Today's outline - March 22, 2022

Today's outline - March 22, 2022

- Generalization of Grover's algorithm

Today's outline - March 22, 2022

- Generalization of Grover's algorithm
- Geometry of amplitude amplification

Today's outline - March 22, 2022

- Generalization of Grover's algorithm
- Geometry of amplitude amplification
- Optimality of Grover's algorithm

Today's outline - March 22, 2022

- Generalization of Grover's algorithm
- Geometry of amplitude amplification
- Optimality of Grover's algorithm

Reading assignment: 9.5 – 9.6, 10.1

Today's outline - March 22, 2022

- Generalization of Grover's algorithm
- Geometry of amplitude amplification
- Optimality of Grover's algorithm

Reading assignment: 9.5 – 9.6, 10.1

Homework Assignment #06:
See Blackboard
Due Thursday, March 31, 2022

Today's outline - March 22, 2022

- Generalization of Grover's algorithm
- Geometry of amplitude amplification
- Optimality of Grover's algorithm

Reading assignment: 9.5 – 9.6, 10.1

Homework Assignment #06:
See Blackboard
Due Thursday, March 31, 2022

Quantum circuit simulator https://algassert.com/quirk

Generalization of Grover's algorithm

The first step in Grover's algorithm is to apply the $Q = -WS_0^\pi WS_G^\pi$ operator to an initial state $|\psi\rangle|-\rangle$

Generalization of Grover's algorithm

The first step in Grover's algorithm is to apply the $Q = -WS_0^\pi WS_G^\pi$ operator to an initial state $|\psi\rangle|-\rangle$

The initial state created by $W|0\rangle = |\psi\rangle$ has uniformly distributed intensities in all states

Generalization of Grover's algorithm

The first step in Grover's algorithm is to apply the $Q = -WS_0^{\pi}WS_G^{\pi}$ operator to an initial state $|\psi\rangle|-\rangle$

The initial state created by $W|0\rangle = |\psi\rangle$ has uniformly distributed intensities in all states

If, instead, we have a transformation U which applied to $|0\rangle$ gives a solution with higher probability, it is possible to generalize Grover's algorithm

Generalization of Grover's algorithm

The first step in Grover's algorithm is to apply the $Q = -WS_0^{\pi} WS_G^{\pi}$ operator to an initial state $|\psi\rangle|-\rangle$

The initial state created by $W|0\rangle = |\psi\rangle$ has uniformly distributed intensities in all states

If, instead, we have a transformation U which applied to $|0\rangle$ gives a solution with higher probability, it is possible to generalize Grover's algorithm

As before, divide the space spanned by $|x\rangle$ into a good subspace $\mathcal{G}$ spanned by $\{|x\rangle | x \in G\}$ and a bad subspace $\mathcal{B}$ spanned by $\{|x\rangle | x \notin G\}$ with projection operators $P_{\mathcal{G}}$ and $P_{\mathcal{B}}$ respectively

Generalization of Grover's algorithm

The first step in Grover's algorithm is to apply the $Q = -WS_0^{\pi} WS_G^{\pi}$ operator to an initial state $|\psi\rangle|-\rangle$

The initial state created by $W|0\rangle = |\psi\rangle$ has uniformly distributed intensities in all states

If, instead, we have a transformation U which applied to $|0\rangle$ gives a solution with higher probability, it is possible to generalize Grover's algorithm

As before, divide the space spanned by $|x\rangle$ into a good subspace $\mathcal{G}$ spanned by $\{|x\rangle|x \in G\}$ and a bad subspace $\mathcal{B}$ spanned by $\{|x\rangle|x \notin G\}$ with projection operators $P_{\mathcal{G}}$ and $P_{\mathcal{B}}$ respectively

The state $|\psi\rangle$ is generated by U

Generalization of Grover's algorithm

The first step in Grover's algorithm is to apply the $Q = -WS_0^\pi WS_G^\pi$ operator to an initial state $|\psi\rangle|-\rangle$

The initial state created by $W|0\rangle = |\psi\rangle$ has uniformly distributed intensities in all states

If, instead, we have a transformation U which applied to $|0\rangle$ gives a solution with higher probability, it is possible to generalize Grover's algorithm

As before, divide the space spanned by $|x\rangle$ into a good subspace $\mathcal{G}$ spanned by $\{|x\rangle|x \in G\}$ and a bad subspace $\mathcal{B}$ spanned by $\{|x\rangle|x \notin G\}$ with projection operators $P_\mathcal{G}$ and $P_\mathcal{B}$ respectively

The state $|\psi\rangle$ is generated by U

$$|\psi\rangle = U|0\rangle$$

Generalization of Grover's algorithm

The first step in Grover's algorithm is to apply the $Q = -WS_0^\pi WS_G^\pi$ operator to an initial state $|\psi\rangle|-\rangle$

The initial state created by $W|0\rangle = |\psi\rangle$ has uniformly distributed intensities in all states

If, instead, we have a transformation U which applied to $|0\rangle$ gives a solution with higher probability, it is possible to generalize Grover's algorithm

As before, divide the space spanned by $|x\rangle$ into a good subspace $\mathcal{G}$ spanned by $\{|x\rangle|x \in G\}$ and a bad subspace $\mathcal{B}$ spanned by $\{|x\rangle|x \notin G\}$ with projection operators $P_\mathcal{G}$ and $P_\mathcal{B}$ respectively

The state $|\psi\rangle$ is generated by U

$$|\psi\rangle = U|0\rangle$$

and can be written

Generalization of Grover's algorithm

The first step in Grover's algorithm is to apply the $Q = -WS_0^\pi WS_G^\pi$ operator to an initial state $|\psi\rangle|-\rangle$

The initial state created by $W|0\rangle = |\psi\rangle$ has uniformly distributed intensities in all states

If, instead, we have a transformation U which applied to $|0\rangle$ gives a solution with higher probability, it is possible to generalize Grover's algorithm

As before, divide the space spanned by $|x\rangle$ into a good subspace $\mathcal{G}$ spanned by $\{|x\rangle | x \in G\}$ and a bad subspace $\mathcal{B}$ spanned by $\{|x\rangle | x \notin G\}$ with projection operators $P_\mathcal{G}$ and $P_\mathcal{B}$ respectively

The state $|\psi\rangle$ is generated by U

$$|\psi\rangle = U|0\rangle = g_0|\psi_G\rangle + b_0|\psi_B\rangle$$

and can be written

Generalization of Grover's algorithm

The first step in Grover's algorithm is to apply the $Q = -WS_0^\pi WS_G^\pi$ operator to an initial state $|\psi\rangle|-\rangle$

The initial state created by $W|0\rangle = |\psi\rangle$ has uniformly distributed intensities in all states

If, instead, we have a transformation U which applied to $|0\rangle$ gives a solution with higher probability, it is possible to generalize Grover's algorithm

As before, divide the space spanned by $|x\rangle$ into a good subspace $\mathcal{G}$ spanned by $\{|x\rangle | x \in G\}$ and a bad subspace $\mathcal{B}$ spanned by $\{|x\rangle | x \notin G\}$ with projection operators $P_\mathcal{G}$ and $P_\mathcal{B}$ respectively

The state $|\psi\rangle$ is generated by U

$$|\psi\rangle = U|0\rangle = g_0|\psi_G\rangle + b_0|\psi_B\rangle$$

and can be written

$$|\psi_G\rangle = \frac{1}{g_0}P_\mathcal{G}|\psi\rangle, \quad |\psi_B\rangle = \frac{1}{b_0}P_\mathcal{B}|\psi\rangle$$

Generalization of Grover's algorithm

The first step in Grover's algorithm is to apply the $Q = -WS_0^\pi WS_G^\pi$ operator to an initial state $|\psi\rangle|-\rangle$

The initial state created by $W|0\rangle = |\psi\rangle$ has uniformly distributed intensities in all states

If, instead, we have a transformation U which applied to $|0\rangle$ gives a solution with higher probability, it is possible to generalize Grover's algorithm

As before, divide the space spanned by $|x\rangle$ into a good subspace $\mathcal{G}$ spanned by $\{|x\rangle|x \in G\}$ and a bad subspace $\mathcal{B}$ spanned by $\{|x\rangle|x \notin G\}$ with projection operators $P_\mathcal{G}$ and $P_\mathcal{B}$ respectively

The state $|\psi\rangle$ is generated by U

$$|\psi\rangle = U|0\rangle = g_0|\psi_G\rangle + b_0|\psi_B\rangle$$

and can be written

$$|\psi_G\rangle = \frac{1}{g_0}P_\mathcal{G}|\psi\rangle, \quad |\psi_B\rangle = \frac{1}{b_0}P_\mathcal{B}|\psi\rangle$$

Since all states are normalized we can write

Generalization of Grover's algorithm

The first step in Grover's algorithm is to apply the $Q = -WS_0^\pi WS_G^\pi$ operator to an initial state $|\psi\rangle|-\rangle$

The initial state created by $W|0\rangle = |\psi\rangle$ has uniformly distributed intensities in all states

If, instead, we have a transformation U which applied to $|0\rangle$ gives a solution with higher probability, it is possible to generalize Grover's algorithm

As before, divide the space spanned by $|x\rangle$ into a good subspace $\mathcal{G}$ spanned by $\{|x\rangle | x \in G\}$ and a bad subspace $\mathcal{B}$ spanned by $\{|x\rangle | x \notin G\}$ with projection operators $P_\mathcal{G}$ and $P_\mathcal{B}$ respectively

The state $|\psi\rangle$ is generated by U

$$|\psi\rangle = U|0\rangle = g_0|\psi_G\rangle + b_0|\psi_B\rangle$$

and can be written

$$|\psi_G\rangle = \frac{1}{g_0}P_\mathcal{G}|\psi\rangle, \quad |\psi_B\rangle = \frac{1}{b_0}P_\mathcal{B}|\psi\rangle$$

Since all states are normalized we can write

$$g_0 = |P_\mathcal{G}|\psi\rangle|, \qquad b_0 = |P_\mathcal{B}|\psi\rangle|$$

Generalization of Grover's algorithm

The first step in Grover's algorithm is to apply the $Q = -WS_0^{\pi}WS_G^{\pi}$ operator to an initial state $|\psi\rangle|-\rangle$

The initial state created by $W|0\rangle = |\psi\rangle$ has uniformly distributed intensities in all states

If, instead, we have a transformation U which applied to $|0\rangle$ gives a solution with higher probability, it is possible to generalize Grover's algorithm

As before, divide the space spanned by $|x\rangle$ into a good subspace $\mathcal{G}$ spanned by $\{|x\rangle | x \in G\}$ and a bad subspace $\mathcal{B}$ spanned by $\{|x\rangle | x \notin G\}$ with projection operators $P_{\mathcal{G}}$ and $P_{\mathcal{B}}$ respectively

The state $|\psi\rangle$ is generated by U

$$|\psi\rangle = U|0\rangle = g_0|\psi_G\rangle + b_0|\psi_B\rangle$$

and can be written

$$|\psi_G\rangle = \frac{1}{g_0}P_{\mathcal{G}}|\psi\rangle, \quad |\psi_B\rangle = \frac{1}{b_0}P_{\mathcal{B}}|\psi\rangle$$

Since all states are normalized we can write

$$g_0 = |P_{\mathcal{G}}|\psi\rangle|, \qquad b_0 = |P_{\mathcal{B}}|\psi\rangle|$$

Note that U does not necessarily produce an equal superposition of all the good states and thus g_0 and b_0 are not determined only by the number of solutions

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi |\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^{\pi}U^{-1}S_G^{\pi}$ can be simplified by recalling that $S_0^{\pi}|\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi |\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big)$$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi|\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle$$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi|\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle = |\psi\rangle - 2\overline{\langle\psi|U|0\rangle}\, U|0\rangle$$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi|\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle = |\psi\rangle - 2\overline{\langle\psi|U|0\rangle}U|0\rangle$$

Since $S_G^\pi|\psi_G\rangle = -|\psi_G\rangle$ and $S_G^\pi|\psi_B\rangle = |\psi_B\rangle$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi |\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle = |\psi\rangle - 2\overline{\langle\psi|U|0\rangle}\,U|0\rangle$$

Since $S_G^\pi|\psi_G\rangle = -|\psi_G\rangle$ and $S_G^\pi|\psi_B\rangle = |\psi_B\rangle$

$$Q|\psi_G\rangle = -US_0^\pi U^{-1} S_G^\pi |\psi_G\rangle$$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi |\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle = |\psi\rangle - 2\overline{\langle\psi|U|0\rangle}\, U|0\rangle$$

Since $S_G^\pi|\psi_G\rangle = -|\psi_G\rangle$ and $S_G^\pi|\psi_B\rangle = |\psi_B\rangle$

$$Q|\psi_G\rangle = -US_0^\pi U^{-1} S_G^\pi |\psi_G\rangle = US_0^\pi U^{-1}|\psi_G\rangle$$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi|\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle = |\psi\rangle - 2\overline{\langle\psi|U|0\rangle}U|0\rangle$$

Since $S_G^\pi|\psi_G\rangle = -|\psi_G\rangle$ and $S_G^\pi|\psi_B\rangle = |\psi_B\rangle$

$$Q|\psi_G\rangle = -US_0^\pi U^{-1} S_G^\pi|\psi_G\rangle = US_0^\pi U^{-1}|\psi_G\rangle = |\psi_G\rangle - 2\overline{g_0}U|0\rangle$$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi|\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle = |\psi\rangle - 2\overline{\langle\psi|U|0\rangle}\,U|0\rangle$$

Since $S_G^\pi|\psi_G\rangle = -|\psi_G\rangle$ and $S_G^\pi|\psi_B\rangle = |\psi_B\rangle$

$$\begin{aligned} Q|\psi_G\rangle &= -US_0^\pi U^{-1}S_G^\pi|\psi_G\rangle = US_0^\pi U^{-1}|\psi_G\rangle = |\psi_G\rangle - 2\overline{g_0}\,U|0\rangle \\ &= |\psi_G\rangle - 2\overline{g_0}g_0|\psi_G\rangle - 2\overline{g_0}b_0|\psi_B\rangle \end{aligned}$$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi|\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle = |\psi\rangle - 2\overline{\langle\psi|U|0\rangle}U|0\rangle$$

Since $S_G^\pi|\psi_G\rangle = -|\psi_G\rangle$ and $S_G^\pi|\psi_B\rangle = |\psi_B\rangle$

$$Q|\psi_G\rangle = -US_0^\pi U^{-1} S_G^\pi|\psi_G\rangle = US_0^\pi U^{-1}|\psi_G\rangle = |\psi_G\rangle - 2\overline{g_0}U|0\rangle$$

$$= |\psi_G\rangle - 2\overline{g_0}g_0|\psi_G\rangle - 2\overline{g_0}b_0|\psi_B\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle$$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi |\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle = |\psi\rangle - 2\overline{\langle\psi|U|0\rangle}\,U|0\rangle$$

Since $S_G^\pi|\psi_G\rangle = -|\psi_G\rangle$ and $S_G^\pi|\psi_B\rangle = |\psi_B\rangle$

$$\begin{aligned} Q|\psi_G\rangle &= -US_0^\pi U^{-1} S_G^\pi|\psi_G\rangle = US_0^\pi U^{-1}|\psi_G\rangle = |\psi_G\rangle - 2\overline{g_0}\,U|0\rangle \\ &= |\psi_G\rangle - 2\overline{g_0}g_0|\psi_G\rangle - 2\overline{g_0}b_0|\psi_B\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle \\ Q|\psi_B\rangle &= -US_0^\pi U^{-1} S_G^\pi|\psi_B\rangle \end{aligned}$$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^{\pi}U^{-1}S_G^{\pi}$ can be simplified by recalling that $S_0^{\pi}|\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^{\pi}U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle = |\psi\rangle - 2\overline{\langle\psi|U|0\rangle}U|0\rangle$$

Since $S_G^{\pi}|\psi_G\rangle = -|\psi_G\rangle$ and $S_G^{\pi}|\psi_B\rangle = |\psi_B\rangle$

$$Q|\psi_G\rangle = -US_0^{\pi}U^{-1}S_G^{\pi}|\psi_G\rangle = US_0^{\pi}U^{-1}|\psi_G\rangle = |\psi_G\rangle - 2\overline{g_0}U|0\rangle$$

$$= |\psi_G\rangle - 2\overline{g_0}g_0|\psi_G\rangle - 2\overline{g_0}b_0|\psi_B\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle$$

$$Q|\psi_B\rangle = -US_0^{\pi}U^{-1}S_G^{\pi}|\psi_B\rangle = -|\psi_B\rangle + 2\overline{b_0}U|0\rangle$$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi|\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle = |\psi\rangle - 2\overline{\langle\psi|U|0\rangle}\, U|0\rangle$$

Since $S_G^\pi|\psi_G\rangle = -|\psi_G\rangle$ and $S_G^\pi|\psi_B\rangle = |\psi_B\rangle$

$$\begin{aligned} Q|\psi_G\rangle &= -US_0^\pi U^{-1} S_G^\pi|\psi_G\rangle = US_0^\pi U^{-1}|\psi_G\rangle = |\psi_G\rangle - 2\overline{g_0}\, U|0\rangle \\ &= |\psi_G\rangle - 2\overline{g_0} g_0|\psi_G\rangle - 2\overline{g_0} b_0|\psi_B\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle \\ Q|\psi_B\rangle &= -US_0^\pi U^{-1} S_G^\pi|\psi_B\rangle = -|\psi_B\rangle + 2\overline{b_0}\, U|0\rangle = -|\psi_B\rangle + 2\overline{b_0} g_0|\psi_G\rangle + 2\overline{b_0} b_0|\psi_B\rangle \end{aligned}$$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1} S_G^\pi$ can be simplified by recalling that $S_0^\pi|\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle = |\psi\rangle - 2\overline{\langle\psi|U|0\rangle}U|0\rangle$$

Since $S_G^\pi|\psi_G\rangle = -|\psi_G\rangle$ and $S_G^\pi|\psi_B\rangle = |\psi_B\rangle$

$$\begin{aligned} Q|\psi_G\rangle &= -US_0^\pi U^{-1} S_G^\pi|\psi_G\rangle = US_0^\pi U^{-1}|\psi_G\rangle = |\psi_G\rangle - 2\overline{g_0}U|0\rangle \\ &= |\psi_G\rangle - 2\overline{g_0}g_0|\psi_G\rangle - 2\overline{g_0}b_0|\psi_B\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle \\ Q|\psi_B\rangle &= -US_0^\pi U^{-1} S_G^\pi|\psi_B\rangle = -|\psi_B\rangle + 2\overline{b_0}U|0\rangle = -|\psi_B\rangle + 2\overline{b_0}g_0|\psi_G\rangle + 2\overline{b_0}b_0|\psi_B\rangle \\ &= -|\psi_B\rangle + 2(1-t)\tfrac{g_0}{b_0}|\psi_G\rangle + 2(1-t)|\psi_B\rangle \end{aligned}$$

Generalization of Grover's algorithm

Since g_0 and b_0 are real, define $t = g_0^2$ and $1 - t = b_0^2$ so that t is the probability that the reversible algorithm U maps $|0\rangle$ to a set of solutions in G

The goal of determining the effect of the transformation $Q = -US_0^\pi U^{-1}S_G^\pi$ can be simplified by recalling that $S_0^\pi|\phi\rangle \equiv |\phi\rangle - 2\langle 0|\phi\rangle|0\rangle$

Thus, for an arbitrary state $|\psi\rangle$

$$US_0^\pi U^{-1}|\psi\rangle = U\big(U^{-1}|\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle|0\rangle\big) = |\psi\rangle - 2\langle 0|U^{-1}|\psi\rangle U|0\rangle = |\psi\rangle - 2\overline{\langle\psi|U|0\rangle}U|0\rangle$$

Since $S_G^\pi|\psi_G\rangle = -|\psi_G\rangle$ and $S_G^\pi|\psi_B\rangle = |\psi_B\rangle$

$$\begin{aligned}
Q|\psi_G\rangle &= -US_0^\pi U^{-1}S_G^\pi|\psi_G\rangle = US_0^\pi U^{-1}|\psi_G\rangle = |\psi_G\rangle - 2\overline{g_0}U|0\rangle \\
&= |\psi_G\rangle - 2\overline{g_0}g_0|\psi_G\rangle - 2\overline{g_0}b_0|\psi_B\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle \\
Q|\psi_B\rangle &= -US_0^\pi U^{-1}S_G^\pi|\psi_B\rangle = -|\psi_B\rangle + 2\overline{b_0}U|0\rangle = -|\psi_B\rangle + 2\overline{b_0}g_0|\psi_G\rangle + 2\overline{b_0}b_0|\psi_B\rangle \\
&= -|\psi_B\rangle + 2(1-t)\tfrac{g_0}{b_0}|\psi_G\rangle + 2(1-t)|\psi_B\rangle = (1-2t)|\psi_B\rangle - 2\sqrt{t(1-t)}|\psi_G\rangle
\end{aligned}$$

Generalization of Grover's algorithm

$$Q|\psi_G\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle, \qquad Q|\psi_B\rangle = (1-2t)|\psi_B\rangle - 2\sqrt{t(1-t)}|\psi_G\rangle$$

Generalization of Grover's algorithm

$$Q|\psi_G\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle, \qquad Q|\psi_B\rangle = (1-2t)|\psi_B\rangle - 2\sqrt{t(1-t)}|\psi_G\rangle$$

Thus, applied to an arbitrary real superposition of $|\psi_G\rangle$ and $|\psi_B\rangle$

Generalization of Grover's algorithm

$$Q|\psi_G\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle, \qquad Q|\psi_B\rangle = (1-2t)|\psi_B\rangle - 2\sqrt{t(1-t)}|\psi_G\rangle$$

Thus, applied to an arbitrary real superposition of $|\psi_G\rangle$ and $|\psi_B\rangle$

$$Q(g_i|\psi_G\rangle + b_i|\psi_B\rangle) = \left(g_i(1-2t) + 2b_i\sqrt{t(1-t)}\right)|\psi_G\rangle + \left(b_i(1-2t) - 2g_i\sqrt{t(1-t)}\right)|\psi_B\rangle$$

Generalization of Grover's algorithm

$$Q|\psi_G\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle, \qquad Q|\psi_B\rangle = (1-2t)|\psi_B\rangle - 2\sqrt{t(1-t)}|\psi_G\rangle$$

Thus, applied to an arbitrary real superposition of $|\psi_G\rangle$ and $|\psi_B\rangle$

$$\begin{aligned} Q(g_i|\psi_G\rangle + b_i|\psi_B\rangle) &= \left(g_i(1-2t) + 2b_i\sqrt{t(1-t)}\right)|\psi_G\rangle + \left(b_i(1-2t) - 2g_i\sqrt{t(1-t)}\right)|\psi_B\rangle \\ &= g_{i+1}|\psi_G\rangle + b_{i+1}|\psi_B\rangle \end{aligned}$$

Generalization of Grover's algorithm

$$Q|\psi_G\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle, \qquad Q|\psi_B\rangle = (1-2t)|\psi_B\rangle - 2\sqrt{t(1-t)}|\psi_G\rangle$$

Thus, applied to an arbitrary real superposition of $|\psi_G\rangle$ and $|\psi_B\rangle$

$$\begin{aligned} Q(g_i|\psi_G\rangle + b_i|\psi_B\rangle) &= \left(g_i(1-2t) + 2b_i\sqrt{t(1-t)}\right)|\psi_G\rangle + \left(b_i(1-2t) - 2g_i\sqrt{t(1-t)}\right)|\psi_B\rangle \\ &= g_{i+1}|\psi_G\rangle + b_{i+1}|\psi_B\rangle \end{aligned}$$

Which give the same recursion relations and solutions as for $U = W$

Generalization of Grover's algorithm

$$Q|\psi_G\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle, \qquad Q|\psi_B\rangle = (1-2t)|\psi_B\rangle - 2\sqrt{t(1-t)}|\psi_G\rangle$$

Thus, applied to an arbitrary real superposition of $|\psi_G\rangle$ and $|\psi_B\rangle$

$$\begin{aligned} Q(g_i|\psi_G\rangle + b_i|\psi_B\rangle) &= \left(g_i(1-2t) + 2b_i\sqrt{t(1-t)}\right)|\psi_G\rangle + \left(b_i(1-2t) - 2g_i\sqrt{t(1-t)}\right)|\psi_B\rangle \\ &= g_{i+1}|\psi_G\rangle + b_{i+1}|\psi_B\rangle \end{aligned}$$

Which give the same recursion relations and solutions as for $U = W$

$$g_{i+1} = g_i(1-2t) + 2b_i\sqrt{t(1-t)}, \qquad b_{i+1} = b_i(1-2t) - 2g_i\sqrt{t(1-t)}$$

Generalization of Grover's algorithm

$$Q|\psi_G\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle, \qquad Q|\psi_B\rangle = (1-2t)|\psi_B\rangle - 2\sqrt{t(1-t)}|\psi_G\rangle$$

Thus, applied to an arbitrary real superposition of $|\psi_G\rangle$ and $|\psi_B\rangle$

$$\begin{aligned} Q(g_i|\psi_G\rangle + b_i|\psi_B\rangle) &= \left(g_i(1-2t) + 2b_i\sqrt{t(1-t)}\right)|\psi_G\rangle + \left(b_i(1-2t) - 2g_i\sqrt{t(1-t)}\right)|\psi_B\rangle \\ &= g_{i+1}|\psi_G\rangle + b_{i+1}|\psi_B\rangle \end{aligned}$$

Which give the same recursion relations and solutions as for $U = W$

$$g_{i+1} = g_i(1-2t) + 2b_i\sqrt{t(1-t)}, \qquad b_{i+1} = b_i(1-2t) - 2g_i\sqrt{t(1-t)}$$

$$g_i = \sin\left((2i+1)\theta\right), \qquad b_i = \cos\left((2i+1)\theta\right), \qquad \sin\theta = \sqrt{t} = g_0$$

Generalization of Grover's algorithm

$$Q|\psi_G\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle, \qquad Q|\psi_B\rangle = (1-2t)|\psi_B\rangle - 2\sqrt{t(1-t)}|\psi_G\rangle$$

Thus, applied to an arbitrary real superposition of $|\psi_G\rangle$ and $|\psi_B\rangle$

$$\begin{aligned} Q(g_i|\psi_G\rangle + b_i|\psi_B\rangle) &= \left(g_i(1-2t) + 2b_i\sqrt{t(1-t)}\right)|\psi_G\rangle + \left(b_i(1-2t) - 2g_i\sqrt{t(1-t)}\right)|\psi_B\rangle \\ &= g_{i+1}|\psi_G\rangle + b_{i+1}|\psi_B\rangle \end{aligned}$$

Which give the same recursion relations and solutions as for $U = W$

$$g_{i+1} = g_i(1-2t) + 2b_i\sqrt{t(1-t)}, \qquad b_{i+1} = b_i(1-2t) - 2g_i\sqrt{t(1-t)}$$

$$g_i = \sin\left((2i+1)\theta\right), \qquad b_i = \cos\left((2i+1)\theta\right), \qquad \sin\theta = \sqrt{t} = g_0$$

For small g_0, g_i will be maximal after $i \approx \frac{\pi}{4g_0}$ iterations

Generalization of Grover's algorithm

$$Q|\psi_G\rangle = (1-2t)|\psi_G\rangle - 2\sqrt{t(1-t)}|\psi_B\rangle, \qquad Q|\psi_B\rangle = (1-2t)|\psi_B\rangle - 2\sqrt{t(1-t)}|\psi_G\rangle$$

Thus, applied to an arbitrary real superposition of $|\psi_G\rangle$ and $|\psi_B\rangle$

$$\begin{aligned} Q(g_i|\psi_G\rangle + b_i|\psi_B\rangle) &= \left(g_i(1-2t) + 2b_i\sqrt{t(1-t)}\right)|\psi_G\rangle + \left(b_i(1-2t) - 2g_i\sqrt{t(1-t)}\right)|\psi_B\rangle \\ &= g_{i+1}|\psi_G\rangle + b_{i+1}|\psi_B\rangle \end{aligned}$$

Which give the same recursion relations and solutions as for $U = W$

$$g_{i+1} = g_i(1-2t) + 2b_i\sqrt{t(1-t)}, \qquad b_{i+1} = b_i(1-2t) - 2g_i\sqrt{t(1-t)}$$

$$g_i = \sin\left((2i+1)\theta\right), \qquad b_i = \cos\left((2i+1)\theta\right), \qquad \sin\theta = \sqrt{t} = g_0$$

For small g_0, g_i will be maximal after $i \approx \frac{\pi}{4g_0}$ iterations

Amplitude amplification allows a solution to be found in $O(\sqrt{1/t})$ iterations unless, $g_0 = 0$ or if it is large

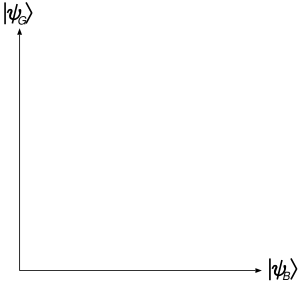
Geometry of amplitude amplification

The transformation consists of repeated applications of $Q = -US_0^{\pi}U^{-1}S_G^{\pi}$

Geometry of amplitude amplification

The transformation consists of repeated applications of $Q = -US_0^\pi U^{-1} S_G^\pi$

Consider the hyperplane spanned by $\{|\psi_G\rangle, |\psi_B\rangle\}$

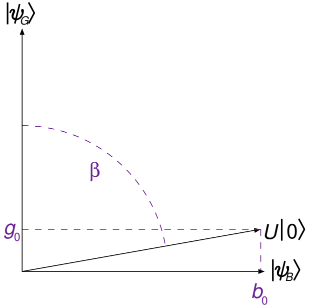


Geometry of amplitude amplification

The transformation consists of repeated applications of $Q = -US_0^\pi U^{-1} S_G^\pi$

Consider the hyperplane spanned by $\{|\psi_G\rangle, |\psi_B\rangle\}$

The application of U to $|0\rangle$ produces a state $|\psi_0\rangle = g_0|\psi_G\rangle + b_0|\psi_B\rangle$



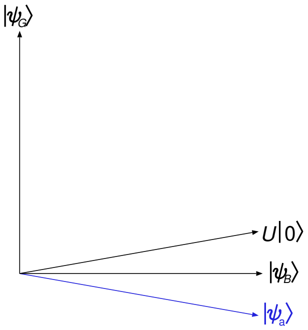
Geometry of amplitude amplification

The transformation consists of repeated applications of $Q = -US_0^{\pi}U^{-1}S_G^{\pi}$

Consider the hyperplane spanned by $\{|\psi_G\rangle, |\psi_B\rangle\}$

The application of U to $|0\rangle$ produces a state $|\psi_0\rangle = g_0|\psi_G\rangle + b_0|\psi_B\rangle$

The transformation S_G^{π} is a reflection about a plane perpendicular to $|\psi_G\rangle$, in this case $|\psi_B\rangle$



Geometry of amplitude amplification

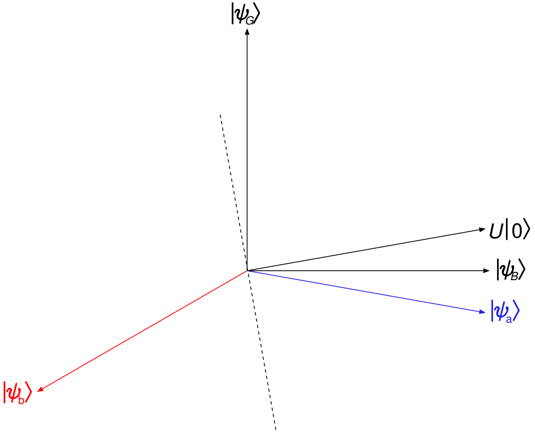
The transformation consists of repeated applications of $Q = -US_0^\pi U^{-1} S_G^\pi$

Consider the hyperplane spanned by $\{|\psi_G\rangle, |\psi_B\rangle\}$

The application of U to $|0\rangle$ produces a state $|\psi_0\rangle = g_0|\psi_G\rangle + b_0|\psi_B\rangle$

The transformation S_G^π is a reflection about a plane perpendicular to $|\psi_G\rangle$, in this case $|\psi_B\rangle$

The transformation $US_0^\pi U^{-1}$ is a reflection about a plane perpendicular to $U|0\rangle$



Geometry of amplitude amplification

The transformation consists of repeated applications of $Q = -US_0^{\pi}U^{-1}S_G^{\pi}$

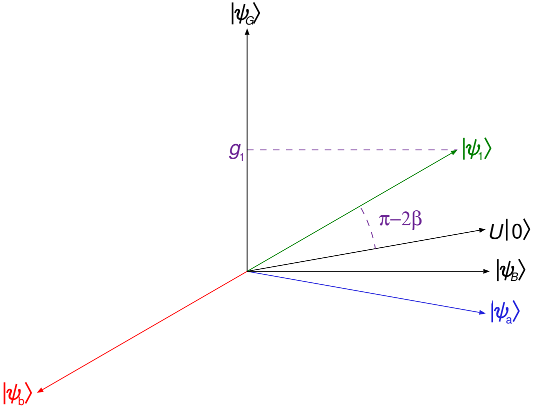
Consider the hyperplane spanned by $\{|\psi_G\rangle, |\psi_B\rangle\}$

The application of U to $|0\rangle$ produces a state $|\psi_0\rangle = g_0|\psi_G\rangle + b_0|\psi_B\rangle$

The transformation S_G^{π} is a reflection about a plane perpendicular to $|\psi_G\rangle$, in this case $|\psi_B\rangle$

The transformation $US_0^{\pi}U^{-1}$ is a reflection about a plane perpendicular to $U|0\rangle$

The negative sign simply inverts the state which is seen to have been rotated by $\pi-2\beta$



Geometry of amplitude amplification

The transformation consists of repeated applications of $Q = -US_0^\pi U^{-1} S_G^\pi$

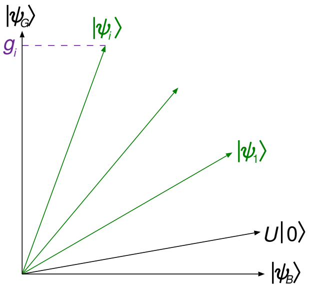
Consider the hyperplane spanned by $\{|\psi_G\rangle, |\psi_B\rangle\}$

The application of U to $|0\rangle$ produces a state $|\psi_0\rangle = g_0|\psi_G\rangle + b_0|\psi_B\rangle$

The transformation S_G^π is a reflection about a plane perpendicular to $|\psi_G\rangle$, in this case $|\psi_B\rangle$

The transformation $US_0^\pi U^{-1}$ is a reflection about a plane perpendicular to $U|0\rangle$

The negative sign simply inverts the state which is seen to have been rotated by $\pi - 2\beta$



Repeated applications bring g_i to its maximum whatever the arbitrary initial state

Optimality of Grover's algorithm

It is useful to prove that Grover's algorithm is the optimal search algorithm

Optimality of Grover's algorithm

It is useful to prove that Grover's algorithm is the optimal search algorithm

Suppose there is a single solution, x, to the oracle transformation, U_P

Optimality of Grover's algorithm

It is useful to prove that Grover's algorithm is the optimal search algorithm

Suppose there is a single solution, x, to the oracle transformation, U_P

Recall that the transformation S_x^π can be computed from the oracle, U_P, thus S_x^π can be used as the interface to the oracle with out loss of generality

Optimality of Grover's algorithm

It is useful to prove that Grover's algorithm is the optimal search algorithm

Suppose there is a single solution, x, to the oracle transformation, U_P

Recall that the transformation S_x^π can be computed from the oracle, U_P, thus S_x^π can be used as the interface to the oracle with out loss of generality

An arbitrary quantum search algorithm can be described as an alternating sequence of unitary transformations independent of x, U_i and calls to the oracle, S_x^π

Optimality of Grover's algorithm

It is useful to prove that Grover's algorithm is the optimal search algorithm

Suppose there is a single solution, x, to the oracle transformation, U_P

Recall that the transformation S_x^π can be computed from the oracle, U_P, thus S_x^π can be used as the interface to the oracle with out loss of generality

An arbitrary quantum search algorithm can be described as an alternating sequence of unitary transformations independent of x, U_i and calls to the oracle, S_x^π

$$|\psi_k^x\rangle = U_k S_x^\pi U_{k-1} S_x^\pi \dots U_1 S_x^\pi U_0 |0\rangle,$$

Optimality of Grover's algorithm

It is useful to prove that Grover's algorithm is the optimal search algorithm

Suppose there is a single solution, x, to the oracle transformation, U_P

Recall that the transformation S_x^π can be computed from the oracle, U_P, thus S_x^π can be used as the interface to the oracle with out loss of generality

An arbitrary quantum search algorithm can be described as an alternating sequence of unitary transformations independent of x, U_i and calls to the oracle, S_x^π

$$|\psi_k^x\rangle = U_k S_x^\pi U_{k-1} S_x^\pi \dots U_1 S_x^\pi U_0 |0\rangle,$$

with the constraint that the probability of finding the solution in k steps is at least 50%

Optimality of Grover's algorithm

It is useful to prove that Grover's algorithm is the optimal search algorithm

Suppose there is a single solution, x, to the oracle transformation, U_P

Recall that the transformation S_x^π can be computed from the oracle, U_P, thus S_x^π can be used as the interface to the oracle with out loss of generality

An arbitrary quantum search algorithm can be described as an alternating sequence of unitary transformations independent of x, U_i and calls to the oracle, S_x^π

$$|\psi_k^x\rangle = U_k S_x^\pi U_{k-1} S_x^\pi \dots U_1 S_x^\pi U_0 |0\rangle, \qquad |\langle x|\psi_k^x\rangle|^2 \geq \tfrac{1}{2}$$

with the constraint that the probability of finding the solution in k steps is at least 50%

The proof of optimality lies in comparing three classes of quantum states:

Optimality of Grover's algorithm

It is useful to prove that Grover's algorithm is the optimal search algorithm

Suppose there is a single solution, x, to the oracle transformation, U_P

Recall that the transformation S_x^π can be computed from the oracle, U_P, thus S_x^π can be used as the interface to the oracle with out loss of generality

An arbitrary quantum search algorithm can be described as an alternating sequence of unitary transformations independent of x, U_i and calls to the oracle, S_x^π

$$|\psi_k^x\rangle = U_k S_x^\pi U_{k-1} S_x^\pi \dots U_1 S_x^\pi U_0 |0\rangle, \qquad |\langle x|\psi_k^x\rangle|^2 \geq \frac{1}{2}$$

with the constraint that the probability of finding the solution in k steps is at least 50%

The proof of optimality lies in comparing three classes of quantum states:

$|x_k'\rangle = e^{i\theta_k^x}|x\rangle$ – the phase adjusted solution with $e^{i\theta_k^x} = \langle x|\psi_k^x\rangle / |\langle x|\psi_k^x\rangle|$ and $\langle x_k'|\psi_k^x\rangle$ real

Optimality of Grover's algorithm

It is useful to prove that Grover's algorithm is the optimal search algorithm

Suppose there is a single solution, x, to the oracle transformation, U_P

Recall that the transformation S_x^π can be computed from the oracle, U_P, thus S_x^π can be used as the interface to the oracle with out loss of generality

An arbitrary quantum search algorithm can be described as an alternating sequence of unitary transformations independent of x, U_i and calls to the oracle, S_x^π

$$|\psi_k^x\rangle = U_k S_x^\pi U_{k-1} S_x^\pi \dots U_1 S_x^\pi U_0 |0\rangle, \qquad |\langle x|\psi_k^x\rangle|^2 \geq \tfrac{1}{2}$$

with the constraint that the probability of finding the solution in k steps is at least 50%

The proof of optimality lies in comparing three classes of quantum states:

$|x_k'\rangle = e^{i\theta_k^x}|x\rangle$ – the phase adjusted solution with $e^{i\theta_k^x} = \langle x|\psi_k^x\rangle / |\langle x|\psi_k^x\rangle|$ and $\langle x_k'|\psi_k^x\rangle$ real

$|\psi_k^x\rangle$ – the state of the computation after k steps

Optimality of Grover's algorithm

It is useful to prove that Grover's algorithm is the optimal search algorithm

Suppose there is a single solution, x, to the oracle transformation, U_P

Recall that the transformation S_x^π can be computed from the oracle, U_P, thus S_x^π can be used as the interface to the oracle with out loss of generality

An arbitrary quantum search algorithm can be described as an alternating sequence of unitary transformations independent of x, U_i and calls to the oracle, S_x^π

$$|\psi_k^x\rangle = U_k S_x^\pi U_{k-1} S_x^\pi \dots U_1 S_x^\pi U_0|0\rangle, \qquad |\langle x|\psi_k^x\rangle|^2 \geq \frac{1}{2}$$

with the constraint that the probability of finding the solution in k steps is at least 50%

The proof of optimality lies in comparing three classes of quantum states:

- $|x_k'\rangle = e^{i\theta_k^x}|x\rangle$ – the phase adjusted solution with $e^{i\theta_k^x} = \langle x|\psi_k^x\rangle / |\langle x|\psi_k^x\rangle|$ and $\langle x_k'|\psi_k^x\rangle$ real
- $|\psi_k^x\rangle$ – the state of the computation after k steps
- $|\psi_k\rangle = U_k U_{k-1} \dots U_1 U_0|0\rangle$ – k transformations without consulting the oracle

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|,$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|,$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \big| |\psi_k^x\rangle - |\psi_k\rangle \big|, \qquad a_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle \big|, \qquad c_{kx} = \big| |x_k'\rangle - |\psi_k\rangle \big|$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \big| |\psi_k^x\rangle - |\psi_k\rangle \big|, \quad a_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle \big|, \quad c_{kx} = \big| |x_k'\rangle - |\psi_k\rangle \big|$$

$$D_k = \frac{1}{N} \sum_x d_{kx}^2,$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \big| |\psi_k^x\rangle - |\psi_k\rangle \big|, \qquad a_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle \big|, \qquad c_{kx} = \big| |x_k'\rangle - |\psi_k\rangle \big|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2,$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2$$

By the definition of $|x_k'\rangle$ we have that $\langle \psi_k^x | x_k' \rangle \geq \frac{1}{\sqrt{2}}$ and

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N} \sum_x d_{kx}^2, \qquad A_k = \frac{1}{N} \sum_x a_{kx}^2, \qquad C_k = \frac{1}{N} \sum_x c_{kx}^2$$

By the definition of $|x_k'\rangle$ we have that $\langle \psi_k^x | x_k' \rangle \geq \frac{1}{\sqrt{2}}$ and

$$a_{kx}^2 = \left| |\psi_k^x\rangle - |x_k'\rangle \right|^2$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2$$

By the definition of $|x_k'\rangle$ we have that $\langle\psi_k^x|x_k'\rangle \geq \frac{1}{\sqrt{2}}$ and

$$a_{kx}^2 = \left| |\psi_k^x\rangle - |x_k'\rangle \right|^2 = \langle\psi_k^x|\psi_k^x\rangle - 2\langle x_k'|\psi_k^x\rangle + \langle x_k'|x_k'\rangle$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2$$

By the definition of $|x_k'\rangle$ we have that $\langle\psi_k^x|x_k'\rangle \geq \frac{1}{\sqrt{2}}$ and

$$a_{kx}^2 = \left| |\psi_k^x\rangle - |x_k'\rangle \right|^2 = \langle\psi_k^x|\psi_k^x\rangle - 2\langle x_k'|\psi_k^x\rangle + \langle x_k'|x_k'\rangle \leq 2 - \sqrt{2}$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N} \sum_x d_{kx}^2, \qquad A_k = \frac{1}{N} \sum_x a_{kx}^2, \qquad C_k = \frac{1}{N} \sum_x c_{kx}^2$$

By the definition of $|x_k'\rangle$ we have that $\langle \psi_k^x | x_k' \rangle \geq \frac{1}{\sqrt{2}}$ and

$$a_{kx}^2 = \left| |\psi_k^x\rangle - |x_k'\rangle \right|^2 = \langle \psi_k^x | \psi_k^x \rangle - 2\langle x_k' | \psi_k^x \rangle + \langle x_k' | x_k' \rangle \leq 2 - \sqrt{2} \quad \longrightarrow \quad A_k \leq 2 - \sqrt{2}$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \big| |\psi_k^x\rangle - |\psi_k\rangle \big|, \qquad a_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle \big|, \qquad c_{kx} = \big| |x_k'\rangle - |\psi_k\rangle \big|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2$$

By the definition of $|x_k'\rangle$ we have that $\langle\psi_k^x|x_k'\rangle \geq \frac{1}{\sqrt{2}}$ and

$$a_{kx}^2 = \big| |\psi_k^x\rangle - |x_k'\rangle \big|^2 = \langle\psi_k^x|\psi_k^x\rangle - 2\langle x_k'|\psi_k^x\rangle + \langle x_k'|x_k'\rangle \leq 2 - \sqrt{2} \quad \longrightarrow \quad A_k \leq 2 - \sqrt{2}$$

Similarly, we can put a bound on c_{kx}^2

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2$$

By the definition of $|x_k'\rangle$ we have that $\langle\psi_k^x|x_k'\rangle \geq \frac{1}{\sqrt{2}}$ and

$$a_{kx}^2 = \left| |\psi_k^x\rangle - |x_k'\rangle \right|^2 = \langle\psi_k^x|\psi_k^x\rangle - 2\langle x_k'|\psi_k^x\rangle + \langle x_k'|x_k'\rangle \leq 2 - \sqrt{2} \quad \longrightarrow \quad A_k \leq 2 - \sqrt{2}$$

Similarly, we can put a bound on c_{kx}^2

$$c_{kx}^2 = \left| |x_k'\rangle - |\psi_k\rangle \right|^2$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2$$

By the definition of $|x_k'\rangle$ we have that $\langle\psi_k^x|x_k'\rangle \geq \frac{1}{\sqrt{2}}$ and

$$a_{kx}^2 = \left| |\psi_k^x\rangle - |x_k'\rangle \right|^2 = \langle\psi_k^x|\psi_k^x\rangle - 2\langle x_k'|\psi_k^x\rangle + \langle x_k'|x_k'\rangle \leq 2 - \sqrt{2} \quad \longrightarrow \quad A_k \leq 2 - \sqrt{2}$$

Similarly, we can put a bound on c_{kx}^2

$$c_{kx}^2 = \left| |x_k'\rangle - |\psi_k\rangle \right|^2 = \left| e^{i\theta_k^x}|x\rangle - |\psi_k\rangle \right|^2$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2$$

By the definition of $|x_k'\rangle$ we have that $\langle\psi_k^x|x_k'\rangle \geq \frac{1}{\sqrt{2}}$ and

$$a_{kx}^2 = \left| |\psi_k^x\rangle - |x_k'\rangle \right|^2 = \langle\psi_k^x|\psi_k^x\rangle - 2\langle x_k'|\psi_k^x\rangle + \langle x_k'|x_k'\rangle \leq 2 - \sqrt{2} \quad \longrightarrow \quad A_k \leq 2 - \sqrt{2}$$

Similarly, we can put a bound on c_{kx}^2

$$c_{kx}^2 = \left| |x_k'\rangle - |\psi_k\rangle \right|^2 = \left| e^{i\theta_k^x}|x\rangle - |\psi_k\rangle \right|^2 = \langle\psi_k|\psi_k\rangle - \overline{e^{i\theta_k^x}\langle\psi_k|x\rangle} - e^{i\theta_k^x}\langle\psi_k|x\rangle + \langle x|x\rangle$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2$$

By the definition of $|x_k'\rangle$ we have that $\langle\psi_k^x|x_k'\rangle \geq \frac{1}{\sqrt{2}}$ and

$$a_{kx}^2 = \left| |\psi_k^x\rangle - |x_k'\rangle \right|^2 = \langle\psi_k^x|\psi_k^x\rangle - 2\langle x_k'|\psi_k^x\rangle + \langle x_k'|x_k'\rangle \leq 2 - \sqrt{2} \quad \longrightarrow \quad A_k \leq 2 - \sqrt{2}$$

Similarly, we can put a bound on c_{kx}^2

$$c_{kx}^2 = \left| |x_k'\rangle - |\psi_k\rangle \right|^2 = \left| e^{i\theta_k^x}|x\rangle - |\psi_k\rangle \right|^2 = \langle\psi_k|\psi_k\rangle - \overline{e^{i\theta_k^x}\langle\psi_k|x\rangle} - e^{i\theta_k^x}\langle\psi_k|x\rangle + \langle x|x\rangle$$
$$= 2 - 2Re\left\{ e^{i\theta_k^x}\langle\psi_k|x\rangle \right\}$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2$$

By the definition of $|x_k'\rangle$ we have that $\langle\psi_k^x|x_k'\rangle \geq \frac{1}{\sqrt{2}}$ and

$$a_{kx}^2 = \left| |\psi_k^x\rangle - |x_k'\rangle \right|^2 = \langle\psi_k^x|\psi_k^x\rangle - 2\langle x_k'|\psi_k^x\rangle + \langle x_k'|x_k'\rangle \leq 2 - \sqrt{2} \quad \longrightarrow \quad A_k \leq 2 - \sqrt{2}$$

Similarly, we can put a bound on c_{kx}^2

$$c_{kx}^2 = \left| |x_k'\rangle - |\psi_k\rangle \right|^2 = \left| e^{i\theta_k^x}|x\rangle - |\psi_k\rangle \right|^2 = \langle\psi_k|\psi_k\rangle - \overline{e^{i\theta_k^x}\langle\psi_k|x\rangle} - e^{i\theta_k^x}\langle\psi_k|x\rangle + \langle x|x\rangle$$
$$= 2 - 2Re\left\{e^{i\theta_k^x}\langle\psi_k|x\rangle\right\} \geq 2 - \left|\langle\psi_k|x\rangle\right|$$

Optimality of Grover's algorithm

Consider the distances between the three pairs of states and their averages

$$d_{kx} = \big| |\psi_k^x\rangle - |\psi_k\rangle \big|, \qquad a_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle \big|, \qquad c_{kx} = \big| |x_k'\rangle - |\psi_k\rangle \big|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2$$

By the definition of $|x_k'\rangle$ we have that $\langle\psi_k^x|x_k'\rangle \geq \frac{1}{\sqrt{2}}$ and

$$a_{kx}^2 = \big| |\psi_k^x\rangle - |x_k'\rangle \big|^2 = \langle\psi_k^x|\psi_k^x\rangle - 2\langle x_k'|\psi_k^x\rangle + \langle x_k'|x_k'\rangle \leq 2-\sqrt{2} \quad \longrightarrow \quad A_k \leq 2-\sqrt{2}$$

Similarly, we can put a bound on c_{kx}^2

$$c_{kx}^2 = \big| |x_k'\rangle - |\psi_k\rangle \big|^2 = \big| e^{i\theta_k^x}|x\rangle - |\psi_k\rangle \big|^2 = \langle\psi_k|\psi_k\rangle - \overline{e^{i\theta_k^x}\langle\psi_k|x\rangle} - e^{i\theta_k^x}\langle\psi_k|x\rangle + \langle x|x\rangle$$

$$= 2 - 2Re\big\{e^{i\theta_k^x}\langle\psi_k|x\rangle\big\} \geq 2 - \big|\langle\psi_k|x\rangle\big|$$

$$C_k = \frac{1}{N}\sum_x c_{kx}^2 \geq 2 - \frac{2}{N}\sum_x \big|\langle\psi_k|x\rangle\big|$$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right|$$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle \psi_k | x \rangle\right|$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right|$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2}$$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right|$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2} \quad \xrightarrow{v_k \equiv 1} \quad \sum_{i=0}^{N-1} u_i \leq \sqrt{N}\sqrt{\sum_{j=0}^{N-1} u_j^2}$$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right| \geq 2 - \frac{2}{\sqrt{N}}\sqrt{\sum_x \left|\langle\psi_k|x\rangle\right|^2}$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2} \quad \xrightarrow{v_k \equiv 1} \quad \sum_{i=0}^{N-1} u_i \leq \sqrt{N}\sqrt{\sum_{j=0}^{N-1} u_j^2}$$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right| \geq 2 - \frac{2}{\sqrt{N}}\sqrt{\sum_x \left|\langle\psi_k|x\rangle\right|^2} = 2 - \frac{2}{\sqrt{2}}$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2} \quad \xrightarrow{v_k \equiv 1} \quad \sum_{i=0}^{N-1} u_i \leq \sqrt{N}\sqrt{\sum_{j=0}^{N-1} u_j^2}$$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right| \geq 2 - \frac{2}{\sqrt{N}}\sqrt{\sum_x \left|\langle\psi_k|x\rangle\right|^2} = 2 - \frac{2}{\sqrt{2}}$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2} \quad \xrightarrow{v_k \equiv 1} \quad \sum_{i=0}^{N-1} u_i \leq \sqrt{N}\sqrt{\sum_{j=0}^{N-1} u_j^2}$$

Thus $C_k \geq 1$ for $N \geq 4$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right| \geq 2 - \frac{2}{\sqrt{N}}\sqrt{\sum_x \left|\langle\psi_k|x\rangle\right|^2} = 2 - \frac{2}{\sqrt{2}}$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2} \quad \xrightarrow{v_k \equiv 1} \quad \sum_{i=0}^{N-1} u_i \leq \sqrt{N}\sqrt{\sum_{j=0}^{N-1} u_j^2}$$

Thus $C_k \geq 1$ for $N \geq 4$

Turning to d_{kx}, first determine how much the distance between $|\psi_k^x\rangle$ and $|\psi_k\rangle$ can increase with each iteration, consider

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right| \geq 2 - \frac{2}{\sqrt{N}}\sqrt{\sum_x \left|\langle\psi_k|x\rangle\right|^2} = 2 - \frac{2}{\sqrt{2}}$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2} \quad \xrightarrow{v_k \equiv 1} \quad \sum_{i=0}^{N-1} u_i \leq \sqrt{N}\sqrt{\sum_{j=0}^{N-1} u_j^2}$$

Thus $C_k \geq 1$ for $N \geq 4$

Turning to d_{kx}, first determine how much the distance between $|\psi_k^x\rangle$ and $|\psi_k\rangle$ can increase with each iteration, consider

$$d_{k+1,x} = \left| |\psi_{k+1}^x\rangle - |\psi_{k+1}\rangle \right|$$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right| \geq 2 - \frac{2}{\sqrt{N}}\sqrt{\sum_x \left|\langle\psi_k|x\rangle\right|^2} = 2 - \frac{2}{\sqrt{2}}$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2} \quad \xrightarrow{v_k \equiv 1} \quad \sum_{i=0}^{N-1} u_i \leq \sqrt{N}\sqrt{\sum_{j=0}^{N-1} u_j^2}$$

Thus $C_k \geq 1$ for $N \geq 4$

Turning to d_{kx}, first determine how much the distance between $|\psi_k^x\rangle$ and $|\psi_k\rangle$ can increase with each iteration, consider

$$d_{k+1,x} = \left||\psi_{k+1}^x\rangle - |\psi_{k+1}\rangle\right| = \left|U_{k+1}S_x^\pi|\psi_k^x\rangle - U_{k+1}|\psi_k\rangle\right|$$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right| \geq 2 - \frac{2}{\sqrt{N}}\sqrt{\sum_x \left|\langle\psi_k|x\rangle\right|^2} = 2 - \frac{2}{\sqrt{2}}$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2} \quad \xrightarrow{v_k \equiv 1} \quad \sum_{i=0}^{N-1} u_i \leq \sqrt{N}\sqrt{\sum_{j=0}^{N-1} u_j^2}$$

Thus $C_k \geq 1$ for $N \geq 4$

Turning to d_{kx}, first determine how much the distance between $|\psi_k^x\rangle$ and $|\psi_k\rangle$ can increase with each iteration, consider

$$d_{k+1,x} = \left||\psi_{k+1}^x\rangle - |\psi_{k+1}\rangle\right| = \left|U_{k+1}S_x^\pi|\psi_k^x\rangle - U_{k+1}|\psi_k\rangle\right| = \left|S_x^\pi|\psi_k^x\rangle - |\psi_k\rangle\right|$$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right| \geq 2 - \frac{2}{\sqrt{N}}\sqrt{\sum_x \left|\langle\psi_k|x\rangle\right|^2} = 2 - \frac{2}{\sqrt{2}}$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2} \quad \xrightarrow{v_k \equiv 1} \quad \sum_{i=0}^{N-1} u_i \leq \sqrt{N}\sqrt{\sum_{j=0}^{N-1} u_j^2}$$

Thus $C_k \geq 1$ for $N \geq 4$

Turning to d_{kx}, first determine how much the distance between $|\psi_k^x\rangle$ and $|\psi_k\rangle$ can increase with each iteration, consider

$$\begin{aligned} d_{k+1,x} &= \left||\psi_{k+1}^x\rangle - |\psi_{k+1}\rangle\right| = \left|U_{k+1}S_x^\pi|\psi_k^x\rangle - U_{k+1}|\psi_k\rangle\right| = \left|S_x^\pi|\psi_k^x\rangle - |\psi_k\rangle\right| \\ &= \left|S_x^\pi(|\psi_k^x\rangle - |\psi_k\rangle) + (S_x^\pi - I)|\psi_k\rangle\right| \end{aligned}$$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right| \geq 2 - \frac{2}{\sqrt{N}}\sqrt{\sum_x \left|\langle\psi_k|x\rangle\right|^2} = 2 - \frac{2}{\sqrt{2}}$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2} \quad \xrightarrow{v_k \equiv 1} \quad \sum_{i=0}^{N-1} u_i \leq \sqrt{N}\sqrt{\sum_{j=0}^{N-1} u_j^2}$$

Thus $C_k \geq 1$ for $N \geq 4$

Turning to d_{kx}, first determine how much the distance between $|\psi_k^x\rangle$ and $|\psi_k\rangle$ can increase with each iteration, consider

$$\begin{aligned} d_{k+1,x} &= \left||\psi_{k+1}^x\rangle - |\psi_{k+1}\rangle\right| = \left|U_{k+1}S_x^\pi|\psi_k^x\rangle - U_{k+1}|\psi_k\rangle\right| = \left|S_x^\pi|\psi_k^x\rangle - |\psi_k\rangle\right| \\ &= \left|S_x^\pi(|\psi_k^x\rangle - |\psi_k\rangle) + (S_x^\pi - I)|\psi_k\rangle\right| \leq \left|S_x^\pi(|\psi_k^x\rangle - |\psi_k\rangle)\right| + \left|(S_x^\pi - I)|\psi_k\rangle\right| \end{aligned}$$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right| \geq 2 - \frac{2}{\sqrt{N}}\sqrt{\sum_x \left|\langle\psi_k|x\rangle\right|^2} = 2 - \frac{2}{\sqrt{2}}$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2} \quad \xrightarrow{v_k \equiv 1} \quad \sum_{i=0}^{N-1} u_i \leq \sqrt{N}\sqrt{\sum_{j=0}^{N-1} u_j^2}$$

Thus $C_k \geq 1$ for $N \geq 4$

Turning to d_{kx}, first determine how much the distance between $|\psi_k^x\rangle$ and $|\psi_k\rangle$ can increase with each iteration, consider

$$\begin{aligned} d_{k+1,x} &= \left||\psi_{k+1}^x\rangle - |\psi_{k+1}\rangle\right| = \left|U_{k+1}S_x^\pi|\psi_k^x\rangle - U_{k+1}|\psi_k\rangle\right| = \left|S_x^\pi|\psi_k^x\rangle - |\psi_k\rangle\right| \\ &= \left|S_x^\pi(|\psi_k^x\rangle - |\psi_k\rangle) + (S_x^\pi - I)|\psi_k\rangle\right| \leq \left|S_x^\pi(|\psi_k^x\rangle - |\psi_k\rangle)\right| + \left|(S_x^\pi - I)|\psi_k\rangle\right| \\ &= d_{kx} + 2\left|\langle x|\psi_k\rangle\right| \end{aligned}$$

Optimality of Grover's algorithm

$$C_k \geq 2 - \left|\langle\psi_k|x\rangle\right| \geq 2 - \frac{2}{\sqrt{N}}\sqrt{\sum_x \left|\langle\psi_k|x\rangle\right|^2} = 2 - \frac{2}{\sqrt{2}}$$

In order to evaluate this, we need to use the Cauchy-Schwartz inequality

$$\sum_i u_i v_i \leq \sqrt{\sum_j u_j^2 \sum_k v_k^2} \quad \xrightarrow{v_k \equiv 1} \quad \sum_{i=0}^{N-1} u_i \leq \sqrt{N}\sqrt{\sum_{j=0}^{N-1} u_j^2}$$

Thus $C_k \geq 1$ for $N \geq 4$

Turning to d_{kx}, first determine how much the distance between $|\psi_k^x\rangle$ and $|\psi_k\rangle$ can increase with each iteration, consider

$$\begin{aligned} d_{k+1,x} &= \left||\psi_{k+1}^x\rangle - |\psi_{k+1}\rangle\right| = \left|U_{k+1}S_x^\pi|\psi_k^x\rangle - U_{k+1}|\psi_k\rangle\right| = \left|S_x^\pi|\psi_k^x\rangle - |\psi_k\rangle\right| \\ &= \left|S_x^\pi(|\psi_k^x\rangle - |\psi_k\rangle) + (S_x^\pi - I)|\psi_k\rangle\right| \leq \left|S_x^\pi(|\psi_k^x\rangle - |\psi_k\rangle)\right| + \left|(S_x^\pi - I)|\psi_k\rangle\right| \\ &= d_{kx} + 2\left|\langle x|\psi_k\rangle\right| \end{aligned}$$

Thus $2|\langle x|\psi_k\rangle|$ bounds the change distance between $|\psi_k^x\rangle$ and $|\psi_k\rangle$ at each iteration

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N} \sum_{x=0}^{N-1} d_{kx}^2$$

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \leq \frac{4k^2}{N}$$

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \leq \frac{4k^2}{N}$$

For $k = 0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \leq \frac{4k^2}{N}$$

For $k = 0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

$$d_{0x} = \left| |\psi_0^x\rangle - |\psi_0\rangle \right| = 0$$

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \leq \frac{4k^2}{N}$$

For $k=0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

$$d_{0x} = \big||\psi_0^x\rangle - |\psi_0\rangle\big| = 0 \longrightarrow D_0 = 0$$

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \le \frac{4k^2}{N}$$

For $k=0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

$$d_{0x} = \left| |\psi_0^x\rangle - |\psi_0\rangle \right| = 0 \longrightarrow D_0 = 0$$

$$D_{k+1} = \frac{1}{N}\sum_{x=0}^{N-1} d_{k+1,x}^2$$

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \le \frac{4k^2}{N}$$

For $k=0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

$$d_{0x} = \big||\psi_0^x\rangle - |\psi_0\rangle\big| = 0 \;\longrightarrow\; D_0 = 0$$

$$D_{k+1} = \frac{1}{N}\sum_{x=0}^{N-1} d_{k+1,x}^2 \le \frac{1}{N}\sum_{x=0}^{N-1}\big(d_{kx} + 2\big|\langle x|\psi_k\rangle\big|\big)^2$$

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \le \frac{4k^2}{N}$$

For $k = 0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

$$d_{0x} = \left||\psi_0^x\rangle - |\psi_0\rangle\right| = 0 \longrightarrow D_0 = 0$$

$$D_{k+1} = \frac{1}{N}\sum_{x=0}^{N-1} d_{k+1,x}^2 \le \frac{1}{N}\sum_{x=0}^{N-1}\left(d_{kx} + 2\left|\langle x|\psi_k\rangle\right|\right)^2$$

$$= \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 + \frac{4}{N}\sum_{x=0}^{N-1}\left|\langle x|\psi_k\rangle\right|^2 + \frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right|$$

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \le \frac{4k^2}{N}$$

For $k=0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

$$d_{0x} = \big\| |\psi_0^x\rangle - |\psi_0\rangle \big\| = 0 \longrightarrow D_0 = 0$$

$$D_{k+1} = \frac{1}{N}\sum_{x=0}^{N-1} d_{k+1,x}^2 \le \frac{1}{N}\sum_{x=0}^{N-1}\left(d_{kx} + 2\big|\langle x|\psi_k\rangle\big|\right)^2$$

$$= \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 + \frac{4}{N}\sum_{x=0}^{N-1}\big|\langle x|\psi_k\rangle\big|^2 + \frac{4}{N}\sum_{x=0}^{N-1}\big|d_{kx}\langle x|\psi_k\rangle\big| = D_k + \frac{4}{N} + \frac{4}{N}\sum_{x=0}^{N-1}\big|d_{kx}\langle x|\psi_k\rangle\big|$$

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \le \frac{4k^2}{N}$$

For $k=0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

$$d_{0x} = \left| |\psi_0^x\rangle - |\psi_0\rangle \right| = 0 \;\longrightarrow\; D_0 = 0$$

$$D_{k+1} = \frac{1}{N}\sum_{x=0}^{N-1} d_{k+1,x}^2 \le \frac{1}{N}\sum_{x=0}^{N-1}\left(d_{kx} + 2\left|\langle x|\psi_k\rangle\right|\right)^2$$

$$= \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 + \frac{4}{N}\sum_{x=0}^{N-1}\left|\langle x|\psi_k\rangle\right|^2 + \frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right| = D_k + \frac{4}{N} + \frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right|$$

Applying the Cauchy-Schwartz inequality

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \leq \frac{4k^2}{N}$$

For $k=0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

$$d_{0x} = \big||\psi_0^x\rangle - |\psi_0\rangle\big| = 0 \longrightarrow D_0 = 0$$

$$D_{k+1} = \frac{1}{N}\sum_{x=0}^{N-1} d_{k+1,x}^2 \leq \frac{1}{N}\sum_{x=0}^{N-1}\left(d_{kx} + 2\big|\langle x|\psi_k\rangle\big|\right)^2$$

$$= \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 + \frac{4}{N}\sum_{x=0}^{N-1}\big|\langle x|\psi_k\rangle\big|^2 + \frac{4}{N}\sum_{x=0}^{N-1}\big|d_{kx}\langle x|\psi_k\rangle\big| = D_k + \frac{4}{N} + \frac{4}{N}\sum_{x=0}^{N-1}\big|d_{kx}\langle x|\psi_k\rangle\big|$$

Applying the Cauchy-Schwartz inequality

$$\frac{4}{N}\sum_{x=0}^{N-1}\big|d_{kx}\langle x|\psi_k\rangle\big| \leq \frac{4}{N}\sqrt{\sum_{y=0}^{N-1} d_{ky}^2 \sum_{z=0}^{N-1}\big|\langle z|\psi_k\rangle\big|^2}$$

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \le \frac{4k^2}{N}$$

For $k=0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

$$d_{0x} = \big||\psi_0^x\rangle - |\psi_0\rangle\big| = 0 \longrightarrow D_0 = 0$$

$$D_{k+1} = \frac{1}{N}\sum_{x=0}^{N-1} d_{k+1,x}^2 \le \frac{1}{N}\sum_{x=0}^{N-1}\left(d_{kx} + 2\left|\langle x|\psi_k\rangle\right|\right)^2$$

$$= \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 + \frac{4}{N}\sum_{x=0}^{N-1}\left|\langle x|\psi_k\rangle\right|^2 + \frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right| = D_k + \frac{4}{N} + \frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right|$$

Applying the Cauchy-Schwartz inequality

$$\frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right| \le \frac{4}{N}\sqrt{\sum_{y=0}^{N-1} d_{ky}^2 \sum_{z=0}^{N-1}\left|\langle z|\psi_k\rangle\right|^2} = \frac{4}{N}\sqrt{ND_k \cdot 1} = 4\sqrt{\frac{D_k}{N}}$$

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \leq \frac{4k^2}{N}$$

For $k=0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

$$d_{0x} = \left||\psi_0^x\rangle - |\psi_0\rangle\right| = 0 \;\longrightarrow\; D_0 = 0$$

$$D_{k+1} = \frac{1}{N}\sum_{x=0}^{N-1} d_{k+1,x}^2 \leq \frac{1}{N}\sum_{x=0}^{N-1}\left(d_{kx} + 2\left|\langle x|\psi_k\rangle\right|\right)^2$$

$$= \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 + \frac{4}{N}\sum_{x=0}^{N-1}\left|\langle x|\psi_k\rangle\right|^2 + \frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right| = D_k + \frac{4}{N} + \frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right|$$

Applying the Cauchy-Schwartz inequality

$$\frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right| \leq \frac{4}{N}\sqrt{\sum_{y=0}^{N-1} d_{ky}^2 \sum_{z=0}^{N-1}\left|\langle z|\psi_k\rangle\right|^2} = \frac{4}{N}\sqrt{ND_k\cdot 1} = 4\sqrt{\frac{D_k}{N}}$$

$$D_{k+1} \leq D_k + \frac{4}{N} + 4\sqrt{\frac{D_k}{N}}$$

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \le \frac{4k^2}{N}$$

For $k=0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

$$d_{0x} = \left\| |\psi_0^x\rangle - |\psi_0\rangle \right\| = 0 \longrightarrow D_0 = 0$$

$$D_{k+1} = \frac{1}{N}\sum_{x=0}^{N-1} d_{k+1,x}^2 \le \frac{1}{N}\sum_{x=0}^{N-1}\left(d_{kx} + 2\left|\langle x|\psi_k\rangle\right|\right)^2$$

$$= \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 + \frac{4}{N}\sum_{x=0}^{N-1}\left|\langle x|\psi_k\rangle\right|^2 + \frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right| = D_k + \frac{4}{N} + \frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right|$$

Applying the Cauchy-Schwartz inequality

$$\frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right| \le \frac{4}{N}\sqrt{\sum_{y=0}^{N-1} d_{ky}^2 \sum_{z=0}^{N-1}\left|\langle z|\psi_k\rangle\right|^2} = \frac{4}{N}\sqrt{ND_k\cdot 1} = 4\sqrt{\frac{D_k}{N}}$$

$$D_{k+1} \le D_k + \frac{4}{N} + 4\sqrt{\frac{D_k}{N}} \le \frac{4k^2}{N} + \frac{4}{N} + 4\sqrt{\frac{4k^2}{N^2}}$$

Optimality of Grover's algorithm

The constraint on D_k can now be obtained by induction with the assumption that

$$D_k = \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 \le \frac{4k^2}{N}$$

For $k=0$, $|\psi_0^x\rangle = U_0|0\rangle = |\psi_0\rangle$ so

$$d_{0x} = \left\| |\psi_0^x\rangle - |\psi_0\rangle \right\| = 0 \longrightarrow D_0 = 0$$

$$D_{k+1} = \frac{1}{N}\sum_{x=0}^{N-1} d_{k+1,x}^2 \le \frac{1}{N}\sum_{x=0}^{N-1}\left(d_{kx} + 2\left|\langle x|\psi_k\rangle\right|\right)^2$$

$$= \frac{1}{N}\sum_{x=0}^{N-1} d_{kx}^2 + \frac{4}{N}\sum_{x=0}^{N-1}\left|\langle x|\psi_k\rangle\right|^2 + \frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right| = D_k + \frac{4}{N} + \frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right|$$

Applying the Cauchy-Schwartz inequality

$$\frac{4}{N}\sum_{x=0}^{N-1}\left|d_{kx}\langle x|\psi_k\rangle\right| \le \frac{4}{N}\sqrt{\sum_{y=0}^{N-1} d_{ky}^2 \sum_{z=0}^{N-1}\left|\langle z|\psi_k\rangle\right|^2} = \frac{4}{N}\sqrt{ND_k \cdot 1} = 4\sqrt{\frac{D_k}{N}}$$

$$D_{k+1} \le D_k + \frac{4}{N} + 4\sqrt{\frac{D_k}{N}} \le \frac{4k^2}{N} + \frac{4}{N} + 4\sqrt{\frac{4k^2}{N^2}} = \frac{4}{N}(k^2+2k+1) = \frac{4(k+1)^2}{N}$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \Big| |\psi_k^x\rangle - |\psi_k\rangle \Big|, \qquad a_{kx} = \Big| |\psi_k^x\rangle - |x_k'\rangle \Big|, \qquad c_{kx} = \Big| |x_k'\rangle - |\psi_k\rangle \Big|$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \big| |\psi_k^x\rangle - |\psi_k\rangle \big|, \qquad a_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle \big|, \qquad c_{kx} = \big| |x_k'\rangle - |\psi_k\rangle \big|$$

$$D_k = \frac{1}{N} \sum_x d_{kx}^2 \le \frac{4k^2}{N},$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2 \le \frac{4k^2}{N}, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2 \le 2 - \sqrt{2},$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2 \le \frac{4k^2}{N}, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2 \le 2 - \sqrt{2}, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2 \ge 1$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \big| |\psi_k^x\rangle - |\psi_k\rangle \big|, \qquad a_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle \big|, \qquad c_{kx} = \big| |x_k'\rangle - |\psi_k\rangle \big|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2 \le \frac{4k^2}{N}, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2 \le 2 - \sqrt{2}, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2 \ge 1$$

The three distances are related as

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \big||\psi_k^x\rangle - |\psi_k\rangle\big|, \qquad a_{kx} = \big||\psi_k^x\rangle - |x_k'\rangle\big|, \qquad c_{kx} = \big||x_k'\rangle - |\psi_k\rangle\big|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2 \leq \frac{4k^2}{N}, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2 \leq 2 - \sqrt{2}, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2 \geq 1$$

The three distances are related as

$$d_{kx} = \big||\psi_k^x\rangle - |x_k'\rangle + |x_k'\rangle - |\psi_k\rangle\big|$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \Big| |\psi_k^x\rangle - |\psi_k\rangle \Big|, \qquad a_{kx} = \Big| |\psi_k^x\rangle - |x_k'\rangle \Big|, \qquad c_{kx} = \Big| |x_k'\rangle - |\psi_k\rangle \Big|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2 \le \frac{4k^2}{N}, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2 \le 2-\sqrt{2}, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2 \ge 1$$

The three distances are related as

$$d_{kx} = \Big| |\psi_k^x\rangle - |x_k'\rangle + |x_k'\rangle - |\psi_k\rangle \Big| = \Big| a_{kx} + c_{kx} \Big|$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \big| |\psi_k^x\rangle - |\psi_k\rangle \big|, \qquad a_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle \big|, \qquad c_{kx} = \big| |x_k'\rangle - |\psi_k\rangle \big|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2 \le \frac{4k^2}{N}, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2 \le 2 - \sqrt{2}, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2 \ge 1$$

The three distances are related as

$$d_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle + |x_k'\rangle - |\psi_k\rangle \big| = \big| a_{kx} + c_{kx} \big| \ge a_{kx} - c_{kx}$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2 \le \frac{4k^2}{N}, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2 \le 2-\sqrt{2}, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2 \ge 1$$

The three distances are related as

$$d_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle + |x_k'\rangle - |\psi_k\rangle \right| = \left| a_{kx} + c_{kx} \right| \ge a_{kx} - c_{kx}$$

$$D_k \ge \frac{1}{N}\left(\sum_{x=0}^{N-1} a_{kx}^2 - 2\sum_{x=0}^{N-1} a_{kx}c_{kx} + \sum_{x=0}^{N-1} c_{kx}^2 \right)$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2 \le \frac{4k^2}{N}, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2 \le 2 - \sqrt{2}, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2 \ge 1$$

The three distances are related as

$$d_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle + |x_k'\rangle - |\psi_k\rangle \right| = \left| a_{kx} + c_{kx} \right| \ge a_{kx} - c_{kx}$$

$$D_k \ge \frac{1}{N}\left(\sum_{x=0}^{N-1} a_{kx}^2 - 2\sum_{x=0}^{N-1} a_{kx}c_{kx} + \sum_{x=0}^{N-1} c_{kx}^2 \right)$$

$$\ge \frac{1}{N}\sum_{x=0}^{N-1} a_{kx}^2 - \frac{2}{N}\sqrt{\sum_{y=0}^{N-1} a_{ky}^2 \sum_{z=0}^{N-1} c_{kz}^2} + \frac{1}{N}\sum_{x=0}^{N-1} c_{kx}^2$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \big| |\psi_k^x\rangle - |\psi_k\rangle \big|, \qquad a_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle \big|, \qquad c_{kx} = \big| |x_k'\rangle - |\psi_k\rangle \big|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2 \le \frac{4k^2}{N}, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2 \le 2-\sqrt{2}, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2 \ge 1$$

The three distances are related as

$$d_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle + |x_k'\rangle - |\psi_k\rangle \big| = \big| a_{kx} + c_{kx} \big| \ge a_{kx} - c_{kx}$$

$$D_k \ge \frac{1}{N}\left(\sum_{x=0}^{N-1} a_{kx}^2 - 2\sum_{x=0}^{N-1} a_{kx}c_{kx} + \sum_{x=0}^{N-1} c_{kx}^2 \right)$$

$$\ge \frac{1}{N}\sum_{x=0}^{N-1} a_{kx}^2 - \frac{2}{N}\sqrt{\sum_{y=0}^{N-1} a_{ky}^2 \sum_{z=0}^{N-1} c_{kz}^2} + \frac{1}{N}\sum_{x=0}^{N-1} c_{kx}^2 \ge A_k - 2\sqrt{A_k C_k} + C_k$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \big| |\psi_k^x\rangle - |\psi_k\rangle \big|, \qquad a_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle \big|, \qquad c_{kx} = \big| |x_k'\rangle - |\psi_k\rangle \big|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2 \le \frac{4k^2}{N}, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2 \le 2-\sqrt{2}, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2 \ge 1$$

The three distances are related as

$$d_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle + |x_k'\rangle - |\psi_k\rangle \big| = \big| a_{kx} + c_{kx} \big| \ge a_{kx} - c_{kx}$$

$$D_k \ge \frac{1}{N}\left(\sum_{x=0}^{N-1} a_{kx}^2 - 2\sum_{x=0}^{N-1} a_{kx}c_{kx} + \sum_{x=0}^{N-1} c_{kx}^2\right)$$

$$\ge \frac{1}{N}\sum_{x=0}^{N-1} a_{kx}^2 - \frac{2}{N}\sqrt{\sum_{y=0}^{N-1} a_{ky}^2 \sum_{z=0}^{N-1} c_{kz}^2} + \frac{1}{N}\sum_{x=0}^{N-1} c_{kx}^2 \ge A_k - 2\sqrt{A_k C_k} + C_k$$

$$\frac{4k^2}{N} \ge D_k \ge A_k - \sqrt{A_k C_k} + C_k$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \big| |\psi_k^x\rangle - |\psi_k\rangle \big|, \qquad a_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle \big|, \qquad c_{kx} = \big| |x_k'\rangle - |\psi_k\rangle \big|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2 \le \frac{4k^2}{N}, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2 \le 2-\sqrt{2}, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2 \ge 1$$

The three distances are related as

$$d_{kx} = \big| |\psi_k^x\rangle - |x_k'\rangle + |x_k'\rangle - |\psi_k\rangle \big| = \big| a_{kx} + c_{kx} \big| \ge a_{kx} - c_{kx}$$

$$D_k \ge \frac{1}{N}\left(\sum_{x=0}^{N-1} a_{kx}^2 - 2\sum_{x=0}^{N-1} a_{kx}c_{kx} + \sum_{x=0}^{N-1} c_{kx}^2 \right)$$

$$\ge \frac{1}{N}\sum_{x=0}^{N-1} a_{kx}^2 - \frac{2}{N}\sqrt{\sum_{y=0}^{N-1} a_{ky}^2 \sum_{z=0}^{N-1} c_{kz}^2} + \frac{1}{N}\sum_{x=0}^{N-1} c_{kx}^2 \ge A_k - 2\sqrt{A_k C_k} + C_k$$

$$\frac{4k^2}{N} \ge D_k \ge A_k - \sqrt{A_k C_k} + C_k = \left(\sqrt{C_k} - \sqrt{A_k}\right)^2$$

Optimality of Grover's algorithm

We have established the following bounds on the distances of interest

$$d_{kx} = \left| |\psi_k^x\rangle - |\psi_k\rangle \right|, \qquad a_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle \right|, \qquad c_{kx} = \left| |x_k'\rangle - |\psi_k\rangle \right|$$

$$D_k = \frac{1}{N}\sum_x d_{kx}^2 \le \frac{4k^2}{N}, \qquad A_k = \frac{1}{N}\sum_x a_{kx}^2 \le 2-\sqrt{2}, \qquad C_k = \frac{1}{N}\sum_x c_{kx}^2 \ge 1$$

The three distances are related as

$$d_{kx} = \left| |\psi_k^x\rangle - |x_k'\rangle + |x_k'\rangle - |\psi_k\rangle \right| = \left| a_{kx} + c_{kx} \right| \ge a_{kx} - c_{kx}$$

$$D_k \ge \frac{1}{N}\left(\sum_{x=0}^{N-1} a_{kx}^2 - 2\sum_{x=0}^{N-1} a_{kx}c_{kx} + \sum_{x=0}^{N-1} c_{kx}^2 \right)$$

$$\ge \frac{1}{N}\sum_{x=0}^{N-1} a_{kx}^2 - \frac{2}{N}\sqrt{\sum_{y=0}^{N-1} a_{ky}^2 \sum_{z=0}^{N-1} c_{kz}^2} + \frac{1}{N}\sum_{x=0}^{N-1} c_{kx}^2 \ge A_k - 2\sqrt{A_k C_k} + C_k$$

$$\frac{4k^2}{N} \ge D_k \ge A_k - \sqrt{A_k C_k} + C_k = \left(\sqrt{C_k} - \sqrt{A_k}\right)^2 \ge \left(1 - \sqrt{2-\sqrt{2}}\right)^2$$

Optimality of Grover's algorithm

Recalling that D_k is bounded, we can write

Optimality of Grover's algorithm

Recalling that D_k is bounded, we can write

$$\frac{4k^2}{N} \geq D_k \geq A_k - \sqrt{A_k C_k} + C_k$$

Optimality of Grover's algorithm

Recalling that D_k is bounded, we can write

$$\frac{4k^2}{N} \geq D_k \geq A_k - \sqrt{A_k C_k} + C_k = \left(\sqrt{C_k} - \sqrt{A_k}\right)^2$$

Optimality of Grover's algorithm

Recalling that D_k is bounded, we can write

$$\frac{4k^2}{N} \geq D_k \geq A_k - \sqrt{A_k C_k} + C_k = \left(\sqrt{C_k} - \sqrt{A_k}\right)^2 \geq \left(1 - \sqrt{2 - \sqrt{2}}\right)^2$$

Optimality of Grover's algorithm

Recalling that D_k is bounded, we can write

$$\frac{4k^2}{N} \geq D_k \geq A_k - \sqrt{A_k C_k} + C_k = \left(\sqrt{C_k} - \sqrt{A_k}\right)^2 \geq \left(1 - \sqrt{2 - \sqrt{2}}\right)^2$$

Recalling that $C_k \geq 1$ only for $N \geq 4$ and $1 \geq 2 - \sqrt{2} \geq A_k$, if $q = 1 - \sqrt{2 - \sqrt{2}}$

Optimality of Grover's algorithm

Recalling that D_k is bounded, we can write

$$\frac{4k^2}{N} \geq D_k \geq A_k - \sqrt{A_k C_k} + C_k = \left(\sqrt{C_k} - \sqrt{A_k}\right)^2 \geq \left(1 - \sqrt{2 - \sqrt{2}}\right)^2$$

Recalling that $C_k \geq 1$ only for $N \geq 4$ and $1 \geq 2 - \sqrt{2} \geq A_k$, if $q = 1 - \sqrt{2 - \sqrt{2}}$

$$\frac{4k^2}{N} \geq q^2$$

Optimality of Grover's algorithm

Recalling that D_k is bounded, we can write

$$\frac{4k^2}{N} \geq D_k \geq A_k - \sqrt{A_k C_k} + C_k = \left(\sqrt{C_k} - \sqrt{A_k}\right)^2 \geq \left(1 - \sqrt{2 - \sqrt{2}}\right)^2$$

Recalling that $C_k \geq 1$ only for $N \geq 4$ and $1 \geq 2 - \sqrt{2} \geq A_k$, if $q = 1 - \sqrt{2 - \sqrt{2}}$

$$\frac{4k^2}{N} \geq q^2 \quad \longrightarrow \quad k \geq \frac{q}{2}\sqrt{N}$$

Optimality of Grover's algorithm

Recalling that D_k is bounded, we can write

$$\frac{4k^2}{N} \geq D_k \geq A_k - \sqrt{A_k C_k} + C_k = \left(\sqrt{C_k} - \sqrt{A_k}\right)^2 \geq \left(1 - \sqrt{2 - \sqrt{2}}\right)^2$$

Recalling that $C_k \geq 1$ only for $N \geq 4$ and $1 \geq 2 - \sqrt{2} \geq A_k$, if $q = 1 - \sqrt{2 - \sqrt{2}}$

$$\frac{4k^2}{N} \geq q^2 \quad \longrightarrow \quad k \geq \frac{q}{2}\sqrt{N}$$

Thus $O(\sqrt{N})$ queries of the oracle are needed to obtain an answer with a probability of success of $|\langle x|\psi_k^x\rangle|^2 \geq \frac{1}{2}$

Optimality of Grover's algorithm

Recalling that D_k is bounded, we can write

$$\frac{4k^2}{N} \geq D_k \geq A_k - \sqrt{A_k C_k} + C_k = \left(\sqrt{C_k} - \sqrt{A_k}\right)^2 \geq \left(1 - \sqrt{2 - \sqrt{2}}\right)^2$$

Recalling that $C_k \geq 1$ only for $N \geq 4$ and $1 \geq 2 - \sqrt{2} \geq A_k$, if $q = 1 - \sqrt{2 - \sqrt{2}}$

$$\frac{4k^2}{N} \geq q^2 \quad \longrightarrow \quad k \geq \frac{q}{2}\sqrt{N}$$

Thus $O(\sqrt{N})$ queries of the oracle are needed to obtain an answer with a probability of success of $|\langle x|\psi_k^x\rangle|^2 \geq \frac{1}{2}$

Since no quantum search algorithm can use fewer than $Q(\sqrt{N})$ queries then Grover's algorithm must be optimal