Algebraic Problems in Computational Complexity

Pranab Sen
School of Technology and Computer Science,
Tata Institute of Fundamental Research, Mumbai 400005, India
pranab@tcs.tifr.res.in

Guide: Prof. R. K. Shyamasundar
Thesis Supervisor: Prof. J. Radhakrishnan
External Examiner: Prof. M. Sohoni

Thesis defence

Main problems studied in this thesis

Goal of computational complexity: Determine the exact amount of resources required to solve a problem by a mathematical model of computation.

In this thesis, we study some problems in computational complexity, where the models of computation have an algebraic flavour.

Predecessor problem	Quantum cell probe model
Round elimination problem	Quantum communication model
Membership problem	Quantum bit probe model
Computation of $S_n^2(X)$	$\Sigma\Pi\Sigma$ arithmetic circuits

Main results: I

Predecessor problem

$\Omega\left(\min\left\{\frac{\log\log m}{\log\log\log m}, \sqrt{\frac{\log n}{\log\log n}}\right\}\right)$ lower bound on #queries in bounded error address-only quantum cell probe model (a new result even for the classical version). (With Venkatesh, ICALP 2001).

Round elimination problem

$[t, a, b]^A$ quantum protocol for $f^{(n)}$ with worst case error $\delta \Rightarrow$
$[t-1, a, b]^B$ quantum protocol for f with worst case error at most $\delta + O\left(\left(\frac{a}{n}\right)^{1/4}\right)$
(a new result even for the classical version). (With Venkatesh, ICALP 2001).

Main results: II

Membership problem

Tradeoff $\sum_{i=0}^{n} \binom{m}{i} \leq \sum_{i=0}^{nt} \binom{s}{i}$ in the exact quantum bit probe model.
$\Omega\left(\frac{n \log(m/n)}{\epsilon^{1/6} \log(1/\epsilon)}\right)$ lower bound on space for the single query bounded ϵ-error quantum bit probe model. (With Radhakrishnan & Venkatesh, FOCS 2000).

Computing $S_n^2(X)$

Exact bound of $\left\lceil \frac{n}{2} \right\rceil$ over $\mathbb{C}$ for all n.
For the odd cover problem, exact bound of $\left\lceil \frac{n}{2} \right\rceil$ for infinitely many odd and even n (Graham-Pollack theorem mod2). (With Radhakrishnan & Vishwanathan, FSTTCS 2000).

The predecessor problem

- Universe $[m]$.

- Store a subset $S \subseteq [m]$, $|S| \leq n$ (usually $m \gg n$), using s cells each of size w bits.

- Given query $x \in [m]$, find predecessor of x in S making at most t cell probes.

Goal: Use small space and few cell probes. Study tradeoffs between s, w and t.

The quantum cell probe model: I

Set S is stored as a table $T[S]$ of s cells, each cell w bits long. Let $s = 2^r$. Note that the quantum bit probe model is nothing but the quantum cell probe model with $w = 1$.

Storage scheme creates a reversible black box O_S corresponding to the table $T[S]$, similar to the one in e.g. Grover's search algorithm,

$$O_S : |j, b, z\rangle \mapsto |j, b \oplus T[S](j), z\rangle,$$

where j is r qubits long and denotes an address in the table $T[S]$, b is w qubits long and denotes the contents of a cell and z denotes the remaining qubits of the query circuit.

Can feed superpositions to O_S too!

The quantum cell probe model: II

Quantum query scheme with t quantum probes is just a sequence of unitary transformations

$$U_0 \rightarrow O_S \rightarrow U_1 \rightarrow O_S \rightarrow \ldots U_{t-1} \rightarrow O_S \rightarrow U_t,$$

where U_j's are arbitrary unitary transformations that do not depend on the set S stored.
For a query $x \in [m]$, the computation starts in an observational basis state $|x\rangle|0\rangle$.
The result of the query is got by measuring some of the wires in the final state of the circuit.
Worst case ϵ-error scheme means that for every (x, S), the measured answer is wrong with probability at most ϵ.

Address-only quantum cell probe model

$$O_S : |j, b, z\rangle \mapsto |j, b \oplus T[S](j), z\rangle.$$

State vector before an application of O_S is a *tensor product* of a state vector on j, z, depending upon query, S and probe number, and a state vector on b, independent of query and S but maybe depending on probe number.
Intuitively, we are using quantum parallelism over ‘address-lines’ only.

In classical querying, state vector on data lines is $|0\rangle$.
In Grover’s algorithm, state vector on data line is $(|0\rangle - |1\rangle)/\sqrt{2}$.
Høyer, Neerbek and Shi’s algorithm (ICALP 2001) is also address-only!

Results about predecessor: I

Universe $[m]$, store $S \subseteq [m]$, $|S| \le n$, answer predecessor queries.

If $s = n^{O(1)}$, $w = (\log m)^{O(1)}$, then

$$t = \Omega\left(\frac{\log\log m}{\log\log\log m}\right) \text{ as a function of } m,$$

$$t = \Omega\left(\sqrt{\frac{\log n}{\log\log n}}\right) \text{ as a function of } n.$$

This result is in the *address-only* quantum cell probe model.

Results about predecessor: II

Universe $[m]$, store $S \subseteq [m]$, $|S| \leq n$, answer predecessor queries.

The lower bound for predecessor in the address-only quantum cell probe model is actually stronger than what was known earlier, even for classical randomised query schemes. Thus, this result proves a new classical lower bound using quantum information theory!

For classical deterministic schemes, Beame and Fich had proved a similar lower bound; however, the proof in the thesis is much simpler.

A matching classical deterministic upper bound was proved by Beame and Fich.

Two-party quantum communication model

$f : X \times Y \to Z$ is a function. In the communication game for f, Alice is given $x \in X$, Bob is given $y \in Y$, and they have to compute $f(x, y)$.

Alice and Bob hold qubits. Initial superposition is $|x\rangle_A|0\rangle_A|y\rangle_B|0\rangle_B$. Alice and Bob take turns to apply unitary transformations and send qubits. Sending qubits does not change the overall state vector, but rather the ownership of the qubits. At end of protocol, last recipient of qubits performs a measurement on the qubits in her possession to obtain an answer. Worst case error ϵ means that for any $(x, y) \in X \times Y$, the measured answer is equal to $f(x, y)$ with probability at least $1 - \epsilon$.

$[t, a, b]^A$ quantum protocol — t rounds of communication, per round message complexity of Alice and Bob a and b qubits respectively, Alice speaks first.

Quantum round elimination lemma: I

$f : X \times Y \to Z$ is a function. In the communication game for $f^{(n)}$, Alice is given $x_1, \ldots, x_n \in X$, Bob is given $i \in [n]$, $y \in Y$, and a copy of $x_1, \ldots, x_{i-1}$; they have to compute $f(x_i, y)$.

Round elimination lemma: Suppose there is a $[t, a, b]^A$ quantum protocol for $f^{(n)}$ with worst case error δ. Then there is a $[t-1, a, b]^B$ quantum protocol for f with worst case error at most $\delta + O\left(\left(\frac{a}{n}\right)^{1/4}\right)$.

Informally, the first message of Alice cannot contain much information about x_i, if $n \gg a$. Hence, the first round can be eliminated without much increase in the error probability.

Quantum round elimination lemma: II

Miltersen, Nisan, Safra and Wigderson (JCSS 1998) had proved a round elimination lemma for classical randomised protocols. Their proof technique was ad hoc.

The quantum round elimination lemma in this thesis is stronger than the classical round elimination lemma of Miltersen et al.! It plays a crucial role in proving the stronger lower bounds for predecessor. The weaker round elimination lemma of Miltersen et al. was unable to prove such strong bounds. Its proof uses quantum information-theoretic techniques, similar to those employed by Nayak, Ta-Shma, Zuckerman and Klauck (STOC 2001). The information-theoretic approach brings out more clearly the intuition behind round elimination.

The membership problem

- Universe $\mathbf{U}$ of size m.

- Store a subset $S \subseteq \mathbf{U}$, $|S| \leq n$ (usually $m \gg n$), using a table of s bits.

- Answer membership queries "*Is* $x \in S$*?*", using at most t bit probes.

Goal: Use small space and few bit probes. Study tradeoffs between s and t.

Results about membership: I

Universe $\mathbf{U}$, $|\mathbf{U}| = m$, store $S \subseteq \mathbf{U}$, $|S| \leq n$, answer membership queries.

In this thesis, set membership is studied in the quantum bit probe model.

Exact quantum:

$$\sum_{i=0}^{n} \binom{m}{i} \leq \sum_{i=0}^{nt} \binom{s}{i}$$

.

⇒ If $t = 1$, $s \geq m$ (Bit vectors optimal for single bit probe).
⇒ If $s = O(n \log m)$, $t = \Omega(\log m)$ (Fredman-Komlós-Szemerédi scheme optimal for information-theoretic minimum space).

Results about membership: II

Universe $\mathbf{U}$, $|\mathbf{U}| = m$, store $S \subseteq \mathbf{U}$, $|S| \leq n$, answer membership queries.

Two-sided error at most ϵ:

$$\text{If } t = 1,\ s = \Omega\left(\frac{n \log(m/n)}{\epsilon^{1/6} \log(1/\epsilon)}\right).$$

A few extensions: Two-sided bounded error multiple quantum bit probes, simpler or stronger proofs for classical versions.

These lower bounds are similar to the classical lower bounds proved by Buhrman, Miltersen, Radhakrishnan and Venkatesh (STOC 2000) and almost match the classical upper bounds.

ΣΠΣ arithmetic circuits

A ΣΠΣ arithmetic circuit is of the form

$$\sum_{i=1}^{r} \prod_{j=1}^{s_i} L_{ij}(X),$$

where each L_{ij} is a (possibly inhomogeneous) linear form in variables $X_1, \ldots, X_n$.

In homogeneous ΣΠΣ circuits, all the $L_{ij}(X)$ are homogeneous i.e. have constant term zero.
Or else the circuit is said to be inhomogeneous.

Computing $S_n^2(X)$ using $\Sigma\Pi\Sigma$ circuits

We want to compute the degree two elementary symmetric polynomial

$$S_n^2(X_1, \ldots, X_n) \triangleq \sum_{1 \le i < j \le n} X_i X_j,$$

using $\Sigma\Pi\Sigma$ arithmetic circuits i.e. we want to write $S_n^2(X_1, \ldots, X_n)$ in the form

$$S_n^2(X_1, \ldots, X_n) = \sum_{i=1}^{r} \prod_{j=1}^{s_i} L_{ij}(X).$$

We want upper and lower bounds on the number of multiplication gates required i.e. on r, in such an expression.

This problem has connections to graph theory!

Graph covering problems and $S_n^2(X_1, \ldots, X_n)$

Graham-Pollack problem: Cover a complete graph by complete bipartite graphs such that each edge is covered *exactly once*. Exact bound of $n-1$ known earlier.
Odd cover problem: Cover a complete graph by complete bipartite graphs such that each edge is covered an *odd number* of times. Trivial upper bound of $n-1$. A lower bound of $\left\lfloor \frac{n}{2} \right\rfloor$ known earlier (Babai-Frankl).

The above problems are related to the number of multiplication gates in ΣΠΣ circuits for $S_n^2(X_1, \ldots, X_n)$, over the fields $\mathbb{R}$ and GF(2) respectively.

Results about computing $S_n^2(X_1, \ldots, X_n)$

Find bounds on r in $S_n^2(X_1, \ldots, X_n) = \sum_{i=1}^{r} \prod_{j=1}^{s_i} L_{ij}(X)$.

Exact bound of $n-1$ on the number of multiplication gates for computing $S_n^2(X_1, \ldots, X_n)$ if the underlying field is $\mathbb{Q}, \mathbb{R}$.
Exact bound of $\left\lceil \frac{n}{2} \right\rceil$ if the underlying field is $\mathbb{C}$.

Exact bound of $\left\lceil \frac{n}{2} \right\rceil$ for infinitely many even and odd n for the odd cover problem.

Similar results for the $1 \bmod p$ cover problem and for computing $S_n^2(X_1, \ldots, X_n)$ over GF(p^r) p odd. In each case, bounds are exact for infinitely many n.

Conclusions

Lower bounds for predecessor in the address-only quantum cell probe model.

A quantum round elimination lemma — used to show rounds vs communication tradeoffs for various communication problems.

Lower bounds for membership in the quantum bit probe model.

Bounds for computing $S_n^2(X_1, \ldots, X_n)$ using $\Sigma\Pi\Sigma$ circuits over various fields, and bounds for the odd cover problem.

Further work

Lower bounds in the general quantum cell probe model.

Using the round elimination technique to prove lower bounds for other data structure (e.g. approximate nearest neighbour on Hamming cube) and communication complexity problems. Quantum lower bound for pointer chasing already done (with Jain and Radhakrishnan, FOCS 2002 and FSTTCS 2002). An important open problem is rounds versus communication tradeoffs for set disjointness. Recently, Razborov (unpublished) proved an $\Omega(\sqrt{n})$ quantum lower bound for set disjointness.

Proving super polynomial lower bounds for $\Sigma\Pi\Sigma$ circuits over infinite fields, computing an explicit function.