1. Classical Circuit

A universal gate set $U$ for classical bits compose of gates with 2 bit input, 1 bit output.

Example: $U \ni \{\text{NOR gates}\}$

Any classical circuit (with bounded gate size) can be converted into gates from $U$.

Original Circuit $\rightarrow$ Circuit built in $U$

$n$ Gates $\Rightarrow$ poly$(n)$ gates

2. Decision problem $\text{PRIM}$

Language: $L \subseteq \{0,1\}^*$ all finite string compose of 0, 1

Decision problem $\text{PRIM}$: Given $x$, decide if $x \in L$

Example:

$L = \{x | x \text{ is a binary representation of a prime}\}$

$L_1$ : Primality testing.

Could be define over $L_\text{Yes}, L_\text{No}$ with $L_\text{Yes} \cap L_\text{No} = \emptyset$

$\text{P (Polynomial time)}$: Language $L \in \text{P}$ if $L_1$ can be solved in polynomial time.

Thus, $\exists$ a classical circuit $C_n$, with poly$(n)$ gates

$C_n(x) = 1$ if $x \in L$

$C_n(x) = 0$ if $x \notin L$

$\text{NP (Nondeterministic Polynomial time)}$: Language $L \in \text{NP}$ if $L_1$ can be "verified" in poly time

$\exists \text{ an } \exists \text{ a classical circuit } C_n \text{, with poly } n \text{ gates}

\forall x \in \{0,1\}^*$ if $x \in L$, $\exists y \in \{0,1\}^*$ with $\text{poly} n \text{ proof}$ that $x \in L$ set $C_n(x,y) = 1$
\( \exists \text{ a classical circuit } C_n \), with poly \( n \) gates

\[ V \times E \text{ into } \{ 0,1 \} \] if \( x \in L \), \( y \in C_n \) \( \iff \) \( C_n(x,y) = 1 \)

\[ x \in E, y \in C_n \] \( \implies \) \( C_n(x,y) = 0 \)

\[ C_n(x) \]

\[ x \left\{ \begin{array}{c} 0 \quad \text{if } x \in L \\ 1 \quad \text{otherwise} \end{array} \right. \]

\[ y \left\{ \begin{array}{c} 0 \quad \text{if } y \in C_n \\ 1 \quad \text{otherwise} \end{array} \right. \]

*Problems with a good validation algorithm*

Example:

\[ \{ (x_1, y_2) \mid G_1, G_2 \text{ graphs, } G_1, G_2 \text{ are isomorphic} \} \quad \text{(Graph isomorphism problem)} \]

\[ y = \text{isomorphism map between } G_1 \text{ and } G_2 \]

Reference:

[SIP06]: Introduction to the Theory of Computation