Уравнения в свободном моноиде (Лекция №2)

Андрей П. Немытых
Институт программных систем РАН
г. Переславль-Залесский

9 сентября 2013 г., Переславль-Залесский

Свободный моноид ранга два

Терема (Нильсен): Матрицы $\mathrm{M} \in \mathcal{M}_2(\mathbb{N}) \subset \mathbf{SL_2}(\mathbb{Z})$ образуют свободный моноид с двумя образующими:

$$\mathrm{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \mathrm{B} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Пусть $\mathcal{C} = \{\mathrm{a}, \mathrm{b}\}$ – алфавит коэффициентов, $\mathcal{V} = \{\mathrm{x_1}, \ldots, \mathrm{x_n}\}$ – алфавит переменных.

Свободный моноид ранга два

Следствие: Для всякой системы $\mathfrak{U} = \{\Phi_j = \Psi_j\}$ уравнений в словах с двухбуквенным алфавитом коэффициентов $\{a, b\}$ можно построить систему $\mathfrak{U}^*$ диафантовых уравнений так, что между решениями $\mathfrak{U}$ и натуральными решениями $\mathfrak{U}^*$ существует взаимноодно-значное соответствие.

Доказательство: Пусть $\gamma(x_i) = \begin{pmatrix} x_{i1} & x_{i2} \\ x_{i3} & x_{i4} \end{pmatrix}, \gamma() = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$
$\gamma(a) = A, \gamma(b) = B, \gamma(\xi_1 \dots \xi_k) = \gamma(\xi_1) \times \dots \times \gamma(\xi_k)$, где $\xi_i \in \mathcal{C} \cup \mathcal{V}$.

$$\{\Phi_j = \Psi_j\} \mapsto \begin{cases} \gamma(\Phi_j) = \gamma(\Psi_j); \\ \\ \forall i.\, \det(\gamma(x_i)) = 1; \end{cases}$$

□

Неравенства и уравнения

Рассматриваются уравнения в свободном моноиде конечного ранга. Пусть $\mathcal{C}$ – алфавит коэффициентов, $\mathcal{V}$ – алфавит переменных.

Предложение 2.1: Неравенство $\Phi \neq \Psi$ в словах в алфавите $\mathcal{C} \cup \mathcal{V}$ эквивалентно формуле:

$$\exists \mathbf{x}\, \exists \mathbf{y}\, \exists \mathbf{z}\ :\ \bigvee_{\mathbf{a} \in \mathcal{C}} (\Phi = \Psi \mathbf{a} \mathbf{x} \vee \Phi \mathbf{a} \mathbf{x} = \Psi) \vee \bigvee_{\mathbf{a}, \mathbf{b} \in \mathcal{C},\ \mathbf{a} \neq \mathbf{b}} (\Phi = \mathbf{x} \mathbf{a} \mathbf{y} \wedge \Psi = \mathbf{x} \mathbf{b} \mathbf{z})$$

Доказательство:

Первый случай соответствует решению такому, что $|\Phi_0| \neq |\Psi_0|$, второй случай решению такому, что $|\Phi_0| = |\Psi_0|$. □

Системы уравнений в свободном моноиде с не менее чем двумя образующими

Предложение 2.2: **Пусть $\mathrm{a}, \mathrm{b} \in \mathcal{C}$, $\mathrm{a} \neq \mathrm{b}$. Дизъюнкция двух уравнений в словах эквивалентна некоторому одному уравнению в словах с двумя дополнительными неизвестными.**

Доказательство:

$$(\Phi_1 = \Psi_1) \vee (\Phi_2 = \Psi_2) \Leftrightarrow (\Phi_1\Psi_2 = \Psi_1\Psi_2) \vee (\Psi_1\Phi_2 = \Psi_1\Psi_2)$$

$\Rightarrow$ **достаточно рассмотреть дизъюнкцию вида** $(\Phi_1 = \Psi) \vee (\Phi_2 = \Psi)$.

Пусть $\mathrm{P} = \Phi_1\Phi_2\Psi\mathrm{a}\Phi_1\Phi_2\Psi\mathrm{b}$, **тогда** P **простое.**

Лемма 2.2.1: **Пусть** $\mathrm{Q} \in (\mathcal{C} \cup \mathcal{V})^+$ **– простое такое, что** $\exists \mathrm{m} \in \mathbb{N} : \mathrm{P}$ **суть приставка слова** Q^{m}. **Тогда** $|\mathrm{Q}| > \frac{1}{2}|\mathrm{P}|$.

$\Rightarrow$ **Если** $|\mathrm{W}| \leq \frac{1}{2}|\mathrm{P}|$, **тогда в** $\mathrm{P}^2\mathrm{W}\mathrm{P}^2$ **нет вхождений** P^2, **кроме выделенных.**

$\Rightarrow (\Phi_1 = \Psi) \vee (\Phi_2 = \Psi) \Leftrightarrow \exists \mathrm{x}\ \exists \mathrm{y}\ :\ \mathrm{x}\mathrm{P}^2\Psi\mathrm{P}^2\mathrm{y} = \mathrm{P}^2\Phi_1\mathrm{P}^2\Phi_2\mathrm{P}^2$ $\square$

Сведение вопроса разрешимости к бинарному алфавиту

Предложение 2.3: **Пусть $\Phi = \Psi$ уравнение в словах над алфавитом констант $\mathcal{C}$ и $\mathcal{B} = \{\mathrm{a}, \mathrm{b}\}$, $\mathrm{a} \neq \mathrm{b}$. Тогда существует уравнение $\mathfrak{U}$ в словах над $\mathcal{B}$ такое, что $\mathfrak{U}$ имеет решение тогда и только тогда, когда $\Phi = \Psi$ имеет невырожденное решение (т.е. $\forall \mathrm{x} \in \mathcal{V}\, |\mathrm{x_0}| > 0$).**

Доказательство:

$\Longrightarrow$).Пусть $\mathcal{C} = \{\mathrm{a_1}, \ldots, \mathrm{a_k}\}$, где $\mathrm{k} > 2$. Рассмотрим гомоморфизм $\eta : (\mathcal{C} \cup \mathcal{V})^* \to (\mathcal{C} \cup \mathcal{V})^*$, где $\eta(\mathrm{a_i}) = \mathrm{ab^i a}$ и $\eta(\mathrm{x}) = \mathrm{axa}$ для $\mathrm{x} \in \mathcal{V}$.

Пусть $\mathrm{x_{1_0}}, \ldots, \mathrm{x_{n_0}}$ невырожденное решение уравнения $\Phi = \Psi$, тогда $\mathrm{x'_{1_0}}, \ldots, \mathrm{x'_{n_0}}$, где $\eta(\mathrm{x_{j_0}}) = \mathrm{ax'_{j_0}a}$, есть невырожденное решение уравнения $\eta(\Phi) = \eta(\Psi)$.

$\Longleftarrow$). .....

Сведение вопроса разрешимости к бинарному алфавиту

Предложение 2.3: **Пусть $\Phi = \Psi$ уравнение в словах над алфавитом констант $\mathcal{C}$ и $\mathcal{B} = \{\mathrm{a}, \mathrm{b}\}$, $\mathrm{a} \neq \mathrm{b}$. Тогда существует уравнение $\mathfrak{U}$ в словах над $\mathcal{B}$ такое, что $\mathfrak{U}$ имеет решение тогда и только тогда, когда $\Phi = \Psi$ имеет невырожденное решение (т.е. $\forall \mathrm{x} \in \mathcal{V}\, |\mathrm{x_0}| > 0$).**

Доказательство:

$\Longrightarrow$). .....

$\Longleftarrow$).Пусть $\mathrm{x}'_{1_0}, \ldots, \mathrm{x}'_{n_0}$ решение уравнения $\eta(\Phi) = \eta(\Psi)$, $\mathrm{x_{j_0}} = \mathrm{a x}'_{j_0} \mathrm{a}$ и $\mu(\mathrm{a_i}) = \mathrm{a b^i a}$, $\mu(\mathrm{x}) = \mathrm{x}$, тогда $\mathrm{x}_{1_0}, \ldots, \mathrm{x}_{n_0}$ – невырожденное решение уравнения $\mu(\Phi) = \mu(\Psi)$ такое, что $\mathrm{x_{j_0}} \in \mathrm{a}\mathcal{B}^*\mathrm{a}$.

Множество $\{[]\} \cup (\mathrm{a}\mathcal{B}^* \cap \mathcal{B}^*\mathrm{a})$ есть свободный подмоноид $\mathcal{B}^*$ с бесконечным базисом $\Sigma = \{\mathrm{a}\} \cup \mathrm{a}\mathcal{B}^*\mathrm{a} \backslash \mathcal{B}^*\mathrm{aa}\mathcal{B}^*$.

$\Longrightarrow$ $\mathrm{x}_{1_0}, \ldots, \mathrm{x}_{n_0}$ – невырожденное решение уравнения $\Phi = \Psi$, если мы отождествим $\mu(\mathcal{C})$ с $\mathcal{C}$. Единственное отличие: $\mathrm{x_{j_0}}$ может содержать конечное число букв из $\Sigma \backslash \mu(\mathcal{C})$.

Сведение вопроса разрешимости к бинарному алфавиту

Предложение 2.3: Пусть $\Phi = \Psi$ уравнение в словах над алфавитом констант $\mathcal{C}$ и $\mathcal{B} = \{\mathrm{a}, \mathrm{b}\}$, $\mathrm{a} \neq \mathrm{b}$. Тогда существует уравнение $\mathfrak{U}$ в словах над $\mathcal{B}$ такое, что $\mathfrak{U}$ имеет решение тогда и только тогда, когда $\Phi = \Psi$ имеет невырожденное решение (т.е. $\forall \mathrm{x} \in \mathcal{V}\, |\mathrm{x_0}| > 0$).

Доказательство:

$\Longleftarrow$)……

$\mathrm{x_{j_0}}$ может содержать конечное число букв из $\Sigma \backslash \mu(\mathcal{C})$.

$$\Longrightarrow \exists \text{ конечное } \mathcal{D} \subseteq \Sigma \backslash \mu(\mathcal{C}) : \Phi\Psi\Big|_{\mathrm{x'_{j_0}} \mapsto \mathrm{x_{j_0}}} \in (\mu(\mathcal{C}) \cup \mathcal{D})^*.$$

Выбирая любое $\rho : \mathcal{D} \to \mu(\mathcal{C})^+$ получаем невырожденное решение $\rho(\mathrm{x_{1_0}}), \ldots, \rho(\mathrm{x_{n_0}})$ уравнения $\mu(\Phi) = \mu(\Psi)$. Композиция:

$$(\mathcal{C} \cup \mathcal{V}) \xrightarrow{\mu} (\mu(\mathcal{C}) \cup \mathcal{V})^* \xrightarrow{\mathrm{x'_{j_0}} \mapsto \mathrm{x_{j_0}}} (\mu(\mathcal{C}) \cup \mathcal{D})^+ \xrightarrow{\rho} \mu(\mathcal{C})^+ \xrightarrow{\mu^{-1}} \mathcal{C}^+$$

даёт невырожденное решение уравнения $\Phi = \Psi$. □

Нетривиальные бескоэффициентные уравнения с двумя неизвестными

Предложение 2.4: Для любого решения x_0, y_0 нетривиального бескоэффициентного уравнения с двумя неизвестными x, y $\exists$ простое слово p такое, что $x_0 \in p^*, y_0 \in p^*$.
Доказательство: Индукция по $|x_0 y_0|$

Достаточно рассмотреть уравнения вида: $x\Phi(x, y) = y\Psi(x, y)$.

Для $|x_0 y_0| = 0$ Пред. 2.4 верно ($\boxplus$). Предположим, что оно верно для $|x_0 y_0| < n$. Пусть $|x_0 y_0| = n$ и $|x_0| \geq |y_0|$.

$\Longrightarrow x_0 = y_0 z_0$, где y_0, z_0 решение уравнения $z\Phi(yz, y) = \Psi(yz, y)$.

Если $\Psi(yz, y) = []$, то $x_0 = y_0$ и $\boxplus$; иначе $z\Phi(yz, y) = y\Psi'(yz, y)$.

Если $y_0 = []$, то $y_0 = (x_0)^0$ и $\boxplus$; иначе $|x_0 y_0| > |z_0 y_0|$ и к (z_0, y_0) применимо предположение индукции$\Longrightarrow \exists\, p : y_0, z_0 \in p^* \Longrightarrow x_0 = y_0 z_0 \in p^*$.
$\square$

Нетривиальные бескоэффициентные уравнения с двумя неизвестными

Предложение 2.4: Для любого решения x_0, y_0 нетривиального бескоэффициентного уравнения с двумя неизвестными x, y $\exists$ простое слово p такое, что $x_0 \in p^*, y_0 \in p^*$.

Следствие 2.4.1: Если $XY = YX$, то $\exists$ простое слово p такое, что $X \in p^*, Y \in p^*$.

Следствие 2.4.1': Если AB простое и $AB = BA$, то либо $A = []$, либо $B = []$.

Следствие 2.4.2: Пусть S, T – простые слова и пусть $S^n = T^m$, $n \geq 1, m \geq 1$. Тогда $S = T$.

Простые свойства

Если $Q = PR$, то пишем $P = \widehat{Q} \angle Q$, $R = \check{Q}$, $Q = \widehat{Q}\,\check{Q}$.

Предложение 2.5: Если S – простое слово и $PS \angle S^n$, то $P \in S^*$.
Доказательство:

$$PSV = S^n \Longrightarrow P = S^k \widehat{S} \Longrightarrow S^n = S^k \widehat{S} SV, n > k \Longrightarrow (\check{S}\widehat{S})^{n-k-1} \check{S} = SV$$

Если $n - k - 1 = 0$, то $\widehat{S} = []$ и $P = S^k$. Если $n - k - 1 > 0$, то $\widehat{S}\check{S} = \check{S}\widehat{S}$ $\Longrightarrow$ либо $\widehat{S} = []$, либо $\check{S} = [] \Longrightarrow$ либо $P = S^k$, либо $P = S^{k+1}$. $\square$

Следствие 2.5.1: Если $PA \angle A^n$, то $\exists$ простое $S : A \in S^*, P \in S^*$.

Следствие 2.5.2: Пусть $PAB \angle B(AB)^n, P \neq [], AB$ – простое. Тогда $P \in B(AB)^*$.

Простые свойства

Предложение 2.5: Если S – простое слово и $PS \angle S^n$, то $P \in S^*$.

Следствие 2.5.2: Пусть $PAB \angle B(AB)^n, P \neq [], AB$ – простое. Тогда $P \in B(AB)^*$.

Доказательство:

Покажем, что $|P| \geq |B|$. От противного.

Если $|P| < |B|$, то $B = PC, APC \angle C(APC)^n$, где $C \neq []$.

$|P| \neq 0 \Longrightarrow n > 0, APC = CAP$, что противоречит 2.4.1', так как APC – простое $\boxplus$.

$\Longrightarrow |P| \geq |B|$

$\Longrightarrow P = BC, CAB \angle (AB)^n$

$\Longrightarrow C \in (AB)^*, P \in B(AB)^*$ $\square$

Благодарю за внимание!