U. Feige, A. Fiat, A. Shamir,

I. Shimshoni, G. Tardos

Planning and Learning in Permutation Groups

Proceedings of the 30-th Symposium

on Foundations of Computer Science

Durham, NC, October 1989, 274–279

NOTATION:

STATES OF THE ENVIRONMENT:

$$S = \{1, 2, \cdots, m\}$$

THE PERMUTATION THAT MAPS j TO i_j IS DENOTED BY $\langle i_1, i_2, \cdots, i_m \rangle$.

PERMUTATIONS ARE COMPOSED FROM LEFT TO RIGHT:

$$2\langle 3,1,2\rangle\langle 3,2,1\rangle = 1\langle 3,2,1\rangle = 3$$

THE BASIC OPERATIONS ARE

$$\Sigma = \{x, y, \cdots\}$$

THEIR INVERSES ARE

$$\Sigma^{-1} = \{x^{-1}, y^{-1}, \cdots\}$$

WORDS w IN $(\Sigma \cup \Sigma^{-1})^*$ ARE REDUCED IF THEY CONTAIN NO ADJACENT INVERSE LETTERS.

THE FORMAL PROBLEM:

GIVEN A SYSTEM OF EQUATIONS OF THE FORM $iW = j$ IN WHICH $i, j \in S$ AND $w \in (\Sigma \cup \Sigma^{-1})^*$, FIND THE UNKNOWN PERMUTATIONS $x, y, \cdots$ IN Σ.

EXAMPLE: $S = \{1,2,3\}$, $\Sigma = \{x, y\}$.

$1xy = 1$ $\quad 2y^{-1}x = 3$ $\quad 1xy^{-1} = 2$

$3yxy = 1$ $\quad 2yxx = 3$ $\quad 3x^{-1}yx^{-1} = 2$

THE TWO NOTIONS OF SOLVABILITY:

SEMANTIC SOLVABILITY

SYNTACTIC SOLVABILITY

THE ALLOWABLE SYNTACTIC OPERATIONS

1. $ie = i$ IS AN EQUATION FOR ALL $i \in S$.
2. IF $iw'w'' = j$ IS AN EQUATION AND $x \in \Sigma$, THEN $iw'xx^{-1}w'' = j$ AND $iw'x^{-1}xw'' = j$ ARE EQUATIONS.
3. IF $iw'xx^{-1}w'' = j$ OR $iw'x^{-1}xw'' = j$ ARE EQUATIONS, THEN $iw'w'' = j$ IS AN EQUATION.
4. IF $iw = j$ IS AN EQUATION, THEN $jw^{-1} = i$ IS AN EQUATION.
5. IF $iw' = j$ AND $jw'' = k$ ARE EQUATIONS, THEN $iw'w'' = k$ IS AN EQUATION.

WE DENOTE THE SET OF ALL THE ORIGINAL AND IMPLIED EQUATIONS BY E AND THE SUBSET OF EQUATIONS WITH REDUCED WORDS BY R.

IN OUR EXAMPLE, WE WANT TO DEDUCE THAT $1y = 2$ FROM:

1. $1xy = 1$
2. $2y^{-1}x = 3$
3. $1xy^{-1} = 2$
4. $3yxy = 1$
5. $2yxx = 3$
6. $3x^{-1}yx^{-1} = 2$

WE START WITH THE INVERSE OF (2):

$$3x^{-1}y = 2$$

WE REPLACE 3 BY $1y^{-1}x^{-1}y^{-1}$ FROM (4):

$$1y^{-1}x^{-1}y^{-1}x^{-1}y = 2$$

WE REPLACE 1 BY $1xy$ FROM (1):

$$1xy\,y^{-1}x^{-1}y^{-1}x^{-1}y = 2$$

WE REPEAT THE LAST STEP:

$$1xyxy\,y^{-1}x^{-1}y^{-1}x^{-1}y = 2$$

WE LET THE WORD COLLAPSE:

$$1y = 2$$

Q.E.D.

AN INTERESTING SPECIAL CASE:

$n = 1$ (PERMUTATIONS WITHOUT INTERNAL STRUCTURE)

GIVEN: A SET OF "KNOWN" WORDS $W \in (\Sigma \cup \Sigma^{-1})^*$

FIND: ALL THE OTHER WORDS WHICH BECOME "KNOWN" VIA GROUP OPERATIONS (ESPECIALLY THE SINGLETON)

THIS IS NOT THE STANDARD WORD PROBLEM IN GROUPS, SINCE $W = e$ AND $W =$ "KNOWN" ARE DIFFERENT!

EXAMPLE: $xyz = e \Rightarrow zxy = e$

$xyz =$ "KNOWN" $\not\Rightarrow zxy =$ "KNOWN"

- "IDENTITY CLOSURE" IS UNDECIDABLE.
- "KNOWLEDGE CLOSURE" IS SOLVABLE IN ALMOST LINEAR TIME.

THE NEW ALGORITHM

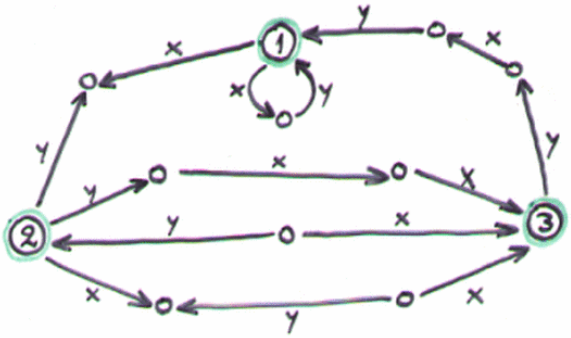
WE CONSTRUCT A DIRECTED GRAPH G WHOSE EDGES ARE LABELLED BY LETTERS FROM Σ. WE INTERPRET ANY UNDIRECTED PATH IN G AS A WORD $W \in (\Sigma \cup \Sigma^{-1})^*$. THE GRAPH CONTAINS n SPECIAL VERTICES, WHICH CORRESPOND TO THE POSSIBLE STATES IN S (THE GRAPH CAN CONTAIN ADDITIONAL, NON-SPECIAL VERTICES).

INITIALLY, G CONTAINS THE n SPECIAL VERTICES AND NO EDGES. FOR EACH EQUATION $iW = j$ WE ADD A NEW PATH FROM SPECIAL VERTEX i TO SPECIAL VERTEX j (VIA NEW INTERMEDIATE VERTICES) IN WHICH THE LABELS AND DIRECTIONS CORRESPOND TO THE LETTERS IN W.

IN OUR EXAMPLE:

$1xy = 1$ $\quad 2y^{-1}x = 3$ $\quad 1xy^{-1} = 2$

$3yxy = 1$ $\quad 2yxx = 3$ $\quad 3x^{-1}yx^{-1} = 2$

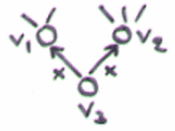


TO SHOW THAT $1y=2$ IS IMPLIED BY THE GIVEN EQUATIONS, WE HAVE TO FIND SOME PATH W FROM 1 TO 2 WHOSE REDUCED FORM IS y.

THE SHORTEST SUCH PATH IS $W=xyxyy^{-1}x^{-1}y^{-1}x^{-1}y$.

THE CRUCIAL OBSERVATION:

IF WE REPLACE IN A GRAPH G



BY

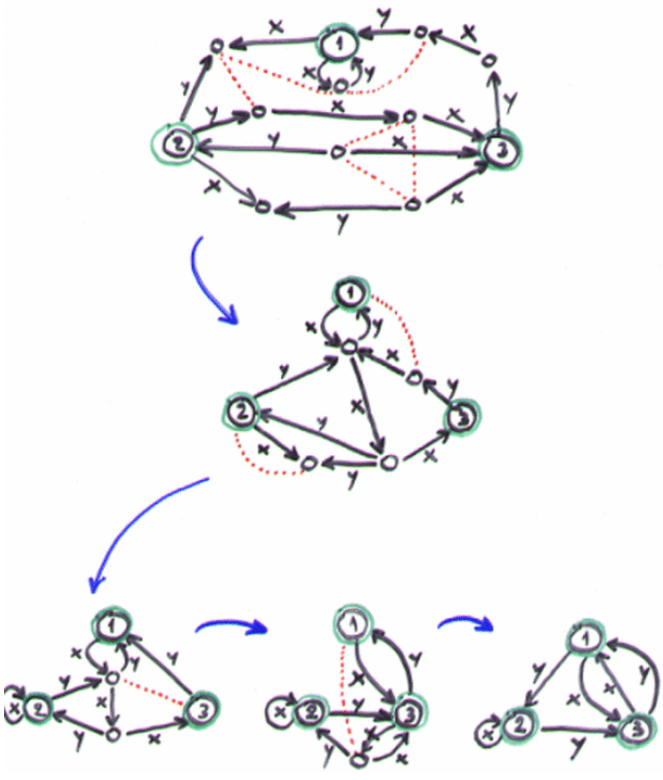
, OR

BY

WE DO NOT CHANGE THE SET OF WORDS WHICH ARE THE REDUCED FORMS OF ALL THE POSSIBLE PATHS BETWEEN A PAIR OF VERTICES IN G.

THIS REDUCTION PROCESS HAS THE CHURCH-ROSSER PROPERTY, SO IT CAN BE APPLIED IN ANY ORDER UNTIL THE GRAPH G BECOMES A REDUCED GRAPH $\overline{G}$.

IN OUR EXAMPLE:



THE REDUCED GRAPH $\overline{G}$ IS DETERMINISTIC AND ALL ITS PATHS ARE ALREADY REDUCED. SO TO CHECK IF $iW=j$ (← REDUCED) IS IMPLIED BY THE ORIGINAL EQUATIONS, JUST FOLLOW THE (UNIQUE, IF IT EXISTS) PATH W FROM i AND CHECK IF IT REACHES j.

THEOREM: A SYSTEM OF EQUATIONS IS SYNTACTICALLY SOLVABLE IFF ALL THE VERTICES IN $\overline{G}$ ARE SPECIAL AND OF MAXIMAL OUTDEGREE.

THEOREM: A SYSTEM OF EQUATIONS IS CONTRADICTORY IF THE ALGORITHM EVER ATTEMPTS TO MERGE TWO SPECIAL VERTICES.

COMPLEXITY:

SYNTACTIC SOLVABILITY CAN BE DECIDED (AND THE ACTUAL SOLUTION FOUND) IN $O(m\,\alpha(m))$ TIME AND $O(m)$ SPACE WHERE

$m = n +$ TOTAL SIZE OF EQUATIONS

THE EXPECTED BEHAVIOUR OF THE ALGORITHM FOR RANDOM EQUATIONS

HOW MANY EQUATIONS ARE REQUIRED TO MAKE THE SYSTEM SYNTACTICALLY SOLVABLE?

ASSUMPTIONS: IN EACH EQUATION $iW=j$:

1. W IS A RANDOMLY CHOSEN REDUCED WORD OF LENGTH r OVER $(\Sigma \cup \Sigma^{-1})$.
2. i IS A RANDOMLY CHOSEN ELEMENT IN S.
3. j IS COMPUTED FROM iW WITH RESPECT TO SOME FIXED, RANDOMLY CHOSEN PERMUTATIONS $x, y \ldots$ SHOULD BE ODD

NOTATION: $|S| = n$, $|\Sigma| = k$, $|W| = r$, THE NUMBER OF EQUATIONS IS t, THE THRESHOLD VALUE OF t WHICH MAKES THE SYSTEM SYNTACTICALLY SOLVABLE WITH PROBABILITY $\geq \frac{1}{2}$ BY t_0.

THEOREM: $t_0 = O\left(n\,(2k-1)^{r/2}\right)$

THEOREM: $t_0 = \Omega\left(n\,(2k-1)^{r/3}/r\right)$

CONJECTURE: $t_0 = \Theta\left(n\,(2k-1)^{r/2}/r\right)$

SUPPORTING EVIDENCE:

FOR $n=1$, $k=2$, VARIABLE LENGTH WORDS:

r	PREDICTED t_0	EXPERIMENTAL t_0
15	253	306
17	668	778
19	1794	2095
21	4870	5272
23	13,340	13,900
25	36,819	37,987
27	102,276	103,225
29	285,667	282,159

AN OUTLINE OF THE LOWER BOUND FOR $n=1$ (THE "KNOWLEDGE CLOSURE"):

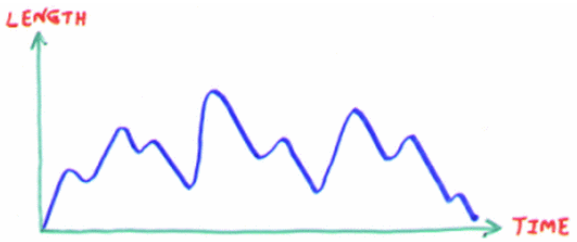
LET $\#$ BE THE NUMBER OF POSSIBLE REDUCED WORDS OF LENGTH r OVER A k ELEMENT ALPHABET Σ.

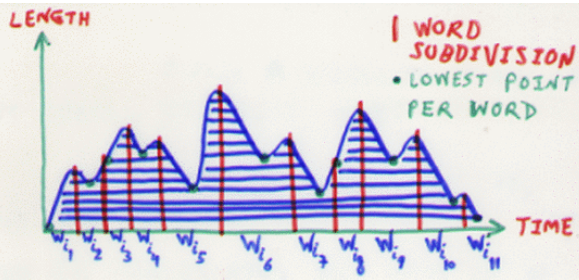
LEMMA: $\# = 2k(2k-1)^{r-1} \approx (2k-1)^r$

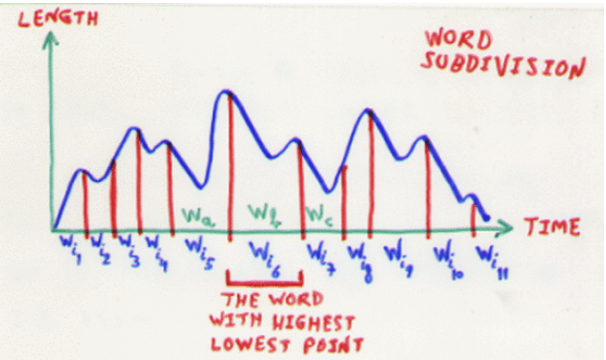
THEOREM: $t_0 = \Omega\left(\sqrt[3]{\#}/r\right)$

PROOF: LET $W_{i_1} W_{i_2} \cdots W_{i_s}$ BE A PRODUCT OF SOME OF THE ORIGINAL WORDS (WITH POSSIBLE REPETITIONS) WHICH REDUCES TO A SINGLE LETTER "x".

THE REDUCTION CAN BE CARRIED OUT FROM LEFT TO RIGHT BY USING A STACK, AND THE LENGTH OF THIS STACK CAN BE DESCRIBED IN A GRAPH:



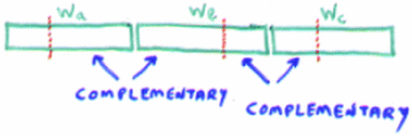




THEOREM: A NECESSARY CONDITION FOR SYNTACTIC SOLVABILITY IS THE EXISTENCE OF THREE ORIGINAL WORDS W_a, W_b, W_c WITH THE PROPERTY THAT W_b IS TOTALLY ANNIHILATED BY W_a AND W_c IN $W_a W_b W_c$.

THEOREM: SUCH A TRIPLET OF WORDS IS LIKELY TO EXIST WHEN $t_o = \Omega\left(\sqrt[3]{\#/n}\right)$.

PROOF: GIVEN t_o RANDOM WORDS, WE CAN CHOOSE $W_a W_b W_c$ IN t_o^3 WAYS. TO BE ANNIHILATED, W_b MUST BE OF THE FORM:



THE PROBABILITY OF THIS IS ABOUT $n/\#$, AND THUS A NECESSARY CONDITION IS

$$t_o^3 \cdot n/\# \geq 1$$

OR

$$t_o = \Omega\left(\sqrt[3]{\#/n}\right)$$

Q.E.D.