Datorzinātnes lietojumi un tās saiknes ar kvantu fiziku
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Quantum Lovasz local lemma

Andris Ambainis (Latvia), Julia Kempe (Tel Aviv), Or Sattath (Hebrew U.)

Heilbronn Quantum Algorithms Day, May 18, 2010

Part 1

(classical) Lovasz local lemma

The setting

- "Bad" events $A_1, \ldots, A_m$.
- $\Pr[A_i] \leq \varepsilon$.
- When can we say that

$$\Pr[\text{none of } A_i] > 0?$$

Obvious results

- A_i independent:
  - Pr [not A_i] $\geq 1-\varepsilon$.
  - Pr [none of A_i] $\geq (1-\varepsilon)^m > 0$.
- No assumptions about A_i:
  - Pr [A_i] $\leq \varepsilon$.
  - Pr [some A_i occurs] $\leq m\cdot\varepsilon$.
  - If $m\cdot\varepsilon < 1$, then Pr [none of A_i] > 0.

Limited independence

- Each A_i is independent of all but at most d other events A_j.
- [Erdös, Lovász, 1975] If $Pr[A_i] \leq \varepsilon$ and $e(d+1)\,\varepsilon < 1$, then

$$Pr\,[\text{none of } A_i] > 0.$$

- Full independence: $m\,\varepsilon < 1$ enough;
- Limited independence: $e\,(d+1)\,\varepsilon < 1$.

Application 1: k-SAT

- k-SAT formula F,
  - $F = F_1 \wedge F_2 \wedge \ldots \wedge F_m$;
  - $F_i = y_{i,1} \vee y_{i,2} \vee \ldots \vee y_{i,k}$;
  - $y_{i,l} = x_j$ or $\neg x_j$.
- Theorem If each F_i has common variables with at most $d=2^k/e-1$ other clauses F_j, then $\exists x_1, \ldots, x_n$: $F(x_1, \ldots, x_n)=\text{TRUE}$.

Proof

- Pick x_i at random:

$$\Pr[x_i = TRUE] = \Pr[x_i = FALSE] = \frac{1}{2}$$

$$F_i = x_1 \vee x_2 \vee \ldots \vee \neg x_k$$

$$\Pr[F_i - false] = \frac{1}{2^k}$$

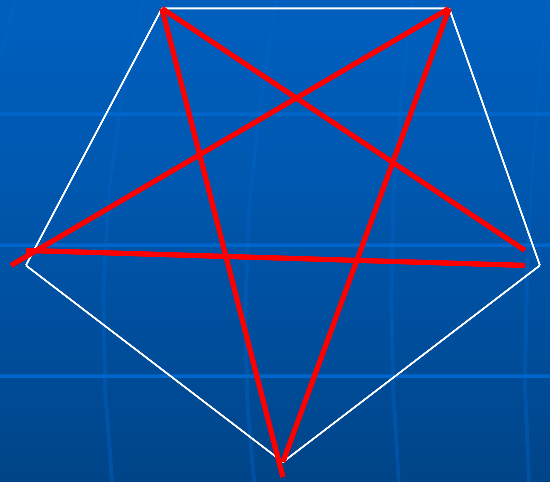
Proof

- "Bad events" - $\Pr[F_i - false] = \frac{1}{2^k}$
- F_i and F_j independent = F_i and F_j have no common variables.
- Each F_i has common variables with at most $d=2^k/e-1$ other F_j.

$$e(d+1)\frac{1}{2^k} < 1$$

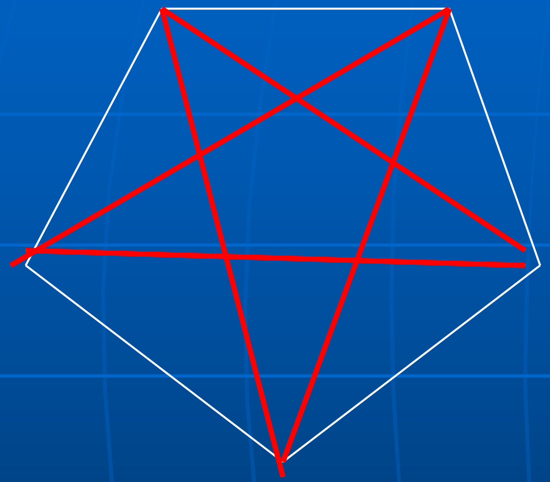
Lovasz local lemma applies

Application 2: Ramsey graphs



- Complete graph K_n.
- Colour edges in two colours so that no K_k has all edges in one colour.

Solution



- Colour edges randomly.
- Events A_i – a fixed k-vertex subgraph has all edges in the same colour.
- Independent for subgraphs with no common edges.

Result

- Theorem If $m \leq \frac{\sqrt{2}}{e} k \, 2^{k/2}$, then edges of

  K_m can be coloured with two colours so that there is no k vertices with all edges among them in one colour.

Other applications

- Coverings of R^3 by unit balls;
- Linear arboricity (partitioning edges of a graph into linear forests).

Quantum Lovasz lemma

Events $\Leftrightarrow$ subspaces

- Finite-dimensional Hilbert space H.
- Events $A_i \Leftrightarrow$ "bad subspaces" S_i.
- Event does not occur $\Leftrightarrow$ a state $|\Psi\rangle$ is orthogonal to S_i.
- Goal: a state $|\Psi\rangle$, $|\Psi\rangle \perp S_i$ for all i.

Hamiltonian version

- Hamiltonian $H = \Sigma_i P_i$.
- Terms $H_i \Leftrightarrow$ subspaces S_i.
- $H_i|\Psi\rangle=0 \Leftrightarrow |\Psi\rangle \perp S_i$.
- Is there a state $|\Psi\rangle$ with $H\,|\Psi\rangle = 0$?

Probability ⇔ dimension

- Relative dimension

$$d(H_i) = \frac{\dim H_i}{\dim H}$$

- $\Pr[A_i] \le \varepsilon \Leftrightarrow d(H_i) \le \varepsilon$.

When are two subspaces independent?

Independence: definition #1

- Bipartite system $H_A \otimes H_B$.
- Subspaces $H_1 \otimes H_B$ and $H_A \otimes H_2$ are independent.

Definition #2

- Classically, A_1, A_2 independent if
  $$\Pr[A_1 \wedge A_2] = \Pr[A_1]\Pr[A_2].$$

$$d(H_i) = \frac{\dim H_i}{\dim H}$$

- Quantumly, H_1, H_2 – independent if
  $$d(H_1 \wedge H_2) = d(H_1)\, d(H_2);$$
  $$d(H_1 \wedge H_2^{\perp}) = d(H_1)\, d(H_2^{\perp});$$
  $$d(H_1^{\perp} \wedge H_2) = d(H_1^{\perp})\, d(H_2);$$
  $$d(H_1^{\perp} \wedge H_2^{\perp}) = d(H_1^{\perp})\, d(H_2^{\perp}).$$

More than 2 subspaces

- H is independent of $H_1, \ldots, H_m$ if H is independent of any combination (union, intersection, complement) of $H_1, \ldots, H_m$.

Quantum LLL

- <u>Theorem</u> Let $H_1, \ldots, H_m$ be subspaces with:
  - $d(H_i) \leq \varepsilon$;
  - Each H_i independent of all but at most d other H_j.
  - $e(d+1)\,\varepsilon < 1$.

Then, there is $|\Psi\rangle$, $|\Psi\rangle \perp H_i$ for all i.

Proof of quantum LLL

Our goal

- Need to show: there exists $|\Psi\rangle$, $|\Psi\rangle \perp H_i$ for all i.
- Equivalently, $|\Psi\rangle \in H_i^\perp$ for all i.

$$\dim \bigcap_i H_i^\perp > 0$$

Main lemma

$$H' = H_{i_1}^{\perp} \cap H_{i_2}^{\perp} \cap \ldots \cap H_{i_j}^{\perp}$$

Then

$$\frac{\dim H_i^{\perp} \cap H'}{\dim H'} \geq 1 - \frac{1}{k+1}$$

for any other H_i.

Corollary:

$$\dim \bigcap_{i=1}^{m} H_i^{\perp} \geq \left(1 - \frac{1}{k+1}\right)^m > 0$$

Application: quantum k-SAT

Quantum SAT

- k-SAT:
  - variables $x_1, \ldots, x_N$.
  - $F = F_1 \wedge \ldots \wedge F_m$;
  - $F_i = y_{i,1} \vee \ldots \vee y_{i,k}$;
  - $y_{i,l} = x_j$ or $\neg x_j$.
- Goal: $F = \text{true}$.

- k-QSAT
  - N qubits;
  - $H = H_1 + \ldots + H_m$;
  - Each H_i involves k qubits;
  - Each H_i – projector to 1 of 2^k dimensions.
- Goal: $H|\Psi\rangle = 0$.

Theorem

- Assume that
  - $H = H_1 + \ldots + H_m$, etc.
  - each H_i has common qubits with at most $d = 2^k/e-1$ other H_j.
- Then there exists $|\Psi\rangle : H|\Psi\rangle = 0$.

Proof

- Each H_i is a projector on S_i:

$$d(S_i) = \frac{1}{2^k}$$

- QLLL:

$$e(d+1)\frac{1}{2^k} < 1 \quad \Rightarrow \quad \left|\Psi\right\rangle : \left|\Psi\right\rangle \perp S_i$$

$$H\left|\Psi\right\rangle = 0$$

Random k-SAT and k-QSAT

Random k-SAT

- $F = F_1 \wedge \ldots \wedge F_m$;
- Each F_i – random k-clause.
- What should m be so that F is satisfiable w.h.p.?

Ratio m/n.

Random k-SAT

- Threshold c_k, for large n:
  - If $m<(c_k-\varepsilon)\, n$, then $F \in SAT$ w.h.p.
  - If $m>(c_k+\varepsilon)\, n$, then $F \notin SAT$ w.h.p.
- $3.52 < c_3 < 4.49$.
- Large k:

$$2^k \ln 2 - O(k) \le c_k \le 2^k \ln 2.$$

Random k-QSAT [Bravyi, 06]

- $H = H_1 + \ldots + H_m$.
- Each H_i – random projector to 1 of 2^k dimensions for random k qubits.
- Do we have $|\Psi\rangle : H|\Psi\rangle = 0$?

Ratio $q_k = m/n$.

Results on quantum k-SAT [Laumann et al., 09]

- $q_2=1/2$.
- For large k, $1-\varepsilon < q_k < 0.574 \bullet 2^k$.

Classically, $c_k < \ln 2 \bullet 2^k = 0.69 \bullet 2^k$.

Huge gap between upper and lower bounds.

Our result

- Theorem

$$q_k \geq \frac{2^k}{8ek^2}$$

- Since each H_i involves k qubits, this corresponds to each H_i having common qubits with $\frac{2^k}{8ek}$ other H_j, on average.

QLLL: $\frac{2^k}{ek}$, worst case.

Solution

- Divide qubits into two sets:
  - “high-degree”: includes all qubits that are contained in many H_j and those that are in H_i with such qubits.
  - “low-degree”.
- Use QLLL on “low-degree” set, another approach on “high-degree” set.
- Combine the two solutions.

[Laumann, et al., 09]

- $H = H_1 + \ldots + H_m$.
- Theorem If $f:\{1, \ldots, m\} \to$ qubits:
  - $f(i)$ – qubit that is involved in H_i;
  - $f(i) \neq f(j)$,

there exists $|\Psi\rangle : H|\Psi\rangle = 0$.