Math-Net.Ru

Общероссийский математический портал

А. В. Тарасов, Некоторые свойства групп инерции булевых бинюнктивных функций и индуктивный метод генерации таких функций, *Дискрет. матем.*, 2002, том 14, выпуск 2, 33–47

DOI: <https://doi.org/10.4213/dm239>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.196.121.252

26 апреля 2023 г., 16:55:40

Некоторые свойства групп инерции булевых бионктивных функций и индуктивный метод генерации таких функций

© 2002 г. А. В. Тарасов

Класс бионктивных булевых функций включает в себя функции, представимые в виде 2-КНФ. Задача перечисления таких функций от произвольного числа переменных в настоящее время не решена. В статье рассмотрены свойства групп инерции бионктивных функций в различных группах и приводится индуктивный метод порождения всех различных представителей классов геометрической эквивалентности бионктивных функций. На основе предложенного метода подсчитано количество бионктивных функций от 5, 6 и 7 переменных.

1. Введение

Одной из важных проблем дискретной математики является задача решения систем булевых уравнений. В общем случае данная задача является NP -трудной, однако, существует ряд классов полиномиально решаемых систем булевых уравнений. В частности, таковыми является класс систем уравнений, порождаемый бионктивными функциями [1–4]. Эти функции порождают системы уравнений без ограничений на выбор неизвестных, совместность которых распознается с линейной от длины записи сложностью [2, 4]. Класс бионктивных функций обозначим через Bi .

Класс Bi состоит из двоичных функций, представимых в виде 2-КНФ, то есть функций вида

$$f(x_1, x_2, \dots, x_n) = \bigwedge_{i=1}^t (x_{s_{i1}}^{a_{i1}} \vee x_{s_{i2}}^{a_{i2}}).$$

В [3] показано, что каждая такая функция имеет единственную, с точностью до выбора некоторых специфических сомножителей, минимальную 2-КНФ. Известны следующие оценки для числа $b(n)$ бионктивных функций от n переменных [4]:

$$n^2/2 \leq \log_2 b(n) \leq n^2.$$

Представляет интерес задача нахождения всех бионктивных функций от малого числа переменных.

С. А. Гизуновым (см. [5]) было подсчитано количество бионктивных функций от 3 и 4 переменных.

В первом параграфе настоящей статьи описаны свойства групп инерции биюнктивных функций в группе Джевонса, группе сдвигов и в симметрической группе.

Второй параграф посвящен формулировке и доказательству основной теоремы о классах эквивалентности биюнктивных функций, на основе которой строится алгоритм генерации. Показывается полиномиальная эквивалентность задачи распознавания эквивалентности биюнктивных функций в группе Джевонса известной задаче распознавания изоморфизма графов, доказывается полиномиальность задачи распознавания эквивалентности биюнктивных функций в группе сдвигов. Построен алгоритм генерации биюнктивных функций и результаты его работы по определению и подсчету различных параметров биюнктивных функций от 5, 6 и 7 переменных, а именно, их весу, мощности группы инерции и длине минимальной 2-КНФ.

2. Некоторые свойства групп инерции биюнктивных функций

Введем следующие обозначения. Пусть B_n — пространство двоичных векторов длины n , $n \geq 1$, Q_n , S_n и Σ_n — группы преобразований пространства B_n , а именно,

$$\Sigma_n = \{g_a: g_a(x) = x \oplus a, x \in B_n, a \in B_n\}$$

— группа сдвигов, S_n — группа перестановок координат векторов из B_n , изоморфная симметрической группе степени n ,

$$Q_n = \{h_{s,a}: s \in S_n, a \in B_n, h_{s,a}(x) = g_a(s(x)) = s(x) \oplus a\}$$

— группа Джевонса, изоморфная произведению групп S_n и Σ_n .

Симметрическую группу на произвольном конечном множестве A обозначим через $\text{Sym}(A)$.

Для произвольной булевой функции f и группы H преобразований пространства B_n обозначим

$$J_H(f) = \{h \in H: \forall x \in B_n f(h(x)) = f(x)\}$$

группу инерции функции f в группе H . В данном параграфе мы рассмотрим строение группы инерции биюнктивных функций в группах Q_n , S_n и Σ_n .

Пусть биюнктивная функция f задана сокращенной КНФ

$$f(x_1, x_2, \dots, x_n) = \bigwedge_{i=1}^t (x_{s_{i1}}^{a_{i1}} \vee x_{s_{i2}}^{a_{i2}}). \quad (1)$$

Для этой 2-КНФ аналогично тому, как это сделано в [2], определим ориентированный граф $G = (V, E)$, где

$$V = \{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n\}, \quad E = \{(x_{s_{i1}}^{a_{i1} \oplus 1}, x_{s_{i2}}^{a_{i2}}), (x_{s_{i2}}^{a_{i2} \oplus 1}, x_{s_{i1}}^{a_{i1}}), i = 1, \dots, t\}.$$

В соответствии с результатами [3] граф G — транзитивный орграф. Обозначим через $J_{Q_n}(f)$ группу инерции функции f в группе Q_n . Группа Q_n действует на множестве B_n , и существует очевидный изоморфизм этой группы в подгруппу группы перестановок вершин графа. Поэтому для краткости будем рассматривать действие группы Q_n на множестве V . Верна следующая лемма.

Лемма 1. *Группа инерции $J_{Q_n}(f)$ имеет вид*

$$J_{Q_n}(f) = \{g \in \text{Aut } G : g(\bar{u}) = \bar{g}(u) \forall u \in V\} = Q_n \cap \text{Aut } G, \quad (2)$$

где $\text{Aut } G$ — группа автоморфизмов графа G .

Доказательство. Пусть $M = \{g \in \text{Aut } G : g(\bar{u}) = \bar{g}(u) \forall u \in V\}$. Очевидно, что $J_{Q_n}(f) < \text{Aut } G$. Также ясно, что $J_{Q_n}(f) \subseteq M$. Покажем обратное включение. Подстановку $g \in M$ запишем в виде

$$g = \begin{pmatrix} x_1 & \dots & x_i & \dots & x_n & \bar{x}_1 & \dots & \bar{x}_i & \dots & \bar{x}_n \\ g(x_1) & \dots & g(x_i) & \dots & g(x_n) & g(\bar{x}_1) & \dots & g(\bar{x}_i) & \dots & g(\bar{x}_n) \end{pmatrix}$$

Для $i = 1, 2, \dots, n$ верно равенство $g(x_i) = x_{k_i}^{b_i}$, где $(k_1, \dots, k_n)$ — перестановка чисел $1, 2, \dots, n$. Тогда $g(\bar{x}_i) = x_{k_i}^{b_i \oplus 1}$. Обозначим через s перестановку $(k_1, \dots, k_n)$, а через b вектор $(b_1, \dots, b_n)$. Из сказанного выше следует, что $g(x_i^a) = x_{s(i)}^a \oplus a \oplus b_i$. Исходя из определения группы Q_n , заключаем, что $g \in Q_n$. Поскольку $g \in \text{Aut } G$, при действии подстановки g граф G , а следовательно, и КНФ (1) не изменяется. Значит, $g \in J_{Q_n}(f)$, и лемма доказана.

Перейдем к описанию некоторых подгрупп группы $J_{Q_n}(f)$. Опишем некоторую систему нормальных делителей этой группы. Заметим, что если $Y_1, \dots, Y_m$ — множества вершин сильно связанных компонент графа G , то $m = 2k$ и для всякого $i = 1, 2, \dots, m$ найдется j такое, что $\bar{Y}_i = Y_j$. Поэтому можно переупорядочить эти множества как $Y_1, \dots, Y_k, \bar{Y}_1, \dots, \bar{Y}_k$. Положим теперь $W_i = Y_i \cup \bar{Y}_i$, $1 \leq i \leq k$. Определим группу $Z_i = \text{Sym}(W_i) \cap Q_n$, $1 \leq i \leq k$. Очевидно, что группа Z_i изоморфна симметрической группе $\text{Sym}(|Y_i|)$. Будем говорить, что разбиение $H_1, \dots, H_k$ множества M инвариантно относительно группы $L < \text{Sym}(M)$, если

$$\forall h \in L \quad \forall H_i, 1 \leq i \leq k, \quad h(H_i) \in \{H_1, \dots, H_k\}.$$

Теорема 1. *Для группы $J_{Q_n}(f)$ верны следующие утверждения.*

- (а) *Разбиения $Y_1, \dots, Y_k, \bar{Y}_1, \dots, \bar{Y}_k$ и $W_1, \dots, W_k$ множества V инвариантны относительно группы $J_{Q_n}(f)$.*
- (б) *Группы Z_i , $1 \leq i \leq k$, нормальны в $J_{Q_n}(f)$.*
- (с) *Если $1 \leq i_1 \leq \dots \leq i_r \leq k$, то группа $Z_{i_1} + \dots + Z_{i_r}$ нормальна в $J_{Q_n}(f)$.*

Доказательство. Поскольку $J_{Q_n}(f) < \text{Aut } G$, любая сильно связанная компонента переходит в изоморфную ей. Поэтому разбиение $Y_1, \dots, Y_k, \bar{Y}_1, \dots, \bar{Y}_k$ инвариантно относительно группы $J_{Q_n}(f)$. Второе утверждение пункта (а) следует из леммы 1.

Докажем утверждение (б). Поскольку орграф G транзитивен, всякая его сильно связанная компонента является полным орграфом. Следовательно, $\text{Aut } G(Y_i) = Z_i$. Покажем, что $Z_i < \text{Aut } G$. Предположим, что $G(Y_j)$ — некоторая другая сильно связанная компонента графа. Возможны в точности два случая: в графе G нет ориентированного пути, соединяющего эти две компоненты, и в графе G есть ориентированный путь из Y_i в Y_j (из Y_j в Y_i), но нет обратного.

Для подстановки h из Z_i покажем, что при действии на множество V граф не изменится. В первом случае легко видеть, что подстановка h не изменяет дуги, инцидентные

вершинам из Y_i . Рассмотрим второй случай. Без ограничения общности можно считать, что в графе G есть ориентированный путь из Y_i в Y_j . В силу транзитивности графа

$$E \supset \{(u, v) : u \in Y_i, v \in Y_j\} = \{(h(u), v) : u \in Y_i, v \in Y_j\}.$$

Следовательно, $Z_i < \text{Aut } G$ и в силу леммы 1 $Z_i < J_{Q_n}(f)$. Докажем нормальность подгруппы Z_i . Для подстановки h из Z_i

$$h(Y_i) = Y_i, \quad h(\bar{Y}_i) = \bar{Y}_i, \quad g^{-1}hg(u) = g(h(g^{-1}(u)))$$

для всех $g \in J_{Q_n}(f)$ и $u \in Y_i$.

Если $g^{-1}(u) \in Y_i$, то в силу а) $g(Y_i) = Y_i$, и $g^{-1}hg \in Z_i$. С другой стороны, если $g^{-1}(Y_i) = Y_j$ или $g^{-1}(Y_i) = \bar{Y}_j$, то $g^{-1}(u) \in Y_j$ ($g^{-1}(u) \in \bar{Y}_j$). При $i \neq j$

$$g^{-1}hg(u) = g(h(g^{-1}(u))), \quad h(g^{-1}(u)) = g^{-1}(u), \quad g^{-1}hg(u) = u.$$

Если же $i = j$, то очевидно, что $g^{-1}hg(u) \in Y_i$, что и требовалось доказать. Отсюда, $g^{-1}Z_i g = Z_i$. Утверждение (с) следует из утверждения (b) очевидным образом. Теорема доказана.

Положим $Z = Z_1 + \dots + Z_k$. Следующий алгоритм находит систему образующих группы H по произвольной 2-КНФ функции f .

Алгоритм 1.

Вход: биюнктивная функция, заданная 2-КНФ (1).

Выход: список из не более $2k$ подстановок, представляющий систему образующих группы Z .

Метод. (1) Строим граф G 2-КНФ (1).

(2) Алгоритмом 5.4 из [6] получаем список сильно связанных компонент графа G .

(3) Выделяем пары инверсных компонент $Y_1, \dots, Y_k, \bar{Y}_1, \dots, \bar{Y}_k$ и строим разбиение $W_1, \dots, W_k$.

(4) Для $i = 1, 2, \dots, k$ выполняем следующие действия:

- если $|W_i| = 2$, то переходим к следующему множеству;
- если $|W_i| = 4$, то есть $Y_i = \{u_1^{(i)}, u_2^{(i)}\}$, то $g_1^{(i)} = (u_1^{(i)}, u_2^{(i)})(\bar{u}_1^{(i)}, \bar{u}_2^{(i)})$;
- если $|W_i| > 4$, $Y_i = \{u_1^{(i)}, \dots, u_{l_i}^{(i)}\}$, то

$$g_1^{(i)} = (u_1^{(i)}, u_2^{(i)})(\bar{u}_1^{(i)}, \bar{u}_2^{(i)}), \quad g_2^{(i)} = (u_1^{(i)}, \dots, u_{l_i}^{(i)})(\bar{u}_1^{(i)}, \dots, \bar{u}_{l_i}^{(i)}).$$

(5) Вывести все полученные подстановки.

Предложение 1. Алгоритм 1 находит систему образующих группы Z со сложностью $O(\max\{n, t\})$, где n — число переменных функции, а t — длина 2-КНФ.

Доказательство. Корректность алгоритма следует из того, что для решения задачи достаточно найти все сильно связанные компонента графа G и построить системы образующих на соответствующих симметрических группах. Поскольку граф G имеет $2n$ вершин и $2t$ дуг, в соответствии с теоремой 5.5 из [6] потребуется $O(\max\{n, t\})$ операций на поиск сильно связанных компонент в шаге 2 алгоритма. Трудоемкость остальных шагов, очевидно, не превысит указанной величины.

Рассмотрим теперь граф $R(G)$. Положим

$$K = \{g \in \text{Aut } R(G) \cap Q_k : |g(Y_i)| = |Y_i|\}.$$

Очевидно, что множество K образует подгруппу в $\text{Aut } R(G)$.

Теорема 2. *Группа K изоморфна факторгруппе группы $J_{Q_n}(f)$ по нормальному делителю Z .*

Доказательство. Построим гомоморфизм $\varphi: J_{Q_n}(f) \rightarrow K$ такой, что $\text{Ker } \varphi = Z$. Пусть

$$g \in J_{Q_n}(f), \quad g(Y_i) = Y_{r_i}^{a_i}, \quad g(\bar{Y}_i) = Y_{r_i}^{a_i \oplus 1}, \quad i = 1, 2, \dots, m.$$

Положим $\varphi(g)(Y_i) = Y_{r_i}^{a_i}$. Очевидно, что $|Y_i| = |Y_{r_i}^{a_i}|$, и, поскольку $g \in \text{Aut } G$, отображение $\varphi(g)$ — подстановка на множестве $\{Y_1, \dots, Y_k, \bar{Y}_1, \dots, \bar{Y}_k\}$, сохраняющая мощности элементов. Покажем, что $\varphi(g)$ — автоморфизм графа G .

Поскольку $g \in \text{Aut } G$, $g(E) = E$, для всех $(u, v) \in E$ справедливо включение $(g(u), g(v)) \in E$. Если при этом $u \in Y_i^a$, $v \in Y_j^b$, то $g(u) \in g(Y_i^a)$, $g(v) \in g(Y_j^b)$ и согласно построению графа $R(G)$ дуга $(g(Y_i^a), g(Y_j^b))$ лежит в множестве $ER(G)$. Значит $g(ER(G)) \subseteq ER(G)$. Аналогично доказывается обратное включение. Следовательно, $\varphi(g) \in \text{Aut } R(G)$, $\varphi(g) \in K$. Покажем, что φ — гомоморфизм.

Предположим, что $g, h \in J_{Q_n}(f)$ и $g(Y_i) = Y_j$, $h(Y_j) = Y_k$. Тогда $\varphi(gh)(Y_i) = Y_k$. С другой стороны, $\varphi(g)\varphi(h)(Y_i) = \varphi(h)(Y_j) = Y_k$. Поэтому φ — гомоморфизм, и $\varphi(J_{Q_n}(f)) < K$. Покажем, что φ — эпиморфизм.

Пусть $h(Y_i^a) = Y_{r_i}^{a \oplus b_i}$, $i = 1, \dots, k$, $a \in \{0, 1\}$. Если для некоторого i

$$Y_i^a = \{y_1^{(i)}, \dots, y_{l_i}^{(i)}\}, \quad Y_{r_i}^{a \oplus b_i} = \{z_1^{(r_i)}, \dots, z_{l_i}^{(r_i)}\},$$

то положим $g(y_j^{(i)}) = z_j^{(r_i)}$. Очевидно, что $g \in Q_n$. Докажем, что $g \in \text{Aut } G$. В противном случае существует дуга $(u, v) \in V$ такая, что $(g(v), g(u)) \notin E$. Тогда, если $u \in Y_i^a$, $v \in Y_j^b$, то $(h(Y_i^a), h(Y_j^b)) \notin ER(G)$ по определению графа $R(G)$, что противоречит тому, что h — автоморфизм $R(G)$.

Таким образом, φ — эпиморфизм. Найдем ядро $\text{Ker } \varphi$. Если g и h таковы, что $\varphi(g) = \varphi(h)$, то $g(Y_i^a) = h(Y_i^a)$ для $1 \leq i \leq k$, $a = 0, 1$. В этом случае легко видеть, что существует подстановка $q_i \in Z_i$ такая, что $g(q_i(u)) = h(u)$ для всех $u \in Y_i^a$. Но тогда $q_1 \dots q_k g = h$. Поэтому $\text{Ker } \varphi < Z$. Обратное очевидно, и по теореме о гомоморфизме групп $K \cong J_{Q_n}(f)/Z$.

Следствие 1. *В условиях теоремы 2 группа $J_{Q_n}(f)$ изоморфна прямому произведению $K \times Z$.*

Аналогично приведенным выше результатам можно сформулировать утверждения, касающиеся групп инерции бионктивных функций в группе подстановок. Для этого введем обозначения

$$P(Y_i^a) = \{x_r \in Y_i^a\}, \quad N(Y_i^a) = \{x_r : \bar{x}_r \in Y_i^a\}, \quad i = 1, 2, \dots, k, \quad a = 0, 1.$$

Очевидно, что $P(Y_i^a) = N(Y_i^{a \oplus 1})$. Группа $J_{S_n}(f)$ включает в себя те и только те подстановки из группы $J_{Q_n}(f)$, которые сохраняют степени литералов, то есть $J_{S_n}(f) = \{(\sigma, 0) \in J_{Q_n}(f)\}$. Аналогично, $J_{\Sigma_n}(f) = \{(\varepsilon, \beta) \in J_{Q_n}(f)\}$. Легко видеть, что $J_{S_n}(f) * J_{\Sigma_n}(f) < J_{Q_n}(f)$. Обратное включение может быть неверным, что иллюстрирует пример функции $f(x_1, x_2) = x_1 \vee \bar{x}_2$.

Теорема 3. Для группы $J_{S_n}(f)$ верны следующие утверждения.

Разбиение $P(Y_1), \dots, P(Y_k), P(\tilde{Y}_1), \dots, P(\tilde{Y}_k)$ множества V инвариантно относительно группы $J_{S_n}(f)$.

Группы $\text{Sym}(P(Y_i^a))$, $1 \leq i \leq k$, нормальны в $J_{S_n}(f)$.

Сумма любых подгрупп из предыдущего пункта нормальна в $J_{S_n}(f)$.

Доказательство теоремы проводится аналогично доказательству теоремы 1.

Группу $\text{Sym}(P(Y_1)) + \dots + \text{Sym}(P(Y_k)) + \text{Sym}(P(\tilde{Y}_1)) + \dots + \text{Sym}(P(\tilde{Y}_k))$ обозначим через U . Верно следующее утверждение.

Предложение 2. Существует алгоритм сложности $O(\max\{n, t\})$, где n — число переменных функции, а t — длина 2-КНФ, который строит систему образующих группы U .

Положим $U' = \{g \in \text{Sym}(V) : \exists h \in U : g(x) = h(x), g(\bar{x}) = h(\bar{x}) \forall x \in X\}$. Ясно, что U' — нормальный делитель группы $J_{S_n}(f)$. Пусть L — группа автоморфизмов графа $R(G)$, сохраняющих для всех вершин значения $P(Y_i^a)$ и $N(Y_i^{a \oplus 1})$.

Теорема 4. Справедливо соотношение $L \cong J_{S_n}(f)/U'$.

Доказательства предложения 2 и теоремы 4 полностью аналогичны доказательствам аналогичных утверждений для $J_{Q_n}(f)$.

Перейдем к исследованию группы $J_{S_n}(f)$. Эта группа является абелевой и, кроме того, она является подпространством в D_n . Поэтому для ее полного описания достаточно лишь найти ее базис. Введем определение.

Определение 1. Сильно связная компонента произвольного орграфа называется изолированной, если она является компонентой связности неориентированного графа, полученного из исходного путем отмены ориентации дуг.

Для краткости в дальнейшем будем считать, что в сильно связных компонентах графа G литералы имеют одинаковые степени.

Пусть $M \subseteq V$. Положим $\text{Ind}(M) = \{i : x_i \in M \text{ либо } \bar{x}_i \in M\}$.

Лемма 2. Пусть $f(x_1 \oplus b_1, \dots, x_n \oplus b_n) = f(x_1, \dots, x_n)$ и $M = \{i : b_i = 1\}$. Тогда в графе G найдутся сильно связные компоненты $Y_{j_1}, \dots, Y_{j_r}$ такие, что $M = \text{Ind}(Y_{j_1} \cup \dots \cup Y_{j_r})$.

Доказательство. Предположим, что для некоторой сильно связной компоненты Y множество $M \cap \text{Ind}(Y)$ непусто, но при этом $\text{Ind}(Y)$ не содержится в M целиком. Без ограничений общности будем считать, что $Y = \{x_1, \dots, x_r\}$. Тогда в сокращенную 2-КНФ функции f входит произведение

$$\varphi(x_1, \dots, x_r) = \bigwedge_{1 \leq i < j \leq r} (x_i \oplus x_j \oplus 1).$$

Предположим, что для вектора $b = (b_1, \dots, b_n)$ выполнены соотношения

$$b_1 = 0, \dots, b_q = 0, b_{q+1} = 1, \dots, b_r = 1, \quad q < r.$$

Тогда для всякого выполняющего вектора функции f вида $a = (a_1, \dots, a_n)$ такого, что $\varphi(a_1, \dots, a_n) = 1$

$$1 = f(a_1, \dots, a_n) = f(a_1, \dots, a_q, a_{q+1} \oplus 1, \dots, a_r \oplus 1, a_{r+1} \oplus b_{r+1}, \dots, a_n \oplus b_n).$$

Следовательно, $\varphi(a_1, \dots, a_q, a_{q+1} \oplus 1, \dots, a_r \oplus 1) = 1$, откуда, $a_i = a_j$, $1 \leq i < j \leq q$, $a_i = a_j$, $q+1 \leq i < j \leq r$, $a_i \neq a_j$ при $1 \leq i \leq q$, $q+1 \leq j \leq r$. С другой стороны, должно выполняться условие $a_1 = \dots = a_r$, что противоречит нашему предположению. Значит, $\text{Ind}(Y) \subset M$ и отсюда легко следует утверждение леммы. Лемма доказана.

Для всякого $M \subset \{1, 2, \dots, n\}$ через $\chi(M)$ обозначим характеристический вектор этого множества.

Теорема 5. *Группа $J_{\Sigma_n}(f)$ является подпространством в B_n , базисом которого являются все различные векторы вида $\chi(\text{Ind}(Y_j))$, $j \in A$, где Y_j , $j \in A$, — все изолированные сильно связанные компоненты графа G .*

Доказательство. Заметим, что если Y — изолированная сильно связанная компонента, то и $\bar{Y}$ — изолированная, причем $\text{Ind}(Y) = \text{Ind}(\bar{Y})$. Пусть $Y = \{x_1, \dots, x_r\}$. Тогда имплицентай f будет функция

$$\varphi(x_1, \dots, x_r) = \bigwedge_{1 \leq i < j \leq r} (x_i \oplus x_j \oplus 1),$$

и имеет место равенство

$$f(x_1, \dots, x_n) = \varphi(x_1, \dots, x_r) h(x_{r+1}, \dots, x_n).$$

Поэтому при инвертировании всех переменных $x_1, \dots, x_r$ функция не изменится, и $\chi(\text{Ind}(Y)) \in J_{\Sigma}(f)$. С другой стороны, согласно лемме 2 для всякого вектора $b \in J_{\Sigma}(f)$ найдутся сильно связанные компоненты $Y_1, \dots, Y_k$ такие, что

$$b = \chi(Y_1 \cup \dots \cup Y_k) = \chi(Y_1) \oplus \dots \oplus \chi(Y_k).$$

Покажем, что эти сильно связанные компоненты — изолированные компоненты. Предположим, что Y — не изолированная компонента и существует вектор $b \in J_{\Sigma_n}(f)$ такой, что $\text{Ind}(Y) \cap M \neq \emptyset$, $M = \{i : b_i = 1\}$. Представим функцию f в виде

$$f(x_1, \dots, x_n) = \varphi(x_1, \dots, x_n) h(x_1, \dots, x_n),$$

где функция h является произведением тех и только тех дизъюнктов из сокращенной КНФ (1), которые не соответствуют дугам компонент Y и $\bar{Y}$. В этом случае множество $\{x_1, \dots, x_r\}$ не является множеством вершин сильно связанной компоненты графа функции h . С другой стороны, функция h существенно зависит от некоторых переменных из $x_1, \dots, x_r$. Отсюда следует, что функция h существенно зависит от всех переменных $x_1, \dots, x_r$. Пусть в графе G есть дуги из Y в x_{r+1} . Тогда функцию f можно представить в виде

$$f(x_1, \dots, x_n) = \varphi(x_1, \dots, x_n) \& (\bar{x}_1 \vee x_{r+1}) \& \dots \& (\bar{x}_r \vee x_{r+1}) \& g'(x_1, \dots, x_n).$$

Поскольку $b \in J_{\Sigma}(f)$ и $b_1 = \dots = b_r = 1$, при $b_{r+1} = 0$ получим, что

$$\begin{aligned} f(x_1 \oplus b_1, \dots, x_n \oplus b_n) \\ = \varphi(x_1, \dots, x_n) \& (x_1 \vee x_{r+1}) \& \dots \& (x_r \vee x_{r+1}) \& h'(x_1 \oplus b_1, \dots, x_n \oplus b_n). \end{aligned}$$

Следовательно, функция x_{r+1} является имплицентай f , что противоречит тому, что в записи (1) все имплиценты простые. Если же $b_{r+1} = 1$, то легко видеть, что вершины $x_1, \dots, x_r, x_{r+1}$ графа G образуют сильно связанную компоненту, что опять приводит нас к противоречию с условием. Следовательно, Y — изолированная компонента. Отсюда легко следует утверждение теоремы. Теорема доказана.

Легко видеть, что приведенный ниже алгоритм 2 находит базис пространства $J_{\Sigma_n}(f)$ со сложностью $O(n^3)$, не превосходящей $O(n^3)$.

Алгоритм 2.

Вход: биюнктивная функция f от n переменных, записанная в виде 2-КНФ (1).

Выход: совокупность n -мерных двоичных векторов, образующих базис пространства $J_{\Sigma_n}(f)$.

Метод. (1) Строим оргграф $G = (V, E)$ для 2-КНФ функции f .

(2) Алгоритмом 5.4 из [6] находим сильно связанные компоненты графа G .

(3) Пусть $Y_1, \dots, Y_k, \bar{Y}_1, \dots, \bar{Y}_k$ — все сильно связанные компоненты. Формируем множества $E(Y_1), \dots, E(Y_k), E(\bar{Y}_1), \dots, E(\bar{Y}_k)$ дуг графа по следующему принципу: если начало и конец дуги принадлежат одной сильно связанной компоненте, то пополняем ею соответствующее множество из $E(Y_1), \dots, E(Y_k), E(\bar{Y}_1), \dots, E(\bar{Y}_k)$, выбрасывая ее из E , а если начало и конец дуги лежат в разных компонентах, то из списка компонент удаляем эти инверсные к ним компоненты, а также удаляем соответствующие множества дуг. Кроме того, из E удаляем все дуги, инцидентные вершинам из этих компонент.

(4) В результате получим список изолированных сильно связанных компонент, после чего составляем базис $J_{\Sigma_n}(f)$ согласно теореме 5.

Результаты данного параграфа дают возможность описывать строение групп $J_{Q_n}(f)$, $J_{S_n}(f)$, $J_{\Sigma_n}(f)$, причем в первом и втором случаях можно эффективно задать систему нормальных делителей, а в третьем указать базис соответствующего пространства.

3. Индуктивный метод генерации классов геометрической эквивалентности биюнктивных функций

Пусть $\text{Bi}(n)$ — множество биюнктивных функций от n переменных. Для произвольной булевой функции $f(x_1, \dots, x_n)$ через $[f]$ будем обозначать класс функций, эквивалентных функции f относительно группы Q_n .

Пусть $\text{Bi}(n-1) = [h_1] \cup [h_2] \cup \dots \cup [h_m]$, где $[h_i] \neq [h_j]$ при $i \neq j$ и $n \geq 2$. Через $g_1, \dots, g_m$ обозначим функции $h_1, \dots, h_m$, рассматриваемые как функции от переменных с несущественной переменной x_n . Верна следующая теорема.

Теорема 6. Для множества $\text{Bi}(n)$ справедлива формула

$$\begin{aligned} \text{Bi}(n) = & [g_1] \cup \dots \cup [g_m \cup [x_n g_1] \cup \dots \cup [x_n g_m] \cup \bigcup_{i=1}^{n-1} \bigcup_{j=1}^m [(x_n \oplus x_i) g_j] \\ & \cup \bigcup_{j=1}^m \bigcup_{k=1}^{n-1} \bigcup_{1 \leq i_1 < \dots < i_k \leq n-1} \bigcup_{a_1, \dots, a_k} \left[\bigwedge_{l=1}^k (x_{i_l}^{a_l} \vee x_n) g_j \right], \quad (3) \end{aligned}$$

где среди перечисленных классов не обязательно все различны.

Доказательство. Как видно из формулы (3), все множество порождаемых классов можно разбить на четыре группы, а именно,

$$\begin{aligned} M_1 &= [g_1] \cup \dots \cup [g_m], \\ M_2 &= [x_n g_1] \cup \dots \cup [x_n g_m], \\ M_3 &= [(x_n \oplus x_1) g_1] \cup \dots \cup [(x_n \oplus x_1) g_m], \\ M_4 &= \bigcup_{j=1}^m \bigcup_{k=1}^{n-1} \bigcup_{1 \leq i_1, \dots, i_k \leq n-1} \bigcup_{a_1, \dots, a_k} \left[\bigwedge_{l=1}^k (x_{i_l}^{a_l} \vee x_n) g_j \right]. \end{aligned}$$

Пусть $f(x_1, \dots, x_n) \in \text{Bi}(n)$. Покажем, что f лежит в одном из $M_1, \dots, M_4$.

Если f имеет несущественную переменную x_k , то очевидно, что $f \in M_1$.

Пусть функция f имеет имплиценту вида x_i^a . Тогда функцию f можно представить в виде $f = x_i^a \& f'$, где f' не зависит существенно от x_i . Если провести замену переменных $x_i^a \rightarrow x_n$, что соответствует преобразованию в группе Q_n , и воспользоваться результатом предыдущего пункта, то получим, что $f \in M_2$.

Предположим теперь, что f не имеет несущественных переменных и имплицент вида x_i^a . Будем считать, что f задана формулой (1), причем в правой части все имплиценты простые. Построим граф G 2-КНФ из правой части (1). Рассмотрим два случая.

Пусть граф G имеет сильно связанные компоненты. В соответствии с результатами [3] это означает, что у функции f есть имплицента вида $x_i \oplus x_j$ или $x_i \oplus x_j \oplus 1$. Предположим, что имеет место первый случай, поскольку второй рассматривается аналогично. У функции f проведем замену переменных $x_j \rightarrow x_n$. Полученная таким образом функция f' эквивалентна f относительно группы Q_n , и ее можно записать в виде $f' = (x_n \oplus x_i) f''$, где функция f'' не зависит существенно от x_n . Тогда, в соответствии с рассмотренным выше первым пунктом, для некоторого j , $1 \leq j \leq m$, функция $f'' \in [g_j]$. Но тогда $f' \in [(x_n \oplus x_i) g_j]$, $1 \leq k \leq n-1$, а значит и $f \in [(x_n \oplus x_k) g_j] \subset M_3$, что и требовалось доказать.

Пусть теперь граф G не имеет сильно связанных компонент. В этом случае граф имеет начальные и конечные вершины. Будем считать, что x_n — конечная вершина графа. Легко видеть, что вершины x_i и $\bar{x}_i$ не могут быть одновременно смежны с x_n , поскольку в этом случае мы получим, что f имеет простую имплиценту длины 1 и попадем в условия второго пункта, рассмотренного выше. Предположим для определенности, что $x_1, x_2, \dots, x_k$ — все вершины, смежные с x_n . Тогда функцию f можно записать в виде

$$f = \bigwedge_{i=1}^k (\bar{x}_i \vee x_n) f',$$

где функция f' не зависит существенно от x_n . В этом случае найдется такая функция g_j , что $f'' \in [g_j]$, $1 \leq j \leq m$. Это означает, что существуют такие подстановка s степени $n-1$ и вектор $b = (b_1, \dots, b_{n-1})$, что

$$f'(x_{s(1)} \oplus b_1, \dots, x_{s(n-1)} \oplus b_{n-1}) = g_j.$$

Но тогда очевидно, что

$$f(x_{s(1)} \oplus b_1, \dots, x_{s(n-1)} \oplus b_{n-1}, x_n) = \bigwedge_{i=1}^k (x_{s(i)}^{b_i \oplus 1} \vee x_n) g_j \in M_4,$$

что и требовалось доказать.

Пользуясь доказанной теоремой, можно порождать биюнктивные функции от n переменных, перечисляя только представителей классов эквивалентности относительно группы Q_n . Для этого достаточно иметь все представители классов геометрической эквивалентности от $n - 1$ переменной. Далее можно построить систему представителей из правой части (3), проверить их попарно на эквивалентность и удалить повторяющиеся классы.

Прежде, чем приступить к изложению алгоритма, докажем некоторые вспомогательные утверждения. Как следует из предыдущих результатов, задача проверки эквивалентности биюнктивных функций относительно преобразований группы Q_n сводится к задаче определения существования изоморфизма специального вида между соответствующими графами. В настоящее время неизвестны полиномиальные алгоритмы распознавания изоморфизма графов. Более того, не доказана также NP -полнота этой задачи (см., например, [7]). Тем не менее, справедлива следующая теорема.

Теорема 7. *Задача проверки эквивалентности биюнктивных функций, заданных произвольными 2-КНФ, относительно преобразований групп S_n и Q_n полиномиально эквивалентна задаче проверки изоморфизма графов. Задача распознавания эквивалентности биюнктивных функций, заданных произвольными 2-КНФ, относительно преобразований группы S_n полиномиальна.*

Доказательство. Сначала покажем, что задача проверки изоморфизма графов полиномиально сводится к задаче проверки эквивалентности биюнктивных функций в группах S_n и Q_n . Пусть $G_1 = (V, E_1)$, $G_2 = (V, E_2)$ — неориентированные графы с множеством вершин $V = \{v_1, \dots, v_n\}$ и множествами ребер E_1 и E_2 без петель и кратных дуг. По этим графам построим биюнктивные функции f_1 и f_2 от n переменных.

При $E_1 = \{\{v_{i1}, v_{i2}\}, i = 1, 2, \dots, t\}$ и $E_2 = \{\{v_{j1}, v_{j2}\}, j = 1, 2, \dots, t\}$ положим

$$f_1 = \bigwedge_{i=1}^t (x_{i1} \vee x_{i2}), \quad f_2 = \bigwedge_{j=1}^t (x_{j1} \vee x_{j2}). \quad (4)$$

Очевидно, что функции f_1 и f_2 монотонны. Ясно, что они эквивалентны относительно группы S_n тогда и только тогда, когда они эквивалентны относительно группы Q_n . Кроме того, легко видеть, что формулы в правой части (4) являются минимальными и сокращенными 2-КНФ. Поэтому любое преобразование, переводящее f_1 в f_2 , является перестановкой переменных в формулах (4), а следовательно, соответствует некоторому изоморфизму графов G_1 и G_2 . В то же время, каждый изоморфизм графов G_1 и G_2 соответствует перестановке переменных в формулах (4). Все использованные преобразования являются, очевидно, полиномиальными. Следовательно, задача проверки изоморфизма графов полиномиально сводится к задаче распознавания эквивалентности биюнктивных функций в группах S_n и Q_n .

Покажем обратное. Сначала рассмотрим задачу распознавания эквивалентности биюнктивных функций в группе Джевонса.

В [7] в качестве примера задачи, полиномиально эквивалентной задаче распознавания изоморфизма графов, приводится задача распознавания изоморфизма конечных моделей, где под конечной моделью понимается совокупность из конечного множества и некоторого набора отношений на нем.

Пусть f_1 и f_2 заданы произвольными 2-КНФ от n переменных. В соответствии с результатами теорем 1.9 и 1.11 из [3], мы можем с полиномиальной сложностью построить

их сокращенные КНФ. Предположим, что

$$f_1(x_1, \dots, x_n) = \bigwedge_{i=1}^t (x_{s_i1}^{a_i1} \vee x_{s_i2}^{a_i2}),$$

$$f_2(x_1, \dots, x_n) = \bigwedge_{j=1}^t (x_{r_j1}^{b_j1} \vee x_{r_j2}^{b_j2}).$$

Пусть $G_1 = (V, E_1)$, $G_2 = (V, E_2)$ — графы их сокращенных КНФ,

$$V = \{x_1, \dots, x_n, \bar{x}_1, \dots, \bar{x}_n\},$$

$$E_1 = \{(x_{s_i1}^{a_i1 \oplus 1}, x_{s_i2}^{a_i2}), (x_{s_i2}^{a_i2 \oplus 1}, x_{s_i1}^{a_i1}), i = 1, \dots, t\},$$

$$E_2 = \{(x_{r_j1}^{b_j1 \oplus 1}, x_{r_j2}^{b_j2}), (x_{r_j2}^{b_j2 \oplus 1}, x_{r_j1}^{b_j1}), j = 1, \dots, t\}.$$

Построим две конечные модели $M_1 = (V, R_{11}, R_{12})$ и $M_2 = (V, R_{21}, R_{22})$, полагая

$$R_{11} = R_{21} = R_1 = \{(x_i, \bar{x}_i), (\bar{x}_i, x_i), i = 1, \dots, t\}, \quad R_{12} = E_1, \quad R_{21} = E_2.$$

Легко видеть, что всякий изоморфизм σ моделей M_1 и M_2 является изоморфизмом графов G_1 и G_2 . В силу того, что σ сохраняет отношение R_1 , следует, что $\sigma(\bar{u}) = \bar{\sigma}(u)$ для всех $u \in V$. Значит, $\sigma \in Q_n$.

Далее, очевидно, что всякое преобразование $\sigma \in Q_n$, переводящее f_1 в f_2 , является изоморфизмом моделей M_1 и M_2 . Кроме того ясно, что все произведенные преобразования задач друг в друга полиномиальны.

Из приведенных рассуждений следует, что задача распознавания эквивалентности биюнктивных функций в группе Джевонса при задании их 2-КНФ полиномиально эквивалентна задаче распознавания изоморфизма графов.

Задача распознавания эквивалентности биюнктивных функций в группе S_n рассматривается аналогично случаю Q_n , однако, здесь в конечные модели M_1 и M_2 следует добавить еще по два одноместных отношения:

$$R_{13} = R_{23} = R_3 = \{(x_i), i = 1, \dots, t\},$$

$$R_{14} = R_{24} = R_4 = \{(\bar{x}_i), i = 1, \dots, t\}.$$

Для доказательства полиномиальности задачи распознавания эквивалентности биюнктивных функций относительно преобразований группы Σ_n достаточно привести полиномиальный алгоритм.

Пусть функции f_1 и f_2 заданы сокращенными КНФ. Без ограничений общности можно полагать, что все простые имплиценты этих функций имеют длину 2. Построим графы G_1 и G_2 этих функций. Предположим сначала, что эти графы не имеют сильно связанных компонент. В этом случае согласно теореме 5 группы инерции функций f_1 и f_2 в группе Σ_n тривиальны и, следовательно, если эти функции эквивалентны относительно группы Σ_n , существует единственный вектор $a = (a_1, \dots, a_n) \in V_n$ такой, что

$$f_1(x_1 \oplus a_1, \dots, x_n \oplus a_n) = f_2(x_1, \dots, x_n).$$

Поскольку графы не имеют сильно связанных компонент, у них есть начальные и конечные вершины. Пусть для простоты $x_1, \dots, x_k$ — начальные вершины графа G_1 , тогда

$\bar{x}_1, \dots, \bar{x}_k$ — его конечные вершины. Если функция f_2 эквивалентна функции f_1 , начальными вершинами графа G_2 должны быть вершины вида $x_1^{a_1}, \dots, x_k^{a_k}$, конечными — их отрицания. В противном случае функции f_1 и f_2 не эквивалентны относительно группы Σ_n . Если же данное условие выполнено, то первыми k координатами вектора, преобразующего f_1 в f_2 будут $a_1, \dots, a_k$. На следующем этапе из графов G_1 и G_2 получаем графы G'_1 и G'_2 , выбросив начальные и конечные вершины и инцидентные им дуги, после чего повторяем предыдущий этап для графов с $2n - 2k$ вершинами. В конце концов мы либо придем к противоречию, либо построим вектор $a = (a_1, \dots, a_n) \in V_n$ такой, что $f_1(x_1 \oplus a_1, \dots, x_n \oplus a_n) = f_2(x_1, \dots, x_n)$. В силу того, что максимальное число дуг в исходных графах не превосходит $4n^2$, общая трудоемкость оценивается величиной $O(n^3)$, что является полиномом от длины записи каждой 2-КНФ.

Предположим теперь, что графы G_1 и G_2 имеют сильно связные компоненты. В этом случае достаточно сравнить компоненты по содержащимся в них литералам и в случае их соответствия провести редукцию обоих графов путем склеивания вершин, входящих в сильно связную компоненту. После этого можно провести описанную выше процедуру. Если же функции имеют простые имплиценты длины 1, их тоже необходимо сравнить, а потом произвести описанные действия. Легко видеть, что во всех случаях трудоемкость оценивается как $O(n^3)$ и, следовательно, полиномиально зависит от длины записи задачи. Теорема доказана.

Рассмотрим метод распознавания эквивалентности биконъюнктивных функций в группе Джевонса. Для сокращения перебора всех $2^n n!$ преобразований группы Q_n воспользуемся разновидностью подхода, предложенного в [7]. Пусть $G_1 = (V, E_1)$, $G_2 = (V, E_2)$ — графы минимальных 2-КНФ функций f_1 и f_2 . Будем считать, что эти функции не имеют простых имплицентов длины 1, а их графы — нетривиальных сильно связных компонент (в противном случае можно провести очевидную конденсацию графа, объединяя вершины, входящие в сильно связную компоненту, в одну). Для каждой вершины v обоих графов определим четырехмерный вектор параметров $r(v) = (k(v), l(v), p(v), q(v))$, где $k(v)$ — полустепень захода вершины v , $l(v)$ — полустепень исхода вершины v , $p(v)$ и $q(v)$ — число таких вершин u , для которых существуют ориентированные пути из u в v и из v в u , соответственно. Очевидно, что если $r(v) = (k(v), l(v), p(v), q(v))$, то $r(\bar{v}) = (l(v), k(v), q(v), p(v))$.

Будем говорить, что $r(u) \leq r(v)$, если $k(u) \leq k(v)$, либо $l(u) \leq l(v)$ при $k(u) = k(v)$, либо $p(u) \leq p(v)$ при $k(u) = k(v)$ и $l(u) = l(v)$, либо $q(u) \leq q(v)$ при $k(u) = k(v)$ и $l(u) = l(v)$, $p(u) = p(v)$.

Пусть $R_1 = (r_1(x_1), \dots, r_1(\bar{x}_n))$ и $R_2 = (r_2(x_1), \dots, r_2(\bar{x}_n))$ — соответствующие таблицы наборов параметров вершин графов G_1 и G_2 , а $S(R_1)$, $S(R_2)$ — те же таблицы, но отсортированные по возрастанию. Очевидно следующее утверждение.

Лемма 3. Если функции f_1 и f_2 эквивалентны относительно преобразований группы Q_n , то $S(R_1) = S(R_2)$. Кроме того, для всякого $\sigma \in Q_n$, преобразующего f_1 в f_2 , и всех $v \in V$ выполнено условие

$$r_2(\sigma(v)) = r_1(v). \quad (5)$$

Пусть таблицы $S(R_1)$ и $S(R_2)$ совпадают, и $S(R_1) = (r(u_1), \dots, r(u_{2n}))$, где $u_1, \dots, u_{2n}$ — некоторая перестановка элементов V . Разобьем все множество вершин графа G_1 на подмножества с одинаковыми значениями параметрического вектора. Это разбиение будет иметь вид

$$V = A_1 \cup A_2 \cup \dots \cup A_m \cup B_1 \cup \dots \cup B_s \cup C_1 \cup \dots \cup C_s,$$

где все вершины из множества A_i имеют параметрические векторы вида (k, k, p, p) и входят в эти множества вместе со своим отрицаниями, а в множества $C_1, \dots, C_s$ входят отрицания вершин из $B_1, \dots, B_s$, соответственно. Через $a_1, \dots, a_m$ обозначим мощности множеств $A_1, \dots, A_m$, а через $b_1, \dots, b_s$ — мощности множеств $B_1, \dots, B_s$. Легко видеть, что объем перебираемых вариантов составит

$$(a_1/2)! \dots (a_m/2)! b_1! \dots b_s!.$$

Наличие соотношения $a_1 + \dots + a_m + 2(b_1 + \dots + b_s) = 2n$ позволяет заключить, что трудоемкость проверки может быть существенно сокращена.

Рассмотрим теперь вопрос об инвариантах бионктивных функций, где под инвариантами будем понимать такие параметры, которые постоянны на всех функциях из класса эквивалентности относительно группы Джевонса. Сформулируем основное утверждение об инвариантах бионктивных функций.

Лемма 4. Пусть f и g — бионктивные функции от n переменных, эквивалентные относительно преобразований группы Q_n . Тогда

- (1) $\|f\| = \|g\|$;
- (2) функции f и g имеют сокращенные 2-КНФ одинаковой длины;
- (3) функции f и g имеют минимальные 2-КНФ одинаковой длины;
- (4) функции f и g имеют одинаковое число простых имплициент длин 1 и 2;
- (5) графы сокращенных (минимальных) 2-КНФ функций f и g имеют одинаковое число сильно связанных компонент, причем наборы мощностей этих компонент одинаковы;
- (6) графы сокращенных (минимальных) 2-КНФ функций f и g имеют одинаковое число начальных, конечных и проходных вершин;
- (7) перманенты матриц смежности графов сокращенных и минимальных 2-КНФ функций f и g равны между собой.

Доказательство. Утверждение (1) следует из общей теории булевых функций, а (2)–(6) — из результатов этого параграфа. Поскольку графы сокращенных (минимальных) 2-КНФ функций f и g изоморфны, матрицы смежности отличаются только перестановкой строк и столбцов. Это означает, что перманенты этих матриц равны.

Перейдем к изложению алгоритма генерации представителей классов эквивалентности бионктивных функций. Легко видеть, что все булевы функции от двух переменных бионктивны. На каждой итерации алгоритма на вход подаются таблицы истинности представителей классов от $n - 1$ переменных. Затем из них образуются таблицы истинности представителей классов из правой части (3). В результате, если на вход подавалось t таблиц истинности, в результате мы получим $N = nt + m3^{n-1}$ представителей классов эквивалентности, поскольку в множествах M_1, M_2 лежит по t классов, в M_3 и M_4 — по $(n - 1)t$ и $t(3^{n-1} - 1)$ классов, соответственно. Трудоемкость порождения представителей составляет $T_1 = 2^n N$. В худшем случае, когда все представители попарно неэквивалентны, проверка представителей на эквивалентность потребует

$$T_2 = 2^n |Q_n| \binom{N}{2} = \binom{N}{2} n! 2^{2n} = O(2^{2n^2})$$

операций с битами. Нетрудно заметить, что трудоемкость предложенного алгоритма существенно меньше трудоемкости полного перебора всех булевых функций с проверкой на бижонктивность, составляющей, как минимум, 2^{2^n+n} элементарных операций.

Трудоемкость второго этапа может быть существенно сокращена при проверке на эквивалентность только функций, обладающих одинаковыми наборами инвариантов. Если мы имеем k множеств представителей с одинаковыми наборами инвариантов мощностей $r_1, \dots, r_k$, то количество проверяемых пар вместо $\binom{N}{2}$ составит

$$R = \binom{r_1}{2} + \dots + \binom{r_k}{2}.$$

В процессе реализации предложенного алгоритма для генерации бижонктивных функций от 5, 6, 7 переменных применение указанных идей сократило время работы программы более, чем в 10 раз.

Результирующий алгоритм имеет следующий вид.

Алгоритм 3 (получение представителей классов геометрической эквивалентности бижонктивных функций от n переменных).

Вход: набор таблиц истинности представителей классов эквивалентности бижонктивных функций $h_1, \dots, h_m$ от $n-1$ переменных (m двоичных векторов длины 2^{n-1}).

Выход: набор таблиц истинности представителей классов эквивалентности бижонктивных функций от n переменных.

Метод. (1) Составляем m таблиц истинности функций $g_1, \dots, g_m$ (m векторов длины 2^n).

(2) По формуле (3) строим представителей классов эквивалентности. Получаем N векторов длины 2^n (где $N = 2m + m3^{n-1}$).

(3) Сортируем полученные векторы по весам.

(4) Для каждой таблицы истинности строим сокращенную 2-КНФ путем проверки всевозможных фиксаций одной или двух переменных.

(5) По полученным в п. 4 сокращенным 2-КНФ строим графы, вычисляем мощности и количество сильно связанных компонент, число начальных, конечных и проходных вершин графов.

(6) Строим минимальные 2-КНФ, вычисляем их длины.

(7) Разбиваем множество таблиц истинности на группы, в которых все функции обладают одинаковым набором параметров в соответствии с леммой 3.

(8) Внутри каждой группы производим попарное сравнение функций на эквивалентность путем перебора элементов группы Q_n в соответствии с формулой (5).

Приведенный алгоритм был реализован для значений $n = 3, 4, 5, 6, 7$, после чего для каждого представителя была подсчитана мощность соответствующего класса и найдено число бижонктивных функций. Проведенный эксперимент подтвердил известные результаты для $n = 3, 4$, кроме того, было получено число бижонктивных функций от 5, 6, 7 переменных, что ранее было неизвестно.

Таблица 1. Таблица параметров классов $Bi(n)$

n — число переменных	3	4	5	6	7
$b(n)$	166	4170	224716	24445368	5167757614
число классов	14	45	196	1360	15631
макс. длина мин. КНФ	3	6	10	15	21
средняя длина мин. КНФ	2.21	3.55	5.25	7.23	13.19

4. Заключение

В статье описаны некоторые свойства групп инерции бионктивных функций в различных группах. Приведен индуктивный метод построения классов геометрической эквивалентности бионктивных функций, на основе приведенного метода подсчитано число бионктивных функций от 5, 6 и 7 переменных, что ранее было неизвестно.

Список литературы

1. Schaefer T., Complexity of satisfiability problems. *Proc. 10 Annual ACM Symposium on Theory of Computing* 1978, 216–226.
2. Данцин Е. Я., Алгоритмика задачи выполнимости. *Вопросы киберн.* (1987) **131**, 7–21.
3. Тарасов А. В., О свойствах функций, представимых в виде 2-КНФ. *Дискретная математика* (2001) **13**, №4, 99–115.
4. Горшков С. П., О пересечении классов мультиафинных, бионктивных слабо положительных и слабо отрицательных булевых функций. *Обзорение прикладной и промышленной математики* (1997) **4**, №2, 238–259.
5. Гизунов С. А., Носов В. А., О классификации всех булевых функций от 4-х переменных по классам Шефера. *Обзорение прикладной и промышленной математики* (1995) **2**, №3, 440–467.
6. Ахо А., Хопкрофт Дж., Ульман Дж., *Построение и анализ вычислительных алгоритмов*. Мир, Москва, 1979.
7. Земляченко В. Н., Корниенко Н. М., Тышкевич Р. И., Проблема изоморфизма графов. *Записки науч. семинаров ЛОМИ АН СССР* (1982) **118**, 83–158.

Статья поступила 15.10.2001.