетворяющем ему наборе замена любой компоненты значением c приводит к набору, также удовлетворяющему p. Для любого множества Y *c-слабоцентральных* предикатов из Π_E клон $\mathrm{pol}_E(Y)$ также называется *c-слабоцентральным*. Иными словами, произвольный клон является *c-слабоцентральным*, если он включает (наименьший по включению) клон $\mathrm{pol}_E(W_E^c)$, описываемый множеством W_E^c всех *c-слабоцентральных* предикатов. (Интересно, что это множество замкнуто операциями проектирования, подстановки переменных, конъюнкции и даже дизъюнкции, но не содержит диагоналей, кроме тривиальных.) В двоичном случае такими наименьшими клонами $\mathrm{pol}_E(W_E^c)$ при различных c из множества $E = \{0, 1\}$ являются клоны неразделённых либо разделённых булевых функций. Слабоцентральные клоны обладают рядом интересных свойств и допускают ряд равносильных определений.

Частным случаем слабоцентральных клонов являются определяемые ниже клоны сохранения c-системы множеств. Назовём c-системой систему $\tilde{\varepsilon}$ подмножеств множества E, обладающую следующими свойствами:

1) наследственностью: если некоторое множество принадлежит системе $\tilde{\varepsilon}$, то и всякая его часть принадлежит $\tilde{\varepsilon}$;
2) слабой центральностью по c: если множество H принадлежит системе $\tilde{\varepsilon}$, то множество $H \cup \{c\}$ также принадлежит ей.

Обозначим через $Q_E(\varepsilon)$ клон функций из P_E, сохраняющих систему ε, и через $\Phi_E(\varepsilon)$ — клон функций, сохраняющих её по некоторой переменной. Несложно понять, что клоны $Q_E(\varepsilon)$ и $\Phi_E(\varepsilon)$ являются c-слабоцентральными.

Введённые клоны имеют важные приложения, отметим следующие два.

Пример 1. Пусть E — конечная верхняя полурешётка и ε — система её подмножеств с нижней гранью. Тогда клон $Q_E(\tilde{\varepsilon})$ совпадает с клоном квазимонотонных функций на полурешётке E, введённых Г. П. Агибаловым [2], а клон $\Phi_E(\tilde{\varepsilon})$ совпадает с клоном слабосущественных квазимонотонных функций из [3].

Пример 2. Как клон сохранения некоторой c-системы можно определить любой (предполный по теореме Розенберга) клон функций из P_E, сохраняющих произвольный отличный от диагонали центральный вполне рефлексивный симметричный предикат.

Проблема полноты в слабоцентральном клоне. Из-за указанных приложений слабоцентральных клонов представляется важной проблема полноты в них.

Теорема 2. Пусть A и B — *c-слабоцентральные* клоны, такие, что $A \subseteq B$. Тогда множество $\tilde{\Lambda}(A, B)$ является безызбыточной A-критериальной системой для клона B; в частности, для произвольных предикатов p и q из $\Lambda(A, B)$ строгое включение $B \cap \mathrm{pol}_E(p) \subset B \cap \mathrm{pol}_E(q)$ невозможно. Более того, для произвольных предикатов p и q из $\Lambda(A, B)$ равенство клонов $B \cap \mathrm{pol}_E(p) = B \cap \mathrm{pol}_E(q)$ равносильно перестановочной эквивалентности этих предикатов.

Сформулированная теорема сводит задачу построения безызбыточной A-критериальной системы в клоне B для слабоцентральных клонов A и B к нахождению B-предельных предикатов из $\Lambda(A, B)$. Помимо этого, имеет место

Следствие 1. Слабоцентральный клон обладает безызбыточной критериальной системой.

Отметим также, что доказанная в [3] теорема легко обобщается как теорема о $\Phi_E(\varepsilon)$-полноте в клоне $Q_E(\varepsilon)$ для произвольной c-системы $\tilde{\varepsilon}$.

ЛИТЕРАТУРА

1. *Парватов Н. Г.* О выделении максимальных подклонов // Прикладная дискретная математика. 2011. № 1. С. 14–25.
2. *Агибалов Г. П.* Дискретные автоматы на полурешётках. Томск: Изд-во Том. ун-та, 1993. 227 с.
3. *Парватов Н. Г.* Теорема о функциональной полноте в классе квазимонотонных функций на конечной полурешётке // Дискр. анализ и исслед. опер. Сер. 1. 2006. Т. 13. № 3. С. 62–82.

УДК 519.7

ОПИСАНИЕ КЛАССА ПОДСТАНОВОК, ПРЕДСТАВИМЫХ В ВИДЕ ПРОИЗВЕДЕНИЯ ДВУХ ПОДСТАНОВОК С ФИКСИРОВАННЫМ ЧИСЛОМ МОБИЛЬНЫХ ТОЧЕК

А. Б. Пичкур

Пусть S_N — группа подстановок степени N; $G \in S_N$; $\Gamma(G) \subseteq \{1, \ldots, N\}$ — множество мобильных точек подстановки G; $2 \leqslant q \leqslant N$; $\Gamma_N(q) = \{G \in S_N : |\Gamma(G)| = q\}$ — множество всех подстановок степени N, имеющих ровно q мобильных точек.

В данной работе описано множество всех подстановок из $\Gamma_N(q) \cdot \Gamma_N(q)$. Данный результат имеет практические приложения в криптографии.

В научной литературе рассматривается схожая задача описания множества подстановок, принадлежащих произведению двух или более классов сопряженных элементов из S_N (или из A_N — знакопеременной группы подстановок) [1 – 6].

Доказаны следующие результаты.