Серия «Математика»
2009. Т. 2, № 2, С. 40—55

Онлайн-доступ к журналу:
http://isu.ru/izvestia

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 519.716.322

Перечисление операторных классов булевых функций *

С. Ф. Винокуров
Восточно-Сибирская государственная академия образования

А. С. Казимиров
Восточно-Сибирская государственная академия образования

Аннотация. Работа посвящена задаче классификации булевых функций. Классификация производится по группе преобразований, являющейся расширением группы инвертирования переменных. Такие преобразования представляют интерес в связи с тем, что сохраняют сложность (количество слагаемых) полиномов, представляющих булевы функции. Группа этих преобразований описана с использованием операторного языка и названа группой операторных преобразований. Для нее решена задача перечисления — одна из подзадач классификации, заключающаяся в нахождении числа классов эквивалентности.

Ключевые слова: булева функция; полиномиальная форма; операторы; специальная операторная форма; классификация по группе преобразований.

Быстрый рост числа булевых функций при увеличении числа переменных приводит к необходимости объединения функций, обладающих некоторым свойством, в классы. В качестве таких классов могут выступать классы эквивалентности относительно групп преобразований. Задача построения полной классификации состоит в нахождении классов эквивалентности (или их представителей) относительно таких групп.

В настоящее время задача построения классификаций булевых функций по различным группам преобразований имеет широкие приложения — от задач логического синтеза до криптографии. Имеется большое количество результатов по группам аффинных преобразований булевых функций и их обобщениям [1,2].

Одним из способов задания булевых функций является полиномиальное представление — в виде суммы по модулю 2 произведений переменных или их отрицаний. При исследовании полиномиальных представлений интересны преобразования, которые сохраняют сложность

* Работа выполнена при финансовой поддержке РФФИ, грант 09-01-00476-а.

(количество слагаемых) полинома. Можно заметить, что аффинные преобразования в общем случае не сохраняют сложность полиномов.

В работе рассматривается группа, являющаяся расширением группы инвертирования переменных и сохраняющая сложность полиномов. Эта группа описана с использованием операторного языка и названа группой операторных преобразований. Для нее решена задача перечисления — одна из подзадач классификации, заключающаяся в нахождении числа классов эквивалентности.

Для обозначения функции $f(x_1, \ldots, x_n)$ в тексте используется запись $f(\tilde{x})$ или f. Наряду с термальным представлением в работе использовано представление функции f в виде вектора $(f_0, \ldots, f_{2^n-1})$, где $f_k = f(\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in \{0, 1\}$, $k = \alpha_1 \cdot 2^{n-1} + \ldots + \alpha_n \cdot 2^0$.

Символами $f^0_{x_i}, f^1_{x_i}, f'_{x_i}$ обозначаются нулевая и единичная остаточные и производная функции f по переменной x_i. Остаточные определяются подстановками констант:

$$f^0_{x_i} = f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n), \;\; f^1_{x_i} = f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n),$$

а производная задается следующим выражением: $f'_{x_i} = f^0_{x_i} \oplus f^1_{x_i}$, где символ $\oplus$ обозначает сумму по модулю 2.

На множестве булевых функций n переменных задается класс операторов, которые будут представляться в виде последовательностей $\mathbf{a}_1 \ldots \mathbf{a}_n$, где $\mathbf{a}_i \in \{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$. В этом случае n будет называться размерностью оператора. Действие оператора $\mathbf{a} = \mathbf{a}_1 \ldots \mathbf{a}_n$ на функцию $f(\tilde{x})$ определяется по правилу: $\mathbf{a}(f(\tilde{x})) = f_n(\tilde{x})$, где $f_0(\tilde{x}) = f(\tilde{x})$ и

$$f_i(\tilde{x}) = \begin{cases} f_{i-1}(\tilde{x}), & \text{если } \mathbf{a}_i = \mathbf{e}; \\ f_{i-1}(x_1, ..., x_{i-1}, \bar{x}_i, x_{i+1}, ..., x_n), & \text{если } \mathbf{a}_i = \mathbf{p}; \\ (f_{i-1}(\tilde{x}))'_{x_i}, & \text{если } \mathbf{a}_i = \mathbf{d}. \end{cases}$$

Представление функции $f(x_1, \ldots, x_n)$ в виде

$$f(\tilde{x}) = \bigoplus_{i=1}^{s} \mathbf{a}^i(h(\tilde{x})), \tag{1}$$

в котором $\mathbf{a}^1, \ldots, \mathbf{a}^s$ — операторы размерности n, называется операторной формой функции f, построенной по функции $h(x_1, \ldots, x_n)$. Через $M(\Phi)$ будем обозначать множество операторов, входящих в операторную форму Φ. Операторную форму назовем редуцированной, если при $i \neq j$ выполняется $\mathbf{a}^i \neq \mathbf{a}^j$. Функция $h(\tilde{x})$ называется базисной, если для любой функции $f(\tilde{x})$ существует представление в виде операторной формы по функции h. Вопросы существования операторных форм подробно изложены в [3].

Из определения оператора следует, что для любой функции h и любого оператора $\mathbf{a} = \mathbf{a}_1 \ldots \mathbf{a}_n$ имеет место следующее равенство:

$$\mathbf{a}(h) = \mathbf{a}_1 \ldots \mathbf{a}_{i-1}\mathbf{a}'_i\mathbf{a}_{i+1} \ldots \mathbf{a}_n(h) \oplus \mathbf{a}_1 \ldots \mathbf{a}_{i-1}\mathbf{a}''_i\mathbf{a}_{i+1} \ldots \mathbf{a}_n(h), \tag{2}$$

здесь $\mathbf{a}_i, \mathbf{a}'_i, \mathbf{a}''_i$ — попарно различные символы из множества $\{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$. Назовем равенство (2) разложением оператора $\mathbf{a}$ по i-ой компоненте. В дальнейшем в разложениях операторов иногда будем опускать функцию h, подразумевая, что равенство выполняется для любой функции, а выражение "оператор входит в операторную форму" будет означать, что оператор порождает слагаемое, которое входит в соответствующую сумму.

Мы будем использовать свойства операторов из [3], которые сформулируем в виде двух утверждений.

Утверждение А [3]. *Для любого оператора* $\mathbf{a}$ *выполняется следующее равенство:*

$$\mathbf{a} = \bigoplus_{k=0}^{2^n-1} \mathbf{b}^k,$$

где $\{\mathbf{b}^k\}$ *— все операторы размерности* n*, отличающиеся в каждой позиции от оператора* $\mathbf{a}$*. Такое представление оператора единственно с точностью до перестановки слагаемых.*

Это представление далее будет называться полным разложением оператора $\mathbf{a}$.

Утверждение В [3]. *Пусть* $\mathbf{a} = \mathbf{a}_1 \dots \mathbf{a}_t$, $\tilde{x} = x_1, \dots, x_n$, $\tilde{y} = y_1, \dots, y_{t-n}$, $\mathbf{a}_{\tilde{x}} = \mathbf{a}_1 \dots \mathbf{a}_n$, $\mathbf{a}_{\tilde{y}} = \mathbf{a}_{n+1} \dots \mathbf{a}_t$*. Для любых функций* $f(\tilde{x})$, $g(\tilde{y})$ *имеет место равенство:*

$$\mathbf{a}(f(\tilde{x}) \cdot g(\tilde{y})) = \mathbf{a}_{\tilde{x}}(f(\tilde{x})) \cdot \mathbf{a}_{\tilde{y}}(g(\tilde{y})).$$

Операторная форма функции f, полученная из представления (1) заменой каждого оператора его полным разложением с последующим удалением пар одинаковых слагаемых, называется специальной операторной формой функции f по функции h и обозначается $SOF_f(h)$.

Теорема 1. *Специальная операторная форма по фиксированной функции* h *является каноническим представлением.*

Доказательство. Пусть функция f представима двумя операторными формами Φ_1 и Φ_2 по функции h. Рассмотрим два вида преобразований операторных форм, которые не изменяют реализуемую функцию:

1) разложение некоторого оператора из операторной формы по одной компоненте;

2) удаление пары одинаковых слагаемых в операторной форме.

Очевидно, что такими преобразованиями любую операторную форму можно привести к редуцированной операторной форме, содержащей только операторы, каждая компонента которых равна $\mathbf{d}$ или $\mathbf{e}$. Достаточно применить первое преобразование для всех операторов по всем компонентам, равным $\mathbf{p}$, и удалить все пары одинаковых слагаемых.

Полученная операторная форма называется **de**-формой и является каноническим представлением булевых функций [3]. Таким образом, указанными преобразованиями каждую из форм Φ_1 и Φ_2 можно привести к одной и той же **de**-форме.

Пусть SOF_1, SOF_2 и SOF_3 — специальные операторные формы, полученные по Φ_1, Φ_2 и **de**-форме функции f соответственно. Покажем, что эти специальные операторные формы совпадают.

Рассмотрим разложение оператора $\mathbf{a} = \mathbf{a}_1 \dots \mathbf{a}_{i-1}\mathbf{p}\mathbf{a}_{i+1} \dots \mathbf{a}_n$ на операторы $\mathbf{b} = \mathbf{a}_1 \dots \mathbf{a}_{i-1}\mathbf{d}\mathbf{a}_{i+1} \dots \mathbf{a}_n$ и $\mathbf{c} = \mathbf{a}_1 \dots \mathbf{a}_{i-1}\mathbf{e}\mathbf{a}_{i+1} \dots \mathbf{a}_n$.

Легко заметить, что половина операторов полного разложения оператора **b** входит в полное разложение оператора **c** — это те операторы, у которых i-ая компонента равна **p**. После удаления пар одинаковых слагаемых в сумме разложений **b** и **c** останутся ровно 2^n операторов, которые составляют полное разложение оператора **a**. Значит, специальная операторная форма не изменится при замене некоторого оператора в исходной операторной форме его разложением по одной из компонент.

Рассмотрим второе преобразование. Если операторная форма Φ содержит два одинаковых слагаемых, то после разложения каждое из них представляется одинаковыми суммами 2^n слагаемых, которые в дальнейшем удаляются для получения специальной операторной формы. Очевидно, что удаление этих слагаемых из операторной формы Φ не изменит специальную операторную форму, построенную по форме Φ.

Поскольку **de**-форма может быть получена преобразованиями первого и второго вида из форм Φ_1 и Φ_2, имеют место равенства: $SOF_1 = SOF_3 = SOF_2$ (здесь равенство форм означает равенство множеств слагаемых этих форм). □

При дальнейшем изложении, если это не будет оговорено отдельно, будем считать, что n-местная базисная функция h является фиксированной и все операторные формы построены по этой функции.

Пусть S — полная группа подстановок на множестве $\{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$. Для элементов группы S будут использованы следующие обозначения:

$$\iota = \begin{pmatrix}\mathbf{dep}\\ \mathbf{dep}\end{pmatrix}, \quad \delta = \begin{pmatrix}\mathbf{dep}\\ \mathbf{dpe}\end{pmatrix}, \quad \varepsilon = \begin{pmatrix}\mathbf{dep}\\ \mathbf{ped}\end{pmatrix},$$
$$\pi = \begin{pmatrix}\mathbf{dep}\\ \mathbf{edp}\end{pmatrix}, \quad \mu = \begin{pmatrix}\mathbf{dep}\\ \mathbf{epd}\end{pmatrix}, \quad \nu = \begin{pmatrix}\mathbf{dep}\\ \mathbf{pde}\end{pmatrix}.$$

Определим преобразование φ операторов размерности n в виде последовательности $\varphi_1 \dots \varphi_n$, где $\varphi_i \in S$. Преобразование φ действует на оператор $\mathbf{a} = \mathbf{a}_1 \dots \mathbf{a}_n$ следующим образом: $\varphi(\mathbf{a}) = \varphi_1(\mathbf{a}_1) \dots \varphi_n(\mathbf{a}_n)$. Таким образом построенное преобразование φ назовем S-преобразованием.

Действие S-преобразований можно распространить на функции. Пусть $f = \bigoplus_{i=1}^{s} \mathbf{a}^i(h)$ — некоторая операторная форма функции f. Тогда

$\varphi(f) = \bigoplus_{i=1}^{s} \varphi(\mathbf{a}^i)(h)$. Следующее утверждение показывает, что определение корректно.

Утверждение 1. *Пусть имеется S-преобразование φ и две операторные формы функции $f(\tilde{x})$ — Φ_1 и Φ_2. Тогда функции $g_1 = \varphi(\Phi_1)$ и $g_2 = \varphi(\Phi_2)$, полученные S-преобразованием этих операторных форм, равны.*

Доказательство. Аналогично с доказательством теоремы 1 рассмотрим два вида преобразований операторных форм, не меняющих реализуемую ими функцию: разложение оператора и удаление пары одинаковых слагаемых. Так же приведем формы Φ_1 и Φ_2 к **de**-форме.

Для индуктивного шага достаточно показать, что если форма Ψ_2 получена из Ψ_1 однократным применением преобразования первого или второго вида, то функции $\varphi(\Psi_1)$ и $\varphi(\Psi_2)$ равны.

В случае применения преобразования второго вида равенство функций $\varphi(\Psi_1)$ и $\varphi(\Psi_2)$ является очевидным.

Пусть теперь Ψ_2 получена из Ψ_1 применением разложения некоторого оператора $\mathbf{a}$ по i-ой компоненте на операторы $\mathbf{b}$ и $\mathbf{c}$. Применим к $\varphi(\Psi_1)$ разложение оператора $\varphi(\mathbf{a})$ по i-ой компоненте на операторы $\mathbf{b}^*$ и $\mathbf{c}^*$. Поскольку φ_i — подстановка на $\{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$ и $\mathbf{a}_i, \mathbf{b}_i, \mathbf{c}_i$ — попарно различные символы из множества $\{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$, то $\varphi_i(\mathbf{a}_i), \varphi_i(\mathbf{b}_i), \varphi(\mathbf{c}_i)$ — также попарно различные символы из множества $\{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$. А значит, имеет место одна из двух систем равенств:

$$\begin{cases} \mathbf{b}^* = \varphi(\mathbf{b}) \\ \mathbf{c}^* = \varphi(\mathbf{c}) \end{cases} \text{ или } \begin{cases} \mathbf{b}^* = \varphi(\mathbf{c}) \\ \mathbf{c}^* = \varphi(\mathbf{b}) \end{cases}.$$

Следовательно, операторная форма, полученная из $\varphi(\Psi_1)$ разложением оператора $\varphi(\mathbf{a})$ по i-ой компоненте, равна $\varphi(\Psi_2)$. Отсюда следует равенство функций $\varphi(\Psi_1)$ и $\varphi(\Psi_2)$. □

Утверждение 2. *Пусть φ является S-преобразованием и $SOF_f(h)$ — специальная операторная форма функции f. Тогда $\varphi(SOF_f(h))$ — специальная операторная форма функции $\varphi(f)$.*

Доказательство. Рассмотрим S-преобразование $\varphi = \varphi_1 \dots \varphi_n$ и полное разложение оператора $\mathbf{a}$:

$$\mathbf{a} = \bigoplus_{k=0}^{2^n-1} \mathbf{b}^k,$$

где $\mathbf{b}^k = \mathbf{b}_1^k \dots \mathbf{b}_n^k$, $\mathbf{b}_i^k = \mathbf{b}_i$, если i-ая цифра в двоичной записи числа k равна 0, и $\mathbf{b}_i^k = \mathbf{c}_i$, если i-ая цифра в двоичной записи числа k равна 1, и $\mathbf{a}_i, \mathbf{b}_i, \mathbf{c}_i$ — попарно различные символы из множества $\{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$. Поскольку φ_i — подстановка на $\{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$, то $\varphi_i(\mathbf{a}_i)$, $\varphi_i(\mathbf{b}_i)$, $\varphi(\mathbf{c}_i)$ — также

попарно различные символы из множества $\{\mathbf{d}, \mathbf{e}, \mathbf{p}\}$. Поэтому полное разложение оператора $\varphi(\mathbf{a})$ имеет вид:

$$\varphi(\mathbf{a}) = \bigoplus_{k=0}^{2^n-1} \varphi(\mathbf{b}^k).$$

Таким образом, некоторый оператор $\mathbf{b}$ входит в полное разложение оператора $\mathbf{a}$ тогда и только тогда, когда оператор $\varphi(\mathbf{b})$ входит в полное разложение оператора $\varphi(\mathbf{a})$.

Пусть оператор $\mathbf{c}$ принадлежит $M(SOF_f(h))$. Рассмотрим прозвольную операторную форму Φ, реализующую данную функцию f. По определению специальной операторной формы найдутся операторы $\mathbf{a}^1$,..., $\mathbf{a}^{2k+1}$ формы Φ такие, что $\mathbf{c}$ входит в полное разложение каждого из операторов $\mathbf{a}^i$ и не входит в полное разложение никакого другого оператора из Φ. Но тогда $\varphi(\mathbf{c})$ входит в полное разложение операторов $\varphi(\mathbf{a}^i)$, а значит, $\varphi(\mathbf{c})$ принадлежит $M(SOF_{\varphi(f)}(h))$. Аналогично, если $\varphi(\mathbf{c})$ принадлежит $M(SOF_{\varphi(f)}(h))$, то $\mathbf{c}$ принадлежит $M(SOF_f(h))$. Значит,

$$\varphi(SOF_f(h)) = SOF_{\varphi(f)}(h).$$

□

Очевидно, что множество S-преобразований n-местных функций является группой, для которой будет использоваться обозначение $S_h(n)$ (в случае фиксированной функции h индекс будем опускать). Легко заметить, что порядок группы $S(n)$ равен 6^n.

Две функции $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$ называются S-эквивалентными, если существует $\varphi \in S(n)$, что $\varphi(f) = g$.

Классы S-эквивалентных функций будем называть S_h-классами, а в случае фиксированной базисной функции h — просто S-классами или операторными классами.

Следующая теорема показывает независимость числа операторных классов от базисной функции.

Теорема 2. *Для любых двух базисных функций $h_1(\tilde{x})$ и $h_2(\tilde{x})$ число S_{h_1}-классов совпадает с числом S_{h_2}-классов.*

Доказательство. Пусть $K_1, \ldots, K_s$ — все различные S_{h_1}-классы. Рассмотрим функции $f_1(\tilde{x}) = SOF_{f_1}(h_1)$, ... , $f_t(\tilde{x}) = SOF_{f_t}(h_1)$, составляющие некоторый класс K_m, представленные соответствующими специальными операторными формами.

Рассмотрим функции $f_1^*, \ldots, f_t^*$, представленные операторными формами:

$$f_j^* = \bigoplus_{\mathbf{a} \in M(SOF_{f_j}(h_1))} \mathbf{a}(h_2).$$

Из свойств специальной операторной формы легко получить, что представления указанного вида являются специальными операторными формами функций $f_1^*, \ldots, f_t^*$ по функции h_2.

Функции f_k и f_l являются S-эквивалентными по функции h_1, значит, найдется такое преобразование $\varphi \in S_{h_1}(n)$, что $\varphi(f_k) = f_l$. Покажем, что тогда существует преобразование $\varphi^* \in S_{h_2}(n)$, для которого выполняется равенство $\varphi^*(f_k^*) = f_l^*$.

Пусть $\varphi = \varphi_1 \ldots \varphi_n$, где $\varphi_i \in S$. Возьмем преобразование φ^* покомпонентно равным преобразованию φ, но действующим по базисной функции h_2: $\varphi^* = \varphi_1 \ldots \varphi_n$, $\varphi^* \in S_{h_2}(n)$. Таким образом, оба преобразования φ и φ^* будут одинаково действовать на любой оператор и множество операторов, но по-разному — на функции.

Равенство множеств $\varphi(M(SOF_{f_k}(h_1))) = M(SOF_{f_l}(h_1))$ следует из утверждения 2, а поскольку преобразования φ и φ^* действуют одинаково на множестве операторов, то $\varphi^*(M(SOF_{f_k}(h_1))) = M(SOF_{f_l}(h_1))$. Отсюда следует равенство $\varphi^*(SOF_{f_k^*}(h_2)) = SOF_{f_l^*}(h_2)$, которое означает, что функции f_k^* и f_l^* принадлежат одному классу S_{h_2}-эквивалентности. Обозначим этот класс через K_m^*.

Пусть функция g^* принадлежит классу K_m^*, то есть найдется преобразование $\psi^* \in S_{h_2}(n)$, что $g^* = \psi^*(f_1^*)$. Возьмем $\psi \in S_{h_1}(n)$, покомпонентно равное ψ^*. Тогда функция $g = \psi(f_1)$ принадлежит K_m. Значит, имеет место равенство $|K_m| = |K_m^*|$.

Из единственности специальной операторной формы следует, что при $K_m \neq K_n$ выполняется $K_m^* \neq K_n^*$. Таким образом, можно установить взаимно однозначное соответствие классов S_{h_1}-эквивалентности и классов S_{h_2}-эквивалентности. □

При дальнейшем изложении будем считать, что базисная функция h равна $x_1 \cdot \ldots \cdot x_n$. Результаты о числе S-классов для данной функции по теореме 2 будут верны для любой базисной функции.

Введем следующие обозначения для невырожденных матриц размерности 2:

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{D} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{E} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

$$\mathbf{P} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{M} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{N} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Каждому S-преобразованию φ размерности n сопоставим матрицу $A(\varphi)$ размерности $2^n \times 2^n$ следующим образом:

1. При $n = 1$ имеет место соответствие:

$$\mathbf{A}(\iota) = \mathbf{I}, \quad \mathbf{A}(\delta) = \mathbf{D}, \quad \mathbf{A}(\varepsilon) = \mathbf{E}, \quad \mathbf{A}(\pi) = \mathbf{P}, \quad \mathbf{A}(\mu) = \mathbf{M}, \quad \mathbf{A}(\nu) = \mathbf{N}.$$

2. При $n > 1$ матрица $\mathbf{A}(\varphi)$ равна кронекерову произведению соответствующих матриц:

$$\mathbf{A}(\varphi) = \mathbf{A}(\varphi_1) \otimes \cdots \otimes \mathbf{A}(\varphi_n).$$

Кронекерова степень матрицы A будет обозначаться:

$$\underbrace{A \otimes A \otimes \cdots \otimes A}_{n} = A^{[n]}.$$

Символом $\mathbf{O}$ обозначим нулевую матрицу, размер которой будет определяться по контексту.

Индукцией легко показать, что $\mathbf{I}^{[n]}$ — единичная матрица размерности $2^n \times 2^n$ и имеют место следующие равенства:

$$\mathbf{M}^{[n]} \cdot \mathbf{N}^{[n]} = \mathbf{I}^{[n]}; \quad \mathbf{M}^{[n]} \cdot \mathbf{M}^{[n]} = \mathbf{N}^{[n]}; \quad \mathbf{N}^{[n]} \cdot \mathbf{N}^{[n]} = \mathbf{M}^{[n]}.$$

Теорема 3. *Для любого S-преобразования $\varphi = \varphi_1 \dots \varphi_n$ и функции f выполняется равенство $\varphi(f) = \mathbf{A}(\varphi) \cdot f$, где функции f и $\varphi(f)$ представлены векторами.*

Доказательство. 1. При $n = 1$ достаточно рассмотреть 6 случаев, поскольку $\varphi \in S$.

Для примера рассмотрим $\varphi = \nu$ и функцию f, представленную операторной формой $f(x) = \overline{x} \cdot f_x^0 \oplus x \cdot f_x^1 = f_x^0 \cdot \mathbf{p}(x) \oplus f_x^1 \cdot \mathbf{e}(x)$. Далее применим преобразование φ к функции f:

$$\varphi(f) = f_x^0 \cdot \nu(\mathbf{p})(x) \oplus f_x^1 \cdot \nu(\mathbf{e})(x) = f_x^0 \cdot \mathbf{e}(x) \oplus f_x^1 \cdot \mathbf{d}(x) = \\ = f_x^0 \cdot x \oplus f_x^1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} f_x^0 \\ f_x^1 \end{pmatrix}.$$

Остальные случаи проверяются аналогично.

2. Пусть $n > 1$ и $\varphi = \varphi_1 \varphi_2 \dots \varphi_n$. Символом $\mathbf{B}$ обозначим матрицу преобразования $\varphi^* = \varphi_2 \dots \varphi_n$. Аналогично пункту 1, для φ_1 достаточно рассмотреть 6 случаев. Доказательство проведем для случая $\varphi_1 = \nu$.

Поскольку S-преобразование действует на оператор покомпонентно, то из утверждения B следует, что для любого преобразования $\psi = \psi_1 \dots \psi_t$ и двух преобразований $\psi_{\tilde{x}} = \psi_1 \dots \psi_n$ и $\psi_{\tilde{y}} = \psi_{n+1} \dots \psi_t$, полученных разбиением его компонент, будет верно равенство:

$$\psi(f(\tilde{x}) \cdot g(\tilde{y})) = \psi_{\tilde{x}}(f(\tilde{x})) \cdot \psi_{\tilde{y}}(g(\tilde{y})). \tag{3}$$

Разобъем множество переменных $\{x_1, \dots, x_n\}$ на два множества $\{x_1\}$ и $\{x_2, \dots, x_n\}$ и применим к ним равенство (3):

$$\varphi(f) = \varphi(\overline{x}_1 f_{x_1}^0 \oplus x_1 f_{x_1}^1) = \nu(\overline{x}_1)\varphi^*(f_{x_1}^0) \oplus \nu(x_1)\varphi^*(f_{x_1}^1) = \\ = \nu(\mathbf{p}(x_1))\mathbf{B}f_{x_1}^0 \oplus \nu(\mathbf{e}(x_1))\mathbf{B}f_{x_1}^1 = \mathbf{e}(x_1)\mathbf{B}f_{x_1}^0 \oplus \mathbf{d}(x_1)\mathbf{B}f_{x_1}^1 = \\ = x_1\mathbf{B}f_{x_1}^0 \oplus \mathbf{B}f_{x_1}^1 = \left(\begin{array}{c|c} \mathbf{O} & \mathbf{B} \\ \hline \mathbf{B} & \mathbf{B} \end{array}\right) \cdot \begin{pmatrix} f_{x_1}^0 \\ f_{x_1}^1 \end{pmatrix} = \left(\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \otimes \mathbf{B}\right) \cdot \begin{pmatrix} f_{x_1}^0 \\ f_{x_1}^1 \end{pmatrix}.$$

Для остальных подстановок равенство проверяется аналогично. □

Функцию f будем называть инвариантной по преобразованию φ, если

$$\varphi(f) = f. \tag{4}$$

Обозначим через $st(\varphi)$ количество n-местных булевых функций, инвариантных по n-местному преобразованию φ. Очевидно, что $st(\varphi)$ есть число решений уравнения (4).

Лемма 1. *Пусть преобразование φ представимо матрицей A. Тогда имеет место равенство $st(\varphi) = 2^{2^n - \mathrm{rank}(A \oplus \mathbf{I}^{[n]})}$.*

Доказательство. Уравнение (4) можно записать в матричной форме: $A \cdot f = f$, или в виде $(A \oplus \mathbf{I}^{[n]})f = 0$. Количество решений этого однородного уравнения равно $2^{2^n - \mathrm{rank}(A \oplus \mathbf{I}^{[n]})}$. □

Лемма 2. $\mathrm{rank}(\mathbf{M}^{[n]} \oplus \mathbf{I}^{[n]}) = \frac{2}{3}(2^n + (-1)^{n+1})$.

Доказательство. При $n < 3$ равенство проверяется непосредственно. При $n \geq 3$ распишем кронекерову степень следующим образом:

$$\mathbf{M}^{[n]} = \mathbf{M} \otimes \mathbf{M}^{[n-1]} = \left(\begin{array}{c|c} 1 & 1 \\ \hline 1 & 0 \end{array}\right) \otimes \mathbf{M}^{[n-1]} = \left(\begin{array}{c|c} \mathbf{M}^{[n-1]} & \mathbf{M}^{[n-1]} \\ \hline \mathbf{M}^{[n-1]} & \mathbf{O} \end{array}\right)$$

и

$$\mathbf{I}^{[n]} = \mathbf{I} \otimes \mathbf{I}^{[n-1]} = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & 1 \end{array}\right) \otimes \mathbf{I}^{[n-1]} = \left(\begin{array}{c|c} \mathbf{I}^{[n-1]} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{I}^{[n-1]} \end{array}\right).$$

Тогда матрица $\mathbf{M}^{[n]} \oplus \mathbf{I}^{[n]}$ будет иметь вид:

$$\mathbf{M}^{[n]} \oplus \mathbf{I}^{[n]} = \left(\begin{array}{c|c} \mathbf{M}^{[n-1]} \oplus \mathbf{I}^{[n-1]} & \mathbf{M}^{[n-1]} \\ \hline \mathbf{M}^{[n-1]} & \mathbf{I}^{[n-1]} \end{array}\right).$$

Воспользуемся записью $A \sim B$ для матриц A и B, получаемых одна из другой линейными преобразованиями строк и столбцов.

Умножая матрицу $\mathbf{M}^{[n]} \oplus \mathbf{I}^{[n]}$ на невырожденные матрицы (выполняя линейные преобразования строк и столбцов), приведем ее к диагональному виду:

$$\mathbf{M}^{[n]} \oplus \mathbf{I}^{[n]} \sim \left(\begin{array}{c|c} \mathbf{I}^{[n-1]} & \mathbf{I}^{[n-1]} \\ \hline \mathbf{O} & \mathbf{I}^{[n-1]} \end{array}\right) \cdot \left(\begin{array}{c|c} \mathbf{I}^{[n-1]} & \mathbf{O} \\ \hline \mathbf{I}^{[n-1]} & \mathbf{M}^{[n-1]} \end{array}\right) \cdot (\mathbf{M}^{[n]} \oplus \mathbf{I}^{[n]}) \cdot$$
$$\cdot \left(\begin{array}{c|c} \mathbf{I}^{[n-1]} & \mathbf{O} \\ \hline \mathbf{M}^{[n-1]} & \mathbf{I}^{[n-1]} \end{array}\right) = \left(\begin{array}{c|c} \mathbf{O} & \mathbf{M}^{[n-1]} \\ \hline \mathbf{M}^{[n-1]} \oplus \mathbf{N}^{[n-1]} \oplus \mathbf{I}^{[n-1]} & \mathbf{O} \end{array}\right).$$

Тогда, используя равенство $\mathrm{rank}(\mathbf{M}^{[n-1]}) = 2^{n-1}$, ранг исходной матрицы можно найти из соотношения:

$$\mathrm{rank}(\mathbf{M}^{[n]} \oplus \mathbf{I}^{[n]}) = 2^{n-1} + \mathrm{rank}(\mathbf{M}^{[n-1]} \oplus \mathbf{N}^{[n-1]} \oplus \mathbf{I}^{[n-1]}).$$

При дальнейшем изложении доказательства для краткости записи будем опускать показатель кронекеровой степени, подразумевая его равным $n-3$.

Рассмотрим матрицу $\mathbf{M}^{[n-1]}\oplus\mathbf{N}^{[n-1]}\oplus\mathbf{I}^{[n-1]}$. Дважды расписываем кронекерову степень, спускаясь к матрицам кронекеровой степени $n-3$:

$$\mathbf{M}^{[n-1]}\oplus\mathbf{N}^{[n-1]}\oplus\mathbf{I}^{[n-1]}=\left(\begin{array}{c|c|c|c}\mathbf{M}\oplus\mathbf{I}&\mathbf{M}&\mathbf{M}&\mathbf{M}\oplus\mathbf{N}\\\hline\mathbf{M}&\mathbf{I}&\mathbf{M}\oplus\mathbf{N}&\mathbf{N}\\\hline\mathbf{M}&\mathbf{M}\oplus\mathbf{N}&\mathbf{I}&\mathbf{N}\\\hline\mathbf{M}\oplus\mathbf{N}&\mathbf{N}&\mathbf{N}&\mathbf{N}\oplus\mathbf{I}\end{array}\right).$$

Умножив матрицу $\mathbf{M}^{[n-1]}\oplus\mathbf{N}^{[n-1]}\oplus\mathbf{I}^{[n-1]}$ слева на матрицу A_1

$$A_1=\left(\begin{array}{c|c|c|c}\mathbf{I}&\mathbf{O}&\mathbf{I}&\mathbf{O}\\\hline\mathbf{O}&\mathbf{I}&\mathbf{I}&\mathbf{O}\\\hline\mathbf{O}&\mathbf{O}&\mathbf{I}&\mathbf{O}\\\hline\mathbf{O}&\mathbf{O}&\mathbf{O}&\mathbf{I}\end{array}\right)\cdot\left(\begin{array}{c|c|c|c}\mathbf{I}&\mathbf{O}&\mathbf{O}&\mathbf{O}\\\hline\mathbf{N}&\mathbf{I}&\mathbf{O}&\mathbf{O}\\\hline\mathbf{O}&\mathbf{I}&\mathbf{I}&\mathbf{O}\\\hline\mathbf{M}&\mathbf{O}&\mathbf{O}&\mathbf{I}\end{array}\right)$$

и справа на матрицу A_2

$$A_2=\left(\begin{array}{c|c|c|c}\mathbf{I}&\mathbf{N}&\mathbf{O}&\mathbf{M}\\\hline\mathbf{O}&\mathbf{I}&\mathbf{I}&\mathbf{O}\\\hline\mathbf{O}&\mathbf{O}&\mathbf{I}&\mathbf{O}\\\hline\mathbf{O}&\mathbf{O}&\mathbf{O}&\mathbf{I}\end{array}\right)\cdot\left(\begin{array}{c|c|c|c}\mathbf{I}&\mathbf{O}&\mathbf{O}&\mathbf{O}\\\hline\mathbf{O}&\mathbf{I}&\mathbf{O}&\mathbf{O}\\\hline\mathbf{I}&\mathbf{O}&\mathbf{I}&\mathbf{O}\\\hline\mathbf{O}&\mathbf{O}&\mathbf{O}&\mathbf{I}\end{array}\right),$$

получим эквивалентную матрицу:

$$\mathbf{M}^{[n-1]}\oplus\mathbf{N}^{[n-1]}\oplus\mathbf{I}^{[n-1]}\sim\left(\begin{array}{c|c|c|c}\mathbf{M}\oplus\mathbf{I}&\mathbf{O}&\mathbf{O}&\mathbf{O}\\\hline\mathbf{O}&\mathbf{O}&\mathbf{M}\oplus\mathbf{N}\oplus\mathbf{I}&\mathbf{O}\\\hline\mathbf{O}&\mathbf{M}\oplus\mathbf{N}\oplus\mathbf{I}&\mathbf{O}&\mathbf{O}\\\hline\mathbf{O}&\mathbf{O}&\mathbf{O}&\mathbf{O}\end{array}\right).$$

Тогда выполняется следующее равенство:

$$\operatorname{rank}(\mathbf{M}^{[n-1]}\oplus\mathbf{N}^{[n-1]}\oplus\mathbf{I}^{[n-1]})=$$

$$=\operatorname{rank}(\mathbf{M}^{[n-3]}\oplus\mathbf{I}^{[n-3]})+2\operatorname{rank}(\mathbf{M}^{[n-3]}\oplus\mathbf{N}^{[n-3]}\oplus\mathbf{I}^{[n-3]}).$$

Введем обозначения: $k_n=\operatorname{rank}(\mathbf{M}^{[n]}\oplus\mathbf{I}^{[n]})$, $l_n=\operatorname{rank}(\mathbf{M}^{[n]}\oplus\mathbf{N}^{[n]}\oplus\mathbf{I}^{[n]})$. Тогда $k_n=2^{n-1}+l_{n-1}$ и $l_{n-1}=k_{n-3}+2\cdot l_{n-3}$. Подставим значение k_{n-3} в выражение для l_{n-1}: $l_{n-1}=2^{n-4}+2\cdot l_{n-3}+l_{n-4}$.

Разрешая это рекуррентное соотношение, получим: $l_{n-1}=\frac{1}{3}(2^{n-1}+2\cdot(-1)^{n+1})$ и $k_n=\frac{2}{3}(2^n+(-1)^{n+1})$.

Окончательное соотношение для ранга матрицы $\mathbf{M}^{[n]}\oplus\mathbf{I}^{[n]}$ примет вид: $\operatorname{rank}(\mathbf{M}^{[n]}\oplus\mathbf{I}^{[n]})=\frac{2}{3}(2^n+(-1)^{n+1})$. □

Лемма 3. $\operatorname{rank}((\mathbf{D}\otimes\mathbf{M}^{[n]})\oplus\mathbf{I}^{[n+1]})=\frac{1}{3}(5\cdot2^n+2(-1)^{n+1})$.

Доказательство. Расписав кронекерову степень и выполнив операции, получим:

$$(\mathbf{D}\otimes\mathbf{M}^{[n]})\oplus\mathbf{I}^{[n+1]} = \left(\begin{array}{c|c} \mathbf{I}^{[n]} & \mathbf{M}^{[n]} \\ \hline \mathbf{M}^{[n]} & \mathbf{I}^{[n]} \end{array}\right).$$

Умножив матрицу $(\mathbf{D}\otimes\mathbf{M}^{[n]})\oplus\mathbf{I}^{[n+1]}$ слева на матрицу B_1 и справа на матрицу B_2, где

$$B_1 = \left(\begin{array}{c|c} \mathbf{I}^{[n]} & \mathbf{O} \\ \hline \mathbf{M}^{[n]} & \mathbf{N}^{[n]} \end{array}\right), \quad B_2 = \left(\begin{array}{c|c} \mathbf{I}^{[n]} & \mathbf{O} \\ \hline \mathbf{N}^{[n]} & \mathbf{I}^{[n]} \end{array}\right),$$

получим:

$$(\mathbf{D}\otimes\mathbf{M}^{[n]})\oplus\mathbf{I}^{[n+1]} \sim \left(\begin{array}{c|c} \mathbf{O} & \mathbf{M}^{[n]} \\ \hline \mathbf{M}^{[n]}\oplus\mathbf{I}^{[n]} & \mathbf{O} \end{array}\right).$$

Тогда $\operatorname{rank}((\mathbf{D}\otimes\mathbf{M}^{[n]})\oplus\mathbf{I}^{[n+1]}) = \operatorname{rank}(\mathbf{M}^{[n]}) + \operatorname{rank}(\mathbf{M}^{[n]}\oplus\mathbf{I}^{[n]})$. Невырожденность матрицы $\mathbf{M}^{[n]}$ и лемма 2 дают окончательную формулу:

$$\operatorname{rank}((\mathbf{D}\otimes\mathbf{M}^{[n]})\oplus\mathbf{I}^{[n+1]}) = 2^n + \frac{2}{3}(2^n + (-1)^{n+1}) = \frac{1}{3}(5\cdot 2^n + 2(-1)^{n+1}).$$

□

Лемма 4. $\operatorname{rank}((\mathbf{I}\otimes A)\oplus\mathbf{I}^{[n]}) = 2\operatorname{rank}(A\oplus\mathbf{I}^{[n-1]})$, *где* A — *матрица S-преобразования размерности* $n-1$.

Доказательство. Расписав кронекерову степень в явном виде

$$(\mathbf{I}\otimes A)\oplus\mathbf{I}^{[n]} = \left(\begin{array}{c|c} A & \mathbf{O} \\ \hline \mathbf{O} & A \end{array}\right)\oplus\left(\begin{array}{c|c} \mathbf{I}^{[n-1]} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{I}^{[n-1]} \end{array}\right) = \left(\begin{array}{c|c} A\oplus\mathbf{I}^{[n-1]} & \mathbf{O} \\ \hline \mathbf{O} & A\oplus\mathbf{I}^{[n-1]} \end{array}\right),$$

получаем $\operatorname{rank}((\mathbf{I}\otimes A)\oplus\mathbf{I}^{[n]}) = 2\operatorname{rank}(A\oplus\mathbf{I}^{[n-1]})$. □

Лемма 5. $\operatorname{rank}((\mathbf{D}^{[2]}\otimes A)\oplus\mathbf{I}^{[n]}) = 2\operatorname{rank}((\mathbf{D}\otimes A)\oplus\mathbf{I}^{[n-1]})$, *где* A — *матрица S-преобразования размерности* $n-2$.

Доказательство. Дважды расписав кронекерову степень и выполнив перестановку строк и столбцов, получим:

$$(\mathbf{D}^{[2]}\otimes A)\oplus\mathbf{I}^{[n]} \sim \left(\begin{array}{c|c|c|c} \mathbf{I}^{[n-2]} & A & \mathbf{O} & \mathbf{O} \\ \hline A & \mathbf{I}^{[n-2]} & \mathbf{O} & \mathbf{O} \\ \hline \mathbf{O} & \mathbf{O} & \mathbf{I}^{[n-2]} & A \\ \hline \mathbf{O} & \mathbf{O} & A & \mathbf{I}^{[n-2]} \end{array}\right).$$

Поскольку матрица $(\mathbf{D}\otimes A)\oplus\mathbf{I}^{[n-1]}$ имеет вид

$$(\mathbf{D}\otimes A)\oplus\mathbf{I}^{[n-1]} = \left(\begin{array}{c|c} \mathbf{I}^{[n-2]} & A \\ \hline A & \mathbf{I}^{[n-2]} \end{array}\right),$$

то выполняется эквивалентность:

$$(\mathbf{D}^{[2]} \otimes A) \oplus \mathbf{I}^{[n]} \sim \left(\begin{array}{c|c} (\mathbf{D} \otimes A) \oplus \mathbf{I}^{[n-1]} & \mathbf{O} \\ \hline \mathbf{O} & (\mathbf{D} \otimes A) \oplus \mathbf{I}^{[n-1]} \end{array} \right).$$

Получили равенство $\operatorname{rank}((\mathbf{D}^{[2]} \otimes A) \oplus \mathbf{I}^{[n]}) = 2\operatorname{rank}((\mathbf{D} \otimes A) \oplus \mathbf{I}^{[n-1]})$. □

Лемма 6. *$st(\varphi_1\varphi_2 \dots \varphi_n) = st(\varphi_{i_1} \dots \varphi_{i_n})$, где $(i_1, \dots, i_n)$ — некоторая перестановка элементов множества $\{1, 2, \dots, n\}$.*

Доказательство. Пусть $\varphi = \varphi_1\varphi_2 \dots \varphi_n$ и $\varphi^* = \varphi_{i_1}\varphi_{i_2} \dots \varphi_{i_n}$. Возьмем функцию f, инвариантную по преобразованию φ: $\varphi(f) = f$. Пусть

$$f(\tilde{x}) = \bigoplus_{k=1}^{s} \mathbf{a}^k(x_1 \cdot \ldots \cdot x_n)$$

— некоторая операторная форма функции f. По утверждению B для любого оператора $\mathbf{a} = \mathbf{a}_1 \dots \mathbf{a}_n$ и функции $\mathbf{a}_1 \dots \mathbf{a}_n(x_1 \cdot \ldots \cdot x_n)$ выполняется:

$$\mathbf{a}_1 \dots \mathbf{a}_n(x_1 \cdot \ldots \cdot x_n) = \mathbf{a}_1(x_1) \cdot \ldots \cdot \mathbf{a}_n(x_n).$$

Пусть перестановка $(j_1, \dots, j_n)$ является обратной к перестановке $(i_1, \dots, i_n)$. Тогда по предыдущему равенству выполняется:

$$\mathbf{a}_1 \dots \mathbf{a}_n(x_{j_1} \cdot \ldots \cdot x_{j_n}) = \mathbf{a}_1(x_{j_1}) \cdot \ldots \cdot \mathbf{a}_n(x_{j_n}) = \mathbf{a}_{i_1}(x_1) \cdot \ldots \cdot \mathbf{a}_{i_n}(x_n).$$

Рассмотрим функцию $g(x_1, \dots, x_n) = f(x_{j_1}, \dots, x_{j_n})$. Согласно приведенным равенствам функция g может быть представлена в виде:

$$g(\tilde{x}) = \bigoplus_{k=1}^{s} \mathbf{a}_{i_1}^k \dots \mathbf{a}_{i_n}^k(x_1 \cdot \ldots \cdot x_n).$$

Для инвариантной по преобразованию φ функции f выполняется

$$f(\tilde{x}) = \bigoplus_{k=1}^{s} \varphi_1(\mathbf{a}_1^k) \dots \varphi_n(\mathbf{a}_n^k)(x_1 \cdot \ldots \cdot x_n).$$

Поскольку функция $g(\tilde{x}) = f(x_{j_1}, \dots, x_{j_n})$, то

$$g(\tilde{x}) = \bigoplus_{k=1}^{s} \varphi_{i_1}(\mathbf{a}_{i_1}^k) \dots \varphi_{i_n}(\mathbf{a}_{i_n}^k)(x_1 \cdot \ldots \cdot x_n) =$$

$$= \bigoplus_{k=1}^{s} \varphi^*(\mathbf{a}_{i_1}^k \dots \mathbf{a}_{i_n}^k)(x_1 \cdot \ldots \cdot x_n) = \varphi^*(g).$$

Получили, что функция g инвариантна по преобразованию φ^*. Таким образом, мы установили однозначное соответствие между множествами функций, инвариантных по преоразованиям φ и φ^*, а значит, $st(\varphi) = st(\varphi^*)$. □

Лемма 7. *$st(\varphi_1\varphi_2\dots\varphi_n) = st(r(\varphi_1)r(\varphi_2)\dots r(\varphi_n))$, где*

$$r(\varphi_i) = \begin{cases} \iota, & \text{если } \varphi_i = \iota; \\ \delta, & \text{если } \varphi_i \in \{\delta, \varepsilon, \pi\}; \\ \mu, & \text{если } \varphi_i \in \{\mu, \nu\}. \end{cases}$$

Доказательство. Положим $\varphi = \varphi_1\varphi_2\dots\varphi_n$ и пусть A обозначает матрицу преобразования $\varphi_2\dots\varphi_n$. Рассмотрим возможные значения φ_1.

1. Пусть $\varphi_1 \in \{\iota, \delta, \mu\}$. По условию леммы $r(\varphi_1) = \varphi_1$.

Тогда верно равенство $\varphi_1\varphi_2\dots\varphi_n = r(\varphi_1)\varphi_2\dots\varphi_n$ и, следовательно, равенство $st(\varphi_1\varphi_2\dots\varphi_n) = st(r(\varphi_1)\varphi_2\dots\varphi_n)$.

2. Пусть $\varphi_1 = \varepsilon$. В этом случае $A(\varphi) = \mathbf{E} \otimes A$.

Выполним преобразования матрицы $A(\varphi) \oplus \mathbf{I}^{[n]}$:

$$(\mathbf{E} \otimes A) \oplus \mathbf{I}^{[n]} \sim \left(\begin{array}{c|c} \mathbf{I}^{[n-1]} & \mathbf{I}^{[n-1]} \\ \hline \mathbf{O} & \mathbf{I}^{[n-1]} \end{array}\right) \cdot ((\mathbf{E} \otimes A) \oplus \mathbf{I}^{[n]}) \cdot \left(\begin{array}{c|c} \mathbf{I}^{[n-1]} & \mathbf{I}^{[n-1]} \\ \hline \mathbf{O} & \mathbf{I}^{[n-1]} \end{array}\right) =$$

$$= \left(\begin{array}{c|c} \mathbf{I}^{[n-1]} & A \\ \hline A & \mathbf{I}^{[n-1]} \end{array}\right) = (\mathbf{D} \otimes A) \oplus \mathbf{I}^{[n]}.$$

По лемме 1 выполняется $st(\varphi_1\varphi_2\dots\varphi_n) = st(r(\varphi_1)\varphi_2\dots\varphi_n)$.

3. Пусть $\varphi_1 = \pi$. В этом случае $A(\varphi) = \mathbf{P} \otimes A$. Преобразуем матрицу $A(\varphi) \oplus \mathbf{I}^{[n]}$:

$$(\mathbf{P} \otimes A) \oplus \mathbf{I}^{[n]} \sim \left(\begin{array}{c|c} \mathbf{I}^{[n-1]} & \mathbf{O} \\ \hline \mathbf{I}^{[n-1]} & \mathbf{I}^{[n-1]} \end{array}\right) \cdot ((\mathbf{P} \otimes A) \oplus \mathbf{I}^{[n]}) \cdot \left(\begin{array}{c|c} \mathbf{I}^{[n-1]} & \mathbf{O} \\ \hline \mathbf{I}^{[n-1]} & \mathbf{I}^{[n-1]} \end{array}\right) =$$

$$= \left(\begin{array}{c|c} \mathbf{I}^{[n-1]} & A \\ \hline A & \mathbf{I}^{[n-1]} \end{array}\right) = (\mathbf{D} \otimes A) \oplus \mathbf{I}^{[n]}.$$

По лемме 1 выполняется $st(\varphi_1\varphi_2\dots\varphi_n) = st(r(\varphi_1)\varphi_2\dots\varphi_n)$.

4. Пусть $\varphi_1 = \nu$. В этом случае $A(\varphi) = \mathbf{N} \otimes A$.

Тогда матрица $A(\varphi) \oplus \mathbf{I}^{[n]}$ приводится к следующему виду:

$$(\mathbf{N} \otimes A) \oplus \mathbf{I}^{[n]} \sim \left(\begin{array}{c|c} \mathbf{O} & \mathbf{I}^{[n-1]} \\ \hline \mathbf{I}^{[n-1]} & \mathbf{O} \end{array}\right) \cdot ((\mathbf{N} \otimes A) \oplus \mathbf{I}^{[n]}) \cdot \left(\begin{array}{c|c} \mathbf{O} & \mathbf{I}^{[n-1]} \\ \hline \mathbf{I}^{[n-1]} & \mathbf{O} \end{array}\right) =$$

$$= \left(\begin{array}{c|c} A \oplus \mathbf{I}^{[n-1]} & A \\ \hline A & \mathbf{I}^{[n-1]} \end{array}\right) = (\mathbf{M} \otimes A) \oplus \mathbf{I}^{[n]}.$$

По лемме 1 выполняется $st(\varphi_1\varphi_2\dots\varphi_n) = st(r(\varphi_1)\varphi_2\dots\varphi_n)$.

Рассмотренные случаи показывают, что равенство $st(\varphi_1\varphi_2\dots\varphi_n) = st(r(\varphi_1)\varphi_2\dots\varphi_n)$ выполняется для любого $\varphi_1 \in S$.

По индукции, с использованием леммы 6, получается окончательное равенство:

$$st(\varphi_1\varphi_2\dots\varphi_n) = st(r(\varphi_1)\dots r(\varphi_n)).$$

□

Леммы 1–7 и лемма Бернсайда [1] позволяют получить формулу для нахождения числа S-классов.

Теорема 4. *Число S-классов $K_S(n)$ булевых функций n переменных выражается формулой*

$$K_S(n) = \frac{1}{6^n}\sum_{m=0}^{n} 2^m C_n^m \left((4^{n-m}-1)2^{\frac{2^{n-m}(2^m+2(-1)^m)}{6}} + 2^{\frac{2^{n-m}(2^m+2(-1)^m)}{3}}\right).$$

Доказательство. Возьмем преобразование

$$\varphi = \underbrace{\iota\dots\iota}_{i}\underbrace{\delta\dots\delta}_{d}\underbrace{\mu\dots\mu}_{m},$$

где $i+d+m=n$. По лемме 1 имеем $st(\varphi) = 2^{2^n - \mathrm{rank}(A(\varphi)\oplus\mathbf{I}^{[n]})}$, где $A(\varphi) = \mathbf{I}^{[i]}\otimes\mathbf{D}^{[d]}\otimes\mathbf{M}^{[m]}$.

Рассмотрим 2 случая.

1. Пусть $d=0$. В этом случае $i = n-m$. Используя лемму 2, получаем:

$$\mathrm{rank}(\mathbf{M}^{[m]}\oplus\mathbf{I}^{[m]}) = \frac{2}{3}(2^m + (-1)^{m+1}).$$

Далее по лемме 4

$$\mathrm{rank}((\mathbf{I}^{[n-m]}\otimes\mathbf{M}^{[m]})\oplus\mathbf{I}^{[n]}) = 2^{n-m}\frac{2}{3}(2^m+(-1)^{m+1}).$$

Тогда число инвариантных функций будет равно

$$st(\varphi) = 2^{2^n - 2^{n-m}\frac{2}{3}(2^m+(-1)^{m+1})}.$$

Согласно леммам 6 и 7, любое преобразование, полученное из φ перестановкой компонент и заменой некоторых μ на ν, будет иметь столько же инвариантных функций. Расставить μ можно C_n^m способами, а заменить их на ν можно 2^m способами, поэтому всего таких преобразований будет $2^m C_n^m$.

2. Пусть $d>0$. По лемме 3:

$$\mathrm{rank}((\mathbf{D}\otimes\mathbf{M}^{[m]})\oplus\mathbf{I}^{[m+1]}) = \frac{1}{3}(5\cdot 2^m + 2(-1)^{m+1}).$$

По лемме 5:

$$\mathrm{rank}((\mathbf{D}^{[d]}\otimes\mathbf{M}^{[m]})\oplus\mathbf{I}^{[d+m+1]}) = 2^{d-1}\frac{1}{3}(5\cdot 2^m + 2(-1)^{m+1}).$$

По лемме 3 имеем окончательное значение ранга:

$$\operatorname{rank}((\mathbf{I}^{[i]} \otimes \mathbf{D}^{[d]} \otimes \mathbf{M}^{[m]}) \oplus \mathbf{I}^{[d+m+1]}) = 2^{i+d-1}\frac{1}{3}(5 \cdot 2^m + 2(-1)^{m+1}).$$

И число инвариантных функций в этом случае будет равно

$$st(\varphi) = 2^{2^n - 2^{i+d-1}\frac{1}{3}(5\cdot 2^m + 2(-1)^{m+1})}.$$

Подставим значение $i = n - m - d$ в это выражение:

$$st(\varphi) = 2^{2^n - 2^{n-m-1}\frac{1}{3}(5\cdot 2^m + 2(-1)^{m+1})}.$$

Применяя опять леммы 6 и 7, получим, что $3^d 2^m C_n^m C_{n-m}^d$ преобразований будут иметь такое же количество инвариантных функций, так как μ можно расставить C_n^m способами, после этого δ можно расставить C_{n-m}^d способами и 3^d способами можно заменить δ на π и ε, 2^m способами — μ на ν.

Теперь используем лемму Бернсайда для S-преобразований в следующей формулировке:

$$K_S(n) = \frac{1}{|S_n|}\sum_{\varphi \in S_n} st(\varphi).$$

В данной сумме сгруппируем одинаковые слагаемые:

$$K_S(n) = \frac{1}{6^n}\sum_{m=0}^{n}\left(2^m C_n^m st(\underbrace{\iota \dots \iota}_{n-m}\underbrace{\mu \dots \mu}_{m}) + \right.$$
$$\left. + \sum_{d=1}^{n-m} 3^d 2^m C_n^m C_{n-m}^d st(\underbrace{\iota \dots \iota}_{n-m-d}\underbrace{\delta \dots \delta}_{d}\underbrace{\mu \dots \mu}_{m})\right).$$

Подставим полученные формулы для числа инвариантных функций:

$$K_S(n) = \frac{1}{6^n}\sum_{m=0}^{n} 2^m C_n^m \left(2^{2^n - 2^{n-m}\frac{2}{3}(2^m + (-1)^{m+1})} + \right.$$
$$\left. + \sum_{d=1}^{n-m} 3^d C_{n-m}^d 2^{2^n - 2^{n-m-1}\frac{1}{3}(5\cdot 2^m + 2(-1)^{m+1})}\right).$$

Первое слагаемое внутри суммы упрощается следующим образом:

$$2^{2^n - 2^{n-m}\frac{2}{3}(2^m + (-1)^{m+1})} = 2^{\frac{2^{n-m}(2^m + 2(-1)^m)}{3}}.$$

Второе слагаемое упрощается с помощью формулы бинома Ньютона:

$$\sum_{d=1}^{n-m} 3^d C_{n-m}^d 2^{2^n - 2^{n-m-1}\frac{1}{3}(5\cdot 2^m + 2(-1)^{m+1})} =$$

$$= 2^{2^n - 2^{n-m-1}\frac{1}{3}(5\cdot 2^m + 2(-1)^{m+1})} \sum_{d=1}^{n-m} 3^d C_{n-m}^d = (4^{n-m}-1)2^{\frac{2^{n-m}(2^m+2(-1)^m)}{6}}.$$

В итоге получается следующая формула для числа S-классов:

$$K_S(n) = \frac{1}{6^n} \sum_{m=0}^{n} 2^m C_n^m \left((4^{n-m}-1)2^{\frac{2^{n-m}(2^m+2(-1)^m)}{6}} + 2^{\frac{2^{n-m}(2^m+2(-1)^m)}{3}} \right).$$

□

Список литературы

1. Логачев О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко — М.: МЦНМО, 2004. — 470 с.
2. Черемушкин А.В. Линейная и аффинная классификация дискретных функций (обзор публикаций) / А.В. Черемушкин // Математические вопросы кибернетики, 2005. — С. 261–280.
3. Избранные вопросы теории булевых функций: Монография / А.С. Балюк, С.Ф. Винокуров, А.И. Гайдуков и др.; Под ред. С.Ф. Винокурова, Н.А. Перязева. — М.: Физматлит, 2001. — 192 с.

S. F. Vinokurov, A. S. Kazimirov
Enumeration of operator classes for boolean functions

Abstract. This paper contains the results for enumeration of S-classes of Boolean functions. S-classification is based on operator representations for Boolean functions which are an extension of EXOR-sum-of-products expressions.

Keywords: boolean function, polynomial form, operator, special normal form, group classification.

Винокуров Сергей Федорович, доктор физико-математических наук, профессор, Восточно-Сибирская государственная академия образования, 664011, Иркутск, ул. Н. Набережная, 6 тел.: (3952)240435 (vin@math.isu.ru)

Казимиров Алексей Сергеевич, кандидат физико-математических наук, Восточно-Сибирская государственная академия образования, 664011, Иркутск, ул. Н. Набережная, 6 тел.: (3952)240435 тел.: (3952)242210 (a.kazimirov@gmail.com)

Vinokurov Sergey, East Siberian State Academy of Education, 6, N. Naberezhnaya St., Irkutsk, 664011 professor, Phone: (3952)240435 (vin@math.isu.ru)

Kazimirov Alexey, East Siberian State Academy of Education, 6, N. Naberezhnaya St., Irkutsk, 664011 Phone: (3952)240435 (a.kazimirov@gmail.com)