2-неотличимое состояние $s' \in S_B$, и обратно, для любого состояния $s' \in S_B$ существует 2-неотличимое состояние $s \in S_A$. Непосредственно из определения неотличимости следует, что $A \overset{2}{\approx} B$. □

Автору представляется весьма перспективным изучение аффинных классов автоматных кривых с целью исследования неотличимости автоматов.

УДК 512.532

П. М. Хрусталев

О ПРЕОБРАЗОВАНИЯХ БУЛЕВЫХ ФУНКЦИЙ

В данной работе исследуется один класс взаимно-однозначных отображений на множестве булевых функций n переменных. Доказывается, что этот класс образует группу относительно композиции, мощность которого равна 2^n. Показывается, что отображения класса сохраняют линейность и самодвойственность булевых функций, а также сохраняют их нелинейность и несамодвойственность. Исследуются ядра отображений класса.

Замена аргумента x_i в булевой функции его отрицанием $\bar{x}_i$ в общем случае изменяет функцию, т.е. $g(x_1,...,x_i,...,x_n) = f(x_1,...,\bar{x}_i,...,x_n) \neq f(x_1,...,x_i,...,x_n)$

Выбор i-го аргумента x_i $(1 \le i \le n)$ определяет отображение $Q_i : F_n \to F_n$ на множестве F_n n таких отображений:

$$f(x_1, \dots, x_n) \xrightarrow{Q_1} f(\bar{x}_1, \dots, x_n),$$

$$\dots$$

$$f(x_1, \dots, x_n) \xrightarrow{Q_n} f(x_1, \dots, \bar{x}_n).$$

Функции Q_i $(f(x_1,\dots,x_i,...,x_n)) = f(x_1,...,\bar{x}_i,...,x_n)$, $1 \le i \le n$, построены из функций $f(x_1,...,x_n)$ и, следовательно, сохраняют некоторые свойства последней, иными словами, являются ее приближенными "копиями" (проекциями).

По такой же схеме из полученных функций построим новые:
$Q_j(Q_i(f(x_1,...,x_i,...,x_n))) = f(x_1,...,\bar{x}_i,...,\bar{x}_j,...,x_n)$, и так далее.

Целью данной статьи является исследование класса всех отображений на множестве F_n, порожденных отображениями $Q_1,...,Q_n$ с помощью суперпозиции S.

Для исследования удобен алгебраический подход и другая индексация базовых (порождающих) отображений.

Базовые отображения $Q_1,...,Q_n$ будем обозначать $Q_{(0,1,...,1)},...,Q_{(1,...,1,0)}$ соответственно, элементы класса - $Q_{(\alpha_1,...,\alpha_n)}$, где $\alpha_i \in \{0,1\}$, $1 \le i \le n$, а суперпозицию $S(Q_{(\beta_1,...,\beta_n)}, Q_{(\alpha_1,...,\alpha_n)}) = Q_{(\gamma_1,...,\gamma_n)}$ заменим операцией $\circ$, где $Q_{(\alpha_1,...,\alpha_n)} \circ Q_{(\beta_1,...,\beta_n)} = Q_{(\gamma_1,...,\gamma_n)}$.

Введя обозначения $x = (x_1,...,x_n)$, $\alpha = (\alpha_1,...,\alpha_n)$, $\beta = (\beta_1,...,\beta_n)$, $\gamma = (\gamma_1,...,\gamma_n)$, $x^\alpha = \left(x_1^{\alpha_1},...,x_n^{\alpha_n}\right) = (x_1 \leftrightarrow \alpha_1,..,x_n \leftrightarrow \alpha_n)$, исследуем класс $\left\{Q_\alpha \mid \alpha \in \{0,1\}^n\right\}$, где $Q_\alpha(f(x)) = f\left(x^\alpha\right)$, $(Q_\alpha \circ Q_\beta)(f) = Q_\beta(Q_\alpha(f))$.

УТВЕРЖДЕНИЕ 1. Класс $\{Q_\alpha\}$ является собственным подклассом класса всех отображений $\{\varphi_k\}$ на множестве F_n.

Доказательство. $|\{\alpha\}| = 2^n$, $|\{k\}| = m^m$, где $m = 2^{2^n}$. Поэтому $\{Q_\alpha\} \subset \{\varphi_k\}$. □

Следствие 1. Мощность класса $\left\{Q_\alpha \mid \alpha \in \{0,1\}^n\right\}$ равна 2^n. □

ТЕОРЕМА 1. Класс $\{Q_\alpha\}$ всех обращений аргументов является группой относительно композиции $\circ$.

Доказательство. Согласно определению, отображения Q_α всюду определены на множестве F_n.

Покажем, что класс $\{Q_\alpha\}$ замкнут относительно композиции $\circ$.

$$(Q_\alpha \circ Q_\beta)(f(x)) = Q_\beta(Q_\alpha(f(x))) = Q_\beta\left(Q_\alpha\left(f\left(x^\alpha\right)\right)\right) = f\left(\left(x^\alpha\right)^\beta\right) = f\left(x^\gamma\right) = Q_\gamma(f(x)),$$

где $\gamma = \alpha \leftrightarrow \beta = \alpha^\beta$, $\alpha,\beta,\gamma \in \{0,1\}^n$.

Но так как множество всех двоичных векторов замкнуто относительно операции эквиваленции, т.е. $\gamma = \alpha \leftrightarrow \beta \in \{0,1\}^n$, то класс $\{Q_\alpha\}$, $\alpha \in \{0,1\}^n$, замкнут относительно композиции $\circ$.

Операция $\circ$ на множестве $\{Q_\alpha\}$ - ассоциативна, поскольку верно, что $Q_\alpha \circ (Q_\beta \circ Q_\gamma) = (Q_\alpha \circ Q_\beta) \circ Q_\gamma$, так как $\alpha \leftrightarrow (\beta \leftrightarrow \gamma) = (\alpha \leftrightarrow \beta) \leftrightarrow \gamma$.

Операция $\circ$ на множестве $\{Q_\alpha\}$ - коммутативна, потому что $Q_\alpha \circ Q_\beta = Q_{(\alpha \leftrightarrow \beta)} = Q_\beta \circ Q_\alpha$.

Следовательно, $(\{Q_\alpha\}, \circ)$ является абелевой полугруппой.

Элемент $Q_1 = Q_{(1,...,1)}$ относительно $\circ$ является нейтральным элементом, так как $Q_\alpha \circ Q_1 = Q_1 \circ Q_\alpha = Q_\alpha$ верно для любого $\alpha \in \{0,1\}^n$, поскольку $\alpha^1 = \alpha \leftrightarrow 1 = 1 \leftrightarrow \alpha = \alpha$, где $\alpha \leftrightarrow 1 = (\alpha_1,...,\alpha_n) \circ (1,...,1) = (\alpha_1 \leftrightarrow 1,...,\alpha_n \leftrightarrow 1)$.

Для каждого элемента Q_α полугруппы $\{Q_\alpha\}$ с единицей Q_1 существует обратный элемент $Q_\alpha^{-1} = Q_\alpha$, ибо $Q_\alpha \circ Q_\alpha = Q_{(\alpha \leftrightarrow \alpha)} = Q_1$.

Таким образом, $(\{Q_\alpha\}, \circ)$ - группа. □

Следствие 2. Если $Q_\alpha \circ Q_\beta = Q_\gamma$, то $Q_\alpha = Q_\beta \circ Q_\gamma$ и $Q_\beta = Q_\alpha \circ Q_\gamma$, где $\gamma = \alpha \leftrightarrow \beta$, $\alpha = \beta \leftrightarrow \gamma$, $\beta = \alpha \leftrightarrow \gamma$.

Справедливость этого утверждения обусловлена тем, что в группах разрешимы уравнения:

$$\begin{cases} a \circ u = c, u = a^{-1} \circ c; \\ v \circ b = c, v = c \circ b^{-1} \end{cases}. \square$$

ТЕОРЕМА 2. Класс линейных функций замкнут относительно любого преобразования из группы $\{Q_\alpha\}$.

Доказательство. Пусть $f(x_1,...,x_n) \in F_n$ - линейная функция, а значит она представима в виде $f(x_1,...,x_n) = a_0 \oplus a_1 x_1 \oplus ... \oplus a_n x_n$.

Тогда функция $Q_\alpha(f(x)) = Q_{(\alpha_1,...,\alpha_n)}(f(x_1,...,x_n)) = f\left(x_1^{\alpha_1},...,x_n^{\alpha_n}\right) =$ $a_0 \oplus a_1(x_1 \oplus \alpha_1 \oplus 1) \oplus ... \oplus a_n(x_n \oplus \alpha_n \oplus 1) = f(x) \oplus c$ есть линейная функция. $\square$

Следствие 3. Класс нелинейных функций замкнут относительно любого преобразования Q_α

Справедливость этого утверждения вытекает из теоремы 2, с учётом взаимной однозначности отображения Q_α.

ТЕОРЕМА 3. Класс самодвойственных функций замкнут относительно любого отображения Q_α.

Доказательство. Если $f(x_1,...,x_n)$ - самодвойственная функция, то $f(x_1, \ldots, x_n) = \bar{f}(\bar{x}_1,...,\bar{x}_n)$. Тогда функция $g(x_1, \ldots, x_n) = Q_\alpha(f(x_1,..., x_n)) =$ $= f(x_1^{\alpha_1},..., x_n^{\alpha_n})$ является самодвойственной, так как $f(x_1^{\alpha_1},..., x_n^{\alpha_n}) =$ $\bar{f}(x_1^{\bar{\alpha}_1},..., x_n^{\bar{\alpha}_n}) = \bar{f}(\bar{x}_1^{\alpha_1},..., \bar{x}_n^{\alpha_n})$.

Из теоремы 3, учитывая, что Q_α - взаимно однозначно, следует, что любая самодвойственная функция имеет образ при отображении Q_α, который не может быть несамодвойственной функцией. Однако Q_α является своим обращением относительно операции $\circ$ (теорема 1). Поэтому образом несамодвойственной функции не может быть самодвойственная функция. Таким образом, имеем:

Следствие 4. Класс несамодвойственных функций замкнут относительно любой операции Q_α обращения аргументов. $\square$

Отображениями Q_α на множестве F_n порождаются ядерные эквивалентности $\varepsilon_\alpha = \mathrm{Ker} Q_\alpha$: $f \varepsilon_\alpha g \Leftrightarrow Q_\alpha(f) = Q_\alpha(g)$.

Из того, что $Q_\alpha : F_n \to F_n$ является взаимно-однозначным отображением, следует, что $(\forall \alpha, \beta)(\varepsilon_\alpha = \varepsilon_\beta = \varepsilon_0)$, где ε_0 - тождественная эквивалентность: $\varepsilon_0 \subseteq F_n^2$, причем $f \varepsilon_0 g \Leftrightarrow f = g$.

Таким образом, классы соответствующего ε_0 разбиения $R_0 = \{\{f\} \mid f \in F_n\}$ являются одноэлементными множествами, число которых равно 2^{2^n}. $\square$