Outline

0. Some areas I work in
1. Motivating Results
2. Classical Circuits
3. Quantum Circuits
4. $QAC^0[K] = QAC^0_{wf} = QACC$
5. TC^0 & iterated multiplication
6. Some upper bound results
7. Conclusion

Some Areas I work in

1. Bounded Arithmetic
   - connections between weak fragments of arithmetic & P = NP question, complexity & cryptography
2. Logic Programming & Nonmonotonic Reasoning
   (AI in general)
   Deductive DB's
3. Implicit characterizations of complexity classes.
4. Quantum Circuits

Motivating Results

- Shor's Algorithm for factoring

- Grover's Algorithm for database search

- Moore '99
  Defines classes QAC^0, $QAC^0[k]$ of quantum operators corresponding to classical circuit classes.

- F-R '98, FGHP '98, YY '99
  give upper bds on p-time quantum classes.

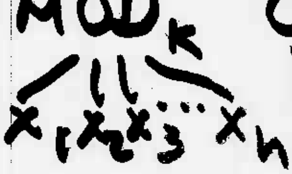
  <u>Ex</u> $NQP = co\text{-}C_=P$

  Can these results be translated to circuit setting?

Classical Circuit Classes

Gates:

Output: 1 iff all $x_i = 1$



Output: 1 iff $\sum_{i=1}^{n} x_i = 0_{mod_K}$

Output: 1 iff $\exists\, x_i = 1$

$\neg x_i$ is 1 iff $x_i = 0$

Consider circuit families built out of these gates, $\{F_n\}_{n=0}^{\infty}$.

Such a family computes a $f^{\underline{n}}$ $\mathbb{N} \to \mathbb{N}$ in the following way: Given input x see how many bits long it is, say n, then feed x into F_n and evaluate.

AC^0 – $f^{\underline{ns}}$ computed by $\{F_n\}$'s when size$(F_n) \le p(n)$ and depth$(F_n) \le d$ for some fixed d

$AC^0(K)$ – allow MOD_K gates.

Remark

FSS, Hastad, Raz, Smolensky

$$AC^0 \subsetneq AC^0[q]$$

$$\neq$$

$$AC^0[p] \subsetneq ACC := \bigcup_k AC^0[k]$$

$q \neq p$ prime

Quantum Circuits

Kronecker Product

$M = [m_{ij}]$
$W = [w_{ij}]$ then $M \otimes W = \begin{bmatrix} m_{11}W & \cdots & m_{1m}W \\ \vdots & \ddots & \\ m_{n1}W & \cdots & m_{nm}W \end{bmatrix}$

Circuit Inputs

Built out of

$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$ $\begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$

$|x_1, \ldots, x_n\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$

So for example

$|0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$

Circuit Gates

(a) $M \in U(2)$

(b) $|x_1 \cdots x_n, x_{n+1}\rangle \mapsto |x_1, \ldots, x_n, f(x_1 \cdots x_n) \oplus x_{n+1}\rangle$
where f is $\wedge$, Mod m, or Mod m, r.

(c) $|x_1, \ldots, x_n, x_{n+1}\rangle \mapsto |x_1 \oplus x_{n+1} \cdots x_n \oplus x_{n+1}, x_{n+1}\rangle$
"fan-out"

(d) $|x_1, \ldots, x_n, x_{n+1}\rangle \mapsto |x_1, \ldots, x_n, x_1 \oplus x_{n+1}\rangle$
or
$|x_1, \ldots, x_n, x_{n+1}\rangle \mapsto |x_1 \oplus x_{n+1}, x_2 \cdots, x_n, x_{n+1}\rangle$
"spaced-not"

Remark

Wang, Sørensen, Mølmer '01 – have proposed a way to directly implement Multi-bit quantum gates without using 1 or 2 bit gates to build them up.

Quantum Classes

A *layer* is a Kronecker product of polynomially many of above types of gates.

QAC^0_{wf} – families of operators $\{F_n\}$ where $F_n \in U(2^{n+p(n)})$ made out of constant number of layers of $U(2)$, quantum AND, fan-out gates. Polynomially many spaced-not layers.

$QAC^0[K]$ – as above except quantum Mod gates instead of fan-out.

$QACC := \cup_K QAC^0[K]$

$QACC^{log}_{pl}$ – allow only log-many spaced not layers.

$QACC^{log}_{gates}$ – allow only log-many gates in circuit.

Fact: (Moore '99) With polynomially many spaced-not layers can make any permutation operator desired. Log-restriction can be viewed as a planarity condition.

$QAC^0[K] = QACC$

Say $\{F_n\}$ QAC^0-reducible to $\{G_n\}$ if can use F_n as gates in some QAC^0 (no fan-in) circuit and by "fixing values" of some lines in this circuit get G_n.

$\{F_n\}$ & $\{G_n\}$ are QAC^0-equivalent if can show each is QAC^0-reducible to other.

Equality $QAC^0[K] = QACC$ means operators in two classes QAC^0-equivalent.

How to prove:

1) Can represent any number $1, \cdots K$ as a tensor product of $\lceil \log_2(K+1) \rceil$ $|0\rangle$'s and $|1\rangle$'s.

1) Let M_q be the operator on $n+1$ such "qudigits" which maps

$$|x_1, \dots, x_n, b\rangle \mapsto |x_1, \dots, x_n, \Sigma x_i + b \bmod q\rangle$$

Let F_q be the operator

$$|x_1, \dots, x_n, b\rangle \mapsto |x_1 + b \bmod q, \dots, x_n + b \bmod q, b\rangle$$

Let H_q be the Hadamard transform

$$H_q|a\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{b=0}^{q-1} \zeta^{ab} |b\rangle$$

k qudigit

$\zeta = e^{\frac{2\pi i}{q}}$

By Barenco et al '95 There is QAC° circuit for this since q fixed.

Can show: $M_q = \left(H_q^{\otimes(n+1)}\right)^{-1} F_q^{-1} H_q^{\otimes(n+1)}$

pf Exercise.

(2) (a) Mod_q and M_q are QAC°-equivalent

(b) F_q and F_2 = fan-out are QAC°-equivalent

pf Hardest case is $M_q \leq_{QAC^0} \mathrm{MOD}_q$

Basic idea is to convert each (q)-qudigit to unary. Since 2^{q} is fixed can do in QAC°.

(3) Use $F_2 \equiv_{QAC^0} M_2 = \mathrm{MOD}_2$ & 1st step result that $\mathrm{MOD}_p \leq_{QAC^0} \mathrm{MOD}_2$

Upper Bounds

Let $\mathcal{C}$ be one of our operator classes.

A language $\underline{L \in N\mathcal{C}}$ if $\exists \{F_n\} \in \mathcal{C}$ and a family $\{\langle \vec{z}_n |\}$ of observations s.t. if $|x| = n$ then $x = x_1 \cdots x_n \in L$ iff

$$|\langle \vec{z}_n | F_n | x_1, \dots, x_n \rangle|^2 > 0$$

Here $\langle \vec{z}_n | := (|\vec{z}_n\rangle)^T$

Conjecture: $NQACC = TC^0$

Can show:

$$NQACC^{\log}_{pl} \subseteq P/poly$$
$$NQACC^{\log}_{gates} \subseteq TC^0$$

To do this need a way to represent amplitudes that can arise in a QACC computation...

Representing Amplitudes

Based on (YY)'s skheme...

Let E be distinct entries that occur in our circuits gates (require fixed with n)

Let A be max algebraic independent subset of E & let $F = \mathbb{Q}(A)$

Let B be a basis of field G generated by $(E - A) \cup \{1\}$ over F.

Can code any α that can arise from applying QACC circuit to input by an elt in G.

Use sequence coding scheme to code elts of G so TC^0 can manipulate them.

Representing $\langle \vec{z}_n | F_n$ as a graph

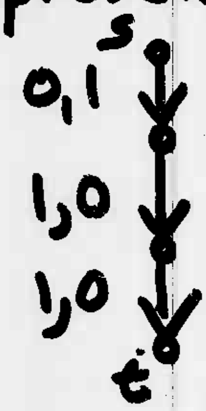
Hope: From graph easy to come up with a TC^0 or P/poly circuit for $\langle \vec{z}_n | F_n | \vec{x} \rangle$

<u>Example</u>:

Consider $\overbrace{\langle 1,0,0 | \mathrm{Mod}_2}^{\langle 1,0,1|} =$

$$\langle 1,0,0 | H_2^{\otimes 3} F H_2^{\otimes 3}$$

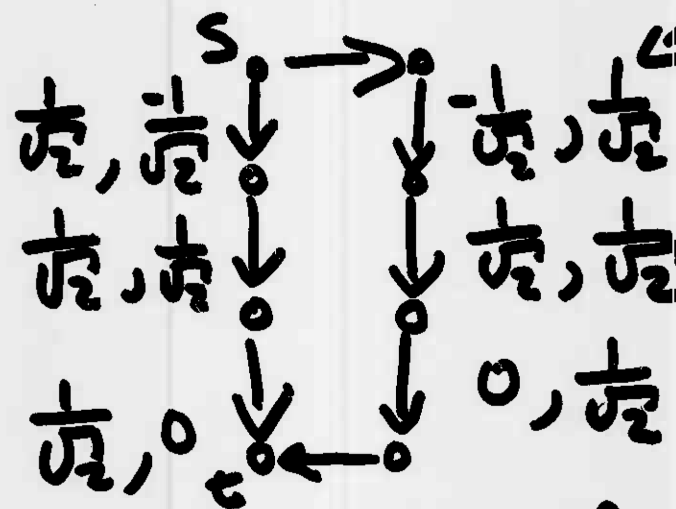
Represent $\langle 1,0,0|$ as



After 1st layer of H_2's

amplitude of $|1,0,1\rangle = \frac{-1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}}$

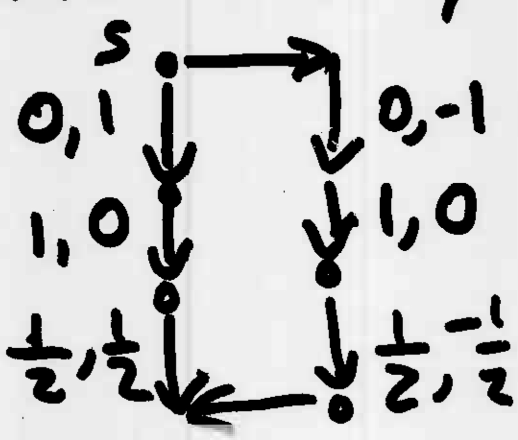
After Fan-out...



Flip of LHS amplitudes

amplitude of $|0,0,0\rangle$
$= \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} + \frac{-1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}}$

After 2nd layer of H_2's



only nonzero vector is $|1,0,1\rangle$ with amplitude 1

Upshots

① Can find a similar correction to do for AND gates.

② Above graphs called tensor graphs. Max Number of vertices of a given height called width. QACC circuits translate to constant width tensor graphs. (Width grows with width of circuit)

<u>Caveat</u> Have to be careful of spaced-not layers.

③ Calculating amplitude of a vector in graph amounts to taking a sum of polynomial product of amplitudes along a path in graph. Log-gates restriction makes sum polynomial size. Gives TC^0 result.

④ For P/poly result...

Since the width is finite can express the amplitude calculation to vertices of height $i+1$ as a finite sum of calculations to height i.

Open Problems

① Get $NQACC \subseteq TC^0$
or $P/poly$.

② Show a problem in NQACC
not in ACC.

③ How hard are fixed levels of
QACC?

④ IS QACC contained in some
fixed level of $qQTC^0$?