ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель—июнь 1998. Серия 1. Том 5, № 2, 28–39

УДК 519.7

О ПОИСКЕ ОПТИМАЛЬНОГО ПОРЯДКА ПЕРЕМЕННЫХ ПРИ СИНТЕЗЕ СХЕМ МЕТОДОМ КАСКАДОВ*)

М. И. Гринчук, В. В. Кочергин

Предложен метод преобразования друг в друга контактных схем, построенных методом каскадов для разного порядка выбора переменных. На его основе создан алгоритм поиска оптимального порядка переменных для синтеза контактных схем методом каскадов, более экономный по сравнению с независимым синтезом схем для каждого порядка переменных. Создание такого алгоритма потребовало решения следующей задачи: найти последовательность $x_1, x_2, \ldots, x_{n!-1}$, где x_i — перестановка n элементов, состоящая из циклов вида $(1, 2, \ldots, k)$, для которой различны все $n!$ произведений $\prod_{i=1}^{m} x_i$, $m = 0, 1, \ldots, n! - 1$.

§ 1. К вопросу о реализации метода каскадов

Известно, что метод каскадов является одним из немногих методов, широко применяемых на практике при синтезе схем различной природы. Хотя этот метод и не является асимптотически оптимальным, однако для многих важных булевых функций построенные с его помощью схемы оказываются достаточно простыми, регулярно устроенными, а иногда и минимальными. К достоинствам метода каскадов можно отнести также прозрачность его стандартной реализации и тот факт, что с его помощью для «почти всех» булевых функций удается построить схемы, которые оказываются сложнее простейших лишь в небольшое число раз.

Известно также, что сложность схемы, которая реализует конкретную булеву функцию и получена методом каскадов, существенно зависит от выбора порядка переменных для разложения. Например, для

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 96–01–01068) и Федеральной целевой программы «Интеграция» (код проекта 473).

функции

$$f(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{i=1}^{n} x_i \ \& \ y_i \pmod 2$$

при разложении по переменным в порядке $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ получается схема (как из функциональных элементов, так и контактная) экспоненциальной сложности, тогда как при порядке $x_1, y_1, x_2, y_2, \ldots, x_n, y_n$ получается схема лишь линейной сложности. (Более подробный анализ этого явления имеется в [1].)

Поэтому при поиске «наиболее простой» схемы для реализации заданной булевой функции оказывается необходимо, вообще говоря, рассматривать все возможные варианты выбора порядка переменных и сравнивать сложность получающихся схем. В настоящей работе рассматривается возможность оптимизации такого перебора.

Для дальнейшего изложения нам потребуется точное определение одного из возможных вариантов метода каскадов для контактных схем.

Пусть дана булева функция $f(x_1, \ldots, x_n)$ и выбран некоторый порядок ее переменных: $x_{i_1}, \ldots, x_{i_n}$, где индексы i_j различны и принимают все значения от 1 до n.

Для каждого j, $1 \leqslant j \leqslant n$, и каждого булевого набора $\sigma = (\sigma_1, \ldots, \sigma_j)$ длины j рассмотрим подфункцию g^j_σ функции f, полученную из f заменой переменных $x_{i_1}, \ldots, x_{i_j}$ константами $\sigma_1, \ldots, \sigma_j$ соответственно. Для общности пусть также определена подфункция g^0_σ для пустого (длины 0) набора σ, совпадающая с исходной функцией f. Очевидно, что при $j = n$ все подфункции g^j_σ являются константами.

Построим множество V подфункций g^j_σ для всех j, $0 \leqslant j \leqslant n$, и всех σ; при этом подфункции, различающиеся только наличием или отсутствием несущественных переменных, будем отождествлять. Будем считать, что множество V содержит функцию, тождественно равную единице (в противном случае добавим ее в это множество). Если же V содержит функцию, тождественно равную нулю, удалим ее из этого множества.

Наконец, построим контактную схему, реализующую функцию f. Вершинами этой схемы объявим элементы множества V, причем полюсами объявим вершины A и B, соответствующие функциям f и 1. Для каждой вершины (т. е. функции) $v \in V$, отличной от константы 1, рассмотрим первую (в списке $x_{i_1}, \ldots, x_{i_n}$) из ее существенных переменных; пусть эта переменная есть x_q. Обозначим через v_0 и v_1 подфункции, получающиеся из v при подстановке соответственно $x_q = 0$ и $x_q = 1$ (каждая из этих подфункций, очевидно, либо является нулевой, либо содержится в множестве V). При $v_0 \not\equiv 0$ вершины v и v_0 соединим контактом с отрицанием переменной x_q. При $v_1 \not\equiv 0$ вершины v и v_1 соединим контактом с переменной x_q.

Построенную контактную схему назовем *каскадной схемой для функции f при порядке переменных $x_{i_1}, \ldots, x_{i_n}$*. Легко видеть, что функция проводимости этой схемы (между полюсами A и B) есть f, а функция проводимости между любой вершиной v и полюсом B есть функция v.

Заметим, что схему, построенную таким образом, можно рассматривать и как ориентированную контактную схему, если считать, что мы добавляли контакты с ориентацией от v к v_0 и v_1; тогда вся схема реализует функцию f при проходе от входного полюса A к выходному полюсу B. В дальнейшем наши схемы будем считать ориентированными.

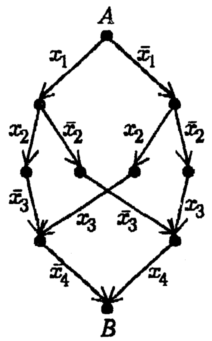

Рис. 1. (Ориентированная) каскадная схема

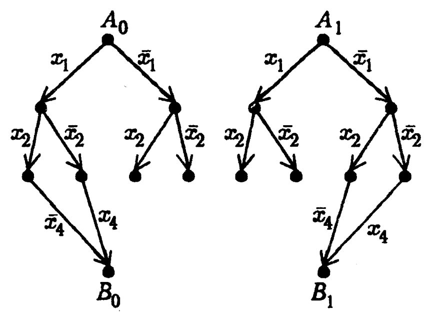

Рис. 2. Построение схем $S_{x_3=0}$ и $S_{x_3=1}$, где S — схема, изображенная на рис. 1; показан результат шагов 1–3

Заметим также, что ориентированные каскадные схемы обладают следующими свойствами:

1) не содержат ориентированных циклов;

2) из каждой вершины выходит не более двух дуг, причем если число таких дуг равно двум, то одна из них помечена символом некоторой переменной, а вторая — отрицанием этой же переменной;

3) если в некоторую вершину схемы входит дуга x_m^{μ} и из этой вершины выходит дуга x_n^{ν}, то переменные x_m и x_n свяжем отношением $>$, т. е. запишем $x_m > x_n$; тогда это отношение можно доопределить до отношения частичного порядка на множестве всех переменных;

4) функции проводимости от различных вершин схемы до полюса B различны.

Легко видеть, что любая ориентированная контактная схема, удовлетворяющая этим четырем условиям, является каскадной схемой, реализующей некоторую булеву функцию; порядок переменных в этой каскадной схеме определяется (вообще говоря, неоднозначно) следующим образом: надо взять частичный порядок, существование которого постулирует свойство 3, и как-либо доопределить его до полного линейного порядка на множестве переменных; этот порядок $x_{i_1} > x_{i_2} > \dots > x_{i_n}$ и даст искомую последовательность переменных.

Естественен вопрос, можно ли из каскадной схемы для одного порядка переменных получить каскадную схему для другого порядка переменных, не прибегая к описанной выше процедуре, а работая только с само́й схемой.

Оказывается, это возможно. Для этого исследуем некоторые естественные операции над ориентированными контактными схемами.

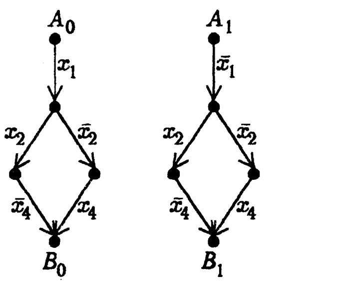

Рис. 3. Полностью построенные схемы $S_{x_3=0}$ и $S_{x_3=1}$

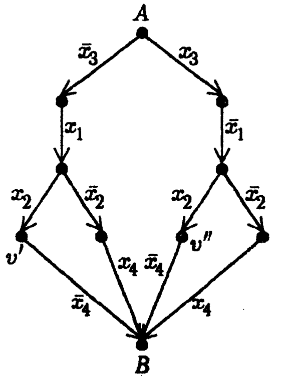

Рис. 4. Сборка схем, показанных на рис. 3

Первая операция — *подстановка в схему константы вместо переменной.* Пусть дана ориентированная контактная схема S (реализующая некоторую булеву функцию f) с входным полюсом A и выходным полюсом B, т. е. ориентированный граф, дуги которого помечены символами переменных и их отрицаний. Пусть x — одна из переменных, c — булева константа. Определим схему $S_{x=c}$ — результат подстановки константы c вместо переменной x:

1) возьмем схему S (см. рис. 1);

2) удалим все дуги, которым приписано $x^{\bar{c}}$;

3) замкнем накоротко каждую дугу, которой приписано x^c, т. е. удалим ее, отождествив связывавшиеся ей вершины (см. рис. 2);

4) будем удалять из схемы те вершины (вместе с инцидентными им дугами), которые не являются полюсами и таковы, что либо в них, либо из них не ведет ни одной дуги; этот процесс продолжим до тех пор, пока не останется таких вершин (см. рис. 3).

Результат этих операций (он определен однозначно) также является, как нетрудно понять, каскадной ориентированной схемой; эту схему обозначим $S_{x=c}$. Она реализует подфункцию функции f, полученную подстановкой константы c вместо переменной x.

Вторая рассматриваемая операция — *сборка* $S = xS_1 \vee \bar{x}S_0$ двух ориентированных каскадных схем S_0 и S_1 (реализующих некоторые функции f_0 и f_1) с использованием дополнительной переменной x; эту операцию будем считать определенной только в том случае, когда частичные порядки $>_0$ и $>_1$ на множестве переменных, заданные схемами S_0 и S_1, можно доопределить до одного и того же частичного порядка $>$.

Пусть A_0 и A_1 — входы, а B_0 и B_1 — выходы схем S_0 и S_1. Сначала построим схему S' следующим образом:

1) введем новую вершину A (вход схемы S');

2) отождествим B_0 и B_1 и полученную вершину объявим выходом B схемы S';

3) если вершина A_0 не изолированная, проведем из A в A_0 дугу, помеченную $\bar{x}$; если вершина A_1 не изолированная, проведем из A в A_1 дугу, помеченную x.

Из способа построения схемы видно, что схема S' (см. рис. 4) обладает свойствами 1)–3) ориентированных каскадных схем и реализует функцию $f = xf_1 \vee \bar{x}f_0$; однако свойство 4) может быть не выполнено. Чтобы оно также выполнялось, применим следующие локальные преобразования:

1) если из некоторой вершины v' выходит только одна дуга и из вершины v'' также выходит только одна дуга, причем эти дуги помечены одинаково и ведут в одну и ту же вершину, то отождествим v' и v'' и удалим одну из упомянутых двух дуг;

2) если из некоторой вершины v' выходят две дуги (в вершины w_0 и w_1) и из вершины v'' также выходят две дуги (в те же вершины w_0 и w_1), причем дуги (v', w_0) и (v'', w_0) помечены одинаково, а (v', w_1) и (v'', w_1) также помечены одинаково, то отождествим v' и v'' и удалим одну из дуг в каждой из упомянутых двух пар;

3) если из некоторой вершины v выходят две дуги, причем они ведут в одну и ту же вершину*) w, то отождествим вершины v и w и удалим эти дуги.

*) Это может быть, только если одна дуга помечена некоторой переменной, а вторая — ее отрицанием. Можно показать, что на самом деле такая ситуация возможна лишь в том случае, когда исходные схемы S_0 и S_1 совпадают. В этом случае указанная переменная — это x.

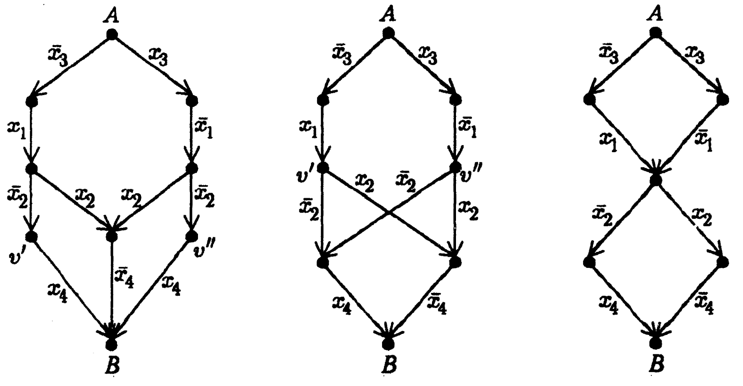

Рис. 5. Последовательность упрощения схемы, показанной на рис. 4

Такие операции будем продолжать до тех пор, пока это возможно (процесс конечен, так как каждый раз число дуг уменьшается, см. рис. 5). Его результат объявим схемой $S = xS_1 \vee \bar{x}S_0$. Реализуемая функция, очевидно, не изменится, т. е. останется $f = xf_1 \vee \bar{x}f_0$.

Легко видеть, что если частичные порядки $>_0$ и $>_1$, заданные схемами S_0 и S_1, можно было доопределить до одного и того же полного линейного порядка $>$, то частичный порядок $>_x$, заданный схемой $S = xS_1 \vee \bar{x}S_0$, можно доопределить до полного линейного порядка, который отличается от $>$ только наличием максимального элемента x.

Из сказанного следует

Лемма 1. *Пусть S — ориентированная каскадная схема, соответствующая порядку переменных $x_{i_1}, \ldots, x_{i_n}$ и реализующая функцию f, $x = x_{i_j}$ — некоторая ее переменная. Тогда схема $S' = xS_{x=1} \vee \bar{x}S_{x=0}$ является ориентированной каскадной схемой, реализующей ту же функцию, но ей соответствует другой порядок переменных, а именно*

$$x, x_{i_1}, \ldots, x_{i_{j-1}}, x_{i_{j+1}}, \ldots, x_{i_n}.$$

Тем самым в результате преобразования схемы S переразложением $xS_{x=1} \vee \bar{x}S_{x=0}$ снова получается каскадная схема, реализующая ту же функцию, но порядок переменных изменяется: первые j циклически переставляются.

Поэтому перебор всех порядков переменных (о чем шла речь в самом начале данной статьи) можно организовать так: сначала построить каскадную схему для какого-либо одного порядка, а затем, пользуясь леммой 1, переразлагать схему, получая всё новые и новые порядки переменных. Идеальной следует считать ситуацию, когда мы каждый раз сможем так выбирать переменные для переразложения, чтобы можно было получить без повторения все $n!$ возможных порядков переменных. В § 2 показано, что это в самом деле возможно.

§ 2. Порождение всех подстановок цепочкой циклов

Итак, рассматривается задача о возможности порождения (без повторения) всех нетождественных подстановок симметрической группы S_n цепочками циклов вида $(1,2),(1,2,3),\ldots,(1,2,\ldots,n)$.

Пусть S_n — симметрическая группа (группа подстановок). Для произвольных элементов a и b этой группы произведение ab определяется следующим образом:

$$ab(i)=b(a(i)), \qquad i=1,2,\ldots,n.$$

Обозначим через C_n множество циклов $\{c_i \mid c_i=(1,2,\ldots,i),\ i=2,3,\ldots,n\}$. Вопрос заключается в том, существует ли такая последовательность $a_1,a_2,\ldots,a_{n!-1}$ элементов множества C_n, что все $n!-1$ подстановок

$$a_1, a_1a_2, \ldots, a_1a_2\ldots a_{n!-1}$$

отличны от тождественной подстановки (будем обозначать ее e) и различны между собой.

Покажем, что для любого $n\geqslant 2$ и всякого k, $2\leqslant k\leqslant n$, можно построить последовательность из $n!-1$ элементов множества C_n, удовлетворяющую определяемому ниже условию $(У_n^k)$.

Будем говорить, что последовательность $a_1,a_2,\ldots,a_{n!-1}$ элементов множества C_n удовлетворяет условию $(У_n^k)$, если:

1) различны все $n!$ подстановок: e, a_1, a_1a_2, $\ldots$, $a_1a_2\ldots a_{n!-1}$;

2) $a_1a_2\ldots a_{n!-1}=c_k^{-1}$.

Лемма 2. *Пусть $a_1,a_2,\ldots,a_{n!-1}$ — последовательность элементов множества C_n, удовлетворяющая условию $(У_n^s)$ для некоторого s, $2\leqslant s\leqslant n$. Тогда для любого цикла c_k, входящего в последовательность $a_1,a_2,\ldots,a_{n!-1}$, найдется последовательность $a_1^{(k)},a_2^{(k)},\ldots,a_{n!-1}^{(k)}$ циклов из C_n, удовлетворяющая условию $(У_n^k)$.*

Доказательство. Пусть $c_k=a_t$. Положим

$$a_1^{(k)}=a_{t+1}, a_2^{(k)}=a_{t+2},\ldots,a_{n!-t-1}^{(k)}=a_{n!-1},$$
$$a_{n!-t}^{(k)}=c_s,$$
$$a_{n!-t+1}^{(k)}=a_1, a_{n!-t+2}^{(k)}=a_2,\ldots,a_{n!-1}^{(k)}=a_{t-1}.$$

Докажем, что последовательность $a_1^{(k)},a_2^{(k)},\ldots,a_{n!-1}^{(k)}$ удовлетворяет условию $(У_n^k)$. Сначала покажем, что все подстановки $a_1^{(k)}$, $a_1^{(k)}a_2^{(k)},\ldots$ $\ldots,a_1^{(k)}a_2^{(k)}\ldots a_{n!-1}^{(k)}$ различны. Предположим, что $a_1^{(k)}a_2^{(k)}\ldots a_i^{(k)}=$ $=a_1^{(k)}a_2^{(k)}\ldots a_j^{(k)}$, причем $i<j$.

Если $j < n! - 1$ или $i > n! - 1$, это равенство выполняться не может в силу того, что последовательность $a_1, a_2, \ldots, a_{n!-1}$ удовлетворяет условию (У_n^s).

Пусть $i \leqslant n! - t \leqslant j$. Обе части исходного равенства домножим слева на $a_1 a_2 \ldots a_{t-1} a_t$. Далее рассмотрим три случая.

1. Пусть выполняются неравенства $i < n! - 1 < j$. Тогда после умножения получаем

$$a_1 a_2 \ldots a_{t-1} a_t a_{t+1} \ldots a_{t+i} = a_1 a_2 \ldots a_{t-1} a_t a_{t+1} \ldots a_{n!-1} c_s a_1 a_2 \ldots a_{j-(n!-t)}.$$

Следовательно,

$$a_1 a_2 \ldots a_{t+i} = a_1 a_2 \ldots a_{j-(n!-t)},$$

причем $t + i > t$, в то время как $j - (n! - t) < t$. Получаем противоречие с тем, что все подстановки $a_1, a_1 a_2, \ldots, a_1 a_2 \ldots a_{n!-1}$ различны.

2. Пусть выполняется равенство $i = n! - 1$. Тогда после умножения получаем

$$a_1 a_2 \ldots a_{n!-1} c_s = a_1 a_2 \ldots a_{n!-1} c_s a_1 a_2 \ldots a_{j-(n!-t)},$$

т. е. $a_1 a_2 \ldots a_{j-(n!-t)} = e$, что невозможно.

3. Пусть выполняется равенство $j = n! - 1$. После умножения получаем

$$a_1 a_2 \ldots a_{t-1} a_t a_{t+1} \ldots a_{t+i} = a_1 a_2 \ldots a_{n!-1} c_s,$$

т. е. $a_1 a_2 \ldots a_{t+i} = e$. Противоречие.

Таким образом, предположение неверно и все подстановки

$$a_1^{(k)},\ a_1^{(k)} a_2^{(k)},\ \ldots,\ a_1^{(k)} a_2^{(k)} \ldots a_{n!-1}^{(k)}$$

различны.

Теперь покажем, что подстановки $a_1^{(k)}$, $a_1^{(k)} a_2^{(k)}$, $\ldots$, $a_1^{(k)} a_2^{(k)} \ldots a_{n!-1}^{(k)}$ отличны от тождественной. Предположим, что это не так, т. е. $a_1^{(k)} a_2^{(k)} \ldots a_i^{(k)} = e$ для некоторого i, $1 \leqslant i \leqslant n! - 1$. Снова рассмотрим три случая.

1. Пусть $i < n! - t$. Тогда $a_{t+1} a_{t+2} \ldots a_{t+i} = e$. Это противоречит тому, что все подстановки a_1, $a_1 a_2$, $\ldots$, $a_1 a_2 \ldots a_{n!-1}$ различны.

2. Пусть $i = n! - t$. Тогда $a_{t+1} a_{t+2} \ldots a_{n!-1} c_s = e$, и поэтому $a_1 a_2 \ldots a_t = e$, что невозможно.

3. Пусть $i > n! - t$. Тогда $a_{t+1} a_{t+2} \ldots a_{n!-1} c_s a_1 \ldots a_{i-(n!-t)} = e$. Домножив слева обе части этого равенства на $a_1 a_2 \ldots a_{t-1} a_t$, получаем $a_1 \ldots a_{i-(n!-t)} = a_1 \ldots a_t$. С учетом оценки $i < n!$ отсюда следует неравенство $i - (n! - t) < t$, что снова невозможно.

Осталось показать, что $a_1^{(k)}a_2^{(k)}\dots a_{n!-1}^{(k)} = c_k^{-1}$. Обе части равенства $a_1a_2\dots a_{n!-1}c_s = e$ домножим слева на подстановку $(a_{t+1}a_{t+2}\dots$ $\dots a_{n!-1}c_s)^{-1}$, а справа — на подстановку $(a_1a_2\dots a_{t-1})^{-1}$. Получим

$$a_t = a_{t-1}^{-1}a_{t-2}^{-1}\dots a_1^{-1}c_s^{-1}a_{n!-1}^{-1}a_{n!-2}^{-1}\dots a_{t+1}^{-1}.$$

Следовательно, $c_k^{-1} = a_1^{(k)}a_2^{(k)}\dots a_{n!-1}^{(k)}$. Лемма 2 доказана.

Теорема. *Для любых натуральных n и k, $2 \leqslant k \leqslant n$, существует последовательность*

$$a_1^{(k,n)}, a_2^{(k,n)}, \dots, a_{n!-1}^{(k,n)}$$

циклов из множества C_n, удовлетворяющая условию $(У_n^k)$.

Доказательство будем вести индукцией по n.

При $n = 2$ утверждение теоремы очевидно.

Пусть $n = 3$. Тогда последовательность c_2, c_3, c_3, c_2, c_3 удовлетворяет условию $(У_3^3)$. В силу леммы 2 утверждение теоремы в этом случае доказано.

Пусть $n \geqslant 4$ и для любого k, $2 \leqslant k \leqslant n-1$, найдется последовательность $a_1^{(k,n-1)}, a_2^{(k,n-1)}, \dots, a_{(n-1)!-1}^{(k,n-1)}$ циклов из множества C_{n-1}, удовлетворяющая условию $(У_{n-1}^k)$ и содержащая все циклы из множества C_{n-1}. Построим последовательность

$$a_1^{(n,n)}, a_2^{(n,n)}, \dots, a_{n!-1}^{(n,n)}$$

циклов из множества C_n, удовлетворяющую условию $(У_n^n)$ и содержащую все циклы из этого множества. Положим

$$\begin{array}{ccccccc}
 & & u_{2,0} & = u_{3,0} = \dots = & u_{n-1,0} & = c_n, \\
u_{1,1} & = & u_{2,1} & = \dots = & u_{n-1,1} & = a_1^{(2,n-1)}, \\
u_{1,2} & = & u_{2,2} & = \dots = & u_{n-1,2} & = a_2^{(2,n-1)}, \\
\multicolumn{6}{c}{\dotfill} \\
u_{1,(n-1)!-1} & = & u_{2,(n-1)!-1} & = \dots = & u_{n-1,(n-1)!-1} & = a_{(n-1)!-1}^{(2,n-1)}.
\end{array}$$

Покажем, что все $(n-1)!(n-1)-1$ подстановок

$$u_{11},\quad u_{11}u_{12},\quad \dots,\quad u_{11}u_{12}\dots u_{1,(n-1)!-1},$$
$$u_{11}u_{12}\dots u_{1,(n-1)!-1}u_{20},\quad u_{11}u_{12}\dots u_{1,(n-1)!-1}u_{20}u_{21},\quad \dots$$
$$\dots,\quad u_{11}u_{12}\dots u_{1,(n-1)!-1}u_{20}u_{21}\dots u_{n-1,(n-1)!-1}$$

отличны от единичной и различны между собой. Действительно, в силу предположения все подстановки

$$u_{11}, u_{11}u_{12},\quad \dots,\quad u_{11}u_{12}\dots u_{1,(n-1)!-1}$$

отличны от единичной и различны между собой. Все они также действуют только на первых $n-1$ элементах, оставляя элемент n неподвижным.

Для любого фиксированного i, $2 \leqslant i \leqslant n-1$, в силу предположения индукции все $(n-1)!$ подстановок

$$\begin{gathered} u_{11}u_{12}\dots u_{1,(n-1)!-1}u_{20}u_{21}\dots u_{i,0}, \\ u_{11}u_{12}\dots u_{1,(n-1)!-1}u_{20}u_{21}\dots u_{i,1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ u_{11}u_{12}\dots u_{1,(n-1)!-1}u_{20}u_{21}\dots u_{i,(n-1)!-1} \end{gathered}$$

различны. Кроме того, при $i < n-1$ для любой подстановки g из этого списка справедливо равенство $g(n-i+1) = n$. Если же $i = n-1$, то справедливо равенство $g(1) = n$.

Таким образом, $(n-1)!(n-1)-1$ исследуемых подстановок отличны от единичной подстановки и различны между собой.

Заметим, что

$$u_{11}u_{12}\dots u_{1,(n-1)!-1}u_{20}u_{21}\dots u_{n-1,(n-1)!-1} = (c_2^{-1}c_n)^{n-2}c_2^{-1} = c_n^{-1}.$$

Теперь отдельно рассмотрим подстановки

$$u_{n-1,0}, u_{n-1,1}, u_{n-1,2}, \dots, u_{n-1,(n-1)!-1}.$$

Как уже отмечалось, $u_{11}u_{12}\dots u_{1,(n-1)!-1}u_{20}u_{21}\dots u_{n-1,j}(1) = n$, $j = 0, 1, \dots, (n-1)!-1$, и все $(n-1)!$ подстановок

$$u_{n-1,0},\ u_{n-1,0}u_{n-1,1},\ \dots,\ u_{n-1,0}u_{n-1,1}\dots u_{n-1,(n-1)!-1}$$

различны. Поэтому, учитывая неравенство

$$u_{11}u_{12}\dots u_{1,(n-1)!-1}u_{20}u_{21}\dots u_{n-1,(n-1)!-1}(2) \neq n-1,$$

можно утверждать, что найдется такой индекс j, что

$$u_{11}u_{12}\dots u_{1,(n-1)!-1}u_{20}u_{21}\dots u_{n-1,j-1}(2) = n-1, \quad u_{n-1,j} = c_{n-1}.$$

В силу предположения индукции найдется последовательность $a_1^{(n-1,n-1)}$, $a_2^{(n-1,n-1)}$, $\dots$, $a_{(n-1)!-1}^{(n-1,n-1)}$ циклов из множества C_{n-1}, удовлетворяющая условию (У_{n-1}^{n-1}). С использованием этой последовательности определим последовательность подстановок $a_1^{(n,n)}$, $a_2^{(n,n)}, \dots, a_{n!-1}^{(n,n)}$

следующим образом:

$$a_1^{(n,n)} = u_{11}, a_2^{(n,n)} = u_{12}, \ldots, a_{(n-1)!-1}^{(n,n)} = u_{1,(n-1)!-1},$$
$$a_{(n-1)!}^{(n,n)} = u_{20}, a_{(n-1)!+1}^{(n,n)} = u_{21}, \ldots, a_{2(n-1)!-1}^{(n,n)} = u_{2,(n-1)!-1},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_{(n-3)(n-1)!}^{(n,n)} = u_{n-2,0}, a_{(n-3)(n-1)!+1}^{(n,n)} = u_{n-2,1}, \ldots, a_{(n-2)(n-1)!-1}^{(n,n)} = u_{n-2,(n-1)!-1},$$
$$a_{(n-2)(n-1)!}^{(n,n)} = u_{n-1,0}, a_{(n-2)(n-1)!+1}^{(n,n)} = u_{n-1,1}, \ldots, a_{(n-2)(n-1)!+j-1}^{(n,n)} = u_{n-1,j-1},$$
$$a_{(n-2)(n-1)!+j}^{(n,n)} = c_n,$$
$$a_{(n-2)(n-1)!+j+1}^{(n,n)} = a_1^{(n-1,n-1)}, a_{(n-2)(n-1)!+j+2}^{(n,n)} = a_2^{(n-1,n-1)}, \ldots$$
$$\ldots, a_{(n-1)(n-1)!+j-1}^{(n,n)} = a_{(n-1)!-1}^{(n-1,n-1)},$$
$$a_{(n-1)(n-1)!+j}^{(n,n)} = c_n,$$
$$a_{(n-1)(n-1)!+j+1}^{(n,n)} = u_{n-1,j+1}, a_{(n-1)(n-1)!+j+2}^{(n,n)} = u_{n-1,j+2}, \ldots$$
$$\ldots, a_{n!-1}^{(n,n)} = u_{n-1,(n-1)!-1}.$$

На самом деле при определении последовательности $a_1^{(n,n)}, a_2^{(n,n)}, \ldots$ $\ldots, a_{n!-1}^{(n,n)}$ была произведена замена подстановки $u_{n-1,j}$ на последовательность подстановок $c_n, a_1^{(n-1,n-1)}, a_2^{(n-1,n-1)}, \ldots, a_{(n-1)!-1}^{(n-1,n-1)}, c_n$.

Отметим, что $c_n a_1^{(n-1,n-1)} a_2^{(n-1,n-1)} \ldots a_{(n-1)!-1}^{(n-1,n-1)} c_n = c_n c_{n-1}^{-1} c_n =$ $= c_{n-1}$. Поэтому

$$a_1^{(n,n)} a_2^{(n,n)} \ldots a_{(n-1)(n-1)!+j}^{(n,n)} = u_{11} u_{12} \ldots u_{1,(n-1)!-1} u_{20} u_{21} \ldots u_{n-1,j},$$
$$a_1^{(n,n)} a_2^{(n,n)} \ldots a_{(n-1)(n-1)!+j+1}^{(n,n)} = u_{11} u_{12} \ldots u_{1,(n-1)!-1} u_{20} u_{21} \ldots u_{n-1,j+1},$$
$$a_1^{(n,n)} a_2^{(n,n)} \ldots a_{n!-1}^{(n,n)} = u_{11} u_{12} \ldots u_{1,(n-1)!-1} u_{20} u_{21} \ldots u_{n-1,(n-1)!-1} = c_n^{-1}.$$

Далее, последовательность подстановок $a_1^{(n-1,n-1)}, a_2^{(n-1,n-1)}, \ldots$ $\ldots, a_{(n-1)!-1}^{(n-1,n-1)}$ удовлетворяет условию $(У_{n-1}^{n-1})$. Поэтому все $(n-1)!$ подстановок

$$a_1^{(n,n)} a_2^{(n,n)} \ldots a_{(n-2)(n-1)!+j}^{(n,n)},$$
$$a_1^{(n,n)} a_2^{(n,n)} \ldots a_{(n-2)(n-1)!+j+1}^{(n,n)},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_1^{(n,n)} a_2^{(n,n)} \ldots a_{(n-1)(n-1)!+j-1}^{(n,n)}$$

различны. Кроме того, для любой подстановки g из этого списка выполняется равенство $g(2) = n$. Таким образом, последовательность подстановок

$$a_1^{(n,n)}, a_2^{(n,n)}, \ldots, a_{n!-1}^{(n,n)}$$

удовлетворяет условию $(У_n^n)$. По построению эта последовательность содержит все циклы из множества C_n.

Для завершения доказательства теоремы достаточно применить лемму 2.

ЛИТЕРАТУРА

1. **Денев Й. Д.** О сравнении сложности разных реализаций функций алгебры логики методом каскадов // Дискретный анализ: Сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1972. Вып. 20. С. 9–15.

Адрес авторов:

МГУ, мех.-мат. факультет,
Воробьевы горы,
119899 Москва, Россия.
E-mail:
grinchuk@nw.math.msu.su,
koch@nw.math.msu.su

Статья поступила
2 февраля 1998 г.