POLYNOMIAL APPROXIMATIONS IN COMPLEXITY THEORY

SRIKANTH SRINIVASAN
DEPARTMENT OF MATHEMATICS
IIT BOMBAY

COMPLEXITY THEORY

→ Want to understand "complexity" of some computational problems.

COMPLEXITY THEORY

→ Want to understand "complexity" of some computational problems.

→ Computational problem: $(f_n : \{0,1\}^n \to \{0,1\})$

$f_n : \{0,1\}^n \to \{0,1\}$ - Bookan function.

COMPLEXITY THEORY

→ Want to understand "complexity" of some computational problems.

→ Computational problem: $(f_n : \{0,1\}^n \to \{0,1\})$

$f_n : \{0,1\}^n \to \{0,1\}$ - Bookan function.

→ Eg: $OR_n(x_1, \ldots, x_n) = \max\{x_1, \ldots, x_n\}$

$AND_n(x_1, \ldots, x_n) = \min\{x_1, \ldots, x_n\}$

$MAJ_n(x_1, \ldots, x_n) = \text{majority}\{x_1, \ldots, x_n\}$

COMPLEXITY THEORY

→ Want to understand "complexity" of some computational problems.

→ Computational problem: $(f_n : \{0,1\}^n \to \{0,1\})$

$f_n : \{0,1\}^n \to \{0,1\}$ - Boolean function.

→ Eg: $OR_n(x_1, \ldots, x_n) = \max\{x_1, \ldots, x_n\}$

$AND_n(x_1, \ldots, x_n) = \min\{x_1, \ldots, x_n\}$

$MAJ_n(x_1, \ldots, x_n) = \text{majority}\{x_1, \ldots, x_n\}$

Symmetric fns: $f(x)$ depends on $\sum_{i=1}^{n} x_i$.

COMPLEXITY THEORY

→ Want: $(f_n)_n$ that cannot be comp-
-uted "efficiently"
by a "simple" Computer Program

COMPLEXITY THEORY

→ Want: $(f_n)_n$ that cannot be comp-
-uted "efficiently"

by a "simple" Computer Program

→ Heart of P vs. NP question.

Approximation method [Razborov '80s]

→ To show: f_n has no simple program.

Approximation method [Razborov '80s]

→ To show: f_n has no simple program.

→ Say $\Pi_n : \{0,1\}^n \to \{0,1\}$ a simple program.

Approximation method [Razborov '80s]

→ To show: f_n has no simple program.

→ Say $\Pi_n : \{0,1\}^n \to \{0,1\}$ a simple program.

→ Approx. Π_n by a "well-behaved" fn. P_n.

Approximation method [Razborov '80s]

→ To show: f_n has no simple program.

→ Say $\Pi_n : \{0,1\}^n \to \{0,1\}$ a simple program.

→ Approx. Π_n by a "well-behaved" fn. P_n.

→ Show that "well-behaved" fns cannot approx. f_n. QED.

Approximation method [Razborov '80s]

→ To show: f_n has no simple program.

→ Say $\Pi_n : \{0,1\}^n \to \{0,1\}$ a simple program.

→ Approx. Π_n by a "well-behaved" fn. P_n.

→ Show that "well-behaved" fns cannot approx. f_n. QED.

→ Typically, well-behaved fns. more amen-able to analysis.

Polynomials

$f : \{0,1\}^n \longrightarrow \{0,1\}, \quad \{0,1\} \subseteq \mathbb{F}$

Polynomials

$f : \{0,1\}^n \longrightarrow \{0,1\}, \quad \{0,1\} \subseteq \mathbb{F}$

→ Interpolation: f can be represented by a polynomial $P \in \mathbb{F}[x_1, \ldots, x_n]$.

Polynomials

$f : \{0,1\}^n \to \{0,1\}$, $\{0,1\} \subseteq \mathbb{F}$

→ Interpolation: f can be represented by a polynomial $P \in \mathbb{F}[x_1, \ldots, x_n]$.

→ Easy fact: $\deg(P) \leq n$

($x_1 x_2^2 x_3 x_4^3 = x_1 x_2 x_3 x_4$)

Polynomials

$f : \{0,1\}^n \to \{0,1\}$, $\{0,1\} \subseteq \mathbb{F}$

→ Interpolation: f can be represented by a polynomial $P \in \mathbb{F}[x_1, \ldots, x_n]$.

→ Easy fact: $\deg(P) \leq n$

$(x_1 x_2^2 x_3 x_4^3 = x_1 x_2 x_3 x_4)$

→ Approximation method: Show that f can be "approximated" by lower degree polys.

Approximation

→ A probabilistic polynomial (of deg $\leq d$) probability distribution over polys (of deg $\leq d$).

Approximation

→ A probabilistic polynomial (of deg $\leq d$) probability distribution over polys (of deg $\leq d$).

→ $\tilde{P} \in \mathbb{F}[x_1, \ldots, x_n]$

Approximation

→ A probabilistic polynomial (of deg $\leq d$) probability distribution over polys (of deg $\leq d$).

→ $\mathbb{P} \in \mathbb{F}[x_1, \ldots, x_n]$

→ $\mathbb{P}$ approximates $f : \{0,1\}^n \to \{0,1\}$ if $\forall a \in \{0,1\}^n$, $\Pr_{\mathbb{P}}[\mathbb{P}(a) = f(a)] \geq \frac{3}{4}$.

Approximation

→ A probabilistic polynomial (of deg $\leq d$) probability distribution over polys (of deg $\leq d$).

→ $\mathbb{P} \in \mathbb{F}[x_1, \ldots, x_n]$

→ $\mathbb{P}$ approximates $f : \{0,1\}^n \to \{0,1\}$ if $\forall a \in \{0,1\}^n$, $\Pr_{\mathbb{P}}[\mathbb{P}(a) = f(a)] \geq \frac{3}{4}$.

→ $\deg(\mathbb{P}) \leq d \implies \text{pdeg}(f) \leq d$.

Example: $OR_n(x_1, \ldots, x_n) = \max\{x_1, \ldots, x_n\}$

Example : $OR_n(x_1, \dots, x_n) = \max\{x_1, \dots, x_n\}$

→ $F = F_2$

→ $\deg(OR_n) = n$.

Example: $OR_n(x_1, \ldots, x_n) = \max\{x_1, \ldots, x_n\}$

→ $\mathbb{F} = \mathbb{F}_2$

→ $\deg(OR_n) = n$.

Clm [Razborov]: $\operatorname{pdeg}(OR_n) \geq 2$.

Example: $OR_n(x_1, \dots, x_n) = \max\{x_1, \dots, x_n\}$

→ $\mathbb{F} = \mathbb{F}_2$

→ $\deg(OR_n) = n$.

Clm [Razborov]: $\operatorname{pdeg}(OR_n) \leq 2$.

Pf: Choose $\alpha \in \mathbb{F}_2^n$ uniformly at random.

$$P_\alpha(x) = \sum_{i=1}^{n} \alpha_i x_i$$

Example: $OR_n(x_1, \dots, x_n) = \max\{x_1, \dots, x_n\}$

→ $\mathbb{F} = \mathbb{F}_2$

→ $\deg(OR_n) = n$.

Clm [Razborov]: $pdeg(OR_n) \leq 2$.

Pf: Choose $\alpha \in \mathbb{F}_2^n$ uniformly at random.

$$P_\alpha(x) = \sum_{i=1}^{n} \alpha_i x_i$$

$$\begin{cases} a = 0 \Rightarrow \Pr[P_\alpha(a) = 0] = 1 \\ a \neq 0 \Rightarrow \Pr[P_\alpha(a) = 1] = \frac{1}{2}. \end{cases}$$

Example: $OR_n(x_1, \dots, x_n) = \max\{x_1, \dots, x_n\}$

→ $\mathbb{F} = \mathbb{F}_2$

→ $\deg(OR_n) = n$.

Clm [Razborov]: $\operatorname{pdeg}(OR_n) \leq 2$.

$\Rightarrow$ Choose $\alpha \in \mathbb{F}_2^n$ uniformly at random.

Pf: $P_\alpha(x) = \sum_{i=1}^{n} \alpha_i x_i$

$$\begin{cases} a = 0 \Rightarrow \Pr[P_\alpha(a) = 0] = 1 \\ a \neq 0 \Rightarrow \Pr[P_\alpha(a) = 1] = \frac{1}{2}. \end{cases}$$

$$\tilde{P}(x) = 1 - (1 - P_\alpha(x))(1 - P_\beta(x))$$

$\alpha, \beta \in_R \mathbb{F}_2^n$.

Example: $OR_n(x_1, \ldots, x_n) = \max\{x_1, \ldots, x_n\}$

→ $\mathbb{F}$ arbitrary.

→ $\deg(OR_n) = n$.

→ $pdeg(OR_n) \leq C \cdot \log n$

Example: $OR_n(x_1, \ldots, x_n) = \max\{x_1, \ldots, x_n\}$

→ $\mathbb{F}$ arbitrary.

→ $\deg(OR_n) = n$.

→ $pdeg(OR_n) \leq C \cdot \log n$

$< n^{\varepsilon}$ for any $\varepsilon > 0$.

Other symmetric functions

$f: \{0,1\}^n \to \{0,1\}$ symmetric if $f(a)$ depends only on $\sum_i a_i$.

Other symmetric functions

$f: \{0,1\}^n \to \{0,1\}$ symmetric if

$f(a)$ depends only on $\sum_i a_i$.

[$OR_n(a) = 1$ if $\sum_i a_i \geq 1$]

Other symmetric functions

$f: \{0,1\}^n \to \{0,1\}$ symmetric if

$f(a)$ depends only on $\sum_i a_i$.

[$OR_n(a) = 1$ if $\sum_i a_i \geq 1$]

[S'13]: $pdeg(f) \leq n^{1/2+\varepsilon}$ for any $\varepsilon > 0$

[AW'15]: $pdeg(f) \leq C \cdot \sqrt{n}$.

Other symmetric functions

$f: \{0,1\}^n \to \{0,1\}$ symmetric if

$f(a)$ depends only on $\sum_i a_i$.

[$OR_n(a) = 1$ if $\sum_i a_i \geq 1$]

[S'13]: $pdeg(f) \leq n^{1/2+\varepsilon}$ for any $\varepsilon > 0$

[AW'15]: $pdeg(f) \leq C \cdot \sqrt{n}$.

[AW'15]: Used to obtain programs for computational problems.

Probabilistic degree lower bounds

→ Want f s.t. $pdeg(f)$ large.

Probabilistic degree lower bounds

→ Want f s.t. $\mathrm{pdeg}(f)$ large.

→ $\mathrm{Maj}_n(a) = 1$ iff $\sum_i a_i > n/2$.

→ [Razborov, Smolensky]: $\mathrm{pdeg}(\mathrm{Maj}_n) \geq c \cdot \sqrt{n}$.

Probabilistic degree lower bounds

→ Want f s.t. $\mathrm{pdeg}(f)$ large.

→ $\mathrm{Maj}_n(a) = 1$ iff $\sum_i a_i > n/2$.

→ [Razborov, Smolensky]: $\mathrm{pdeg}(\mathrm{Maj}_n) \geq c \cdot \sqrt{n}$.

→ Best possible result for a symm. fn.

Probabilistic degree lower bounds

→ Want f s.t. $\mathrm{pdeg}(f)$ large.

→ $\mathrm{Maj}_n(a) = 1$ iff $\sum_i a_i > n/2$.

→ [Razborov, Smolensky]: $\mathrm{pdeg}(\mathrm{Maj}_n) \geq c \cdot \sqrt{n}$.

→ Best possible result for a symm. fn.

→ [S'13]: Any f s.t. $\mathrm{pdeg}(f) \geq n^{1/2+\varepsilon}$ would have many interesting complexity theory applications.

Other symmetric fns.

$\rightarrow$ $c \cdot \sqrt{n} \leq \underset{[R,S]}{} \text{pdeg}(\text{Maj}_n) \leq \underset{[AW]}{} c \cdot \sqrt{n}$

Other symmetric fns.

→ $c \cdot \sqrt{n} \leq \underset{[R,S]}{} \text{pdeg}(\text{Maj}_n) \leq \underset{[AW]}{} c \cdot \sqrt{n}$

→ Other symmetric fns?

Other symmetric fns.

→ $c \cdot \sqrt{n} \leq \text{pdeg}(\text{Maj}_n) \leq c \cdot \sqrt{n}$

[R,S] [AW]

→ Other symmetric fns?

→ $OR_n = \max\{x_1, \ldots, x_n\}$

Other symmetric fns.

→ $c \cdot \sqrt{n} \leq \text{pdeg}(\text{Maj}_n) \leq C \cdot \sqrt{n}$

[R,S] [AW]

→ Other symmetric fns?

→ $OR_n = \max\{x_1, \ldots, x_n\}$

→ $\text{char}(\mathbb{F}) = p > 0$

$1 \leq \text{pdeg}(OR_n) \leq C_p$

pdeg (OR_n) when char $(F) = 0$

→ [BRS'91, Tarui'91] $pdeg(OR_n) \leq c \cdot \log n$

pdeg (OR_n) when char $(F) = 0$

→ [BRS'91, Tarui'91] $pdeg(OR_n) \leq c \cdot \log n$

→ [MNV'15, HS'15]

$$pdeg(OR_n) \geq (\log n)^{1/2-\varepsilon} \quad \forall \varepsilon > 0$$

pdeg (OR_n) when char $(\mathbb{F}) = 0$

→ [BRS'91, Tarui'91] $\text{pdeg}(OR_n) \leq c \cdot \log n$

→ [MNV'15, HS'15]

$$\text{pdeg}(OR_n) \geq (\log n)^{1/2-\varepsilon} \quad \forall \varepsilon > 0$$

Ideas: Extension of Littlewood-Offord anticoncentration to low-degree polys.

pdeg (OR_n) when char $(\mathbb{F}) = 0$

→ [BRS'91, Tarui'91] $\text{pdeg}(OR_n) \leq c \cdot \log n$

→ [MNV'15, HS'15]

$$\text{pdeg}(OR_n) \geq (\log n)^{1/2-\varepsilon} \quad \forall \varepsilon > 0$$

Ideas: Extension of Littlewood-Offord anticoncentration to low-degree polys.

→ [BHMS'18]: $\text{pdeg}^*(OR_n) \geq c \cdot \log n$

$*$ - restricted class of polynomials.

Summary

→ Computational hardness of Boolean fns

↕

Polynomial approximations of Boolean fns.

Summary

→ Computational hardness of Boolean fns

↕

Polynomial approximations of Boolean fns.

→ Probabilistic approximations useful in this setting.

Summary

→ Computational hardness of Boolean fns

↕

Polynomial approximations of Boolean fns.

→ Probabilistic approximations useful in this setting.

→ Much known for symm. fns. but simple qns. remain open.

Summary

→ Computational hardness of Boolean fns

↕

Polynomial approximations of Boolean fns.

→ Probabilistic approximations useful in this setting.

→ Much known for symm. fns. but simple qns. remain open.

Thanks!