Math-Net.Ru

Общероссийский математический портал

А. Е. Андреев, А. А. Часовских, Автоматная сложность
двуместных булевых базисов, *Дискрет. матем.*, 1996,
том 8, выпуск 4, 123–133

DOI: <https://doi.org/10.4213/dm545>

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: 54.162.127.20

26 апреля 2023 г., 18:37:23

Автоматная сложность двуместных булевых базисов

© 1996 г. А. Е. Андреев, А. А. Часовских

Рассматривается задача о минимально возможном числе состояний для автомата, вычисляющего значения булевых выражений заданной длины в различных операторных базисах. Установлено, что множество всех базисов распадается на три класса, в зависимости от порядка роста логарифма необходимого числа состояний: константного, логарифмического или линейного. Получена критериальная система из пяти базисов, каждый из которых классифицирован в указанном смысле, а определение класса любого заданного множества операций осуществляется проверкой включения в базисы критериальной системы. Это позволило провести полную классификацию базисов операций с рассматриваемой точки зрения. В работе приводится доказательство полученных результатов.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, грант 95-01-00707.

В настоящей работе мы приводим доказательство результата, анонсированного в [1].

Формулы рассматриваются в операторной форме над множеством из всех двуместных операций и отрицания [2]. Понятие формулы над базисом (в базисе) мы трактуем, как обычно, но не подразумеваем в формулах переменных. Вместо них уже стоят константы 0 и 1. Выражение указанного типа подается на конечный автомат, который должен вычислить его значение.

Под словом вычислить мы подразумеваем, что автомат имеет финальные состояния 0 и 1 и после просмотра формулы он попадает в финальное состояние соответствующее значению формулы.

В настоящей заметке рассматривается задача о минимально возможном числе состояний для автомата, вычисляющего значения булевых выражений заданной длины в различных операторных базисах.

Используемое здесь понятие автомата (инициального, конечного) соответствует [3], однако мы рассматриваем не общий случай, а автомат без выхода.

Таким образом, автоматом A называется пятерка (V, Q, φ, q_0, Q') , причем V, Q — конечные множества, называемые входным алфавитом и алфавитом состояний соответственно, φ — функция переходов,

$$\varphi: V \times Q \mapsto Q,$$

q_0 — начальное состояние, $q_0 \in Q$, Q' — множество заключительных состояний $Q' \subseteq Q$, $Q' = \{0, 1\}$.

Входной алфавит V автомата A состоит из левой и правой круглых скобок, констант 0 и 1, а также символов логических операций.

Длиной формулы называется количество букв алфавита V , содержащихся в ней.

В дальнейшем мы используем логические операции, которые выражаются через операции $(x_1 \wedge x_2)$, $(x_1 \vee x_2)$, $\neg x$ следующим образом:

$$\begin{aligned} x \setminus &= \neg x, \\ (x_1 \oplus x_2) &= (\neg x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2), \\ (x_1 \sim x_2) &= (x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2), \\ (x_1 \rightarrow x_2) &= (\neg x_1 \vee x_2), \\ (x_1 \leftarrow x_2) &= (x_1 \vee \neg x_2), \\ (x_1 \mid x_2) &= \neg(x_1 \wedge x_2), \\ (x_1 \downarrow x_2) &= \neg(x_1 \vee x_2), \\ (x_1 > x_2) &= (x_1 \wedge \neg x_2), \\ (x_1 < x_2) &= (\neg x_1 \wedge x_2). \end{aligned}$$

Таким образом, операция отрицания имеет префиксную и суффиксную формы, а любая двуместная операция получает свое обозначение. Все двуместные операции, а также обе формы отрицания объединим в множество Ω .

Пусть F — подмножество Ω . Тогда существует автомат, вычисляющий формулы над F длины, не большей n . Наименьшее k такое, что существует автомат с 2^k состояниями (это соответствует структурному автомату с k задержками [4]), вычисляющий формулы над F длины, не большей n , обозначим $S_F(n)$.

Через K_0 , D_0 , L_0 , P_0 , R_0 обозначим следующие множества операций:

$$\begin{aligned} K_0 &= \{(x_1 \wedge x_2)\}, \\ D_0 &= \{(x_1 \vee x_2)\}, \\ L_0 &= \{\neg x, x \setminus, (x_1 \oplus x_2), (x_1 \sim x_2)\}, \\ P_0 &= \{x \setminus, (x_1 \vee x_2), (x_1 \wedge x_2), (x_1 \rightarrow x_2), (x_1 < x_2)\}, \\ R_0 &= \{x \setminus, (x_1 \leftarrow x_2), (x_1 > x_2), (x_1 \mid x_2), (x_1 \downarrow x_2)\}. \end{aligned}$$

Замыкание [5] множества функций R алгебры логики обозначим $[R]$. Тогда $[K_0]$ и $[D_0]$ — множества монотонных функций с одной нижней единицей и одним верхним нулем соответственно, а $[L_0]$ — множество всех линейных функций.

Теорема 1. Пусть $F \subseteq \Omega$, $F \neq \emptyset$.

(1) Если F содержится хотя бы в одном из множеств K_0 , D_0 , L_0 , то

$$S_F(n) = 1.$$

(2) Если F не содержится ни в одном из множеств K_0 , D_0 , L_0 и содержится в каком-нибудь из множеств P_0 , R_0 , то

$$S_F(n) \asymp \log n.$$

Рис. 1.

(3) Если F не содержится ни в одном из множеств L_0 , P_0 , R_0 , то

$$S_F(n) \asymp n.$$

Доказательство. 1. Пусть F содержится хотя бы в одном из множеств K_0 , D_0 , L_0 . Любой автомат, вычисляющий формулы над F , имеет два заключительных состояния, поэтому $S_F(n) \geq 1$. С другой стороны, на рис. 1a, 1b, 1c приведены диаграммы переходов автоматов, вычисляющих формулы любой длины над K_0 , D_0 , L_0 соответственно и имеющих два состояния. Первое утверждение теоремы доказано.

2. Пусть множество F не содержится ни в одном из множеств K_0 , D_0 , L_0 и содержится в P_0 . Докажем сначала, что порядок роста последовательности $S_F(n)$ не менее, чем $\log n$. Имеет место хотя бы один из следующих пяти случаев.

(a) $\{(x_1 \wedge x_2), (x_1 \vee x_2)\} \subseteq F$;

(b) $(x_1 \rightarrow x_2) \in F$;

(c) $(x_1 < x_2) \in F$;

(d) $\{x \setminus, (x_1 \wedge x_2)\} \subseteq F$;

$$(e) \{x\}, (x_1 \vee x_2)\} \subseteq F.$$

Выберем натуральное число n и в каждом из перечисленных пяти случаев определим последовательности символов $A_k, B_k, k = 1, \dots, n-1$, следующим образом.

В случае (а) положим

$$A_k = \underbrace{((1 \wedge ((1 \wedge \dots ((1 \wedge ((0 \wedge ((0 \wedge \dots ((0 \wedge 0,$$

$$B_k = \underbrace{)) \vee 1)) \vee 1) \dots \vee 1)) \vee 0)) \vee 0) \dots \vee 0)}_{n-k \text{ единиц}} \underbrace{)) \vee 0)}_{k \text{ нулей}}).$$

В случае (b) положим

$$A_k = \underbrace{((1 \rightarrow (((1 \rightarrow (\dots ((1 \rightarrow (((0 \rightarrow (((0 \rightarrow (\dots ((0 \rightarrow (0,$$

$$B_k = \underbrace{ \rightarrow 0)) \rightarrow 1) \rightarrow 0)) \rightarrow 1) \dots \rightarrow 0)) \rightarrow 1) \rightarrow 0)) \rightarrow 0) \rightarrow 0)) \rightarrow 0) \dots \rightarrow 0)) \rightarrow 0)}_{n-k \text{ единиц}} \underbrace{ \rightarrow 0)) \rightarrow 0)}_{2k \text{ нулей}}).$$

В случае (с) положим

$$A_k = \underbrace{((0 < (((0 < (\dots ((0 < ((1 < (((1 < (\dots ((1 < (1,$$

$$B_k = \underbrace{< 1)) < 0) < 1)) < 0) \dots < 1)) < 0) < 1)) < 1) < 1)) < 1) \dots < 1)) < 1)}_{n-k \text{ единиц}} \underbrace{< 1)) < 1)}_{2k \text{ единиц}}).$$

В случае (d) положим

$$A_k = \underbrace{(1 \wedge (1 \wedge \dots (1 \wedge (0 \wedge (0 \wedge \dots (0 \wedge 0,$$

$$B_k = \underbrace{)) \dots)}_{n-k-1 \text{ скобок}} \setminus \underbrace{)) \dots)}_{k+1 \text{ скобок}}).$$

В случае (е) положим

$$A_k = \underbrace{(0 \vee (0 \vee \dots (0 \vee (1 \vee (1 \vee \dots (1 \vee 1,$$

$$B_k = \underbrace{)) \dots)}_{n-k-1 \text{ скобок}} \setminus \underbrace{)) \dots)}_{k+1 \text{ скобок}}).$$

В каждом из рассматриваемых пяти случаев для любых натуральных чисел k и $s, k < n, s < n$, последовательность символов $A_k B_s$ является формулой над алфавитом V . При этом в случаях (а), (b) и (е) $A_k B_k = 1$, а в случаях (с) и (d) $A_k B_k = 0, k = 1, \dots, n-1$. Если же $k < s$, то в случаях (а) и (b) $A_k B_s = 0$, в случае (с) $A_k B_s = 1$, в случае (d) $A_s B_k = 1$, а в случае (е) $A_s B_k = 0$.

Если автомат A вычисляет все формулы над F длины, не большей n , то, как следует из предыдущих рассмотрений, состояния, в которые он переходит при

Рис. 2.

подаче последовательностей A_k и A_s при $s \neq k$, отличимы. Поэтому автомат A имеет не менее $n - 2$ попарно отличимых состояний и порядок роста последовательности $S_F(n)$ не менее, чем $\log n$.

Покажем далее, что порядок роста последовательности $S_F(n)$ не более, чем $\log n$. На рис. 2 и 3 изображены фрагменты диаграммы переходов автомата A , вычисляющего все формулы над P_0 длины, не большей n . Не определенные в диаграмме переходы можно доопределить произвольным образом. Начальное состояние автомата помечено символом $*$. Фрагмент B_0 имеет $n + 1$ состояние. Он служит для пропуска подформулы глубины, не большей n , в обрабатываемой автомата формуле. Это означает, что, начиная обработку любой подформулы из начального состояния фрагмента B_0 , по последнему символу подформулы автомат выйдет из рассматриваемого фрагмента. Когда на вход автомата A поступает символ $($, соответствующий операции, которая имеет глубину i в обрабатываемой формуле, то автомат переходит в i -й блок B_1 . После обработки символа $)$ указанной операции, осуществляется переход из i -го блока по стрелке, ведущей вверх. Если переход осуществляется по первой или второй стрелке (считая слева направо), то значение всей подформулы, заключенной в указанных скобках, равно 1. В противном случае это значение равно 0. Число состояний этого автомата растет по порядку как n^2 . Отсюда вытекает нужное утверждение. Таким образом, второе утверждение теоремы для множества P_0 доказано.

Докажем утверждение 2 теоремы для множества R_0 . Пусть $F \not\subseteq L_0$ и $F \subseteq R_0$. Покажем, что порядок роста $S_F(n)$ не менее, чем $\log n$.

Имеет место один из следующих случаев.

- (a) $(x_1 \mid x_2) \in F$;
- (b) $(x_1 \downarrow x_2) \in F$;
- (c) $(x_1 \leftarrow x_2) \in F$;

А

Рис. 3.

(d) $(x_1 > x_2) \in F$.

В первом случае положим

$$A_k = \underbrace{((1|((1| \dots ((1|((0|((0| \dots ((0|0,}_{k \text{ единиц} \quad n-k+1 \text{ нулей}} \\ B_k = \underbrace{)|0\rangle)|0\rangle \dots |0\rangle)|1\rangle)|1\rangle \dots |1\rangle)}_{n-k \text{ нулей} \quad k \text{ единиц}}.$$

Во втором случае положим

$$A_k = \underbrace{((0 \downarrow ((0 \downarrow \dots ((0 \downarrow ((1 \downarrow ((1 \downarrow \dots ((1 \downarrow 1,$$

$$B_k = \underbrace{)) \downarrow 1)) \downarrow 1) \dots) \downarrow 1)) \downarrow 0)) \downarrow 0) \dots) \downarrow 0)}_{n-k \text{ единиц}} \underbrace{)) \downarrow 0)) \downarrow 0) \dots) \downarrow 0)}_{k \text{ нулей}}.$$

В третьем случае положим

$$A_k = \underbrace{((0 \leftarrow (0 \leftarrow ((0 \leftarrow (0 \leftarrow \dots ((0 \leftarrow (0 \leftarrow ((0 \leftarrow (1 \leftarrow ((0 \leftarrow (1 \leftarrow \dots ((0 \leftarrow (1 \leftarrow 0$$

$$B_k = \underbrace{)) \leftarrow 0))) \leftarrow 0) \dots) \leftarrow 0)) \leftarrow 1))) \leftarrow 1) \dots) \leftarrow 1)}_{n-k \text{ нулей}} \underbrace{)) \leftarrow 1))) \leftarrow 1) \dots) \leftarrow 1)}_{k \text{ единиц}}$$

В четвертом случае положим

$$A_k = \underbrace{((1 > (1 > ((1 > (1 > \dots ((1 > (1 > ((1 > (0 > ((1 > (0 > \dots ((1 > (0 > 1$$

$$B_k = \underbrace{)) > 1))) > 1) \dots) > 1)) > 0))) > 0) \dots) > 0)}_{n-k \text{ единиц}} \underbrace{)) > 1))) > 1) \dots) > 1)}_{k \text{ нулей}}$$

Пусть k и s — натуральные числа и $0 < k < s < n$. Нетрудно видеть, что в каждом из четырех рассматриваемых случаев последовательности $A_k B_k$ и $A_k B_s$ являются формулами и значения этих формул следующие: в случаях 1 и 3

$$A_k B_k = 1, \quad A_k B_s = 0;$$

в случаях 2 и 4

$$A_k B_k = 0, \quad A_k B_s = 1.$$

Пусть теперь автомат A вычисляет все формулы над F длины, не большей n . Выберем последовательности A_k , $k = 1, 2, \dots, n-1$, в соответствии с тем, как это было определено для случая, который имеет место. Из приведенных выше равенств следует, что, перерабатывая разные последовательности из множества $\{A_k, k = 1, 2, \dots, n-1\}$, автомат A перейдет в отличимые состояния. Поэтому A соответствует структурному автомату, имеющему по порядку не менее $\log n$ задержек. Оценка снизу для последовательности $S_F(n)$ доказана.

Доказательство верхней оценки вытекает из существования автомата, имеющего по порядку n^2 состояний и вычисляющего все формулы над F длины, не большей n . Фрагменты диаграммы переходов такого автомата изображены на рис. 4 и 5. Для этих рисунков справедливы все комментарии, приведенные выше для рис. 2 и 3. Второе утверждение теоремы полностью разобрано.

3. Для доказательства третьего утверждения теоремы нам понадобятся вспомогательные утверждения.

Через $\Phi(F)$ обозначим множество формул над F , $F \subseteq \Omega$.

Лемма 1. Если для некоторых слов $\alpha_1, \alpha_2, \beta, \gamma$ в алфавите V выполнены соотношения

$$\alpha_i x_1 \beta x_2 \gamma \in \Phi(F), \quad i = 1, 2,$$

Рис. 4.

и формулы $\alpha_1 x_1 \beta x_2 \gamma$, $\alpha_2 x_1 \beta x_2 \gamma$ реализуют функции $x_1 \vee x_2$, $\neg x_1 \vee x_2$ соответственно, то

$$S_F(n) \asymp n.$$

Доказательство. Пусть автомат A вычисляет все формулы над F длины, не большей n . Через k обозначим целую часть числа

$$\frac{n-1}{\max(|\alpha_1|, |\alpha_2|) + |\beta| + |\gamma| + 1} + 1$$

Для последовательностей $a_1, \dots, a_{k-1}, b_1, \dots, b_k$, $a_i \in \{\alpha_1, \alpha_2\}$, $i = 1, \dots, k-1$, $b_j \in \{0, 1\}$, $j = 1, \dots, k$, через $\Psi(a_1, a_2, \dots, a_{k-1}, b_1, b_2, \dots, b_k)$ обозначим формулу

$$a_1 a_2 \dots a_{k-2} \underbrace{a_{k-1} b_k \beta b_{k-1} \gamma \beta b_{k-2} \gamma \dots \beta b_2 \gamma \beta b_1 \gamma}_{\text{}}.$$

Пусть $a_1, a_2, \dots, a_{k-1}$ и $a'_1, a'_2, \dots, a'_{k-1}$ — два различных набора из нулей и единиц и i — минимальный индекс со свойством $a_i \neq a'_i$. Тогда

$$\Psi(a_1, a_2, \dots, a_{k-1}, \underbrace{0, \dots, 0}_{k-i-1}, \underbrace{1, 0, \dots, 0}_i) \neq \Psi(a'_1, a'_2, \dots, a'_{k-1}, \underbrace{0, \dots, 0}_{k-i-1}, \underbrace{1, 0, \dots, 0}_i)$$

и, перерабатывая последовательности $a_1, a_2, \dots, a_{k-1}$ и $a'_1, a'_2, \dots, a'_{k-1}$, автомат A переходит в отличимые состояния. Таким образом, рассматриваемый автомат имеет не менее 2^{k-1} попарно отличимых состояний и соответствует структурному автомату, имеющему не менее $k-1 \asymp n$ задержек. Лемма доказана.

Лемма 2. Пусть $F \subseteq \Omega$, $F \not\subseteq \Theta$ для каждого Θ , $\Theta \in \{L_0, P_0, R_0\}$. Тогда

(1) в V^* найдутся слова $\alpha_1, \alpha_2, \beta$ такие, что

$$\alpha_i x \beta \in \Phi(F), \quad i = 1, 2,$$

и формулы $\alpha_1 x \beta$, $\alpha_2 x \beta$ реализуют функции x и $\neg x$;

A

Рис. 5.

(2) в V^* найдутся слова α', β', γ' такие, что

$$\alpha'x_1\beta'x_2\gamma' \in \Phi(F)$$

и формула $\alpha'x_1\beta'x_2\gamma'$ реализуют функцию $x_1 \vee x_2$.

Доказательство. Докажем первое утверждение леммы. Рассмотрим два случая. В первом случае

$$(F \cap L_0) \setminus \{x\} \neq \emptyset.$$

Поэтому выполнено хотя бы одно из следующих трех включений:

$$\begin{aligned}\{\neg x, \neg\neg x\} &\subseteq \Phi(F), \\ \{(1 \oplus x), (0 \oplus x)\} &\subseteq \Phi(F), \\ \{(1 \sim x), (0 \sim x)\} &\subseteq \Phi(F).\end{aligned}$$

Во втором случае

$$(F \cap L_0) \setminus \{x\} = \emptyset.$$

Поэтому из условия леммы

$$\begin{aligned}(F \cap P_0) \setminus \{x\} &\neq \emptyset, \\ (F \cap R_0) \setminus \{x\} &\neq \emptyset.\end{aligned}$$

Пусть

$$\begin{aligned}(x_1 \circ x_2) &\in (F \cap P_0) \setminus \{x\}, \\ (x_1 \star x_2) &\in (F \cap R_0) \setminus \{x\}.\end{aligned}$$

Тогда каждая из функций x , $\neg x$ реализуется некоторой формулой из множества $\{(0 \circ x), (1 \circ x), (0 \star x), (1 \star x)\}$. Утверждение 1 леммы доказано.

Далее, в F содержится формула, реализующая двуместную нелинейную функцию алгебры логики. Навешивая (при необходимости) отрицания на переменные этой функции и на всю функцию, получим формулу $\alpha'x_1\beta'x_2\gamma'$, реализующую функцию $x_1 \vee x_2$, где $\{\alpha', \beta', \gamma'\} \subseteq V^*$. Утверждение 2 леммы, а, следовательно, и вся лемма, доказаны.

Перейдем к доказательству утверждения 3 теоремы. Требуемая оценка снизу для последовательности $S_F(n)$ вытекает из двух предыдущих лемм. Получим оценку сверху. Для этого укажем способ построения диаграммы переходов автомата с входным алфавитом V , выходным алфавитом $\{0, 1\}$, имеющего не более $2 + |V|^n - 1/(|V| - 1)$ состояний и вычисляющего все формулы над Ω длины, не большей n .

Вершины диаграммы переходов, соответствующие состояниям автомата, расположим на $n + 1$ ярусах с номерами $0, 1, \dots, n$. На нулевом ярусе расположим только вершину, соответствующую начальному состоянию. На n -ом ярусе расположим только две вершины, соответствующие заключительным состояниям 0 и 1. На ярусе с номером i , $i = 1, \dots, n - 1$, расположим $|V|^i$ вершин. Для определения функции переходов автомата будем последовательно просматривать все вершины каждого яруса, кроме n -го, продвигаясь от i -го яруса к $(i + 1)$ -му, $i = 0, 1, \dots, n - 2$. Пусть рассматривается некоторая вершина q из яруса с номером i , $i \in \{0, 1, \dots, n - 2\}$. Тогда может оказаться, что из вершины, соответствующей начальному состоянию, по ранее построенным ребрам графа $r_1, r_2, \dots, r_k$ в q ведет ориентированный путь $r_1, r_2, \dots, r_k$ (и притом единственный). Для вершины из нулевого яруса полагаем, что такой путь существует, но он не содержит ребер. Пусть также этим ребрам приписаны соответственно буквы $a_1, a_2, \dots, a_k$ из входного алфавита V . Тогда для каждой буквы a из алфавита V выполним следующие действия. Если слово $a_1a_2 \dots a_k a$ является формулой над Ω и имеет значение b , $b \in \{0, 1\}$, то добавим ориентированное ребро из вершины q в вершину, соответствующую заключительному состоянию b ,

и припишем этому ребру букву a . Если слово $a_1a_2 \dots a_ka$ не является формулой над множеством Ω , но является началом какой-нибудь из формул, то выберем в $(i+1)$ -ом ярусе вершину q' , в которую еще не входит ни одного ребра, и добавим ребро из q в q' , которому припишем букву a . Если рассматриваемая вершина q содержится в $(n-1)$ -ом ярусе, то для каждой буквы a из V выполним описанные выше построения лишь в том случае, когда слово $a_1a_2 \dots a_ka$ является формулой над множеством Ω .

После того, как будет просмотрена последняя вершина $(i-1)$ -го яруса, недостающие переходы доопределим произвольным образом. Нетрудно видеть, что автомат, задаваемый так построенной диаграммой переходов удовлетворяет всем необходимым условиям. Теорема доказана.

Теорема позволяет определить порядок роста последовательности $S_F(n)$ для любого множества F операций. Пусть, например,

$$F_1 = \{(x_1 \vee x_2), \neg x\}, \quad F_2 = \{(x_1 \mid x_2)\}.$$

Тогда по теореме выполнены соотношения

$$S_{F_1}(n) \asymp n, \quad S_{F_2}(n) \asymp \log n.$$

Таким образом, порядок роста последовательностей $S_{F_1}(n)$ и $S_{F_2}(n)$ различен, несмотря на то, что как F_1 , так и F_2 являются полными [5] в классе функций алгебры логики.

Список литературы

1. Андреев А. Е., Часовских А. А. Сложность автоматов, вычисляющих значения формул. *Вестник МГУ, сер.1: мат., мех.* (1996) №4, 22–24.
2. Kleene S. C. *Mathematical Logic*. Wiley, New York, 1967.
3. Gill A. *Introduction to the Theory of Finite-State Machines*. McGraw-Hill, New York, 1962.
4. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. *Введение в теорию автоматов*. Наука, Москва, 1985.
5. Post E. L. Two-valued iterative systems of mathematical logic. *Ann. Math. Studies* (1941) №5.

Статья поступила 23.10.96.