Makanin's Algorithm by Diekart

April 20, 2023

Free Monoids

- → Given a set S, the free monoid on S is the set S' of all lists (finite sequences) of elements of S, made into a monoid using concatenation.
- → The identity element of the free monoid is the empty string.
- → In the paper, the symbol 1 denotes empty string (and also the Natural number)

Notation

- $\rightarrow$ Variables : Ω
- $\rightarrow$ Constants : A $= \{a, b, c..\}$
- $\rightarrow$ Word : L $\in (A \cup \Omega)^*$
- $\rightarrow$ Word equation : $L = R$ such that $(L, R) \in (A \cup \Omega)^*$ x $(A \cup \Omega)^*$
- $\rightarrow$ Length of word equation : $|w| = |w_1| + |w_2|$
- $\rightarrow$ System of word eqns : $\{L_1 = R_1 \ , \ L_2 = R_2, ..., L_k = R_k\}$
- $\rightarrow$ Solution : $\sigma : (A \cup \Omega)^* \rightarrow A^*$ such that $\sigma(L_i) = \sigma(R_i) \ \forall \ 1 \leq i \leq k$.
  The homomorphism leaves the letters of A invariant.
  So a solution can also be represented by a mapping $\sigma : \Omega \rightarrow A^*$
- $\rightarrow$ Solution is non-singular if $\sigma(x) \neq 1 \ \forall \ x \in \Omega$. Otherwise its singular
- $\rightarrow$ A word is *primitive* if it can't be written in form $p = r^\alpha$ with $\alpha \neq 1$
- $\rightarrow$ $log \ \alpha = max\{1, \lceil log_2 \alpha \rceil\}$
- $\rightarrow$ Two words $x, y \in A^*$ are conjugate if $x = uv$ and $y = vu$ for some $u, v \in A^*$. OR we can also say x, y are conguent is $\exists z$ such that $xz = zy$. Equivalent definitions.

Matiyasevich 1968

1. Given : Let $E = \{L_1 = R_1, \ldots, L_k = R_k\}$ with each variable ocuring atmost twice.
2. $\|E\| = \sum_{i=1}^{k} |L_i R_i|$ denotes denotional length of E.
3. Inductive proof. Base case :
4. The first step is to guess whether is there is a singular solution. i.e. There is a solution $\sigma : \Omega \to A^*$ where $\sigma(x) = 1$ for some $x \in \Omega$
   4.1 Choose some $x \in \Omega$ and replace all occurrences of x by a empty word
   4.2 We obtain a new system of equation E' which we can recursively decide whether has a solution or not.

4 Finding the non singular solutions.

Any equation will always be of form

$x \cdots = a \cdots$ with $x \in \Omega, a \in A$

$x \cdots = y \cdots$ with $x \in \Omega, y \in \Omega, x \neq y$

We can write $x = az$ or $x = yz$ and replace all occurrences of x with az or yz

After replacing, we can cancel either a or y.

Number of variables are same and $\|E'\| \leq \|E\|$

If E' is solvable, so is E.

5 How does it find the solution and halt?

Proposition 2.1

Let $x, y, z \in A^*$ be words, $y, z \neq 1$. Then the following assertions are equivalent:

1. $xy = zx$,
2. $\exists r, s \in A^*, s \neq 1, \alpha \geq 0 : x = (rs)^\alpha r, y = sr$, and $z = rs$.

Proposition 2.2

Let $p \in A^*$ be primitive and $p^2 = xpy$ for some $x, y \in A^*$. Then we have either $x = 1$ or $y = 1$ (but not both).

Frame Title