HONORS
ALGORITHMS

2025-02-26

p1

Boolean circuit

gates, wires : digraph

$\wedge, \vee$ $\quad \neg$

DAG

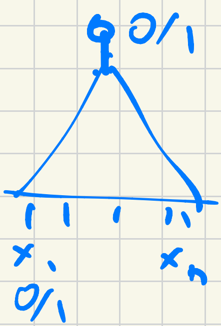
input gates

$\underbrace{x_i \quad \bar{x}_i}_{\text{literals}}$

Decision problem:

input $\underline{x} = (x_1 \cdots x_n)$ satisfies the circuit C if $C(x_1 \cdots x_n) = 1$

satisfying assignment



Q: Given C

$\exists?\ \underline{x}$ $\quad C(\underline{x}) = 1$

SAT satisfiability problem

Given a graph G
is it 3-colorable i.e. $\chi(G) \leq 3$

3COL

3COL $\propto$ SAT
reduction

Karp reduction:

$f : \{\text{graphs}\} \longrightarrow$ Boolean circuits

input to 3COL (set of 3-colorable graph)

input to SAT (set of satisfiable Boolean ckts)

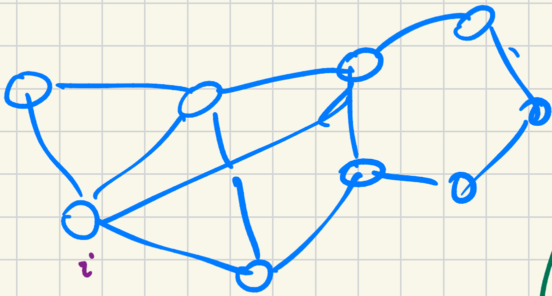
s.t.

① f is poly-time computable

② $(\forall G)\left(G \in 3COL \iff f(G) \in SAT\right)$

colors

R G B



$G \in 3COL \iff F \in SAT$

$x_{i1} = 1$ if i is RED

$x_{i2} = 1$ if i is GREEN

$x_{i3} = 1$ if i is BLUE

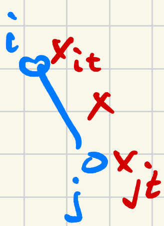
$t, s \in [3]$ $\underbrace{x_{it} = 1 \Rightarrow x_{is} = 0}$ $s \neq t$ — $\underbrace{\overline{x_{it}} \vee \overline{x_{is}}}$ — Clauses

each vertex has exactly one color

$\neg(x_{i1} = x_{i2} = x_{i3} = 0)$ — $\underbrace{x_{i1} \vee x_{i2} \vee x_{i3}}$ — Clauses

---

$t \in [3]$ if $i \sim j$ and $x_{it} = 1$ then $x_{jt} = 0$



$x_{it} \to \neg x_{jt}$

$\underbrace{\overline{x_{it}} \vee \overline{x_{jt}}}$ — Clauses

$A \to B$ means $\neg A \vee B$

$F = \bigwedge \text{Clauses}$

$F(x_{it} \mid i \in [n], t \in [3])$: CNF circuit p4

Σ finite alphabet

Σ^* set of all finite strings from Σ
words

$\Sigma = \{A, B, X\}$

$ABBBXAXXX \in \Sigma^*$

Language: $L \subseteq \Sigma^*$

computing a language L
means
given $x \in \Sigma^*$
decide $x \overset{?}{\in} L$

solving this decision problem

membership problem

$\underline{P}$: set of languages computable in polynomial time

example: $DIV = \{(x,y) \mid x, y \in \mathbb{Z}, x \mid y\}$

divisor

is ~~matrix~~ integer multiplication in $\underline{P}$?

multiplication of integer matrices can be performed in poly time

$k \times k$ matrices : product computable by $O(k^3)$ arithm. operations

if max bitlength of entries is ℓ

then we work with numbers of bitlength $\leq \ell$ for multiple, $\leq 2\ell$ for addition

---

NOT in $\mathbb{P}$

b/c NOT a DESISION PROBLEM

b/c has a multi-bit output

---

decision problem about Σ^* :

<u>predicate</u> on Σ^*: $f : \Sigma^* \to \{0,1\}$

PRIMALITY : given $x \in \mathbb{N}$ is it a prime ?

<u>Thm</u> <u>PRIMALITY IN $\mathbb{P}$</u> | Agrawal Kayal Saxena

identification

languages $\longleftrightarrow$ decision problems (predicates)

given lang L $\longrightarrow$ decision probl. f

$L \subseteq \Sigma^*$

$\forall x \in \Sigma^*$

$$f(x) = \begin{cases} 1 & \text{if } x \in L \\ 0 & \text{if } x \in \Sigma^* \setminus L \\ & (x \notin L) \end{cases}$$

inverse:

given decision problem f $\longrightarrow$ language L

$$L = f^{-1}(1)$$
$$= \{ x \in \Sigma^* \mid f(x) = 1 \}$$

$\mathbf{P}$ is a class of languages

nondeterministic polynomial time

~~random~~ guess, divine inspiration

NP : class of languages

p7

examples:

SAT $\in$ NP

3COL $\in$ NP

COMPOSITE NUMBERS $\in$ NP

FACT $\in$ NP (decision version of factoring)

feasibility of generalized SUDOKU $\in$ NP

---

puzzle x

purported solution y ← "witness"

verifiable in poly time