CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

LABORATOIRE DE RECHERCHE EN
INFORMATIQUE

Quantum Algorithms for the Triangle Problem

Frédéric Magniez

http://www.lri.fr/~magniez

joint work with

Miklos Santha — CNRS-LRI (Université Paris-Sud)
Mario Szegedy — Rutgers University

Oracle Input

- A (non-oriented) graph G on n vertices given as a black-box

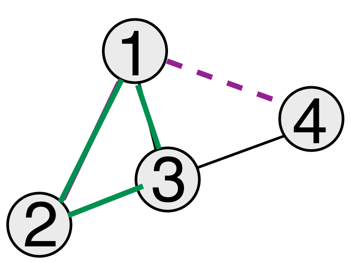
Output

- A triangle, if there is any
- Reject, otherwise

Query model

- Query: $(i, j) \in [n]^2$
- Answer: 1 if $(i, j) \in G$, 0 otherwise
- Complexity: number of queries (**QQC**)

Input:



Oracle Adjacency function

	1:	2:	3:	4:
1:	0		1	
2:	1	0	1	0
3:	1	1	0	1
4:	0	0	1	0

Queries: $(1, 2) \mapsto 1$
$(1, 4) \mapsto 0$
$\vdots$

Ouput: $(1, 2, 3)$

Monotone Graph Properties

Generalities

- Deterministically: $\Theta(n^2)$ [Rivest, Vuillemin'76]
- Randomly: $\Omega(n^{4/3} \log^{1/3} n)$ [Hajnal'91; Chakrabarti, Khot'01]
  Conjecture: $\Theta(n^2)$
- Quantumly: $\Omega(n^{2/3} \log^{1/6} n)$ [Yao'01]
  Conjecture: $\Omega(n)$

Observations on $\mathbf{QQC}$

- Any complexity in $[n, n^2]$ is possible
- Most of *natural* properties have complexity in $\{n, n^{3/2}, n^2\}$

Examples

- Having an edge, a star: $\Theta(n)$
- Connectivity, ...: $\tilde{\Theta}(n^{3/2})$ [Dürr, Heiligman, Høyer, Mhalla'04]
- Majority: $\Theta(n^2)$

Multiplication

- Checking $A \times B \stackrel{?}{=} C$

  Randomly (time & query): $\Theta(n^2)$

  Quantumly: $[\Omega(n^{3/2}), O(n^{5/3})]$ [Ambainis, Buhrman, Høyer, Karpinski, Kurar, Midrijanis'02]

- Computing $A \times B = ?$

  Random & Quantum time : $O(n^{2.38})$

Relation to Triangle

- Randomly

  Query: $\Theta(n^2)$

  Time: $O(n^{2.38})$ from a reduction to Matrix Multiplication

- Quantumly, the situation is different:

  $$\mathbf{QQC}(\text{Triangle}) = o(n^{3/2})$$ [Next slide...]

Previous results

- Randomly
  Tight bound: $\Theta(n^2)$
- Quantumly
  Lower bound: $\Omega(n)$ (best possible using adversary methods)
  Upper bound: $O(n^{3/2}), O(n+\sqrt{n|G|})$ [Buhrman, Dürr, Heiligman, Høyer, M, Santha, Wolf'01]
  $O(n\sqrt{d})$

This Talk

- Using $O(\log n)$ qubits: $\tilde{O}(n^{10/7}) = O(n^{1.43})$
- Using $O(n)$ qubits: $O(n^{1.3})$

Main tool: Grover search

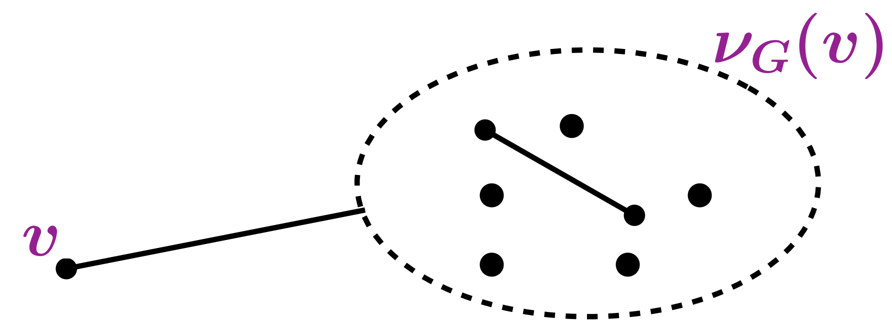
- Oracle Input: $f : [n] \to \{0,1\}$
- Output: x such that $f(x) = 1$
- **QQC** $= \Theta(\sqrt{n})$

Triangle between candidates

- Additional input: a set of triangles $T \subseteq [n]^3$
- Output: A triangle of G among those of T, if there is any
- **QQC** $= O(\sqrt{|T|})$

Triangle with a golden edge

- Additional input: a set of edges $E \subseteq [n]^2$
- Output: A triangle of G containing an edge of E
- **QQC** $= O(\sqrt{|E|} + \sqrt{n|E \cap G|})$ by a generalization of [BDHHMSW'01]



Naive algorithm

1. While $\exists v : d_G(v) \geq n^{1-\delta}$
   a. Compute $\nu_G(v)$
   b. If $G \cap \nu_G(v)^2 \neq \emptyset$, output the triangle induced by v
   c. Otherwise disconnect v from G
2. Do [BDHHMSW'01] Algorithm

Query complexity

1. Search: $\sqrt{n}$, degree checking: $n^{\delta/2}$ $\rightarrow n^{(1+\delta)/2}$
   a. Computation: n
   b. Intersection: $\sqrt{|\nu_G(v)|^2} \leq n$

   Number of iterations: W
2. Standard algorithm: $n^{(3-\delta)/2}$

Total: $T = W \times n + n^{(3-\delta)/2}$

Lucky: $W \leq n^2/(n^{1-\delta})^2 \leq n^{2\delta} \implies T \leq n^{1.4}$ when $\delta = 1/5$

Unlucky: $W \leq n \implies T \leq n^2$ when $\delta = 0$

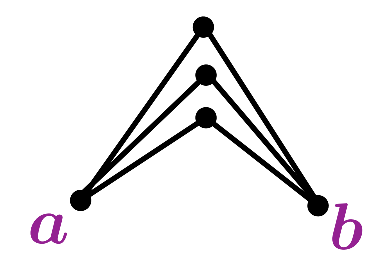
Preparation

1. Let $k = \Theta(n^{3/7}) \times \log n$
2. Randomly choose $v_1, v_2, \ldots, v_k \in [n]$
3. Compute every neighborhood $\nu_G(v_i)$
4. If $G \cap (\nu_G(v_i))^2 \neq \emptyset$, then output the triangle induced by v_i (Quantum)
5. Otherwise $G \subseteq G' = [n]^2 \setminus \cup (\nu_G(v_i))^2$

Query complexity: $k \times n + k \times O(\sqrt{n^2}) = O(n^{10/7})$

Definition

$$G^{\langle t \rangle} \stackrel{\text{def}}{=} \{(a,b) : |\{v : (a,v),(v,b) \in G\}| \leq t\}$$



$(a,b) \in G^{\langle 3 \rangle}$

Main lemma

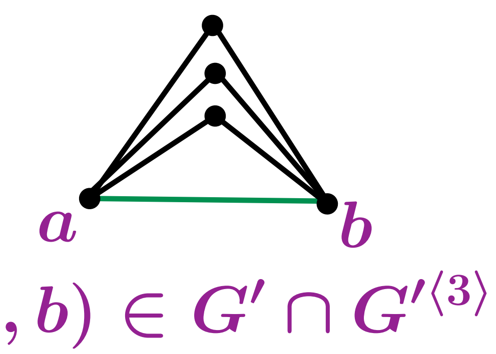
$$G' \subseteq G^{\langle n^{4/7} \rangle}$$ (with high probability)

Proof

$$(a,b) \notin G^{\langle n^{4/7} \rangle} \implies \Pr_v[a,b \in \nu_G(v)] > \frac{n^{4/7}}{n} = \frac{1}{n^{3/7}}$$

$$\ldots \implies (a,b) \notin G'$$ (with high probability)

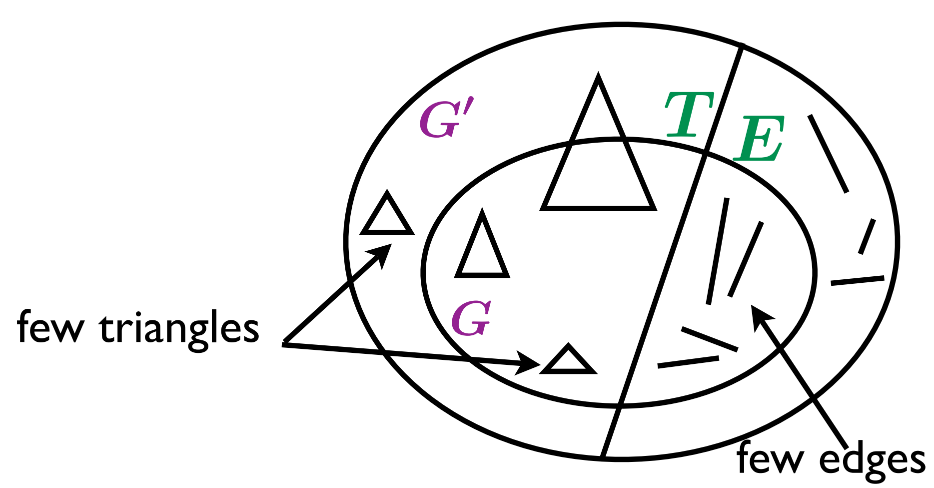
Fact: $G' \subseteq G'^{\langle t \rangle} \implies |\text{Triangles}(G')| \leq n^2 \times t$



Theorem

If $G' \subseteq G^{\langle n^{4/7} \rangle}$, then using $O(n^{9/7})$ (quantum) queries G' can be efficiently partitioned into $T \cup E$ such that:

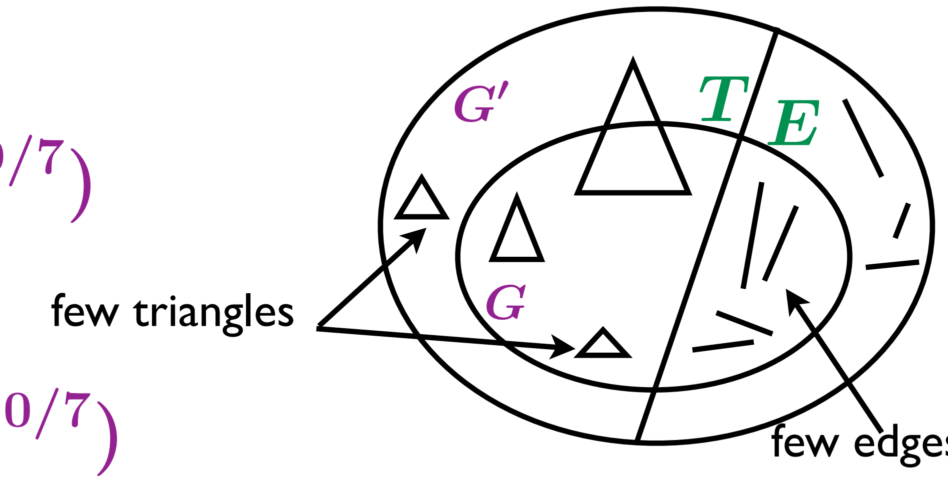
- T contains only $O(n^{3-1/7})$ triangles
- $E \cap G$ has size $O(n^{2-1/7})$



Overall complexity

Construction of G': $O(n^{10/7})$

Classification of G': $O(n^{9/7})$



Find a triangle inside G: $O(n^{10/7})$

Quantum - Search for a triangle in G among all triangles inside T

$$|\text{Triangles}(T)| = O(n^{3-1/7}) \implies O(\sqrt{n^{3-1/7}}) = O(n^{10/7})$$

Quantum - Search for a triangle in G intersecting with E

$$|E \cap G| = O(n^{2-1/7}) \implies O(n + \sqrt{n \times n^{2-1/7}}) = O(n^{10/7})$$

Theorem

$$\mathbf{QQC}(\text{Triangle}) = \tilde{O}(n^{10/7})$$

k-Collision problem (on a finite set S)

- Oracle Input: A function f which determines a k-ary relation $\mathcal{C} \subseteq S^k$
- Output: An element of $\mathcal{C}$ if there is any, reject otherwise

Examples

- Grover search: $k = 1, S = [n], f : [n] \to \{0, 1\}$
  $\mathcal{C} = \{x : f(x) = 1\}$
- Element distinctness: $k = 2, S = [n], f : [n] \to [n]$
  $\mathcal{C} = \{(x, y) : x < y, f(x) = f(y)\}$
- Triangle: $S = [n], f_G : [n]^2 \to \{0, 1\}$
  $k = 3, \mathcal{C} = \{\text{Triangles}(G)\}$
  $k = 2, \mathcal{C} = \{\text{Triangle edges}(G)\}$

Remark: Triangle edge $\xrightarrow{+O(\sqrt{n})\ \text{queries}}$ Triangle

Database built from f

- Query language: $A \subseteq S \mapsto D(A)$
- Checking procedure: Given $D(A)$, find a collision in A^k, if there is any

Costs in queries to f

$A \subseteq S, |A| = r$

- Setup cost $s(r)$: to setup $D(A)$
- Update cost $u(r)$: to update $D(A) \mapsto D(A')$ when $A' = A \pm \{x\}$
- Checking cost $c(r)$

Examples

Problem	*Collision relation*	*Database*	*Setup*	*Update*	*Checking*
Grover	$x : f(x) = 1$	$f\|_A$	r	1	0
ED	$x < y : f(x) = f(y)$	$f\|_A$	r	1	0
Triangle	Triangle edges	$G\|_A$	r^2	r	$?$

Theorem (Ambainis)

$$\mathbf{QQC} = O(s(r) + (\tfrac{n}{r})^{k/2} \times (c(r) + \sqrt{r} \times u(r)))$$

$n = |S|$

Checking cost for Triangle edges

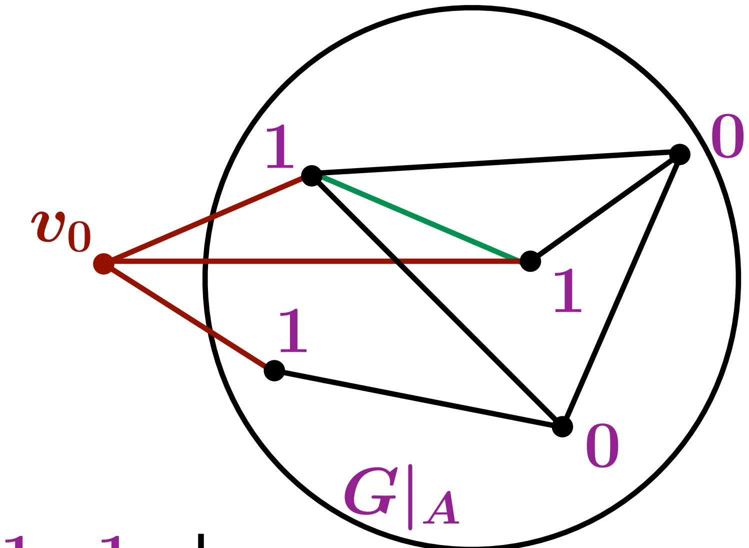
Subproblem

- Oracle Input: $G \subseteq [n]^2$
- Additional inputs: a vertex $v_0 \in [n]$, and $G|_A$ (from database)
- Output: A triangle containing v_0 and an edge of $G|_A$, if there is any

Reduction: $c(r) \leq \sqrt{n} \times \mathbf{QQC}(\text{Subproblem})$

Encoding of Subproblem

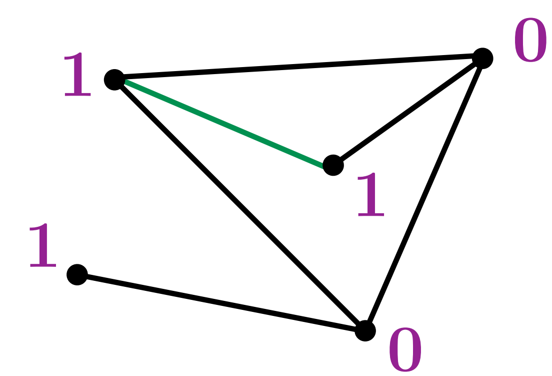
$$f : A \longrightarrow \{0,1\}$$
$$v \mapsto \begin{cases} 1 : (v_0, v) \in G \\ 0 : (v_0, v) \notin G \end{cases}$$



$v_0 \times G|_A$ contains a triangle iff $G|_A$ has a $1-1$ edge

Graph Collision Problem

Problem



- Oracle Input: $f : [r] \to \{0,1\}$
- Additional input: a graph $H \subseteq [r]^2$
- Output

  An edge $(u,v) \in H : f(u) = f(v) = 1$, if there is any

  Reject, otherwise

Theorem

$\mathbf{QQC} = \Omega(\sqrt{r})$ (best possible using adversary methods)

$\mathbf{QQC} = O(r^{2/3})$

Proof

Collision relation $k=2$	*Database*	*Setup*	*Update*	*Checking*
$(u,v) \in G : f(u) = f(v) = 1$	$f\|_A$	r'	1	0

$$\begin{aligned}\mathbf{QQC} &= O(r' + (\tfrac{r}{r'})^{2/2}(0 + \sqrt{r'} \times 1)) \\ &= O(r' + \tfrac{r}{\sqrt{r'}}) \\ &\to O(r^{2/3}) \qquad (r' = r^{2/3})\end{aligned}$$

Theorem

$$\mathbf{QQC}(\text{Triangle}) = O(n^{1.3})$$

Proof

Collision relation $k = 2$	*Database*	*Setup*	*Update*	*Checking*
Triangle edges	$G\vert_A$	r^2	r	$\sqrt{n} \times r^{2/3}$

$$\begin{aligned}\mathbf{QQC} &= O(r^2 + (\tfrac{n}{r})^{2/2}(\sqrt{n} \times r^{2/3} + \sqrt{r} \times r)) \\ &= O(r^2 + \tfrac{n}{r^{1/3}}(\sqrt{n} + r^{5/6})) \\ &\rightarrow O(n^{1.2} + n^{1.3} + n^{1.3}) \qquad {\scriptstyle (r = n^{3/5})}\end{aligned}$$

Improvement?

$$\mathbf{QQC}(\text{GraphCollision}) = O(\sqrt{r}) \implies \mathbf{QQC}(\text{Triangle}) = O(n^{1.25})$$

Having a copy of a given graph

- Parameter: a graph H with $l > 3$ vertices
- Oracle Input: $G \subseteq [n]^2$
- Output: A copy of H, if there is any

Theorem

$$\mathbf{QQC} = O(n^{2-2/l})$$

Proof

Collision relation $k = l - 1$	*Database*	*Setup*	*Update*	*Checking*
$l-1$ H-vertices	$G\|_A$	r^2	r	$\sqrt{n} \times r^{(l-1)/l}$

$$\begin{aligned}\mathbf{QQC} &= O(r^2 + (\tfrac{n}{r})^{(l-1)/2}(\sqrt{n} \times r^{(l-1)/l} + \sqrt{r} \times r)) \\ &= O(r^2 + (\tfrac{n}{r})^{(l-3)/2} \times \tfrac{n^{3/2}}{r^{1/l}} + (\tfrac{n}{r})^{(l-4)/2} \times n^{3/2}) \\ &\to O(n^{2-2/l} + o(n^{2-2/l}) + n^{2-2/l}) \qquad {\scriptstyle (r = n^{1-1/l})}\end{aligned}$$

Corollary

Monotone graph properties whose 1-certificates have at most $l > 3$ vertices

$$\mathbf{QQC} = O(n^{2-2/l})$$

Conclusion

Quantum query complexity of Triangle Problem

- Using $O(\log n)$ qubits and Grover search:

$$\tilde{O}(n^{10/7}) = O(n^{1.43})$$

- Using $O(n)$ qubits and Database reformulation of Ambainis QW:

$$O(n^{1.3})$$

- Tight bound?

  Best possible lower bound using adversary methods: $\Omega(n)$

  Best possible upper bound using second algorithm: $O(n^{1.25})$

Extension to Monotone Graph Properties

$$\textbf{QQC} = O(n^{2-2/l})$$

l: vertex certificate size

Bipartite Perfect Matching and Determinant

Determinant

- Checking $\det(A) \stackrel{?}{=} 0$

Query (random & quantum): $\Theta(n^2)$

Time (random & quantum): $O(n^{2.38})$

[Ambainis, Buhrman, Høyer, Karpinski, Kurar, Midrijanis'02; Santha'03]

Relation to Bipartite Perfect Matching

- Randomly

Query: $\Theta(n^2)$

Time: $O(n^{2.38})$ from a reduction to Determinant

- Quantumly

Query: $[\Omega(n^{3/2}), O(n^2)]$ [Ambainis, Karpinski'02, Dürr'03]

Time: $O(n^2)$ [Ambainis, Karpinski'02]

- Question:

$$\mathbf{QQC}(\mathrm{BPM}) \stackrel{?}{=} o(n^2)$$