

SOLVING EQNS IN STRINGS

ON MAKANIN'S ALGORITHM

- (Claudio Gutiérrez)

→ Word eqns

$$x x a b x b y = a b a b b a b a b b b a a b b a a$$

- This is a simple pattern matching problem. However it becomes a word eqn when variables are on both sides.

$$x a x b y = b y b y x$$

- First solution: Lentin, Plotkin, Siekmann (70s) gave algorithm which gives solution if can find one otherwise it runs forever.
- In 1977, Makanin solved the decidability problem for word eqns & proved it decidable. ~~The~~
- Later Jaffar, extended Makanin's algo to give all solution.
- Plandowski, Rytter, Jez used decomposition to solve it in PSPACE.

Definitions:

- $C = \{a_1 \dots a_k\}$ constant
- $D = \{v_1, v_2, \dots\}$ variables.
- $w \in C \cup D$ word
- $|w|$ = length of word.

exponent of periodicity $(w) = p$ if $w = uv^p z$ $u, v, z \in C \cup D$
 $v \neq \emptyset$

$$w = aababab$$

$$w = a(ab)^2b$$

$$\boxed{Eop(w) = 2}$$

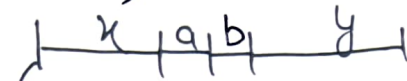
- $\{w_1, w_2\}$: word eqn $w_1 = w_2$
- Unifier (ε) : $U = (u_1 \dots u_n)$ such that $w_1 = w_2$ when variables (x_1, x_2, \dots, x_n) are replaced by (u_1, \dots, u_n) .

Basically a solution.

- $Eop(u)$ is the maximal exponent of periodicity of the words u_i ??

Graphical representation

$$xaby = ybax \leftarrow$$

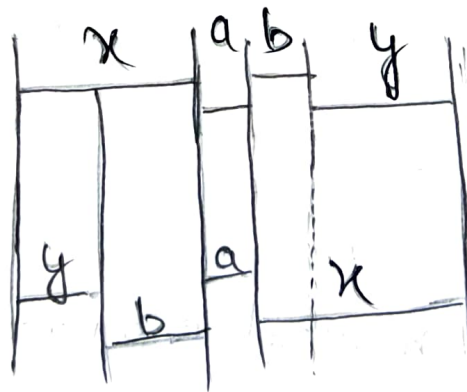


• boundaries.

- unit length is given to constants.
- length of variable can change.

Now we overlap and try to find such boundaries for the system in which the words b/w the boundaries are same.

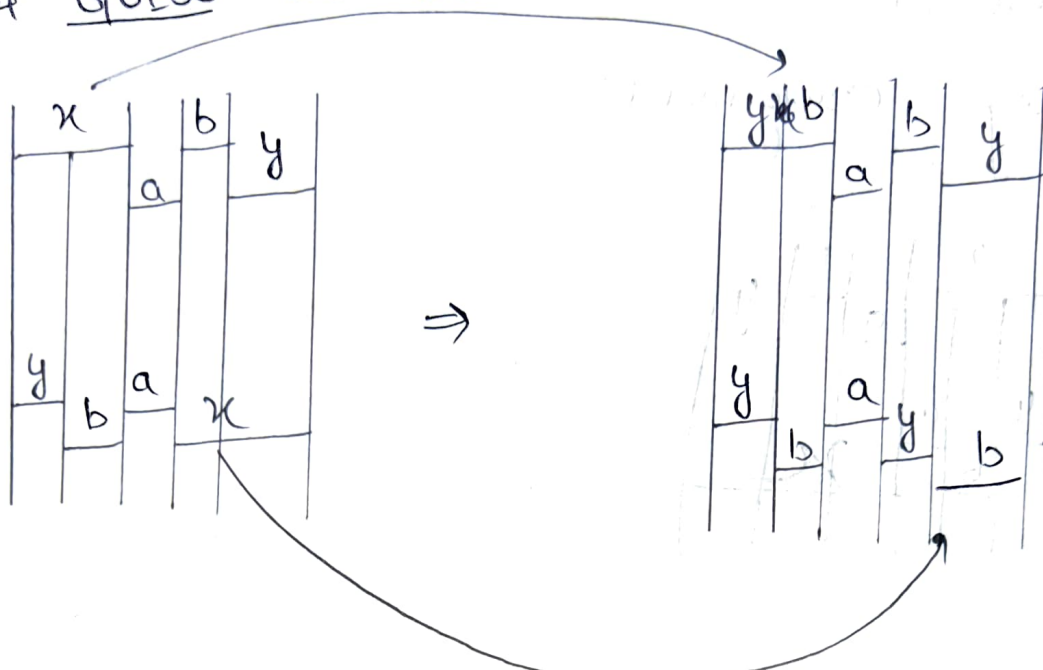
One such arrangement of boundaries.



Now we replace variable from left to right.

$$\boxed{x = yb}$$

- Now we replace all occurrences of x with 'yb' & GUESS the new boundaries.



Now we start replacing again.

$$\checkmark y = y$$

$$\checkmark b = b$$

$$\checkmark a = a$$

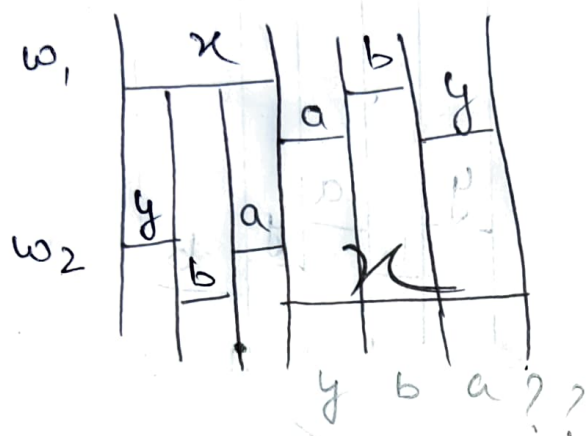
$$\boxed{b = y}$$

Now replace ~~to~~ all y with 'b'.

So we get : $\boxed{y = b}$
 $\boxed{x = yb = bb}$ Solution

Another example

boundary arrangement:



(b) ...

$x = y b a$...

$$a = y$$

$$y = a$$

Problems:

- number of occurrence of some variable starts growing after replacement.
- endless loop. ($xa = ax$) ??

$$\begin{array}{|c|c|} \hline x & a \\ \hline a & x \\ \hline \end{array} \quad \underline{xa = a?}$$

- what to do if there is no evident replacement.
(b) ??

Solution: One way

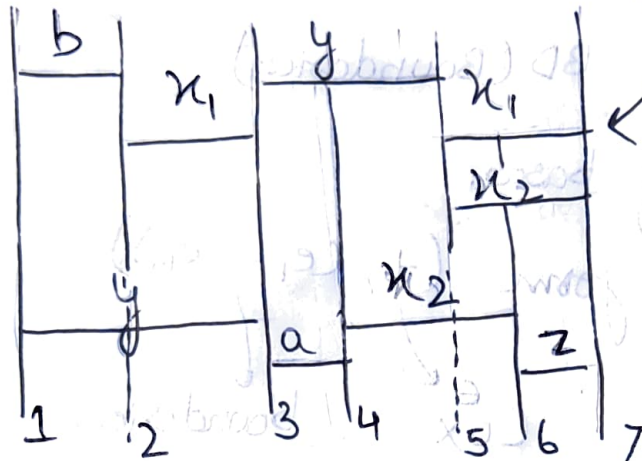
- Each variable can only occur twice in a word eqn.
- Any word eqn w/ more than two occurrences of a variable can be converted into system of eqns w/ at most two occurrences

$$b \underline{x} y \underline{x} = y a \underline{x} z$$

$$\left\{ \begin{array}{l} b x_1 y x_1 = y a x_2 z \\ x_1 = x_2 \end{array} \right\}$$

Generalised eqns: (Representation of graphical form in eqns)

$$\begin{cases} b x_1 y x_1 = y a x_2 z \\ x_1 = x_2 \end{cases}$$



GEN¹($b x_1 y x_1 = y a x_2 z$):

$$C = \{a, b\}$$

$$X = \{x_1, x_2, y, z\}$$

$$BD = \{1, 2, \dots, 7\}$$

$$BS = \{(b, (1, 2)), (a, (3, 4)), (x_1, (2, 3)), (x_1, (5, 7)),$$

$$(y, (3, 5)), (y, (1, 3)), (x_2, (4, 6)), (x_2, (5, 7))$$

$$(z, (6, 7))\}$$

GE consists of:

(1) C : constants
 X : variables

(2) linear ordered set BD (Boundaries)

(3) finite set BS of bases.

bs is of form $(t, (e_1, \dots, e_n))$
 \downarrow \downarrow
 $C \cup X$ boundaries.

Condition 1: for each variable in X ,
there are only two bases ~~are~~ called
duals denoted by x & \bar{x} . their boundary
sequence E_x & $E_{\bar{x}}$ must be same length.

This ensures that atmost two occurrence of
a variable happens.

Condition 2: For each base of a constant;
the boundary sequence has exactly two
consecutive elements.

Notations

~~In~~ • Pair (i, j) of boundaries is called indecomposable

if $j = i + 1$

• $\text{column}(bs) = (\text{left}(bs), \text{right}(bs))$

• base is empty if column is empty

• eqn is solved if ~~all~~ variable bases are empty.

Definition : Solution (Unifier) for a GE ~~if~~
is a function 'f' that ~~for some~~
assigns each in-de-composable column to a word.

• For each constant (c) \downarrow
~~col~~ $U(\text{col}(bs)) = c$
Unifier \downarrow

• $U(\text{col}(x)) = U(\text{col}(\bar{x}))$

basically both occurrences of the variable get same word.

• U is strict if $U(i, i+1) \neq \emptyset$ for all $i \in BD$.

• The exponent of periodicity of U is
maximal exponent of periodicity of the words
 $U(\text{col}(x))$??

Def 4:

Let G be a group and $f: G \rightarrow G$ a function.

$$f(x) = (x^2 + 1) \pmod{p}$$

Let p be a prime. If f is a permutation of \mathbb{Z}_p , then f is called a permutation polynomial over \mathbb{Z}_p .

Let f be a function from \mathbb{Z}_p to \mathbb{Z}_p . If f is a permutation of \mathbb{Z}_p , then f is called a permutation polynomial over \mathbb{Z}_p .

$$f(x) = (x^2 + 1) \pmod{p}$$

$$f(x) = (x^2 + 1) \pmod{p}$$

Let p be a prime. If f is a permutation of \mathbb{Z}_p , then f is called a permutation polynomial over \mathbb{Z}_p .

Let p be a prime. If f is a permutation of \mathbb{Z}_p , then f is called a permutation polynomial over \mathbb{Z}_p .

Let p be a prime. If f is a permutation of \mathbb{Z}_p , then f is called a permutation polynomial over \mathbb{Z}_p .

Let p be a prime. If f is a permutation of \mathbb{Z}_p , then f is called a permutation polynomial over \mathbb{Z}_p .

Let p be a prime. If f is a permutation of \mathbb{Z}_p , then f is called a permutation polynomial over \mathbb{Z}_p .

Transformation algorithm

$$GE = (C, X, BD, BS)$$

Definition 7: Carrier of GE ' x_c '

x_c : smallest left boundary i.e. leftmost variable.

• if there are two leftmost variables choose the one w/ biggest rightmost boundary i.e. the bigger of the two.

$$l_c = \text{left}(x_c)$$

$$r_c = \text{right}(x_c)$$

critical boundary $cr = \min\{\text{LEFT}(y) : x_c \in \text{col}(y)\}$

if cr is empty; $cr = r_c$

↓
this basically means that choose the leftmost boundary in all the columns that x_c is a part of ??

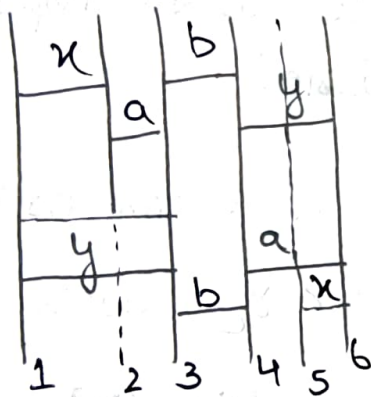
Definition 10: Let b_s be a non carrier base of GE.

→ b_s is superflows if $\text{col}(b_s) = (l, j) < l_c$

→ b_s is transport if $l_c \leq \text{left}(b_s) < c_x$

or
 $\text{col}(b_s) = (c_x, c_x)$

→ b_s is fixed if it is not superflows or transport.

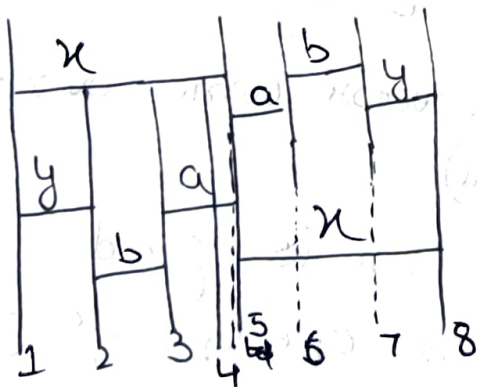


Carrier: y (leftmost, biggest)

$$l_c = 1$$

$$r_c = 3$$

$$c_x = 3$$

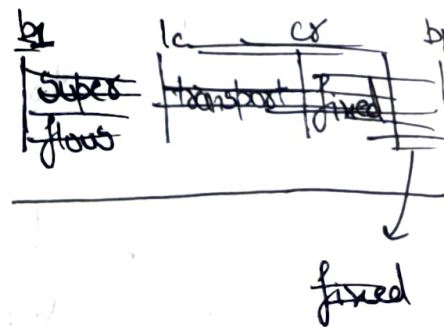


Carrier: x

$$l_c = 1$$

$$r_c = 5$$

$$c_x = 4$$



b_1 | l_c | r_c | r_c | b_M
 Super flows | transport | fixed | fixed |

these are the bases we are moving.

Notation: For each i such that $l_c \leq i \leq r_c$;
 we will introduce a new symbol i^{tr}
 and denote $\underline{tr(E_x)} = \underline{tr(e_1, e_2, \dots, e_n)} = \underline{(e_1^{tr}, \dots, e_n^{tr})}$

After transport of 'x' what happens to the boundedness.

Definition 9: point of GE is a linear order (\leq)
 on ~~$\{e_i\}_{l_c \leq i \leq r_c}$~~ i^{tr} on $l_c \leq i \leq r_c$ such that,

if $j < k$ ~~in~~ \leq extends the order of BD and
 before transport $j^{tr} < k^{tr}$ for $l_c \leq j \leq k \leq r_c$
 then $j^{tr} < k^{tr}$

?? $\cdot tr(E_c) = \bar{E}_c$ (the structure carries over to dual)

• if x is transport, \bar{x} is fixed
 then if for some $e_i \in E_x$, $e_i^{tr} = \bar{e}_i$
 then $tr(E_x) = E_{\bar{x}}$.

• Constants remain unchanged.