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

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

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

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

Надо доказать свойство гомоморфизма:

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

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

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

$$h(u) * h(v) = h(a_1...a_n) * h(a'_1...a'_n) = \\ (a_1...a_n)^{\mathcal{B}} * (a'_1...a'_n)^{\mathcal{B}} = (a_1...a_n a'_1...a'_n)^{\mathcal{B}}$$

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

Пример 1.1 (Примеры свободных моноидов и их гомоморфных образов)**.** *Пусть дан алфавит $A = \{1\}$, который образует множество слов $A^* = \{\varepsilon, 1, 11, ...\}$ и моноид $\mathcal{A} = (A^*; \&, \varepsilon)$, тогда*

1. *$\mathcal{B} = (1; \cdot, 1)$, порождённый элементами A является гомоморфным образом $\mathcal{A}$, $h : A \to B$, $h(1...1) = 1$*

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

Определение 1.2 (Циклический моноид)**.** Циклический моноид - моноид порождённый одним элементом. $< a >$ - циклический моноид, порождённый элементом a.

$e, a, a^1, a^2, a^3, ...$ - элементы моноида $< a >$

1. $a^i \neq a^j$ при $i \neq j$

   $h :< a >\to (\{a\}^*; \&)$, $h(a^i) = i$ - изоморфизм.

2. $a^i = a^j$ при $i \neq j$

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

$$r = (k - i)mod(j - i)$$

$$r < j - i$$

   тогда

$$a^k = a^i \underbrace{a^{j-i}...a^{j-i}}_{y} a^r =$$

$$(a^i a^{j-i}) \underbrace{a^{j-i}...a^{j-i}}_{y-1} a^r \overset{(a^i a^{j-i} = a^{i+j-i} = a^j = a^i)}{=} a^i \underbrace{a^{j-i}...a^{j-i}}_{y-1} a^r =$$

$$a^i a^r = a^{i+r} (r < j - i; i + r < j)$$

к чему весь этот список?

Пример 1.2 (Пример циклического моноида)**.** $< a >= (\{e, a, ...\}; *)$

Таблица умножения $(*)$ *-*

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

Теорема 1.2. *Если j - наименьшее число такое что $a^i = a^j$ для какого-то $i < j$, то $< a >$ содержит ровно j элементов*

Доказательство.

$$\underbrace{e, a^1, ..., a^{j-1}}_{\textit{нет равных}}, \underbrace{a^j = a^i, a^{j+1} = a^{i+1}, ...}_{\textit{повоторяющиеся}}$$

если j - номер наименьшего повтора, тогда

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

$$x + y = k, \qquad k = i + (k - i \cdot z + r$$
$$r = (k-i)mod(j-i)$$
$$a^k = a^{i+z}$$

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

□

Определение 1.3 (Моноид типа $(i, j-i)$)**.** Моноид типа $(i, j-i)$ - моноид с элементами

???

Теорема 1.3. *В моноиде типа $(i, j-i)$, где $i > 0$ существует идемпотент $b \neq e$*

Доказательство.

□