Week 5 Monday

Monday, April 29, 2019 11:33 AM

Mon } lecture.
Wed }

Fri: Review / discussion.

Mon: Midterm / HW3.

Wed: } Gp discussion.
Fri: }

Recall: Let k be any field. ($\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p$ etc.)

$k[x_1, x_2, \dots, x_n]$ = ring of polynomial with coeff in k.

An arithmetic circuit is a graph where.

1). Vertices are labelled "$\times$" or "+"

2). input are $x_1, \dots x_n$ or constant.

3) one output.

Complexity of f is the minimum # of "$\times$" and "+" steps in an arithmetic circuits which computes f

Char p

1) Let R be a ring of char p. (ie. $p \cdot x = 0 \ \forall x \in R$)

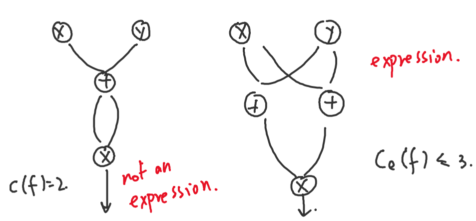
$(a+b)^p = a^p + b^p$

2) In $\mathbb{Z}/p$. we have. $\forall a \in \mathbb{Z}/p$ $a^p = a$ in $\mathbb{Z}/p$.

3) Polynomial x and x^p in $\mathbb{Z}/p[x]$ are different even though they have same evaluation.

<u>Variation:</u> An expression is an arithmetic circuits where the output of every "$\times$" or "+" node is used only once as the input of another node.

$(x+y)^2$.



Most polynomials have large complexity.

Proposition. A random homogeneous polynomial $f(x_1, \dots x_n)$ of degree d has complexity $c(f) \geq \binom{n+d-1}{d}$ Special polynomials have small complexity.

Proof: For any $s > 0$, $s \in \mathbb{Z}$.

$V_s = \{ f \in k[x_1, \dots x_n]_d \mid C(f) \leq s \} \subset k[x_1 \dots x_n]_d = k^N$, $N = \binom{n+d-1}{d}$

V_0 = { x_i [illegible] is constant in k } dimension = 1

$V_0 = \{x_i, a \mid a \text{ is constant in } k\}$ dimension = 1

$V_1 = \{a x_i, x_i x_j, x_i + x_j\}$ dimension = 1

$V_2 = \{a_1 x_1 + a_2, \ldots$ at most 2 constants$\}$

V_s has dimension $\leq S$ because it uses at most s constants.

If $s < N$, then any polynomial $f \in k[x_1, \ldots x_d]_n \setminus V_s$ has complexity $> s$

$\square$.

Corollary: A random homogeneous polynomial $f(x_1, \ldots x_n)$ of degree n has complexity $C(f) \geq 2^{n-2}$.

proof: $C(f) \geq \binom{n+n-1}{n} = \binom{2n-1}{n} = \dfrac{(2n-1)(2n-2)\cdots(n+1)}{n(n-1)\cdots 2 \cdot 1}$

Sequence of polynomials:

Consider polynomials: $f_n(x_1, \ldots x_{m_n})$ for $n = 1, 2, 3, \ldots$ m_n = # of variables.

Define. We say $\{f_n\}$ is p-computable. if m_n, $\deg(f_n)$ and $C(f_n)$ are polynomial bounded.

eg. ① $f_n(x_1 \ldots x_n) = x_1^n + \cdots + x_n^n$.

$f_1 = x_1$ $\quad$ $m_n = n$.

$f_2 = x_1^2 + x_2^2$ $\quad$ $\deg(f_n) = n$.

$\vdots$ $\quad$ $C(f_n) = n(n-1) + (n-1) = n^2 - 1$

$\Rightarrow \{f_n\}$ is p-computable.

② $f_n = x_1^{(2^n)}$ $\quad$ $m_n = 1$

$\deg(f_n) = 2^n \leftarrow$ not polynomial bounded $\Longrightarrow$ $\{f_n\}$ is not p-computable.

③ $f_n = x_1 + x_2 + \cdots + x_{2^n}$. $\quad$ $m_n = 2^n$. $\Rightarrow$ not p computable.

④ $f_n = x_1 x_2 \cdots x_n$. $\quad$ $m_n = n$.

$\deg(f_n) = 1$

$C(f_n) = n-1$

$\Rightarrow \{f_n\}$ is p-computable.

Defn: $VP^k = VP = \{$ p-computabe sequence $\{f_n\}\}$

$VP_e = \{$ Sequence $\{f_n(x_1, \ldots x_{m_n})\}$ such that $m_n, \deg(f_n)$ and $C_e(f_n)$ are polynomially bounded$\}$

$VP_e \subset VP$