

グラフの問題に対する パラメータ化量子クエリ計算量

寺尾 樹哉¹, 森 立平²

1. 京都大学 数理解析研究所 D1
2. 名古屋大学 多元数理科学研究科

量子情報技術研究会 (QIT51)@高松
11月27日(水)

クエリ計算量

関数 f が陽にではなく、
オラクルで与えられてる！

オラクル O_f

$$f: \{1, \dots, N\} \rightarrow \{0, 1\}$$



クエリ計算量

アルゴリズム



f の性質

i での値
をクエリ



$f(i)$ を返す

オラクル O_f

$f: \{1, \dots, N\} \rightarrow \{0, 1\}$



オラクルへのクエリ回数を評価

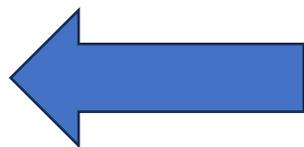
量子クエリ計算量

量子アルゴリズム



f の性質

$|i, b\rangle$



$|i, b \oplus f(i)\rangle$

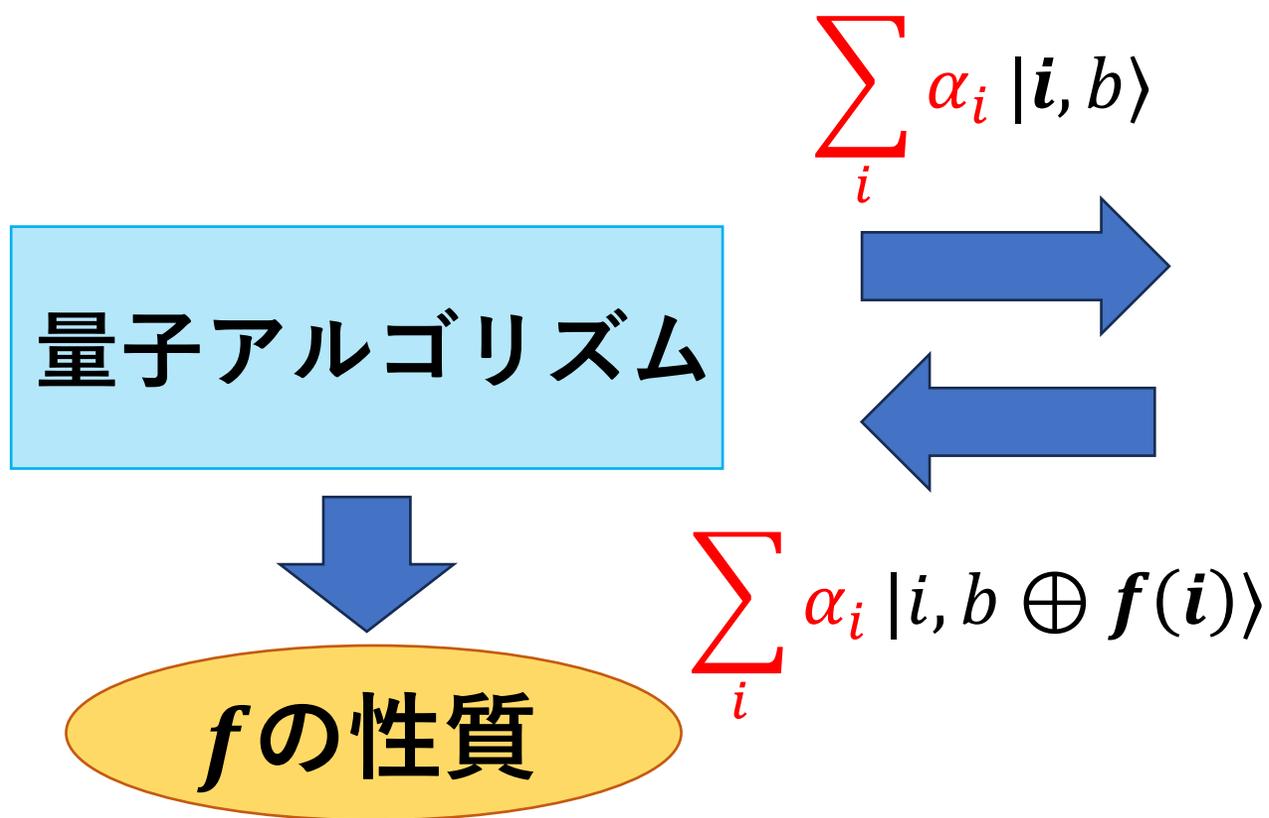
量子オラクル O_f

$f: \{1, \dots, N\} \rightarrow \{0, 1\}$



オラクルへのクエリ回数を評価

量子クエリ計算量



量子オラクル \mathcal{O}_f

$f: \{1, \dots, N\} \rightarrow \{0, 1\}$



👉 オラクルへのクエリ回数を評価

Groverのアルゴリズム

入力： $f: \{1, \dots, N\} \rightarrow \{0, 1\}$ へのオラクルアクセス

出力： $f(i) = 1$ なる $i \in \{1, \dots, N\}$ を一つ

古典

$\Theta(N)$ クエリは
誤り確率高々 $1/3$ には必要

Groverのアルゴリズム

入力： $f: \{1, \dots, N\} \rightarrow \{0, 1\}$ へのオラクルアクセス

出力： $f(i) = 1$ なる $i \in \{1, \dots, N\}$ を一つ

古典

$\Theta(N)$ クエリは
誤り確率高々 $1/3$ には必要

量子

$O(\sqrt{N})$ クエリで誤り確率高々 $1/3$
[Grover '96]

$\Omega(\sqrt{N})$ クエリは必要
[Bennett-Bernstein-Brassard-Vazirani '97]

Groverのアルゴリズム

入力： $f: \{1, \dots, N\} \rightarrow \{0, 1\}$ へのオラクルアクセス

出力： $f(i) = 1$ なる $i \in \{1, \dots, N\}$ を一つ

古典

$\Theta(N)$ クエリは
誤り確率高々 $1/3$ には必要

量子

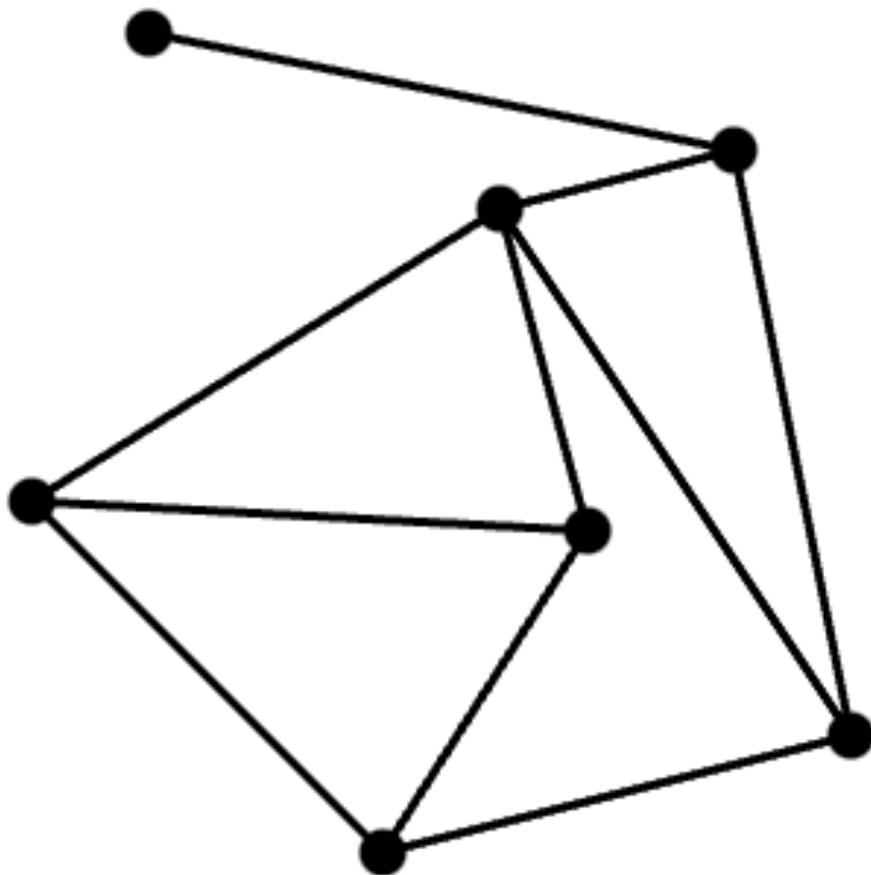
意義①: 量子計算の優位性!

$O(\sqrt{N})$ クエリで誤り確率高々 $1/3$
[Grover '96]

意義②: 量子計算の限界!

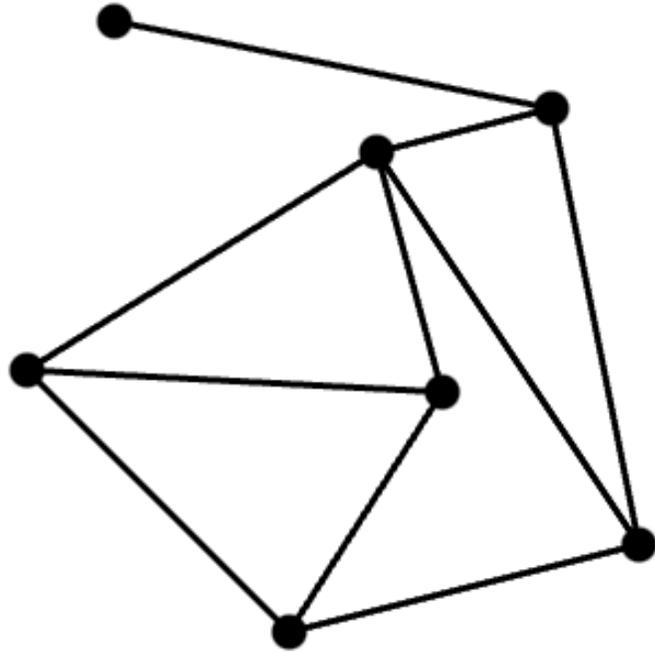
$\Omega(\sqrt{N})$ クエリは必要
[Bennett-Bernstein-Brassard-Vazirani '97]

グラフの問題の量子クエリ計算量



$n = \text{頂点数}$

グラフの問題の量子クエリ計算量



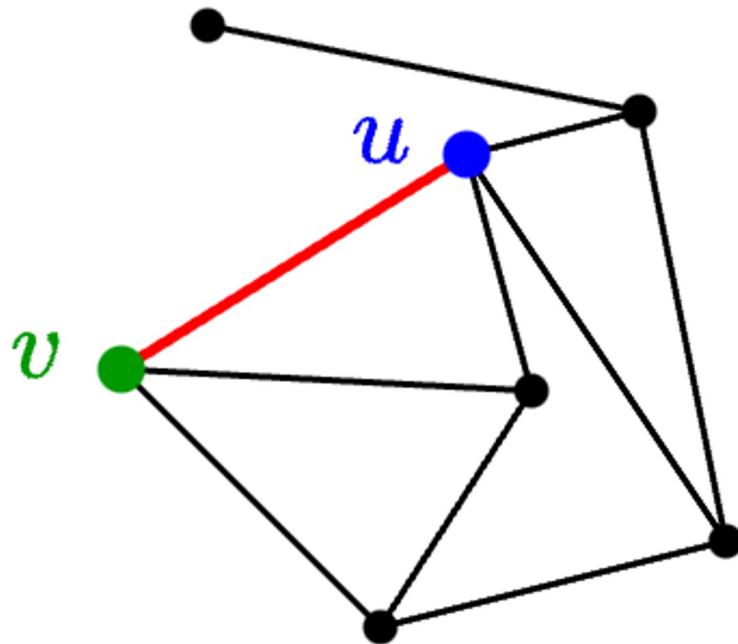
隣接行列モデル

量子オラクルで隣接行列 $E_M: \{1, \dots, n\} \times \{1, \dots, n\} \rightarrow \{0, 1\}$ にアクセス

$$E_M(u, v) = 1 \Leftrightarrow (u, v) \in E(G)$$

n = 頂点数

グラフの問題の量子クエリ計算量



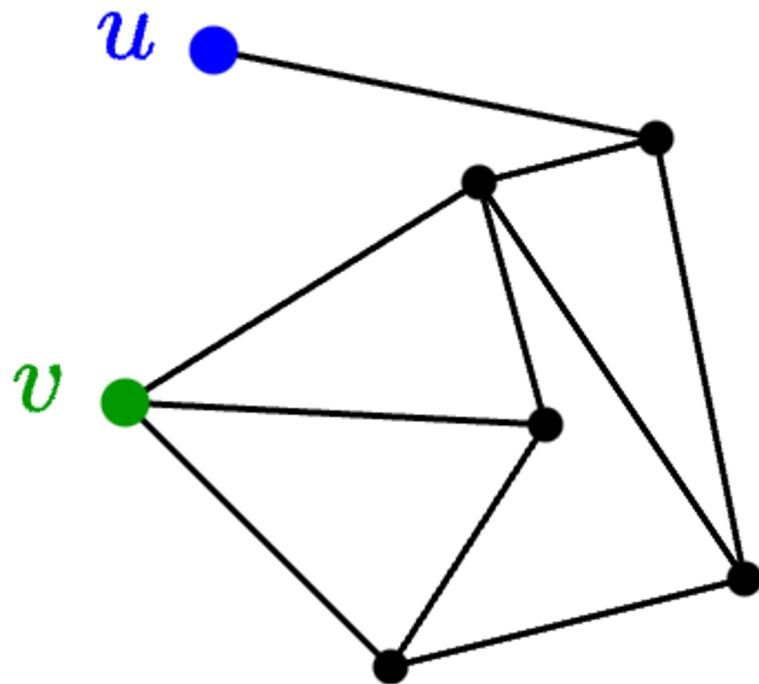
隣接行列モデル

量子オラクルで隣接行列 $E_M: \{1, \dots, n\} \times \{1, \dots, n\} \rightarrow \{0, 1\}$ にアクセス

2頂点のペア u, v をクエリした時,
間に辺が**ある** or ないを返す

n = 頂点数

グラフの問題の量子クエリ計算量



隣接行列モデル

量子オラクルで隣接行列 $E_M: \{1, \dots, n\} \times \{1, \dots, n\} \rightarrow \{0, 1\}$ にアクセス

2頂点のペア u, v をクエリした時、
間に辺がある or **ない** を返す

n = 頂点数

先行研究: グラフの問題の量子クエリ計算量

古典では $\Theta(n^2)$ の問題でも...

- 連結性判定 : $\Theta(n^{3/2})$ [Dürr-Heiligman-Høyer-Mhalla '06]
- 最大マッチング : $O(n^{7/4})$ [Kimmel-Witter '21], $\Omega(n^{3/2})$ [Zhang '04]
- 最小カット : $\Theta(n^{3/2})$ [Apers-Lee '21]

$n =$ 頂点数

先行研究: グラフの問題の量子クエリ計算量

- 連結性判定 : $\Theta(n^{3/2})$ [Dürr-Heiligman-Høyer-Mhalla '06]
- 最大マッチング : $O(n^{7/4})$ [Kimmel-Witter '21], $\Omega(n^{3/2})$ [Zhang '04]
- 最小カット : $\Theta(n^{3/2})$ [Apers-Lee '21]

頂点被覆, ハミルトン路, クリーク問題などの他の問題でも $O(n^{2-\epsilon})$ を達成できるか?

$n =$ 頂点数

先行研究: グラフの問題の量子クエリ計算量

- 連結性判定 : $\Theta(n^{3/2})$ [Dürr-Heiligman-Høyer-Mhalla '06]
- 最大マッチング : $O(n^{7/4})$ [Kimmel-Witter '21], $\Omega(n^{3/2})$ [Zhang '04]
- 最小カット : $\Theta(n^{3/2})$ [Apers-Lee '21]

頂点被覆, ハミルトン路, クリーク問題などの他の問題でも $O(n^{2-\epsilon})$ を達成できるか?

パラメータ化計算量を考える!

$n =$ 頂点数

先行研究: グラフの問題の量子クエリ計算量

- 連結性判定 : $\Theta(n^{3/2})$ [Dürr-Heiligman-Høyer-Mhalla '06]
- 最大マッチング : $O(n^{7/4})$ [Kimmel-Witter '21], $\Omega(n^{3/2})$ [Zhang '04]
- 最小カット : $\Theta(n^{3/2})$ [Apers-Lee '21]

頂点被覆, ハミルトン路, クリーク問題などの他の問題でも $O(n^{2-\epsilon})$ を達成できるか?

パラメータ化計算量を考える!

- k -クリーク : $\tilde{O}(n^{2-2/k})$ [Magniez-Santha-Szegedy '05]

$n =$ 頂点数

先行研究: グラフの問題の量子クエリ計算量

- 連結性判定: $\Theta(n^{3/2})$ [Dürr-Heiligman-Høyer-Mhalla '06]
- 最大マッチング: $O(n^{7/4})$ [Kimmel-Witter '21], $\Omega(n^{3/2})$ [Zhang '04]
- 最小カット: $\Theta(n^{3/2})$ [Apers-Lee '21]

頂点被覆, ハミルトン路, クリーク問題などの他の問題でも $O(n^{2-\epsilon})$ を達成できるか?

パラメータ化計算量を考える!

- k -クリーク: $\tilde{O}(n^{2-2/k})$ [Magniez-Santha-Szegedy '05]



k : 定数



k : より大 (例, $k = \Theta(\log n)$, $k = \Theta(\sqrt{n})$)

n = 頂点数

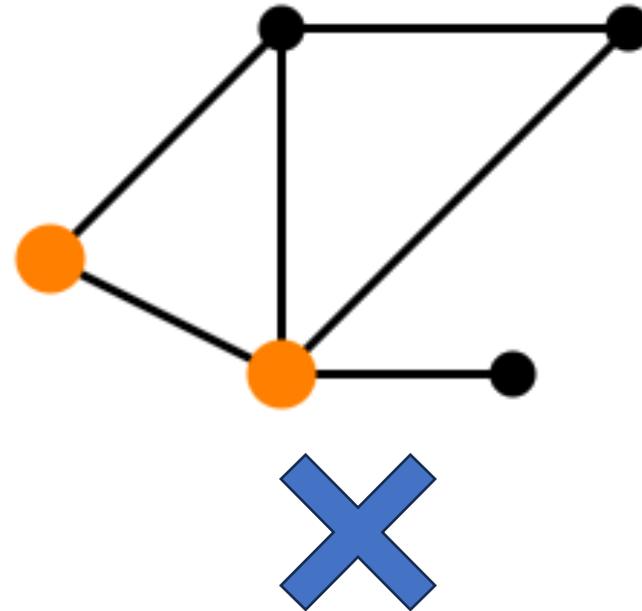
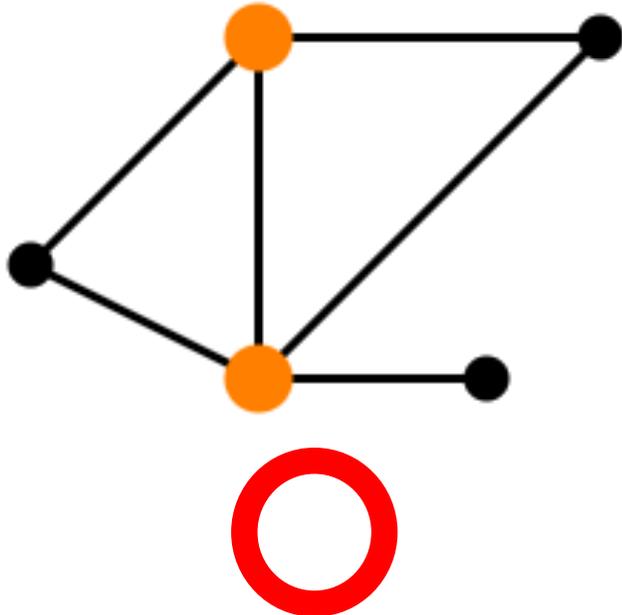
k -頂点被覆問題

入力：グラフ G と整数 k

問題：大きさ k 以下の頂点被覆 $S \subseteq V$ が G に存在するか？

G のどの辺も端点の少なくとも一方は S に属す

例)



k -頂点被覆問題

入力：グラフ G と整数 k

問題：大きさ k 以下の頂点被覆 $S \subseteq V$ が G に存在するか？

	パラメータ化なし	パラメータ化あり
古典時間計算量	NP-hard	FPT
	$\text{poly}(n, k)$ は無理	$f(k) \cdot \text{poly}(n)$

k -頂点被覆問題

入力：グラフ G と整数 k

問題：大きさ k 以下の頂点被覆 $S \subseteq V$ が G に存在するか？

	パラメータ化なし	パラメータ化あり
古典時間計算量	NP-hard	FPT
量子クエリ計算量	自明な $O(n^2)$ しか知られず	??

k -頂点被覆問題

入力：グラフ G と整数 k

問題：大きさ k 以下の頂点被覆 $S \subseteq V$ が G に存在するか？

	パラメータ化なし	パラメータ化あり
古典時間計算量	NP-hard	FPT
量子クエリ計算量	自明な $O(n^2)$ しか知られず	??

本研究: FPTのような量子クエリ計算量, i.e., $O(f(k) \cdot n^{2-\epsilon})$

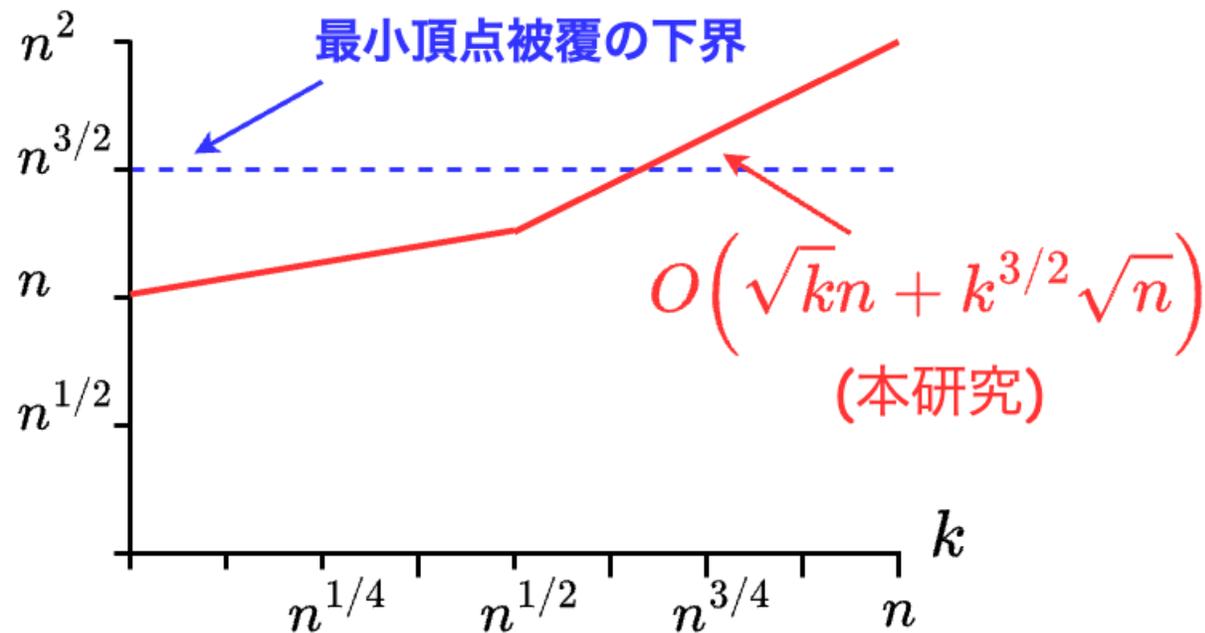
主結果①: 頂点被覆問題に対する パラメータ化量子クエリ計算量

定理

大きさ k 以下の頂点被覆を持つかの判定問題の量子クエリ計算量

上界: $O(\sqrt{kn} + k^{3/2}\sqrt{n})$

FPTのような計算量, i.e., $O(f(k) \cdot n^{2-\epsilon})$



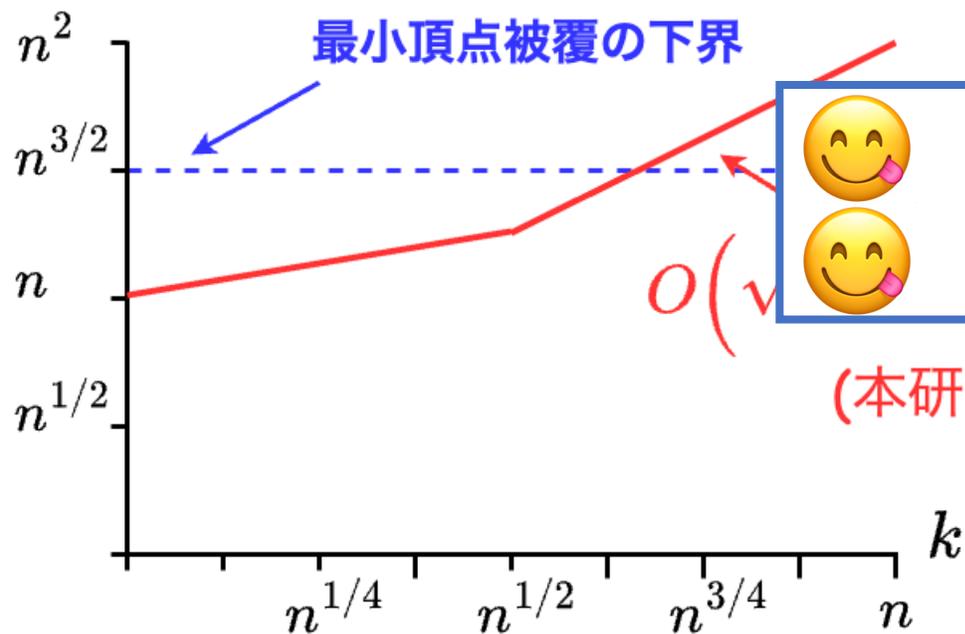
主結果①: 頂点被覆問題に対する パラメータ化量子クエリ計算量

定理

大きさ k 以下の頂点被覆を持つかの判定問題の量子クエリ計算量

上界: $O(\sqrt{kn} + k^{3/2}\sqrt{n})$

FPTのような計算量, i.e., $O(f(k) \cdot n^{2-\epsilon})$



k : 定数



k : より大 (例, $k = \Theta(\log n)$, $k = \Theta(\sqrt{n})$)

(本研究)

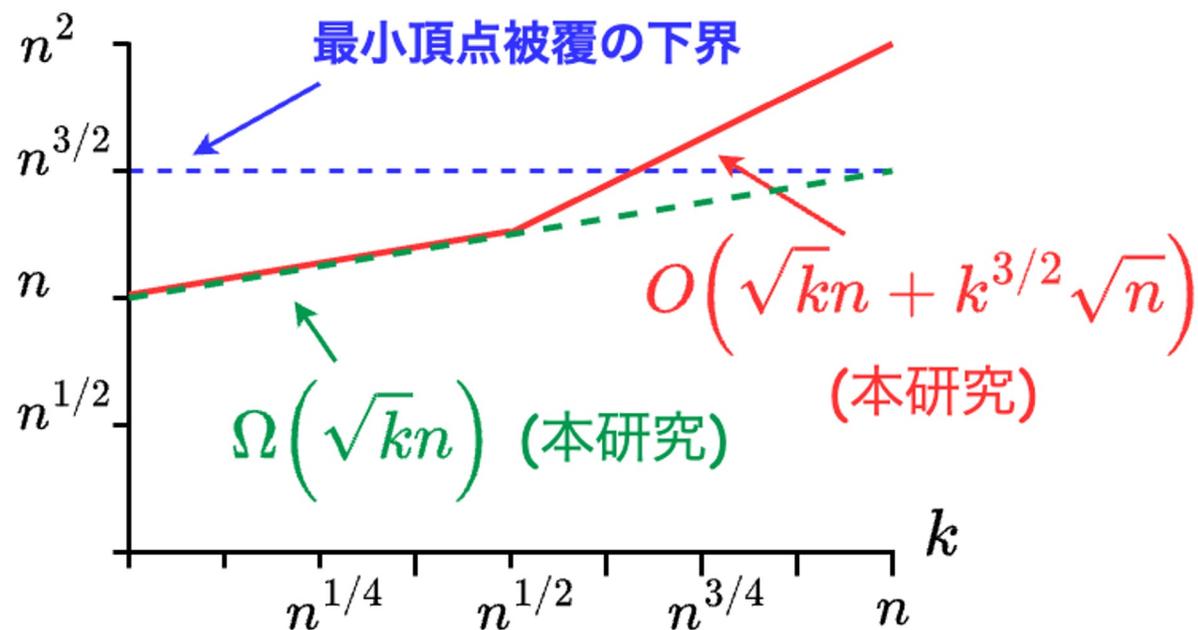
主結果①: 頂点被覆問題に対する パラメータ化量子クエリ計算量

定理

大きさ k 以下の頂点被覆を持つかの判定問題の量子クエリ計算量

上界: $O(\sqrt{kn} + k^{3/2}\sqrt{n})$

下界: $\Omega(\sqrt{kn})$ ($k \leq (1 - \epsilon)n$ の時)



$k = O(\sqrt{n})$ のとき
 $\Theta(\sqrt{kn})$ で最適！！

主結果①: 頂点被覆問題に対する パラメータ化量子クエリ計算量

定理

大きさ k 以下の頂点被覆を持つかの判定問題の量子クエリ計算量

上界: $O(\sqrt{kn} + k^{3/2}\sqrt{n})$

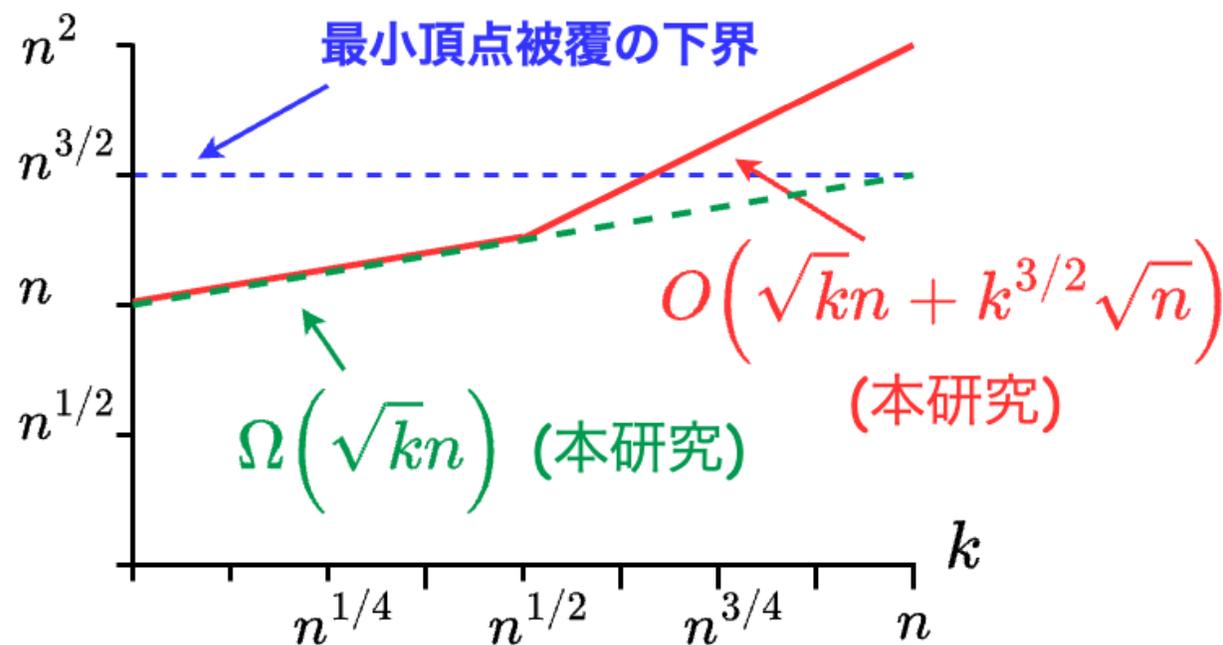
下界: $\Omega(\sqrt{kn})$ ($k \leq (1 - \epsilon)n$ の時)

意義

- 最小頂点被覆の上界 $O(n^2)$, 下界 $\Omega(n^{3/2})$ [Zhang '04] をパラメータ化により改善

手法

- 量子クエリカーネル化



カーネル化 (kernelization)

カーネル

入力：インスタンス (G, k)

出力：別の**等価で小さな**インスタンス (G', k')

or (G, k) がYesインスタンス or Noインスタンスだと断定

- (G, k) がYesインスタンス $\Leftrightarrow (G', k')$ がYesインスタンス
- $|E(G')| \leq f(k)$
- $k' \leq g(k)$

Buss-Goldsmithによる k -頂点被覆のカーネル化

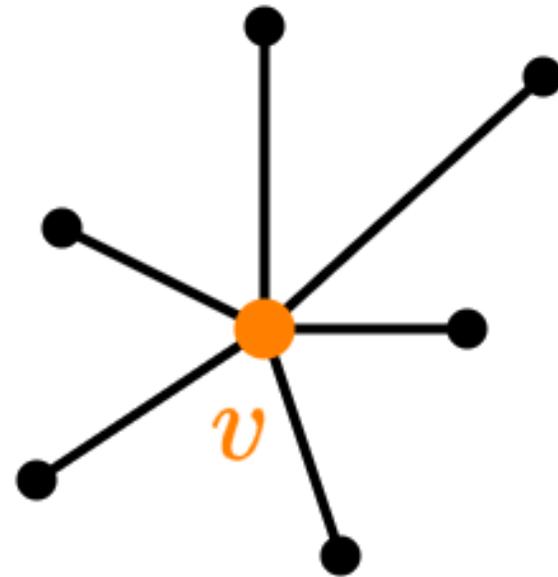
Rule 1. 孤立点 v がある時, $(G, k) \rightarrow (G - v, k)$

Buss-Goldsmithによる k -頂点被覆のカーネル化

Rule 1. 孤立点 v がある時、 $(G, k) \rightarrow (G - v, k)$

Rule 2. **次数 $k + 1$ 以上**の頂点 v がある時、

v を選ばなければ、
 v と接続する頂点を全て
選ばないといけない

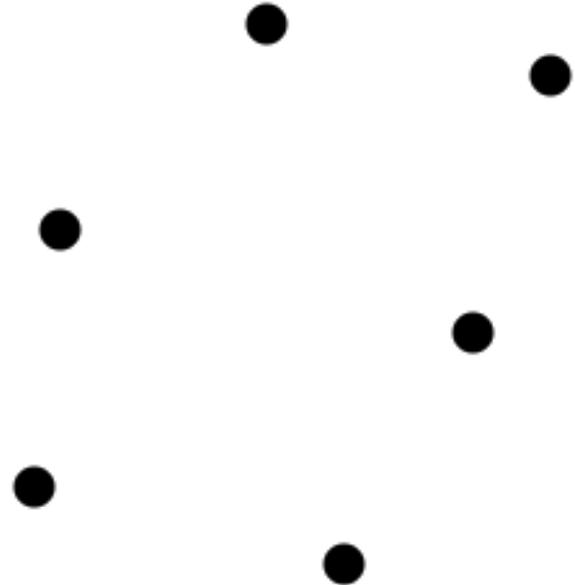


Buss-Goldsmithによる k -頂点被覆のカーネル化

Rule 1. 孤立点 v がある時、 $(G, k) \rightarrow (G - v, k)$

Rule 2. **次数 $k + 1$ 以上の頂点 v がある時、 $(G, k) \rightarrow (G - v, k - 1)$**

サイズ k 以下の頂点被覆
は必ず v を含む。



Buss-Goldsmithによる k -頂点被覆のカーネル化

Rule 1. 孤立点 v がある時、 $(G, k) \rightarrow (G - v, k)$

Rule 2. 次数 $k + 1$ 以上の頂点 v がある時、 $(G, k) \rightarrow (G - v, k - 1)$

サイズ k 以下の頂点被覆
は必ず v を含む。

事実: Rule1, 2の適用後 G の辺の本数が
 k^2 本より多いならNoインスタンス

新しいアプローチ: 量子クエリカーネル化

入力: **量子オラクル**でアクセスするインスタンス (G, k)

出力: **ビット列として**別の**等価な**インスタンス (G', k') を得る

or (G, k) がYesインスタンス or Noインスタンスだと断定

- (G, k) がYesインスタンス $\Leftrightarrow (G', k')$ がYesインスタンス

新しいアプローチ: 量子クエリカーネル化

入力: 量子オラクルでアクセスするインスタンス (G, k)

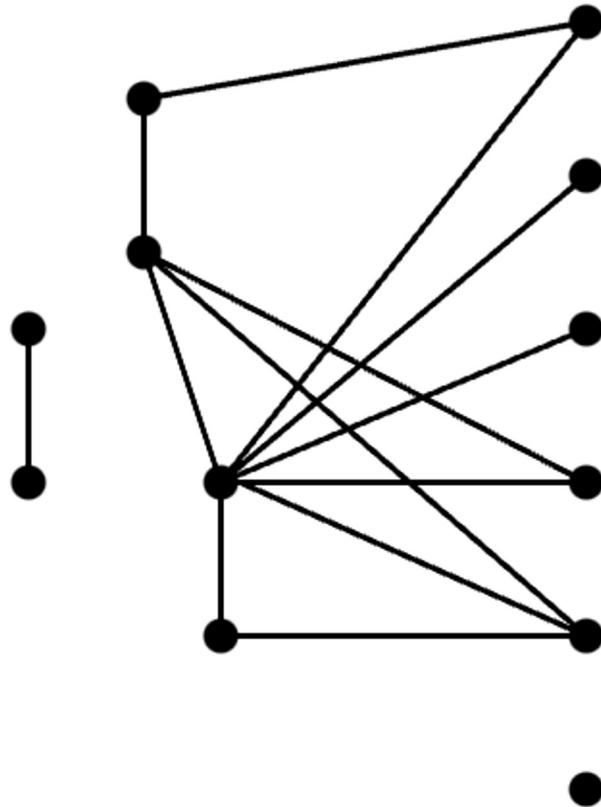
出力: **ビット列として**別の**等価な**インスタンス (G', k') を得る

or (G, k) がYesインスタンス or Noインスタンスだと断定

- (G, k) がYesインスタンス $\Leftrightarrow (G', k')$ がYesインスタンス

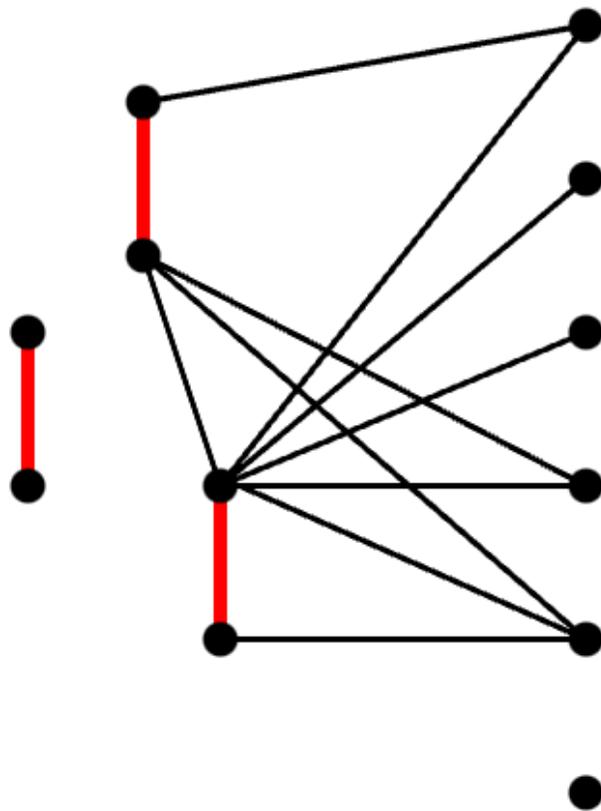
 量子クエリカーネル化後は、 (G', k') に
古典のアルゴリズムを適用するだけ!

k -頂点被覆問題に対する 量子に適した(古典の)カーネル化



k -頂点被覆問題に対する 量子に適した(古典の)カーネル化

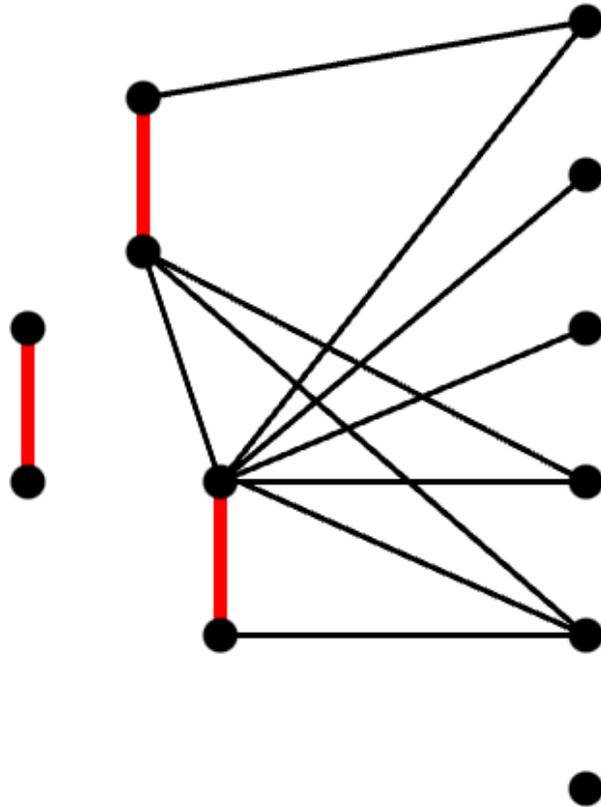
Step1 極大マッチング M を見つける



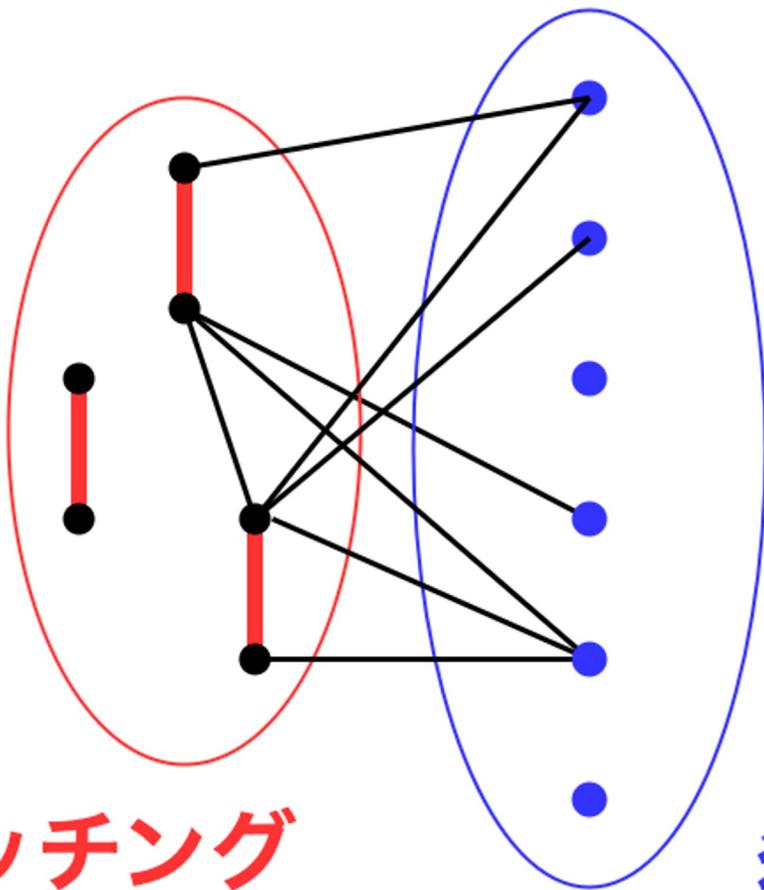
k -頂点被覆問題に対する 量子に適した(古典の)カーネル化

Step1 極大マッチング M を見つける

if $|M| > k$: then Noインスタンス



重要な観察: 極大マッチングの構造



極大マッチング

独立集合



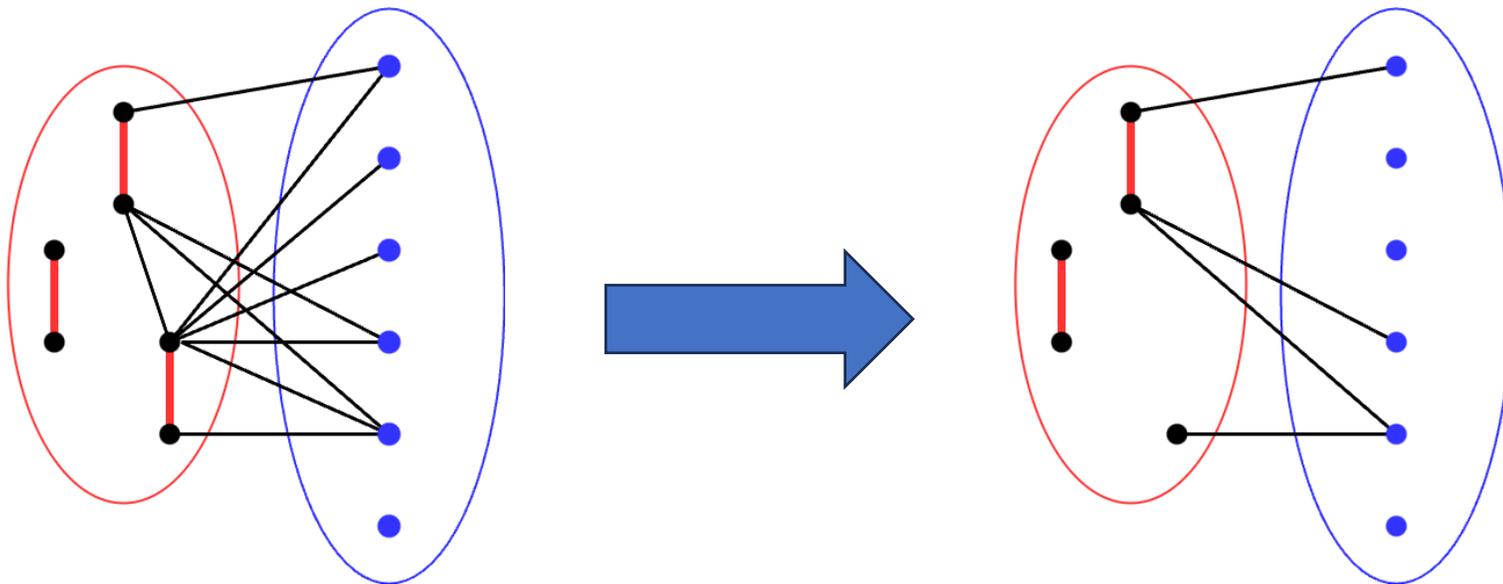
すべての辺は、極大マッチングの端点を端点としてもつ！

k -頂点被覆問題に対する 量子に適した(古典の)カーネル化

Step1 極大マッチング M を見つける
if $|M| > k$: then Noインスタンス

Step2 **M に属す辺の各端点 v のみ**に対して, **Rule 2**を適用

Rule 2 次数 $k + 1$ 以上の頂点 v がある時、 **$(G, k) \rightarrow (G - v, k - 1)$**

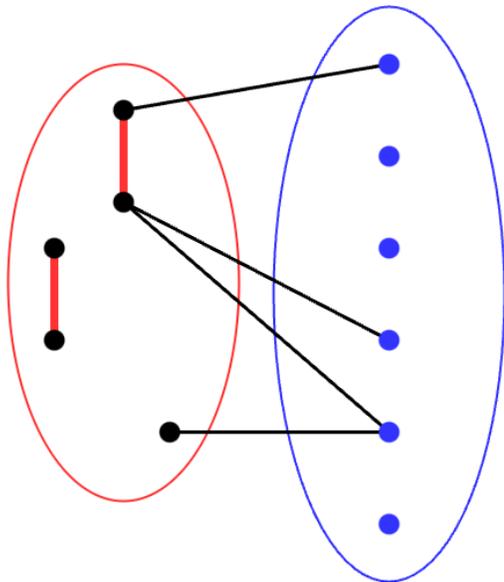


k -頂点被覆問題に対する 量子に適した(古典の)カーネル化

Step1 極大マッチング M を見つける
if $|M| > k$: then Noインスタンス

Step2 M に属す辺の各端点 v のみに対して, **Rule 2**を適用

Rule 2 次数 $k + 1$ 以上の頂点 v がある時、 $(G, k) \rightarrow (G - v, k - 1)$



補題:

Step1, 2の後, $|E(G)| \leq 2k^2$

k -頂点被覆問題に対する量子クエリカーネル化

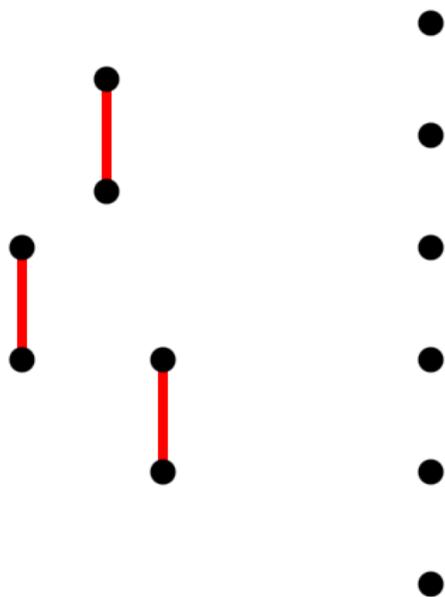
サイズ $k + 1$ 以上のマッチング

Step1 **Grover**探索で

or

を見つける

サイズ k 以下の極大マッチング



補題: Step1は $O(\sqrt{kn})$ クエリでできる

k -頂点被覆問題に対する量子クエリカーネル化

サイズ $k+1$ 以上のマッチング

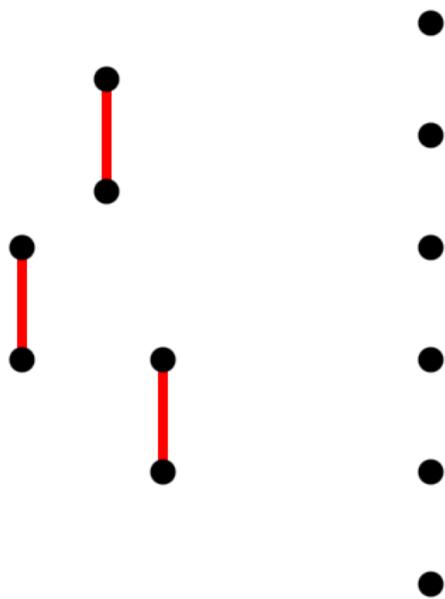
Step1 Grover探索で

or

をみつける

サイズ k 以下

Noインスタンス



補題: Step1は $O(\sqrt{kn})$ クエリでできる

k -頂点被覆問題に対する量子クエリカーネル化

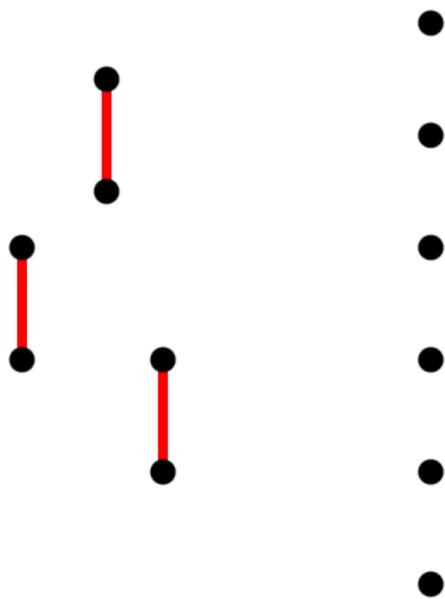
サイズ $k + 1$ 以上のマッチング

Step1 Grover探索で

or

を見つける

サイズ k 以下の極大マッチング



補題: Step1は $O(\sqrt{kn})$ クエリでできる

k -頂点被覆問題に対する量子クエリカーネル化

サイズ $k + 1$ 以上のマッチング

Step1

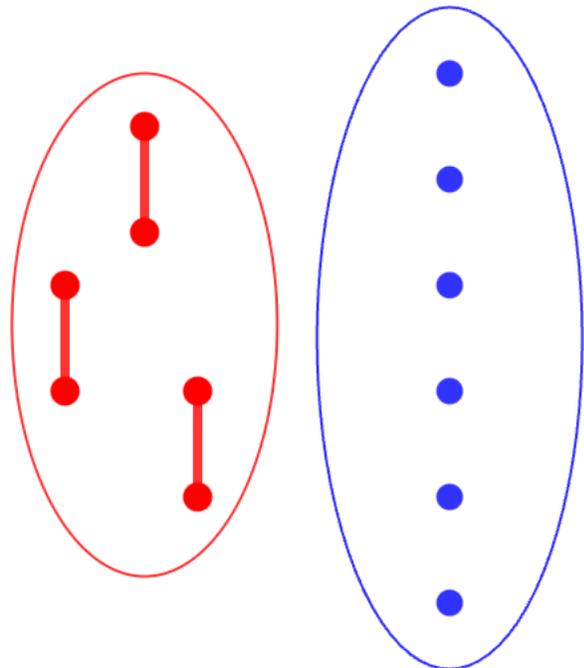
or

を見つける

サイズ k 以下の極大マッチング M

Step2

M に属す辺の各端点 v のみに対して、



k -頂点被覆問題に対する量子クエリカーネル化

サイズ $k + 1$ 以上のマッチング

Step1

or

を見つける

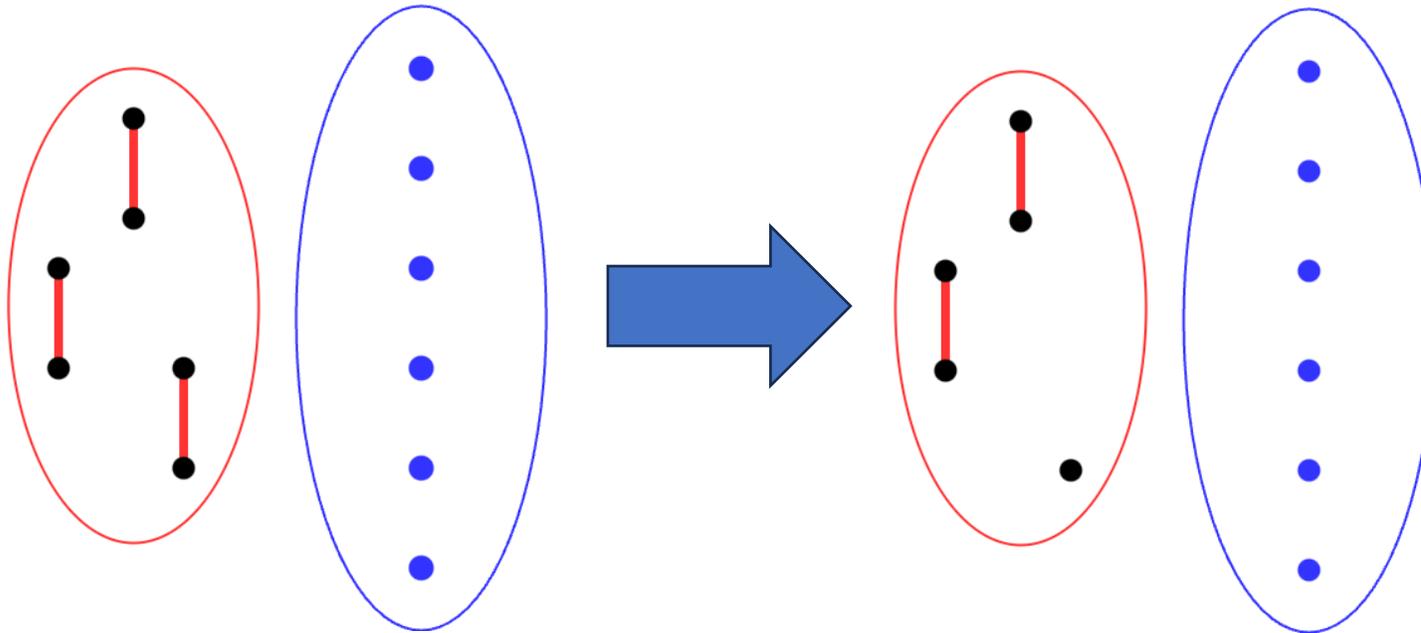
サイズ k 以下の極大マッチング M

Step2

M に属す辺の各端点 v のみに対して、

if v の次数 $> k$: then v を削除, $k \leftarrow k - 1$

else: v と接続する辺を全てみつける



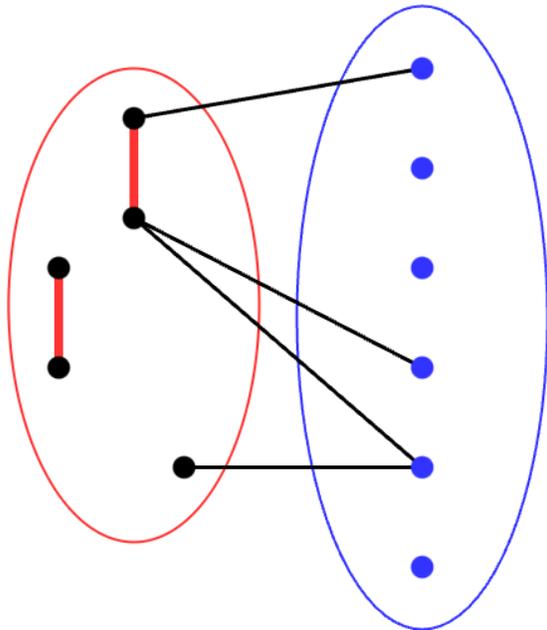
k -頂点被覆問題に対する量子クエリカーネル化

サイズ $k + 1$ 以上のマッチング

Step1 or をみつける

サイズ k 以下の極大マッチング M

Step2 M に属す辺の各端点 v のみに対して、
if v の次数 $> k$: then v を削除, $k \leftarrow k - 1$
else: v と接続する辺をGrover探索で全てみつける



k -頂点被覆問題に対する量子クエリカーネル化

サイズ $k + 1$ 以上のマッチング

Step1

or

を見つける

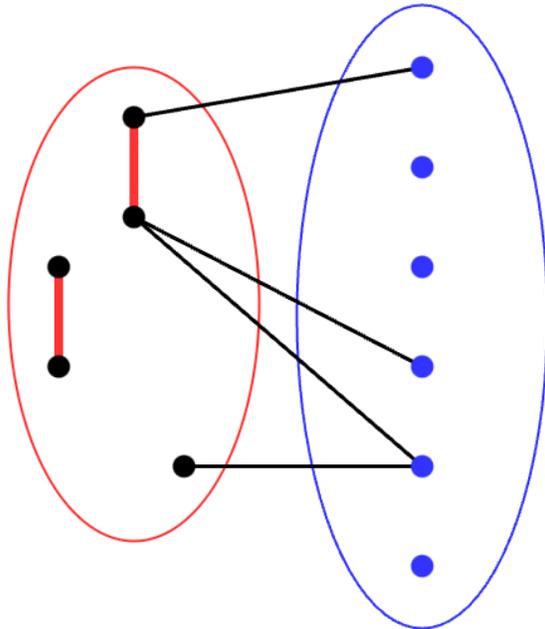
サイズ k 以下の極大マッチング M

Step2

M に属す辺の各端点 v のみに対して、

if v の次数 $> k$: then v を削除, $k \leftarrow k - 1$

else: v と接続する辺をGrover探索で全てを見つける



カーネルをビット列として
得た！

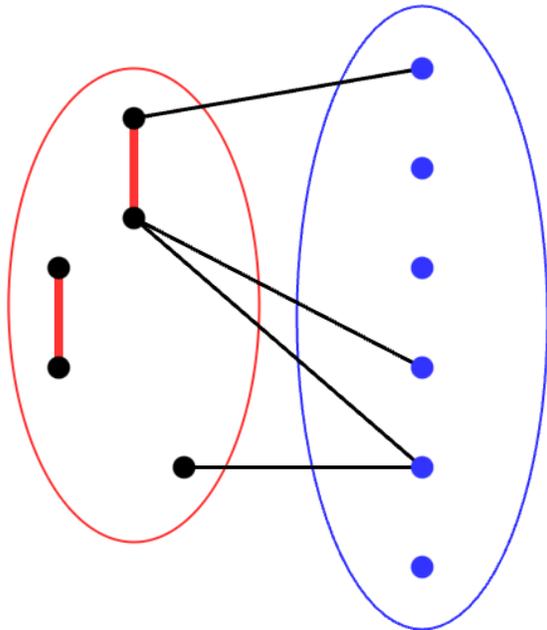
k -頂点被覆問題に対する量子クエリカーネル化

サイズ $k + 1$ 以上のマッチング

Step1 or をみつける

サイズ k 以下の極大マッチング M

Step2 M に属す辺の各端点 v のみに対して、
if v の次数 $> k$: then v を削除, $k \leftarrow k - 1$
else: v と接続する辺をGrover探索で全てみつける



補題:

Step2は $O(k^{3/2}\sqrt{n})$ クエリ
でできる

k -頂点被覆問題に対する量子クエリカーネル化

サイズ $k + 1$ 以上のマッチング

Step1 Grover探索で

or

をみつける

サイズ k 以下の極大マッチング

$O(\sqrt{kn})$ クエリ

Step2 M に属す辺の各端点 v のみに対して、

if v の次数 $> k$: then v を削除, $k \leftarrow k - 1$

else: v と接続する辺をGrover探索で全てみつける

$O(k^{3/2}\sqrt{n})$ クエリ

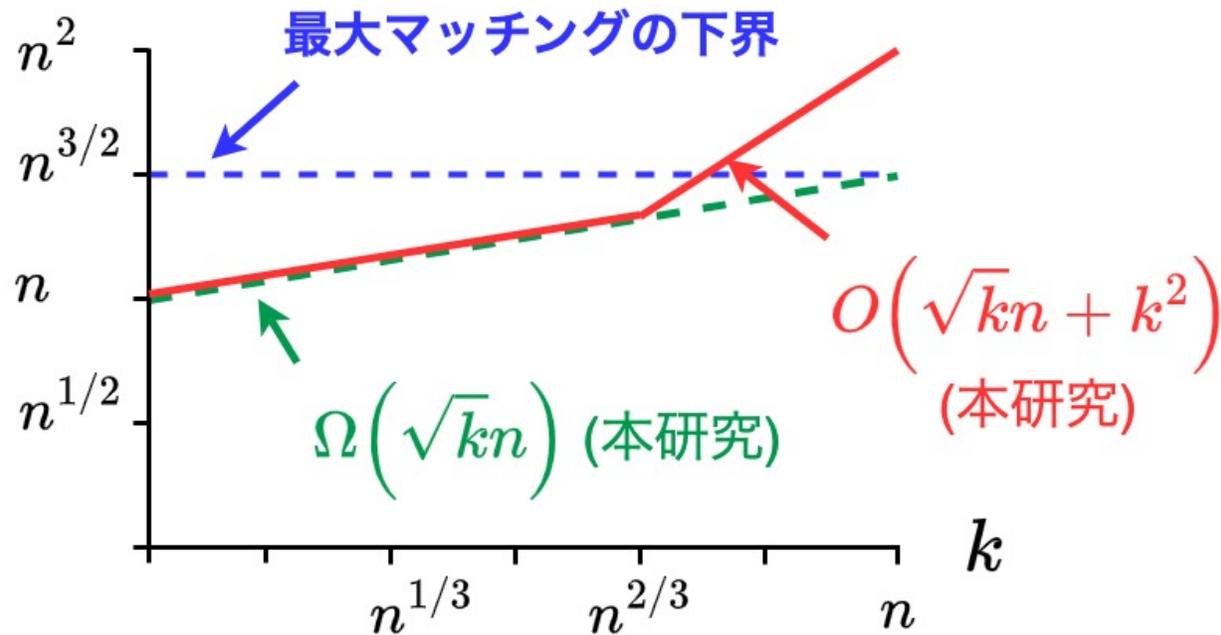
主結果②: マッチング問題に対する パラメータ化量子クエリ計算量

定理

大きさ k 以上のマッチングを持つかの判定問題の量子クエリ計算量

上界: $O(\sqrt{kn} + k^2)$

下界: $\Omega(\sqrt{kn})$



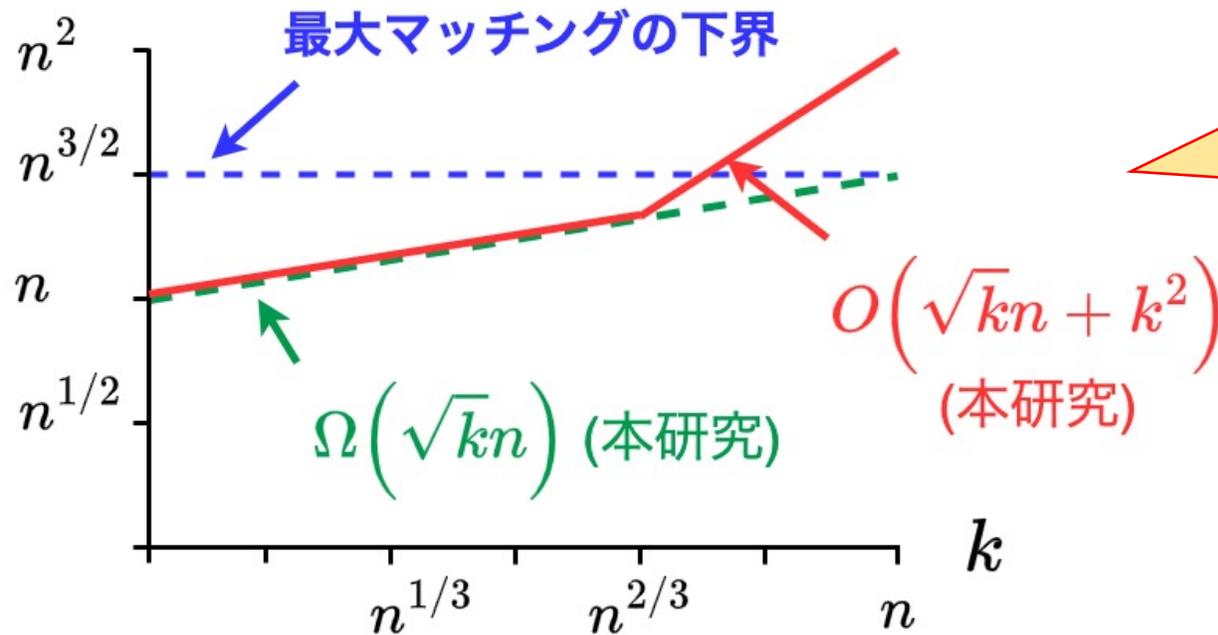
主結果②: マッチング問題に対する パラメータ化量子クエリ計算量

定理

大きさ k 以上のマッチングを持つかの判定問題の量子クエリ計算量

上界: $O(\sqrt{kn} + k^2)$

下界: $\Omega(\sqrt{kn})$



$k = O(n^{2/3})$ のとき
 $\Theta(\sqrt{kn})$ で最適！！

主結果②: マッチング問題に対する パラメータ化量子クエリ計算量

定理

大きさ k 以上のマッチングを持つかの判定問題の量子クエリ計算量

上界: $O(\sqrt{kn} + k^2)$

下界: $\Omega(\sqrt{kn})$

意義

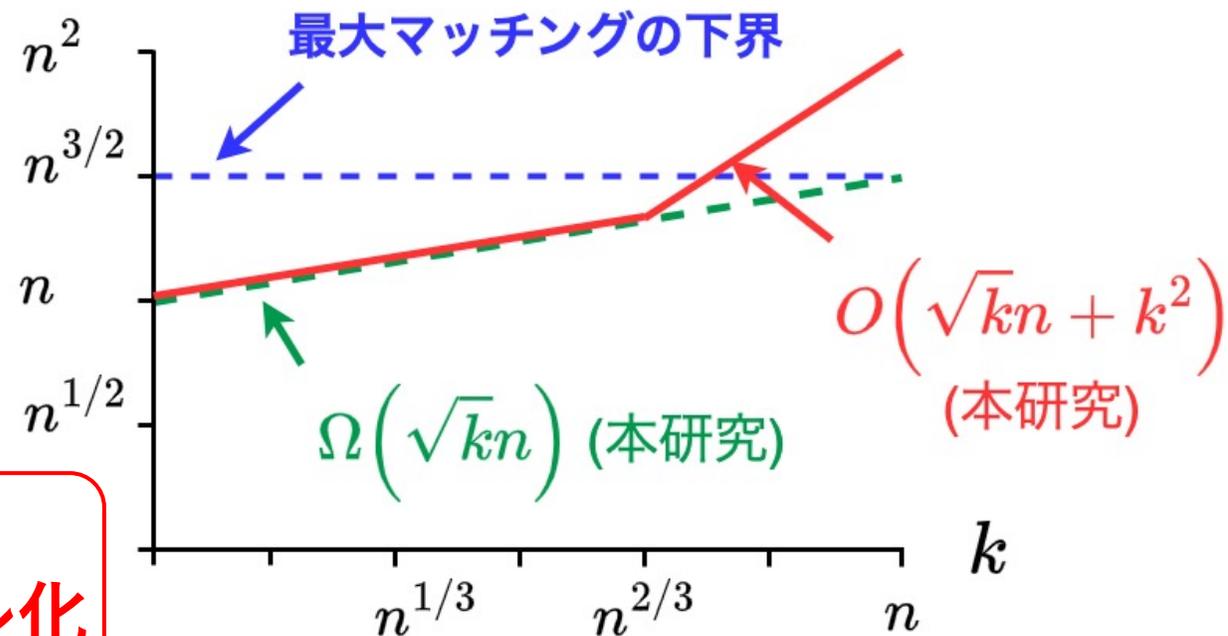
- 最大マッチングの上界 $O(n^{7/4})$

[Kimmel-Witter '21],

下界 $\Omega(n^{3/2})$ [Zhang '04] を
パラメータ化により改善

手法

- 増加路探索 + 量子クエリカーネル化



結論

- **パラメータ化量子クエリ計算量**について考察
- 頂点被覆問題とマッチング問題に対して、**パラメータがそんなに大きくない時に最適な**パラメータ化量子クエリ計算量を導出

結論

- **パラメータ化量子クエリ計算量**について考察
- 頂点被覆問題とマッチング問題に対して、**パラメータがそんなに大きくない時に最適なパラメータ化量子クエリ計算量**を導出

Message

 **カーネル化のような古典のテクニック**を賢く使うことで、量子クエリ計算量を改善できる！

Appendix

Quantum Query Algo for k -matching

a matching of size at least $k + 1$

Step1 Find

or

← $O(\sqrt{kn})$ queries

a maximal matching of size at most k

Quantum Query Algo for k -matching

a matching of size at least $k + 1$

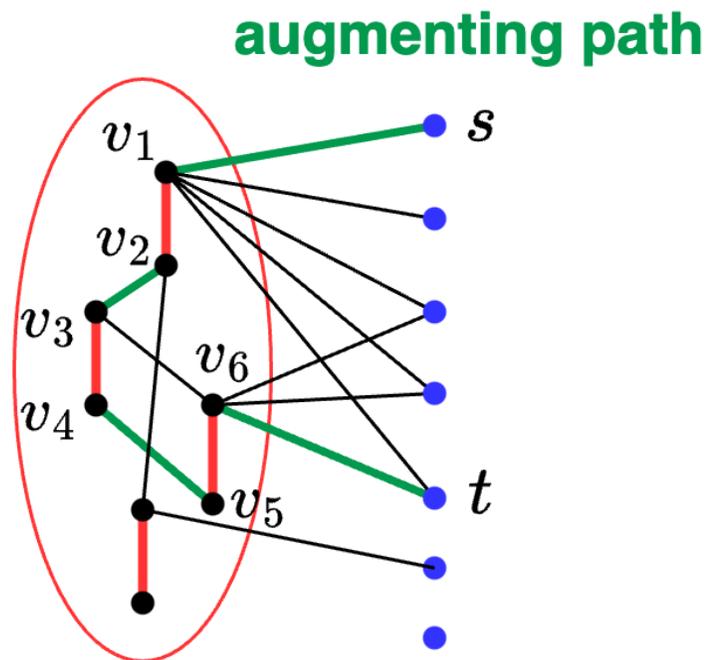
Step1 Find

or

← $O(\sqrt{kn})$ queries

a maximal matching M of size at most k

Step2 Repeatedly find an augmenting path and augment along it



maximal matching M

$|M|$ increases by 1!

Quantum Query Algo for k -matching

a matching of size at least $k + 1$

Step1 Find

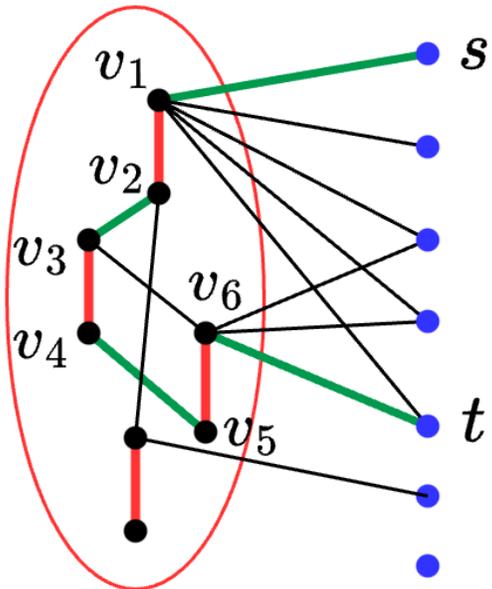
or

← $O(\sqrt{kn})$ queries

a maximal matching M of size at most k

Step2 Repeatedly find an augmenting path and augment along it

augmenting path



maximal matching M

Lem:

Step2 uses $O(k^2)$ queries +
amortized $O(\sqrt{n})$ queries per one
augmentation

Quantum Query Algo for k -matching

a matching of size at least $k + 1$

Step1 Find

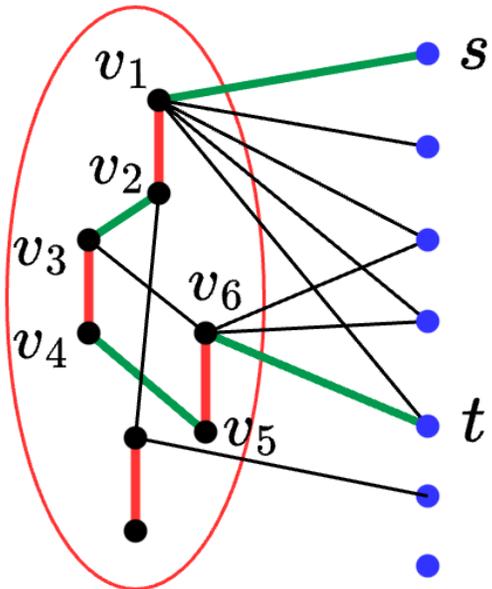
or

← $O(\sqrt{kn})$ queries

a maximal matching M of size at most k

Step2 Repeatedly find an augmenting path and augment along it

augmenting path



maximal matching M

Lem:

Step2 uses $O(k^2)$ queries +
amortized $O(\sqrt{n})$ queries per one
augmentation

$O(k^2 + k\sqrt{n})$ queries