Теория и реализация языков программирования. Задание 3: Вычислительные возможности конечных автоматов

Сергей Володин, 272 гр.

задано 2013.09.18

Упражнение 1

Пусть $\sim \subset X \times X$. $C(x) = \{z \in X | x \sim z\}$, $C(y) = \{w \in X | y \sim z\}$.
Пусть $\exists z \in C(x) \cap C(y)$. Тогда $x \sim z, y \sim z$, и $w \in C(x) \overset{\text{def}}{\Leftrightarrow} x \sim w \underset{\text{транз. симм.}}{\overset{z \sim x}{\Leftrightarrow}} z \sim w \overset{y \sim z}{\Leftrightarrow} y \sim w \overset{\text{def}}{\Leftrightarrow} w \in C(y)$, то есть, $C(x) = C(y)$.
В противном случае $\rceil(\exists z \in C(x) \cap C(y)) \Leftrightarrow C(x) \cap C(y) = \varnothing$. Получаем, что возможны два случая:

1. $C(x) \cap C(y) = \varnothing$ *(не пересекаются)*
2. $C(x) = C(y)$ *(совпадают)*

Упражнение 2

Пусть $\varphi \colon \Sigma^* \supseteq X \longrightarrow \Delta^*$. $\varphi(\sigma_i) \overset{\text{def}}{=} \delta_i \in \Delta^*$, $|\sigma_i| = 1$.

1. *(единственность)* Предположим, что существует такое φ — морфизм. Тогда $\forall w = w_1 ... w_n \in X, |w_i| = 1 \hookrightarrow \varphi(w) \equiv \varphi(w_1 ... w_n) = \varphi(w_1) \cdot \varphi(w_2 ... w_n) = ... = \varphi(w_1) \cdot ... \cdot \varphi(w_n) \in \Delta^*$. Для $w = \varepsilon$ получаем $\varphi(\varepsilon) = \varepsilon$, так как φ — морфизм: $w_0 \overset{\text{def}}{=} \varphi(\varepsilon) = \varepsilon$. $\varphi(\varepsilon) \equiv \varphi(\varepsilon\varepsilon) = \varphi(\varepsilon)\varphi(\varepsilon) = w_0 w_0 \Rightarrow w_0 = w_0 w_0 \Rightarrow |w_0| = |w_0||w_0| \Rightarrow w_0 = \varphi(\varepsilon) = \varepsilon$.

   Таким образом, получаем, что такой морфизм единственный (если существует).

2. *(существование)* Докажем, что определенное выше отображение φ — морфизм: пусть $x, y \in X$. Рассмотрим случаи:

   a. $|x| = 0, |y| = 0 \Rightarrow \varphi(xy) = \varphi(\varepsilon\varepsilon) = \varphi(\varepsilon) = \varepsilon = \varepsilon\varepsilon = \varphi(\varepsilon)\varphi(\varepsilon)$
   b. $|x| = 0, |y| > 0 \Rightarrow \varphi(xy) = \varphi(y) = \varepsilon\varphi(y) = \varphi(x)\varphi(y)$
   c. $|x| > 0, |y| = 0 \Rightarrow \varphi(xy) = \varphi(x) = \varphi(x)\varepsilon = \varphi(x)\varphi(y)$
   d. $|x| > 0, |y| > 0 \Rightarrow \varphi(xy) = \varphi(x_1 ... x_m y_1 ... y_n) = \underbrace{\varphi(x_1) ... \varphi(x_m)}\underbrace{\varphi(y_1) ... \varphi(y_n)} = \varphi(x)\varphi(y)$.

Таким образом, если заданы значения $\varphi(\sigma_i), \sigma_i \in X \subset \Sigma^*$, то морфизм $\varphi \colon \Sigma^* \supseteq X \longrightarrow \Delta^*$ с этими значениями существует и единственнен.

Задача 1

Определим $R_3 : \mathsf{REG} \ni X \longrightarrow \mathbb{N} \cup \{0\}$ — количество применений правила 3 из определения регулярности X. В случае $X = AB$ или $X = A|B, A, B \in \mathsf{REG}$ $R_3(X) \overset{\text{def}}{=} 1 + R_3(A) + R_3(B)$. В случае $X = A^*, A \in \mathsf{REG}$, определим $R_3(X) \overset{\text{def}}{=} 1 + R_3(A)$. В случае $X = \varnothing$ или $X = \{\sigma\}$ определим $R_3(X) \overset{\text{def}}{=} 0$. Функция $R_3(X)$ определена корректно, так как определение регулярного языка корректное.
Пусть $\varphi \colon \Sigma^* \supset X \longrightarrow Y \subset \Delta^*$ — морфизм, $X \in \mathsf{REG}$. Докажем, что $Y \equiv \varphi(X) \in \mathsf{REG}$ индукцией по $R_3(X)$:
$P(i) = (\forall X \in \mathsf{REG} \colon R_3(X) \leqslant i \; \forall \varphi$ — морфизм $\hookrightarrow \varphi(X) \in \mathsf{REG})$.

1. Докажем $P(0)$: пусть $X \in \mathsf{REG} \colon R_3(X) = 0$. Тогда X получен без применения третьего правила. Значит, $\forall \varphi$ — морфизм либо $X = \varnothing \Rightarrow \varphi(X) = \varnothing$, либо $X = \{\sigma\} \Rightarrow \varphi(X) = \{\varphi(\sigma)\} = \{w\}, w \in \Delta^*$.

   Докажем, что $\Delta^* \supset \{w\} \in \mathsf{REG}$. $\{w\} \equiv \{\sigma_1 ... \sigma_n\} \equiv \{\sigma_1\} \cdot ... \cdot \{\sigma_n\}$. Поскольку $\{\sigma_i\} \in \mathsf{REG}$, и регулярные языки замкнуты относительно конкатенации (по определению), получаем требуемое.

   Итак, $\varphi(X) \in \mathsf{REG} \blacksquare$

2. Пусть $P(n)$. Докажем $P(n+1)$. Пусть $\mathsf{REG} \ni X \colon R_3(X) \leqslant n+1$. Если $R_3(X) < n+1$, $P(n) \Rightarrow X \in \mathsf{REG}$.
   $\sphericalangle X \colon R_3(X) = n + 1$. Возможны случаи:

   a. $X = WZ$, $W, Z \in \mathsf{REG}$. Тогда $\varphi(X) \equiv \varphi(WZ) = \{\varphi(wz) | w \in W, z \in Z\} = \{\varphi(w)\varphi(z) | w \in W, z \in Z\} = \{\varphi(w) | w \in W\} \cdot \{\varphi(z) | z \in Z\} = \varphi(W)\varphi(Z)$. $R_3(X) = 1 + R_3(W) + R_3(Z) = n + 1 \Rightarrow R_3(W), R_3(Z) \leqslant n \overset{P(n)}{\Rightarrow} \varphi(W), \varphi(Z) \in \mathsf{REG} \Rightarrow \varphi(X) = \varphi(W)\varphi(Z) \in \mathsf{REG}$.

b. $X = W|Z$, $W, Z \in \mathsf{REG}$. Тогда $\varphi(X) \equiv \varphi(W|Z) \equiv \varphi(W)|\varphi(Z)$. Аналогично $R_3(W), R_3(Z) \leqslant n \overset{P(n)}{\Rightarrow} \varphi(W), \varphi(Z) \in \mathsf{REG} \Rightarrow \varphi(X) = \varphi(W)|\varphi(Z) \in \mathsf{REG}$.

c. $X = W^*, W \in \mathsf{REG}$. Тогда $R_3(X) = 1 + R_3(W) = n + 1 \Rightarrow R_3(W) = n \overset{P(n)}{\Rightarrow} \varphi(W) \in \mathsf{REG} \Rightarrow \varphi(W^*) = \varphi(\varepsilon|W|WW|...) = \varphi(\varepsilon)|\varphi(W)|\varphi(WW)... \overset{\varphi(\varepsilon)=\varepsilon}{=} \varepsilon|\varphi(W)|\varphi(WW)... = \varphi(W)^* \in \mathsf{REG}$.

Получаем $\forall i \geqslant 0 \hookrightarrow P(i) \Rightarrow \forall X \in \mathsf{REG}\, \forall \varphi$ — морфизм $\hookrightarrow \varphi(X) \in \mathsf{REG}$ ■

Задача 2

1. Нет. Пусть $\Sigma = \{0, 1\}$, $L = \Sigma^*$. Определим $\varphi\colon L \longrightarrow L\colon \forall w \in L \hookrightarrow \varphi(w) = \varepsilon$. В этом случае φ — морфизм, так как $\forall x \in L\, \forall y \in L \hookrightarrow \varphi(xy) = \varepsilon = \varepsilon\varepsilon = \varphi(x)\varphi(y)$. Тогда $\forall \varnothing \neq X \subset L \hookrightarrow \varphi(X) = \{\varepsilon\}$, так как $\forall w \in L \hookrightarrow \varphi(w) = \varepsilon$. Поскольку $\varphi(\varepsilon) = \varepsilon \in L$, $\varphi^{-1}(\varepsilon) \ni \varepsilon \Rightarrow \varphi^{-1}(L) \supset \{\varepsilon\} \neq \varnothing \Rightarrow \varphi^{-1}(L) \neq \varnothing \Rightarrow \varphi(\varphi^{-1}(L)) = \{\varepsilon\} \neq L$.
   Таким образом, $\exists L \subseteq \Sigma^*\, \exists \varphi$ — морфизм: $\varphi(\varphi^{-1}(L)) \neq L$.

2. Нет. Пусть $\Sigma = \{a, b\}$, $L = \{b\}^*$, $\varphi(a) \overset{\text{def}}{=} \varphi(b) \overset{\text{def}}{=} a$. Доопределим φ так, чтобы оно было морфизмом (это возможно, см. упражнение 2). Тогда $\varphi(L) \equiv \varphi(\{b^*\}) \ni \varphi(b) = a \Rightarrow \varphi^{-1}(\varphi(L)) \supset \varphi^{-1}(a) \ni a \notin L \Rightarrow \varphi^{-1}(\varphi(L)) \nsubseteq L \Rightarrow \varphi^{-1}(\varphi(L)) \neq L$.
   Таким образом, $\exists L \subseteq \Sigma^*\, \exists \varphi$ — морфизм: $\varphi^{-1}(\varphi(L)) \neq L$.

3. Нет. Пусть $\Sigma = \{a, b\}$, $L = \{ab\}$, морфизм $\varphi\colon \Sigma^* \longrightarrow \Sigma^*$ — из предыдущего пункта. Тогда $\varphi(L) = \{\varphi(ab)\} = \{\varphi(a)\varphi(b)\} = \{aa\}$, $\varphi^{-1}(L) = \{x \in \Sigma^* | \varphi(x) \in \{ab\}\} = \{x \in \Sigma^* | \varphi(x) = ab\} = \varnothing$, так как $\varphi(\Sigma^*) = \varphi((a|b)^*) \overset{1.2.c}{=} (\varphi(a|b))^* = \{\varphi(a), \varphi(b)\}^* = \{a\}^* = a^* \not\ni ab$. Тогда $\varphi(\varphi^{-1}(L)) = \varphi(\varnothing) = \varnothing \not\ni aa \in \varphi^{-1}(aa) = \varphi^{-1}(\varphi(L))$.
   Таким образом, $\exists L \subseteq \Sigma^*\, \exists \varphi$ — морфизм: $\varphi(\varphi^{-1}(L)) \neq \varphi^{-1}(\varphi(L))$.

Упражнение

Докажем, что не всякий обратный морфизм — морфизм, то есть $\exists \Sigma\, \exists \Delta\, \exists \varphi\colon \Sigma^* \longrightarrow \Delta^*\colon \exists w_1 \in \Delta^*\, \exists w_2 \in \Delta^*\colon \varphi^{-1}(w_1 w_2) \neq \varphi^{-1}(w_1) \cdot \varphi^{-1}(w_2)$ *(здесь немного модифицировано определение морфизма для φ^{-1}, так как множество значений φ^{-1} — это 2^{Σ^*}, а не Σ^*).*
Пусть $\Sigma = \Delta = \{a, b\}$, $\varphi(a) \overset{\text{def}}{=} \varphi(b) \overset{\text{def}}{=} ab$. Доопределим φ так, чтобы оно было морфизмом (это возможно, см. упражнение 2). Тогда $\varphi^{-1}(a) = \varphi^{-1}(b) = \varnothing$, так как $\forall \varepsilon \neq w \in \Sigma^* \hookrightarrow |\varphi(w)| \geqslant 2$ и $|\varphi(\varepsilon)| = |\varepsilon| = 0$, то есть, значение $|\varphi(w)| = 1$ не достигается. Отсюда $\varphi^{-1}(a) \cdot \varphi^{-1}(b) = \varnothing$, но $\varphi^{-1}(ab) \supset \{a, b\} \Rightarrow \varphi^{-1}(ab) \neq \varnothing$. Поэтому $\varphi^{-1}(ab) \neq \varphi^{-1}(a)\varphi^{-1}(b)$ ■

Задача 3

(Хопкрофт. 4.2.4. Обратный гомоморфизм)
$\Delta^* \supset L \in \mathsf{REG} \Rightarrow \exists \mathcal{A} = (Q, \Delta, q_0, \gamma, F)$ — ДКА: $L(\mathcal{A}) = L$. Построим НКА $\mathcal{A}' = (Q', \Sigma, q_0, \gamma', F)$ для $L^{-1} \overset{\text{def}}{=} \varphi^{-1}(L)$. Определим $\gamma'(q, \sigma) = \gamma(q, \varphi(\sigma))$. Докажем, что тогда $\gamma'(q, w) = \gamma(q, \varphi(w))$:
$P(i) = \{\forall w \in \Sigma^*\colon |w| \leqslant i \hookrightarrow \gamma'(q, w) = \gamma(q, \varphi(w))\}$.

1. Докажем для $i = 0 \Rightarrow w = \varepsilon$. $\gamma'(q, \varepsilon) \overset{\text{не определено}}{=} \varnothing \overset{\text{ДКА}}{=} \gamma(q, \varepsilon) = \gamma(q, \varphi(\varepsilon))$
2. Пусть $P(i) \Rightarrow \forall w \in \Sigma^*\colon |w| \leqslant i \hookrightarrow \gamma'(q, w) = \gamma(q, \varphi(w))$. Пусть $\sigma \in \Sigma, |w| = i$. Тогда $\gamma'(q, w\sigma) = \gamma'(\gamma'(q, w), \sigma) = \gamma(\gamma'(q, w), \varphi(\sigma)) \overset{\text{P(i)}}{=} \gamma(\gamma(q, \varphi(w)), \varphi(\sigma)) = \gamma(q, \varphi(w)\varphi(\sigma)) = \gamma(q, \varphi(w\sigma)) \Rightarrow P(i+1)$.

Тогда $x \in L^{-1} \Leftrightarrow \varphi(x) \in L \Leftrightarrow \varphi(x) \in L(\mathcal{A}) \Leftrightarrow \gamma(q_0, \varphi(x)) = q \in F \Leftrightarrow \gamma'(q_0, x) = q \in F \Leftrightarrow x \in L(\mathcal{A}') \Rightarrow L^{-1} \equiv \varphi^{-1}(L) \in \mathsf{REG}$ ■

Задача 4

Пусть языки $\Sigma^* \supset X, Y \in \mathsf{REG}$. Докажем, что

1. $X \cup Y \in \mathsf{REG}$: из определения регулярности $\forall X, Y \in \mathsf{REG} \hookrightarrow X \cup Y \in \mathsf{REG}$ ■
2. $\overline{X} \overset{\text{def}}{=} \Sigma^* \backslash X \in \mathsf{REG}$: $X \in \mathsf{REG} \Rightarrow \exists$ полный ДКА $\mathcal{A}\colon L(\mathcal{A}) = X$. $F' \overset{\text{def}}{=} Q \backslash F$, $\mathcal{A}'$ — автомат $\mathcal{A}$ с множеством принимающих состояний F'. Докажем, что $L(\mathcal{A}') = \Sigma^* \backslash X$: $w \in \Sigma^*$, $(q_0, w) \vdash^* (q_w, \varepsilon)$ *(здесь используется полнота).* $w \in X \Leftrightarrow w \in L(\mathcal{A}) \Leftrightarrow q_w \in F \Leftrightarrow \urcorner(q_w \in Q \backslash F) \Leftrightarrow \urcorner(q_w \in F') \Leftrightarrow \urcorner(w \in L(\mathcal{A}'))$. Но $w \in X \Leftrightarrow \urcorner(w \in \Sigma^* \backslash X)$, откуда $\urcorner(w \in \Sigma^* \backslash X) \Leftrightarrow \urcorner(w \in L(\mathcal{A}'))$ и Получаем ДКА $\mathcal{A}'\colon L(\mathcal{A}') = \Sigma^* \backslash X \underset{\text{семинаре}}{\overset{\text{на}}{\Rightarrow}} \Sigma^* \backslash X \in \mathsf{REG}$ ■
3. $X \cap Y \in \mathsf{REG}$: $X \cap Y = \overline{\overline{X} \cup \overline{Y}}$. $X, Y \in \mathsf{REG} \overset{(2)}{\Rightarrow} \overline{X}, \overline{Y} \in \mathsf{REG} \overset{(1)}{\Rightarrow} \overline{X} \cup \overline{Y} \in \mathsf{REG} \overset{(2)}{\Rightarrow} \overline{\overline{X} \cup \overline{Y}} \in \mathsf{REG}$ ■

$$w \in X \cap Y \Leftrightarrow \begin{cases} w \in X \\ w \in Y \end{cases} \Leftrightarrow \begin{cases} \urcorner(w \in \overline{X}) \\ \urcorner(w \in \overline{Y}) \end{cases} \Leftrightarrow \urcorner \left[\begin{array}{l} w \in \overline{X} \\ w \in \overline{Y} \end{array} \right. \Leftrightarrow \urcorner(w \in \overline{X} \cup \overline{Y}) \Leftrightarrow w \in \overline{\overline{X} \cup \overline{Y}} \text{ (подразумевается } w \in \Sigma^*\text{)} \blacksquare$$

4. $X \backslash Y \in \mathsf{REG}$: $X \backslash Y = X \cap \overline{Y}$. $Y \in \mathsf{REG} \overset{(2)}{\Rightarrow} \overline{Y} \in \mathsf{REG} \overset{(3)}{\Rightarrow} X \cap \overline{Y} \in \mathsf{REG}$ ■

$$w \in X \cap \overline{Y} \Leftrightarrow \begin{cases} w \in X \\ w \in \overline{Y} \end{cases} \Leftrightarrow \begin{cases} w \in X \\ \neg(w \in Y) \end{cases} \Leftrightarrow w \in X \backslash Y \text{ (подразумевается } w \in \Sigma^*) \ ■$$

Задача 5

$\Sigma \overset{\text{def}}{=} \{a\}$. Предположим, что $\Sigma^* \subset L = \{a^{2^n} | n \geqslant 0\} \in \mathsf{REG} \underset{\text{о накачке}}{\overset{\text{по лемме}}{\Rightarrow}} \exists p = p_0 \geqslant 1 \colon \forall w \in L \hookrightarrow (w = xyz, |y| \geqslant 1, |xy| \leqslant p, (\forall i \geqslant 0 \hookrightarrow xy^iz \in L))$. Фиксируем $n = n_0 = p, w_0 = a^{2^p} \in L$. Получаем $w_0 = x_0y_0z_0, |y0| \geqslant 1, |x_0y_0| \leqslant p$. Поскольку $L \subset a^*, y \in a^*$, откуда $y = a^j$, $j \geqslant 1$. Аналогично $x = a^i, z = a^k \Rightarrow w_0 = a^{2^p} = xyz = a^{i+j+k} \Rightarrow i + j + k = 2^p$. По лемме должно выполняться $xy^2z = a^{i+2j+k} \in L \Rightarrow a^{i+2j+k} = a^{2^q}$, откуда $i+2j+k = 2^q \Rightarrow j = 2^q - 2^p \geqslant 2^{p+1} - 2^p = 2^p(2-1) = 2^p$. Но $|x_0y_0| \leqslant p \Rightarrow |y_0| \leqslant p$. Получаем $p \geqslant |y_0| = j \geqslant 2^p$ — противоречие, т.к. $\forall p \geqslant 1 \hookrightarrow p < 2^p$.

Значит, предположение неверно, и $L \notin \mathsf{REG}$ ■

Задача 6

1. Да. $L_1 = \{a^{2013n+5} | n \in \mathbb{N} \cup \{0\}\} \cap \{a^{509k+29} | k \in \mathbb{N}, k \geqslant 401\}$. $w \in L_1 \Leftrightarrow \exists n_w \in \mathbb{N} \cup \{0\}, 401 \leqslant k_w \in \mathbb{N} \colon w = a^{2013n_w+5} = a^{509k_w+29}$.

   Решим в целых числах $2013n + 5 = 509k + 29 \Leftrightarrow 2013n - 509k = 24 \Leftrightarrow (*)$ — линейное диофантово уравнение, $24 \vdots 1 = gcd(2013, 509) \Rightarrow$ решение существует, и $(*) \Leftrightarrow \left\| \begin{matrix} n \\ k \end{matrix} \right\| = \left\| \begin{matrix} x_0 \\ y_0 \end{matrix} \right\| + t \left\| \begin{matrix} x \\ y \end{matrix} \right\|$; $x_0, y_0, x, y, t \in \mathbb{Z}$, x_0, y_0, x, y — фиксированные, $t \geqslant t_0$ — параметр. Тогда $2013n + 5 = 509k + 29 = 2013(x_0 + xt) + 5 = pt + q$, $p, q \in \mathbb{Z}$ — фиксированные, $\mathbb{Z} \ni t \geqslant 0$ — параметр.

   Получаем $L_1 = \{a^{pt+q} | \mathbb{Z} \ni t \geqslant 0\} = \{a^{pt} | \mathbb{Z} \ni t \geqslant 0\} \cdot \{a^q\} = \{(a^p)^t | \mathbb{Z} \ni t \geqslant 0\} \cdot \{a^q\} = (a^p)^* a^q \equiv (\underbrace{a...a}_p)^* \underbrace{a...a}_q$ — задается регулярным выражением ■

2. Нет. Предположим, что $L_2 = \{a^{200n^2+1} | \mathbb{Z} \ni n \geqslant 1000\} \in \mathsf{REG} \underset{\text{о накачке}}{\overset{\text{по лемме}}{\Rightarrow}} \exists p \geqslant 1 \colon \forall w \in L_2 \hookrightarrow (w = xyz, |y| \geqslant 1, |xy| \leqslant p, (\forall i \geqslant 0 \hookrightarrow xy^iz \in L_2))$. Выберем $\mathbb{Z} \ni n = \max\{p, 1000\} \geqslant 1000 \Rightarrow w \overset{\text{def}}{=} a^{200n^2+1} \in L_2$. Получаем $\exists x, y, z \colon |y| \geqslant 1, |xy| \leqslant p \colon w = xyz$, откуда $x = a^i, y = a^j, z = a^k, i + j + k = 200n^2 + 1$. Также получаем $xy^2z \in L_2$. Но $xy^2z = a^{i+2j+k} = a^{200m^2+1} \Rightarrow i + 2j + k = 200m^2 + 1 \geqslant 200(n+1)^2 + 1 \Rightarrow j \geqslant [200(n+1)^2 + 1] - [200n^2 + 1] = 200 + 400n \geqslant 200 + 400p$. С другой стороны, $|xy| \leqslant p \Rightarrow j = |y| \leqslant p \Rightarrow p \geqslant j \geqslant 200 + 400p \Rightarrow 399p + 200 \leqslant 0$ при $p \geqslant 1$ — противоречие.

   Значит, предположение неверно, и $L_2 \notin \mathsf{REG}$ ■

3,4. **Можно не читать, доказательство не закончено** Да. $L_3 = \{\text{itoa}_2(x) | 0 \leqslant x \mod 3 = 2\}$, где $\text{itoa}_2(x)$ — запись числа x в двоичной системе счисления, начиная со старших разрядов. Построим ДКА $\mathcal{A}$: $L(\mathcal{A}) = L_3$, чем докажем $L_3 \in \mathsf{REG}$. Реализуем алгоритм деления в столбик на конечном автомате $\mathcal{A}$.
Формализуем деление на 3 в столбик с остатком в двоичной системе счисления. Пусть $|\text{itoa}_2(x)| = n$. Функции $p, r \colon \overline{0, n} \longrightarrow \mathbb{N} \cup \{0\}$. $P(i) \overset{\text{def}}{=} \{x = 3p(i) + r(i), r(i) < 3 \cdot 2^{n-i}\}$. Определим эти функции индуктивно и докажем $\forall i \in \overline{0, n} \hookrightarrow P(i)$.

   (a) Определение: $p(0) \overset{\text{def}}{=} 0, r(0) \overset{\text{def}}{=} x$. Доказательство $P(0)$: $x = 3 \cdot 0 + x$, $r(0) = x = \sum\limits_{k=0}^{n-1} 2^k x_{n-k} < 2^n < 3 \cdot 2^n$.

   (b) Пусть $p(k), r(k)$ определены для $k \in \overline{0, i}, \forall k \in \overline{0, i} \hookrightarrow P(k)$. Определим $p(i+1), r(i+1)$ и докажем $P(i+1)$

      1. Если $r(i) < 3 \cdot 2^{n-i-1}$, то $p(i+1) \overset{\text{def}}{=} p(i)$, $r(i+1) \overset{\text{def}}{=} r(i)$. $x \overset{P(i)}{=} 3p(i) + r(i) \equiv 3p(i+1) + r(i+1)$, $r(i+1) \equiv r(i) \overset{\text{случай}}{<} 3 \cdot 2^{n-i-1} \Rightarrow P(i+1)$ ■

      2. Иначе, если $r(i) \geqslant 3 \cdot 2^{n-i-1}$, $p(i+1) \overset{\text{def}}{=} p(i) + 2^{n-i-1}$, $r(i+1) \overset{\text{def}}{=} r(i) - 3 \cdot 2^{n-i-1} \overset{\text{случай}}{\geqslant} 0 \Rightarrow 3p(i+1) + r(i+1) = 3p(i) + 3 \cdot 2^{n-i+1} + r(i) - 3 \cdot 2^{n-i+1} = 3p(i) + r(i) = x$. $r(i) \overset{P(i)}{<} 3 \cdot 2^{n-i} \Leftrightarrow r(i) < 3 \cdot 2^{n-i-1} + 3 \cdot 2^{n-i-1} \Leftrightarrow r(i) - 3 \cdot 2^{n-i-1} < 3 \cdot 2^{n-i-1} \Leftrightarrow r(i+1) < 3 \cdot 2^{n-i-1}$. Получаем $P(i+1)$ ■

   Получаем $P(n) \Rightarrow x = 3p(n) + r(n), r(n) < 3 \cdot 2^{n-n} = 3 \Rightarrow p(n)$ — частное, $r(n)$ — остаток.

   Дальше была идея формально доказать, что строку можно разбить на куски длиной не более, чем 3 символа $\{0, 11, 101, 100\}$ *(«пропусков» вида (b.1) не больше трех подряд не в конце и не в начале слова) и что после прочтения каждого куска можно только хранить одно из трех чисел* $\{0, 1, 2\}$ *в состоянии автомата, а в конце это число и будет остатком...*