PONDERING ABOUT

QPCP's

(QUANTUM PROBABILISTICALLY CHECKABLE PROOFS)

OR:

CAN ENERGY GAPS OF LOCAL HAMILTONIANS BE AMPLIFIED?

DORIT AHARONOV
HEBREW UNIVERSITY

ONGOING WORK WITH

ITAI ARAD
U.C. BERKELEY

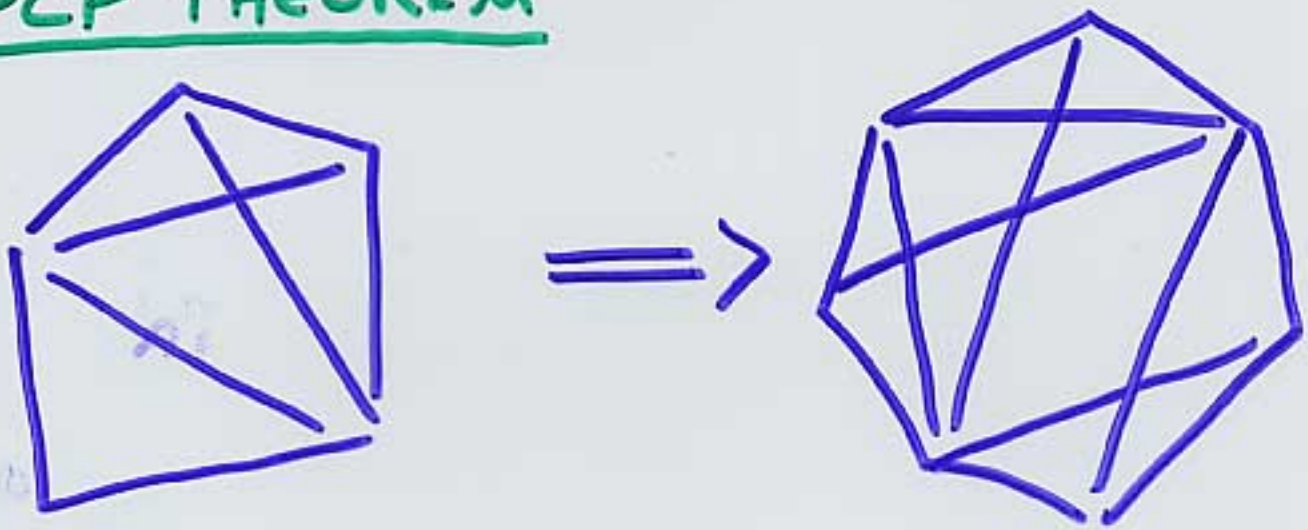
PCP

$|E| = m$

NP-HARD TO DECIDE:

$$\frac{gv}{m} = 0 \quad \text{OR} \quad \frac{gv}{m} \geq \frac{1}{m}$$

PCP THEOREM



G $\qquad\qquad$ G'

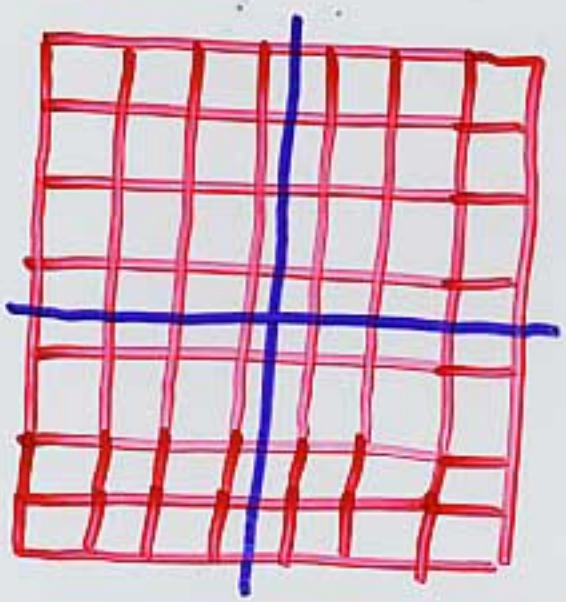
$$\frac{gv(G)}{m} = 0 \longrightarrow \frac{gv(G')}{m'} = 0$$

$$\frac{gv(G)}{m} \geq \frac{1}{m} \longrightarrow \frac{gv(G')}{m'} = \text{CONST!}$$

} NP HARD !

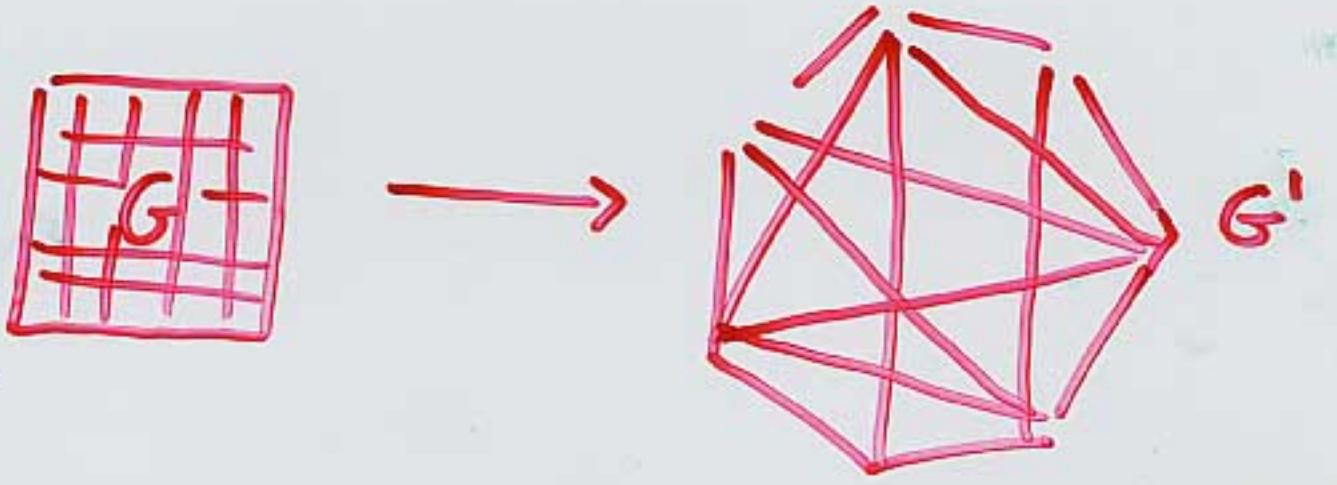
INDEED, PROBABILISTICALLY CHEAKABLE PROOF !

BUT....



ISN'T THIS A POLYTIME ALG FOR $gv \pm \frac{1}{\ell} \cdot m$?

NO PCP IN DIM = CONST



PCP WORKS WITH HIGHLY CONNECTED GRAPHS (EXPANDERS..)

HISTORY

BABAI, FORTNOW, LEVIN, SZEGEDY
BABAI, FORTNOW, LUND
GOLDWASSER, MICALI, RACKOFF
} [91, 92]

ARORA, SAFRA
ARORA, LUND
MOTWANI, SUDAN, SZEGEDY
} q = CONST!

$q \downarrow$

BELLARE, GOLDWASSER, LUND, RUSSELL
BELLARE, COPPERSMITH, HASTAD, KIWI, SUDAN

HASTAD $q = 3$ BITS!

NEW PROOF: DINUR [06]

QUANTUM NP [KITAEV '99]

$$H = \sum_{i \sim j} H_{ij}$$ ← PROJECTIONS

LOCAL HAMILTONIAN PROBLEM

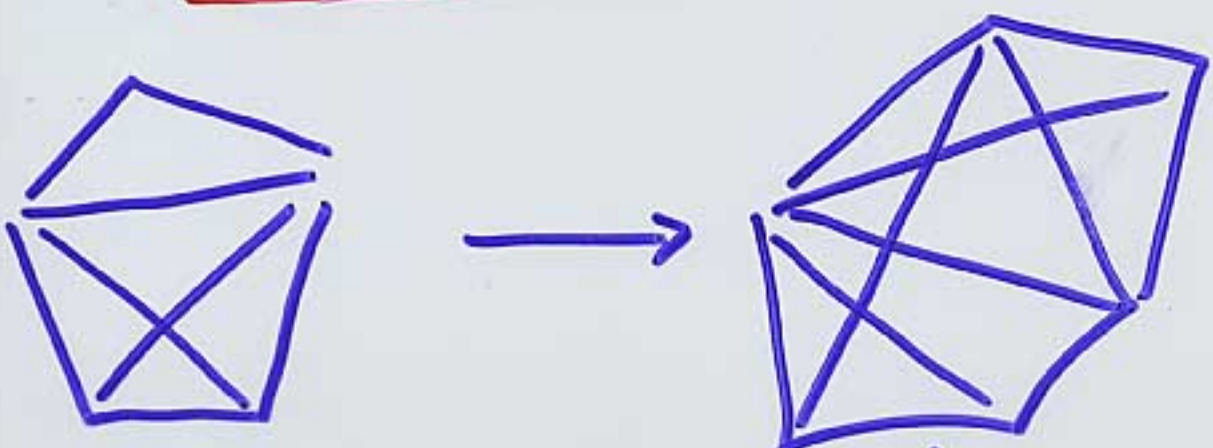
$g_0(H) = 0$ OR $g_0(H) \geq \frac{1}{\text{poly}(m)}$

CAN BE VERIFIED EASILY (BY A QUANTUM VERIFIER!)

IF CORRECT : JUST GIVE THE $|gs\rangle$.

LOCAL HAMILTONIAN IS QNP - COMPLETE.

QUANTUM PCP ?



$g_0(H) = 0 \longrightarrow g_0(H') = 0$

$g_0(H) \geq \frac{1}{m} \longrightarrow g_0(H') \geq \text{CONST}!$

POSSIBLE IMPLICATIONS OF QPCP

1) Inability to Approx $g_s(H) \pm \varepsilon.m$

(EVEN WITH A Q. COMPUTER)

2) SPECTRAL GAP AMPLIFICATIONS.

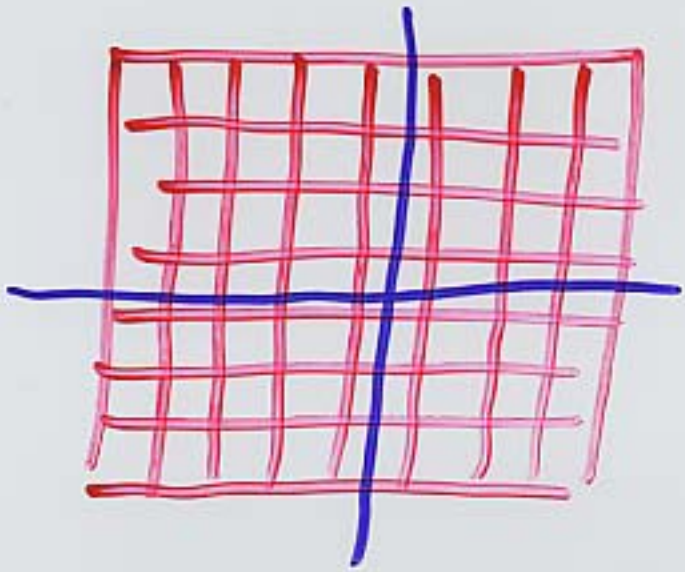
PROMISE GAP IN QPCP $\neq$ SPECTRAL GAP.

BUT... DINUR'S CONSTRUCTION CAN BE MODIFIED TO AMPLIFY SPECTRAL GAP.

* $H \longrightarrow H'$ W. AMPLIFIED SPECTRAL GAP.

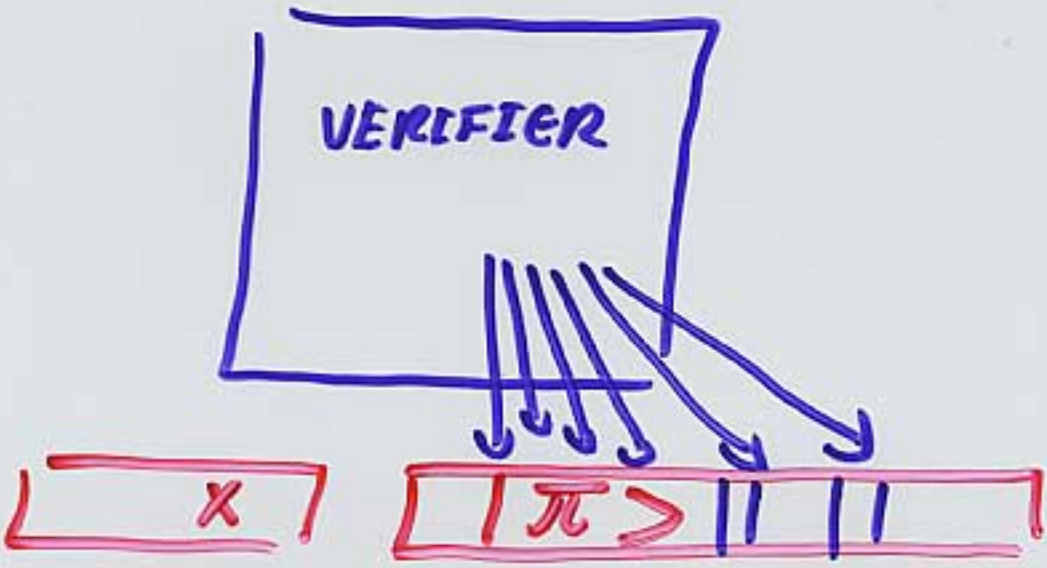
* IMPLICATIONS TO FAULT TOLERANT ADIABATIC COMPUTATION.

ONCE AGAIN - DIM ≠ CONST



IF DIM BOUNDED - CAN ALWAYS APPROX TO WITHIN $\pm \varepsilon_0 m$ $\forall \varepsilon_0$.

MAYBE WE CAN PROVE WEAKER QPCP THEOREMS ?



1) MAYBE ALLOW V TO ACCESS $\log n$ LOCATIONS ?

2) MAYBE PROVE

$$QMA = \left\{ g v = 0 \text{ OR } g v > \frac{m}{\log m} \right\}$$

3) MAYBE ALLOW V ACCESS TO RANDOMLY CHOSEN q = CONST QUBITS, BUT GIVE HIM THE FULL MATRIX?

(MIXING-QPCP)

OUTLINE OF REST OF TALK:

DINUR'S PROOF -

A SKETCH...

OUR RESULTS.

QPCP DIFFICULTIES

ONE OF THE MORE INTERESTING IMPLICATIONS - SETTLING QPCP

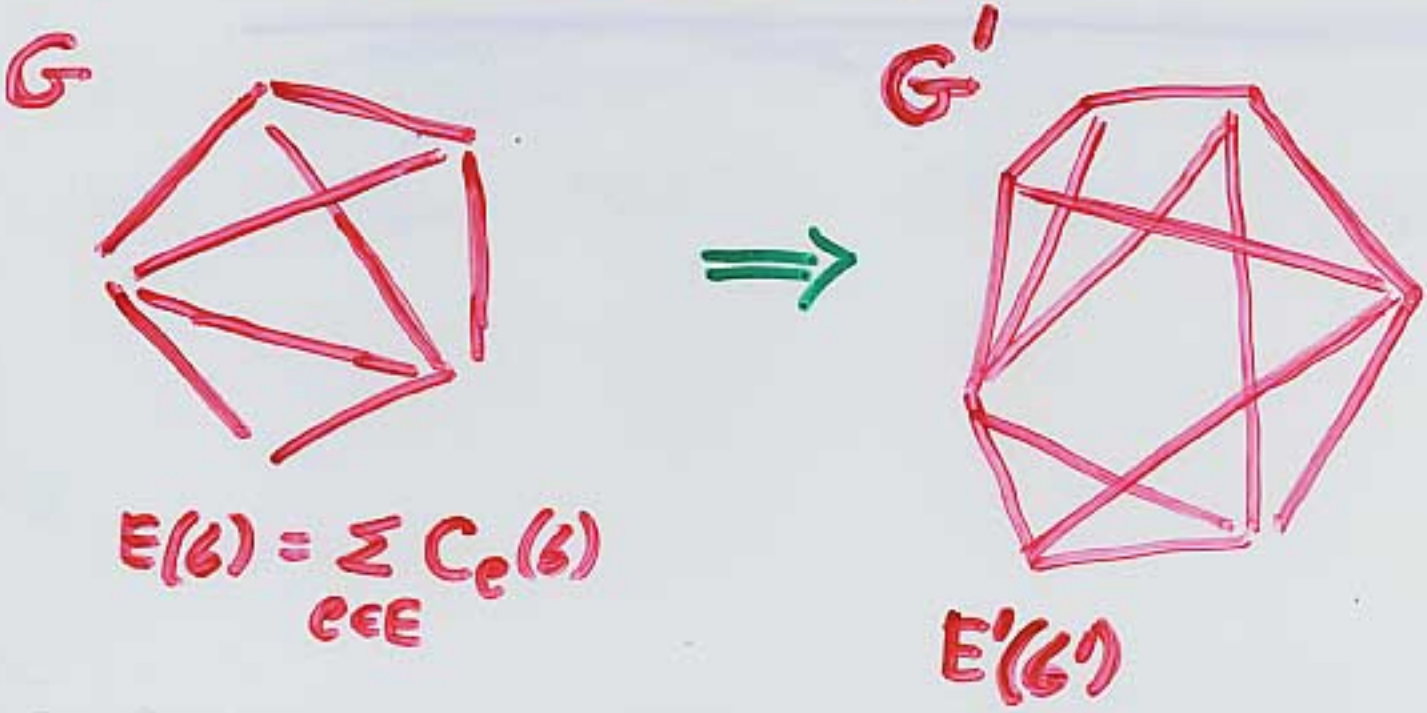
SEEMS TO CLASH WITH NO-CLONING

BUT NO PROOF OF THAT!

BEEN IN THAT STORY..

13 YEARS AGO, QECC SEEMED TO DO THAT TOO...

GENERAL OUTLINE



S.t: $gv(G) = 0 \Rightarrow Gv(G') = 0$

$gv(G) > 0 \Rightarrow gv(G') \geq \varepsilon_0 m'$

CENTRAL NOTION: EXPANDERS

DEGREE (VALENCY) = d (CONST)

YET - BEHAVES RANDOMLY.

MIXES RAPIDLY...

ON ONE HAND - MIXES ERRORS. DESTRIBUTES...

ON THE OTHER - $|E| = d \cdot |V|$

USE EXPANDERS FOR $\log(m)$ ITERATIONS.

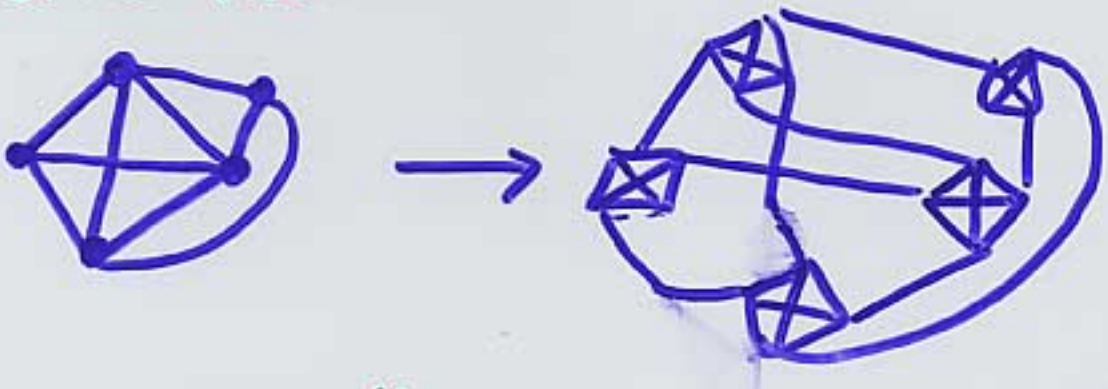
$\frac{1}{m} \xrightarrow{\times 2} \cdots \xrightarrow{\times 2}$ CONST. & SIZE' = poly!

ONE ITERATION:

$g_U \to g_U \times \text{const}$

$|G| \to |G| \times \text{const}$

1) DEGREE REDUCTION



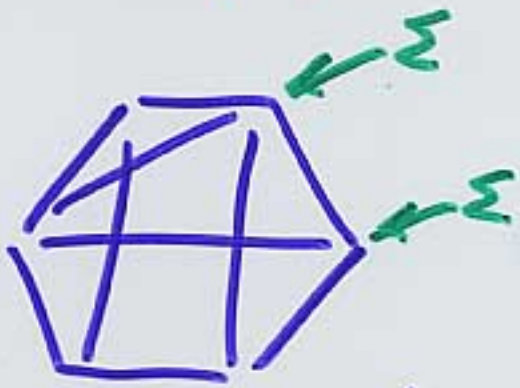
2) "EXPANDERIZE": $G \to G \cup \text{EXPANDER}$

CONSISTENCY CONSTRAINTS $\Rightarrow$ EXPANDER OF SMALL DEGREE, g_U O.K

3) GAP AMPLIFICATION.

EXPANDER SMALL DEGREE

$\Longrightarrow$

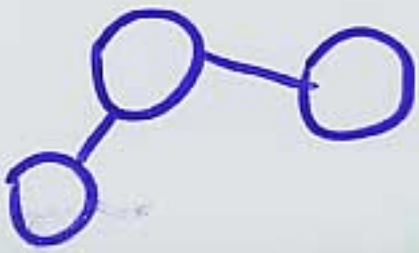


G

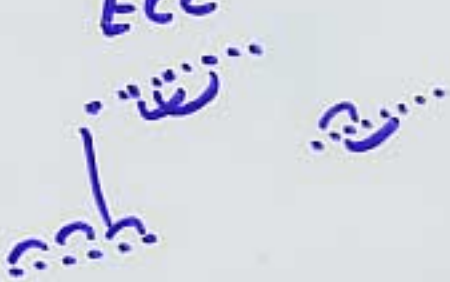
G', $g_U(G') > c g_U(G)$

BUT: $|\Sigma|$ HUGE!

4) ALPHABET REDUCTION.

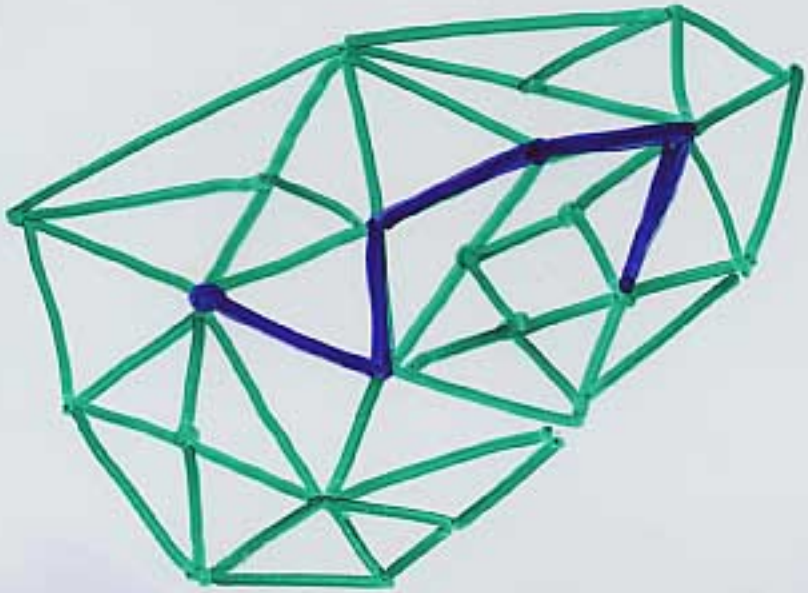


$\Longrightarrow$



GAP AMPLIFICATION

MAIN IDEA: t-WALKS ON EXPANDERS.



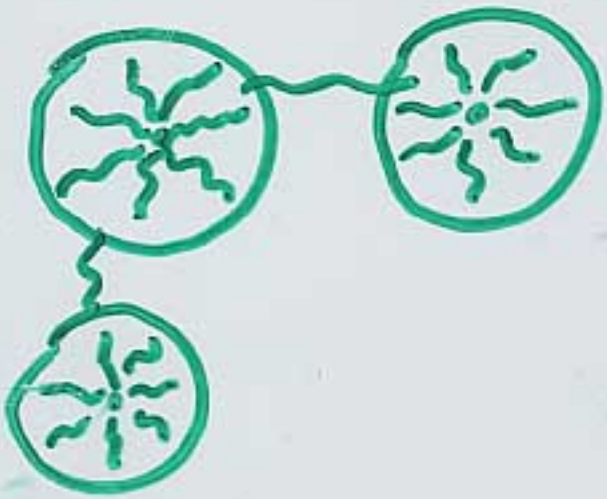
t-steps.

EACH t-WALK $\Rightarrow$ NEW CONSTRAINT.

RAPID MIXING $\Rightarrow$ MANY t-WALKS WILL "CATCH" THE PROBLEM.

factor of t amplification!

BUT - NO LONGER A GRAPH!



NEW VERTICES:

SPHERES OF t-WALKS.

$|E| = |V| d^t$

NEW CONSTRAINT:

CONSISTENCY,

& INHERITED CONSTRAINTS

CAN WE GENERALIZE TO Q?

Main Problem: Lots of consistency checks!

SEEMS TO VIOLATE NO-CLONING THM...

ISOLATE OTHER ESSENTIAL INGREDIANT:

t-WALKS →

CONSTRAINT:
$\Pi_{ABC} \Pi_{BAC} \cdots$

$$H_{t\text{-walk}} = I - P_{ABC\cdots}$$

$$H' = \sum_{t\text{-walks}} H_{t\text{-walk}}$$

HOW MUCH LARGER IS $g\frac{v(H')}{m'}$

COMPARED TO $g\frac{v(H)}{m}$?

HMMM...

EXAMPLE $t=2$.

$A = 100 \times 001$, $B = 100 \times 001$.

1) $|\psi\rangle = |0\,0\,1\rangle$. $\frac{E}{m} = \frac{1}{2}$. ✓

$\frac{E'}{m'} = \frac{1}{1} = 1$.

2) $|\psi\rangle = \sqrt{1-\varepsilon}\,|000\rangle + \sqrt{\varepsilon}\,|111\rangle$.

$\frac{E}{m} = \frac{\varepsilon+\varepsilon}{2} = \varepsilon$. ✗

$\frac{E'}{m'} = \varepsilon$!

CAPYTALYST CASE - OK

SOCIALIST CASE - NO AMPLIFICATION!

QUANTUM (WEAK) GAP AMPLIFICATION FOR t-WALKS:

$$g^v(H') > \left[1 + O\left(\frac{t}{\log(m)}\right)\right] \frac{g^v(H)}{m}$$

MAIN OBSERVATION - SOCIALEST CASE CAN'T HAPPEN.

$$|\psi\rangle = \underset{A\cap B}{|\alpha\rangle} + \underset{(A\cup B)^c}{|\beta\rangle} + \underset{\text{REST}}{|\gamma\rangle}$$

NO AMPLIFICATION:

$$\varepsilon = E_A(|\psi\rangle) = \||\beta\rangle\|^2 + \|(I-P_A)|\gamma\rangle\|^2$$

$$\varepsilon = E_B(|\psi\rangle) = \||\beta\rangle\|^2 + \|(I-P_B)|\gamma\rangle\|^2$$

$$\varepsilon = E_{A\cap B}|\psi\rangle = \||\beta\rangle\|^2 + \||\gamma\rangle\|^2.$$

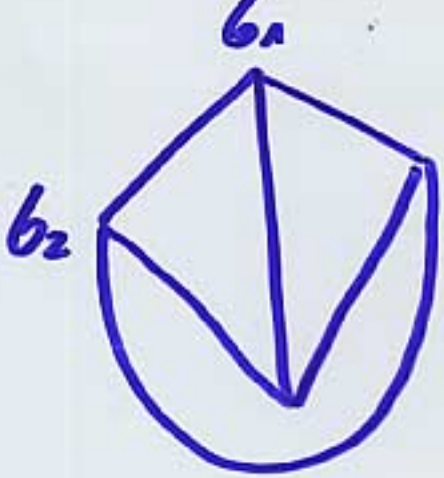
$$\Longrightarrow \quad |\gamma\rangle = 0 \; !$$

$$\Longrightarrow \quad P_A|\psi\rangle \in A\cap B.$$

SIMILARLY: $P_A|\psi\rangle \in A\cap C$!

$$\Longrightarrow \quad P_A|\psi\rangle \in A\cap B\cap C\cdots \quad \Rightarrow g^v = 0 \; !$$

NP



$$E(G_1, G_2 \cdots G_n) = \sum_{i \neq j} C_{ij}(G_i, G_j)$$

$\exists \vec{G}$ s.t $E(\vec{G}') = 0$?

CAN EASILY VERIFY $E(\vec{G}') = 0$ GIVEN $\vec{G}$.

NP PROBLEMS: EASY TO VERIFY GIVEN A HINT (MAYBE HARD TO FIND!)

ANOTHER EXAMPLE:
CORRECT MATHEMATICAL THEOREMS

& THOUSAND OTHER EXAMPLES...

NP-COMPLETENESS.

e.g: GRAPH COLORABILITY IS NP-COMPLETE

$X \longrightarrow G$

$x \in YES \rightarrow g^{\upsilon}(G) = 0$
$x \in NO \rightarrow g^{\upsilon}(G) \geq 1.$

} HARD PROBLEM !

CONCLUSIONS

- QPCP IS AN IMPORTANT & FUNDAMENTAL QUESTION. (IN BOTH DIRECTIONS)

- HOPE YOU HAVE GOTTEN SOME FLAVOR OF DINUR'S BEAUTIFUL PROOF!

- INTERESTING PRELIMINARY QUANTUM RESULTS.