Single Level Conjecture for Quadratic Functions and Graphs

Stasys Jukna

Lithuanian Academy of Sciences
Vilnius, Lithuania

&

University of Frankfurt
Frankfurt a.M., Germany

Outline

1. Graph complexity + motivation [1] [2]
   - Monotone l.b.'s for graphs $\Rightarrow$ non-monotone l.b.'s boolean functions
   - Use graphs to violate "largeness" condition of "natural proofs"
2. The conjecture:
   - Single level circuit $\Rightarrow$ only one level of AND gates $\Rightarrow$ depth-3 circuit
   - Single level circuits for graphs and quadratic functions are almost optimal
3. Disproof of the conjecture for bounded and unbouded fanin circuits

[1] P. Pudlák, V. Rödl, P. Savický: Graph complexity (1986)

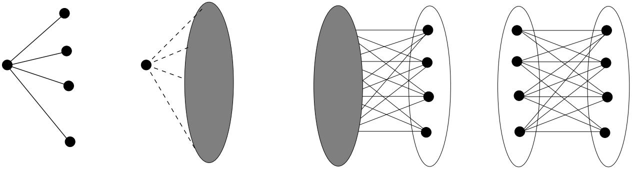
[2] A. Razborov: Bounded-depth formulae over the basis $\{\&, \oplus\}$ and some combinatorial problem (1988)

Circuit complexity of a graph – What is this?

- Graph $G = (V, E)$ $\Rightarrow$ boolean functions $f : \{0,1\}^V \to \{0,1\}$
- $f(X)$ represents a graph $\iff$ accepts edges & rejects non-edges:

$$f(0,\ldots,0,\overset{u}{1},0,\ldots,0,\overset{v}{1},0,\ldots,0) = 1 \iff uv \in E$$

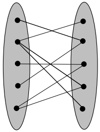
- $\Rightarrow$ on inputs with more/less than two 1's can take arbitrary values !
- $f(x_1,x_2,x_3,x_4) = (x_1 \vee x_2) \wedge (x_3 \vee x_4)$ represents $K_{2,2}$ = 4-cycle C_4
- x_u represents a complete star around u



single variable   negated variable   OR gate   Parity gate

Quadratic functions instead graphs?

- Quadratic function $f_G(X) = \bigvee_{uv \in E} x_u x_v$ represents $G = (V, E)$
- But ... many different functions may represent the same graph!
- And ... representation can be exponentially cheaper:
  $\exists$ graphs G with $\text{Circuit}^+(f_G) \geq 2^{\text{Circuit}^+(G)}$ (unbounded fanin)
- Perfect matching $\Rightarrow$ $\text{Circuit}^+(f_G) = \Omega(n)$ but $\text{Circuit}^+(G) = O(\log n)$



Saturated extension G of $H \subseteq U \times W$

= two cliques with graph H inbetween

$$f_G(X) = \bigvee_{uv \in H} x_u x_v \vee Th_2^U \vee Th_2^W$$

Observation

G saturated $\Rightarrow$ $f_G(X)$ is the unique monotone function representing G

$\Rightarrow$ $\text{Circuit}^+(G) = \text{Circuit}^+(f_G)$ $\Rightarrow$ enough to deal with quadratic functions !

Monotone bounds ... Why interesting?

- Boolean functions $\chi_m(x,y)$ = bipartite graphs $G \subseteq U \times W$ with $U = W = \{0,1\}^m$ and u and v adjacent in $G \iff \chi(\vec{u},\vec{v}) = 1$
- Random graph $\Rightarrow$ $\text{Circuit}^+(G) = \Omega(n^2/\log n)$

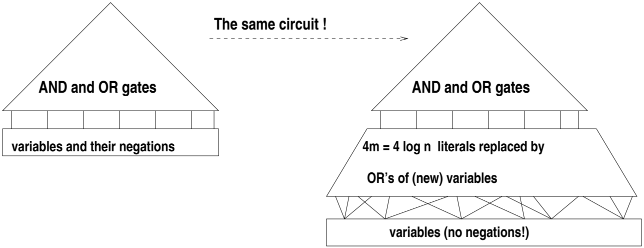
Magnification Lemma

$$\text{Circuit}(\chi_m) \geq \text{Circuit}^+(G) \qquad \text{(unbounded fanin)}$$

$$\text{Circuit}(\chi_m) \geq \text{Circuit}^+(G) - 12n \qquad \text{(bounded fanin)}$$

- $\text{Circuit}^+(G) \geq (12+\epsilon)n \Rightarrow \text{Circuit}(\chi_m) = \Omega(n) = \Omega(2^m)$
- Linear monotone bounds for graphs $\Rightarrow$ non-monotone circuit bounds**!**
- G_n = clique K_{n-1} + isolated vertex u_0 = graph represented by $\neg x_{u_0}$
- lover bound for Th_2^n $\Rightarrow$ $\text{Circuit}^+(G_n) \geq 2n - O(1)$ [Sgal 1986] **!**

Proof of Magnification Lemma



- $\chi_{2m}(y_1,\dots,y_m,y_{m+1},\dots,y_{2m})$
- Literal y_i^σ with $i \leq m$ accepts vector $uv \in \{0,1\}^{2m} \iff u(i)=\sigma$

  $\iff$ the OR $\bigvee_{w:w(i)=\sigma} x_w$ accepts $(0,\dots,0,\overset{u}{1},0,\dots,0,\overset{v}{1},0,\dots,0)$

Theorem (Pudlák–Rödl–Savický 1986)

$c \cdot \log_2 n$ boolean sums can be computed with $3cn$ fanin-2 OR gates

The graph-theoretic approach already works !

- $\Sigma_3^{\oplus}$ = Σ_3-circuits with Parity gates on the bottom level
- Only two lower bounds known [Grolmusz 1998, Pudlák–Rödl 2004]
- Using graphs $\Rightarrow$ easy proofs and for many other functions !

Theorem (S.J. 2004)

For every $n \times n$-graph H we have $\Sigma_3^{\oplus}(H) \geq \dfrac{|H|}{n \cdot \text{Clique}(H)}$

- Disjointness Function $DISJ_m(x,y) = 1 \iff \sum_{i=1}^{m} x_i y_i = 0$
- $DISJ_m$ = adjacency function of $n \times n$ Kneser graph H with $n = 2^m$
  - vertices = subsets $u \subseteq \{1,\ldots,m\}$, and u and v adjacent $\iff u \cap v = \emptyset$
- Theorem + Magnification Lemma $\Rightarrow$
  $\Sigma_3^{\oplus}(DISJ_m) \geq \Sigma_3^{\oplus}(H) = n^{\Omega(1)} = 2^{\Omega(m)}$

Single level conjecture for *unbounded* fanin circuits

- Single level circuits = Σ_3^+-circuits = monotone depth-3 circuits
- Unbounded fanin $\Rightarrow$ quadratic savings: $\Sigma_3^+(f_G) \leq 2n$ for all G:

$$f_G(X) = \bigvee_{u \in V} x_u \wedge \Big(\bigvee_{v : uv \in E} x_v \Big)$$

Why interesting? (Valiant 1977 + Magnification Lemma)

$\Sigma_3^+(G) \geq n^\epsilon$ for constant $\epsilon > 0 \Rightarrow$ super-linear lower bound for NC^1 !

But ... monotone depth-3 circuits may be quite powerful:

Theorem (S.J. 2005)

$\Sigma_3^+(G) = O(\Delta \log n)$ where Δ = maximum degree of G

Depth-3 circuits may be too weak!

Problem (Pudlák–Rödl–Savický 1986)

Show that depth-3 circuits for graphs may be far from optimal

Lemma (Magnification Lemma + Lokam 2003)

Depth-3 circuits may be by a factor of $\Omega(\sqrt{\log n})$ worse than optimal ones

Proof.

- Sylvester $n \times n$ graph $H \subseteq \mathbb{F}^r \times \mathbb{F}^r$ with $n = 2^r$ and
  $uv \in H \iff \langle u, v \rangle = 0$
- $IP_r = \sum_{i=1}^r x_i y_i \pmod 2 \;\Rightarrow\;$ characteristic function of H
- $\mathrm{Circuit}^+(H) \le \mathrm{Circuit}(IP_r) = O(r) = O(\log n)$ (Magnific. Lemma)
- $\Sigma_3^+(H) = \Omega(\log^{3/2} n)$ (Lokam 2003)
- $\Rightarrow\; Gap(H) = \Omega(\sqrt{\log n})$

∎

Bounded fanin circuits – The Conjecture

- Single level circuit $\Rightarrow$ only one level of AND gates

$$\bigvee_{i=1}^{t} \left(\bigvee_{u \in A_i} x_u \right) \wedge \left(\bigvee_{v \in B_i} x_v \right)$$

- # of AND gates = nondeterministic communication complexity
- $\Rightarrow$ graph complexity = generalization of communication complexity !

Single Level Conjecture (named so by Lenz and Wegener 1987)

Single-level circuits for quadratic functions are almost optimal:

$$Gap(n) := \max_{n\text{-vertex } G} \frac{\text{single-level complexity of } G \text{ or } f_G}{\text{complexity of } G \text{ or } f_G} = O(1).$$

Algebraic version is true $\Rightarrow$ The Conjecture is born!

- Quadratic functions over $GF(2)$: $f_A(x) = x^\top Ax$
- Model = circuits over $\{\oplus, \wedge, 1\}$ with fanin-2 gates
- Measure = multiplicative complexity = number of $\wedge$-gates
- Single level = sum of products of linear forms = $\sum_{i=1}^{t} L_{i,1} \wedge L_{i,2}$

Theorem (Mirwald–Schnorr 1987)

All optimal circuits for quadratic functions f_A are single level circuits

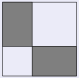
- $\Rightarrow$ for quadratic functions $Gap_{\{\oplus,\wedge,1\}}(n) = 1$
- Would hold also for graphs $\Rightarrow$ lower bounds for $\{\oplus, \wedge, 1\}$-circuits !
- But ... for graphs the result does not hold anymore ...

Algebraic version fails for graphs

Theorem (S.J. 2006)

For graphs $\Rightarrow$ $Gap_{\{\oplus,\wedge,1\}}(n) = \Omega(n/\log n)$ (perfect matching)

Proof

- Single level circuit = sum of products of linear forms
- Linear form (parity) represents "double-clique"  $\Rightarrow$ has rank ≤ 2
- $\Rightarrow$ Single Level Circuit$^+(G) \geq \frac{1}{4}\text{rk}(G)$
- $\Rightarrow$ Single Level Circuit$^+(M_n) = \Omega(n)$ for perfect matching $M_n \subseteq V_1 \times V_2$
- But Circuit$(M_n) = O(\log n)$:
  - $F(X) = \bigwedge_{i=1}^{r} \bigoplus_{w \in S_i} x_w$ with $r = \log n$ and
    $S_i = \{w \ : \ w_i = 0 \text{ if } w \in V_1, \text{ and } w_i = 1 \text{ if } w \in V_2\}$
  - $\bigoplus_{w \in S_i} x_w$ accepts $uv \iff u_i = v_i$
  - $F(X)$ accepts $uv \iff \forall i \ u_i = v_i \iff u = v \iff uv \in M_n$ $\square$

Boolean version over $\{\vee,\wedge,0,1\} \;\Rightarrow\;$ known results

For quadratic functions:

- *Krichevski 1964* $\;\Rightarrow\; Gap(f_{K_n}) = 1$
- *Bloniarz 1979* $\;\Rightarrow\; Gap(f_G) = O(1)$ for almost all quadr. functions
- *Lenz–Wegener 1987* $\;\Rightarrow\; Gap_{\text{mult}}(f_G) \geq 4/3$ for multiplicative complexity
- *Bublitz 1986* $\;\Rightarrow\; Gap_{\text{form}}(f_G) \geq 8/7$ for formulas
- *Amano–Maruoka 2004* $\;\Rightarrow\; Gap(\{f_G\}) \geq 29/28$ for sets of quadr. funct.
- But ... for circuits and single f_G even $Gap(f_G) > 1$ remained unknown !

For graphs:

- *Pudlák–Rödl–Savický 1986*:
  - Single Level $\text{Formula}^+(G) = \Omega(\frac{n^2}{\log n})$
  - $\text{Formula}_{\{\oplus,\wedge,1\}}(G) = O(n\log n) \;\Rightarrow\; \text{Circuit}^+(G) = O(n\log n)$
- $\Rightarrow$ still ... neither $Gap(G) > 1$ nor $Gap_{\text{form}}(G) > 1$ was known !

Monotone bounds ... Why difficult?

- $\text{Circuit}^+(f_G) = \Theta(n^2/\log n)$ for almost all G $\Rightarrow$ counting
- Razborov's method is symmetric $\Rightarrow$ minimum of AND and OR gates
- $\Rightarrow$ cannot yield lower bounds $\text{Circuit}^+(f_G) > n$:

$$f_G(X) = \bigvee_{uv \in E} x_u x_v = \bigvee_{u \in V} x_u \wedge \Big(\bigvee_{v : uv \in E} x_v \Big)$$

Theorem (S.J. 2004)

$G = (V, E)$ is C_3, C_4-free $\Rightarrow$ $\text{Formula}^+(f_G) \geq |E|/2$

For Erdős–Rényi graph G $\Rightarrow$ $\text{Formula}^+(f_G) = \Omega(n^{3/2})$

- But ... no such bound for quadratic functions of saturated graphs !
- Would the Conjecture be true $\Rightarrow$ life would be easy! But ...

Disproof of the Conjecture (bounded fanin circuits)

- For all graphs G:
  - single-level complexity of $f_G = O\left(\frac{n^2}{\log n}\right)$ (Bloniarz, 1979)
  - unrestricted complexity of $f_G = \Omega(n)$ (constant fanin) (trivial)
- $\Rightarrow Gap(n) = O\left(\frac{n}{\log n}\right)$

Theorem: (constant fanin circuits)

Circuit gap $Gap(n) = \Omega\left(\frac{n}{\log^3 n}\right)$ (Sylvester graphs)

Multiplicative gap $Gap_{\text{mult}}(n) = \Omega\left(\frac{n}{\log n}\right)$ (perfect matching)

Formula gap $Gap_{\text{form}}(n) = n^{\Omega(1)}$ (Kneser graphs)

Proof

- Need quadratic lower bound for single level $\Rightarrow$ Razborov cannot help
- What then? $\Rightarrow$ Try a direct argument!

Technical Lemma (General Lower Bound)

$$H \subseteq U \times W \;\Rightarrow\; \text{Single Level Circuit}^{+}(H) \geq \frac{|H|}{\text{Clique}(H)^3}$$

Proof (sketch):

- Single level circuits have the form $\bigvee_{i=1}^{t} \left(\bigvee_{u \in A_i} x_u \right) \wedge \left(\bigvee_{v \in B_i} x_v \right)$
- $\Rightarrow$ relation to disjunktive complexity of boolean sums
- small cliques $\Rightarrow$ small “overlap” of boolean sums (technical part)
- $\Rightarrow$ need many fanin-2 OR gates [Wegener 1980] $\square$

Proof (cntd.)

- Graph is Ramsey graph if $|H| = \Omega(n^2)$ and[3] $\text{Clique}(H) = O(\log n)$
- $\Rightarrow$ Single Level $\text{Circuit}^+(H) = \Omega\left(n^2/\log^3 n\right)$
- $\Rightarrow$ All Ramsey graphs are hard for single level circuits
- Ramsey graphs exist (Erdős, probabilistic argument)
- But ... $\text{Circuit}(H) = \Omega\left(n^2/\log n\right)$ for most such graphs !
- $\Rightarrow$ Need Ramsey graphs with $\text{Circuit}^+(H) = O(n)$

- Idea: take an easy graph and force induced Ramsey subgraph in it
- Sylvester $n \times n$ graph H with $n = 2^r$
  - Vertices = vectors $u \in \mathbb{F}^r$ where $\mathbb{F} = GF(2)$
  - Edges = pairs uv with $\langle u, v\rangle = 0$

[3] ... and $\text{Clique}(\overline{H}) = O(\log n)$, but we don't need this ...

Proof (end)

Lemma (Pudlák–Rödl–Savický 1986 + Berkowitz 1982)

Sylvester graphs have small monotone circuits

Lemma

Sylvester $n \times n$ graph contains an induced Ramsey $\sqrt{n} \times \sqrt{n}$ graph

Proof (inspired by [Pudlák–Rödl, 2004])

- Probabilistic argument $\Rightarrow$ $\exists S \subseteq \mathbb{F}^r$ s.t. $|S| = 2^{r/2} = \sqrt{n}$ and
  $(*)$ $|S \cap V| < r$ for all vector spaces $V \subseteq \mathbb{F}^r$ with $\dim(V) \leq r/2$.
- $A \times B$ clique in $H[S]$ $\Rightarrow$ $A \cdot \mathbf{x} = \mathbf{0}$ for all $\mathbf{x} \in B$
- $\dim(\operatorname{span} A) + \dim(\operatorname{span} B) \leq r$ $\Rightarrow$ w.l.o.g. $\dim(\operatorname{span} A) \leq r/2$
- $\Rightarrow$ $|A| \leq |S \cap \operatorname{span} A| \leq r$ by $(*)$
- $\Rightarrow$ no cliques $K_{r,r}$ in $H[S]$ $\square$

Conclusion

- Graph-theoretic approach to circuit lower bounds?
- $\Rightarrow$ Already works!
- Known methods (Razborov +) do not work for graphs
- Goal: What circuits for graphs look like?
- Most "natural circuits for graphs $\Rightarrow$ single level circuits
- Main message of this talk $\Rightarrow$ single level circuits may be too weak:
  - No Mirwald–Schnorr phenomenon over $\{\oplus, \wedge, 1\}$ for graphs
  - Single level conjecture badly fails over $\{\vee, \wedge, 0, 1\}$
- Unbounded fanin single level (= monotone Σ_3) $\Rightarrow$ still strong enough
- $\Rightarrow$ can yield super-linear lower bound for NC^1 !

What next?

- $a(G)$:= min # of indep. sets covering all non-edges of G
- Expander mixing lemma $\Rightarrow$ $a(G) = \Omega(\sqrt{d})$ for d-regular Ramanujan graphs
- Need robust expanders G: $a(G') \geq$ large even if we remove $(1 - n^{-\epsilon})$ fraction of edges
- Are (dense) Ramanujan graphs robust?

A more “prosaic” problem $P(\epsilon)$

If communication matrix of f in $2m$ variables has $\geq 2^{(1+\epsilon)m}$ zeroes and has no submatrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ then $NCC(f) = \Omega(m)$? Or at least $DNF(f) = 2^{\Omega(m)}$?

- For $\epsilon = 1/2$ $\Rightarrow$ $P(\epsilon)$ = true
- If true for some $\epsilon < 1/2$ $\Rightarrow$ superlinear bound for NC^1 circuits !

Thank you!