# The detectability lemma and quantum gap amplification 

Dorit Aharonov ${ }^{1}$, Itai Arad ${ }^{1}$, Zeph Landau ${ }^{2}$ and Umesh Vazirani ${ }^{2}$<br>${ }^{1}$ School of Computer Science and Engineering,<br>The Hebrew University,<br>Jerusalem, Israel<br>${ }^{2}$ Electrical Engineering and Computer Science, UC Berkeley, California, USA

October 2, 2009

## Quantum Hamiltonian complexity



## CSP in quantum language

## MAX-3-SAT

## Settings:

- $n$ bits: $x_{1}, \ldots x_{n}$
- $M$ constraints:

$$
f\left(x_{1}, \ldots, x_{n}\right)=C_{1} \wedge \cdots \wedge C_{M}
$$

- $C_{i}$-3-local CNF clause

Goal: find the minimal possible \# of violations

## Example:

$C_{i}=\left(x_{k} \vee \bar{x}_{\ell} \vee x_{m}\right)$
Violating when $\left(x_{k}, x_{\ell}, x_{m}\right)=(0,1,0)$

MAX-3-SAT - in quantum language

## Settings:

- Hilbert space of $n$ qubits $-2^{n}$ basis states:

$$
|00 \cdots 00\rangle,|00 \cdots 01\rangle, \ldots,|11 \cdots 11\rangle
$$

- Hamiltonian with $M$ terms:

$$
H=Q_{1}+\ldots+Q_{M}
$$

- $Q_{i}-3$-local "classical projections"

Goal: approximate the lowest eigenvalue of $H: \lambda(H)=0 \quad$ or $\quad \lambda(H) \geq 1$.


$$
\text { CSP is satisfiable } \Leftrightarrow \lambda(H)=0
$$

Moving to eigenvectors and eigenvalues
Local Hamiltonian: $H=Q_{1}+Q_{2}+\ldots \quad 2^{n} \times 2^{n}$ matrix
$C_{i}=\left(x_{k} \vee \bar{x}_{\ell} \vee x_{m}\right)$
Violating when $\left(x_{k}, x_{\ell}, x_{m}\right)=(0,1,0)$


Eigenvectors: $H\left|x_{1}, \ldots, x_{n}\right\rangle=(\#$ violations $)\left|x_{1}, \ldots, x_{n}\right\rangle$

Eigenvalue of $\left|x_{1}, \ldots, x_{n}\right\rangle$ : \# of violations.
$\lambda(H)=$ Lowest eigenvalue $=$ minimal \# of violations.

The problem: Decide whether $\lambda(H)=0 \quad$ or $\quad \lambda(H) \geq 1$

## Moving to the general quantum CSP

## Quantum CSP (The Local Hamiltonian problem)

$H=\sum_{i=1}^{M} Q_{i} \quad$ general local projections

$$
\lambda(H)=\text { lowest eigenvalue of } H
$$

$$
\text { Decide: } \lambda(H)=0 \quad \text { or } \quad \lambda(H) \geq \frac{1}{\operatorname{poly}(n)}
$$

## Note:

$Q_{i}$ are no longer diagonal in the standard basis, and the eigenvectors of $H$ are superpositions:

$$
|\psi\rangle=\overbrace{a_{1}|0 \cdots 00\rangle+a_{2}|0 \cdots 01\rangle+\ldots}^{2^{n} \text { terms }}
$$

A different view on LH:

$$
\begin{aligned}
\lambda(H) & =\min _{\psi}\langle\psi| H|\psi\rangle \\
& =\min _{\psi}\langle\psi| \sum_{i} Q_{i}|\psi\rangle \\
& =\min _{\psi} \sum_{i}\langle\psi| Q_{i}|\psi\rangle
\end{aligned}
$$

$$
\begin{aligned}
0 \leq\langle\psi| Q_{i}|\psi\rangle \leq 1- & \text { The energy of the constraint: } \\
& \text { how much it is violated. }
\end{aligned}
$$

(compare to 0 or 1 in the classical case)

## Hamiltonian Complexity - The quantum analog of CSP

## Quantum NP (QMA)

Decision problems that can be solved with a quantum witness $|\psi\rangle$ and a polynomial quantum verifier $V_{x}$.

$$
\begin{array}{ll}
x \in L: & \exists\left|\psi_{x}\right\rangle \text { s.t. } \operatorname{Pr}\left[V\left(x,\left|\psi_{x}\right\rangle\right)=\text { yes }\right] \geq 2 / 3, \\
x \notin L: & \forall|\phi\rangle, \operatorname{Pr}[V(x,|\phi\rangle)=\text { yes }] \leq 1 / 3 .
\end{array}
$$



## Quantum Cook-Levin

The Local-Hamiltonian problem is QMA-complete (Kitaev, 98).

- Inclusion is the easy direction
- Hardness is similar to Cook-Levin - but with some quantum twists.


## Central results in Hamiltonian Complexity

Many results and techniques can be imported from CSP to Hamiltonian complexity:

- Reductions using Gadgets
- 2-Local (even planar) Hamiltonian is QMA complete
- Satisfaction Threshold
- Lovasz local lemma

But sometimes things are different:

- Local Hamiltonian in 1d is QMA-complete (but 1d CSP is in P).

Aharonov, van Dam, Kempe, Landau, Lloyd, Regev '04
Kempe, Kitaev, Regev '04
Oliveira, Terhal '05
Najag '07
Shondhi '09
Bravyi '09
Ambainis, Kempe, Sattath '09

> What about Quantum PCP (QPCP) ?

## Quantum PCP

Two ways to formulate the QPCP conjecture:

## QPCP conjecture I

$\forall L \in$ QMA there is a quantum verifier that has access to only $q$ random qubits from the witness.

Quantum reduction
$\qquad$

## QPCP conjecture II

Deciding whether

- $\lambda(H)=0$ or
- $\lambda(H) \geq c \cdot M$
is QMA-hard.

This is, however, a difficult problem

## Difficulties in proving QPCP

## Main Problem: no cloning <br> There is no quantum transformation $|\psi\rangle|0\rangle \mapsto|\psi\rangle|\psi\rangle$ for all $|\psi\rangle$

- No cloning was thought to prevent QECCs - but QECCs exist!
- QPCP seems to require even more (QECCs are not locally decodable)

Possible implications of resolving this question:


We focus on a central ingredient in Dinur's PCP proof, which does not require cloning: Gap Amplification

## What we want to amplify

## In the Classical case

UNSAT $\xlongequal{\text { def }} \frac{\min \text { \# violations }}{M}$

Find an efficient transformation to a new CSP s.t.,


## In the Quantum case

QUNSAT $\xlongequal{\text { def }} \frac{\lambda(H)}{M}$

Find an efficient transformation to a new L.H. s.t.,

QUNSAT


The probability of detecting a violation in a random constraint

## Classically:

$M$ constraints

violations
$p$ - Probability of picking a violated constraint

## Quantumly:

## Quantum Measurement



In our case, when measuring $Q_{i}$ :

$$
\begin{aligned}
\operatorname{Pr}[1] & =\| Q_{i}|\psi\rangle \|^{2}=\langle\psi| Q_{i}|\psi\rangle \\
& =\text { constraint's energy }
\end{aligned}
$$

The probability of measuring a violation for a random $i$.

$$
p=\frac{\# \text { of violations }}{M} \geq \mathrm{UNSAT}
$$

$$
p=\frac{1}{M} \sum_{i}\langle\psi| Q_{i}|\psi\rangle=\frac{\lambda(H)}{M} \geq \text { QUNSAT }
$$

We want to amplify the probability of measuring a violation

## Amplification by repitition

## Classically

- Pick $t$ random constraints
- Probability of at least 1 violation:

$$
\operatorname{Pr}=1-(1-p)^{t} \simeq t \cdot p
$$

- New system size: $M^{t}$

violations


## Quantumly, this also works:

- Choose $t$ random constraints
- Measure them one after the other
- After every measurement, the system collapses into a new state: $\left|\psi_{1}\right\rangle \rightarrow\left|\psi_{2}\right\rangle \rightarrow \cdots \rightarrow\left|\psi_{t}\right\rangle$, but always:

$$
\frac{\sum_{i}\left\langle\psi_{j}\right| Q_{i}\left|\psi_{j}\right\rangle}{M} \geq \frac{\lambda(H)}{M}
$$

- Probability of measuring at least one violation:

$$
\operatorname{Pr} \geq 1-(1-\lambda(H) / M)^{2} \simeq t \cdot \lambda(H) / M
$$

## Amplification with expanders

## Ajtai et al, Impagliazzo \& Zuckerman - RP \& BPP amp'



## Expander graphs

Taking a $t$-walk on a $d$-regular expander graph is almost like picking $t$ random edges.
Advantage: The new system is much smaller: $M d^{t}$ (instead of $M^{t}$ )


## Quantum Conspiration?

## Conspiration Theory

- Classical correlations decay exponentially fast on an expander, but is this also true for quantum correlations?
- How do we know that the expander is "random enough"? - Can the system trick us by collapsing adversely ?



## Quantum World

Classical World

- Classically: well-defined partition.
- Quantumly: no assignment $\Rightarrow$ no partition.


Energy distribution


- Is there a distribution of assignments? For two constraints $A, B, \operatorname{Pr}(A=1, B=0)$ is not well defined:

$$
\operatorname{Pr}[(A=1) \rightarrow(B=0)]=\|(I-B) A|\psi\rangle\left\|^{2} \neq\right\| A(I-B)|\psi\rangle \|^{2}=\operatorname{Pr}[(B=0) \rightarrow(A=1)]
$$

$A$ and $B$ do not commute $\Rightarrow$ no distribution over assignments

## Our Results

## Quantum Gap Amplification

Consider a quantum CSP problem on a $d$-regular expander graph $G=(V, E)$ with a second largest eigvenvalue $0<\lambda<1$. The edges are projections and the vertices are qudits of dimension $W$.


Let $G^{t}$ be the hyper graph of $t$-walks derived from $G$, and for each such $t$-walk define a projection into the intersection of all accepting subspaces along the walk.

Then:

$$
\operatorname{QUNSAT}\left(G^{t}\right) \geq c(\lambda) K(q, d) \min (t \cdot \operatorname{QUNSAT}(G), 1)
$$

## Layers



- Typically, constraints can be arranged in a finite number $g$ of layers.
- In a fixed layer, all projections commute and can be measured simultaneously there exists an underlying joint probability distribution.
- With respect to one layer, we have a distribution of classical systems:


We can use the classical PCP result on each member.

- There are only $g$ layers $\Rightarrow$ there must be a layer with a constant energy.

But there's a problem . . .

## The problem (yet another conspiration)

- It is trivial to satisfy all constraints in one fixed layer.
- But not simultaneously in all layers (because $\lambda(H)>0$ ).
- What if the violation/satisfation distribution in every layer conspires to be:



## No amplification:

- In the "no violations" part there is no amplification because all constraints are satisfied.
- In the "full violations" part there is no amplification because we have reached the maximum.

We must somehow rule out this possibility if we want to show amplification

## The detectability lemma

The detectability lemma ( $\ell=0$ case)

## Settings:

$\Rightarrow \Pi^{(j)}$ is the projection into the satisfying subspace of the $j$ 'th layer
$\Rightarrow$ Minimal energy is $\epsilon_{0} \stackrel{\text { def }}{=} \lambda(H)>0$
$\Rightarrow$ Projections are taken from a fixed set.

## Then:

$$
\| \Pi^{(1)} \cdots \Pi^{(g)}|\psi\rangle \|^{2} \leq \frac{1}{\epsilon_{0} / c+1} \simeq 1-\epsilon_{0} / c
$$

where $c$ is constant independent of $n$.

In a sequential measurent of all layers, the probability of not detecting any violations is bounded away from 1 by a constant.

## Corollary

There must be at least one layer $j$ with a constant projection on the violating subspace

$$
\|\left(I-\Pi^{(j)}\right)|\psi\rangle \| \geq c^{\prime}
$$

## General outline of the proof

- Define

$$
|\Omega\rangle \stackrel{\text { def }}{=} \Pi^{(1)} \cdots \Pi^{(g)}|\psi\rangle
$$

We wish to show $\|\Omega\|^{2} \leq \frac{1}{\epsilon_{0} / c+1}$.

- Note:

$$
\|\Omega\|^{2} \epsilon_{0} \leq\langle\Omega| H|\Omega\rangle
$$

- We prove:

$$
\begin{gathered}
\langle\Omega| H|\Omega\rangle \leq c\left(1-\|\Omega\|^{2}\right) \\
\Downarrow \\
\|\Omega\|^{2} \epsilon_{0} \leq c\left(1-\|\Omega\|^{2}\right) \\
\Downarrow \\
\|\Omega\|^{2} \leq \frac{1}{\epsilon_{0} / c+1}
\end{gathered}
$$

- In the commuting case, $\langle\Omega| H|\Omega\rangle=0$ (trivial)
- In the general case, we show that energy contribution due to non-commuteness is exponentially decreasing.
- We must find a way to quantify non-commuteness.


## The XY decomposition I - Pyramids

## Pyramids

- For every projection $Q$, we define a set of projections $\operatorname{Pyr}[Q]$
- $H_{p y r}$ - The supporting Hilbert space.



## The XY decomposition

$$
\begin{aligned}
H_{p y r} & =X \oplus Y \\
X & =\text { common eigenvectors } \\
Y & =\text { The rest } \\
P_{X}, P_{Y} & =\text { Projections to } X, Y
\end{aligned}
$$

## Observations:

- $P_{X}, P_{Y}$ commute with all $Q^{\prime} \in \operatorname{Pyr}[Q]$
- $\left\|P_{Y}\left(\prod_{Q^{\prime} \in \operatorname{Pyr}[Q]} Q^{\prime}\right) P_{Y}\right\| \leq \theta<1$
- If the projections are drawn from a fixed set, $\theta<1$ is constant!


## The XY decomposition II - Ponzis

A Ponzi is a set of constraints from a fixed layer, whose pyramids don't intersect


- A constant number of Ponzi's is needed to cover all constraints
- $E_{p o n z}$ - The energy operator of a Ponzi.
- The entire Hilbert space is decomposed in terms of XY sectors $\nu$ :

$$
\begin{aligned}
\text { An XY sector: } \nu & =(X, X, Y, X, Y, \ldots) \\
\text { Projection onto } \nu: P_{\nu} & =P_{X} \otimes P_{X} \otimes P_{Y} \otimes P_{X} \cdots \\
|\nu| & =\text { No. of } Y \text { spaces } \\
|\Omega\rangle & =\sum_{\nu} P_{\nu}|\Omega\rangle \stackrel{\text { def }}{=} \sum_{\nu}\left|\Omega_{\nu}\right\rangle
\end{aligned}
$$

- $E_{\text {ponz }}$ commutes with the decomp':

$$
\langle\Omega| E_{\text {ponz }}|\Omega\rangle=\sum_{\nu}\left\langle\Omega_{\nu}\right| E_{p o n z}\left|\Omega_{\nu}\right\rangle
$$

## The energy of Ponzi



Exponential decay: $\left\|P_{\nu} D P_{\nu}\right\| \leq \theta^{|\nu|}$

- Only the Y pyramids contribute to $\left\langle\Omega_{\nu}\right| E_{\text {ponz }}\left|\Omega_{\nu}\right\rangle$, but their norm decays exponentially!

$$
\left\langle\Omega_{\nu}\right| E_{p o n z}\left|\Omega_{\nu}\right\rangle \leq|\nu| \theta^{|\nu|}\left\|\phi_{\nu}\right\|^{2}
$$

- We obtain an upper bound: $\langle\Omega| E_{\text {ponz }}|\Omega\rangle \leq \sum_{s=0}^{\infty} s \theta^{s}$.


## The energy of Ponzi



Exponential decay: $\left\|P_{\nu} D P_{\nu}\right\| \leq \theta^{|\nu|}$

- Only the Y pyramids contribute to $\left\langle\Omega_{\nu}\right| E_{\text {ponz }}\left|\Omega_{\nu}\right\rangle$, but their norm decays exponentially!

$$
\left\langle\Omega_{\nu}\right| E_{p o n z}\left|\Omega_{\nu}\right\rangle \leq|\nu| \theta^{|\nu|}\left\|\phi_{\nu}\right\|^{2}
$$

- We obtain an upper bound: $\langle\Omega| E_{\text {ponz }}|\Omega\rangle \leq \sum_{s=0}^{\infty} s \theta^{s}$.


## Open questions

- The quantum amplification lemma is trivial to prove when all the projections commute (one does not need the detectability lemma). Still it is not clear:
- if the quantum PCP can be proved for commuting Hamiltonians
- what is the complexity of this special class? is it NP? QMA ?
- Can the XY decomposition or the detectability lemma be used elsewhere to handle the non-commuteness of the LH problem?
- Are there any interesting implications of the detectability lemma and the XY decomposition to solid-state physics?
- Currently, the detectability lemma allows us an RP type of amplification (one-sided errors). Can it be generalized to prove a BPP type of amplification (two-sided errors) ?
- What is the right definition of quantum PCP? (one-sided errors/two sided errors?)
- Can we prove a quantum PCP with exponential witness ?
- If there is no quantum PCP theorem, then what is the complexity of approximating QUNSAT $(H)$ up to a constant? It must be NP-hard - but is it inside NP?


## Open questions

- The quantum amplification lemma is trivial to prove when all the projections commute (one does not need the detectability lemma). Still it is not clear:
- if the quantum PCP can be proved for commuting Hamiltonians
- what is the complexity of this special class? is it NP? QMA ?

$$
0
$$ handle the non-commuteness of the LH problem?

- Are there any interesting implications of the detectability lemma and the $X Y$ decomposition to solid-state physics?
- Currently, the detectability lemma allows us an RP type of amplification (one-sided errors). Can it be generalized to prove a BPP type of amplification (two-sided errors) ?
- What is the right definition of quantum PCP? (one-sided errors/two sided errors?)
- Can we prove a quantum PCP with exponential witness ?
- If there is no quantum PCP theorem, then what is the complexity of approximating QUNSAT $(H)$ up to a constant? It must be NP-hard - but is it inside NP?


## Open questions

- The quantum amplification lemma is trivial to prove when all the projections commute (one does not need the detectability lemma). Still it is not clear:
- if the quantum PCP can be proved for commuting Hamiltonians
- what is the complexity of this special class? is it NP? QMA ?
- Can the $X Y$ decomposition or the detectability lemma be used elsewhere to handle the non-commuteness of the LH problem?
- Are there any interesting implications of the detectability lemma and the XY decomposition to solid-state physics?
- Currently, the detectability lemma allows us an RP type of amplification (one-sided errors). Can it be generalized to prove a BPP type of amplification (two-sided errors) ?
- What is the right definition of quantum PCP? (one-sided errors/two sided errors?)
- Can we prove a quantum PCP with exponential witness ?
- If there is no quantum PCP theorem, then what is the complexity of approximating QUNSAT ( $H$ ) up to a constant? It must be NP-hard - but is it inside NP?


## Open questions

- The quantum amplification lemma is trivial to prove when all the projections commute (one does not need the detectability lemma). Still it is not clear:
- if the quantum PCP can be proved for commuting Hamiltonians
- what is the complexity of this special class? is it NP? QMA ?
- Can the $X Y$ decomposition or the detectability lemma be used elsewhere to handle the non-commuteness of the LH problem?
- Are there any interesting implications of the detectability lemma and the $X Y$ decomposition to solid-state physics?
- Currently, the detectability lemma allows us an RP type of amplification (one-sided errors). Can it be generalized to prove a BPP type of amplification (two-sided errors) ?
- What is the right definition of quantum PCP? (one-sided errors/two sided errors?)
- Can we prove a quantum PCP with exponential witness ?
- If there is no quantum PCP theorem, then what is the complexity of approximating QUNSAT $(H)$ up to a constant? It must be NP-hard - but is it inside NP?


## Open questions

- The quantum amplification lemma is trivial to prove when all the projections commute (one does not need the detectability lemma). Still it is not clear:
- if the quantum PCP can be proved for commuting Hamiltonians
- what is the complexity of this special class? is it NP? QMA ?
- Can the $X Y$ decomposition or the detectability lemma be used elsewhere to handle the non-commuteness of the LH problem?
- Are there any interesting implications of the detectability lemma and the $X Y$ decomposition to solid-state physics?
- Currently, the detectability lemma allows us an RP type of amplification (one-sided errors). Can it be generalized to prove a BPP type of amplification (two-sided errors) ?
- What is the right definition of quantum PCP? (one-sided errors/two sided errors?)
- Can we prove a quantum PCP with exponential witness ?
- If there is no quantum PC.P theorem then what is the complexity of approximating


## Open questions

- The quantum amplification lemma is trivial to prove when all the projections commute (one does not need the detectability lemma). Still it is not clear:
- if the quantum PCP can be proved for commuting Hamiltonians
- what is the complexity of this special class? is it NP? QMA ?
- Can the $X Y$ decomposition or the detectability lemma be used elsewhere to handle the non-commuteness of the LH problem?
- Are there any interesting implications of the detectability lemma and the $X Y$ decomposition to solid-state physics?
- Currently, the detectability lemma allows us an RP type of amplification (one-sided errors). Can it be generalized to prove a BPP type of amplification (two-sided errors) ?
- What is the right definition of quantum PCP? (one-sided errors/two sided errors?)
- Can we prove a quantum PCP with exponential witness?
- If there is no quantum PCP theorem, then what is the complexity of approximating


## Open questions

- The quantum amplification lemma is trivial to prove when all the projections commute (one does not need the detectability lemma). Still it is not clear:
- if the quantum PCP can be proved for commuting Hamiltonians
- what is the complexity of this special class? is it NP? QMA ?
- Can the $X Y$ decomposition or the detectability lemma be used elsewhere to handle the non-commuteness of the LH problem?
- Are there any interesting implications of the detectability lemma and the $X Y$ decomposition to solid-state physics?
- Currently, the detectability lemma allows us an RP type of amplification (one-sided errors). Can it be generalized to prove a BPP type of amplification (two-sided errors) ?
- What is the right definition of quantum PCP? (one-sided errors/two sided errors?)
- Can we prove a quantum PCP with exponential witness ?
- If there is no quantum PCP theorem, then what is the complexity of approximating
QUNSAT $(H)$ up to a constant? It must be NP-hard - but is it inside NP?


## Open questions

- The quantum amplification lemma is trivial to prove when all the projections commute (one does not need the detectability lemma). Still it is not clear:
- if the quantum PCP can be proved for commuting Hamiltonians
- what is the complexity of this special class? is it NP? QMA ?
- Can the $X Y$ decomposition or the detectability lemma be used elsewhere to handle the non-commuteness of the LH problem?
- Are there any interesting implications of the detectability lemma and the $X Y$ decomposition to solid-state physics?
- Currently, the detectability lemma allows us an RP type of amplification (one-sided errors). Can it be generalized to prove a BPP type of amplification (two-sided errors) ?
- What is the right definition of quantum PCP? (one-sided errors/two sided errors?)
- Can we prove a quantum PCP with exponential witness ?
- If there is no quantum PCP theorem, then what is the complexity of approximating QUNSAT $(H)$ up to a constant? It must be NP-hard - but is it inside NP?

