From Super-Linear to Super-Polynomial Lower Bounds?

For the Lipton 60th Theory Symposium, 4/27/08

Kenneth W. Regan

`regan@cse.buffalo.edu`

Department of Computer Science and Engineering

University at Buffalo (SUNY)

Buffalo, NY 14260-2000

Boolean Circuit Lower Bounds

- $3n$ full Boolean basis
- $\simeq 3.5n \to 4n \to 4.5n \to 5n - o(n)$ (1984–2005) over the AND, OR, NOT basis.
- No $\omega(n)$ bounds known for E $\cup$ NP.
- $\Omega(n^k)$ (any fixed k) known for S_2^p, ZPP$^{\mathrm{NP}}$... [Kannan 1982...Santhanam 2007].

Uniform Models

- Situation not much better even for the basic "1D" multitape Turing machine.
- Only a few NP-complete problems are known even to inherit the $\Omega(n \log_*^{1/4} n)$ time lower bound of [PPST83] for NLIN.
- Example: "Can we complete this arc-node diagram to a DFA with at most k inequivalent states?" [Grandjean]. None of the "original 21."
- RJL and. . . attempted to extend to 2D-TMs.

Tradeoffs

- Fortnow$\to$Lipton-Viglas$\to$F–van Melkebeek $\to$ R. Williams: For SAT, $n^{1-\epsilon}$ space $\implies \Omega(n^{1+\delta})$ time.
- But: sorting is easy yet requires $T(S+\nu) = \Omega(n^2)$ even for NTMs or NRAMs [after Mansour-Nisan-Tiwari, 1993].
- Size-depth tradeoffs for circuits are legion. . . E.g. [IPS97] depth-d threshold circuits for the NC^1-complete Boolean sentence value problem need size $\Omega(n^{1+\epsilon_d})$ (*counting wires*).

Structured Circuits

E.g. meshes, planar/log-genus, non-expanding...

- $\simeq \Omega(n^{1+1/d})$ size lower bounds, usually via

Graph Separators, e.g. Lipton-Tarjan: Planar $\implies$ separator of size $O(\sqrt{N}) \implies$ bounds with $d \simeq 1$.

Summer for Separators? Combine with random restrictions...?

Simplest $\omega(n)$ function?

$\Sigma = \{\,0, 1, 2\,\}$, $f(x) =$ move all 2s flush-right in x. E.g. $f(01212202) = 01102222$.

- $f(\lambda) = \lambda$, $f(0x) = 0f(x)$, $f(1x) = 1f(x)$, $f(2x) = f(x)2$.
- Stable sort of poset $0, 1 < 2$.
- $O(n \log n)$ “Troolean” circuit upper bound by AKS networks.
- Wlog. $n = 2^k$, x has $n/2$-many 2s.

Arithmetical Circuits

Best unrestricted lower bound for polynomial families $f(x_1, \ldots, x_n)$ over $F = \mathbf{C}, \mathbf{R}, \mathbf{Q}, \ldots$ is $\Omega(n \log n)$, by (Baur)-Strassen, but it applies to some simple functions, such as

$$f = x_1^n + x_2^n + \cdots + x_n^n.$$

Valiant's Lin-Log Challenge

Construct *explicit* families of *linear* transformations A_n on F^n that do not have Boolean/arithmetic circuits of linear size *and logarithmic depth*.

Separators/segregators/etc. digested but not decisive here.

Structured Arithmetical...

Formulas, bounded-depth, layered, multi-linear...

With bounded field constants on wires—:

- A_n requires $\log_2(|\det A_n|)$ size [Morgenstern, 1973].
- Since $\det \textit{DFT}_n = n^{n/2}$, the FFT's $O(n \log n)$ is tight among bc-circuits.
- Matrix mult. ($n = N^2$), convolution, polynomial mult., and some other bi-linear forms require bc-size $\Omega(n \log n)$ [Raz, Bürgisser-Lotz 2002-04].

Toward Unbounded Constants?

[Jansen-Regan]: Allow $|\det|$-1 matrices A, B “for free” at inputs, i.e. lower-bound the whole $SL_n(C)$ orbit $\{\, f(Ax, By) \,\}$.

- A, B have bounded *condition number* $\implies$ Raz’ method works, but otherwise?
- Not restricted to $(1-\epsilon)n$ unbounded constants.
- Leads to apparently-open problems in (random) Fourier minors...

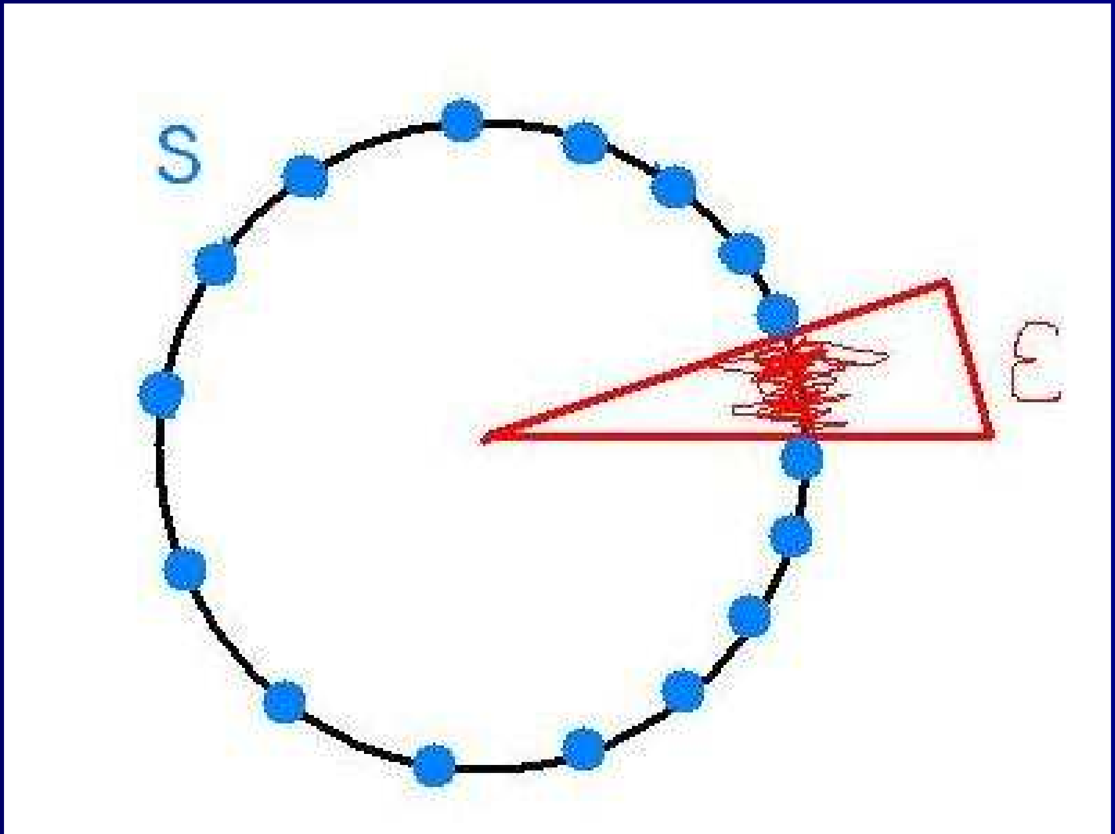
A Circle Problem

Given a set S of n points on the unit circle, define their *chordal product*

$$\mathit{cp}(S) = \Pi_{i<j} ||x_i - x_j||_2 = |\det(x_i^k)|.$$

- Max $= \det(\mathit{DFT}_n) = 2^{(n/2)\log n}$ when S are the nth roots of unity.
- Define $g_\epsilon(n) =$ max when S may not touch $(0, \epsilon)$.

Taking Out a Nibble



Would Euler be surprised?

Theorem. [who?] For every fixed ϵ, $g_\epsilon(n) \longrightarrow 0$ faster than $1/2^{cn \log n}$, any c.

- To extend the [Raz, BüLo] lower bounds, we needed “slower” whenever $\epsilon = \epsilon_n \longrightarrow 0$.
- But Jansen proved “faster” when $\epsilon_n \simeq 1/n^{1/5}$.
- $\epsilon_n \simeq 1/n^{1/4} \implies$ “slower,” but not our desired bound.
- Open: Close gap? Exact value, S for $g_\epsilon(n)$?

Numerical Instability and Cancella

Since “an average chord” has length $\sqrt{2}$, why isn’t *cp*$(\{\,\omega^i\,\})$ estimated by $\sqrt{2}^{\binom{n}{2}} = 2^{\Theta(n^2)}$?

- $\log\det($*DFT*$_n) = \Theta(n\log n)$, not $\Theta(n^2)$.
- We can arrange $\log$ *cp*$(\cdots)$ so that all powers of n above 1 **cancel**.
- Can this help us understand algebraic cancellations that enable poly-time algorithms? and lower bounds?

Super-linear really means...

(*) $\Omega(n^{1+\epsilon})$ where ϵ does not depend on any other parameter, such as depth or mesh dimension.

E.g. can we find length-linear functions computable in $O(n)$ time but whose inversion requires $\Omega(n^{1+\epsilon})$ time in almost all cases?

- If so, are they usefully one-way?
- Do they imply the existence of one-way functions with super-poly guarantee?

Allender-Koucký, 2008:

If L is self-reducible by networks $E_{n,\delta}$ of

- width-n^δ L-gates, and
- bounded fan-in gates

and depth $O(1/\delta)$, then (*) $\implies$ L does not have polynomial-size circuits of the kind (*) applied to.

E.g. $\Omega(n^{1+\epsilon})$ size on TC^0 circuits for BSVP (same ϵ for all depths d) $\implies$ TC$^0 \neq$ NC^1,

Arithmetization

- If w is a wire from a NAND(u, v) gate g, we can capture this by the equation $w = 1 - uv$, in a basis where $0 =$ *false* and $1 =$ *true*.
- Not disturbed by adding $x^2 = x$ to the equation set, for all variables x.
- The latter addition makes all polynomials reduce to multi-linear ones, which have degree at most n.
- Ditto $\{ -1, 1 \}$ basis, NAND by $w = (1/2)(1 - uv - u - v)$, add $x^2 = 1$.

Degrees of Degree

- Low: $d = n^{O(1)}$.
- High: $d = 2^{n^{O(1)}}$, d not low.
- Very High: $d = 2^{2^n}$.

Poly-size circuits can achieve high degree by iterated squaring, but formulas cannot.

Low-Degree Suffices

[Valiant et al.] Poly-size circuits for a low-degree polynomial over $\mathbb{C}, \mathbb{R}, \mathbb{Q} \ldots$ can be made to have depth $O(\log^2 n)$.

Like saying "Low-Degree P = NC^2."

Question: Can high-degree information ever be relevant to whether a polynomial is in VP?

La Manche?

- Can we tie complexity to mathematical quantities of lonegr vintage?
- Can high-degree information over infinite fields (of characteristic zero) matter to Boolean complexity?

Low-Degree Bridge

Theorem [Baur-Strassen]

$$C(f) \geq \log_2 \text{gdeg}(\{\, y_i - \partial f/\partial x_i \,\}).$$

Here $\text{gdeg}(\cdots) =$ the max finite $\cap$ with an n-dim. affine linear subspace of $\mathbf{C}^{2n}$.

E.g. $f = x_1^n + \cdots x_n^n$, $\text{gdeg}(\cdots) = (n-1)^n$.

But for f of degree d, $\text{gdeg}(\cdots) \leq d^n$, so for $d = n^{O(1)}$ it's $O(n \log n)$. Catch-22: Proof of Theorem entails this.

Extending the Degree Method...

Can we find a quantity $\mu(f)$ such that:

1. $C(f) \geq \log_2(f)$,
2. For some f, $\mu(f) = \text{double-exp}(n)$,

3a. Deciding $\mu(f) \geq K$ almost always needs time (say) K^ϵ, *and/or*

3b. Few (extensions of Boolean) functions have very-high $\mu(f)$.

$\Longrightarrow$ can circumvent "Natural Proofs," "Algebrization" barriers.

Template Example

$\mu(f) =$ # of "minimal monomials" $m \in (\partial f)$, i.e. $m \in (\partial f)$ but no proper divisor of m is.

- $\mu(\det_n) = 0$.
- $\mu(\text{perm}_n)$ is evidently **huge** (related results are known for $(\partial^{n-3}\text{perm}_n)$).
- $(\partial f \cdot g) \subseteq (f, g)$: if $pf + gq$ is a monomial, can we say the $*$ gate $g * f$ is "redundant"?

Super-Natural but Refuted. . .

- For *generic* f, $\mu(\partial f) = 0$.
- How to decide $\mu(f) \geq K$, other than by counting? Let alone that Gröbner basis algorithms (GBA) can take double-exp time.
- Alas, there are f with $O(n)$-size circuits of constant degree 6 (some variables squared) and $\mu(f) = 2^{2^n}$.
- Catch-22: Also proves EXSPACE-hardness of computing $\mu(f)$.

Other VHD Ideas

- Mulmuley-Sohoni: Mumford stability, *obstructions*—analogy, $\simeq$ VHD(Max Flow/Min Cut). (NB: GBA = VHD(Gaussian elimination).)
- Joel Freidman: de Rham cohomology, representations, categories. . .
- But, HD/LD: Raz [2008], "Elusive" functions, $\simeq$ co-NEXP properties.
- "Algebrization" $\Longrightarrow$? LD methods cannot work?

Refining Math Into Combinatorics

Mathematical Theory
$\longrightarrow$ Formal system F that comprehends it
$\longrightarrow$ Arithmetic
$\longrightarrow$ Combinatorial “power cells.”

Cf. Lipton-DeMillo-and-many: Arbitrarily fast-growing functions can have DLOGTIME inverses.

Is “Tropical” Topical?

[Speyer, Sturmfels et al.] Much of the structure of algebraic geometry is preserved when:

- $+$ plays the role of $*$, and
- $\max a, b$ plays the role of $+$.

KWR: Use $a@b = \log(\exp(a) + \exp(b))$ instead of $\max$?

End (of the beginning?)