

Структуры над словами: уравнения

Летняя практика, Переславль-Залесский
3–7 июля, 2023 г.



Уравнения в словах. Определения

Даны алфавит констант Σ (здесь рассматриваем константные скобочные структуры типа $('A' ('B'))$ в роли констант), алфавит строковых и буквенных переменных V .

Уравнение в словах — равенство вида $\Psi = \Phi$, где $\Psi, \Phi \in \{\Sigma \cup V\}^*$.

Решить уравнение в словах — найти все такие подстановки σ переменных, входящих в $\Psi \Phi$, что $\Psi\sigma = \Phi\sigma$.

Проблема существования корней уравнений в словах разрешима (Маканин). Множество решений уравнения в общем виде представляется графом сложной структуры.

Уравнение $\Psi = \Phi$ квадратичное, если ни одна переменная из V типа строка не входит в $\Psi = \Phi$ более, чем дважды.



Преобразование Нильсена

Лемма Леви

Если уравнение в словах имеет вид $x \Phi_1 = y \Phi_2$, тогда выполнено хотя бы одно из условий $x = y x' \vee y = x y'$ (возможно, для разных решений выполнены разные условия).

Рассмотрим произвольное решение уравнения, описываемое подстановкой σ . Если $|x\sigma| \geq |y\sigma|$, то $x = y x'$, в противном случае $|y\sigma| \geq |x\sigma|$ (даже строго больше), поэтому $y = x y'$.

Ветвление по подстановкам вида $x \mapsto y x'$ и $y \mapsto x y'$ называется преобразованием Нильсена. Оно может применяться как слева (по умолчанию), так и справа.



Системы уравнений

Пусть в Σ есть хотя бы две буквы. По каждой системе

$$\begin{aligned}\Phi_1 &= \Psi_1 \\ \Phi_2 &= \Psi_2\end{aligned}\tag{1}$$

можно построить уравнение, имеющее те же самые корни:

$$\Phi_1 \mathbf{A} \Phi_2 \Phi_1 \mathbf{B} \Phi_2 = \Psi_1 \mathbf{A} \Psi_2 \Psi_1 \mathbf{B} \Psi_2\tag{2}$$

Заметим, что $|\Phi_1 \mathbf{A} \Phi_2| = |\Phi_1 \mathbf{B} \Phi_2|$, и $|\Psi_1 \mathbf{A} \Psi_2| = |\Psi_1 \mathbf{B} \Psi_2|$.

Поэтому уравнение (2) эквивалентно системе:

$$\Phi_1 \mathbf{A} \Phi_2 = \Psi_1 \mathbf{A} \Psi_2 \text{ и } \Phi_1 \mathbf{B} \Phi_2 = \Psi_1 \mathbf{B} \Psi_2.$$

Предположим, что есть решение этой системы, определяемое подстановкой σ . Поскольку σ сохраняет константы, получаем

$$(\Phi_1 \sigma) \mathbf{A} (\Phi_2 \sigma) = (\Psi_1 \sigma) \mathbf{A} (\Psi_2 \sigma),$$

$$(\Phi_1 \sigma) \mathbf{B} (\Phi_2 \sigma) = (\Psi_1 \sigma) \mathbf{B} (\Psi_2 \sigma).$$



Системы уравнений

Пусть в Σ есть хотя бы две буквы. По каждой системе

$$\begin{aligned}\Phi_1 &= \Psi_1 \\ \Phi_2 &= \Psi_2\end{aligned}\tag{1}$$

можно построить уравнение, имеющее те же самые корни:

$$\Phi_1 \mathbf{A} \Phi_2 \Phi_1 \mathbf{B} \Phi_2 = \Psi_1 \mathbf{A} \Psi_2 \Psi_1 \mathbf{B} \Psi_2\tag{2}$$

Уравнение (2) эквивалентно системе:

$$\Phi_1 \mathbf{A} \Phi_2 = \Psi_1 \mathbf{A} \Psi_2 \text{ и } \Phi_1 \mathbf{B} \Phi_2 = \Psi_1 \mathbf{B} \Psi_2.$$

Предположим, что есть решение этой системы, определяемое подстановкой σ . Поскольку σ сохраняет константы, получаем

$$(\Phi_1\sigma) \mathbf{A} (\Phi_2\sigma) = (\Psi_1\sigma) \mathbf{A} (\Psi_2\sigma),$$

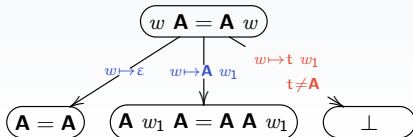
$$(\Phi_1\sigma) \mathbf{B} (\Phi_2\sigma) = (\Psi_1\sigma) \mathbf{B} (\Psi_2\sigma). \text{ Пусть } \Phi_1\sigma = (\Psi_1\sigma) \mathbf{A} \Theta, \text{ тогда}$$

$$\mathbf{A} \Theta \mathbf{B} (\Phi_2\sigma) = \mathbf{B} (\Psi_2\sigma), \text{ что невозможно. Аналогично, если}$$

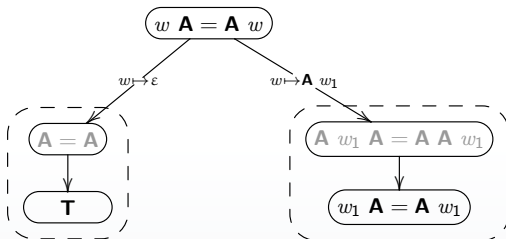
$\Psi_1\sigma = (\Phi_1\sigma) \mathbf{A} \Theta$. Поэтому $\Phi_1\sigma = \Psi_1\sigma$ и $\Phi_2\sigma = \Psi_2\sigma$, значит, σ — решение исходной системы (1).



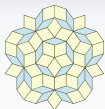
Дерево решения уравнения



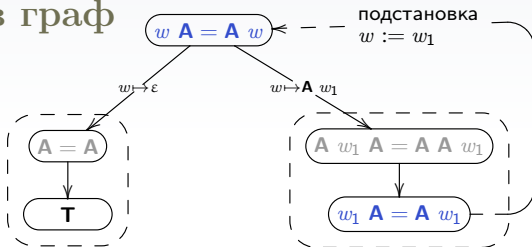
Если значение переменной w не пусто, то начинается с \mathbf{A} , либо уравнение не выполняется.



После подстановок $w \mapsto \varepsilon$, $w \mapsto \mathbf{A} w_1$ равные термы слева и справа сокращаются. Ветви дерева, приводящие к противоречию, отбрасываются.



Свёртка дерева решения уравнения в граф



Уравнение $w_1 \mathbf{A} = \mathbf{A} w_1$ повторяет исходное с точностью до переименования w_1 в w . Его развёртка происходит точно так же, поэтому можно просто сослаться на узел с исходным уравнением.

Построен граф описания корней уравнения $w \mathbf{A} = \mathbf{A} w$. Наличие в нем листьев, содержащих \mathbf{T} , свидетельствует о существовании корней уравнения. Множество корней: $w \in \mathbf{A}^*$.



Метод Матиясевича

Дано уравнение в словах $\Phi_1^0 = \Phi_2^0$, $\Phi_i \in \{\Sigma \cup V\}^*$. Помещаем это уравнение в корень дерева.

Правила развертки узла с уравнением $t_1 \Phi_1 = t_2 \Phi_2$:

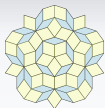
- Пусть $t_1 = t_2$. Заменяем уравнение в узле на $\Phi_1 = \Phi_2$.
- Уравнение $\Psi_1 = \Psi_2$, где $\Psi_i \in \{V_e\}^*$, $\Psi_j = \varepsilon$, $i \neq j$, объявляем листом и помечаем **T**.
- Пусть $t_i = t$ (буквенная переменная), $t_j = \mathbf{A}$. Строим потомок $\Phi_1 \sigma = \Phi_2 \sigma$, где $t \sigma = \mathbf{A}$, а для остальных $v \in V$ $v \sigma = v$. Аналогично для $t_j = t'$.
- Пусть $t_i = x$, $t_j = (\mathbf{A} | t)$ (буква или буквенная переменная). Строим два потомка, соответствующих подстановкам $x \sigma_1 = \varepsilon$, $x \sigma_2 = (\mathbf{A} | t) x$.
- Пусть $t_i = x$, $t_j = y$. Строим потомки по подстановкам $x \sigma_1 = y x$, $x \sigma_2 = x y$, $x \sigma_3 = y$.
- Если уравнение в текущем узле повторяет уравнение в узле-предке, строим обратное ребро в графе.



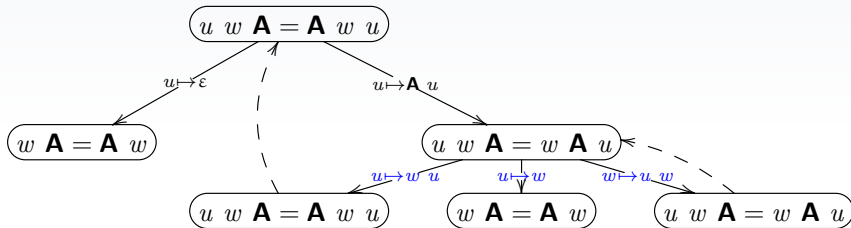
Соглашение об именах

При построении подстановок согласно преобразованию Нильсена (вида $x \mapsto ux'$) обычно за суффиксом x' закрепляется имя x . Например, в методе Матиясевича (см. ниже) таким образом удаётся избавиться от необходимости искать переименовки, чтобы факторизовать пути развёртки уравнений.

- Плюсы: дешёвое сравнение меток узлов, сохранение информации о том, суффикс какой исходной переменной рассматривается.
- Минус: иногда свёртка по переименовке (а не по точному совпадению) позволяет получить намного более короткое описание решений.

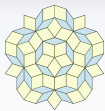


Поиск конкретных решений

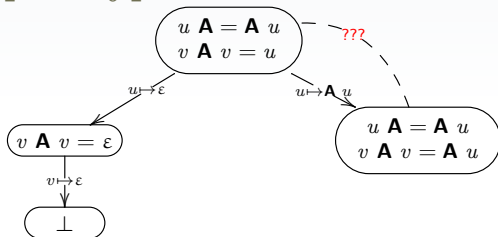


$u = \mathbf{A}$, $w = \mathbf{B}$ — решение уравнения $u w \mathbf{A} = \mathbf{A} w u$.

Этому решению не соответствует никакого пути в графе развёртки, оканчивающегося узлом **T**. Причина — в нулевом индуктивном переходе $w \mapsto \varepsilon w$ (после отцепления от u буквы \mathbf{A}), соответствующем переходу в цикл по ветви $w \mapsto u w$. Для того, чтобы получить корректное описание решений, в метод Матиясевича нужно добавить выходы по $u \mapsto \varepsilon$, $w \mapsto \varepsilon$.



Нетривиальность совместной развёртки уравнений



Как только в системе появляется переменная, встречающаяся больше двух раз по совокупности, алгоритм построения графа развёртки перестаёт работать, потому что появляется возможность бесконечного разрастания уравнений.

Для квадратичных уравнений алгоритм Матиясевича является разрешающим (всегда завершается и даёт точный ответ о существовании корней).



Сложность задачи

Длина минимального решения уравнения:

$$x_n \mathbf{A} x_n \mathbf{B} x_{n-1} \mathbf{B} x_{n-2} \dots \mathbf{B} x_1 = \mathbf{A} x_n x_{n-1}^2 \mathbf{B} x_{n-2}^2 \mathbf{B} \dots \mathbf{B} x_1^2 \mathbf{B} \mathbf{A}^2$$

экспоненциальна по n .



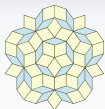
Специальные уравнения

- Уравнения сопряжённости слов Φ_1 и Φ_2 :
 $\Phi_1 \Phi_2 x = x \Phi_2 \Phi_1$, где $\Phi_i \in \Sigma^*$. Они имеют решения вида $q^n \Phi_1$, где q — это корень слова $\Phi_1 \Phi_2$ (в том числе если $\Phi_1 \Phi_2$ простое, то $q = \Phi_1 \Phi_2$).
Например, рассмотрим **АВАВ** $x = x$ **ВАВА**. Здесь $\Phi_1 = \mathbf{A}$, $\Phi_2 = \mathbf{BAV}$. $(\Phi_1 \Phi_2)^n \Phi_1$ — это **(АВАВ)ⁿ А**, однако очевидно, что при таком описании теряется, например, корень **АВА**. Правильный ответ здесь: **(АВ)ⁿ А**.
- Уравнения сопряжённости общего вида: $xw = wy$. Их решения описываются в параметрах: $x = z_1 z_2$, $y = z_2 z_1$, $w = (z_1 z_2)^n z_1$. Видно, что это просто обобщение предыдущего класса уравнений.



Хорошие классы уравнений

- Уравнения от одной переменной. Разрешимы за линейное время.
- Квадратичные уравнения (каждая переменная имеет не больше чем 2 вхождения в обе части). Сложность решения: NP-трудна.
- Straight-line (прямолинейные) уравнения. Кратность (относительно всего уравнения) всех переменных хотя бы в одной части уравнения равна 1.
- Уравнения, сводящиеся к системе, где одно уравнение принадлежит классу выше, а остальные — уравнения вида $x_i \Phi_i = \Psi_i x_i$, где Φ_i, Ψ_i — константы (см. ниже).



Преобразование Нильсена и прямолинейные уравнения

Граф развёртки прямолинейного уравнения посредством преобразования Нильсена конечен.

Напомним, что (строгий) порядок \triangleleft на n -ках называют лексикографическим, если $\langle \alpha_1, \dots, \alpha_n \rangle \triangleleft \langle \beta_1, \dots, \beta_n \rangle \Leftrightarrow \exists j (\forall i (i < j \Rightarrow \alpha_i = \beta_i) \ \& \ \alpha_j < \beta_j)$.

Пусть $\Phi = \Psi$ — прямолинейное уравнение с правой частью, линейной относительно уравнения. Введём на уравнениях следующий лексикографический порядок:

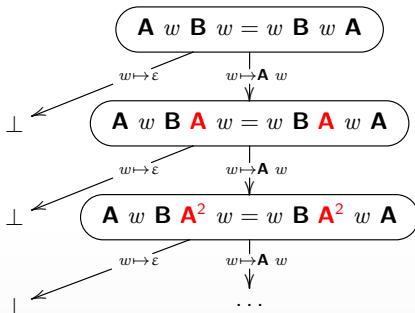
$$\langle \Phi_1 = \Psi_1 \rangle \prec \langle \Phi_2 = \Psi_2 \rangle \Leftrightarrow \langle |\Psi_1|, |\Phi_1| \rangle <_{\text{LEX}} \langle |\Psi_2|, |\Phi_2| \rangle$$

Тогда любая подстановка (с последующим сокращением равных префиксов) будет строго уменьшать уравнение относительно порядка \prec .



Эвристики: разрезание

При непосредственном применении преобразования Нильсена уравнение $\mathbf{A} w \mathbf{B} w = w \mathbf{B} w \mathbf{A}$ уходит в бесконечную развёртку, из-за наличия более чем двух вхождений w .



Однако можно заметить, что это левая и правая части уравнения разбиваются на префиксы и суффиксы одинаковой длины: $\mathbf{A} w \mathbf{B} w = w \mathbf{B} w \mathbf{A}$

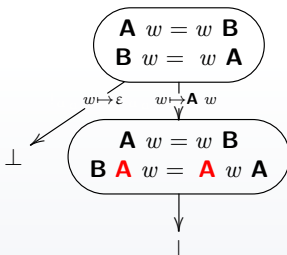


Эвристики: разрезание

При непосредственном применении преобразования Нильсена уравнение $\mathbf{A} w \mathbf{B} w = w \mathbf{B} w \mathbf{A}$ уходит в бесконечную развёртку, из-за наличия более чем двух вхождений w .

Однако можно заметить, что это левая и правая части уравнения разбиваются на префиксы и суффиксы одинаковой длины: $\mathbf{A} w \mathbf{B} w = w \mathbf{B} w \mathbf{A}$

После разбиения на систему более простых уравнений, противоречивость доказывается за один шаг развёртки.





Эвристики: разрезание

Скажем, что уравнение $\Phi = \Psi$ содержит равносоставленные префиксы, если у него существует представление $\Phi_1\Phi_2 = \Psi_1\Psi_2$ такое, что:

- совокупное число всех констант в Φ_1 и Ψ_1 одинаково.

Формально:
$$\sum_{\gamma_i \in \Sigma} |\Phi_1|_{\gamma_i} = \sum_{\gamma_i \in \Sigma} |\Psi_1|_{\gamma_i}$$

- кратности всех переменных в Φ_1 и Ψ_1 совпадают.

Формально: $\forall w \in V(|\Phi_1|_w = |\Psi_1|_w)$.

Аналогичное понятие имеет смысл и для суффиксов.



Безопасность эвристики разрезания

Можно показать, что переход от уравнения $\Phi_1\Phi_2 = \Psi_1\Psi_2$ к системе равносоставленных:

$$\begin{cases} \Phi_1 = \Psi_1 \\ \Phi_2 = \Psi_2 \end{cases} \quad (3)$$

безопасен в смысле завершаемости развёртки.

Если развёртка посредством преобразования Нильсена уравнения $\Phi_1\Phi_2 = \Psi_1\Psi_2$, где Φ_1 и Ψ_1 равносоставленны, завершается, то завершается и развёртка системы (3).

Действительно, совокупная длина системы (3) после любой последовательности подстановок будет не больше, чем длина уравнения. Она может оказаться меньше, поскольку сокращения равных префиксов возможны не только в префиксах Φ_1 и Ψ_1 , но и «из середины»: в Φ_2 и Ψ_2 .



Эвристики: применение подсчёта

- Уравнение вида $w u u = u \mathbf{A} u w v$ не поддаётся эвристике разрезания из-за вхождения v в конец правой части, блокирующего появление равносоставленных суффиксов. Однако видно, что это уравнение несовместно, поскольку совокупная длина подстановок в его правую часть всегда больше, чем в левую. Формально, если отображать все значения переменных в длины, а буквы — в 1, получим несовместное уравнение:

$$|w| + 2 \cdot |u| < |w| + 2 \cdot |u| + |v| + 1$$

- Образ уравнения $u u \mathbf{A} u = w \mathbf{A} \mathbf{A} w w$ при вычислении длин совместен в \mathbb{R} (и в \mathbb{Q}):

$$3 \cdot |u| + 1 \stackrel{?}{=} 3 \cdot |w| + 2$$

Однако решений в \mathbb{N} (подразумевается, что $0 \in \mathbb{N}$) не существует, что опровергает существование решения у исходного уравнения в словах.



Эвристики: применение подсчёта

- Образы частей уравнения u и $\mathbf{A}w = w$ и $\mathbf{B}u$ по длинам совпадают. Но при подсчёте только вхождений букв \mathbf{A} в части уравнений опять возникает противоречие:

$$|w|_{\mathbf{A}} + 2 \cdot |u|_{\mathbf{A}} + 1 > |w|_{\mathbf{A}} + 2 \cdot |u|_{\mathbf{A}}$$

- Похожую эвристику можно применить и к уравнению $\mathbf{ABC}w\mathbf{C}u\mathbf{C}u = u\mathbf{C}u\mathbf{C}w\mathbf{CBA}$, если считать не отдельные буквы (их количество будет совпадать, а *подслова* \mathbf{AB}):

$$|w|_{\mathbf{AB}} + 2 \cdot |u|_{\mathbf{AB}} + 1 > |w|_{\mathbf{AB}} + 2 \cdot |u|_{\mathbf{AB}}$$

Действительно, все возможные вхождения \mathbf{AB} в части уравнения либо целиком лежат внутри значений w и u , либо явны, поскольку все вхождения переменных в уравнение отделены от соседних термов буквами \mathbf{C} . Очевидно, возможны иные случаи.



Эвристики: применение подсчёта

Действительно, рассмотрим то же уравнение без разделителей
C: $\mathbf{AB}wuu = uuw\mathbf{BA}$. Формальное отображение $x \mapsto |x|_{\mathbf{AB}}$,
 $\mathbf{AB} \mapsto 1$, $\mathbf{BA} \mapsto 0$, аналогичное сделанному ранее, приведёт к
противоречию. Однако уравнение совместно, если положить
 $w \mapsto \mathbf{A}$, $u \mapsto \varepsilon$.

Посмотрим теперь на результат подстановки внимательно:

$$\mathbf{AB} \mathbf{A} = \mathbf{A} \mathbf{BA}$$

Красным фоном выделены вхождения букв в значение w ,
синим — явные вхождения в уравнение; красным цветом
шрифта выделены искомые вхождения подстроки \mathbf{AB} . Видно,
что прямой подсчёт был ошибочным из-за перекрёстного
вхождения \mathbf{AB} : первая его буква принадлежала значению w ,
вторая — множеству констант уравнения.



Эвристики: применение подсчёта

Скажем, что $\gamma_1\gamma_2$ ($\gamma_1 \neq \gamma_2$) может иметь перекрёстное вхождение в решение уравнения $\Phi_1 = \Phi_2$, если:

- в Φ_1 или в Φ_2 есть вхождения двух переменных (возможно, различных) подряд;
- или в Φ_i какая-то из переменных соседствует с γ_2 слева;
- или в Φ_i какая-то из переменных соседствует с γ_1 справа.

Если все три условия насчёт $\Phi_1 = \Phi_2$ ложны, то к нему можно применять эвристику оценки числа пар $\gamma_1\gamma_2$ посредством простого подсчёта.

Случай $\gamma_1 = \gamma_2$ создаёт дополнительную сложность: при нём могут перекрываться и явные вхождения $\gamma_1\gamma_1$ в уравнение.



Задача на однозначность

Какие слова сопоставляются с образцом $x_1 x_2 x_2 x_1$ неоднозначно?

Решим уравнение неоднозначности: $x_1 x_2 x_2 x_1 = z_1 z_2 z_2 z_1$.
Заметим, что это уравнение эквивалентно системе

$$\begin{cases} x_1 x_2 = z_1 z_2 \\ x_2 x_1 = z_2 z_1 \end{cases} \quad (4)$$

Допустив, что $|x_1| > |z_1|$, применим двухстороннюю лемму Леви:

$$\begin{cases} x_1 = z_1 x_{1,s} \\ x_1 = x_{1,p} z_1 \end{cases} \quad (5)$$

Значит,

$x_{1,s} = u v$, $x_{1,p} = v u$, $z_1 = (v u)^n v$. Тогда $x_1 = (v u)^{n+1} v$. При этом полагаем $(v u)$ простым словом.



Задача на однозначность

Какие слова сопоставляются с образцом $x_1 x_2 x_2 x_1$ неоднозначно?

Решим уравнение неоднозначности: $x_1 x_2 x_2 x_1 = z_1 z_2 z_2 z_1$.
Заметим, что это уравнение эквивалентно системе

$$\begin{cases} x_1 x_2 = z_1 z_2 \\ x_2 x_1 = z_2 z_1 \end{cases} \quad (4)$$

$x_{1,s} = uv$, $x_{1,p} = vu$, $z_1 = (vu)^n v$. Тогда $x_1 = (vu)^{n+1} v$. При этом полагаем (vu) простым словом. Подставляя полученные значения в систему (4), имеем $x_2 vu = uvx_2$. Это опять уравнение сопряжения. Если сопряжение такое же, как для z_1 (т.е. x_2 имеет вид $(vu)^m u$), тогда мы получаем, что $x_1 x_2 x_2 x_1 = (vu)^{n+2} (uv)^{n+2}$. Частный случай этого решения — если $v = \varepsilon \vee u = \varepsilon$.



Задача на однозначность

Какие слова сопоставляются с образцом $x_1 x_2 x_2 x_1$ неоднозначно?

Решим уравнение неоднозначности: $x_1 x_2 x_2 x_1 = z_1 z_2 z_2 z_1$.
Заметим, что это уравнение эквивалентно системе

$$\begin{cases} x_1 x_2 = z_1 z_2 \\ x_2 x_1 = z_2 z_1 \end{cases} \quad (4)$$

Пусть $x_1 = (vu)^{n+1}v$, $x_2 vu = uvx_2$, причём vu — простое и $v \neq \varepsilon$, $u \neq \varepsilon$. Предположим теперь, что существуют такие v_1 , u_1 , что $vu = v_1 u_1$, $uv = u_1 v_1$, но $|v| \neq |v_1|$. Если окажется, что u_1 или v_1 — пустое слово, тогда $vu = uv$, поэтому vu — не простое. Иначе можно заметить, что система уравнений на u , v , u_1 , v_1 в точности повторяет (4), но $|v| < |x_1|$. По индукции, этот процесс рано или поздно приведёт к $|v_i| = \varepsilon$ или $|u_i| = \varepsilon$ (и будет получено противоречие с начальными условиями).



Задача на однозначность

Какие слова сопоставляются с образцом $x_1 x_2 x_2 x_1$ неоднозначно?

Решим уравнение неоднозначности: $x_1 x_2 x_2 x_1 = z_1 z_2 z_2 z_1$.

Заметим, что это уравнение эквивалентно системе

$$\begin{cases} x_1 x_2 = z_1 z_2 \\ x_2 x_1 = z_2 z_1 \end{cases} \quad (4)$$

Таким образом, удалось показать, что решениями системы (4) будут лишь слова вида $(vu)^{n+2}(uv)^{n+2}$, а значит, при сопоставлении только с такими словами образца $x_1 x_2 x_2 x_1$ может возникнуть неоднозначность (причём перебор при сопоставлении в этом случае достаточно делать лишь по степеням vu).