

1 Циклические моноиды, свободные моноиды .

Определение 1.1 (Свободный моноид). Свободный моноид - моноид, элементами которого являются конечные последовательности (строки) элементов носителя моноида. Свободный моноид на множестве $A \neq \emptyset$ это $\mathcal{A} = (A^*; \&, \varepsilon)$, A^* - множество всех слов в алфавите A , $\&$ - конкатенация, ε - пустое слово.

Теорема 1.2. Любой моноид, порождённый элементами множества, на котором есть свободный моноид, является гомоморфным образом этого моноида

ДОКАЗАТЕЛЬСТВО. Пусть $A \neq \emptyset$, $\mathcal{A} = (A^*; \&)$, $\mathcal{B} = (\{t^{\mathcal{B}}(a_1, \dots, a_n) : a_1, \dots, a_n \in A\}; *)$ и $h : \mathcal{A} \rightarrow \mathcal{B}$ - Гомоморфизм

$$h(a_1 \dots a_n) = (a_1, \dots, a_n)^{\mathcal{B}}$$

$$h(\varepsilon) = e^{\mathcal{B}}$$

Надо доказать свойство гомоморфизма:

$$h(u \& v) = h(u) * h(v)$$

Пусть $u = a_1 \dots a_n$, $v = a'_1 \dots a'_n$, тогда

$$h(u \& v) = h(uv) = h(a_1 \dots a_n a'_1 \dots a'_n) = (a_1 \dots a_n a'_1 \dots a'_n)^{\mathcal{B}}$$

$$h(u) * h(v) = h(a_1 \dots a_n) * h(a'_1 \dots a'_n) =$$

$$(a_1 \dots a_n)^{\mathcal{B}} * (a'_1 \dots a'_n)^{\mathcal{B}} = (a_1 \dots a_n a'_1 \dots a'_n)^{\mathcal{B}}$$

Из этого следует что $h(u \& v) = h(u) * h(v)$ □

Пример 1.3 (Примеры свободных моноидов и их гомоморфных образов). Пусть дан алфавит $A = \{1\}$, который образует множество слов $A^* = \{\varepsilon, 1, 11, \dots\}$ и моноид $\mathcal{A} = (A^*; \&, \varepsilon)$, тогда

1. $\mathcal{B} = (1; \cdot, 1)$, порождённый элементами A является гомоморфным образом \mathcal{A} , $h : \mathcal{A} \rightarrow \mathcal{B}$, $h(1 \dots 1) = 1$
2. $\mathcal{C} = (\omega; +, 0)$, порождённый элементами A (натуральные числа можно получить сложением единицы) является гомоморфным образом \mathcal{A} , $h : \mathcal{A} \rightarrow \mathcal{B}$, $h(\underbrace{1 \dots 1}_n) = n$

Определение 1.4 (Циклический моноид). Циклический моноид - моноид порождённый одним элементом. $\langle a \rangle$ - циклический моноид, порождённый элементом a .

$e, a, a^1, a^2, a^3, \dots$ - элементы моноида $\langle a \rangle$

1. $a^i \neq a^j$ при $i \neq j$

$h : \langle a \rangle \rightarrow (\{a\}^*; \&), h(a^i) = i$ - изоморфизм.

2. $a^i = a^j$ при $i \neq j$

$$k = i + (k - i) = i + y(j - i) + r$$

$$r = (k - i) \bmod (j - i)$$

$$r < j - i$$

тогда

$$\begin{aligned} a^k &= a^i \underbrace{a^{j-i} \dots a^{j-i}}_y a^r = \\ &= (a^i a^{j-i}) \underbrace{a^{j-i} \dots a^{j-i}}_{y-1} a^r \stackrel{(a^i a^{j-i} = a^{i+j-i} = a^j = a^i)}{=} a^i \underbrace{a^{j-i} \dots a^{j-i}}_{y-1} a^r = \\ &= a^i a^r = a^{i+r} (r < j - i; i + r < j) \end{aligned}$$

к чему весь этот список?

Пример 1.5 (Пример циклического моноида). $\langle a \rangle = (\{e, a, \dots\}; *)$

Таблица умножения $(*)$ -

	e	a	a^2
e	a	a	a^2
a	a	a^2	a
a^2	a^2	a	a^2

Теорема 1.6. Если j - наименьшее число такое что $a^i = a^j$ для какого-то $i < j$, то $\langle a \rangle$ содержит ровно j элементов

Доказательство.

$$\underbrace{e, a^1, \dots, a^{j-1}}_{\text{нет равных}}, \underbrace{a^j = a^i, a^{j+1} = a^{i+1}, \dots}_{\text{повторяющиеся}}$$

если j - номер наименьшего повтора, тогда

$$a^x * a^y = \begin{cases} a^{x+y}, & \text{если } x + y < j \\ a^{i+(x+y-i) \bmod (j-i)}, & \text{если } x + y \geq i \end{cases}$$

$$\begin{aligned} x + y &= k, & k &= i + (k - i \cdot z + r \\ r &= (k - i) \bmod (j - i) \\ a^k &= a^{i+z} \end{aligned}$$

$$a^{x+y} = a^k = a^{i+(x+y-i) \bmod (j-i)}$$

□

Определение 1.7 (Моноид типа $(i, j-i)$). Моноид типа $(i, j-i)$ - моноид с элементами

???

Теорема 1.8. В моноиде типа $(i, j-i)$, где $i > 0$ существует идемпотент $b \neq e$

Доказательство. ???

□