Уравнения в свободном моноиде и язык программирования Рефал (Лекция №1)

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

12 и 19 августа 2013 г., Переславль-Залесский

Нормальные алгорифмы Маркова

Алфавит: $\mathcal{A} = \{\mathrm{a}, \mathrm{b}\}$.

Пример схемы нормального алгорифма в двубуквенном алфавите:

$$\begin{cases} \mathrm{ab} \to \mathrm{baa} \\ \mathrm{b} \to \\ \to . \end{cases}$$

Начальное слово: aaab

$$\underbrace{\mathrm{aaa}}_{3}\mathrm{b} \Rightarrow \mathrm{aabaa} \Rightarrow \mathrm{abaaaa} \Rightarrow \mathrm{baaaaaa} \Rightarrow \underbrace{\mathrm{aaaaaa}}_{6}$$

$$\underbrace{\mathrm{a}\ldots\mathrm{a}}_{\mathrm{n}}\underbrace{\mathrm{b}\ldots\mathrm{b}}_{\mathrm{m}} \mapsto \underbrace{\mathrm{a}\ldots\mathrm{a}}_{\mathrm{n}\times 2^{\mathrm{m}}}$$

Правила преобразования строки

$$\begin{cases} l_1 \to r_1 \\ l_2 \to r_2 \\ \quad \dots \\ l_k \to r_k \end{cases}$$

Некоторые предложения объявлены заключительными.

[1]: s := начальная строка;
[2]: i := 0; M := ∅; /* Шаг преобразования: [2–10]. */
[3]: Пока $(M = \emptyset) \wedge (i < k)$
[4]: { $i := i + 1$;
[5]: Решить уравнение $x\, l_i\, y = s$. M := множество решений.
[6]: }
[7]: Если $M \neq \emptyset$,
[8]: то { $(x_0, y_0) := (u, v) \in M$ такой, что $ln(u) = \min_{(x,y)\in M} ln(x)$;
[9]: $s := x_0\, r_i\, y_0$;
[10]: }
[11]: Если $(M \neq \emptyset) \wedge (r_i$ не заключительное), то перейти к [2];
[12]: Выдать результат s.

Рефал (В.Ф. Турчин)

$$\begin{cases} l_1 & \to & r_1 \\ l_2 & \to & r_2 \\ & \dots & \\ l_k & \to & r_k \end{cases}$$

– Множество данных D – свободный моноид относительно операции приписывания. На D определена ещё одна унарная операция, позволяющая строить произвольные деревья.
$d ::= [] \mid c \mid d_1\ d_2 \mid (d)$ – $c \in$ символы

– Синтаксис Рефала позволяет закодировать левую часть любой конечной системы уравнений в D вида: $l_i = d$, где $d \in D$.

– Конечная система уравнений в свободном моноиде (с не менее чем двумя образующими) эквивалентна некоторому уравнению в этом моноиде.

Рефал

Система уравнений в D:

$$\begin{cases} \mathrm{l_1} = \mathrm{r_1} \\ \mathrm{l_2} = \mathrm{r_2} \\ \quad \ldots \\ \mathrm{l_k} = \mathrm{r_k} \end{cases}$$

записывается в виде:

$$(\mathrm{l_1})(\mathrm{l_2})\ldots(\mathrm{l_k}) = (\mathrm{r_1})(\mathrm{r_2})\ldots(\mathrm{r_k})$$

Системы уравнений в свободном моноиде с не менее чем двумя образующими

Лемма: Для всякой системы уравнений в словах с n неизвестными можно построить уравнение в словах с n неизвестными, эквивалентное этой системе.

Доказательство (А.Б. Ливчак):

Рассмотрим две образующие a, b. $\mathrm{a} \neq \mathrm{b}$. Система

$$\begin{cases} \Phi_1 = \Psi_1 \\ \Phi_2 = \Psi_2 \end{cases}$$

эквивалентна уравнению

$$\Phi_1 \mathrm{a} \Phi_2 \Phi_1 \mathrm{b} \Phi_2 = \Psi_1 \mathrm{a} \Psi_2 \Psi_1 \mathrm{b} \Psi_2$$

□

Классики

– **А.А. Марков (1954) построил алгоритм распознающий существование решений у уравнений в словах с двумя неизвестными. Поставил задачу доказательства алгоритмической неразрешимости распознавания существования решений у произвольного уравнения в словах (n неизвестных).**

– **Ю.И. Хмелевский (1967) построил алгоритм распознающий существование решений для $n = 3$.**

– **Г.С. Маканин (1977) построил алгоритм распознающий существование решений для произвольного n.**

О постановке задачи решения уравнений в словах

- **Решить уравнение в словах.**
  - **Что это означает, если множество решений уравнения бесконечно?**
  - **Вопрос о структуре этого множества решений нетривиален.**
- **Алгоритм Маканина перечисляет множество решений, если оно не пусто.**

Почему задача решения уравнений в словах сложная?

Пусть алфавит $\mathcal{A} = \{\mathrm{a}\}$. Уравнения в словах

– $\Phi = \Psi$ **кодируют диофантовые уравнения:** $|\Phi| = |\Psi|$.

– $\mathrm{x}\Phi = \Psi$ **кодируют диофантовые неравенства:** $|\Phi| \leq |\Psi|$

Алгоритмы для некоторых классов уравнений

- **Уравнения с постоянными правыми частями:**
  - $\Phi = \mathrm{C}_0$, **где** C_0 **константа.**
- **Уравнения с одной неизвестной.**
- **Квадратичные уравнения.**

Определение. **Уравнение в словах** $\Phi = \Psi$ **называется квадратичным, если каждая переменная входит в уравнение не более двух раз.**

Анализ нормальных алгорифмов Маркова

Алфавит: $\mathcal{A} = \{\mathrm{a}, \mathrm{b}\}$.

$$\begin{cases} \mathrm{ab} \to \mathrm{baa} \\ \mathrm{b} \to \\ \quad \to . \end{cases}$$

Анализируем алгорифм с параметризованным начальным словом.

Параметризованное начальное слово:
$\mathrm{P\,a\,a\,a\,Q}$, **где** P **и,** Q **параметры**

Возникают уравнения с параметрами:

$$\mathrm{x\,a\,b\,y} = \mathrm{P\,a\,a\,a\,Q}$$
$$\mathrm{x\,b\,y} = \mathrm{P\,a\,a\,a\,Q}$$
$$\mathrm{x\,y} = \mathrm{P\,a\,a\,a\,Q}$$

Анализ Рефал программ

$$\begin{cases} (\mathbf{e.x})(\mathbf{e.x}) \ \to \ \ldots \\ \qquad\qquad \ldots\ldots\ldots \end{cases}$$

Анализируем программу с параметризованными входными данными.

Параметризованные входные данные:
$(\Phi(\mathbf{p_1},\ldots,\mathbf{p_n}))\,(\Psi(\mathbf{p_1},\ldots,\mathbf{p_n}))$**, где** $\mathbf{p_1},\ldots,\mathbf{p_n}$ **параметры.**

Возникают уравнения произвольного вида:

$$\Phi(\mathbf{p_1},\ldots,\mathbf{p_n}) = \Psi(\mathbf{p_1},\ldots,\mathbf{p_n})$$

Здесь уравнение на параметры.

Простейший пример

Квадратичное уравнение с одной переменной. x **– переменная,** a **– коэффициент.**

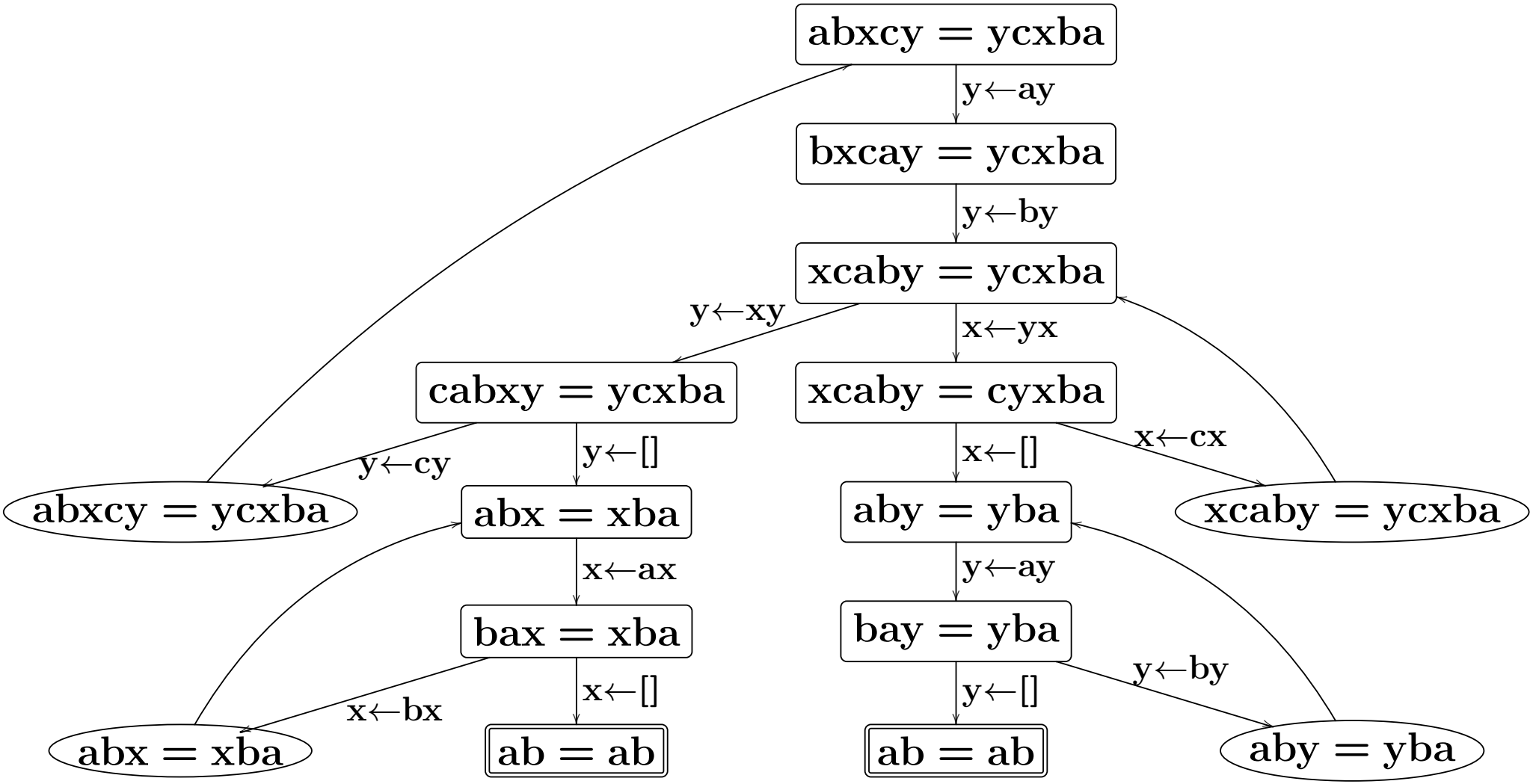
$$\mathrm{x\,a = a\,x}$$

Множество решений: a^***.**

Квадратичные уравнения

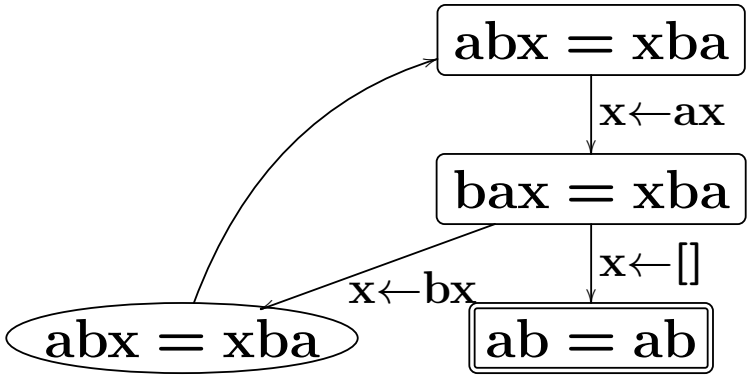
Пример решения квадратичного уравнения. x, y **– переменные,** $\mathrm{a}, \mathrm{b}, \mathrm{c}$ **– коэффициенты.**

$$\mathrm{a\,b\,x\,c\,y} = \mathrm{y\,c\,x\,b\,a}$$


abxcy = ycxba
y←ay
bxcay = ycxba
y←by
xcaby = ycxba
y←xy
x←yx
cabxy = ycxba
xcaby = cyxba
y←cy
y←[]
x←[]
x←cx
abxcy = ycxba
abx = xba
aby = yba
xcaby = ycxba
x←ax
y←ay
bax = xba
bay = yba
x←bx
x←[]
y←[]
y←by
abx = xba
ab = ab
ab = ab
aby = yba

$$\mathrm{a\,b\,x\,c\,y = y\,c\,x\,b\,a}$$

Частное решение: $(x_0, y_0) = (a, aba)$



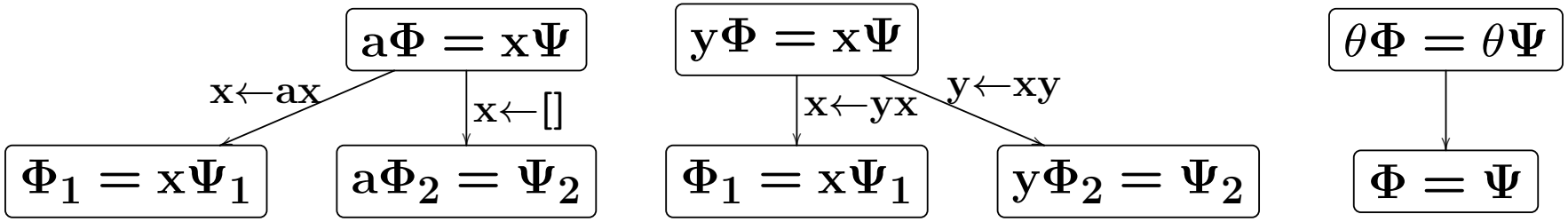
Общее решение уравнения $abx = xba$ **:** $x = (ab)^*a$

Множество частных решений исходного уравнения:
$(x, y) = ((ab)^*a, ab(ab)^*a)$

Алгоритм решения квадратичных уравнений

$\Phi = \Psi$

$\mathrm{a} \in \mathcal{C}, \mathrm{x}, \mathrm{y} \in \mathcal{V}, \theta, \rho \in \mathcal{C} \cup \mathcal{V}$, где $\mathrm{x} \neq \mathrm{y}$, $\mathcal{C}$ – алфавит коэффициентов, $\mathcal{V}$ – алфавит переменных.



Для каждого преобразования: $|\Phi_i = \Psi_i| \leq |\theta\Phi = \rho\Psi|$, алфавиты переменных и коэффициэнтов не увеличиваются.

Следовательно, на каждом пути развёртки дерева либо существует тождество, либо два совпадающих уравнения. Т.е. алгоритм завершает работу построением ориентированного графа G.

Уравнение $\Phi = \Psi$ имеет решение тогда и только тогда, когда в G существует лист (выходная вершина).

Некоторые понятия алгоритма Маканина

Пусть $\mathcal{A}$ – алфавит коэффициентов. Слова $\mathrm{y}, \mathrm{z} \in \mathcal{A}^*$ называются сопряжёнными, если существует $\mathrm{x} \in \mathcal{A}^*$ такое, что $\mathrm{xy} = \mathrm{zx}$.

Предложение 1. **Пусть $\mathrm{x}, \mathrm{y}, \mathrm{z} \in \mathcal{A}^*$ и $\mathrm{y}, \mathrm{z} \neq []$, тогда $\mathrm{xy} = \mathrm{zx} \Leftrightarrow \exists \mathrm{r}, \mathrm{s} \in \mathcal{A}^*, \mathrm{s} \neq [], \mathrm{n} \in \mathbb{N} : \mathrm{x} = (\mathrm{rs})^{\mathrm{n}}\mathrm{r}, \mathrm{y} = \mathrm{sr}, \mathrm{z} = \mathrm{rs}$.**

Слово $\mathrm{p} \in \mathcal{A}^*$ называется простым, если его нельзя представить в виде $\mathrm{p} = \mathrm{r}^{\mathrm{n}}$, где $\mathrm{r} \in \mathcal{A}^+$ (не пусто) и $\mathrm{n} > 1$.

Предложение 2. **Пусть $\mathrm{p} \in \mathcal{A}^*$ простое и $\mathrm{p}^2 = \mathrm{xpy}, \mathrm{x}, \mathrm{y} \in \mathcal{A}^*$, тогда либо $\mathrm{x} = []$, либо $\mathrm{y} = []$.**

Определение. **Показателем периодичности слова $w \in \mathrm{A}^*$ называется**

$$\mathbf{exp}(w) = \mathbf{max}\{\mathbf{n} \in \mathbb{N} |\ \exists \mathbf{r}, \mathbf{s}, \mathbf{p} \in \mathcal{A}^*, \mathbf{p} \neq [], w = \mathbf{r}\mathbf{p}^{\mathbf{n}}\mathbf{s}\}.$$

Определение. **Пусть $\mathbf{p} \in \mathcal{A}^+$ простое. $\mathbf{p}$-Устойчивым нормальным разложением слова $\mathbf{w} \in \mathcal{A}^*$ называется его представление в виде**

$$\mathbf{w} = \mathbf{u_0}\,\mathbf{p}^{\mathbf{n_1}}\,\mathbf{u_1} \ldots \mathbf{p}^{\mathbf{n_k}}\,\mathbf{u_k}$$

такое, что $\forall \mathbf{i}.\mathbf{p}^2$ не является делителем (подсловом) $\mathbf{u_i}$;

(i) если $\mathbf{k} \geq 1$, тогда

$\mathbf{u_0} \in \mathcal{A}^*\,\mathbf{p}$;

$\forall \mathbf{i}, \mathbf{0} < \mathbf{i} < \mathbf{k}.\mathbf{u_i} \in \mathcal{A}^*\,\mathbf{p} \cap \mathbf{p}\,\mathcal{A}^*$;

$\mathbf{u_k} \in \mathbf{p}\,\mathcal{A}^*$;

(ii) $\mathbf{k}$ минимальное из всех таких возможных представлений.

p-Устойчивое нормальное разложение слова

Пример. Пусть $\mathrm{p} = \mathrm{aba}, \mathrm{w} = \mathrm{ab}(\mathrm{aba})^5\mathrm{ba}(\mathrm{aba})^4\mathrm{ba}$. Тогда p-устойчивое нормальное разложение слова w суть $\mathrm{ab}\underbrace{\mathrm{aba}}_{\mathrm{p}}\,\mathrm{p}^3\,\overbrace{\mathrm{ab}\underbrace{\mathrm{aba}}_{\mathrm{p}}}^{\mathrm{p}}\,\mathrm{p}^3\,\overbrace{\mathrm{ababa}}^{\mathrm{p}}$.

Теорема. Пусть $\mathrm{p} \in \mathcal{A}^+$ простое. Для любого слова $\mathrm{w} \in \mathcal{A}^*$ существует и единственно p-устойчивое нормальное разложение.

Уравнения с одной неизвестной

– **Уравнения вида** $\Phi = \mathrm{v}$, **где** $\mathrm{v} \in \mathcal{A}^*$ **решаются просто.**

– **Достаточно рассмотреть уравнения вида** $\mathrm{ux}\Phi = \mathrm{xv}\Psi$,
где $\mathrm{u} \in \mathcal{A}^+$, $\mathrm{v} \in \mathcal{A}^*$ **и** $|\mathrm{v}|$ **максимальна.**
Рассмотрим произвольное невырожденное решение $\mathrm{x} \neq []$.

$\exists\, \mathrm{w} \in \mathcal{A}^+ : \mathrm{x}$ **является решением уравнения сопряжения** $\mathrm{ux} = \mathrm{xw}$;

$\Rightarrow\ \exists\, \mathrm{r}, \mathrm{s} \in \mathcal{A}^*, \mathrm{n} \in \mathbb{N} : \mathrm{x} = (\mathrm{rs})^{\mathrm{n}}\mathrm{r}, \mathrm{w} = \mathrm{sr}, \mathrm{u} = \mathrm{rs}$

$\Rightarrow\ \exists$ **простое слово** p **и** $\mathrm{g}, \mathrm{t} \in \mathcal{A}^*, \mathrm{m} \in \mathbb{N} : \mathrm{x} = \mathrm{p}^{\mathrm{m}}\mathrm{g}, \mathrm{p} = \mathrm{gt}$

$\Rightarrow\ \mathrm{x}$ **имеет вид** $\mathrm{x} = \mathrm{p}^{\mathrm{m}}\mathrm{g}, \mathrm{p} = \mathrm{gt}$, **где** p **– простой корень из** u

Перебираем все приставки g **слова** p.

Алгоритм решения уравнений с одной неизвестной

Достаточно рассмотреть уравнения вида $\mathbf{uxΦ = xvΨ}$, где $\mathbf{u} \in \mathcal{A}^+$, $\mathbf{v} \in \mathcal{A}^*$ и $|\mathbf{v}|$ максимальна. Рассмотрим произвольное невырожденное решение $\mathbf{x} \neq []$.

$\mathbf{x}$ имеет вид $\mathbf{x = p^m g, p = gt}$, где $\mathbf{p}$ – простой корень из $\mathbf{u}$
Пусть $\mathbf{g}$ приставка слова $\mathbf{p}$.

$\mathbf{m} \in \{0, 1\}$: **проверяем подстановкой;**

$\mathbf{m > 1 : x = pp^{m-2}pg, p = gt}$

Находим $\mathbf{p}$-устойчивые нормальные разложения:

$$\mathbf{uxΦ = u_0\, p^{i_1 m+n_1}\, u_1 \ldots p^{i_k m+n_k}\, u_k}$$

$$\mathbf{xvΨ = v_0\, p^{i'_1 m+n'_1}\, v_1 \ldots p^{i'_j m+n'_j}\, v_j}$$

где $\mathbf{i_l, i'_l} \in \mathbb{N}, \mathbf{n_l, n'_l} \in \mathbb{Z}$.

Алгоритм решения уравнений с одной неизвестной

p-устойчивое нормальное разложение:

$$\mathbf{ux\Phi = u_0\, p^{i_1 m+n_1}\, u_1 \ldots p^{i_k m+n_k}\, u_k = v_0\, p^{i'_1 m+n'_1}\, v_1 \ldots p^{i'_j m+n'_j}\, v_k = xv\Psi}$$

Получаем линейную диофантовую систему на $m > 1$ **:**
$(i_l - i'_l)m = n_l - n'_l$ **для всех** $1 \le l \le k$**.**

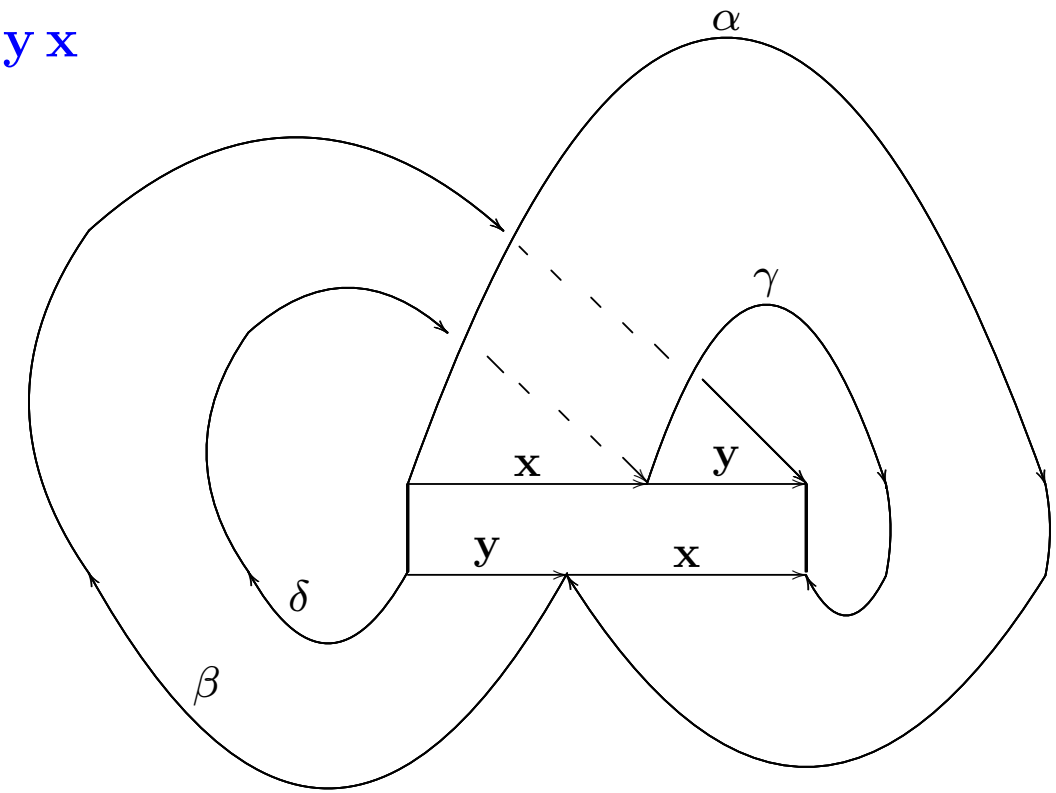
Она может:

- **быть противоречивой;**
- **иметь одно решение;**
- **быть тождеством** $\forall\, m > 1$**.**

Геометрия квадратичных уравнений (И.Г. Лысёнок)

Рассматриваем только те квадратичные уравнения, в которые каждая переменная входит ровно два раза. Каждому такому уравнению можно сопоставить двумерное многообразие с краем.

Пример: $\mathrm{x\,y = y\,x}$



Граница – связное многообразие $\delta^{-1}\alpha\beta\gamma^{-1}$.

Уравнения в свободной группе с конечным числом образующих

$$\Phi(x_1, \ldots, x_n, a_1, \ldots, a_m) = 1$$

где $a_1, \ldots, a_m \in \mathcal{A}$, $x_1, \ldots, x_n \in \mathcal{V}$.

– Г.С. Маканин (1982) построил алгоритм распознающий существование решений в свободной группе.

– А.А. Разборов (1987) описал структуру множеств решений таких уравнений.

– А.Г. Мясников, О. Харлампович, З. Села (1990-е годы) улучшили результат Разборова.

Благодарю за внимание!