4/16/2019.

Monday 5/6 : midterm
HW 3 due

5/8 } no class. group discussion for project
5/10

Potential project group - email by wed.

* Recap: Complexity theory

Setup: · Problem: Language $A \subset \{0,1\}^*$ determine if $w \in A$.
· Computational model: Turing Machine
· Complexity class: $P \subset NP$

Main Thm : (Cook-Levin)
The language SAT and 3-SAT are NP-complete.

Using the Thm, one can show many other languages are NP-complete. (CLIQUE, 3COLOR, PERFECT, HAMPATH)

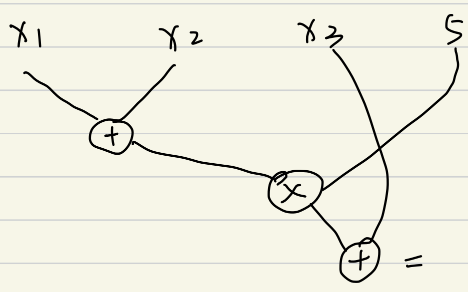
* Transition to algebraic complexity theory

Let k be a field, ex: $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}/p$ where p is prime.
(everything we do depends on k)

Define the ring $k[x_1, \cdots, x_n]$ = set of all polynomials $f(x_1, \cdots, x_n)$ with coefficient in k.

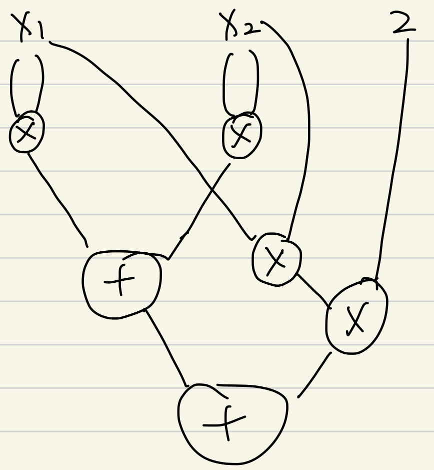
Def[1]: The complexity of a polynomial $f \in k[x_1, \cdots, x_n]$ is the minimal number of addition and multiplication needed to compute f.
Denoted the complexity of f as $C(f)$.

An arithmetic circuit is a directed graph where
· vertices are labeled as "+" or "x"
· no cycles.
· input (sources) of the graph are variables $x_1, \cdots, x_n$ or constant in K
· output is what circuit computes.

Ex:  $= (x_1+x_2)5 + x_3.$

The complexity of f is the minimum number of "+" and "×" in an arithmetic circuit computes f.

Ex: $f(x_1, x_2) = x_1^2 + 2x_1x_2 + x_2^2 = (x_1+x_2)^2$



6 "+" and "×"

Prop: $c(f) = 2$

For $f \in k[x_1, x_2]$: complexity 0 : $f = x_1, \cdots, x_n$ or $f = \alpha$, $\alpha \in k$.

complexity 1 : x_ix_j

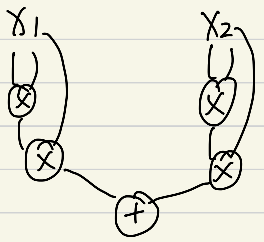
$x_i + x_j$

αx_i

$\alpha + x_i$

$\Rightarrow c(f) = 2.$

Ex: $f(x) = x_1^3 + x_2^3$

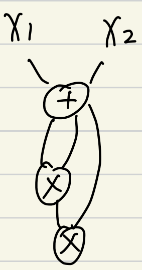


$c(f) = 5$

let's consider $k = \mathbb{Z}/3 \Rightarrow 3 = 0$

then $f(x) = x_1^3 + x_2^3 = (x_1 + x_2)^3 = x_1^3 + \underline{3x_1^2x_2} + \underline{3x_1x_2^2} + x_2^3$

$0x_1^2x_2$ $\quad$ $0x_1x_2^2$



$c(f) = 3.$

* Characteristic

Let R be a ring, the characteristic of R is the minimum integer $n > 0$ s.t. $\forall x \in R$, $nx = x + x + \cdots + x = 0$.
If $\nexists\, n$, the characteristic of R is 0.

Ex: Characteristic of $\mathbb{Z}/n$ is n

$$\left.\begin{array}{l} \mathbb{Z} \\ \mathbb{Q} \\ \mathbb{R} \\ \mathbb{C}[x_1, \cdots, x_n] \end{array}\right\} 0$$

$\mathbb{Z}/p[x_1, \cdots, x_n]$ is p

Special property in $\mathbb{Z}/p[x_1, \cdots, x_n]$ characteristic p when p is prime

1. $(a+b)^p = a^p + b^p$
2. For $\mathbb{Z}/p$, $\forall \alpha \in \mathbb{Z}/p$, $\alpha^p = \alpha$ (Fermat's little Thm)

$\forall \alpha \in \mathbb{Z}$, $\alpha^p \equiv \alpha \pmod p$

$\Rightarrow \alpha^{p-1} \equiv 1 \pmod p$

Key point: Let $K = \mathbb{Z}/p$
then let $f_1(x) = x$, $f_2(x) = x^p$.
clearly $f_1 \neq f_2$ as polynomials, but they have the same values, ie, $\forall \alpha \in \mathbb{Z}/p$, $f_1(\alpha) = f_2(\alpha)$.

If $f(x) = x^p$, the arithmetic circuit

input $\otimes$

output $\otimes$ does not compute f.