О языке описания свойств параметризованных конфигураций

(уравнение Хмелевского в словах)

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

Совместное рабочее совещание ИПС РАН и МГТУ имени Н.Э. Баумана
по функциональному языку программирования Рефал
8 июня 2021 г., Москва

Системы уравнений в свободном конечнопорожденном моноиде

Определение. Пусть даны конечный алфавит констант Σ и алфавит переменных $\mathcal{V}$. Уравнением в словах из Σ^* называется выражение вида:

$$\mathbf{\Phi} = \mathbf{\Psi}, \text{ где } \mathbf{\Phi}, \mathbf{\Psi} \in \{\mathbf{\Sigma} \cup \mathcal{V}\}^*.$$

Если $|\mathbf{\Phi}\,\mathbf{\Psi}|_{\Sigma} = 0$, то уравнение называется бескоэффициентным.

Примеры: Пусть $\mathrm{A} \in \Sigma, \quad \mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{v} \in \mathcal{V}$.

$\mathbf{x}\,\mathbf{A} = \mathbf{A}\,\mathbf{x}$,
$\mathbf{x}\,\mathbf{y}\,\mathbf{z} = \mathbf{z}\,\mathbf{v}\,\mathbf{x}$ – бескоэффициентное уравнение Хмелевского.

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 $\Sigma = \{\mathrm{A}\}$. Уравнения в словах

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

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

Простые алгоритмы для некоторых классов уравнений

– **Уравнения с постоянными правыми частями:**

  – $\Phi = C_0$, **где** $C_0 \in \Sigma^*$ **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: для любой $x \in \mathcal{V}$ $|\Phi\,\Psi|_x \leq 2$.**

Анализ Рефал программ

$$\begin{cases} (\mathrm{e.x})(\mathrm{e.x}) \ \rightarrow \ \ldots \\ \qquad\qquad \ldots\ldots\ldots \end{cases}$$

Анализируем программу с параметризованными входными данными.

Параметризованные входные данные:
$(\Phi(\mathrm{p}_1,\ldots,\mathrm{p}_\mathrm{n}))\,(\Psi(\mathrm{p}_1,\ldots,\mathrm{p}_\mathrm{n}))$**, где** $\mathrm{p}_1,\ldots,\mathrm{p}_\mathrm{n}$ **параметры.**

Возникают уравнения произвольного вида:

$$\Phi(\mathrm{p}_1,\ldots,\mathrm{p}_\mathrm{n}) = \Psi(\mathrm{p}_1,\ldots,\mathrm{p}_\mathrm{n})$$

Здесь уравнение на параметры.

Простейший пример

Квадратичное уравнение с одной переменной. x – переменная, A – коэффициент.

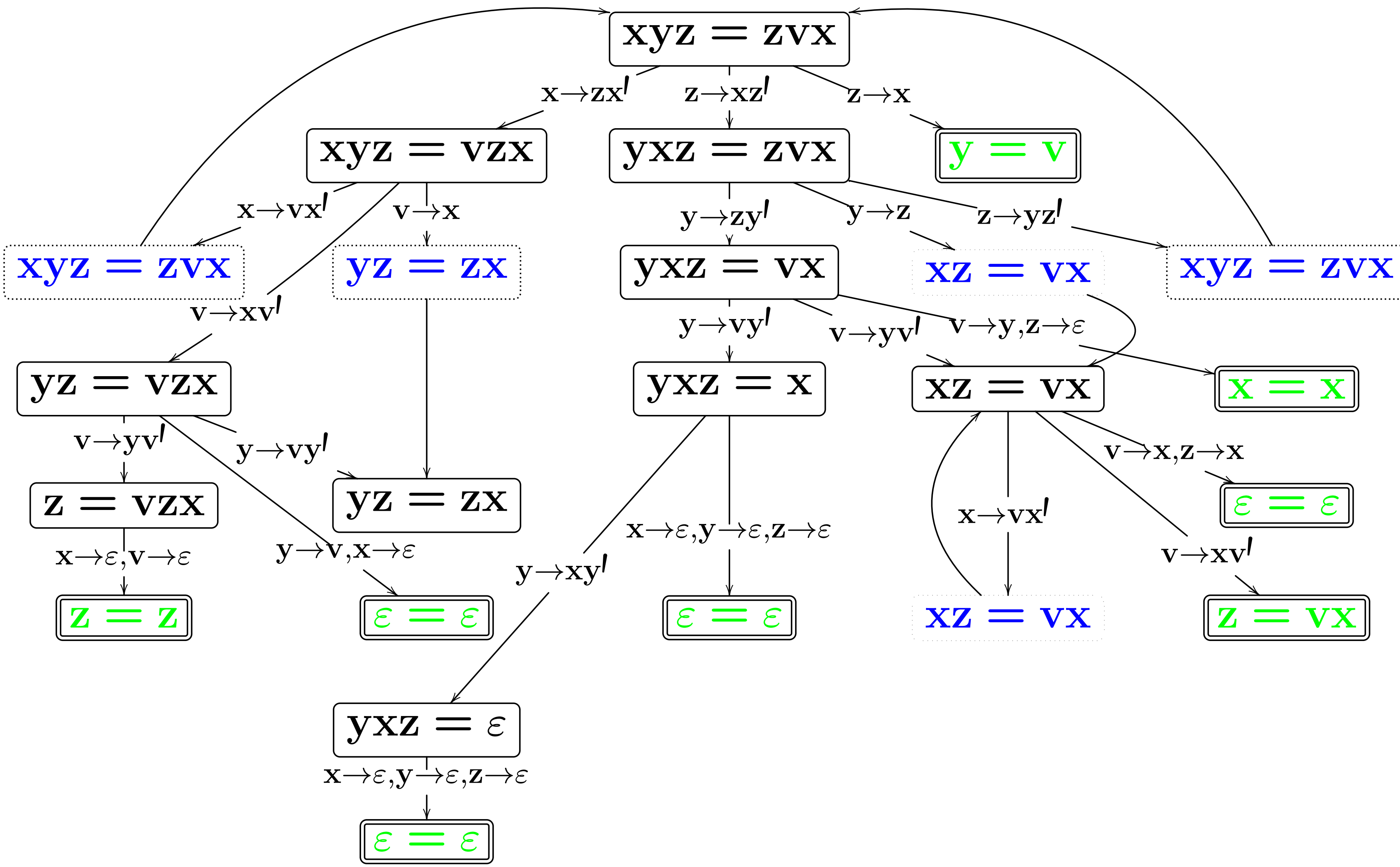
$$\mathrm{x\,A = A\,x}$$

Множество решений: A^*.

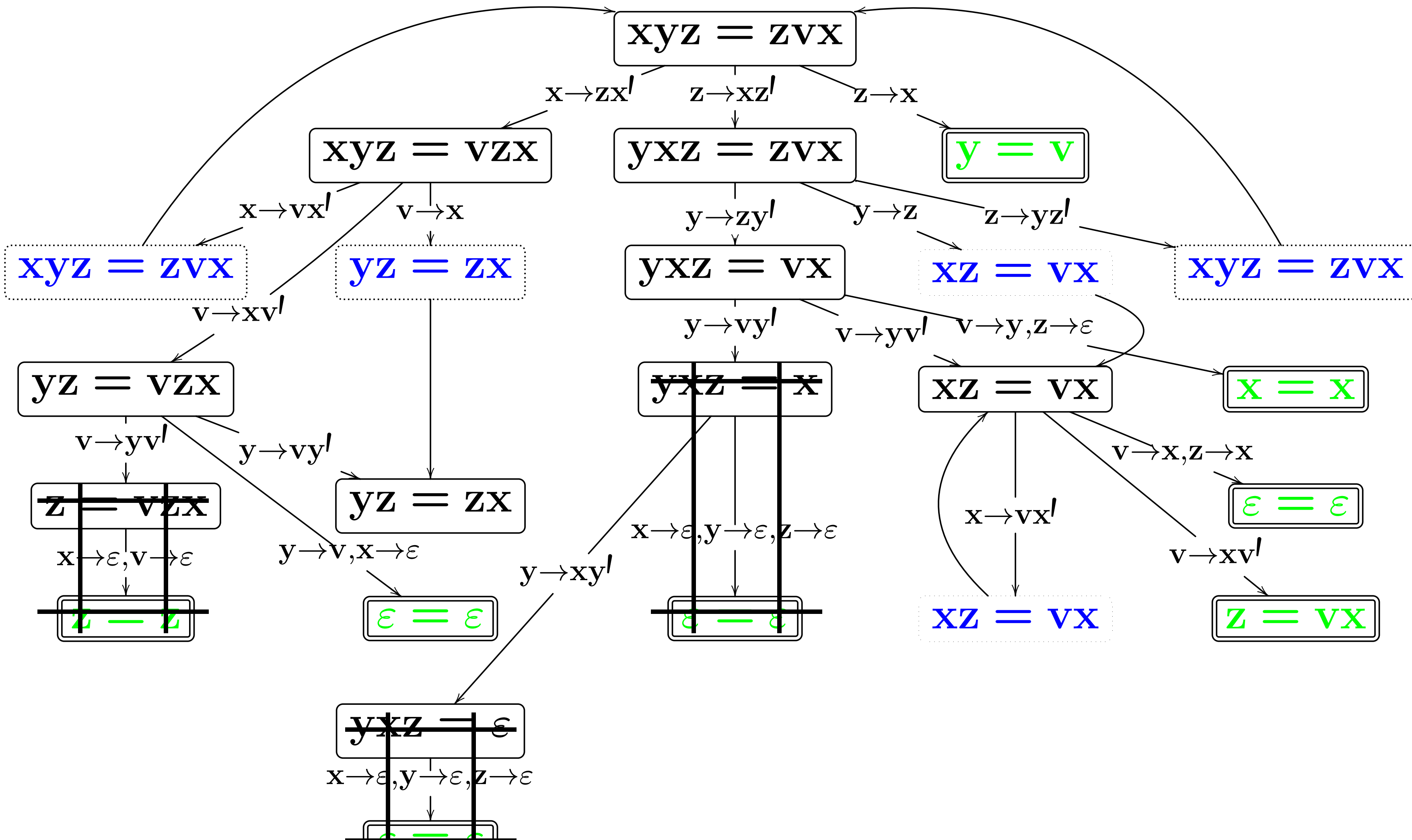
Квадратичные уравнения

Пример решения квадратичного уравнения. Уравнение Хмелевского, $\mathrm{x, y, z, v}$ – переменные.

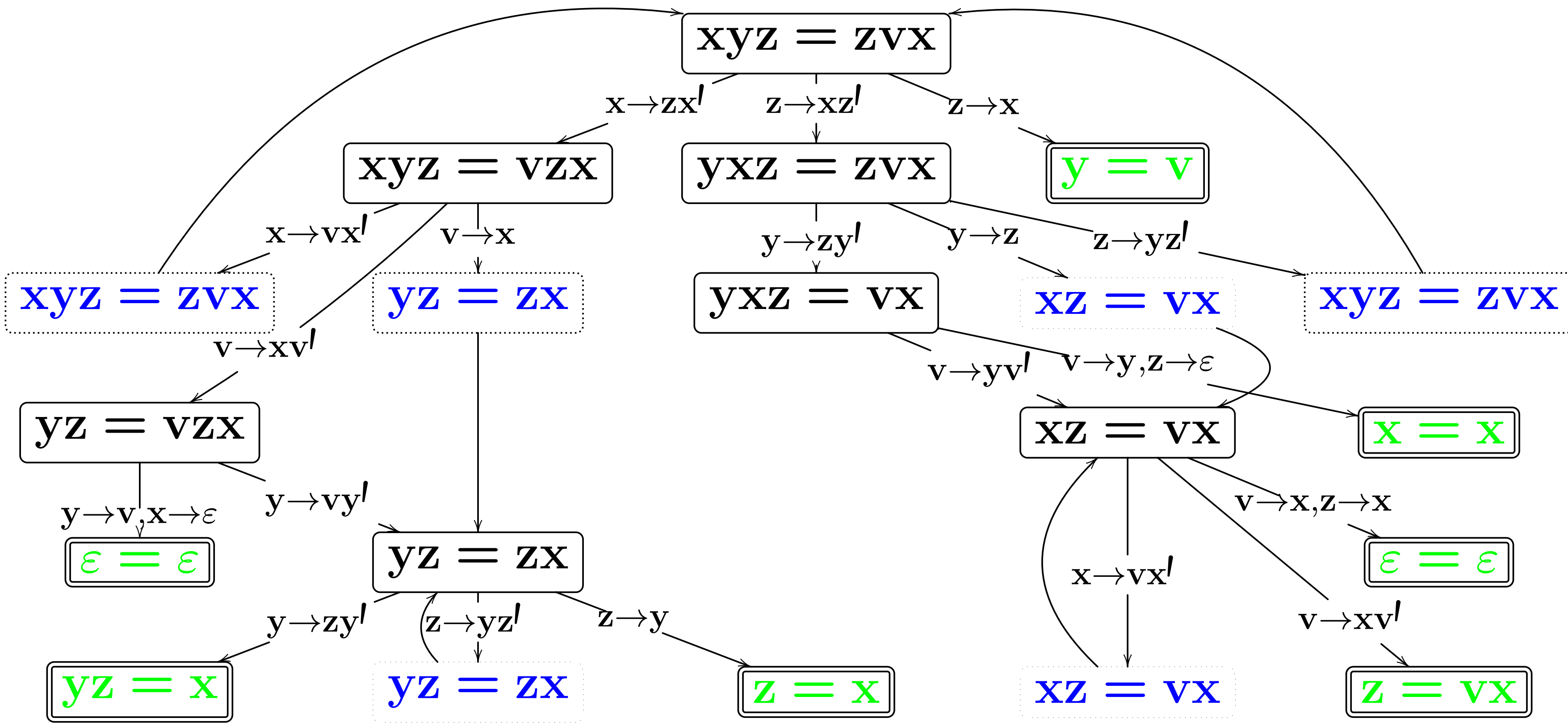
$$\mathrm{x\,y\,z = z\,v\,x}$$



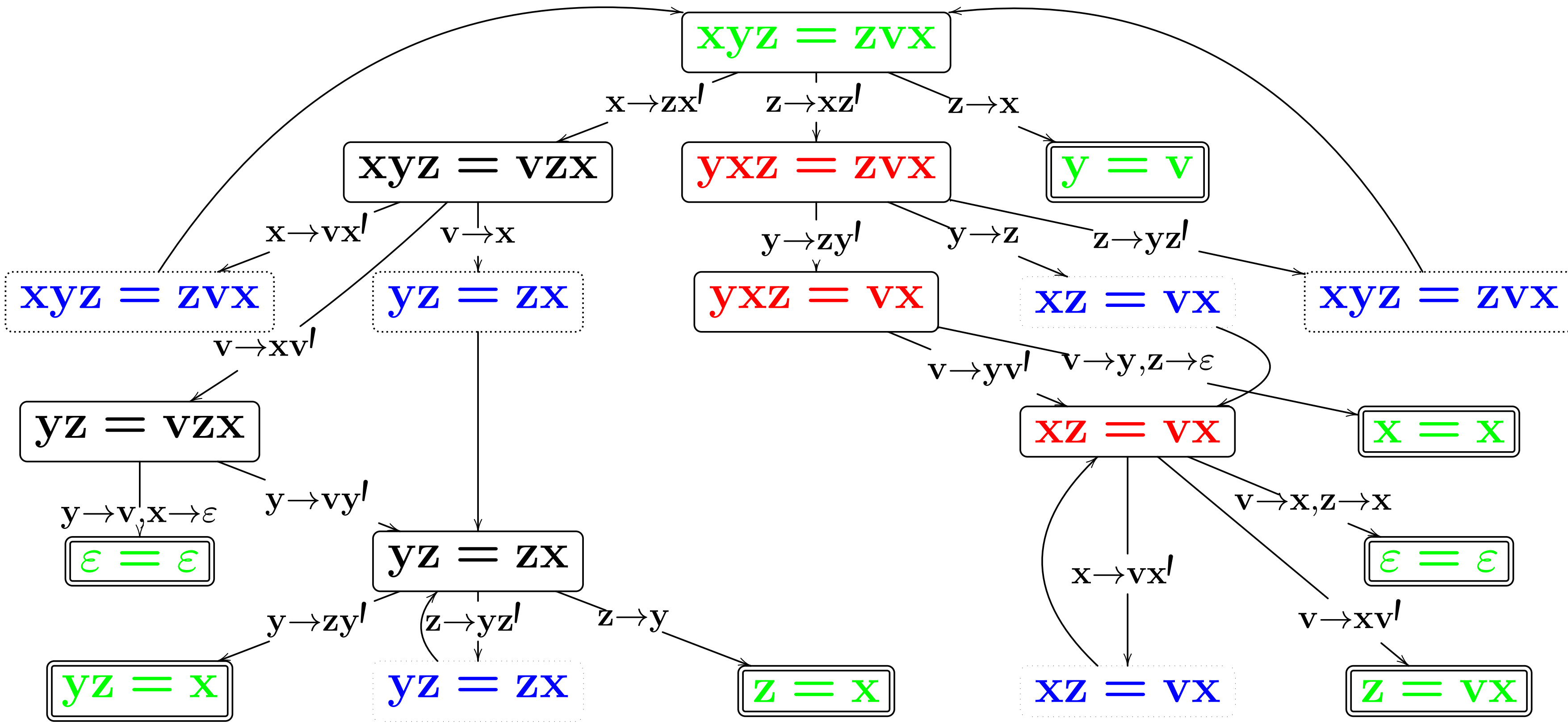
Здесь любая $u \in \mathcal{V}$, вхождение которой в сужение на ребре E имеет вид u', пробегает (под)множество Σ^{+}. Во входной вершине ребра E штрих над переменными не ставится.



Здесь значение u_0 $\forall u \in \mathcal{V}$, вхождение которой в сужение на ребре E имеет вид u', такое, что $|u_0| > 0$. В вершинах E штрих не ставится.



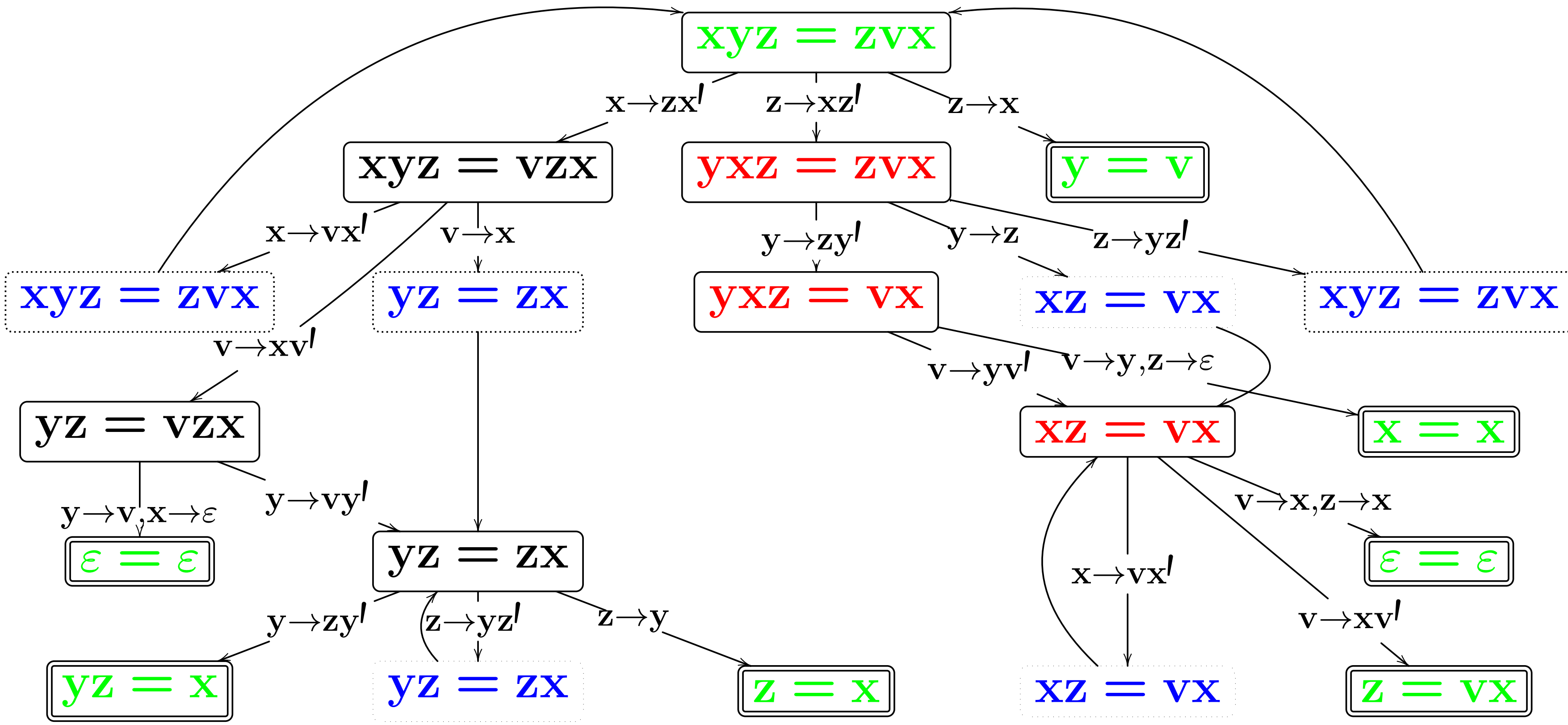
Здесь значение u_0 $\forall u \in \mathcal{V}$, вхождение которой в сужение на ребре E имеет вид u', такое, что $|u_0| > 0$. В вершинах E штрих не ставится.



$z \to xz'$, $y \to zy'$, $v \to yv'$, $(x \to vx')^n$, $v \to xv'$, $z \to vx$, **где** $n \geq 0$.

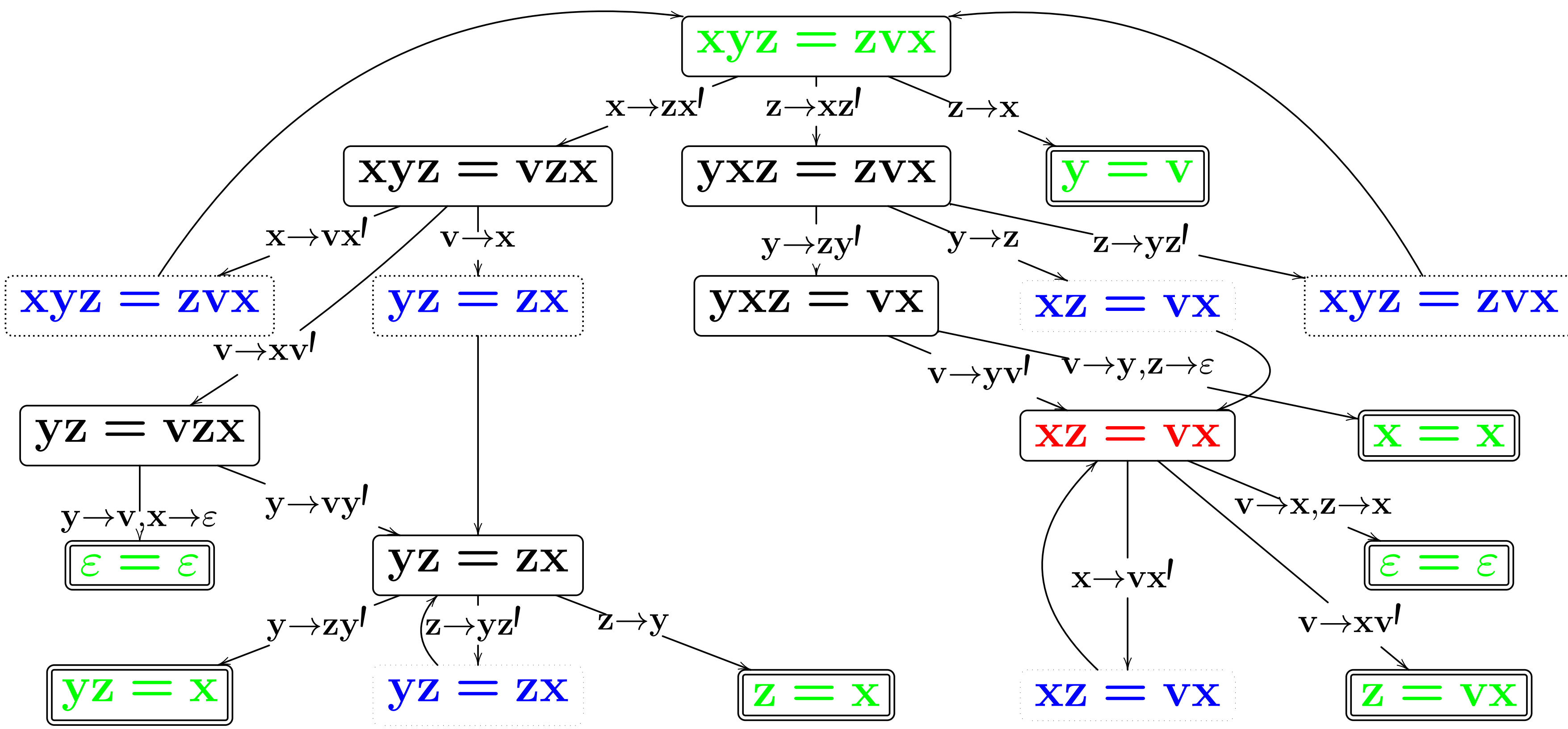
$z \to xz'$, $y \to zp$, $v \to pv'$, $x \to v^n s$, $v \to sr$, $z \to rs$, **где** p, r, s **параметры.**

$z \to (sr)^n srs$, $y \to rsp$, $v \to psr$, $x \to (sr)^n s$, $v \to sr$, $z \to rs$;



$z \to (sr)^n srs,\ y \to rsp,\ v \to psr,\ x \to (sr)^n s,\ v \to sr,\ z \to rs$;

Пример семейства решений: $x = (sr)^n s,\ y = rsp,\ z = (sr)^n srs,\ v = psr,$ **где** $\mathbb{N} \ni n \geq 0,\ p, r, s$ **– параметры, принимающие значения в** Σ^***.**



$\mathrm{z} \to (\mathrm{sr})^{\mathrm{n}}\mathrm{srs},\ \mathrm{y} \to \mathrm{rsp},\ \mathrm{v} \to \mathrm{psr},\ \mathrm{x} \to (\mathrm{sr})^{\mathrm{n}}\mathrm{s},\ \mathrm{v} \to \mathrm{sr},\ \mathrm{z} \to \mathrm{rs}$;

Множество решений уравнения сопряжения $\mathrm{xz} = \mathrm{vx}$ **:**

$\mathrm{x} = (\mathrm{sr})^{\mathrm{n}}\mathrm{s},\ \mathrm{z} = \mathrm{rs},\ \mathrm{v} = \mathrm{sr}$, **где** $\mathbb{N} \ni \mathrm{n} \geq 0,\ \mathrm{r}, \mathrm{s}$ **– словарные параметры.**

Определение. Пусть $\mathbf{z}, \mathbf{v} \in \mathcal{V}^*$. Слово $\mathbf{v}$ называется сопряженным слову $\mathbf{z}$, если существует $\mathbf{x} \in \mathcal{V}^*$ такое, что $\mathbf{x}\,\mathbf{z} = \mathbf{v}\,\mathbf{x}$.

Если моноид M одновременно является группой относительно операции в M, тогда отношение сопряженности в моноиде M есть групповое отношение сопряженности:

$$\mathbf{x}\,\mathbf{z} = \mathbf{v}\,\mathbf{x} \Leftrightarrow \mathbf{v} = \mathbf{x}\,\mathbf{z}\,\mathbf{x}^{-1}.$$

Множество решений уравнения сопряжения $\mathrm{x\,z = v\,x}$:
$\mathrm{x} = (\mathrm{sr})^{\mathrm{n}}\mathrm{s},\ \mathrm{z} = \mathrm{rs},\ \mathrm{v} = \mathrm{sr}$, где $\mathbb{N} \ni \mathrm{n} \geq 0,\ \mathrm{r}, \mathrm{s}$ – словарные параметры.

Следствие 1: Слово v сопряжено слову z тогда и только тогда, когда существует циклическая перестановка σ букв в слове z такая, что $\sigma(\mathrm{z}) = \mathrm{v}$.

Следствие 2: Отношение сопряженности в свободном моноиде является отношением эквивалентности.

Пусть дан алфавит $\mathcal{A}$. Определим множество $\mathcal{P}$ параметрических слов: (1) $\mathcal{A}^* \subset \mathcal{P}$; (2) если $\phi \in \mathcal{P}$, n – натуральный параметр, тогда $\phi^{\mathbf{n}} \in \mathcal{P}$; (3) если $\phi_1, \phi_2 \in \mathcal{P}$, тогда $\phi_1\phi_2 \in \mathcal{P}$.

Нас будут интересовать параметрические слова в алфавите $\Sigma \cup \mathcal{V}$.
Термы $\mathrm{p} \in \mathcal{V}$ будем называть словарными параметрами.

Пример параметрического слова:
$((\mathbf{s}\,\mathbf{A}\,\mathbf{r})^{\mathbf{n}}\,\mathbf{s})^{\mathbf{m}}\mathbf{s}^{\mathbf{n}}$**,**
где $\mathbb{N} \ni \mathrm{n}, \mathrm{m} \geq 0,\ \mathrm{r}, \mathrm{s}$ – параметры, принимающие значения в Σ^*.

Пусть дано уравнение в словах $\mathcal{E}$ от n переменных $\mathrm{x_1}, \ldots, \mathrm{x_n}$.

Определение. **n-ка парам. слов $(\phi_{\mathbf{1}}, \ldots, \phi_{\mathbf{n}})$ называется параметрическим подмножеством решений уравнения $\mathcal{E}$, если при любой подстановке σ конкретных значений параметров n-ка**

$$(\sigma(\phi_{\mathbf{1}}), \ldots, \sigma(\phi_{\mathbf{n}}))$$

есть решение уравнения $\mathcal{E}$.

Определение. **Множество решений уравнения $\mathcal{E}$ параметризуемо, если существует конечное множество $\mathcal{M}$ параметрических подмножеств решений уравнения $\mathcal{E}$ такое, что для каждого решения $(\overline{\mathrm{x_1}}, \ldots, \overline{\mathrm{x_n}})$ уравнения $\mathcal{E}$ $\exists \mathrm{M} \in \mathcal{M}$ и подстановка σ конкретных значений параметров в M такая, что**

$$\sigma(\mathrm{M}) = (\overline{\mathrm{x_1}}, \ldots, \overline{\mathrm{x_n}}).$$

Пусть дан алфавит $\mathcal{A}$.

Определим множество $\mathcal{P}$ параметрических слов: (1) $\mathcal{A}^* \subset \mathcal{P}$; (2) если $\phi \in \mathcal{P}$, $\mathbf{n}$ – натуральный параметр, тогда $\phi^{\mathbf{n}} \in \mathcal{P}$; (3) если $\phi_1, \phi_2 \in \mathcal{P}$, тогда $\phi_1\phi_2 \in \mathcal{P}$.

Нас будут интересовать параметрические слова в алфавите $\Sigma \cup \mathcal{V}$. Термы $\mathbf{p} \in \mathcal{V}$ будем называть словарными параметрами.

Пример:

Множество решений уравнения сопряжения $\mathbf{x}\,\mathbf{z} = \mathbf{v}\,\mathbf{x}$ параметризуемо:

$\mathbf{x} = (\mathbf{s}\,\mathbf{r})^{\mathbf{n}}\mathbf{s}$, $\mathbf{z} = \mathbf{r}\,\mathbf{s}$, $\mathbf{v} = \mathbf{s}\,\mathbf{r}$,

где $\mathbb{N} \ni \mathbf{n} \geq 0$, $\mathbf{r}, \mathbf{s}$ – параметры, принимающие значения в Σ^*.

Лемма $\aleph$. **Для всякого бескоэффициентного уравнения в словах $\Phi = \Psi$ в свободном моноиде с не менее чем двумя образующими и любого его параметрического решения ξ результат подстановки σ натуральным параметрам любых конкретных значений из $\mathbb{N}_0$ – $\sigma(\xi)$ – является решением уравнения $\Phi = \Psi$.**

Доказательство:

Почти очевидно. $\square$

Две теоремы Ю.И. Хмелевского

Теорема 1. (Хмелевский)
Множество решений любого бескоэффициентные уравнения с тремя переменными параметризуемо.

Теорема 2. (Хмелевский)
Множество решений бескоэффициентного уравнения $\mathrm{x\,y\,z} = \mathrm{z\,v\,x}$ в свободном моноиде с не менее чем двумя образующими непараметризуемо.

Слова Фибоначчи

Определение. Словами Фибоначчи называются элементы последовательности $\{\mathbf{w_n}\}$ слов такой, что

$$\begin{aligned}
&\mathbf{w_0} = \mathbf{A},\\
&\mathbf{w_1} = \mathbf{B},\\
&\mathbf{w_{n+2}} = \mathbf{w_{n+1}}\,\mathbf{w_n}.
\end{aligned}$$

Свойство 1. $\forall \mathbf{n} > 0.\ \mathbf{f_n} = |\mathbf{w_n}|$, где $\mathbf{f_n}$ — $\mathbf{n}$-ое число Фибоначчи.

Слова Фибоначчи

Обозначим $\mathrm{pref_n(w)}, \mathrm{suf_n(w)}$ **префикс и суфикс длины** n **слова** w**, соответственно.**

Свойство 2. **Для всех** $\mathrm{n} \geq 2$

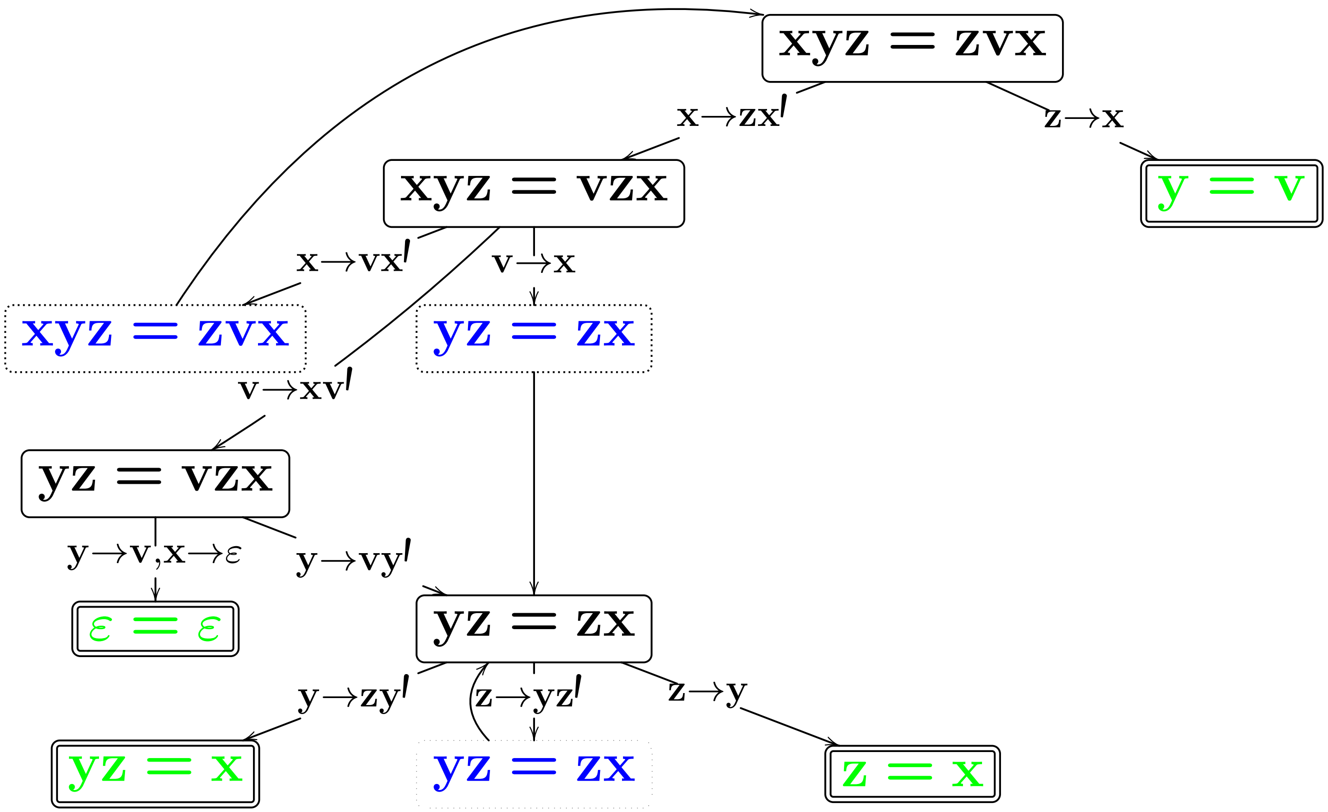
$$\mathrm{suf_2(w_n)} = \begin{cases} \mathrm{B\,A}, \text{если } \mathrm{n} \text{ чётное;} \\ \mathrm{A\,B}, \text{если } \mathrm{n} \text{ нечётное.} \end{cases}$$

Свойство 3.
$\forall \mathrm{n} \in \mathbb{N}, \mathrm{u} \in \Sigma, \mathrm{u} \neq \epsilon$ **слово** u^4 **не является подсловом слова** $\mathrm{w_n}$**.**

Утверждение 1. $\mathrm{x\,y\,z = z\,v\,x} \quad \Rightarrow \quad \mathrm{y = v}$ **или** $\mathrm{Alpha(x\,z) \subseteq Alpha(y\,v)}$.

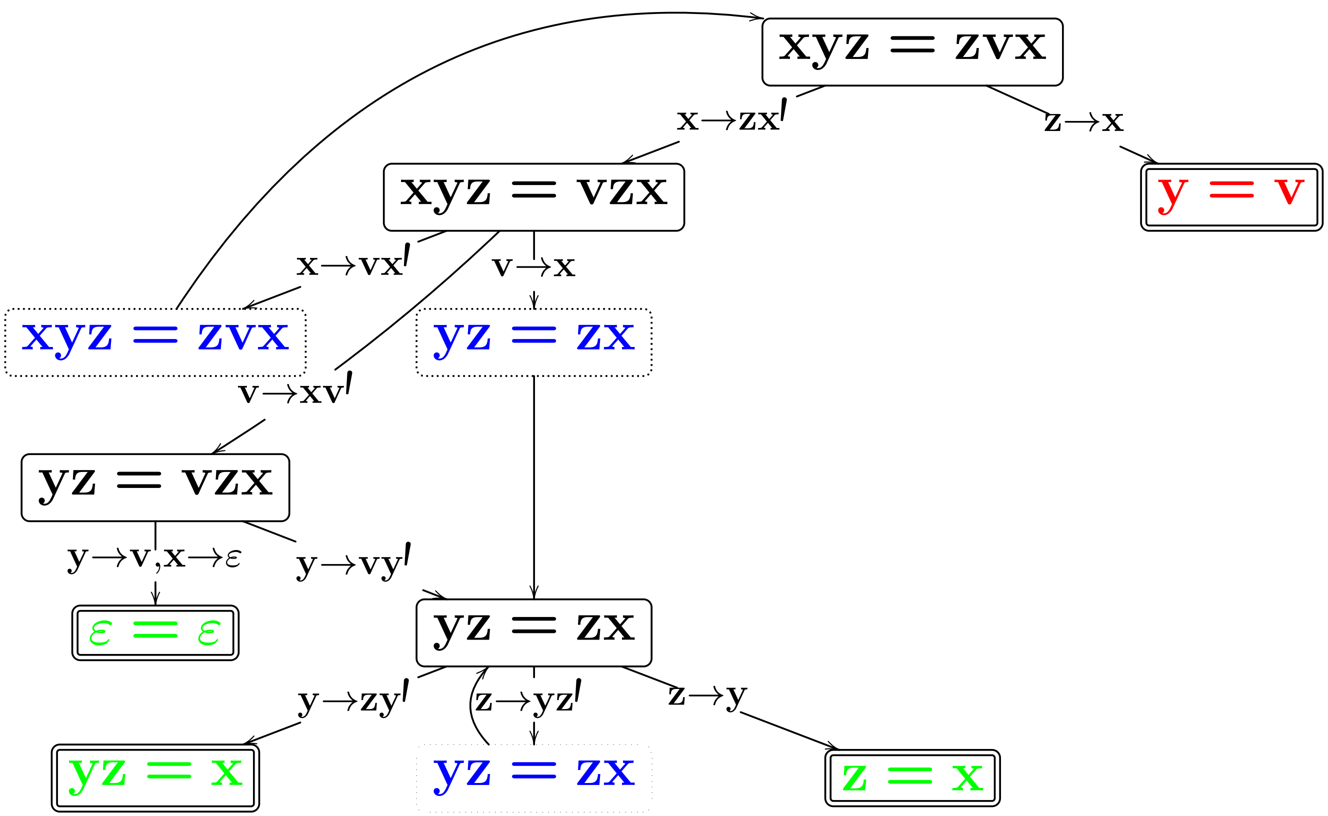
Доказательство Утв. 1.

Из симметрии уравнения можно предполагать, что $|\mathrm{x}| \geq |\mathrm{z}|$.



Утверждение 1. $x\,y\,z = z\,v\,x \quad \Rightarrow \quad y = v$ **или** $\mathrm{Alpha}(x\,z) \subseteq \mathrm{Alpha}(y\,v)$.

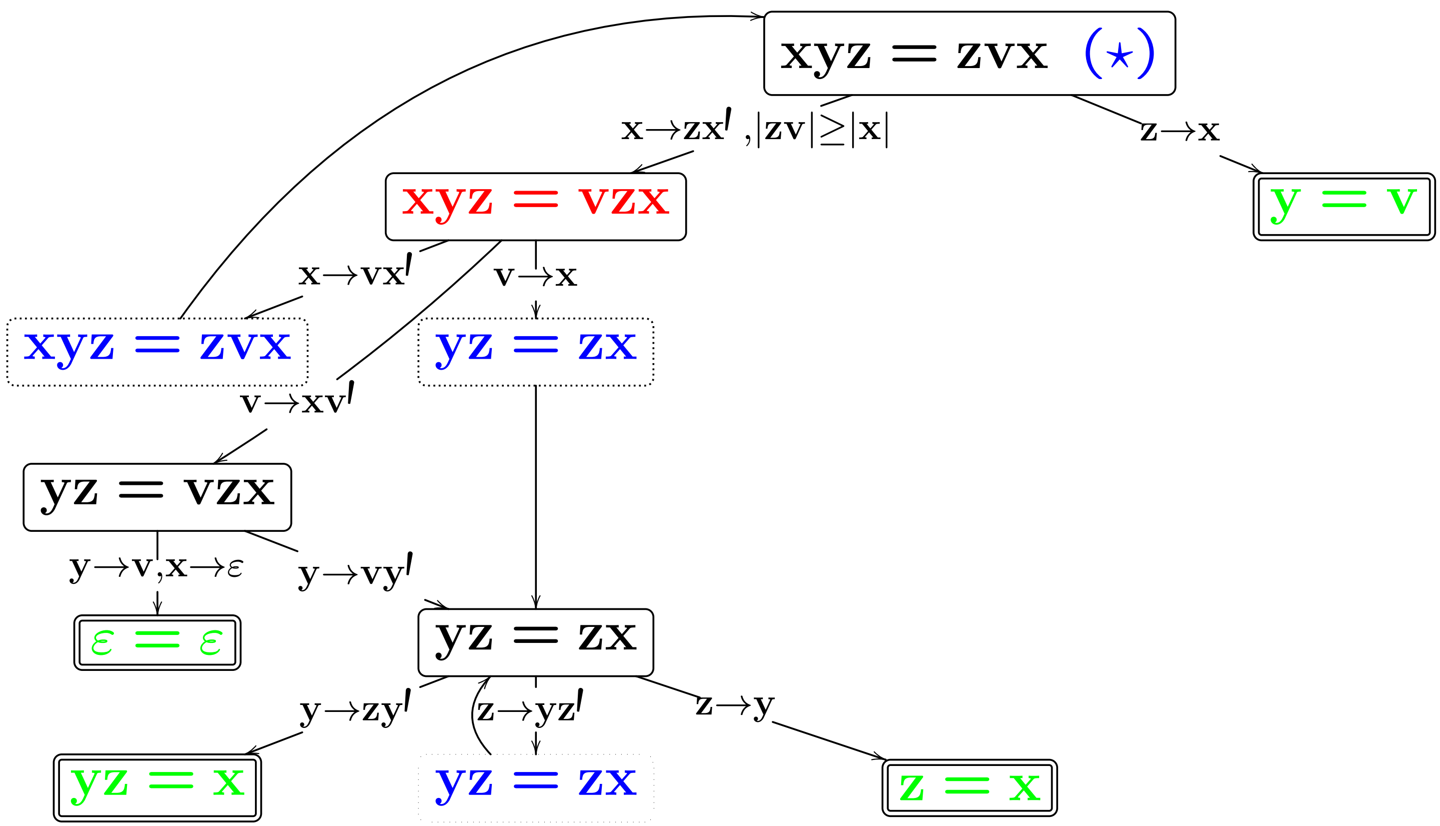
Доказательство Утв. 1.



Выделенный случай **тривиален.** $\boxdot$

Утверждение 1. $x\,y\,z = z\,v\,x \quad \Rightarrow \quad y = v$ **или** $\mathrm{Alpha}(x\,z) \subseteq \mathrm{Alpha}(y\,v)$.

Доказательство Утв. 1. (II)



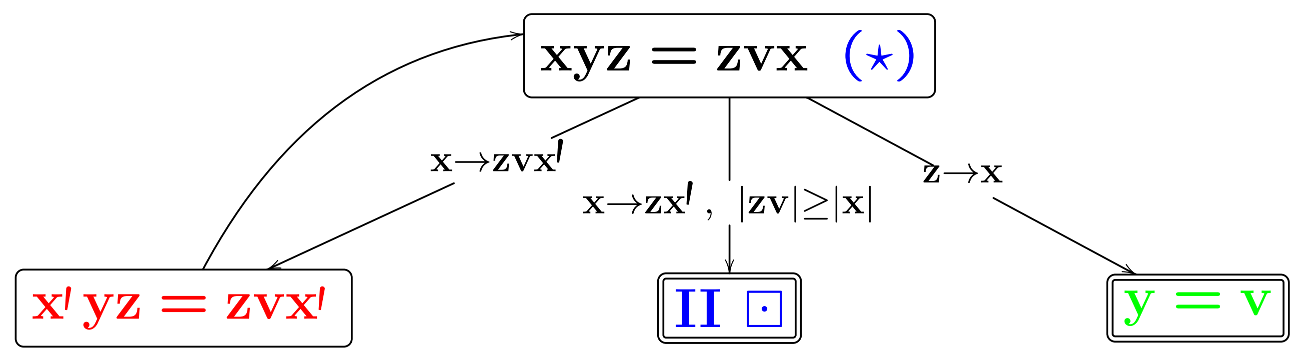
Здесь: $X = Z\,Q' = P'\,Z \Rightarrow Z = (s\,r)^n s,\ Q' = r\,s,\ P' = s\,r,\ X = (s\,r)^{n+1} s$, **где** $s, r \in \Delta^*,\ P, Q \in \Delta^+$.

Из уравнения $(\star)$ **имеем:** Q' **есть начало** V, P' **– конец** Y.

Если $\gamma \in \mathrm{Alpha}(X\,Z) \subseteq \Delta$, **то** $|sr|_\gamma > 0 \Rightarrow (\gamma \in \mathrm{Alpha}(Y\,V))$. $\boxdot$

Утверждение 1. $\mathbf{x\,y\,z = z\,v\,x \quad \Rightarrow \quad y = v}$ **или** $\mathbf{Alpha(x\,z) \subseteq Alpha(y\,v)}$.

Доказательство Утв. 1. (III)



Здесь: Либо $\mathbf{(Z\,V = \epsilon) \Rightarrow Y = \epsilon}$**, либо** $\mathbf{|X'| < |X|}$.
Индукция по длине $\mathbf{|X|}$.
Шаг индукции: так как $\mathbf{X = Z\,V\,X'}$**, то**
$\mathbf{(Alpha(X'\,Z) \subseteq Alpha(Y\,V)) \Rightarrow (Alpha(X\,Z) \subseteq Alpha(Y\,V))}$.
Базис индукции: доказан в случаях $\mathbf{(I)}$, $\mathbf{(II)}$. $\boxdot$

Теорема 2. (Хмелевский)
Множество решений бескоэффициентного уравнения $x\,y\,z = z\,v\,x$ в свободном моноиде с не менее чем двумя образующими непараметризуемо.

Идея доказательства Чейзлер (E. Czeizler, 2005).

Предположим обратное: Тогда,

- либо длины всех 4-х коорд. проекций T_i парам. решения уравнения, т.е. над алфавитом Δ, равномерно ограничены;
- либо $\exists T_i.\ \forall N_0 \in \mathbb{N}.\, \exists(u \in T_i, h \in \Delta^+, u_1, u_2 \in \Delta^*, n > N_0)$ такие, что $u = u_1\, h^n\, u_2$.

С другой стороны, построим бесконечную последовательность решений, компоненты которых – подслова слов Фибоначчи, и коорд. проекции этой последовательности не содержат четвертых степеней непустых подслов.

Получили противоречие. $\square$

Теорема 2. (Хмелевский)
Множество решений бескоэффициентного уравнения

$$\mathrm{x\,y\,z} = \mathrm{z\,v\,x} \qquad (\star)$$

в свободном моноиде с не менее чем двумя образующими непараметризуемо.

Доказательство Чейзлер (E. Czeizler, 2005).

Предположим обратное: $\exists$ конечное число 4-ок парам. слов $(\mathrm{T}_1, \mathrm{T}_2, \mathrm{T}_3, \mathrm{T}_4)$, параметризующих множество корней $(\mathrm{x}, \mathrm{y}, \mathrm{z}, \mathrm{v})$ уравнения $(\star)$.

$\mathrm{K} \triangleq (\mathrm{K}_1, \mathrm{K}_2, \mathrm{K}_3, \mathrm{K}_4)$ – одна из таких 4-ок, Δ и Λ суть алфавиты словарных и натуральных параметров 4-ки K, соответственно. $\sigma(\mathrm{K}) = \Pi \triangleq (\mathrm{X}, \mathrm{Y}, \mathrm{Z}, \mathrm{V})$ – результат постановки σ некоторых конкретных значений натуральных параметров.

По Лемме-$\aleph$ Π есть корень уравнения $\mathrm{x\,y\,z} = \mathrm{z\,v\,x}$ $(\star)$ над алфавитом Δ. Следовательно, $|\mathrm{Y}|_\Delta = |\mathrm{V}|_\Delta$.

Пусть $G_n \triangleq \mathrm{pref}_{f_{n-2}}(w_n)$ **для всех** $n \geq 2$.

Свойство: $\forall n = 2k \geq 4.\ w_{n-2}G_{n-1} = G_n$.
Доказательство: Индукция по k. $\boxdot$

Пример:
$$w_0 = A,\ w_1 = B,\ w_2 = B\,A,\ w_3 = B\,A\,B,\ w_4 = B\,A\,B\,B\,A, \dots$$
$$G_2 = \epsilon, \quad G_3 = B, \quad G_4 = B\,A\,B, \dots$$

Свойство 2. Для всех $k \geq 1$ $\mathrm{suf}_2(w_{2k}) = B\,A,\ \mathrm{suf}_2(w_{2k+1}) = A\,B$.

Докажем, что $\forall n = 2k, k > 1.\ (X, Y, Z, V) \triangleq (G_n, B\,A, G_{n-1}, A\,B)$ **корень уравнения Хмелевского** $x\,y\,z = z\,v\,x$ **над алфавитом** Σ.

Нужно доказать: $\forall n = 2k, k > 1.\ G_n\,B\,A\,G_{n-1} = G_{n-1}\,A\,B\,G_n$.

$\mathrm{pref}_{f_{n-2}}(w_n)\,B\,A\,G_{n-1} = \mathrm{pref}_{f_{n-1}-2}(w_{n-1})\,A\,B\,G_n$ – по определению G_n
$w_n\,G_{n-1} = w_{n-1}\,G_n$ – Свойство 2
$w_{n-1}\,w_{n-2}\,G_{n-1} = w_{n-1}\,G_n$
$w_{n-2}\,G_{n-1} = G_n$ $\boxdot$

По предположению, множество решений уравнения Хмелевского

$$\mathbf{x\,y\,z = z\,v\,x}$$

параметризуемо.

$\Rightarrow$

$\forall \mathbf{n} = 2\mathbf{k} \geq 4$ **существуют параметрическое решение**

$$\mathbf{K_n} \triangleq (\mathbf{K_{1,n}}, \mathbf{K_{2,n}}, \mathbf{K_{3,n}}, \mathbf{K_{4,n}})$$

и подстановка $\sigma_{\mathbf{n}}$ конкретных значений натуральных параметров такая, что

$$\sigma_{\mathbf{n}}(\mathbf{K_n}) = (\mathbf{G_n},\ \mathbf{B\,A},\ \mathbf{G_{n-1}},\ \mathbf{A\,B}).$$

$\sigma_{\mathbf{n}}(\mathbf{K_n}) = (\mathbf{G_n}, \mathbf{B\,A}, \mathbf{G_{n-1}}, \mathbf{A\,B})$

Докажем, что длина $|\sigma(\mathbf{K_1})| = |\mathbf{G_n}|$ равномерно ограничена по $\mathbf{n}$.

1. $\sigma_{\mathbf{n}}(\mathbf{K_{1,n}}) = \mathbf{G_n}$ **есть префикс $\mathbf{w_n}$, который не содержит подслов вида $\mathbf{u}^4 \neq \epsilon \Rightarrow$ для каждого натурального нат. параметра $\mathbf{m}$ в $\mathbf{K_{1,n}}$ имеем $\sigma_{\mathbf{n}}(\mathbf{m}) < 4$.** **– Свойство 2.**

2. $\sigma_{\mathbf{n}}(\mathbf{K_{2,n}}) = \mathbf{B\,A},\ \sigma_{\mathbf{n}}(\mathbf{K_{4,n}}) = \mathbf{A\,B} \Rightarrow \sigma_{\mathbf{n}}(\mathbf{K_{2,n}}) \neq \sigma_{\mathbf{n}}(\mathbf{K_{4,n}})$
   $\Rightarrow \mathbf{Alpha}(\sigma_{\mathbf{n}}(\mathbf{K_{1,n}})\,\sigma_{\mathbf{n}}(\mathbf{K_{3,n}})) \subset \mathbf{Alpha}(\sigma_{\mathbf{n}}(\mathbf{K_{2,n}})\,\sigma_{\mathbf{n}}(\mathbf{K_{4,n}}))$ **– Утв. 1.**
   Число параметров $|\sigma_{\mathbf{n}}(\mathbf{K_{2,n}})|_\Delta = |\mathbf{B\,A}|_\Delta = |\sigma_{\mathbf{n}}(\mathbf{K_{4,n}})|_\Delta = |\mathbf{A\,B}|_\Delta \leq \mathbf{2}$
   $\Rightarrow |\mathbf{Alpha}(\sigma_{\mathbf{n}}(\mathbf{K_{1,n}})\,\sigma_{\mathbf{n}}(\mathbf{K_{3,n}}))| \leq \mathbf{2} \Rightarrow |\mathbf{Alpha}(\mathbf{K_{1,n}}\,\mathbf{K_{3,n}})| \leq \mathbf{2}$
   $\Rightarrow \exists \mathbf{Const}\,\forall \mathbf{n}.|\mathbf{K_{1,n}}| = |\mathbf{G_n}| \leq \mathbf{Const}$

$\boxdot$

Что противоречит неограниченному росту длин слов Фибоначчи.

Полученное противоречие доказывает Теорему Хмелевского 2.

$\square$