

Разрешимые случаи задачи об A -полноте для дефинитных автоматов*

Д. Н. Жук

В работе рассматриваются системы вида $M = F \cup \nu$, где F — некоторый класс Поста, а ν — конечная система дефинитных автоматов. Выделены некоторые классы Поста, для которых проблема A -полноты для систем вида $F \cup \nu$ алгоритмически разрешима.

Введение

В работах [10, 3] установлена алгоритмическая неразрешимость задач о полноте и A -полноте относительно операций суперпозиции и обратной связи для конечных систем автоматных функций. Для систем автоматов, содержащих все булевы функции, указанные задачи алгоритмически разрешимы [4]. Д. Н. Бабин исследовал на полноту и A -полноту системы вида $F \cup \nu$, где F — некоторый класс Поста, а ν — конечная система автоматных функций. Ему удалось построить классификацию классов Поста по их способности гарантировать разрешимость проблемы полноты для конечных систем автоматов. Оказалось, что проблемы полноты и A -полноты для систем вида $F \cup \nu$ разрешимы точно тогда, когда F содержит либо функцию $x + y + z$, либо функцию $xy \vee yz \vee xz$ [6].

Похожие результаты были получены для дефинитных автоматов. Было показано, что в классе дефинитных автоматов задачи о полноте и A -полноте относительно операции суперпозиции алгоритмически неразрешимы [7]. Ранее автор показал, что для систем дефинитных автоматов вида $P_2 \cup \nu$ существует алгоритм проверки на полноту и

*Работа выполнена при финансовой поддержке РФФИ (грант 06-01-00240).

A -полноту таких систем автоматов [8]. Для каждого конечного ν он заключается в проверке непринадлежности ν конечному числу предполных классов. Естественно исследовать на A -полноту системы вида $F \cup \nu$, где F — некоторый класс Поста, а ν — конечная система дефинитных автоматов. Возникает разделение классов Поста на сильные и слабые по их способности гарантировать разрешимость проблемы A -полноты для дефинитных автоматов. В данной работе выделены сильные классы Поста.

Автор выражает благодарность своему научному руководителю Кудрявцеву В. Б. за оказанную помощь и поддержку в исследовании задачи и написании данной работы.

1. Основные понятия и результаты

Пусть $\mathbb{N} = \{1, 2, 3, \dots\}$ — множество всех натуральных чисел, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, $E_2 = \{0, 1\}$, E_2^l — множество всех слов длины l в алфавите E_2 , E — множество всех бесконечных последовательностей нулей и единиц. Далее такие последовательности называем сверхсловами. Множество E^n состоит из всех наборов $(\alpha_1, \alpha_2, \dots, \alpha_n)$, где $\alpha_i \in E$. Если $a, b \in E_2$, то \bar{a} — отрицание a , $a \vee b$ — дизъюнкция a и b , $a \& b$ — конъюнкция a и b , $a + b$ — сложение по модулю 2. Множество всех булевых функций будем обозначать P_2 .

Пусть α — слово или сверхслово, тогда $\alpha(n)$ — n -ый элемент α . Обозначим через $|\alpha|$ длину слова α ; для сверхслова α будем полагать, что $|\alpha| = \infty$. Для слова α , такого что $|\alpha| \geq k$, определим ${}_k\alpha = \alpha(|\alpha| - k + 1) \dots \alpha(|\alpha| - 1)\alpha(|\alpha|)$. Для слова или сверхслова α , такого что $|\alpha| \geq k$ положим ${}_k\alpha = \alpha(1)\alpha(2) \dots \alpha(k)$, ${}_l{}_k\alpha = \alpha(k - l + 1)\alpha(k - l + 2) \dots \alpha(k)$. Для произвольного слова α определим слово $\alpha^s = \underbrace{\alpha\alpha \dots \alpha}_s$ и сверхслово $\alpha^\infty = \alpha\alpha\alpha \dots$.

Функция $T : E^n \rightarrow E$ называется дефинитным автоматом с n входами высоты h , если существуют функции $f_j : (E_2^j)^n \rightarrow E_2$ ($j = 1, 2, 3, \dots, h$), такие что для любых $x_1, x_2, \dots, x_n \in E$ выполняется:

$$T(x_1, x_2, \dots, x_n)(1) = f_1([{}_1x_1, {}_1x_2, \dots, {}_1x_n]),$$

$$\begin{aligned}
T(x_1, x_2, \dots, x_n)(2) &= f_2(\lceil_2 x_1, \lceil_2 x_2, \dots, \lceil_2 x_n), \\
&\dots \\
T(x_1, x_2, \dots, x_n)(h) &= f_h(\lceil_h x_1, \lceil_h x_2, \dots, \lceil_h x_n), \\
T(x_1, x_2, \dots, x_n)(h+1) &= f_h(\lceil_h \lceil_{h+1} x_1, \lceil_h \lceil_{h+1} x_2, \dots, \lceil_h \lceil_{h+1} x_n), \\
&\dots \\
T(x_1, x_2, \dots, x_n)(h+i) &= f_h(\lceil_h \lceil_{h+i} x_1, \lceil_h \lceil_{h+i} x_2, \dots, \lceil_h \lceil_{h+i} x_n), \\
&\dots
\end{aligned}$$

Таким образом, согласно нашему определению автомат высоты h является также автоматом высоты $h+1$. Элемент $T(x_1, x_2, \dots, x_n)(j)$ будем называть элементом на выходе автомата T в момент времени j , а $x_i(j)$ — элементом, подаваемым на i -ый вход в момент времени j . Для $j = 1, \dots, h-1$ функция f_j определяет элемент на выходе автомата T в момент времени j , а функция f_h определяет элемент на выходе автомата, начиная с момента времени h .

Пусть T — автомат высоты h . Для $p \in \mathbb{N}$ определим функцию $T^p : (E_2^p)^n \rightarrow E_2$. Если $p \leq h$, то положим

$$T^p(\alpha_1, \alpha_2, \dots, \alpha_n) = f_p(\alpha_1, \alpha_2, \dots, \alpha_n).$$

Для $p > h$ положим

$$T^p(\alpha_1, \alpha_2, \dots, \alpha_n) = f_h(\lceil_h \alpha_1, \lceil_h \alpha_2, \dots, \lceil_h \alpha_n).$$

Таким образом, для любого s функция T^s определяет элемент на выходе автомата T в момент времени s .

Функции f_j , где $j = 1, \dots, h$, будем называть порождающими. Нетрудно убедиться, что для задания дефинитного автомата необходимо задать высоту автомата и порождающие функции. Для $p \leq h$ функции T^p также будем называть порождающими. Доопределим естественным образом каждый автомат на словах длины p . Будем полагать, что для любых $\alpha_1, \alpha_2, \dots, \alpha_n \in E_2^p$ выполняется $T(\alpha_1, \alpha_2, \dots, \alpha_n) = \beta$, где $\beta \in E_2^p$ и $\beta(s) = T^s(\lceil_s \alpha_1, \lceil_s \alpha_2, \dots, \lceil_s \alpha_n)$ для любого $s \leq p$.

Множество всех дефинитных автоматов обозначим \mathcal{P}_a . Для $T \in \mathcal{P}_a$ через $h(T)$ обозначим наименьшую высоту автомата h , через $n(T)$ обозначим количество входов автомата T . Множество всех автоматов

высоты не более h обозначим \mathcal{P}_a^h . Ясно, что каждой булевой функции из \mathcal{P}_2 соответствует дефинитный автомат высоты 1. Будем использовать стандартные обозначения для автоматов из \mathcal{P}_a^1 , а именно: \bar{x} , $x \& y = xy$, $x \vee y$, $x + y$ — дефинитные автоматы T_1 , T_2 , T_3 и T_4 высоты 1, такие что выполняется $T_1^1(\alpha) = \bar{\alpha}$, $T_2^1(\alpha, \beta) = \alpha \& \beta$, $T_3^1(\alpha, \beta) = \alpha \vee \beta$, $T_4^1(\alpha, \beta) = \alpha + \beta$.

Автомат S_c высоты 2 с одним входом, для которого $S_c^1(\alpha) = c$, $S_c^2(\alpha) = \alpha(1)$, назовём задержкой с начальным состоянием c .

Пусть $M \subseteq \mathcal{P}_a$. Фиксируем некоторое счётное множество $U = \{u_1, u_2, u_3, \dots\}$, элементы которого будем называть переменными. Индуктивно определим понятие термина над множеством M :

- 1) Если $u \in U$, то u — терм над M .
- 2) Если F — автомат с $n \in \mathbb{N}$ входами, $F \in M$, $\tau_1, \tau_2, \dots, \tau_n$ — термы над M , то выражение $F(\tau_1, \tau_2, \dots, \tau_n)$ — терм над M .

Термы, отличные от переменных, назовём собственными. Пусть τ — произвольный терм, (x_1, x_2, \dots, x_m) — набор попарно различных переменных, содержащий все переменные, использованные при построении термина τ . Тогда через $\tau(x_1, x_2, \dots, x_m)$ обозначим функцию $\tau : E^m \rightarrow E$, определяемую индуктивно:

- 1) Если $\tau = x_c$ — переменная, $\gamma = (\gamma^1, \gamma^2, \dots, \gamma^m) \in E^m$, то определим

$$\tau(x_1, x_2, \dots, x_m)(\gamma) = \gamma^c.$$

- 2) Если $\tau = F(\tau_1, \tau_2, \dots, \tau_n)$, $\gamma = (\gamma^1, \gamma^2, \dots, \gamma^m) \in E^m$, то определим

$$\begin{aligned} \tau(x_1, x_2, \dots, x_m)(\gamma) &= \\ &= F(\tau_1(x_1, x_2, \dots, x_m)(\gamma), \dots, \tau_n(x_1, x_2, \dots, x_m)(\gamma)). \end{aligned}$$

О функции T , такой что $T = \tau(x_1, x_2, \dots, x_m)$ для некоторого собственного термина τ над множеством M , будем говорить, что она получена термальными операциями из дефинитных автоматов множества M . Нетрудно проверить, что функция T также будет дефинитным автоматом, поэтому мы можем ввести на множестве \mathcal{P}_a оператор замыкания $[]$ относительно термальных операций — такое отображение, которое каждому множеству $M \subseteq \mathcal{P}_a$ сопоставляет множество

$[M]$ всех автоматов, которые можно получить термальными операциями из автоматов множества M . Определённый выше оператор замыкания также известен как оператор замыкания относительно операции суперпозиции [9].

Множество M называется замкнутым, если $[M] = M$; множество M называется полным, если $[M] = \mathcal{P}_a$. Пусть $\tau \in \mathbb{N}$, скажем, что автоматы T_1 и T_2 с n входами τ -равны, если для любого $i \leq \tau$ выполняется $T_1^i = T_2^i$. Обозначим через $[M]_\tau$ множество всех дефинитных автоматов, τ -равных получающимся из M с помощью термальных операций. Множество M называется A -полным, если $[M]_\tau = \mathcal{P}_a$ для любого τ . Определим $[M]_A = \bigcap_{\tau=1}^{\infty} [M]_\tau$. Проблема A -полноты для \mathcal{P}_a состоит в описании всех A -полных множеств M . Множество M называется A -замкнутым, если $[M]_A = M$; M называется A -предполным, если $[M]_A \neq \mathcal{P}_a$ и для любой $f \notin M$ выполняется $[M \cup \{f\}]_A = \mathcal{P}_a$.

Нетрудно заметить, что дефинитные автоматы — это все автоматы, которые можно получить с помощью термальных операций из автоматов из P_2 и задержки. Другими словами $[P_2 \cup S_c] = \mathcal{P}_a$, где S_c — задержка с начальным состоянием c . Отсюда, в частности, следует, что $[\{\bar{x} \vee \bar{y}, S_c\}] = \mathcal{P}_a$.

Постом полностью описаны все замкнутые относительно операции суперпозиции классы булевых функций [1, 2]. Все они конечнопорожденные и образуют счётную решетку по включению.

Пусть F — замкнутый класс булевых функций. Определим проблему A -ПОЛНОТА(F): дана конечная система ν дефинитных автоматов, заданных своими порождающими функциями; требуется установить, A -полна ли система $F \cup \nu$. Ранее было показано, что для верхнего элемента решётки $F = P_2$ проблема A -ПОЛНОТА(F) алгоритмически разрешима [8], а для нижнего элемента решетки проблема A -ПОЛНОТА(F) алгоритмически неразрешима [7].

Нетрудно убедиться, что если $F \subseteq F'$ и проблема A -ПОЛНОТА(F) алгоритмически разрешима, то A -ПОЛНОТА(F') также алгоритмически разрешима. Аналогично, если F^* — класс, двойственный к F относительно замены 0 на 1, и проблема A -ПОЛНОТА(F) алгоритмически разрешима, то A -ПОЛНОТА(F^*) также алгоритмически разрешима.

Воспользуемся обозначениями из [1]. Для $\mu \geq 2$

$$h_\mu(x_1, x_2, \dots, x_{\mu+1}) = \bigvee_{i=1}^{\mu+1} x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_{\mu+1},$$

h_μ^* — функция, двойственная к h_μ . В частности

$$h_2(x_1, x_2, x_3) = x_1 x_2 \vee x_2 x_3 \vee x_1 x_3.$$

$$F_2^3 = [\{h_3^*\}], F_6^3 = [\{h_3\}], D_2 = [\{h_2\}], L_4 = [\{x + y + z\}].$$

Теорема 1. *Проблема А-ПОЛНОТА(F) алгоритмически разрешима для каждого $F \in \{F_2^3, F_6^3, D_2, L_4\}$.*

2. Основные утверждения

Определение 1. Говорим, что автомат с n входами $T \in \mathcal{P}_a$ сохраняет $C \subseteq E_2^p$, если для любых $\alpha_1, \alpha_2, \dots, \alpha_n \in C$ выполняется $T(\alpha_1, \alpha_2, \dots, \alpha_n) \in C$.

Определение 2. Говорим, что автомат с n входами $T \in \mathcal{P}_a$ сохраняет $C \subseteq E_2^p \times E_2^p$, если для любых $(\alpha_1, \beta_1), \dots, (\alpha_n, \beta_n) \in C$ выполняется $(T(\alpha_1, \dots, \alpha_n), T(\beta_1, \dots, \beta_n)) \in C$.

Для $C \subseteq E_2^p$, либо $C \subseteq E_2^p \times E_2^p$ через $U(C)$ обозначим класс всех автоматов, сохраняющих C .

Снова воспользуемся обозначениями из [1].

$D_3 \subset P_2, D_3 = [\{x\bar{y} \vee x\bar{z} \vee \bar{y}\bar{z}\}]$ — множество всех самодвойственных функций в P_2 .

$L_1 \subset P_2, L_1 = [\{x + y, 1\}]$ — множество всех линейных функций в P_2 .

$A_1 \subset P_2, A_1 = [\{x \vee y, xy, 0, 1\}]$ — множество всех монотонных функций в P_2 .

Пусть $p \in \mathbb{N}$, $\alpha_1, \alpha_2, \dots, \alpha_n \in E_2^{p-1}$, T — дефинитный автомат с n входами. Тогда через $T^{p, (\alpha_1, \alpha_2, \dots, \alpha_n)}$ обозначим функцию из P_2 , такую что

$$T^{p, (\alpha_1, \alpha_2, \dots, \alpha_n)}(b_1, b_2, \dots, b_n)$$

для любых $b_1, b_2, \dots, b_n \in E_2$.

Определим семейства, которые нам понадобятся в дальнейшем.

1) Рассмотрим два семейства классов

$$\begin{aligned}\tilde{C} &= \{U(C) | \exists p, C \subset E_2^p, \forall \alpha \in E_2^{p-1} \exists b \in E_2 (\alpha b \in C)\} \\ \tilde{C}^h &= \{U(C) | \exists p \leq h, C \subset E_2^p, \forall \alpha \in E_2^{p-1} \exists b \in E_2 (\alpha b \in C)\}\end{aligned}$$

2) Для $p \geq 2$ определим класс $\tilde{S}_p \subseteq \mathcal{P}_a$. Пусть $C \subseteq E_2^p \times E_2^p$,

$$C = \{(\alpha, \beta) |]_{p-2}\alpha =]_{p-2}\beta, \alpha(p) = \beta(p)\}.$$

Тогда $\tilde{S}_p = U(C)$. Легко проверить, что \tilde{S}_p — множество автоматов, у которых выход в момент времени p не зависит от входа в момент времени $p - 1$. Пусть

$$\begin{aligned}\tilde{S} &= \{\tilde{S}_p | p \geq 2\}, \\ \tilde{S}^h &= \{\tilde{S}_p | 2 \leq p \leq h\}.\end{aligned}$$

3) Для $p \geq 1$ определим класс $\tilde{D}_p \subseteq \mathcal{P}_a$.

$$T \in \tilde{D}_p \Leftrightarrow \forall \alpha_1, \dots, \alpha_n \in E_2^{p-1} (T^{p, (\alpha_1, \dots, \alpha_n)} \in D_3).$$

То есть, \tilde{D}_p — множество всех автоматов, у которых выход в момент времени p самодвойственно зависит от входа в момент времени p . Пусть

$$\begin{aligned}\tilde{D} &= \{\tilde{D}_p | p \geq 1\}. \\ \tilde{D}^h &= \{\tilde{D}_p | 1 \leq p \leq h\}.\end{aligned}$$

4) Для $p \geq 1$ определим класс $\tilde{L}_p \subseteq \mathcal{P}_a$.

$$T \in \tilde{L}_p \Leftrightarrow \forall \alpha_1, \dots, \alpha_n \in E_2^{p-1} (T^{p, (\alpha_1, \dots, \alpha_n)} \in L_1).$$

То есть, \tilde{L}_p — множество всех автоматов, у которых выход в момент времени p линейно зависит от входа в момент времени p . Пусть

$$\begin{aligned}\tilde{L} &= \{\tilde{L}_p | p \geq 1\}. \\ \tilde{L}^h &= \{\tilde{L}_p | 1 \leq p \leq h\}.\end{aligned}$$

5) Для $p \geq 1$ определим класс $\tilde{A}_p \subseteq \mathcal{P}_a$.

$$T \in \tilde{A}_p \Leftrightarrow \forall \alpha_1, \dots, \alpha_n \in E_2^{p-1} (T^{p, (\alpha_1, \dots, \alpha_n)} \in A_1).$$

То есть \tilde{A}_p — множество всех автоматов, у которых выход в момент времени p монотонно зависит от входа в момент времени p . Пусть

$$\begin{aligned} \tilde{A} &= \{\tilde{A}_p | p \geq 1\}. \\ \tilde{A}^h &= \{\tilde{A}_p | 1 \leq p \leq h\}. \end{aligned}$$

6) Для $p \geq 2$ определим класс $\tilde{K}_p \subseteq \mathcal{P}_a$. Пусть $K_p \subseteq E_2^p \times E_2^p$,

$$K_p = \{(\alpha ab, \alpha cd) | \alpha \in E_2^{p-2}, a, b, c, d \in E_2 (a + b = c + d)\}.$$

Тогда $\tilde{K}_p = U(K_p)$. Пусть

$$\begin{aligned} \tilde{K} &= \{\tilde{K}_p | p \geq 2\}. \\ \tilde{K}^h &= \{\tilde{K}_p | 2 \leq p \leq h\}. \end{aligned}$$

Обозначим $\tilde{W} = \tilde{C} \cup \tilde{S} \cup \tilde{D} \cup \tilde{L} \cup \tilde{A} \cup \tilde{K}$.

Утверждение 1. *Каждый класс из \tilde{W} является A -предполным классом.*

Следует отметить, что эти семейства A -предполных классов ранее исследовались В. А. Бувичем для конечных автоматов [5].

Утверждение 2. *Пусть $M \subseteq \mathcal{P}_a$, $x + y + z \in M$, тогда M — A -полно тогда и только тогда, когда для любого $V \in \tilde{W}$ выполняется $M \not\subseteq V$.*

Утверждение 3. *Пусть $M \subseteq \mathcal{P}_a$, $h_k \in M$, $k \geq 2$, тогда M — A -полно тогда и только тогда, когда для любого $V \in \tilde{W}$ выполняется $M \not\subseteq V$.*

Обозначим $\tilde{W}_1^h = \tilde{C}^{2^{2h+1}+4h} \cup \tilde{S}^h \cup \tilde{D}^h \cup \tilde{L}^h \cup \tilde{K}^{h+1}$.

Утверждение 4. *Пусть $M \subseteq \mathcal{P}_a^h$, $x + y + z \in M$, тогда M — A -полно тогда и только тогда, когда для любого $V \in \tilde{W}_1^h$ выполняется $M \not\subseteq V$.*

Обозначим $\widetilde{W}_2^h = \widetilde{C}^{3h+3h} \cup \widetilde{S}^h \cup \widetilde{D}^h \cup \widetilde{A}^h$.

Утверждение 5. Пусть $M \subseteq \mathcal{P}_a^h, h_2 \in M$, тогда M — A -полно тогда и только тогда, когда для любого $V \in \widetilde{W}_2^h$ выполняется $M \not\subseteq V$.

Обозначим $\widetilde{W}_3^h = \widetilde{C}^{4h \cdot 2^{8h^2} + 4h} \cup \widetilde{S}^h \cup \widetilde{A}^h$.

Утверждение 6. Пусть $M \subseteq \mathcal{P}_a^h, h_3^* \in M$, тогда M — A -полно тогда и только тогда, когда для любого $V \in \widetilde{W}_3^h$ выполняется $M \not\subseteq V$.

Доказательство теоремы 1. Для определённости положим $F = D_2$. Пусть дана конечная система ν дефинитных автоматов. Выберем h так, чтобы $\nu \subseteq \mathcal{P}_a^h$. Из утверждения 5 следует, что $F \cup \nu$ — A -полно тогда и только тогда, когда для любого $V \in \widetilde{W}_2^h$ выполняется $\{h_2\} \cup \nu \not\subseteq V$. Для каждого $V \in \widetilde{W}_2^h$ существует алгоритм проверки принадлежности $\{h_2\} \cup \nu$ множеству V , а множество \widetilde{W}_2^h конечно. Значит, проблема A -ПОЛНОТА(F) алгоритмически разрешима. Теорема доказана.

3. Доказательство утверждений

Лемма 1. Для любого $C \subseteq E_2^p$ множество $U(C)$ A -замкнуто.

Доказательство. Сначала покажем, что класс $U(C)$ замкнут. Пусть автомат T реализуется термом

$$T_0(T_1(x_1, x_2, \dots, x_n), \dots, T_m(x_1, x_2, \dots, x_n)).$$

Рассмотрим произвольные $\alpha_1, \alpha_2, \dots, \alpha_n \in C$.

Пусть $T_i(\alpha_1, \alpha_2, \dots, \alpha_n) = \beta_i \in C$ для $i \in \{1, 2, \dots, m\}$. Так как $T_0 \in U(C)$, то $T_0(\beta_1, \beta_2, \dots, \beta_m) = \gamma \in C$. Значит $T(\alpha_1, \alpha_2, \dots, \alpha_n) = \gamma \in C$ и $T \in U(C)$. То есть $[U(C)] = U(C)$.

Но очевидно, что если автоматы Q_1 и Q_2 p -равны и $Q_1 \in U(C)$, то $Q_2 \in U(C)$. Значит $[U(C)]_p \subseteq U(C)$. Тогда

$$U(C) \subseteq [U(C)]_A \subseteq [U(C)]_p \subseteq U(C)$$

и $[U(C)]_A = U(C)$. Лемма установлена.

Следующая лемма доказывается полностью аналогично.

Лемма 2. Для любого $C \subseteq E_2^p \times E_2^p$ множество $U(C)$ A -замкнуто.

Для $d \in E_2, q \in \mathbb{N}$ определим $C_{d,q} = \{\alpha \in E_2^q \mid \alpha(q) = d\}$. $U(C_{d,q})$ можно понимать, как класс всех автоматов, сохраняющих d в момент времени q . Пусть

$$\begin{aligned}\tilde{C}_d &= \{U(C_{d,q}) \mid q \geq 1\}, \\ \tilde{C}_d^h &= \{U(C_{d,q}) \mid 1 \leq q \leq h\}.\end{aligned}$$

Лемма 3. Пусть $C \subset E_2^p$, причём для любого $\alpha \in E_2^{p-1}$ существует $b \in E_2$, такое что $\alpha b \in C$, тогда $M = U(C)$ — A -предполный класс в \mathcal{P}_a .

Доказательство. Из леммы 1 следует, что $[M]_A = M$. Так как $C \neq E_2^p$, то найдётся автомат $T \in \mathcal{P}_a$, такой что $T(x) = \alpha 0^\infty$ для любого $x \in E$, где $\alpha \in E_2^p, \alpha \notin C$. Тогда $T \notin M$ и $M \neq \mathcal{P}_a$.

Теперь докажем, что для произвольного автомата с n выходами $T \notin M$ выполняется $[M \cup \{T\}] = \mathcal{P}_a$. Так как $T \notin M$, то существуют $\alpha_1, \alpha_2, \dots, \alpha_n \in C$ такие что $T(\alpha_1, \alpha_2, \dots, \alpha_n) \notin C$. Для любого i рассмотрим автомат с одним входом T_i , такой что $T_i(x) = \alpha_i 0^\infty$ для любого $x \in E$. Легко проверить, что $T_i \in M$ для любого i .

Пусть $Q \in \mathcal{P}_a, Q$ — автомат с n входами. Покажем, что $Q \in [M \cup \{T\}]$. Положим $h = \max(p + 1, h(Q))$. Определим автомат Q_0 высоты h с $n + 1$ входом. Пусть

$$Q_0^s(\beta_1, \beta_2, \dots, \beta_n, \beta_{n+1}) = Q^s(\beta_1, \beta_2, \dots, \beta_n),$$

если $s \neq p$, либо $s = p$ и $\beta_{n+1} \notin C$; иначе выберем для $\gamma =]_{p-1}Q(\beta_1, \beta_2, \dots, \beta_n)$ такое b_γ , что $\gamma b_\gamma \in C$ и положим

$$Q_0^s(\beta_1, \beta_2, \dots, \beta_n, \beta_{n+1}) = b_\gamma.$$

Легко проверить, что $Q_0 \in M$ и

$$Q(x_1, x_2, \dots, x_n) = Q_0(x_1, x_2, \dots, x_n, T(T_1(x_1), T_2(x_1), \dots, T_n(x_1))).$$

Значит $Q \in [M \cup \{T\}]$ и $[M \cup \{T\}] = \mathcal{P}_a$. Лемма доказана.

Лемма 4. \tilde{S}_p — A -предполный класс в \mathcal{P}_a .

Доказательство. Из леммы 2 следует, что $[\tilde{S}_p]_A = \tilde{S}_p$. Нетрудно убедиться, что единичная задержка с начальным состоянием 0 не принадлежит \tilde{S}_p , значит $\tilde{S}_p \neq \mathcal{P}_a$.

Теперь докажем, что для произвольного автомата с n выходами $T \notin \tilde{S}_p$ выполняется $[\tilde{S}_p \cup \{T\}] = \mathcal{P}_a$. По определению $\tilde{S}_p = U(C)$, где $C \subseteq E_2^p \times E_2^p$,

$$C = \{(\alpha, \beta) \mid]_{p-2}\alpha =]_{p-2}\beta, \alpha(p) = \beta(p)\}.$$

Так как $T \notin \tilde{S}_p$, то существуют пары $(\alpha_1, \beta_1), \dots, (\alpha_n, \beta_n) \in C$, такие что

$$T(\alpha_1, \alpha_2, \dots, \alpha_n) = \gamma, T(\beta_1, \beta_2, \dots, \beta_n) = \delta,$$

причём $(\gamma, \delta) \notin C$. Значит $\gamma(p) \neq \delta(p)$. Для определённости будем считать, что $\gamma(p) < \delta(p)$. Для каждого i определим автомат с одним входом $T_i : T_i(\epsilon) = \alpha_i 0^\infty$, если $\epsilon(p-1) = 0$; и $T_i(\epsilon) = \beta_i 0^\infty$, если $\epsilon(p-1) = 1$. Легко проверить, что $T_i \in \tilde{S}_p$ для любого i . Пусть $R(x) = T(T_1(x), T_2(x), \dots, T_n(x))$. Тогда $R^p(\alpha) = \alpha(p-1)$ для любого $\alpha \in E_2^p$.

Определим Q — автомат с двумя входами высоты $p+1$: $Q^1(a, b) = 1$; $Q^s(\alpha, \beta) = \alpha(s-1)$ для $s \neq p$ и $s \geq 2$; $Q^p(\alpha, \beta) = \beta(p)$. Нетрудно убедиться, что $Q \in \tilde{S}_p$. Автомат $G(x) = Q(x, R(x)) \in [\tilde{S}_p \cup \{T\}]$ является единичной задержкой с начальным состоянием 1. Легко проверить, что $P_2 \subset \tilde{S}_p$. Значит $[\tilde{S}_p \cup \{T\}] \supseteq [P_2 \cup \{G\}] = \mathcal{P}_a$. Лемма доказана.

Лемма 5. \tilde{D}_p — A -предполный класс в \mathcal{P}_a .

Доказательство. Покажем, что класс \tilde{D}_p A -замкнут. Пусть автомат T реализуется термом

$$T_0(T_1(x_1, x_2, \dots, x_n), \dots, T_m(x_1, x_2, \dots, x_n)).$$

Рассмотрим произвольное $r = (\alpha_1, \alpha_2, \dots, \alpha_n) \in (E_2^{p-1})^n$. Пусть $T_i(r) = \beta_i$ для любого $i \in \{1, 2, \dots, m\}$, $r_0 = (\beta_1, \beta_2, \dots, \beta_m)$. Легко проверить, что для любых $b_1, b_2, \dots, b_n \in E_2$ выполняется

$$T^{p,r}(b_1, b_2, \dots, b_n) = T_0^{p,r_0}(T_1^{p,r}(b_1, b_2, \dots, b_n), \dots, T_m^{p,r}(b_1, b_2, \dots, b_n)).$$

Так как $T_0^{p,r_0}, T_1^{p,r}, T_2^{p,r}, \dots, T_m^{p,r} \in D_3$, а класс D_3 замкнут в P_2 , то $T^{p,r} \in D_3$. То есть $[\tilde{D}_p] = \tilde{D}_p$. Но очевидно, что если автоматы Q_1 и Q_2 p -равны и $Q_1 \in \tilde{D}_p$, то $Q_2 \in \tilde{D}_p$. Значит $[\tilde{D}_p]_p \subseteq \tilde{D}_p$. Тогда

$$\tilde{D}_p \subseteq [\tilde{D}_p]_A \subseteq [\tilde{D}_p]_p \subseteq \tilde{D}_p$$

и $[\tilde{D}_p]_A = \tilde{D}_p$.

Константа 0 не принадлежит \tilde{D}_p , значит $\tilde{D}_p \neq \mathcal{P}_a$.

Теперь докажем, что для произвольного автомата с n выходами $T \notin \tilde{D}_p$ выполняется $[\tilde{D}_p \cup \{T\}] = \mathcal{P}_a$.

Так как $T \notin \tilde{D}_p$, то существуют $\alpha_1, \dots, \alpha_n \in E_2^{p-1}$, $b_1, \dots, b_n \in E_2$, $d \in E_2$, такие что

$$T(\alpha_1 b_1, \alpha_2 b_2, \dots, \alpha_n b_n) = T(\alpha_1 \bar{b}_1, \alpha_2 \bar{b}_2, \dots, \alpha_n \bar{b}_n) = d,$$

Для каждого i определим автомат с одним входом $T_i : T_i(\epsilon) = \alpha_i b_i 0^\infty$, если $\epsilon(p) = 0$; и $T_i(\epsilon) = \alpha_i \bar{b}_i 0^\infty$, если $\epsilon(p) = 1$. Легко проверить, что $T_i \in \tilde{D}_p$ для любого i .

Пусть $R(x) = T(T_1(x), T_2(x), \dots, T_n(x))$. Нетрудно убедиться, что $R^p(\alpha) = d$ для любого $\alpha \in E_2^p$.

Определим Q — автомат с одним входом высоты $p+1 : Q^s(\alpha) = d$ для $s \neq p$; $Q^p(\alpha) = \alpha(p)$. Легко проверить, что $Q \in \tilde{D}_p$. Автомат $G(x) = Q(R(x)) \in [\tilde{D}_p \cup \{T\}]$ является константой d . Теперь рассмотрим автомат $Q_0(x_1, x_2) = S_0(x_1) + x_2 + d$, где S_0 — единичная задержка с начальным состоянием 0. Нетрудно убедиться, что $Q_0 \in \tilde{D}_p$.

Легко проверить, что $S_0(x) = Q_0(x, G(x))$, значит S_0 принадлежит $[\tilde{D}_p \cup \{T\}]$. Учитывая, что $D_3 \subset \tilde{D}_p$, $[D_3 \cup \{d\}] = P_2$ и $[P_2 \cup \{S_0\}] = \mathcal{P}_a$, получаем $[\tilde{D}_p \cup \{T\}] = \mathcal{P}_a$. Лемма доказана.

Следующие две леммы доказываются аналогично.

Лемма 6. \tilde{L}_p — A -предполный класс в \mathcal{P}_a .

Лемма 7. \tilde{A}_p — A -предполный класс в \mathcal{P}_a .

Лемма 8. \tilde{K}_p — A -предполный класс в \mathcal{P}_a .

Доказательство. Из леммы 2 следует, что $[\tilde{K}_p]_A = \tilde{K}_p$. Рассмотрим автомат T_0 высоты p с одним входом: $T_0^s(\alpha) = 0$, если $s < p$; $T_0^p(\alpha) = \alpha(p)$. Легко проверить, что $(0^p, 0^{p-2}11) \in K_p$, $T_0(0^p) = 0^p$, $T_0(0^{p-2}11) = 0^{p-1}1$, а $(0^p, 0^{p-1}1) \notin K_p$. Значит, T_0 не принадлежит \tilde{K}_p и $\tilde{K}_p \neq \mathcal{P}_a$.

Теперь докажем, что для произвольного автомата T с n выходами, такого что $T \notin \tilde{K}_p$, выполняется $[\tilde{K}_p \cup \{T\}] = \mathcal{P}_a$. Так как $T \notin \tilde{K}_p$, то существуют пары $(\alpha_1, \beta_1), \dots, (\alpha_n, \beta_n) \in K_p$, такие что $T(\alpha_1, \alpha_2, \dots, \alpha_n) = \gamma$, $T(\beta_1, \beta_2, \dots, \beta_n) = \delta$, причём $(\gamma, \delta) \notin K_p$. Для любого i определим автомат с одним входом $T_i : T_i(\epsilon) = \alpha_i 0^\infty$, если $\epsilon(p-1) = 0$; и $T_i(\epsilon) = \beta_i 0^\infty$, если $\epsilon(p-1) = 1$. Легко проверить, что $T_i \in \tilde{K}_p$ для любого i . Заметим, что $x_1 + x_2 \in \tilde{K}_p$. Также все автоматы, выход которых не зависит от входа, принадлежат \tilde{K}_p . Если это не вызывает противоречий, в формулах такие автоматы будем обозначать сверхсловом, которое они дают на выходе.

Пусть $R(x) = T(T_1(x), T_2(x), \dots, T_n(x))$. Легко проверить, что $R(\epsilon) = \gamma$, если $\epsilon \in E_2^p$, $\epsilon(p-1) = 0$; и $R(\epsilon) = \delta$, если $\epsilon \in E_2^p$, $\epsilon(p-1) = 1$. Пусть $R_0(x) = R(x) + \gamma 0^\infty \in [\tilde{K}_p \cup \{T\}]$.

Рассмотрим два случая. Пусть $\gamma(p-1) = \delta(p-1)$, тогда R_0 обладает следующим свойством: $R_0^s(\epsilon) = 0$ для $s \leq p-1$; $R_0^p(\epsilon) = \epsilon(p-1)$. Определим автомат R_1 с одним входом. Пусть $R_1^s(\epsilon) = 0$ для $s \leq p-2$; $R_1^{p-1}(\epsilon) = \epsilon(p-1)$; $R_1^p(\epsilon) = \epsilon(p-1)$; $R_1^s(\epsilon) = R_0^s(\epsilon)$, если $s > p$. Легко проверить, что $R_1 \in \tilde{K}_p$. Тогда автомат $R_2(x) = R_1(x) + R_0(x)$ обладает следующим свойством: $R_2^s(\epsilon) = 0$ если $s \neq p-1$; $R_2^{p-1}(\epsilon) = \epsilon(p-1)$.

Рассмотрим второй случай. Пусть $\gamma(p-1) \neq \delta(p-1)$, тогда R_0 обладает следующим свойством: $R_0^s(\epsilon) = 0$ для $s \leq p-2$; $R_0^{p-1}(\epsilon) = \epsilon(p-1)$; $R_0^p(\epsilon) = 0$. Определим автомат $R_3 \in \tilde{K}_p$ с одним входом. Пусть $R_3^s(\epsilon) = 0$ для $s \leq p$; $R_3^s(\epsilon) = R_0^s(\epsilon)$, если $s > p$. В этом случае обозначим $R_2(x) = R_0(x) + R_3(x)$. То есть в обоих случаях получили автомат R_2 , который в момент времени $p-1$ работает, как тождественный, а в остальные моменты времени как константа 0.

Определим автомат с одним входом $R_4 : R_4^s(\epsilon) = 0$, если $s \notin \{p-1, p\}$; $R_4^s(\epsilon) = \epsilon(s)$, если $s \in \{p-1, p\}$. Легко проверить, что $R_4 \in \tilde{K}_p$.

Пусть $R_5(x) = R_4(x) + R_2(x)$, тогда R_5 обладает следующим свойством: $R_5^s(\epsilon) = 0$ для $s \neq p$; $R_5^p(\epsilon) = \epsilon(p)$.

Определим Q — автомат с двумя входами высоты $p+1$: $Q^s(\alpha, \beta) = 0$

для $s \neq p$; $Q^p(\alpha, \beta) = (\alpha(p-1) + \alpha(p)) \& (\beta(p-1) + \beta(p))$. Нетрудно убедиться, что $Q \in \tilde{K}_p$. Автомат $Q_1(x_1, x_2) = Q(R_5(x_1), R_5(x_2)) \in [\tilde{K}_p \cup \{T\}]$ обладает следующим свойством: $Q_1^s(\alpha, \beta) = 0$ для $s \neq p$; $Q_1^p(\alpha, \beta) = \alpha(p) \& \beta(p)$.

Определим Q_2 — автомат с двумя входами высоты $p+1$: $Q_2^s(\alpha, \beta) = \alpha(s) \& \beta(s)$ для $s \neq p$; $Q_2^p(\alpha, \beta) = \alpha(p-1) \& \beta(p-1)$. Нетрудно убедиться, что $Q_2 \in \tilde{K}_p$. Но

$$x_1 \& x_2 = Q_2(x_1, x_2) + R_5(Q_2(x_1, x_2)) + Q_1(x_1, x_2).$$

Так как $0, 1, x_1 + x_2 \in \tilde{K}_p$ и $\{[x_1 + x_2, 0, 1, x_1 \& x_2]\} = P_2$, то $P_2 \subseteq [\tilde{K}_p \cup \{T\}]$.

Определим автомат с одним входом $G_1 : G_1^1(\epsilon) = 1$; $G_1^s(\epsilon) = \epsilon(s-1)$ для $s \geq 2, s \neq p$; $G_1^p(\epsilon) = \epsilon(p-2)$, если $p \geq 3$; $G_1^p(\epsilon) = 1$, если $p = 2$. Также определим G_2 — автомат с одним входом: $G_2^s(\epsilon) = 0$ для $s \notin \{p-1, p\}$; $G_2^{p-1}(\epsilon) = \epsilon(p-1)$; $G_2^p(\epsilon) = \epsilon(p-1)$. Нетрудно убедиться, что $G_1, G_2 \in \tilde{K}_p$.

Тогда $G(x) = G_1(x) + R_5(G_1(x)) + R_5(G_2(x)) \in [\tilde{K}_p \cup \{T\}]$, причём $G(x)$ — единичная задержка с начальным состоянием 1. Но $[P_2 \cup G] = \mathcal{P}_a$, значит $[\tilde{K}_p \cup \{T\}] = \mathcal{P}_a$. Лемма доказана.

Утверждение 1 следует из лемм 3–8.

Лемма 9. Пусть $M \subseteq \mathcal{P}_a$, для любого $V \in \{U(C_{0,1}), U(C_{1,1}), \tilde{D}_1, \tilde{L}_1, \tilde{A}_1\}$ выполняется $M \not\subseteq V$, тогда $[M]_1 = \mathcal{P}_a$.

Доказательство. Для произвольного множества $W \subseteq \mathcal{P}_a$ определим множество

$$W^1 = \{f \in P_2 \mid \exists T \in W, f = T^1\}.$$

Нетрудно убедиться, что для любого $W \subseteq \mathcal{P}_a$ выполняется $[W]^1 = [W^1]$.

Покажем, что $[M^1] = P_2$. Предположим, что это не так, тогда по теореме о полноте [1, 2] множество M^1 содержится в одном из классов C_2, C_3, D_3, L_1, A_1 , где C_2 — класс всех булевых функций, сохраняющих 1, а C_3 — класс всех булевых функций, сохраняющих 0. Если $M^1 \subseteq C_2$, то нетрудно убедиться, что $M \subseteq U(C_{1,1})$, что противоречит условию. Аналогично, если $M^1 \subseteq C_3$, то $M \subseteq U(C_{0,1})$,

что противоречит условию. Если $M^1 \subseteq D_3$, то легко проверить, что $M \subseteq D_1$, что невозможно. Аналогично, если $M^1 \subseteq L_1$ или $M^1 \subseteq A_1$, то $M \subseteq \tilde{L}_1$ или $M \subseteq \tilde{A}_1$, что невозможно. Таким образом $[M^1] = P_2$. Тогда $[M]^1 = P_2$ и $[M]_1 = P_a$.

Лемма 10. Пусть $M \subseteq \mathcal{P}_a$, $p \in \mathbb{N}$, $\delta_1, \delta_2 \in E_2^p$, $C = \{(T(\delta_1), T(\delta_2)) | T \in [M], n(T) = 1\}$. Тогда M сохраняет C .

Доказательство. Пусть $T \in M$ — автомат с n входами, $(\alpha_i, \beta_i) \in C$ для $i = 1, 2, \dots, n$. Для каждого i рассмотрим автомат $T_i \in [M]$ такой, что $T_i(\delta_1) = \alpha_i$, $T_i(\delta_2) = \beta_i$. Автомат $T'(x) = T(T_1(x), T_2(x), \dots, T_n(x))$ принадлежит $[M]$. Значит $(T'(\delta_1), T'(\delta_2)) \in C$. Но $T'(\delta_1) = T(\alpha_1, \alpha_2, \dots, \alpha_n)$, $T'(\delta_2) = T(\beta_1, \beta_2, \dots, \beta_n)$. Отсюда следует, что $T \in U(C)$. Лемма доказана.

Лемма 11. Пусть $M \subseteq \mathcal{P}_a$ и для любого $V \in \tilde{C} \cup \tilde{D}$ выполняется $M \not\subseteq V$, тогда для любых $p \in \mathbb{N}$ и $\alpha \in E_2^p$ существует автомат с одним входом $Z_\alpha \in [M]$, такой что $Z_\alpha(\beta) = \alpha$ для любого $\beta \in E_2^p$.

Доказательство. Сначала покажем, что если $M \subseteq U(C)$, где $C \subset E_2^p$, то для какого-то $V \in \tilde{C}$ выполняется $M \subseteq V$. Для каждого l от 1 до p построим множество

$$C_l = \{l\gamma | \gamma \in C\}.$$

Легко проверить, что для любого l выполняется $M \subseteq U(C_l)$. Рассмотрим максимальное l , такое что $C_l = E_2^l$. Если такого l не существует, то положим $l = 0$. Тогда $M \subseteq U(C_{l+1}) \in \tilde{C}$.

Перейдём к доказательству леммы. Будем доказывать индукцией по p . Пусть

$$C = \{(T(0^p), T(0^{p-1}1)) | T \in [M], n(T) = 1\}.$$

Очевидно, что C не пусто. Из леммы 10 следует, что M сохраняет C .

Пусть C_1 — множество всех γ , таких что $(\gamma, \gamma) \in C$. Предположим, что C_1 не пусто. Покажем, что $M \subseteq U(C_1)$. Пусть $T \in M$ — автомат с n входами, $\alpha_1, \alpha_2, \dots, \alpha_n \in C_1$, $T(\alpha_1, \alpha_2, \dots, \alpha_n) = \gamma$. Так как T сохраняет C , и для любого i выполняется $(\alpha_i, \alpha_i) \in C$, то $(\gamma, \gamma) \in C$, значит T сохраняет C_1 и $M \subseteq U(C_1)$. Если $C_1 \neq E_2^p$, то для какого-то

$V \in \tilde{C}$ выполняется $M \subseteq V$, что противоречит условию. Значит $C_1 = E_2^p$. Если $p \geq 2$, то по предположению индукции существует автомат с одним входом $Z_{0^{p-1}} \in [M]$, такой что $Z_{0^{p-1}}(\beta) = 0^{p-1}$ для любого $\beta \in E_2^{p-1}$. Если же $p = 1$, то через $Z_{0^{p-1}}$ обозначим произвольный автомат с одним входом из $[M]$. Так как $C_1 = E_2^p$, то для любого $\alpha \in E_2^p$ существует автомат $Z'_\alpha \in [M]$, такой что $Z'_\alpha(0^p) = Z'_\alpha(0^{p-1}1) = \alpha$. Тогда автомат $Z_\alpha(x) = Z'_\alpha(Z_{0^{p-1}}(x))$ — искомый и лемма доказана.

Теперь рассмотрим случай, когда C_1 пусто. Пусть C_2 — множество всех γ , таких что для какого-то $\delta \in E_2^p$ выполняется $(\gamma, \delta) \in C$. Так как M сохраняет C , то M сохраняет C_2 . Если $C_2 \neq E_2^p$, то для какого-то $V \in \tilde{C}$ выполняется $M \subseteq V$, что противоречит условию. Значит $C_2 = E_2^p$. Тогда $0^{p-1}1 \in C_2$ и существует автомат $T_0 \in [M]$, такой что $T_0(0^p) = 0^{p-1}1$. Так как C_1 пусто, то $T_0(0^{p-1}1) = 0^p$. Пусть $\gamma \in E_2^{p-1}$. Если $p \geq 2$, то по предположению индукции существует автомат с одним входом $Z_\gamma \in [M]$, такой что $Z_\gamma(\beta) = \gamma$ для любого $\beta \in E_2^{p-1}$. Если же $p = 1$, то через Z_γ обозначим произвольный автомат с одним входом из $[M]$. Так как C_1 пусто, то $Z_\gamma(0^p) \neq Z_\gamma(0^{p-1}1)$. Если $Z_\gamma(0^p) = \gamma 0$, то обозначим $Z'_\gamma(x) = Z_\gamma(x)$, иначе $Z'_\gamma(x) = Z_\gamma(T_0(x))$. Получим, что $Z'_\gamma(0^{p-1}b) = \gamma b$ для любого $\gamma \in E_2^{p-1}$, $b \in E_2$. Так как $M \not\subseteq \tilde{D}_p$, то существует автомат с n входами $T \in M$, $T \notin \tilde{D}_p$. Значит для каких-то $\gamma_1, \gamma_2, \dots, \gamma_n \in E_2^{p-1}$ выполняется

$$T^{p,(\gamma_1, \gamma_2, \dots, \gamma_n)} \notin D_3.$$

Тогда для каких-то $b_1, b_2, \dots, b_n \in E_2$ выполняется

$$T^{p,(\gamma_1, \gamma_2, \dots, \gamma_n)}(b_1, b_2, \dots, b_n) = T^{p,(\gamma_1, \gamma_2, \dots, \gamma_n)}(\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n).$$

Для каждого i от 1 до n обозначим через T_i автомат $Z'_{\gamma_i}(x)$, если $b_i = 1$; автомат $Z'_{\gamma_i}(T_0(x))$, если $b_i = 0$. Пусть $R(x) = T(T_1(x), T_2(x), \dots, T_n(x)) \in [M]$. Нетрудно убедиться, что $R(0^p) = R(0^{p-1}1)$. Но в этом случае C_1 не пусто. Получили противоречие. Лемма доказана.

Доказательство утверждения 2. Необходимость следует из утверждения 1. Докажем достаточность.

Из леммы 11 следует, что для любых $p \in \mathbb{N}$ и $\alpha \in E_2^p$ существует автомат с одним входом $Z_\alpha \in [M]$, такой что $Z_\alpha(\beta) = \alpha$ для любого $\beta \in E_2^p$.

Индукцией по p будем доказывать, что $[M]_p = \mathcal{P}_a$. Для $p = 1$ это следует из леммы 9. Докажем шаг индукции. Пусть $p \geq 2$. Так как $M \notin \tilde{L}_p$, то существует автомат R' и $\alpha_1, \alpha_2, \dots, \alpha_n \in E_2^{p-1}$, такие что

$$R'^{p,(\alpha_1, \alpha_2, \dots, \alpha_n)} \notin L_1.$$

Известно, что подстановкой констант вместо переменных можно из любой нелинейной функции из P_2 получить нелинейную функцию от двух переменных. Отсюда следует, что в автомат R' вместо некоторых переменных можно подставить автоматы вида Z_β , где $\beta \in E_2^p$, так, что мы получим автомат $R \in [M]$ с двумя входами, такой что $R \notin \tilde{L}_p$. Определим функцию

$$l(a_1, a_2, \dots, a_p, b_1, b_2, \dots, b_p) = R^p(a_1 a_2 \dots a_p, b_1 b_2 \dots b_p).$$

Рассмотрим полином Жегалкина функции l и представим её в виде

$$l = a_p b_p l_1 + a_p l_2 + b_p l_3 + l_4,$$

где функции l_1, l_2, l_3, l_4 зависят от переменных $a_1, a_2, \dots, a_{p-1}, b_1, b_2, \dots, b_{p-1}$.

Так как $R \notin \tilde{L}_p$, то l_1 не совпадает с константой 0. Если l_1 не является константой 1 и существенно зависит от переменной a_j , то рассмотрим автомат

$$\begin{aligned} \widehat{R}(x_1, x_2) = R(x_1 + Z_{0^{j-1}10^{p-j}}(x_1) + Z_{0^p}(x_1), x_2) + \\ + R(x_1, x_2) + Z_{0^p}(x_1) \in [M]. \end{aligned}$$

Представим \widehat{R} в таком же виде, что и R . Получим новые функции $\widehat{l}_1, \widehat{l}_2, \widehat{l}_3, \widehat{l}_4$. Легко убедиться, что \widehat{l}_1 не совпадает с константой 0, причём степень \widehat{l}_1 меньше, чем степень l_1 . Если \widehat{l}_1 не совпадает с константой 1, то мы применяем к \widehat{R} то же преобразование, что мы применяли к R . Таким образом, мы можем уменьшать степень l_1 до тех пор, пока l_1 не будет совпадать с константой 1. Поэтому далее будем полагать, что $l_1(a_1, a_2, \dots, a_{p-1}, b_1, b_2, \dots, b_{p-1}) \equiv 1$.

Рассмотрим автомат

$$\widetilde{R}(x_1, x_2) = R(x_1, x_2 + Z_{0^{p-1}}(x_2) + Z_{0^p}(x_2)) + R(x_1, x_2) + Z_{0^p}(x_1) \in [M]$$

и

$$\tilde{l}(a_1, a_2, \dots, a_p, b_1, b_2, \dots, b_p) = \tilde{R}^p(a_1 a_2 \dots a_p, b_1 b_2 \dots b_p).$$

Получим, что

$$\tilde{l}(a_1, a_2, \dots, a_p, b_1, b_2, \dots, b_p) = a_p + l_3(a_1, a_2, \dots, a_{p-1}, b_1, b_2, \dots, b_{p-1}),$$

причём автомат \tilde{R} $(p-1)$ -равен константе 0.

Пусть $R_0 = \tilde{R}(x_1, x_1) + x_1 + Z_{0^p}(x_1) \in [M]$. Легко проверить, что для $s \leq p-1$ выполняется $R_0^s(\alpha) = \alpha(s)$, а выход автомата R_0 в момент времени p не зависит от входа в момент времени p .

Определим автомат W_0 с одним входом высоты $p-1$. $W_0^s(\alpha) = 0$, если $1 \leq s \leq p-2$; $W_0^{p-1}(\alpha) = \alpha(p-1)$. По предположению индукции существует автомат $W_1 \in [M]$, $(p-1)$ -равный автомату W_0 . Тогда автомат $W_2(x) = R_0(W_1(x)) \in [M]$ обладает следующим свойством: если $s \leq p-2$, то $W_2^s(\alpha) = 0$; $W_2^{p-1}(\alpha) = \alpha(p-1)$; $W_2^p(a_1 a_2 \dots a_p) = r(a_{p-1})$, где r — некоторая функция из P_2 . То есть выход автомата W_2 в момент времени p зависит только от входа в момент времени $p-1$. Если $r(0) = 1$, то вместо W_2 рассмотрим автомат $W_2(x) + Z_{0^{p-1}}(x) + Z_{0^p}(x)$. Поэтому будем считать, что $r(0) = 0$.

В случае, если функция r константа 0, положим $W_3(x) = W_2(x)$. Рассмотрим случай, когда функция r не константа. В этом случае $r(a_{p-1}) = a_{p-1}$. Пусть

$$C = \{(T(0^p), T(0^{p-2}11)) \mid T \in [M], n(T) = 1\}.$$

Из леммы 10 следует, что M сохраняет C . Покажем, что $K_p \subseteq C$. Рассмотрим произвольное $(\alpha, \beta) \in K_p$. Если $\alpha = \beta$, то очевидно $(Z_\alpha(0^p), Z_\alpha(0^{p-2}11)) = (\alpha, \alpha) \in C$. Пусть $\alpha \neq \beta$. Так как $x_1 + x_2 + x_3$ сохраняет C и $(\alpha, \alpha), (0^p, 0^p), (0^p, 0^{p-2}11) \in C$, то

$$(\alpha + 0^p + 0^p, \alpha + 0^{p-2}11 + 0^p) = (\alpha, \beta) \in C.$$

Значит $K_p \subseteq C$. Так как $M \not\subseteq \tilde{K}_p$, то $K_p \neq C$ и существует пара $(\alpha, \beta) \in C$, такая что $\alpha(p-1) + \alpha(p) + \beta(p-1) + \beta(p) = 1$. Тогда для $c = \alpha(p-1) + \beta(p-1)$, $d = \alpha(p) + \beta(p)$ выполняется

$$\begin{aligned} (\alpha + \alpha + 0^p, \beta + \alpha + 0^p) &= (0^p, 0^{p-2}cd) \in C, \\ (\alpha + \alpha + 0^p, \beta + \alpha + 0^{p-2}11) &= (0^p, 0^{p-2}\bar{c}\bar{d}) \in C, \end{aligned}$$

причём $c + d = 1$. Таким образом $(0^p, 0^{p-2}10) \in C$. Тогда существует автомат $T_0 \in [M]$, такой что $0^p = T_0(0^p)$, $0^{p-2}10 = T_0(0^{p-2}11)$. Тогда автомат $W_3(x) = T_0(W_2(x)) \in [M]$ обладает следующим свойством: если $s \leq p - 2$, то $W_3^s(\alpha) = 0$; $W_3^{p-1}(\alpha) = \alpha(p - 1)$; $W_3^p(\alpha) = 0$.

Так как $M \not\subseteq \tilde{S}_p$, то существует автомат T и слова $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n \in E_2^p$, такие что $]_{p-2}\alpha_i =]_{p-2}\beta_i$, $\alpha_i(p) = \beta_i(p)$ для любого i и

$$T^p(\alpha_1, \alpha_2, \dots, \alpha_n) < T^p(\beta_1, \beta_2, \dots, \beta_n).$$

Для каждого i от 1 до n положим

$$T_i(x) = \begin{cases} Z_{\alpha_i}(x), & \text{если } \alpha_i = \beta_i, \\ W_3(x) + Z_{\alpha_i}(x) + Z_{0^p}(x), & \text{если } \alpha_i \neq \beta_i. \end{cases}$$

Легко проверить, что $T_i(\delta) = \alpha_i$, если $\delta \in E_2^p$ и $\delta(p-1) = 0$; $T_i(\delta) = \beta_i$, если $\delta \in E_2^p$ и $\delta(p-1) = 1$. Пусть $G_0(x) = T(T_1(x), T_2(x), \dots, T_n(x)) \in [M]$. Тогда $G_0^p(\alpha) = \alpha(p-1)$, $G_0^{p-1}(\alpha) = g_0(\alpha(p-1))$, где g_0 — некоторая функция из P_2 . При этом для любого $s \leq p - 2$ выход автомата G_0 в момент времени s не зависит от того, что подается на вход. Пусть $\beta = G_0(0^p)$. Рассмотрим автомат $G_1(x) = G_0(x) + Z_\beta(x) + Z_{0^p}(x) \in [M]$. Легко проверить, что $G_1^p(\alpha) = \alpha(p - 1)$, $G_1^{p-1}(\alpha) = g_1(\alpha(p - 1))$, где $g_1(0) = 0$, $G_1^s(\alpha) = 0$ для любого $s \leq p - 2$. Если g_1 константа 0, то положим $G(x) = G_1(x)$, иначе положим $G(x) = G_1(x) + W_3(x) + Z_{0^p}(x)$. Таким образом $G^p(\alpha) = \alpha(p - 1)$, $G^s(\alpha) = 0$ для любого $s < p$.

Вспомним описание автомата \tilde{R} и функции \tilde{l}

$$\tilde{l}(a_1, a_2, \dots, a_p, b_1, b_2, \dots, b_p) = a_p + l_3(a_1, a_2, \dots, a_{p-1}, b_1, b_2, \dots, b_{p-1}).$$

По предположению индукции существует автомат $T_2 \in [M]$, такой что

$$T_2^{p-1}(a_1 a_2 \dots a_{p-1}) = l_3(a_1, a_2, \dots, a_{p-1}, a_1, a_2, \dots, a_{p-1}).$$

Пусть $W_4(x) = G(T_2(x)) + \tilde{R}(x, x) + Z_{0^p}(x) \in [M]$. Легко проверить, что $W_4^p(\alpha) = \alpha(p)$, $W_4^s(\alpha) = 0$ для любого $s < p$.

Вспомним определение автомата R , $R \notin \tilde{L}_p$. Для каких-то $\gamma_1, \gamma_2 \in E_2^{p-1}$ выполняется $R^{p, (\gamma_1, \gamma_2)} \notin L_1$. Положим

$$R_3(x_1, x_2) = R(Z_{\gamma_1 0}(x_1) + W_4(x_1) + Z_{0^p}(x_1), Z_{\gamma_2 0}(x_1) + W_4(x_2) + Z_{0^p}(x_1)).$$

Получаем, что выход автомата R_3 не зависит от того, что подается на вход в любой момент времени s , где $s < p$. При этом $R_3^p(\alpha_1, \alpha_2) = R^{p, (\gamma_1, \gamma_2)}(\alpha_1(p), \alpha_2(p))$. Известно [2], что $\{x_1 + x_2 + x_3, 0, 1, R^{p, (\gamma_1, \gamma_2)}\}$ — полная система в P_2 . Поэтому существует автомат $T_{x_1 \& x_2} \in [M]$, такой что $T_{x_1 \& x_2}^p(\beta_1 a_1, \beta_2 a_2) = a_1 \& a_2$ для любых $\beta_1, \beta_2 \in E_2^{p-1}$, $a_1, a_2 \in E_2$. По предположению индукции найдётся автомат $T \in [M]$, который $(p-1)$ -равен автомату $x_1 \& x_2$. Пусть

$$R_4(x_1, x_2) = W_4(T_{x_1 \& x_2}(x_1, x_2)) + T(x_1, x_2) + W_4(T(x_1, x_2)) \in [M].$$

Легко проверить, что R_4 p -равен автомату $x_1 \& x_2$.

Рассмотрим произвольный автомат $G_3 \in [M]$, который $(p-1)$ -равен единичной задержке с начальным состоянием 1. Пусть $G_4(x_1) = G(x) + G_3(x) + W_4(G_3(x)) \in [M]$. Легко проверить, что G_4 p -равен единичной задержке с начальным состоянием 1. Но задержка, $x_1 + x_2 + x_3$, $x_1 \& x_2$, 0 и 1 составляют полную систему в \mathcal{P}_a . Значит

$$[M]_p \supseteq [\{G_4, x_1 + x_2 + x_3, R_4, Z_{0^p}, Z_{1^p}\}]_p = \mathcal{P}_a.$$

Шаг индукции доказан и утверждение установлено.

Доказательство утверждения 3. Необходимость следует из утверждения 1. Докажем достаточность.

Из леммы 11 следует, что для любых $p \in \mathbb{N}$ и $\alpha \in E_2^p$ существует автомат с одним входом $Z_\alpha \in [M]$, такой что $Z_\alpha(\beta) = \alpha$ для любого $\beta \in E_2^p$.

Индукцией по p будем доказывать, что $[M]_p = \mathcal{P}_a$. Для $p = 1$ это следует из леммы 9. Докажем шаг индукции. Пусть $p \geq 2$. Обозначим через $H \in [M]$ автомат h_2 , если $k = 2$, и автомат, равный $h_k(x_1, x_2, x_3, Z_{1^p}(x_1), \dots, Z_{1^p}(x_1))$, если $k > 2$. Легко проверить, что H и h_2 p -равны. Так как $M \not\subseteq \tilde{A}_p$, то существует автомат T и $\alpha_1, \alpha_2, \dots, \alpha_n \in E_2^{p-1}$, такие что $T^{p, (\alpha_1, \alpha_2, \dots, \alpha_n)} \notin A_1$. Тогда для каких-то $b_1, b_2, \dots, b_n, c_1, c_2, \dots, c_n \in E_2$, таких что $b_j \leq c_j$ для любого j , выполняется

$$T^{p, (\alpha_1, \alpha_2, \dots, \alpha_n)}(b_1, b_2, \dots, b_n) > T^{p, (\alpha_1, \alpha_2, \dots, \alpha_n)}(c_1, c_2, \dots, c_n).$$

Для каждого $\alpha \in E_2^{p-1}$ определим $W_\alpha(x) = H(Z_{\alpha_0}(x), Z_{\alpha_1}(x), x)$. Для каждого i от 1 до n обозначим через T_i автомат $Z_{\alpha_i b_i}(x)$,

если $b_i = c_i$; автомат $W_{\alpha_i}(x)$, если $b_i < c_i$. Пусть $R(x) = T(T_1(x), T_2(x), \dots, T_n(x)) \in [M]$. Нетрудно убедиться, что для любых $b \in E_2$ и $\alpha \in E_2^{p-1}$ выполняется $R(\alpha b) = \beta \bar{b}$, где $\beta = T(\alpha_1, \alpha_2, \dots, \alpha_n)$.

По предположению индукции существует автомат $R_0 \in [M]$, который $(p-1)$ -равен автомату \bar{x} . Легко проверить, что автомат

$$R_1(x) = H(R_0(x), Z_{1^{p-1}0}(x), Z_{0^p}(x))$$

$(p-1)$ -равен автомату \bar{x} , а в момент времени p возвращает 0. Тогда автомат

$$R_2(x) = H(R_1(x), R(x), Z_{\bar{\beta}_1}(x)) \in [M]$$

p -равен автомату \bar{x} .

Так как $M \not\subseteq \tilde{S}_p$, то существует автомат T и слова $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n \in E_2^p$, такие что $]_{p-2}\alpha_i =]_{p-2}\beta_i$, $\alpha_i(p) = \beta_i(p)$ и

$$T^p(\alpha_1, \alpha_2, \dots, \alpha_n) < T^p(\beta_1, \beta_2, \dots, \beta_n).$$

Для каждого i от 1 до n обозначим через T_i автомат $H(Z_{\alpha_i}(x), Z_{\beta_i}(x), x)$, если $\alpha_i(p-1) \leq \beta_i(p-1)$; автомат $H(Z_{\alpha_i}(x), Z_{\beta_i}(x), R_2(x))$, если $\alpha_i(p-1) > \beta_i(p-1)$. Легко проверить, что $T_i(\delta) = \alpha_i$, если $\delta \in E_2^p$ и $\delta(p-1) = 0$; $T_i(\delta) = \beta_i$, если $\delta \in E_2^p$ и $\delta(p-1) = 1$. Пусть

$$G(x) = T(T_1(x), T_2(x), \dots, T_n(x)) \in [M].$$

Легко проверить, что $G^p(\gamma) = \gamma(p-1)$.

По предположению индукции существует автомат $G_0 \in [M]$, который $(p-1)$ -равен задержке с начальным состоянием 1. Легко проверить, что автомат

$$G_1(x) = H(G_0(x), T_{1^{p-1}0}(x), T_{0^p}(x))$$

$(p-1)$ -равен задержке, а в момент времени p возвращает 0. Автомат

$$G_2(x) = H(G_1(x), T_{0^{p-1}1}(x), T_{0^p}(x)) \in [M]$$

$(p-1)$ -равен константе 0, а в момент времени p работает как задержка. Нетрудно убедиться, что автомат $G_3(x) = H(G_1(x), G_2(x), Z_{1^p})$ p -равен задержке с начальным состоянием 1. Но отрицание и h_k составляют полную систему в P_2 , значит, отрицание, задержка и h_k составляют полную систему в \mathcal{P}_a . Тогда

$$[M]_p \supseteq [\{R_2, G_3, h_k\}]_p = \mathcal{P}_a.$$

Шаг индукции доказан и утверждение установлено.

Лемма 12. Пусть $M \subseteq \mathcal{P}_a^h$, $M \subseteq V \in \tilde{S}$, тогда существует $V' \in \tilde{S}^h$, такое что $M \subseteq V'$.

Доказательство. Пусть $V = \tilde{S}_p$. Если $p \leq h$, то $V' = V$ и лемма доказана. Пусть $p > h$. Рассмотрим автомат с n входами $T \in M$. Покажем, что $T \in \tilde{S}_h$. Пусть $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n \in E_2^h$, причём $]_{p-2}\alpha_i =]_{p-2}\beta_i$ и $\alpha_i(p) = \beta_i(p)$ для любого i . Для $i = 1, 2, \dots, n$ определим $\alpha'_i = 0^{p-h}\alpha_i$, $\beta'_i = 0^{p-h}\beta_i$. Так как $T \in \tilde{S}_p$, то

$$T^p(\alpha'_1, \alpha'_2, \dots, \alpha'_n) = T^p(\beta'_1, \beta'_2, \dots, \beta'_n).$$

Но T — автомат высоты h , значит

$$\begin{aligned} T^p(\alpha'_1, \alpha'_2, \dots, \alpha'_n) &= T^h(\alpha_1, \alpha_2, \dots, \alpha_n), \\ T^p(\beta'_1, \beta'_2, \dots, \beta'_n) &= T^h(\beta_1, \beta_2, \dots, \beta_n). \end{aligned}$$

Отсюда следует, что

$$T^h(\alpha_1, \alpha_2, \dots, \alpha_n) = T^h(\beta_1, \beta_2, \dots, \beta_n).$$

Значит $T \in \tilde{S}_h$. Тогда $M \subseteq \tilde{S}_h = V'$ и лемма доказана.

Лемма 13. Пусть $M \subseteq \mathcal{P}_a^h$, $M \subseteq V \in \tilde{D}$, тогда существует $V' \in \tilde{D}^h$, такое что $M \subseteq V'$.

Доказательство. Пусть $V = \tilde{D}_p$. Если $p \leq h$, то $V' = V$ и лемма доказана. Пусть $p > h$. Рассмотрим автомат с n входами $T \in M$. Покажем, что $T \in \tilde{D}_h$. Пусть $\alpha_1, \alpha_2, \dots, \alpha_n \in E_2^h$. Для $i = 1, 2, \dots, n$ определим $\beta_i = 0^{p-h}\alpha_i$. Так как $T \in \tilde{D}_p$, то выполняется

$$T^{p,(\beta_1, \beta_2, \dots, \beta_n)} \in D_3.$$

Но T — автомат высоты h , значит

$$T^{p,(\beta_1, \beta_2, \dots, \beta_n)} = T^{h,(\alpha_1, \alpha_2, \dots, \alpha_n)}.$$

Тогда $T^{h,(\alpha_1, \alpha_2, \dots, \alpha_n)} \in D_3$ и $T \in \tilde{D}_h$. Значит $M \subseteq \tilde{D}_h = V'$ и лемма доказана.

Следующие три леммы доказываются полностью аналогично.

Лемма 14. Пусть $M \subseteq \mathcal{P}_a^h$, $M \subseteq V \in \tilde{L}$, тогда существует $V' \in \tilde{L}^h$, такое что $M \subseteq V'$.

Лемма 15. Пусть $M \subseteq \mathcal{P}_a^h$, $M \subseteq V \in \tilde{A}$, тогда существует $V' \in \tilde{A}^h$, такое что $M \subseteq V'$.

Лемма 16. Пусть $M \subseteq \mathcal{P}_a^h$, $M \subseteq V \in \tilde{C}_d$, где $d \in E_2$, тогда существует $V' \in \tilde{C}_d^h$, такое что $M \subseteq V'$.

Лемма 17. Пусть $M \subseteq \mathcal{P}_a^h$, $M \subseteq V \in \tilde{K}$, тогда существует $V' \in \tilde{K}^{h+1}$, такое что $M \subseteq V'$.

Доказательство. Пусть $V = \tilde{K}_p$. Если $p \leq h+1$, то $V' = V$ и лемма доказана. Пусть $p > h+1$. Рассмотрим автомат с n входами $T \in M$. Покажем, что $T \in \tilde{K}_{h+1}$. Пусть $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n \in E_2^{h+1}$, причём для любого i выполняется $(\alpha_i, \beta_i) \in K_{h+1}$. Для $i = 1, 2, \dots, n$ определим $\alpha'_i = 0^{p-h-1}\alpha_i$, $\beta'_i = 0^{p-h-1}\beta_i$. Нетрудно убедиться, что для любого i выполняется $(\alpha'_i, \beta'_i) \in K_p$. По условию $T \in \tilde{K}_p$, значит пара $(T(\alpha'_1, \alpha'_2, \dots, \alpha'_n), T(\beta'_1, \beta'_2, \dots, \beta'_n))$ принадлежит K_p . Так как T — автомат высоты h , то

$$[{}_2T(\alpha'_1, \alpha'_2, \dots, \alpha'_n) = [{}_2T(\alpha_1, \alpha_2, \dots, \alpha_n)$$

и

$$[{}_2T(\beta'_1, \beta'_2, \dots, \beta'_n) = [{}_2T(\beta_1, \beta_2, \dots, \beta_n).$$

Отсюда следует, что пара $(T(\alpha_1, \alpha_2, \dots, \alpha_n), T(\beta_1, \beta_2, \dots, \beta_n))$ принадлежит K_{h+1} . Значит $T \in \tilde{K}_{h+1}$. Тогда $M \subseteq \tilde{K}_{h+1} = V'$ и лемма доказана.

Для $q \geq 2$, $B \subseteq \{1, 2, 3, \dots, q-1\}$, $d \in E_2$ определим

$$L_{B,d}^q = \{\alpha \in E_2^q \mid \alpha(q) + \sum_{i \in B} \alpha(i) = d\}.$$

Определим два подсемейства $\tilde{C}_L \subset \tilde{C}$, $\tilde{C}_L^h \subset \tilde{C}^h$:

$$\tilde{C}_L = \{U(L_{B,d}^q) \mid q \geq 2, B \subseteq \{1, 2, 3, \dots, q-1\}, d \in E_2\}$$

$$\tilde{C}_L^h = \{U(L_{B,d}^q) \mid 2 \leq q \leq h, B \subseteq \{1, 2, 3, \dots, q-1\}, d \in E_2\}$$

Лемма 18. Пусть $V \in \tilde{C}$, $x + y + z \in V$, тогда $V \in \tilde{C}_L$.

Доказательство. Пусть $V = U(C)$, где $C \subset E_2^q$, причём для любого $\alpha \in E_2^{q-1}$ существует $b \in E_2$, такое что $\alpha b \in C$. Тогда либо $0^q \in C$, либо $0^{q-1}1 \in C$. Если $0^q, 0^{q-1}1 \in C$, то для любых $\alpha \in E_2^{q-1}, b \in E_2$, таких что $\alpha b \in C$, выполняется $\alpha b + 0^q + 0^{q-1}1 = \alpha \bar{b} \in C$. Значит, $C = E_2^q$, что невозможно.

Пусть $0^{q-1}d \in C$. Определим множество $B \subseteq \{1, 2, 3, \dots, q-1\}$: $i \in B$ тогда и только тогда, когда $0^{i-1}10^{q-i-1}d \notin C$. Покажем, что $C = L_{B,d}^q$.

Пусть $\alpha \in L_{B,d}^q$. Докажем, что $\alpha \in C$. Будем доказывать индукцией по количеству единиц в слове $\lfloor_{q-1}\alpha$. Если их нет, то утверждение следует из того, что $0^{q-1}d \in C$. Докажем шаг индукции. Рассмотрим i , такое что $\alpha(i) = 1$. Если $i \in B$, то $\alpha + 0^{i-1}10^{q-i-1}1$ принадлежит $L_{B,d}^q$ и $\lfloor_{q-1}(\alpha + 0^{i-1}10^{q-i-1}1)$ содержит на одну единицу меньше. Тогда по предположению индукции $\alpha + 0^{i-1}10^{q-i-1}1 \in C$. Так как $x + y + z$ сохраняет C , то

$$(\alpha + 0^{i-1}10^{q-i-1}1) + (0^{i-1}10^{q-i-1}\bar{d}) + (0^{q-1}d) = \alpha \in C.$$

Если $i \notin B$, то $\alpha + 0^{i-1}10^{q-i}$ принадлежит $L_{B,d}^q$ и $\lfloor_{q-1}(\alpha + 0^{i-1}10^{q-i})$ содержит на одну единицу меньше. Тогда по предположению индукции $\alpha + 0^{i-1}10^{q-i} \in C$. Так как $x + y + z$ сохраняет C , то

$$(\alpha + 0^{i-1}10^{q-i}) + (0^{i-1}10^{q-i-1}d) + (0^{q-1}d) = \alpha \in C.$$

То есть мы доказали, что $L_{B,d}^q \subseteq C$.

Теперь докажем, что если $\alpha \in C$, то $\alpha \in L_{B,d}^q$. Предположим, что это не так и $\alpha \notin L_{B,d}^q$, тогда $\alpha + 0^{q-1}1 \in L_{B,d}^q$. Значит $\alpha + 0^{q-1}1 \in C$ и $(\alpha + 0^{q-1}1) + \alpha + 0^{q-1}d = 0^{q-1}\bar{d} \in C$. Получили противоречие. То есть $L_{B,d}^q = C$ и лемма доказана.

Лемма 19. Пусть $M \subseteq \mathcal{P}_a^h$, $M \subseteq V \in \tilde{C}_L$, тогда существует $V' \in \tilde{C}_L^{2^{2h+1}+4h}$, такое что $M \subseteq V'$.

Доказательство. Рассмотрим минимальное q_0 , такое что $M \subseteq U(L_{B_0,d}^{q_0})$. Если $q_0 \leq 2^{2h+1} + 4h$, то $V' = V$ и лемма доказана. Предположим, что это не так. Каждому i сопоставим число $r(i)$: $r(i) = 0$, если $i \notin B_0$; $r(i) = 1$, если $i \in B_0$.

Идея доказательства заключается в следующем. Рассмотрим слово

$$r(h)r(h+1)r(h+2)\dots r(q_0-h)$$

в алфавите $\{0, 1\}$. Если q_0 достаточно велико, то в этом слове найдутся два совпадающих подслова длины $2h$, таких что между началами этих подслов находится четное число единиц. Тогда мы можем «вырезать» часть между началами этих подслов и по получившемуся слову построить $L_{B',d}^{q'}$, такое что $M \subseteq U(L_{B',d}^{q'})$ и $q' < q_0$. Тем самым мы уменьшим q_0 . А мы предположили, что оно минимально.

Для каждого i от $3h$ до $q_0 - h$ рассмотрим набор

$$(r(i-2h+1), r(i-2h+2), \dots, r(i-2), r(i-1), r(i)).$$

Этот набор может принимать 2^{2h} различных значений. По предположению $q_0 > 2^{2h+1} + 4h$, поэтому найдутся числа l_1, l_2, l_3 , такие что $3h \leq l_1 < l_2 < l_3 \leq q_0 - h$ и $r(l_1 - j) = r(l_2 - j) = r(l_3 - j)$ для любого $j, 0 \leq j < 2h$.

Пусть n_1 — количество чисел j , таких что $l_1 < j \leq l_2$ и $j \in B_0$; аналогично n_2 — количество чисел j , таких что $l_2 < j \leq l_3$ и $j \in B_0$. Если n_1 четно, то положим $i_1 = l_1, i_2 = l_2$; если n_2 четно, то положим $i_1 = l_2, i_2 = l_3$; иначе положим $i_1 = l_1, i_2 = l_3$. Таким образом количество чисел j , таких что $i_1 < j \leq i_2$ и $j \in B_0$, чётно.

Пусть $q' = q_0 - (i_2 - i_1)$. Рассмотрим множество $B' \subseteq \{1, 2, 3, \dots, q' - 1\}$, такое что $j \in B'$ точно тогда, когда $j \leq i_1$ и $j \in B_0$, либо $j > i_1$ и $j + (i_2 - i_1) \in B_0$.

Покажем, что $M \subseteq U(L_{B',d}^{q'})$. Рассмотрим произвольный автомат с n входами $T \in M$ и произвольные $\alpha_1, \alpha_2, \dots, \alpha_n \in L_{B',d}^{q'}$. Будем доказывать индукцией по суммарному количеству единиц в словах $]_{q'-1}\alpha_1,]_{q'-1}\alpha_2, \dots,]_{q'-1}\alpha_n$, что $\beta = T(\alpha_1, \alpha_2, \dots, \alpha_n)$ принадлежит $L_{B',d}^{q'}$. Докажем базис индукции. Пусть

$$\beta_0 = T(0^{q'-1}d, 0^{q'-1}d, \dots, 0^{q'-1}d),$$

$$\gamma_0 = T(0^{q_0-1}d, 0^{q_0-1}d, \dots, 0^{q_0-1}d),$$

$$T^h(0^h, 0^h, \dots, 0^h) = b.$$

Нетрудно проверить, что $\gamma_0 = (]_{i_1} \beta_0) b^{i_2 - i_1} ([_{q' - i_1} \beta_0)$. Так как $0^{q_0 - 1} d \in L_{B_0, d}^{q_0}$, то $\gamma_0 \in L_{B_0, d}^{q_0}$. Значит $\gamma_0(q_0) + \sum_{i \in B_0} \gamma_0(i) = d$. Но $\gamma_0(q_0) = \beta_0(q')$ и

$$\begin{aligned} \sum_{i \in B_0} \gamma_0(i) &= \left(\sum_{i \in B_0, i \leq i_1} \gamma_0(i) + \sum_{i \in B_0, i > i_2} \gamma_0(i) \right) + \sum_{i \in B_0, i_1 < i \leq i_2} \gamma_0(i) = \\ &= \sum_{i \in B'} \beta_0(i) + \sum_{i \in B_0, i_1 < i \leq i_2} \gamma_0(i), \end{aligned}$$

причем i_1 и i_2 были выбраны так, чтобы $\sum_{i \in B_0, i_1 < i \leq i_2} \gamma_0(i) = 0$. Отсюда следует, что $\beta_0(q') + \sum_{i \in B'} \beta_0(i) = d$ и $\beta_0 \in L_{B', d}^{q'}$.

Теперь докажем шаг индукции. Пусть для каких-то j_0 и i_0 , $i_0 < q'$, выполняется $\alpha_{j_0}(i_0) = 1$. Положим $\alpha' = \alpha_{j_0} + 0^{i_0 - 1} 10^{q' - i_0 - 1} 1$, если $i_0 \in B'$; и $\alpha' = \alpha_{j_0} + 0^{i_0 - 1} 10^{q' - i_0}$, если $i_0 \notin B'$. Легко проверить, что $\alpha' \in L_{B', d}^{q'}$. По предположению индукции

$$\beta' = T(\alpha_1, \alpha_2, \dots, \alpha_{i_0 - 1}, \alpha', \alpha_{j_0 + 1}, \dots, \alpha_n) \in L_{B', d}^{q'}.$$

Пусть $i_0 \leq i_1 - h$. Для $i = 1, 2, \dots, n$ определим $\gamma_i = (]_{i_1} \alpha_i) 0^{i_2 - i_1} ([_{q' - i_1} \alpha_i)$, $\gamma' = (]_{i_1} \alpha') 0^{i_2 - i_1} ([_{q' - i_1} \alpha')$. Легко проверить, что $\gamma', \gamma_1, \gamma_2, \dots, \gamma_n \in L_{B_0, d}^{q_0}$. Пусть

$$\begin{aligned} \delta &= T(\gamma_1, \gamma_2, \dots, \gamma_{j_0 - 1}, \gamma_{j_0}, \gamma_{j_0 + 1}, \dots, \gamma_n) \in L_{B_0, d}^{q_0}, \\ \delta' &= T(\gamma_1, \gamma_2, \dots, \gamma_{j_0 - 1}, \gamma', \gamma_{j_0 + 1}, \dots, \gamma_n) \in L_{B_0, d}^{q_0}. \end{aligned}$$

Нетрудно проверить, что $]_{i_1} \delta =]_{i_1} \beta$, $\delta(q_0) = \beta(q')$, $]_{i_1} \delta' =]_{i_1} \beta'$, $\delta'(q_0) = \beta'(q')$. Пусть

$$\delta_0 = \delta + \delta' + 0^{q_0 - 1} d, \beta_0 = \beta + \beta' + 0^{q' - 1} d,$$

тогда $]_{i_1} \delta_0 =]_{i_1} \beta_0$, $\delta_0(q_0) = \beta_0(q')$. Так как $x + y + z \in U(L_{B_0, d}^{q_0})$, то $\delta_0 \in L_{B_0, d}^{q_0}$. Легко проверить, что если $i_0 + h \leq j < q_0$, то $\delta_0(j) = 0$. Аналогично, если $i_0 + h \leq j < q'$, то $\beta_0(j) = 0$. Так как $i_0 + h \leq i_1$, то

$\delta_0 = (\lfloor_{i_1} \beta_0) 0^{i_2-i_1} (\lfloor_{q'-i_1} \beta_0)$. Значит $\beta_0 \in L_{B',d}^{q'}$. Но $\beta = \beta_0 + \beta' + 0^{q'-1}d$, поэтому $\beta \in L_{B',d}^{q'}$.

Пусть $i_0 > i_1 - h$. Для $i = 1, 2, \dots, n$ определим $\gamma_i = (\lfloor_{i_1-2h} \alpha_i) 0^{i_2-i_1} (\lfloor_{q'-i_1+2h} \alpha_i)$, $\gamma' = (\lfloor_{i_1-2h} \alpha') 0^{i_2-i_1} (\lfloor_{q'-i_1+2h} \alpha')$. Легко проверить, что $\gamma', \gamma_1, \gamma_2, \dots, \gamma_n \in L_{B_0,d}^{q_0}$. Пусть

$$\delta = T(\gamma_1, \gamma_2, \dots, \gamma_{j_0-1}, \gamma_{j_0}, \gamma_{j_0+1}, \dots, \gamma_n) \in L_{B_0,d}^{q_0},$$

$$\delta' = T(\gamma_1, \gamma_2, \dots, \gamma_{j_0-1}, \gamma', \gamma_{j_0+1}, \dots, \gamma_n) \in L_{B_0,d}^{q_0}.$$

Нетрудно проверить, что $\lfloor_{q_0-i_2+h} \delta = \lfloor_{q'-i_1+h} \beta$, $\lfloor_{q_0-i_2+h} \delta' = \lfloor_{q'-i_1+h} \beta'$. Пусть

$$\delta_0 = \delta + \delta' + 0^{q_0-1}d, \beta_0 = \beta + \beta' + 0^{q'-1}d,$$

тогда $\lfloor_{q_0-i_2+h} \delta_0 = \lfloor_{q'-i_1+h} \beta_0$. Так как $x+y+z \in U(L_{B_0,d}^{q_0})$, то $\delta_0 \in L_{B_0,d}^{q_0}$. Легко проверить, что если $j < i_0 + (i_2 - i_1)$, то $\delta_0(j) = 0$. При этом $i_2 - h = (i_1 - h) + (i_2 - i_1) < i_0 + (i_2 - i_1)$, значит $\lfloor_{i_2-h} \delta_0 = 0^{i_2-h}$. Аналогично, если $j < i_0$, то $\beta_0(j) = 0$ и $\lfloor_{i_1-h} \beta_0 = 0^{i_1-h}$. Отсюда следует, что $\delta_0 = (\lfloor_{i_1-h} \beta_0) 0^{i_2-i_1} (\lfloor_{q'-i_1+h} \beta_0)$. Так как $\delta_0 \in L_{B_0,d}^{q_0}$, то $\beta_0 \in L_{B',d}^{q'}$. Но $\beta = \beta_0 + \beta' + 0^{q'-1}d$, поэтому $\beta \in L_{B',d}^{q'}$.

Шаг индукции доказан. Значит произвольный автомат $T \in M$ принадлежит $U(L_{B',d}^{q'})$, где $q' < q_0$. А мы предполагали, что q_0 — минимальное такое число. Получили противоречие. Лемма доказана.

Доказательство утверждения 4. Необходимость следует из утверждения 1. Докажем достаточность. Предположим, что M — не A -полно. Покажем, что для какого-то $V \in \widetilde{W}_1^h$ выполняется $M \subseteq V$. Из утверждения 2 следует, что для какого-то $V' \in \widetilde{W}$ выполняется $M \subseteq V'$.

Легко убедиться, что для любого $\widetilde{A}_p \in \widetilde{A}$ выполняется $x + y + z \notin \widetilde{A}_p$. Значит $V' \notin \widetilde{A}$. То есть, мы получили, что $V' \in \widetilde{C} \cup \widetilde{S} \cup \widetilde{D} \cup \widetilde{L} \cup \widetilde{K}$. Тогда из леммы 18 следует, что

$$V' \in \widetilde{C}_L \cup \widetilde{S} \cup \widetilde{D} \cup \widetilde{L} \cup \widetilde{K}.$$

Из лемм 19, 12, 13, 14 и 17 следует, что существует

$$V \in \widetilde{C}_L^{2^{2h+1}+4h} \cup \widetilde{S}^h \cup \widetilde{D}^h \cup \widetilde{L}^h \cup \widetilde{K}^{h+1} \subseteq \widetilde{W}_1^h,$$

такое что $M \subseteq V$. Утверждение доказано.

Для $1 \leq p < q$ определим

$$M_{p,q}^= = \{\alpha \in E_2^q \mid \alpha(p) = \alpha(q)\},$$

$$M_{p,q}^{\neq} = \{\alpha \in E_2^q \mid \alpha(p) \neq \alpha(q)\}.$$

Пусть $q \geq 2$, $B, D \subseteq \{1, 2, 3, \dots, q-1\}$, $B \cap D = \emptyset$, тогда

$$M_{B,D}^{q,1} = \{\alpha \in E_2^q \mid \forall i \in B \quad (\alpha(i) \leq \alpha(q)), \forall i \in D \quad (\alpha(i) \vee \alpha(q) = 1)\},$$

$$M_{B,D}^{q,0} = \{\alpha \in E_2^q \mid \forall i \in B \quad (\alpha(i) \geq \alpha(q)), \forall i \in D \quad (\alpha(i) \& \alpha(q) = 0)\}.$$

Пусть $M_q = (\bigcup_{1 \leq p < q} \{M_{p,q}^=, M_{p,q}^{\neq}\}) \cup (\bigcup_{B \cup D \neq \emptyset} \{M_{B,D}^{q,0}, M_{B,D}^{q,1}\})$. Определим два подсемейства $\tilde{C}_M \subset \tilde{C}$, $\tilde{C}_M^h \subset \tilde{C}^h$:

$$\tilde{C}_M = \{U(C) \mid C \in M_q, q \geq 2\},$$

$$\tilde{C}_M^h = \{U(C) \mid C \in M_q, 2 \leq q \leq h\}.$$

Лемма 20. Пусть $V \in \tilde{C}$, $h_2 \in V$, тогда $V \in \tilde{C}_M \cup \tilde{C}_0 \cup \tilde{C}_1$.

Доказательство. Пусть $V = U(C)$, где $C \subset E_2^q$, причём для любого $\alpha \in E_2^{q-1}$ существует $b \in E_2$, такое что $\alpha b \in C$. Если $q = 1$, то очевидно $V \in \tilde{C}_0 \cup \tilde{C}_1$.

Далее будем считать, что $q \geq 2$. Пусть существует $i \in \{1, 2, \dots, q-1\}$, такое что для любого $\gamma \in C$ выполняется $\gamma(i) = \gamma(q)$. Легко проверить, что в этом случае $C = M_{i,q}^=$ и $V = U(M_{i,q}^=) \in \tilde{C}_M$. Аналогично, пусть существует $i \in \{1, 2, \dots, q-1\}$, такое что для любого $\gamma \in C$ выполняется $\gamma(i) \neq \gamma(q)$. В этом случае легко показать, что $C = M_{i,q}^{\neq}$ и $V = U(M_{i,q}^{\neq}) \in \tilde{C}_M$. Далее будем полагать, что для любого $i \in \{1, 2, \dots, q-1\}$ существуют $\alpha_1, \alpha_2 \in C$, такие что $\alpha_1(i) = \alpha_1(q)$ и $\alpha_2(i) \neq \alpha_2(q)$.

Пусть B_1 — множество всех $i \in \{1, 2, \dots, q-1\}$, таких что для любого $\alpha \in C$ выполняется $\alpha(i) \leq \alpha(q)$; B_0 — множество всех $i \in \{1, 2, \dots, q-1\}$, таких что для любого $\alpha \in C$ выполняется $\alpha(i) \geq \alpha(q)$; D_1 — множество всех $i \in \{1, 2, \dots, q-1\}$, таких что для любого $\alpha \in C$ выполняется $\alpha(i) \vee \alpha(q) = 1$; D_0 — множество всех $i \in \{1, 2, \dots, q-1\}$, таких что для любого $\alpha \in C$ выполняется $\alpha(i) \& \alpha(q) = 0$.

Если $B_1 \cap D_1 \neq \emptyset$, то для $i \in B_1 \cap D_1$ и любого $\alpha \in C$ выполняется $\alpha(i) \leq \alpha(q)$ и $\alpha(i) \vee \alpha(q) = 1$. Значит $\alpha(q) = 1$. Тогда $C = C_{1,q}$ и $V = U(C_{1,q}) \in \tilde{C}_1$. Аналогично, если $B_0 \cap D_0 \neq \emptyset$, то $C = C_{0,q}$ и $V = U(C_{0,q}) \in \tilde{C}_0$. Далее будем полагать, что $B_1 \cap D_1 = B_0 \cap D_0 = \emptyset$.

Предположим, что $B_1 \cup D_1 \neq \emptyset$ и $B_0 \cup D_0 \neq \emptyset$. Пусть существуют $i_1 \in B_1$, $i_0 \in B_0$, тогда $\alpha(i_1) \leq \alpha(q) \leq \alpha(i_0)$. Если $i_1 = i_0$, то для любого $\alpha \in C$ выполняется $\alpha(i_1) = \alpha(q)$, а этот случай уже разобран. Если $i_1 \neq i_0$, то для любого $\alpha \in C$ выполняется $\alpha(i_1) \leq \alpha(i_0)$. А это противоречит тому, что для любого $\alpha \in E_2^{p-1}$ существует $b \in E_2$, такое что $\alpha b \in C$.

Разберем остальные случаи. Пусть существуют $i_1 \in B_1$, $i_0 \in D_0$, тогда для любого $\alpha \in C$ выполняется $\alpha(i_0) \& \alpha(i_1) \leq \alpha(i_0) \& \alpha(q) = 0$. А это противоречит тому, что для любого $\alpha \in E_2^{p-1}$ существует $b \in E_2$, такое что $\alpha b \in C$.

Пусть существуют $i_1 \in D_1$, $i_0 \in B_0$, тогда для любого $\alpha \in C$ выполняется $\alpha(i_1) \vee \alpha(i_0) \geq \alpha(i_1) \vee \alpha(q) = 1$. А это противоречит тому, что для любого $\alpha \in E_2^{p-1}$ существует $b \in E_2$, такое что $\alpha b \in C$.

Пусть существуют $i_1 \in D_1$, $i_0 \in D_0$, тогда $\alpha(i_1) \vee \alpha(q) = 1$ и $\alpha(i_0) \& \alpha(q) = 0$. Если $i_1 = i_0$, то для любого $\alpha \in C$ выполняется $\alpha(i_1) \neq \alpha(q)$, а этот случай уже разобран. Если $i_1 \neq i_0$, то для любого $\alpha \in C$ выполняется $\alpha(i_1) \geq \alpha(i_0)$. А это противоречит тому, что для любого $\alpha \in E_2^{p-1}$ существует $b \in E_2$, такое что $\alpha b \in C$.

Значит, либо $B_0 \cup D_0 = \emptyset$, либо $B_1 \cup D_1 = \emptyset$. Рассмотрим первый случай. Покажем, что $C = M_{B_1, D_1}^{q,1}$. Легко проверить, что $C \subseteq M_{B_1, D_1}^{q,1}$. Для произвольного $\alpha \in M_{B_1, D_1}^{q,1}$ покажем, что $\alpha \in C$. По индукции будем доказывать, что для любого $Q \subseteq \{1, 2, \dots, q-1\}$ существует $\beta \in C$, такое что $\alpha(j) = \beta(j)$ для любого $j \in Q$ и $\beta(q) = \alpha(q)$.

Докажем базис индукции. Пусть $Q = \{j\}$, $j \in B_1$. Тогда для любого $\gamma \in C$ выполняется $\gamma(j) \leq \gamma(q)$. Предположим, что не существует $\beta \in C$, такого что $\beta(j) = \alpha(j)$ и $\beta(q) = \alpha(q)$. Тогда либо для любого $\gamma \in C$ выполняется $\gamma(q) = 1$, либо для любого $\gamma \in C$ выполняется $\gamma(j) = \gamma(q)$, либо для любого $\gamma \in C$ выполняется $\gamma(j) = 0$. В первом случае $V \in \tilde{C}_1$, второй случай уже разобран, а третий случай невозможен. Значит искомое β существует.

Пусть $Q = \{j\}$, $j \in D_1$. Тогда для любого $\gamma \in C$ выполняется $\gamma(j) \vee \gamma(q) = 1$. Предположим, что не существует $\beta \in C$, такого что

$\beta(j) = \alpha(j)$ и $\beta(q) = \alpha(q)$. Тогда либо для любого $\gamma \in C$ выполняется $\gamma(j) = 1$, либо для любого $\gamma \in C$ выполняется $\gamma(q) = 1$, либо для любого $\gamma \in C$ выполняется $\gamma(j) \neq \gamma(q)$. Первый случай невозможен, во втором случае $V \in \tilde{C}_1$, а третий случай уже разобран. Значит искомое β существует.

Пусть $Q = \{j\}$, $j \notin B_1 \cup D_1$. Предположим, что не существует $\beta \in C$, такого что $\beta(j) = \alpha(j)$ и $\beta(q) = \alpha(q)$. Тогда $j \in B_0 \cup D_0 \cup B_1 \cup D_1$. Но мы рассматриваем случай, когда $B_0 \cup D_0 = \emptyset$ и $j \notin B_1 \cup D_1$. Значит искомое β существует.

Теперь докажем шаг индукции. Пусть $|Q| \geq 2$. Очевидно найдутся различные подмножества Q_1, Q_2 множества Q , такие что $|Q_1| = |Q_2| = |Q| - 1$. По предположению индукции найдутся $\beta_1, \beta_2 \in C$, такие что $\beta_k(j) = \alpha(j)$ для любого $j \in Q_k$, $k = 1, 2$, а также $\beta_1(q) = \beta_2(q) = \alpha(q)$. По определению семейства \tilde{C} для какого-то $\delta \in C$ выполняется $]_{q-1}\alpha =]_{q-1}\delta$. Тогда возьмём $\beta = h_2(\beta_1, \beta_2, \delta) \in C$, причём $\beta(j) = \alpha(j)$ для любого $j \in Q$ и $\beta(q) = \alpha(q)$.

Таким образом, мы доказали, что для любого $Q \subseteq \{1, 2, \dots, q-1\}$, существует $\beta \in C$, такое что $\alpha(j) = \beta(j)$ для любого $j \in Q$ и $\beta(q) = \alpha(q)$. В частности это верно для $Q = \{1, 2, \dots, q-1\}$, значит $\alpha \in C$ и $C = M_{B_1, D_1}^{q, 1}$. Так как $C \neq E_2^q$, то $B_1 \cup D_1 \neq \emptyset$.

Полностью аналогично рассматривается случай $B_1 \cup D_1 = \emptyset$. Лемма доказана.

Лемма 21. Пусть $M \subseteq \mathcal{P}_a^h$, $M \subseteq V \in \tilde{C}_M$, тогда существует $V' \in \tilde{C}_M^{3h+3h}$, такое что $M \subseteq V'$.

Доказательство. Пусть $V = U(M_{p,q}^-)$. Рассмотрим минимальное q_0 , такое что $M \subseteq U(M_{p_0, q_0}^-)$.

Пусть $p_0 > h$. Рассмотрим автомат с n входами $T \in M$. Покажем, что $T \in U(M_{h, q_0 - p_0 + h}^-)$. Пусть $\alpha_1, \alpha_2, \dots, \alpha_n \in M_{h, q_0 - p_0 + h}^-$. Для $i = 1, 2, \dots, n$ определим $\alpha'_i = 0^{p_0 - h} \alpha_i$. Легко проверить, что $\alpha'_1, \alpha'_2, \dots, \alpha'_n \in M_{p_0, q_0}^-$. Так как $M \subseteq U(M_{p_0, q_0}^-)$, то $T(\alpha'_1, \alpha'_2, \dots, \alpha'_n) \in M_{p_0, q_0}^-$. По условию T — автомат высоты h , значит

$$\begin{aligned} T^{p_0}(\text{]}_{p_0}\alpha'_1, \text{]}_{p_0}\alpha'_2, \dots, \text{]}_{p_0}\alpha'_n) &= T^h(\text{]}_h\alpha_1, \text{]}_h\alpha_2, \dots, \text{]}_h\alpha_n), \\ T^{q_0}(\alpha'_1, \alpha'_2, \dots, \alpha'_n) &= T^{q_0 - p_0 + h}(\alpha_1, \alpha_2, \dots, \alpha_n). \end{aligned}$$

Тогда $T(\alpha_1, \alpha_2, \dots, \alpha_n) \in M_{h, q_0 - p_0 + h}^-$ и $M \subseteq U(M_{h, q_0 - p_0 + h}^-)$. Но мы предполагали, что q_0 — минимальное. Получили противоречие.

Пусть $q_0 - p_0 > h$. Рассмотрим автомат с n входами $T \in M$. Покажем, что $T \in U(M_{p_0, p_0 + h}^-)$. Рассмотрим слова $\alpha_1, \alpha_2, \dots, \alpha_n \in M_{p_0, p_0 + h}^-$. Для $i = 1, 2, \dots, n$ определим $\alpha'_i = (]_{p_0} \alpha_i) 0^{q_0 - p_0 - h} (]_h \alpha_i)$. Легко проверить, что $\alpha'_1, \alpha'_2, \dots, \alpha'_n \in M_{p_0, q_0}^-$. Так как $M \subseteq U(M_{p_0, q_0}^-)$, то $T(\alpha'_1, \alpha'_2, \dots, \alpha'_n) \in M_{p_0, q_0}^-$. По условию T — автомат высоты h , значит

$$\begin{aligned} T^{p_0} (]_{p_0} \alpha'_1,]_{p_0} \alpha'_2, \dots,]_{p_0} \alpha'_n) &= T^{p_0} (]_{p_0} \alpha_1,]_{p_0} \alpha_2, \dots,]_{p_0} \alpha_n), \\ T^{q_0} (\alpha'_1, \alpha'_2, \dots, \alpha'_n) &= T^{p_0 + h} (\alpha_1, \alpha_2, \dots, \alpha_n). \end{aligned}$$

Тогда $T(\alpha_1, \alpha_2, \dots, \alpha_n) \in M_{p_0, p_0 + h}^-$ и $M \subseteq U(M_{p_0, p_0 + h}^-)$. Но мы предполагали, что q_0 — минимальное. Получили противоречие. Значит $q_0 = p_0 + (q_0 - p_0) \leq 2h < 3^h + 3h$ и $M \subseteq U(M_{p_0, q_0}^-) \in \tilde{C}_M^{3^h + 3h}$. Полностью аналогично рассматривается случай, когда $V = U(M_{p, q}^\neq)$.

Теперь пусть $V = U(M_{B, D}^{q, 1})$, где $q \geq 2$, $B, D \subseteq \{1, 2, 3, \dots, q - 1\}$, $B \cap D = \emptyset$, $B \cup D \neq \emptyset$. Рассмотрим минимальное q_0 , такое что для каких-то B_0 и D_0 выполняется $M \subseteq U(M_{B_0, D_0}^{q_0, 1})$, причём $B_0 \cup D_0 \neq \emptyset$. Если $q_0 \leq 3^h + 3h$, то лемма доказана. Предположим, что это не так.

Каждому i от h до $q_0 - h$ сопоставим число $r(i) : r(i) = 1$, если $i \in B_0$; $r(i) = 2$, если $i \in D_0$; $r(i) = 3$ иначе.

Идея доказательства заключается в следующем. Рассмотрим слово

$$r(h)r(h+1)r(h+2)\dots r(q_0-h)$$

в алфавите $\{1, 2, 3\}$. Если q_0 достаточно велико, то в этом слове найдутся два совпадающих подслова длины h . Тогда мы можем «вырезать» часть между началами двух подслов и по получившемуся слову построить множество $M_{B', D'}^{q', 1}$, такое что $M \subseteq U(M_{B', D'}^{q', 1})$, $B' \cup D' \neq \emptyset$ и $q' < q_0$. Тем самым мы уменьшим q_0 . А мы предположили, что оно минимально.

Для каждого i от $2h$ до $q_0 - h$ рассмотрим набор

$$(r(i-h+1), r(i-h+2), \dots, r(i-2), r(i-1), r(i)).$$

Этот набор может принимать 3^h различных значений. Так как по предположению $q_0 > 3^h + 3h$, то найдутся числа i_1 и i_2 , такие что $i_1 < i_2$ и $r(i_1 - j) = r(i_2 - j)$ для любого j , $0 \leq j < h$.

Пусть $q' = q_0 - (i_2 - i_1)$. Рассмотрим множество $B' \subseteq \{1, 2, 3, \dots, q' - 1\}$, такое что $j \in B'$ точно тогда, когда $j \leq i_1$ и $j \in B_0$, либо $j > i_1$ и $j + (i_2 - i_1) \in B_0$. Также рассмотрим множество $D' \subseteq \{1, 2, \dots, q' - 1\}$, такое что $j \in D'$ точно тогда, когда $j \leq i_1$ и $j \in D_0$, либо $j > i_1$ и $j + (i_2 - i_1) \in D_0$.

Предположим, что $B' \cup D' = \emptyset$. Тогда определим множества $B'_0, D'_0 \subseteq \{1, 2, \dots, q_0 - h - 1\}$. Пусть $j \in B'_0$ точно тогда, когда $j + h \in B_0$. Аналогично $j \in D'_0$ точно тогда, когда $j + h \in D_0$. Покажем, что $M \subseteq U(M_{B'_0, D'_0}^{q_0-h, 1})$. Рассмотрим произвольный автомат с n входами $T \in M$ и произвольные $\alpha_1, \alpha_2, \dots, \alpha_n \in M_{B'_0, D'_0}^{q_0-h, 1}$. Легко проверить, что для любого i выполняется $0^h \alpha_i \in M_{B_0, D_0}^{q_0, 1}$. Значит

$$T(0^h \alpha_1, 0^h \alpha_2, 0^h \dots, 0^h \alpha_n) = \beta \in M_{B_0, D_0}^{q_0, 1}.$$

Пусть $\gamma = T(\alpha_1, \alpha_2, \dots, \alpha_n)$. Легко проверить, что $[\downarrow_{q_0-2h}(\beta) = \downarrow_{q_0-2h}(\gamma)]$. Учитывая, что в B'_0 и D'_0 нет j , такого что $j \leq h$, получаем, что $\gamma \in M_{B'_0, D'_0}^{q_0-h, 1}$. Значит $M \subseteq U(M_{B'_0, D'_0}^{q_0-h, 1})$, причём $B'_0 \cup D'_0 \neq \emptyset$. Но мы предполагали, что q_0 — минимальное такое число. Получили противоречие.

Теперь рассмотрим случай, когда $B' \cup D' \neq \emptyset$. Покажем, что $M \subseteq U(M_{B', D'}^{q', 1})$. Рассмотрим произвольный автомат с n входами $T \in M$ и произвольные $\alpha_1, \alpha_2, \dots, \alpha_n \in M_{B', D'}^{q', 1}$. Докажем, что для $\beta = T(\alpha_1, \alpha_2, \dots, \alpha_n)$ выполняется $\beta \in M_{B', D'}^{q', 1}$.

Для $i = 1, 2, \dots, n$ определим $\gamma_i = (\downarrow_{i_1} \alpha_i) \xi_1(\downarrow_{q'-i_1} \alpha_i)$, где $|\xi_1| = i_2 - i_1$, $\xi_1(j) = 0$ точно тогда, когда $j + i_1 \in B_0$. Покажем, что $\gamma_1, \gamma_2, \dots, \gamma_n \in M_{B_0, D_0}^{q_0, 1}$.

Если $j \in B_0$, $j \leq i_1$, то $j \in B'$, значит $\gamma_i(j) = \alpha_i(j) \leq \alpha_i(q') = \alpha_i(q_0)$. Если $j \in B_0$, $j > i_2$, то $j - (i_2 - i_1) \in B'$, значит $\gamma_i(j) = \alpha_i(j - (i_2 - i_1)) \leq \alpha_i(q') = \alpha_i(q_0)$. Если $j \in B_0$, $i_1 < j \leq i_2$, то $\gamma_i(j) = 0$. Аналогично доказывается, если $j \in D_0$.

Таким образом, мы доказали, что $\gamma_1, \gamma_2, \dots, \gamma_n \in M_{B_0, D_0}^{q_0, 1}$. Тогда $T(\gamma_1, \gamma_2, \dots, \gamma_n) = \delta_1 \in M_{B_0, D_0}^{q_0, 1}$. Легко проверить, что $[\downarrow_{i_1} \beta = \downarrow_{i_1} \delta_1]$ и $\beta(q') = \delta_1(q_0)$.

Аналогично для $i = 1, 2, \dots, n$ определим $\eta_i = \xi_2[\downarrow_{q'-i_1+h} \alpha_i]$, где $|\xi_2| = i_2 - h$, $\xi_2(j) = 0$ точно тогда, когда $j \in B_0$. Покажем, что $\eta_1, \eta_2, \dots, \eta_n \in M_{B_0, D_0}^{q_0, 1}$.

Если $j \in B_0, j \leq i_2 - h$, то $\eta_i(j) = 0$. Если $j \in B_0, j > i_2 - h$, то $j - (i_2 - i_1) \in B'$, значит $\eta_i(j) = \alpha_i(j - (i_2 - i_1)) \leq \alpha_i(q') = \eta_i(q_0)$. Аналогично доказывается, если $j \in D_0$.

Таким образом $\eta_1, \eta_2, \dots, \eta_n \in M_{B_0, D_0}^{q_0, 1}$. Тогда $T(\eta_1, \eta_2, \dots, \eta_n) = \delta_2 \in M_{B_0, D_0}^{q_0, 1}$. Учитывая, что высота автомата T не более чем h , легко проверить, что $[q' - i_1 \beta = [q_0 - i_2 \delta_2$.

Если $j \in B'$, то либо $j \leq i_1, j \in B_0$ и $\beta(j) = \delta_1(j) \leq \delta_1(q_0) = \beta(q')$, либо $j > i_1, j + (i_2 - i_1) \in B_0$ и $\beta(j) = \delta_2(j + (i_2 - i_1)) \leq \delta_2(q_0) = \beta(q')$. Если $j \in D'$, то либо $j \leq i_1, j \in B_0$ и $\beta(j) \vee \beta(q') = \delta_1(j) \vee \delta_1(q_0) = 1$, либо $j > i_1, j + (i_2 - i_1) \in B_0$ и $\beta(j) \vee \beta(q') = \delta_2(j + (i_2 - i_1)) \vee \delta_2(q_0) = 1$. Значит $\beta \in M_{B', D'}^{q', 1}$.

То есть, произвольный автомат $T \in M$ принадлежит $U(M_{B', D'}^{q', 1})$, где $B' \cup D' \neq \emptyset$ и $q' < q_0$. А мы предполагали, что q_0 — минимальное такое число. Получили противоречие. Полностью аналогично рассматривается случай когда $V = U(M_{B, D}^{q_0, 0})$. Лемма доказана.

Доказательство утверждения 5. Необходимость следует из утверждения 1. Докажем достаточность. Предположим, что M — не A -полно. Покажем, что для какого-то $V \in \widetilde{W}_3^h$ выполняется $M \subseteq V$. Из утверждения 3 следует, что для какого-то $V' \in \widetilde{W}$ выполняется $M \subseteq V'$. Покажем, что для любого $p \geq 2$ выполняется $h_2 \notin \widetilde{K}_p = U(K_p)$. В самом деле,

$$(0^p, 0^p), (0^p, 1^p), (0^{p-1}1, 0^{p-1}1) \in K_p,$$

$$h_2(0^p, 0^p, 0^{p-1}1) = 0^p, h_2(0^p, 1^p, 0^{p-1}1) = 0^{p-1}1.$$

При этом $(0^p, 0^{p-1}1) \notin K_p$. Значит $V' \notin \widetilde{K}$.

Также легко убедиться, что для любого $\widetilde{L}_p \in \widetilde{L}$ выполняется $h_2 \notin \widetilde{L}_p$. Значит $V' \notin \widetilde{L}$. То есть, мы получили, что $V' \in \widetilde{C} \cup \widetilde{S} \cup \widetilde{D} \cup \widetilde{A}$. Тогда из леммы 20 следует, что

$$V' \in \widetilde{C}_M \cup \widetilde{C}_0 \cup \widetilde{C}_1 \cup \widetilde{S} \cup \widetilde{D} \cup \widetilde{A}.$$

Из лемм 21, 16, 12, 13 и 15 следует, что существует

$$V \in \widetilde{C}_M^{3^h+3h} \cup \widetilde{C}_0^h \cup \widetilde{C}_1^h \cup \widetilde{S}^h \cup \widetilde{D}^h \cup \widetilde{A}^h \subseteq \widetilde{W}_2^h,$$

такое что $M \subseteq V$. Утверждение доказано.

Пусть $q \geq 2$, $N_q = \{(a, b) | 1 \leq a \leq b < q\}$, $B \subseteq N_q$, $D \subseteq \{1, 2, \dots, q-1\}$.
 Определим

$$F_{B,D}^q = \{\alpha \in E_2^q | \forall (n_1, n_2) \in B (\alpha(n_1) \vee \alpha(n_2) \vee \alpha(q) = 1), \\ \forall i \in D (\alpha(i) \leq \alpha(q))\}.$$

Определим два подсемейства $\tilde{C}_F \subset \tilde{C}$, $\tilde{C}_F^h \subset \tilde{C}^h$:

$$\tilde{C}_F = \{U(F_{B,D}^q) | q \geq 2, B \subseteq N_q, D \subseteq \{1, 2, \dots, q-1\}, B \cup D \neq \emptyset\} \\ \tilde{C}_F^h = \{U(F_{B,D}^q) | 2 \leq q \leq h, B \subseteq N_q, D \subseteq \{1, 2, \dots, q-1\}, B \cup D \neq \emptyset\}$$

Лемма 22. Пусть $V \in \tilde{C}$, $h_3^* \in V$, тогда $V \in \tilde{C}_M \cup \tilde{C}_F \cup \tilde{C}_0 \cup \tilde{C}_1$.

Доказательство. Пусть $V = U(C)$, где $C \subset E_2^q$, причём для любого $\alpha \in E_2^{q-1}$ существует $b \in E_2$, такое что $\alpha b \in C$. Если $q = 1$, то очевидно $V \in \tilde{C}_0 \cup \tilde{C}_1$.

Далее будем считать, что $q \geq 2$. Пусть $0^q \in C$, покажем, что в этом случае $h_2 \in V$. Пусть $\alpha_1, \alpha_2, \alpha_3 \in C$. Тогда нетрудно убедиться, что $h_2(\alpha_1, \alpha_2, \alpha_3) = h_3^*(\alpha_1, \alpha_2, \alpha_3, 0^q) \in C$. Значит, $h_2 \in V$ и утверждение леммы следует из леммы 20.

Пусть $0^q \notin C$, тогда $0^{q-1} \in C$. Так как $h_3^*(x_1, x_1, x_2, x_2) = x_1 \vee x_2 \in V$, и для любого $\alpha \in E_2^{q-1}$ существует $b \in E_2$, такое что $\alpha b \in C$, то для любого $\alpha \in E_2^{q-1}$ выполняется $\alpha b \vee 0^{q-1} 1 = \alpha 1 \in C$.

Пусть $B \subseteq N_q$ — множество всех пар (n_1, n_2) , где $1 \leq n_1 \leq n_2 < q$, таких что для любого $\alpha \in C$ выполняется $\alpha(n_1) \vee \alpha(n_2) \vee \alpha(q) = 1$. Пусть D — множество всех i , $1 \leq i < q$, таких что для любого $\alpha \in C$ выполняется $\alpha(i) \leq \alpha(q)$. Покажем, что $C = F_{B,D}^q$. Легко проверить, что $C \subseteq F_{B,D}^q$. Рассмотрим произвольное $\alpha \in F_{B,D}^q$, такое что $\alpha(q) = 0$. Докажем, что $\alpha \in C$. По индукции будем доказывать, что для любого $Q \subseteq \{1, 2, \dots, q-1\}$ существует $\beta \in C$, такое что $\beta(q) = 0$ и $\alpha(j) = \beta(j)$ для любого $j \in Q$.

Докажем базис индукции. Пусть $Q = \{j\}$, $\alpha(j) = 1$, тогда $j \notin D$, значит существует $\beta \in C$, такое что $\beta(j) = 1$, $\beta(q) = 0$. Пусть $Q = \{j\}$, $\alpha(j) = 0$, тогда $(j, j) \notin B$, значит существует $\beta \in C$, такое что $\beta(j) = \beta(q) = 0$. Аналогично, если $Q = \{j_1, j_2\}$, $\alpha(j_1) = \alpha(j_2) = 0$, тогда $(j_1, j_2) \notin B$, значит существует $\beta \in C$, такое что $\beta(j_1) = \beta(j_2) = \beta(q) = 0$.

Теперь докажем шаг индукции. Пусть $|Q| > 1$ и для какого-то $l \in Q$ выполняется $\alpha(l) = 1$. Тогда $l \notin D$, значит найдётся $\gamma \in C$, такое что $\gamma(l) = 1$, $\gamma(q) = 0$. По предположению индукции найдётся $\beta_0 \in C$, такое что $\beta_0(q) = 0$ и $\beta_0(j) = \alpha(j)$ для любого $j \in Q \setminus \{l\}$. Тогда возьмём $\beta = h_3^*(\beta_0, \beta_0, \gamma, 0^{l-1}10^{q-l-1}1) \in C$. Легко проверить, что $\beta(j) = \beta_0(j)$ для любого $j \in Q \setminus \{l\}$, $\beta(l) = 1$, $\beta(q) = 0$. Значит $\beta(j) = \alpha(j)$ для любого $j \in Q$.

Пусть $|Q| > 2$ и для любого $l \in Q$ выполняется $\alpha(l) = 0$. Очевидно найдутся попарно различные подмножества Q_1, Q_2, Q_3 множества Q , такие что $|Q_1| = |Q_2| = |Q_3| = |Q| - 1$. По предположению индукции найдутся $\beta_1, \beta_2, \beta_3 \in C$, такие что $\beta_1(q) = \beta_2(q) = \beta_3(q) = 0$ и $\beta_k(j) = \alpha(j)$ для любого $j \in Q_k$, $k = 1, 2, 3$. Возьмём $\beta = h_3^*(\beta_1, \beta_2, \beta_3, 0^{q-1}1) \in C$. Легко проверить, что $\beta(q) = 0$ и $\beta(j) = \alpha(j)$ для любого $j \in Q$.

Таким образом, мы доказали, что для любого $Q \subseteq \{1, 2, \dots, q-1\}$, существует $\beta \in C$, такое что $\beta(q) = 0$ и $\alpha(j) = \beta(j)$ для любого $j \in Q$. В частности это верно для $Q = \{1, 2, \dots, q-1\}$, значит $\alpha \in C$ и $C = F_{B,D}^q$. Так как $C \neq E_2^q$, то $B \cup D \neq \emptyset$ и $V \in \tilde{C}_F$. Лемма доказана.

Лемма 23. Пусть $M \subseteq \mathcal{P}_a^h$, $M \subseteq V \in \tilde{C}_F$, тогда существует $V' \in \tilde{C}_F^{4h \cdot 2^{8h^2} + 4h} \cup \tilde{C}_F^h$, такое что $M \subseteq V'$.

Доказательство. Пусть $V = U(F_{B,D}^q)$, где $q \geq 2$, $B \subseteq N_q$, $D \subseteq \{1, 2, \dots, q-1\}$, $B \cup D \neq \emptyset$.

Если для $(n_1, n_2) \in B$, $n_1 < n_2$, не существует $\eta \in F_{B,D}^q$, такого что $\eta(n_1) = \eta(q) = 0$, то во множестве B пару (n_1, n_2) можно заменить на пару (n_1, n_1) , при этом множество $F_{B,D}^q$ не изменится. Аналогично, если не существует $\eta \in F_{B,D}^q$, такого что $\eta(n_2) = \eta(q) = 0$, то пару (n_1, n_2) можно заменить на пару (n_2, n_2) . Поэтому далее будем полагать, что если $(n_1, n_2) \in B$, $n_1 < n_2$, то найдутся слова $\eta_1, \eta_2 \in F_{B,D}^q$, такие что

$$\eta_1(n_1) = \eta_1(q) = \eta_2(n_2) = \eta_2(q) = 0.$$

Пусть существует $(n_1, n_2) \in B$, такое что $h \leq n_1 \leq n_2 \leq q - h$ и $|n_1 - n_2| \geq h$. Покажем, что в этом случае $M \subseteq U(C_{1,h})$, то есть каждый автомат из M сохраняет единицу в момент времени h . Пусть T — автомат с n входами, $T \in M$. Рассмотрим произвольные $\alpha_1, \alpha_2, \dots, \alpha_n \in E_2^h$, такие что $\alpha_1(h) = \alpha_2(h) = \dots = \alpha_n(h) = 1$.

Докажем, что для $\beta = T(\alpha_1, \alpha_2, \dots, \alpha_n)$ выполняется $\beta(h) = 1$. Выберем произвольные слова $\gamma_1, \gamma_2, \dots, \gamma_n \in E_2^q$, такие что для любого i выполняется

$$[h]_{n_1} \gamma_i = [h]_{n_2} \gamma_i = [h]_q \gamma_i = \alpha_i.$$

$\gamma_i(q) = 1$ для любого i , поэтому $\gamma_i \in F_{B,D}^q$. Так как $M \subseteq U(F_{B,D}^q)$, то

$$T(\gamma_1, \gamma_2, \dots, \gamma_n) = \delta \in F_{B,D}^q.$$

Так как $T \in \mathcal{P}_a^h$, то $\delta(n_1) = \delta(n_2) = \delta(q) = \beta(h)$. Но $\delta \in F_{B,D}^q$, а $(n_1, n_2) \in B$, значит $\beta(h) = 1$. Таким образом, мы показали, что $M \subseteq U(C_{1,h}) \in \tilde{C}_1^h$.

Осталось рассмотреть случай, когда для любой пары $(n_1, n_2) \in B$ либо $n_1 < h$, либо $n_2 > q - h$, либо $|n_1 - n_2| < h$.

Рассмотрим минимальное q_0 , такое что для каких-то B_0 и D_0 выполняется $M \subseteq U(F_{B_0, D_0}^{q_0})$, причём $B_0 \cup D_0 \neq \emptyset$. Если $q_0 \leq 4h \cdot 2^{8h^2} + 4h$, то лемма доказана. Предположим, что это не так.

Каждому i от h до $q_0 - h$ сопоставим набор $r(i) = (a_1, a_2, a_3, \dots, a_{4h})$, где $a_1, a_2, \dots, a_{4h} \in E_2$. Если $j \leq h$, то $a_j = 1$ тогда и только тогда, когда $(j, i) \in B_0$. Если $h < j \leq 2h$, то $a_j = 1$ тогда и только тогда, когда $(i + j - 2h, i) \in B_0$. Если $2h < j \leq 3h$, то $a_j = 1$ тогда и только тогда, когда $(i, i + j - 2h) \in B_0$. Если $3h < j < 4h$, то $a_j = 1$ тогда и только тогда, когда $(i, q + j - 4h) \in B_0$. Если $j = 4h$, то $a_j = 1$ тогда и только тогда, когда $i \in D_0$. Нетрудно убедиться, что набор $r(i)$ определяет все пары из B_0 , в которых может присутствовать число i .

Идея доказательства заключается в следующем. Рассмотрим слово

$$r(h)r(h+1)r(h+2)\dots r(q_0-h)$$

в алфавите E_2^{4h} . Если q_0 достаточно велико, то в этом слове найдутся два совпадающих подслова длины $2h$, находящиеся на расстоянии больше h . Тогда мы можем «вырезать» часть между началами двух подслов и по получившемуся слову построить множество $F_{B', D'}^{q'}$, такое что $M \subseteq U(F_{B', D'}^{q'})$, $B' \cup D' \neq \emptyset$ и $q' < q_0$. Тем самым мы уменьшим q_0 , а мы предполагали, что оно минимально.

Для каждого $i = (4l + 3) \cdot h$, где $0 \leq l \leq 2^{8h^2}$, рассмотрим набор

$$(r(i - 2h + 1), r(i - 2h + 2), \dots, r(i - 2), r(i - 1), r(i)).$$

Этот набор может принимать $(2^{4h})^{2h} = 2^{8h^2}$ различных значений. Так как по предположению $q_0 > 4h \cdot 2^{8h^2} + 4h$, то найдутся различные числа $i_1 = (4l_1 + 3) \cdot h$ и $i_2 = (4l_2 + 3) \cdot h$, такие что $i_1 < i_2$ и $r(i_1 - j) = r(i_2 - j)$ для любого j , $0 \leq j < 2h$. В этом случае очевидно $i_2 - i_1 \geq 4h$, $3h \leq i_1, i_2 < q_0 - h$.

Пусть $q' = q_0 - (i_2 - i_1)$. Рассмотрим множество $B' \subseteq N_{q'}$, такое что $(n'_1, n'_2) \in B'$ точно тогда, когда выполняется одно из следующих условий:

- 1) $n'_1 \leq n'_2 \leq i_1, (n'_1, n'_2) \in B_0$,
- 2) $n'_1 \leq i_1, n'_2 > q' - h, (n'_1, n'_2 + (i_2 - i_1)) \in B_0$,
- 3) $n'_1 > i_1 - h, n'_2 > i_1, (n'_1 + (i_2 - i_1), n'_2 + (i_2 - i_1)) \in B_0$,
- 4) $n'_1 < h, n'_2 > i_1, (n'_1, n'_2 + (i_2 - i_1)) \in B_0$.

Также рассмотрим множество $D' \subseteq \{1, 2, \dots, q' - 1\}$, такое что $j \in D'$ точно тогда, когда $j < i_1$ и $j \in D_0$, либо $j > i_1$ и $j + (i_2 - i_1) \in D_0$.

Предположим, что $B' \cup D' = \emptyset$. Тогда определим множества $B'_0 \subseteq N_{q_0-h}, D'_0 \subseteq \{1, 2, \dots, q_0 - h - 1\}$. Пусть $(n_1, n_2) \in B'_0$ точно тогда, когда $(n_1 + h, n_2 + h) \in B_0$. Аналогично $j \in D'_0$ точно тогда, когда $j + h \in D_0$. Покажем, что $M \subseteq U(F_{B'_0, D'_0}^{q_0-h})$. Рассмотрим произвольный автомат с n входами $T \in M$ и произвольные $\alpha_1, \alpha_2, \dots, \alpha_n \in F_{B'_0, D'_0}^{q_0-h}$. Легко проверить, что для любого i выполняется $0^h \alpha_i \in F_{B_0, D_0}^{q_0}$. Значит

$$T(0^h \alpha_1, 0^h \alpha_2, 0^h \dots, 0^h \alpha_n) = \beta \in F_{B_0, D_0}^{q_0}.$$

Пусть $\gamma = T(\alpha_1, \alpha_2, \dots, \alpha_n)$. Легко проверить, что $[\downarrow_{q_0-2h}(\beta) = \downarrow_{q_0-2h}(\gamma)]$. Учитывая, что в B'_0 нет пары (n_1, n_2) , в которой $n_1 \leq h$, и в D'_0 нет j , такого что $j \leq h$, получаем, что $\gamma \in F_{B'_0, D'_0}^{q_0-h}$. Значит $M \subseteq U(F_{B'_0, D'_0}^{q_0-h})$, причём $B'_0 \cup D'_0 \neq \emptyset$. Но мы предполагали, что q_0 — минимальное такое число. Получили противоречие.

Теперь рассмотрим случай, когда $B' \cup D' \neq \emptyset$. Покажем, что $M \subseteq U(F_{B', D'}^{q'})$. Рассмотрим произвольный автомат с n входами $T \in M$ и произвольные $\alpha_1, \alpha_2, \dots, \alpha_n \in F_{B', D'}^{q'}$. Докажем, что для $\beta = T(\alpha_1, \alpha_2, \dots, \alpha_n)$ выполняется $\beta \in F_{B', D'}^{q'}$. Предположим, что это не так.

Для $i = 1, 2, \dots, n$ определим $\gamma_i = (\downarrow_{i_1} \alpha_i) \xi([\downarrow_{q'-i_1+2h} \alpha_i])$, где $|\xi| = i_2 - i_1 - 2h$, $\xi(j) = 0$ точно тогда, когда $j + i_1 \in D_0$. Покажем, что $\gamma_1, \gamma_2, \dots, \gamma_n \in F_{B_0, D_0}^{q_0}$.

Если $j \in D_0$, $j \leq i_1$, то $j \in D'$, значит $\gamma_i(j) = \alpha_i(j) \leq \alpha_i(q') = \gamma_i(q_0)$. Если $j \in D_0$, $j > i_2 - 2h$, то $j - (i_2 - i_1) \in D'$, значит $\gamma_i(j) = \alpha_i(j - (i_2 - i_1)) \leq \alpha_i(q') = \gamma_i(q_0)$. Если $j \in D_0$, $i_1 < j \leq i_2 - 2h$, то $\gamma_i(j) = 0$.

Пусть $(n_1, n_2) \in B_0$. Покажем, что для любого i выполняется $\gamma_i(n_1) \vee \gamma_i(n_2) \vee \gamma_i(q_0) = 1$. Если $n_1 \leq n_2 \leq i_1$, либо $n_1 \leq i_1$ и $n_2 > q_0 - h$, либо $n_1 > i_2 - h$ и $n_2 > i_2$, либо $n_1 < h$ и $n_2 > i_2$, то это следует из определения множества B' .

Если $i_1 < n_1 \leq i_2 - 2h$ и $\gamma_i(n_1) = 0$, то $n_1 \in D_0$, $n_1 < n_2$. Но тогда не существует слова $\eta \in B_0$, такого что $\eta(n_2) = \eta(q_0) = 0$. А мы полагали, что это не так. Аналогично доказывается, если $i_1 < n_2 \leq i_2 - 2h$ и $\gamma_i(n_2) = 0$.

Пусть $n_1 < h$ и $i_2 - 2h < n_2 \leq i_2$. Так как $r(n_2) = r(n_2 - (i_2 - i_1))$, то $(n_1, n_2 - (i_2 - i_1)) \in B_0$. Значит $(n_1, n_2 - (i_2 - i_1)) \in B'$ и $\alpha_i(n_1) \vee \alpha_i(n_2 - (i_2 - i_1)) \vee \alpha_i(q') = 1$ для любого i . Учитывая определение γ_i , получаем $\gamma_i(n_1) \vee \gamma_i(n_2) \vee \gamma_i(q_0) = 1$.

Пусть $i_2 - 2h < n_1 \leq i_2 - h$ и $n_2 > q - h$. Так как $r(n_1) = r(n_1 - (i_2 - i_1))$, то $(n_1 - (i_2 - i_1), n_2) \in B_0$. Значит $(n_1 - (i_2 - i_1), n_2 - (i_2 - i_1)) \in B'$ и $\alpha_i(n_1 - (i_2 - i_1)) \vee \alpha_i(n_2 - (i_2 - i_1)) \vee \alpha_i(q') = 1$ для любого i . Учитывая определение γ_i , получаем $\gamma_i(n_1) \vee \gamma_i(n_2) \vee \gamma_i(q_0) = 1$.

Осталось рассмотреть случай, когда $i_2 - 2h < n_1 \leq n_2 \leq i_2$. Так как $r(n_1) = r(n_1 - (i_2 - i_1))$, то $(n_1 - (i_2 - i_1), n_2 - (i_2 - i_1)) \in B_0$. Значит $(n_1 - (i_2 - i_1), n_2 - (i_2 - i_1)) \in B'$ и $\alpha_i(n_1 - (i_2 - i_1)) \vee \alpha_i(n_2 - (i_2 - i_1)) \vee \alpha_i(q') = 1$ для любого i . Учитывая определение γ_i , получаем $\gamma_i(n_1) \vee \gamma_i(n_2) \vee \gamma_i(q_0) = 1$.

Таким образом, мы доказали, что $\gamma_1, \gamma_2, \dots, \gamma_n \in F_{B_0, D_0}^{q_0}$. Тогда $T(\gamma_1, \gamma_2, \dots, \gamma_n) = \delta \in F_{B_0, D_0}^{q_0}$. Учитывая, что T — автомат высоты h , легко проверить, что $\beta = ([i_1 \delta])([q_0 - i_2 \delta])$, причём $[h]_{i_1} \delta = [h]_{i_2} \delta$. По предположению $\beta \notin F_{B', D'}^{q'}$. Если для какого-то $j \in D'$ выполняется $\beta(j) = 1$, $\beta(q) = 0$, то либо $j \leq i_1$, $j \in D_0$ и $\delta(j) = 1$, либо $j > i_1$, $j + (i_2 - i_1) \in D_0$ и $\delta(j + (i_2 - i_1)) = 1$. Оба случая невозможны.

Осталось рассмотреть случай, когда для какой-то пары $(n'_1, n'_2) \in B'$ выполняется $\beta(n'_1) = \beta(n'_2) = \beta(q') = 0$. Если $n'_1 \leq n'_2 \leq i_1$, то $\delta(n'_1) = \beta(n'_1) = 0$, $\delta(n'_2) = \beta(n'_2) = 0$, $\delta(q') = \beta(q_0) = 0$. Но $\delta \in F_{B_0, D_0}^{q_0}$ и $(n'_1, n'_2) \in B_0$. Получили противоречие.

Если $n'_1 \leq i_1$, $n'_2 > q' - h$, то $\delta(n'_1) = \beta(n'_1) = 0$, $\delta(n'_2 + (i_2 - i_1)) = \beta(n'_2) = 0$, $\delta(q') = \beta(q_0) = 0$. Но $\delta \in F_{B_0, D_0}^{q_0}$ и $(n'_1, n'_2 + (i_2 - i_1)) \in B_0$.

Получили противоречие.

Если $n'_1 > i_1 - h$, $n'_2 > i_1$, то $\delta(n'_1 + (i_2 - i_1)) = \beta(n'_1) = 0$, $\delta(n'_2 + (i_2 - i_1)) = \beta(n'_2) = 0$, $\delta(q') = \beta(q_0) = 0$. Но $\delta \in F_{B_0, D_0}^{q_0}$ и $(n'_1 + (i_2 - i_1), n'_2 + (i_2 - i_1)) \in B_0$. Получили противоречие.

Если $n'_1 < h$ и $n'_2 > i_1$, то $\delta(n'_1) = \beta(n'_1) = 0$, $\delta(n'_2 + (i_2 - i_1)) = \beta(n'_2) = 0$, $\delta(q') = \beta(q_0) = 0$. Но $\delta \in F_{B_0, D_0}^{q_0}$ и $(n'_1, n'_2 + (i_2 - i_1)) \in B_0$. Получили противоречие.

Значит произвольный автомат $T \in M$ принадлежит $U(F_{B', D'}^{q'})$, где $B' \cup D' \neq \emptyset$ и $q' < q_0$. А мы предполагали, что q_0 — минимальное такое число. Получили противоречие, лемма доказана.

Доказательство утверждения 6. Необходимость следует из утверждения 1. Докажем достаточность. Предположим, что M — не A -полно. Покажем, что для какого-то $V \in \widetilde{W}_3^h$ выполняется $M \subseteq V$. Из утверждения 3 следует, что для какого-то $V' \in \widetilde{W}$ выполняется $M \subseteq V'$. Покажем, что для любого $p \geq 2$ выполняется $h_3^* \notin \widetilde{K}_p = U(K_p)$. В самом деле,

$$(0^p, 0^p), (0^p, 1^p), (0^{p-1}1, 0^{p-1}1) \in K_p, \\ h_3^*(0^p, 0^p, 0^p, 0^{p-1}1) = 0^p, h_3^*(0^p, 0^p, 1^p, 0^{p-1}1) = 0^{p-1}1.$$

При этом $(0^p, 0^{p-1}1) \notin K_p$. Значит $V' \notin \widetilde{K}$.

Также легко убедиться, что для любого $\widetilde{L}_p \in \widetilde{L}$ выполняется $h_3^* \notin \widetilde{L}_p$. Значит $V' \notin \widetilde{L}$. Аналогично для любого $\widetilde{D}_p \in \widetilde{D}$ выполняется $h_3^* \notin \widetilde{D}_p$. Значит $V' \notin \widetilde{D}$.

То есть, мы получили, что $V' \in \widetilde{C} \cup \widetilde{S} \cup \widetilde{A}$. Из леммы 22 получаем, что

$$V' \in \widetilde{C}_M \cup \widetilde{C}_F \cup \widetilde{C}_0 \cup \widetilde{C}_1 \cup \widetilde{S} \cup \widetilde{A}.$$

Из лемм 20, 22, 16, 12 и 15 следует, что существует

$$V \in \widetilde{C}_M^{3h+3h} \cup \widetilde{C}_F^{4h \cdot 2^{8h^2} + 4h} \cup \widetilde{C}_0^h \cup \widetilde{C}_1^h \cup \widetilde{S}^h \cup \widetilde{A}^h,$$

такое что $M \subseteq V$. Учитывая, что $4h \cdot 2^{8h^2} + 4h > 3^h + 3h > h$, получаем $V \in \widetilde{W}_3^h$. Утверждение доказано.

Список литературы

- [1] Post E. Two-Valued Iterative Systems of Mathematical Logic. Princeton: Princeton Univ. Press, 1941.
- [2] Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. М.: Наука, 1966.
- [3] Буевич В. А. Об алгоритмической неразрешимости распознавания A -полноты для о.д.-функций // Математический заметки. Т. 12. № 6. 1972. С. 687–697.
- [4] Бабин Д. Н. Разрешимый случай задачи о полноте автоматных функций // Дискретная математика. 1992. Т. 4, вып. 4. С. 41–56.
- [5] Буевич В. А. Условия A -полноты для конечных автоматов. Ч. 1, 2. М.: Изд-во МГУ, 1986, 1987.
- [6] Бабин Д. Н. О классификации автоматных базисов Поста по разрешимости свойств полноты и A -полноты // Доклады Академии наук. № 4. Т. 367. 1999. С. 439–441
- [7] Буевич В. А., Клиндухова Т. Э. Об алгоритмической неразрешимости задач об A -полноте и полноте для дефинитных ограниченно-детерминированных функций // Математические вопросы кибернетики. Вып. 10. 2001.
- [8] Жук Д. Н., Присмотров Ю. Н. О проблеме полноты в классе автоматов без обратной связи // Интеллектуальные системы. Т. 11, вып. 1–4. 2007.
- [9] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. М.: Наука, 1985.
- [10] Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. 1964. Т. 155.