Сложность автоматов, вычисляющих значения формул над базисом, состоящим из одной булевской функции (записанной в операторном виде)

А.А. Кудрин

Общая задача, которой посвящена данная статья, может быть сформулирована следующим образом. В множестве булевских функций P^2 зафиксируем некоторое конечное подмножество $F \subseteq P^2$. Далее будем строить над этим множеством формулы в смысле суперпозиции [1]. Однако, мы не будем предполагать в формулах переменных, вместо них уже стоят константы 0 и 1. Совокупность этих выражений обозначим через $\Phi(F)$, элементы этого множества и будут являться объектами нашего рассмотрения.

Таким образом, элементы множества $\Phi(F)$ представляют собой слова над некоторым конкретным алфавитом V. В частности, если все функции из F заданы в операторной форме, то этот алфавит будет иметь вид $V_{op} = \{\alpha_1, ..., \alpha_k, (,), 0, 1\}$, где символы $\alpha_1, ..., \alpha_k$ есть значки булевских операторов; если если все функции из F заданы в префиксной форме (то есть в виде $f(x, y)$), то этот алфавит будет иметь вид $V_{pr} = \{f_1, ..., f_k, (,), 0, 1\}$, где символы $f_1, ..., f_k$ есть значки функциональных символов.

Пусть теперь у нас есть элемент $\psi \in \Phi(F)$. Число символов соответствующего алфавита V, содержащихся в слове ψ, назовем длиной формулы ψ и обозначим через $|\psi|$.

Множество формул над F, длина которых не превышает некоторой константы n, обозначим через $\Phi_n(F) = \{\psi \in \Phi(F) | |\psi| \leqslant n\}$.

Произвольная формула из множества $\Phi_n(F)$ подается на вход конечного инициального автомата A без выхода [2], $A = (V, Q, \varphi, q_0)$, который должен вычислить значение функции, реализуемой данной формулой (здесь символами V, Q, φ, q_0 обозначены входной алфавит, алфавит состояний, функция переходов и начальное состояние соответственно). Под термином «вычислить» мы подразумеваем следующее: автомат A вычисляет $\Phi_n(F) \Leftrightarrow$

$$\exists q^0, q^1 \in Q : \forall \alpha \in \Phi_n(F), \bar{\varphi} = \begin{cases} q^0, \text{если } \alpha = 0 \\ q^1, \text{ если } \alpha = 1 \end{cases}.$$

Здесь под метаобозначением $\alpha = const$ подразумевается тот факт, что значение функции, реализуемой формулой α равняется указанной константе.

Требуется оценить минимально возможное число состояний автомата A, вычисляющего $\Phi_n(F)$, как функцию параметров F и n. Данную оценку будем проводить при помощи величины $S_F(n) = \min\{\log_2 |Q| : A \text{ вычисляет } \Phi_n(F)\}$.

Поставленная таким образом задача корректна в том смысле, что если на вход изучаемого автомата A подается формула из множества $\Phi_n(F)$, то автомат вычисляет (в указанном смысле) значение функции, реализуемой данной формулой. Различные вариации этой задачи могут появляться, если мы будем рассматривать разные формы записи функций из множества F (операторную, префиксную, польскую), а также варьировать число переменных в этих функциях.

Один из первых результатов в данной области был получен А.Е. Андреевым и А.А. Часовских [3]. Ими был рассмотрен случай, когда в множестве F могли содержаться только двуместные функции (существенно зависящие от всех переменных), записанные в операторном виде (множество таких функций обозначим через Ω^2). Сформулируем этот результат, так как он потребуется для дальнейшего изложения.

Определим следующие классы функций:

$$K_0 = \{(x \& y)\}, D_0 = \{(x \vee y)\}, L_0 = \{(x \sim y), (x \oplus y)\}$$

$$P_0 = \{(x \& y), (x \vee y), (x < y), (x \to y)\}$$

$$R_0 = \{(x \leftarrow y), (x > y), (x \downarrow y), (x | y)\}$$

Сформулируем теперь теорему, которая позволяет оценить порядок величины $S_F(n)$ в зависимости от вида множества F.

Теорема 1. *Пусть* $F \subseteq \Omega^2, F \neq \emptyset$.
1. Если $F = K_0$ *или* $F = D_0$ *или* $F \subseteq L_0$, *то* $(\forall n) S_F(n) = 1$.
2. Если не выполняются условия пункта 1 Теоремы и $F \subseteq P_0$ *(или* $F \subseteq R_0$*), то* $S_F(n) \asymp \log_2 n$.
3. Во всех остальных случаях $S_F(n) \asymp n$.

Естественным продолжением этой задачи является увеличение числа переменных функций, входящих в множество F. Формально говоря, в предыдущем случае в множество F могли входить булевы функции, длина записи которых в операторном виде равнялась 5 (в смысле длины слова в соответствующем алфавите, состоящем из значков булевых операторов, открывающей и закрывающей скобок, символа запятая и символов переменных). Теперь будем рассматривать функции, длина записи которых в операторном виде равняется 9. То есть функции вида $((x \circ y) * z)$ и $(x \circ (y * z))$, где символы $\circ$ и $*$ – есть значки булевых операторов.

Сформулируем результат, полученный в этом случае, при дополнительном условии $|F| = 1$ (то есть в множестве F содержится ровно одна функция). Здесь как обычно через $[F]$ будем обозначать замыкание множества функций F [1].

Теорема 2. *Пусть* $|F| = 1$ *и* $F = \{((x \circ y) * z)\}$ *или* $F = \{(x \circ (y * z))\}$, *тогда*
1. Если $F \subseteq [D_0]$ *или* $F \subseteq [K_0]$ *или* $F \subseteq [L_0]$, *то* $(\forall n) S_F(n) = 1$.
2. Если не выполняются условия пункта 1 Теоремы и функции $(x \circ y), (x * y) \in P_0 \cup R_0$, *то* $S_F(n) \asymp \log_2 n$.
3. Во всех остальных случаях $S_F(n) \asymp n$.

Доказательство. Доказательство пункта 1 данной теоремы полностью повторяет аналогичные выкладки для п. 1 Теоремы 1 [3].

Докажем пункт 2. Вначале покажем, что $S_F(n) \lesssim \log_2 n$. Указанное неравенство очевидно выполняется, если одновременно и операция $(x \circ y)$, и операция $(x * y)$ принадлежат либо классу P_0, либо классу R_0 (см. пункт 2 Теоремы 1, [3]).

Пусть теперь одна из операций принадлежит классу P_0, а вторая – классу R_0. Без ограничения общности можно считать, что $(x \circ y) \in P_0$, а $(x * y) \in R_0$.

Рассмотрим сначала случай, когда множество F имеет вид

$$F = \{((x \circ y) * z)\}.$$

Определим на множестве $P_0 \cup R_0$ следующие классы функций.

$$I^1 = \{(x\alpha y) | \exists i : (i\alpha y) = y\},$$

$$N^1 = \{(x\alpha y) | \exists i : (i\alpha y) = \overline{y}\},$$

$$I^2 = \{(x\alpha y) | \exists i : (x\alpha i) = x\},$$

$$N^2 = \{(x\alpha y) | \exists i : (x\alpha i) = \overline{x}\}.$$

Верхний индекс здесь означает место переменной, вместо которой подставляется константа. Также можно заметить, что на множестве $P_2(2)$ справедливы соотношения $P_0 = I^1 \setminus L_0$ и $R_0 = N^1 \setminus L_0$. Далее определим класс $S^i = \{(x\alpha y) | (x\alpha i) = const\}$. Введем отношение эквивалентности C:

$$(x\alpha_1 y) \sim_C (x\alpha_2 y) \Leftrightarrow \exists i : (x\alpha_1 y), (x\alpha_2 y) \in S^i \text{ или } (x\alpha_1 y) = (x\alpha_2 y).$$

Заметим, что отношение эквивалентности C устанавливает взаимооднозначное соответствие между классами I^2 и N^2, то есть

$$\forall (x\alpha_1 y) \in I^2, \exists! (x\alpha_2 y) \in N^2 : (x\alpha_1 y) \sim_C (x\alpha_2 y).$$

Таким образом, отношение эквивалентности C разбивает множество $P_0 \cup R_0$ на двухэлементные подмножества, где один элемент принадлежит классу I^2, а второй – классу N^2. Сформулируем дополнительное утверждение.

Утверждение 1. *Если на множестве* $P_0 \cup R_0$ $(x\alpha_1 y) \sim_C (x\alpha_2 y)$, *то либо* $(x\alpha_1 y), (x\alpha_2 y) \in P_0$, *либо* $(x\alpha_1 y), (x\alpha_2 y) \in R_0$.

Доказательство. Случай, когда $(x\alpha_1 y) = (x\alpha_2 y)$ тривиален. Поэтому можно считать, что эти функции различны. Без ограничения общности положим, что $(x\alpha_1 y), (x\alpha_2 y) \in S^1$, тогда $(x\alpha_1 1) = (x\alpha_2 1) = a$ (так как по условию $(x\alpha_1 y) \sim_C (x\alpha_2 y)$).

По условию утверждения обе функции нелинейны и существенно зависят от всех своих аргументов (и, в рассматриваемом случае, различны). Тогда без ограничения общности можно считать, что $(0\alpha_1 0) = a$, $(1\alpha_1 0) = \overline{a}$, тогда $(0\alpha_2 0) = \overline{a}$, $(1\alpha_2 0) = a$.

Таким образом, если $a = 1$, то $(1\alpha_1 y) = y$, а $(0\alpha_2 y) = y$, что означает, что $(x\alpha_1 y), (x\alpha_2 y) \in I^1 = P_0$ (на множестве $P_0 \cup R_0$). В противном случае, то есть когда $a = 0$, обе изучаемые функции принадлежат классу $N^1 = R_0$ (на множестве $P_0 \cup R_0$).

Тогда справедлива следующая лемма.

Лемма 1. *Пусть* $|F| = 1$ *и* $F = \{((x \circ y) * z)\}$, *где* $(x \circ y), (x * y) \in P_0 \cup R_0$, *тогда существуют булевы функции* $x\alpha_1 y$ *и* $x\alpha_2 y$ *одновременно принадлежащие либо классу* P_0, *либо классу* R_0 *такие, что* $((x \circ y) * z) \equiv ((x\alpha_1 y)\alpha_2 z)$.

Доказательство. Можно считать, что функции $(x \circ y)$ и $(x * y)$ не принадлежат одновременно ни P_0, ни R_0, так как в противном случае доказательство становится тривиальным.

Без ограничения общности можно считать, что $(x \circ y) \in P_0$ и $(x * y) \in R_0$ (симметричный случай рассматривается аналогично).

Тогда положим $(x\alpha_1 y) = \overline{x \circ y}$, очевидно, что $(x\alpha_1 y) \in R_0$.

Определим оператор α_2 следующим образом: $(x\alpha_2 y) \sim_C (x * y)$ и $(x\alpha_2 y) \neq (x * y)$. Можно считать, что $(x * y) \in I^2$, тогда $(x\alpha_2 y) \in N^2$ (по построению).

Докажем, что $((x \circ y) * z) \equiv ((x\alpha_1 y)\alpha_2 z)$. По построению очевидно, что $\exists j : (x\alpha_2 j) = (x * j) = const$ (так как $(x\alpha_2 y) \sim_C (x * y)$, то $\exists j : (x\alpha_2 j), (x * j) \in S^j$), тогда $((x \circ y) * j) = ((x\alpha_1 y)\alpha_2 j)$.

Так как $\overline{(x*y)} \in I^2$, то $(x*\bar{j}) = x$, а $(x\alpha_2\bar{j}) = \bar{x}$, тогда $((x\circ y)*\bar{j}) = \overline{(x\circ y)} = \overline{(x\alpha_1 y)} = ((x\alpha_1 y)\alpha_2\bar{j})$. Что и требовалось доказать.

Следствие из Леммы 1. Если $F = \{((x\circ y)*z)\}$, где функции $(x\circ y), (x*y) \in P_0 \cup R_0$, то $S_F(n) \lesssim \log_2 n$.

Доказательство. Действительно, утверждение Леммы 1 позволяет нам получить искомую оценку сверху для функции $S_F(n)$. Согласно Лемме мы можем преобразовать исходную функцию $((x\circ y)*z)$ к виду $((x\alpha_1 y)\alpha_2 z)$ таким образом, что булевы функции $x\alpha_1 y$ и $x\alpha_2 y$ одновременно принадлежат либо классу P_0, либо классу R_0. Для функции $((x\alpha_1 y)\alpha_2 z)$, согласно результатам [3] (пункт 2 Теоремы 1), справедлива оценка $S_F(n) \lesssim \log_2 n$, то есть существует автомат A, который вычисляет $\Phi_n(F)$, причем логарифм числа его состояний не превосходит (по порядку) величины $\log_2 n$. Теперь, если мы во входном алфавите данного автомата заменим значки α_1, α_2 на значки $\circ, *$ соответственно (не изменяя при этом структуру автомата), то мы получим автомат A', который вычисляет $\Phi_n(F)$ для исходного множества F с такой же сложностью.

При этом очевидно, что функция $((x|y) < z) = ((x\& y)\& z)$, а $((x \downarrow y) \to z) = ((x \vee y) \vee z)$ и в этих случаях $S_F(n) = 1$.

В качестве интересного обобщения этого Утверждения приведем следующий результат

Обобщение Леммы 1. Пусть дана функция

$$((\ldots((y_0\alpha_n y_n)\alpha_{n-1}y_{n-1})\ldots)\alpha_1 y_1),$$

где для любого i $(x\alpha_i y) \in P_0 \cup R_0$. Тогда существует набор булевских функций $(x\beta_i y) \in P_0(R_0), i = 1, \ldots, n$ такой, что

$$((\ldots((y_0\alpha_n y_n)\alpha_{n-1}y_{n-1})\ldots)\alpha_1 y_1) \equiv ((\ldots((y_0\beta_n y_n)\beta_{n-1}y_{n-1})\ldots)\beta_1 y_1).$$

Доказательство. Проведем доказательство по индукции.

Базис индукции доставляет нам доказанная выше Лемма 1 (случай $n = 2$). Пусть доказываемое утверждение верно для $n = k-1$. Рассмотрим случай $n = k : ((\ldots((y_0\alpha_k y_k)\alpha_{k-1}y_{k-1})\ldots)\alpha_1 y_1)$. Обозначим $(y_0\alpha_k y_k)$ через Y_0. Тогда по предположению индукции

$$((\ldots((y_0\alpha_k y_k)\alpha_{k-1}y_{k-1})\ldots)\alpha_1 y_1) = ((\ldots(Y_0\alpha_{k-1}y_{k-1})\ldots)\alpha_1 y_1) =$$
$$= ((\ldots(Y_0\gamma_{k-1}y_{k-1})\ldots)\gamma_1 y_1),$$

где набор булевских функций $(x\gamma_i y), i = 1, \ldots, k-1$ таков, что все эти функции принадлежат одновременно либо классу P_0, либо классу R_0. Без ограничения общности предположим, что $(x\alpha_1 y) \in P_0$, а $(x\gamma_i y) \in R_0, i = 1, \ldots, k-1$ (если все эти функции принадлежат одному и тому же классу, то доказательство становится тривиальным). Применим Лемму 1 к функции $((y_0\alpha_k y_k)\gamma_{k-1}y_{k-1})$, тогда получим

$$((y_0\alpha_k y_k)\gamma_{k-1}y_{k-1}) = ((y_0\beta_k y_k)\beta_{k-1}y_{k-1}),$$

причем $(x\beta_k y), (x\beta_{k-1}y) \in R_0$. Далее положим $(x\gamma_i y) \equiv (x\beta_i y)$ для $i = 1, .., k-2$ и получим таким образом искомый результат.

Таким образом, доказательство оценки сверху для случая $F = \{((x\circ y)*z)\}$ проведено полностью. Из доказательства видно, что в данном случае удалось достаточно эффективно «редуцировать» рассматриваемую задачу к соответствующим выкладкам Теоремы 1 при помощи «алгебраических» рассуждений. Доказательство же аналогичной оценки для случая $F = \{(x\circ(y*z))\}$ осуществляется при помощи непосредственного построения соответствующих автоматов. Эти выкладки достаточно громоздки, и поэтому, на наш взгляд, не имеет смысла приводить их в данной заметке. Поэтому ограничимся лишь формулировкой общего результата.

Лемма 2. *Пусть* $|F| = 1$ *и* $F = \{(x\circ(y*z))\}$, *где* $(x\circ y), (x*y) \in P_0 \cup R_0$, *тогда* $S_F(n) \lesssim \log_2 n$.

Перейдем теперь к доказательству нижних оценок. При этом нам достаточно рассматривать случаи, когда оба оператора, присутствующие в записи базисной функции различны, так как в противном случае все требуемые оценки получаются непосредственно из [3].

Лемма 3. *Пусть* $F = \{(x\circ(y*z))\}$, *где функции* $(x\circ y), (x*y) \in P_0 \cup R_0$ *и различны, тогда*

1. Если $F = \{(x > (y|z)\}$ *или* $F = \{(x \leftarrow (y \downarrow z))\}$, *то* $S_F(n) = 1$.

2. Во всех остальных случаях $S_F(n) \gtrsim \log_2 n$.

Доказательство. Непосредственная проверка показывает, что $(x > (y|z)) = (x\&(y\&z))$ и $(x \leftarrow (y \downarrow z)) = (x \vee (y \vee z))$, то есть в этих двух случаях базисная функция может быть выражена в виде формулы из K_0 и D_0 соответственно. Этот случай описывается п. 1 Теоремы, доказанным выше. Используя технику, аналогичную технике Леммы 1, можно показать, что никакая другая базисная функция, удовлетворяющая условиям данной Леммы не может быть выражена в виде формулы над K_0 или D_0.

Определим класс функций $F^i = \{(x\alpha y)|(i\alpha y) = const\}$.

Без ограничения общности предположим, что $(x \circ y) \in F^i$. Далее зафиксируем у рассматриваемой функции первый аргумент (положим его равным $\bar{i}$), тогда введем обозначение $(\bar{i} \circ (x * y)) = (x * y)^\sigma$, где $\sigma \in \{0, 1\}$. Рассмотрим теперь множество $G = \{(\bar{i} \circ (x * y)) = (x * y)^\sigma\}$, получающееся из исходного базиса F путем указанной «редукции». Очевидно, что $S_F(n) \geqslant S_G(n)$. Таким образом, если мы докажем, что $S_G(n) \gtrsim \log_2 n$, то получим искомый результат.

Однако последнее утверждение непосредственно следует из [3], если $(x * y)^\sigma \neq (x\&y)$ или $(x * y)^\sigma \neq (x \vee y)$.

Допустим теперь, что $(x * y)^\sigma = (x\&y)$ или $(x * y)^\sigma = (x \vee y)$.

Пусть $\sigma = 1$ (то есть $(x * y) = (x\&y)$ или $(x * y) = (x \vee y)$), но тогда $(x \circ y) \in I^1 = \{(x\alpha y)|\exists i : (i\alpha y) = y\}$. Таким образом, нам осталось рассмотреть множества F вида $F = \{(x \circ (y\&z))\}$ и $F = \{(x \circ (y \vee z))\}$, где $(x \circ y) \in I^1$. Рассмотрим следующую «редукцию» этих множеств $G = \{(x \circ (y\&1))\}$ и $G = \{(x \circ (y \vee 0))\}$. Очевидно, что $S_F(n) \geqslant S_G(n)$. Таким образом, если мы докажем, что $S_G(n) \gtrsim \log_2 n$, то получим искомый результат. Последнее непосредственно следует из [3], если операция $\circ$ отлична от операций $\&$ и $\vee$. То есть в данном случае нам осталось доказать искомую оценку лишь для двух базисов $F = \{(x \vee (y\&z))\}$ и $F = \{(x\&(y \vee z))\}$.

Приведем доказательство оценки $S_F(n) \gtrsim \log_2 n$ для случая $F = \{(x \vee (y\&z))\}$ (второй случай рассматривается аналогично).

Пусть автомат A вычисляет $\Phi_n(F)$. Введем следующие обозначения $A = (0\vee$ и $B = (1\vee$.

Теперь над алфавитом $V = \{(,), \vee, \&, 0, 1\}$ рассмотрим множество $W_k \subseteq \Phi_n(F)$ (где $k =]\frac{n}{8}[$), состоящее из слов вида $w_i = \overbrace{\underbrace{A...A}_{i-1}BA...A}^{k}$.

Очевидно, что $|W_k| = k$.

Докажем, что для любой пары таких слов $w_i, w_j (i \neq j)$ найдется слово t такое, что:

1. Слова $w_i t$ и $w_j t$ являются элементами множества $\Phi_n(F)$.
2. $w_i t \neq w_j t$ (знак $\neq$ понимается в смысле различия значений функций, реализуемых данными формулами).

Слово t в данном случае будет иметь вид $c_0\&c_k))\&c_{k-1}))\&...\&c_1))$, где $c_i, i = 0, ..., k$ – булевские константы (очевидно, что выражения $w_i t$ и $w_j t$ будут формулами над F).

Без ограничения общности предположим, что $i > j$, тогда положим

$$c_l = \begin{cases} 0, l = j \\ \bar{1}, 1 \leqslant l \leqslant j - 1 \end{cases}$$

Остальные константы доопределяются произвольно.

Непосредственной проверкой доказывается, что $w_i t \neq w_j t$.

Таким образом, перерабатывая всевозможные пары различных элементов w_i, w_j автомат A, вычисляющий значения формул над $\Phi_n(F)$, переходит в отличимые состояния. Следовательно, рассматриваемый автомат имеет не менее $k \asymp n$ попарно отличимых состояний, следовательно $S_F(n) \gtrsim \log_2 n$.

Допустим, что $\sigma = 0$ (то есть $(x * y) = (x \downarrow y)$ или $(x * y) = (x|y)$). При этом $(x \circ y) \in N^1 = \{(x\alpha y)|\exists i : (i\alpha y) = \overline{y}\}$. В данном случае нерассмотренными остаются множества F вида $F = \{(x \circ (y|z))\}$ и $F = \{(x \circ (y \downarrow z))\}$, где $(x \circ y) \in N^1$.

Применяя рассуждения, аналогичные случаю $\sigma = 1$ (с той лишь разницей, что нам не надо рассматривать случаи, описанные в п. 1 данной Леммы), мы получаем искомый результат.

Лемма 4. *Пусть* $F = \{((x \circ y) * z)\}$, *где функции* $(x \circ y), (x * y) \in P_0 \cup R_0$, *и различны, тогда*

1. Если $F = \{((x \downarrow y) \to z)\}$ *или* $F = \{((x|y) < z)\}$, *то* $S_F(n) = 1$.
2. Во всех остальных случаях $S_F(n) \gtrsim \log_2 n$.

Доказательство. Доказательство пункта 1 данной леммы непосредственно заключено в Следствии из Леммы 1 (см. выше). Оттуда же следует, что никакая другая базисная функция (отличная от функций, упомянутых в пункте 1), удовлетворяющая условиям данной Леммы, не может быть выражена в виде формулы над K_0 или D_0.

Перейдем к доказательству пункта 2.

Без ограничения общности предположим, что $(x * y) \in S^i$. Далее зафиксируем у рассматриваемой функции второй аргумент (положим его равным $\bar{i}$), тогда введем обозначение $((x \circ y) * \bar{i}) = (x \circ y)^\sigma$, где $\sigma \in \{0, 1\}$. Рассмотрим теперь множество $G = \{((x \circ y) * \bar{i}) = (x \circ y)^\sigma\}$, получающееся из исходного базиса F путем указанной «редукции». Очевидно, что $S_F(n) \geqslant S_G(n)$. Таким образом, если мы докажем, что $S_G(n) \gtrsim \log_2 n$, то получим искомый результат.

Однако последнее утверждение непосредственно следует из [3], если $(x \circ y)^\sigma \neq (x \& y)$ или $(x \circ y)^\sigma \neq (x \vee y)$.

Пусть теперь $(x \circ y)^\sigma = (x \& y)$ или $(x \circ y)^\sigma = (x \vee y)$. Допустим, что $\sigma = 1$ ($(x \circ y) = (x \& y)$ или $(x \circ y) = (x \vee y)$), но тогда $(x * y) \in I^2 = \{(x \alpha y) | \exists i : (x \alpha i) = x\}$. Таким образом, нам осталось рассмотреть Множества F вида $F = \{((x \& y) * z)\}$ и $F = \{((x \vee y) * z)\}$, где $(x * y) \in I^2$.

Рассмотрим следующую «редукцию» этих множеств $G = \{((1 \& y) * z)\}$ и $G = \{((0 \vee y) * z)\}$. Очевидно, что $S_F(n) \geqslant S_G(n)$. Таким образом, если мы докажем, что $S_G(n) \gtrsim \log_2 n$, то получим искомый результат. Последнее непосредственно следует из [3], если операция $*$ отлична от операций $\&$ и $\vee$. То есть в данном случае нам осталось доказать искомую оценку лишь для двух базисов $F = \{((x \& y) \vee z)\}$ и $F = \{((x \vee y) \& z)\}$.

Приведем доказательство оценки $S_F(n) \gtrsim \log_2 n$ для случая $F = \{((x \vee y) \& z)\}$ (второй случай рассматривается аналогично).

Пусть автомат A вычисляет $\Phi_n(F)$. Введем следующие обозначения $A = ((0\vee$ и $B = ((1\vee$.

Теперь над алфавитом $V = \{(,), \vee, \&, 0, 1\}$ рассмотрим множество $W_k \subseteq \Phi_n(F)$ (где $k = \left]\frac{n}{8}\right]$), состоящее из слов вида $w_i = \overbrace{\underbrace{A...A}_{i-1}BA...A}^{k}$. Очевидно, что $|W_k| = k$.

Докажем, что для любой пары таких слов $w_i, w_j (i \neq j)$ найдется слово t такое, что:
1. Слова $w_i t$ и $w_j t$ являются элементами множества $\Phi_n(F)$.
2. $w_i t \neq w_j t$ (знак $\neq$ понимается в смысле различия значений функций, реализуемых данными формулами)

Слово t в данном случае будет иметь вид $c_0))\&c_k))\&c_{k-1}))\&...\&c_1)$, где $c_i, i = 0, ..., k$ – булевские константы (очевидно, что выражения $w_i t$ и $w_j t$ будут формулами над F).

Без ограничения общности предположим, что $i > j$, тогда положим

$$c_l = \begin{cases} 0, l = j + 1 \\ \bar{1}, 1 \leqslant l \leqslant j \end{cases}$$

Остальные константы доопределяются произвольно. Непосредственной проверкой доказывается, что $w_i t \neq w_j t$.

Таким образом, перерабатывая всевозможные пары различных элементов w_i, w_j, автомат A, вычисляющий значения формул над $\Phi_n(F)$, переходит в отличимые состояния. Следовательно, рассматриваемый автомат имеет не менее $k \asymp n$ попарно отличимых состояний, следовательно, $S_F(n) \gtrsim \log_2 n$.

Допустим, что $\sigma = 0$ (то есть $(x \circ y) = (x \downarrow y)$ или $(x \circ y) = (x|y)$). При этом $(x * y) \in N^2 = \{(x \alpha y) | \exists i : (x \alpha i) = \bar{i}\}$. В данном случае нерассмотренными остаются множества F вида $F = \{((x \downarrow y) * z))\}$ и $F = \{(x|y) * z))\}$, где $(x * y) \in N^2$.

Применяя рассуждения, аналогичные случаю $\sigma = 1$ (с той лишь разницей, что нам не надо рассматривать случаи, описанные в п. 1 данной Леммы), мы получаем искомый результат.

Перейдем теперь к доказательству пункта 3 Теоремы 2. Очевидно, что в данном случае достаточно доказать, что $S_F(n) \gtrsim n$, так как заведомо существует автомат (построенный на основе бинарного дерева), который вычисляет $\Phi_n(F)$ таким образом, что $S_F(n) \asymp n$.

Лемма 5. *Пусть* $F = \{((x \circ y) * z)\}$ *или* $F = \{(x \circ (y * z))\}$, *где одна из функций* $(x \circ y), (x * y)$ *лежит в множестве* $P_0 \cup R_0$, *а вторая – в множестве* $I^1 \cap N^1$. *Тогда* $S_F(n) \gtrsim n$.

Доказательство. Очевидно, что $I^1 \cap N^1 = \{(x \oplus y), (x \sim y)\}$. Без ограничения общности будем далее считать, что $(x \circ y) \in P_0 \cup R_0$, а $(x * y) \in I^1 \cap N^1$, а также, что $(x \circ y) \in S^j$.

Рассмотрим вначале случай $F = \{((x \circ y) * z)\}$.

Введем следующие обозначения

$A = ((a_1 \circ a_2) * (($ и $B = ((a_3 \circ a_4) * (($, где константы a_1, a_2, a_3, a_4 подобраны таким образом, что $(a_1 \circ a_2) = 0, (a_3 \circ a_4) = 1$.

Теперь над алфавитом $V = \{(,), \circ, *, 0, 1\}$ рассмотрим множество $W_k \subseteq \Phi_n(F)$ (где $k = \left]\frac{n}{15}\right]$), состоящее из слов вида $d = \theta_1...\theta_k$, и где $\theta_i \in \{A, B\}$. Очевидно, что $|W_k| = 2^k$.

Рассмотрим два слова из этого множества: $d = \theta_1...\theta_k$ и $r = \gamma_1...\gamma_k$, где $\theta_i, \gamma_i \in \{A, B\}$.

Докажем, что для любой пары различных слов такого типа существует слово t такое, что:

1. Слова dt и rt являются формулами над F длины не более чем n (то есть элементами $\Phi_n(F)$).
2. $dt \neq rt$ (знак $\neq$ понимается в смысле различия значений функций, реализуемых данными формулами).

Слово t в данном случае будет иметь вид $c_0 \circ c_k) * 0)) \circ c_{k-1}) * 0)) \circ ... \circ c_1) * 0)$, где $c_i, i = 0, ..., k$ – булевские константы.

Пусть $i = \max\{s : \theta_1 = \gamma_1, ..., \theta_k = \gamma_k\}$. Без ограничения общности будем считать, что $\theta_{i+1} = A$, а $\gamma_{i+1} = B$. Тогда определим $c_i, i = 0, ..., k$ следующим образом

$$c_i = \begin{cases} j, i = s+1 \\ \bar{j}, 1 \leqslant i \leqslant s \end{cases}$$

Остальные константы доопределяются произвольно.

Непосредственной проверкой доказывается, что $dt \neq rt$. Этот факт объясняется следующим образом

$$A\theta_{i+1}...\theta_k c_0 \circ c_k) * 0)) \circ ... \circ c_i) * 0) = b,$$

тогда как

$$A\gamma_{i+1}...\gamma_k c_0 \circ c_k) * 0)) \circ ... \circ c_i) * 0) = \bar{b},$$

тогда $dt = b^\sigma \neq b^{\bar{\sigma}} = rt$.

Таким образом, перерабатывая различные последовательности $\theta_1...\theta_k$, $\gamma_1...\gamma_k$, автомат A, вычисляющий значения формул над $\Phi_n(F)$, переходит в отличимые состояния. Следовательно, рассматриваемый автомат имеет не менее 2^k попарно отличимых состояний и реализуется схемой, содержащей не менее $k \asymp n$ задержек, следовательно $S_F(n) \gtrsim n$.

Случаи $F = \{((x * y) \circ z)\}$, $F = \{(x \circ (y * z))\}$, $F = \{(x * (y \circ z))\}$ рассматриваются аналогично.

Таким образом, доказательство Теоремы 2 проведено полностью.

В заключение опишем один результат, связанный с префиксной записью функций из множества F (см. [4]). Рассмотрим множество двуместных булевых функций (в префиксном виде), существенно зависящих от всех своих переменных, и одноместной функции отрицания – Ω^2_{pr}.

$$K_{pr} = \{f_\&(x,y)\}, D_{pr} = \{f_\vee(x,y)\}, L_{pr} = \{f_\sim(x,y), f_\oplus(x,y)\},$$

$$P_{pr} = \{(f_\&(x,y), f_\vee(x,y), f_<(x,y), f_\to(x,y)\},$$

$$R_{pr} = \{f_\leftarrow(x,y), f_>(x,y), f_\downarrow(x,y), f_|(x,y)\}.$$

Сформулируем теперь теорему, которая позволяет оценить порядок величины $S_F(n)$ в зависимости от вида множества F.

Теорема 3. *Пусть* $F \subseteq \Omega^2_{pr}, F \neq \emptyset$.

1. Если $F = K_{pr}$ *или* $F = D_{pr}$ *или* $F \subseteq L_0$, *то для любого* n $S_F(n) = 1$.

2. Если не выполняются условия пункта 1 Теоремы, и $|F| = 1, F \subseteq P_{pr} \cup R_{pr}$*, или* $|F| = 2$ *и* $F = \{f(x,y), f_{\neg}(x)\}$*, где* $f(x,y) \in R_{pr}$*, то* $S_F(n) \asymp \log_2 n$.

3. Во всех остальных случаях $S_F(n) \asymp n$.

Список литературы

[1] Гаврилов Г.П., Кудрявцев В.Б., Яблонский С.В. Функции алгебры логики и классы Поста. М.: Наука, 1966.

[2] Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов М.: Наука, 1985.

[3] Андреев А.Е., Часовских А.А. Сложность автоматов, вычисляющих значения формул // Вестник МГУ. Сер. Мат., мех. 1996. №4.

[4] Кудрин А.А. Сложность автоматов, вычисляющих значения функций, заданных в префиксном виде // Вестник МГУ. Сер. Мат., мех. 1998. №1.

Оценка отклонения разделяющей плоскости пороговой функции от вершин единичного куба

М.В. Носов

В работе получена нижняя оценка расстояния от вершин единичного куба до разделяющей плоскости для произвольной пороговой функции. Аналогичным образом могут быть получены нижние оценки для произвольных двух конечных множеств, разделимых гиперплоскостью. С использованием преобразования спрямления получаются нижние оценки расстояний для конечных множеств, разделимых более сложными поверхностями. В линейном случае эти оценки дают верхние оценки числа исправлений в теореме Новикова для алгоритма Розенблата.

Используя известную технику, докажем два утверждения. Пусть $F(t)$ – пороговая функция, $t = (t_1, \ldots, t_n)$.

Лемма 1. *Любая пороговая функция* $F(t)$ *может быть задана гиперплоскостью, определяемой уравнением* $c_1t_1 + \ldots + c_nt_n + c_0 = 0$ *так, что*

$$F(t) = 1 \iff c_1t_1 + \ldots + c_nt_n + c_0 \geqslant 1,$$

$$F(t) = 0 \iff c_1t_1 + \ldots + c_nt_n + c_0 \leqslant -1.$$

Утверждение 1. *Пусть* B^n *–* n*-мерный единичный куб,* $F(t)$ *– пороговая функция, тогда существует такое задание* $F(t)$ *гиперплоскостью, что расстояние от любой вершины* B^n *до этой гиперплоскости не меньше, чем* $1/(\sqrt{n(n+1)^{n+1}})$.