Title: Hamiltonian Oracles

Date: Apr 19, 2006 04:00 PM

URL: http://pirsa.org/06040019

Abstract: Hamiltonian oracles are the continuum limit of the standard unitary quantum oracles. In addition to being a potentially useful tool in the study of standard oracles, Hamiltonian oracles naturally introduce the concept of fractional queries and are amenable to study using techniques of differential equations and geometry. As an example of these ideas we shall examine the Hamiltonian oracle corresponding to the problem of oracle interrogation. This talk is intended for all those who wish to apply their knowledge of differential geometry without the risk of creating an event horizon.

Hamiltonian Oracles

(based on quant-ph/0602032)

Carlos Mochon

Perimeter Institute for Theoretical Physics

Hamiltonians are not sandwiches

- From Dave Bacon's blog (Dec 2005):

  Physicists are the ones who think that NP stands for "not polynomial" and computer scientists are the ones who think that a Hamiltonian is some sort of sandwich.

Hamiltonian oracles

Evolve according to the Schödinger equation:

$$\frac{d}{dt}|\psi(t)\rangle = -i\left(H_x + H'(t)\right)|\psi(t)\rangle$$

- H_x is the Hamiltonian oracle.
  Depends on hidden parameter x.
- $H'(t)$ is the control Hamiltonian.
  Can be time dependent and arbitrarily strong but cannot depend on x. Also $|\psi(0)\rangle$ is independent of x.
- Goal: find x (or some property of x).
- Example: $H_x = |x\rangle\langle x|$ for $x = 0, \ldots, N-1$.

Hamiltonian Oracles $\neq$ Physics

- Hidden parameters $x \in \{0,1\}^n$.
- H_x couples $O(\log n)$ particles.
- H_x generally has eigenvalues 0 and $\pm\pi$.
- $H'(t)$ can be arbitrarily complicated.
- Only resource we care about: query time.

Other variants of the problem include Hamiltonian Identification, Parameter Estimation, etc.

Relation to unitary oracles

Unitary oracles lead to an evolution

$$|\psi_x(t+1)\rangle = O_x U(t)|\psi_x(t)\rangle.$$

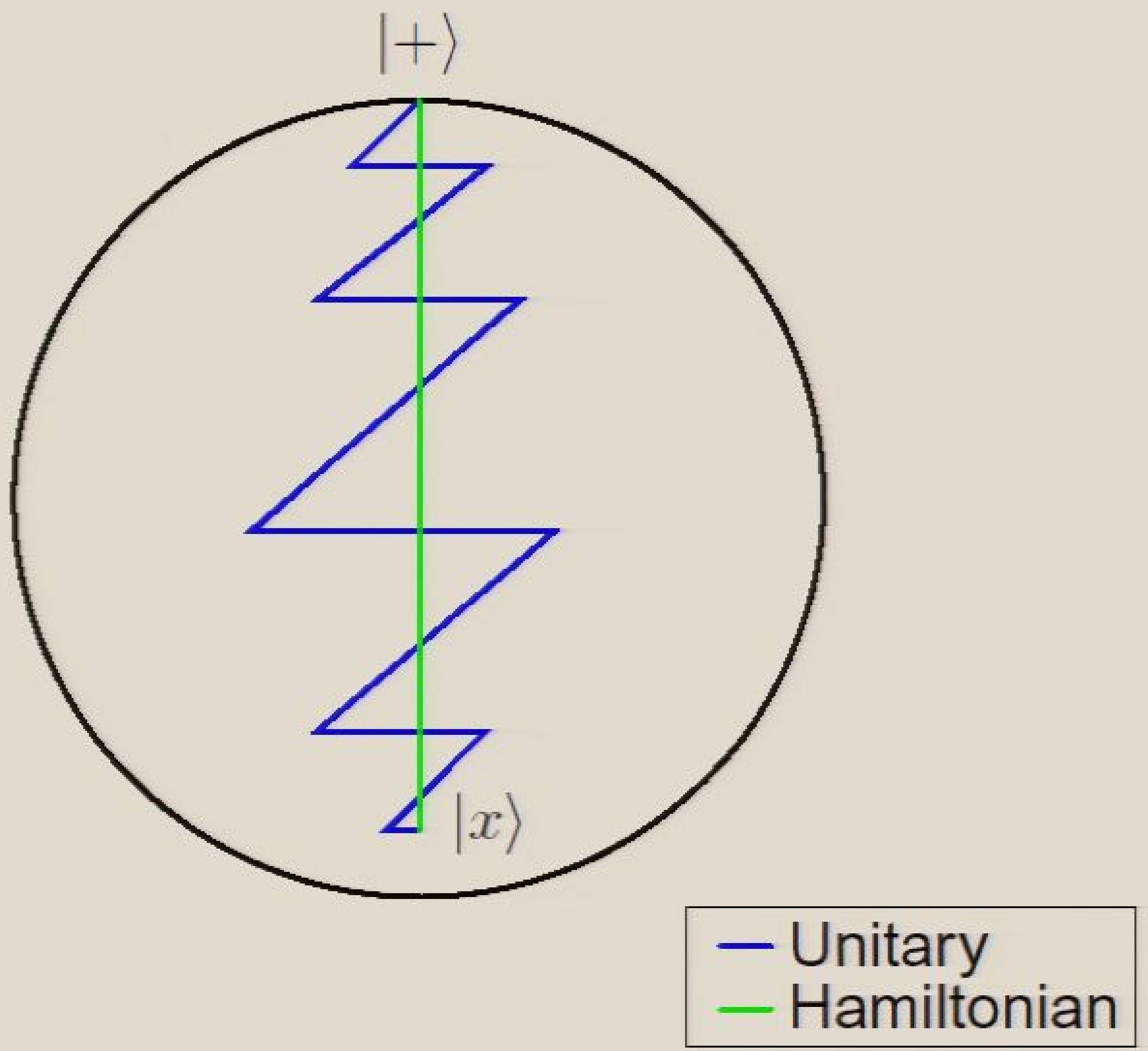
- O_x is the unitary oracle.
- $U(t)$ is the control unitaries.

We shall be interested in Hamiltonian oracles that satisfy

$$O_x = e^{-iH_x}$$

$\Longrightarrow$ The Hamiltonian oracle query time is a lower bound on the query complexity of the unitary oracle.

Grover on the Bloch Sphere



Motivation

Use Hamiltonian oracles to lower-bound unitary oracles.

- Pros
  - Smooth curves.
  - Simpler to achieve zero error.
  - Differential equations are easier than difference equations.
  - Connections to differential geometry.
  - New tools: fractional queries, different speed queries.
- Cons
  - Infinite number of variables to optimize over.
  - Geometry is hard.

Prior Work

- *Analog analogue of a digital quantum computation*, Farhi and Gutmann (quant-ph/9612026).
- Papers on continuous Grover search: Fenner, Roland, Cerf, et al.
- Continuous walk and spatial search: Farhi, Gutmann, Childs, Goldstone, et al.
- Papers on identifying Hamiltonians: A–Z.
- Geometry and quantum computing: Nielsen, Khaneja, Brockett, Glaser, et al.

Results 1 (Grover search)

- Farhi and Gutmann Grover protocol (using $E = \pi$):

$$T = \frac{\sqrt{N}}{2}.$$

- Improved protocol for one-item Grover search:

$$\begin{aligned} T &= \frac{N}{\pi\sqrt{N-1}} \arccos \frac{1}{\sqrt{N}} \\ &\simeq \frac{\sqrt{N}}{2} - \frac{1}{\pi} + O\left(\frac{1}{\sqrt{N}}\right). \end{aligned}$$

Assuming the marked state is a computational basis state.

Oracle Interrogation

- Hidden string: $x \in \{0,1\}^n$. Goal: find x.
- Unitary Oracle: $j \in \{1,\ldots,n\}$

$$O_x|j\rangle = (-1)^{x_j}|j\rangle.$$

- Hamiltonian Oracle: $j \in \{1,\ldots,n\}$ and $k \in \{0,1\}$

$$H_x|j,k\rangle = \pi(-1)^k x_j|j,k\rangle.$$

Note that $e^{-iH_x} = O_x \otimes I$.

Results 2 (Oracle Interrogation)

- Discrete case (van Dam): $T = \frac{n}{2} + \Theta(\sqrt{n})$.
  - For zero error needs $T = n$.
- Continuous case: $T \geq \frac{n}{\pi e} + \Omega(1) \simeq 0.117n$.
  - Speedup possible for zero error.
  - For $n = 2$, the minimum query time can be computed from the metric

$$ds^2 = \frac{4}{\pi^2}\left(d\theta^2 + \tan^2\theta d\phi^2\right),$$

as the distance between $(\pi/2, 0)$ and $(\pi/4, \pi/4)$.

Oracle Interrogation

- Hidden string: $x \in \{0,1\}^n$. Goal: find x.
- Unitary Oracle: $j \in \{1,\ldots,n\}$

$$O_x|j\rangle = (-1)^{x_j}|j\rangle.$$

- Hamiltonian Oracle: $j \in \{1,\ldots,n\}$ and $k \in \{0,1\}$

$$H_x|j,k\rangle = \pi(-1)^k x_j|j,k\rangle.$$

Note that $e^{-iH_x} = O_x \otimes I$.

Results 1 (Grover search)

- Farhi and Gutmann Grover protocol (using $E = \pi$):

$$T = \frac{\sqrt{N}}{2}.$$

- Improved protocol for one-item Grover search:

$$\begin{aligned} T &= \frac{N}{\pi\sqrt{N-1}} \arccos \frac{1}{\sqrt{N}} \\ &\simeq \frac{\sqrt{N}}{2} - \frac{1}{\pi} + O(\frac{1}{\sqrt{N}}). \end{aligned}$$

Assuming the marked state is a computational basis state.

Oracle Interrogation

- Hidden string: $x \in \{0,1\}^n$. Goal: find x.
- Unitary Oracle: $j \in \{1,\ldots,n\}$

$$O_x|j\rangle = (-1)^{x_j}|j\rangle.$$

- Hamiltonian Oracle: $j \in \{1,\ldots,n\}$ and $k \in \{0,1\}$

$$H_x|j,k\rangle = \pi(-1)^k x_j|j,k\rangle.$$

Note that $e^{-iH_x} = O_x \otimes I$.

Oracle Interrogation

- Hidden string: $x \in \{0,1\}^n$. Goal: find x.
- Unitary Oracle: $j \in \{1,\ldots,n\}$

$$O_x|j\rangle = (-1)^{x_j}|j\rangle.$$

- Hamiltonian Oracle: $j \in \{1,\ldots,n\}$ and $k \in \{0,1\}$

$$H_x|j,k\rangle = \pi(-1)^k x_j|j,k\rangle.$$

Note that $e^{-iH_x} = O_x \otimes I$.

Results 2 (Oracle Interrogation)

- Discrete case (van Dam): $T = \frac{n}{2} + \Theta(\sqrt{n})$.
  - For zero error needs $T = n$.
- Continuous case: $T \geq \frac{n}{\pi e} + \Omega(1) \simeq 0.117n$.
  - Speedup possible for zero error.
  - For $n = 2$, the minimum query time can be computed from the metric

$$ds^2 = \frac{4}{\pi^2}\left(d\theta^2 + \tan^2\theta d\phi^2\right),$$

as the distance between $(\pi/2, 0)$ and $(\pi/4, \pi/4)$.

...and now for the actual talk

The Gram matrix

For x and y taking values among the hidden strings, let

$$G_{x,y}(t) = \langle \psi_x(t) | \psi_y(t) \rangle.$$

- Smooth evolution.
  (Even if $|\psi_x(t)\rangle$ behaves wildly.)
- Describes current knowledge of hidden string.
  Complete knowledge of x implies $G = I$.
- Object of study in adversary methods.

Evolution of the Gram matrix

The Gram matrix can evolve according to the rule

$$\frac{dG(t)}{dt} = -i \, \mathrm{Tr}_{\mathcal{M}}[\tilde{H}\tilde{G}(t) - \tilde{G}(t)\tilde{H}]$$

for any positive operator $\tilde{G}$ on $\mathcal{A} \otimes \mathcal{M}$ satisfying

$$\mathrm{Tr}_{\mathcal{M}}[\tilde{G}(t)] = G(t),$$

where $\mathcal{A}$ is the space of hidden strings, $\mathcal{M}$ is the space of queries and

$$\tilde{H} = \sum_x |x\rangle\langle x|_{\mathcal{A}} \otimes (H_x)_{\mathcal{M}} \, .$$

Alice and Bob in Oracleland

- Alice is the oracle.
  Knows hidden string $x \in \{0,1\}^n$.
- Bob is the Hero seeking Knowledge.
  Can ask questions $i \in \{1,\ldots,n\}$.
- One query is the following two messages
  - Bob sends $|i\rangle_{\mathcal{M}}$ to Alice.
  - Alice applies the oracle unitary

$$|x\rangle_{\mathcal{A}} \otimes |i\rangle_{\mathcal{M}} \longrightarrow (-1)^{x_i}|x\rangle_{\mathcal{A}} \otimes |i\rangle_{\mathcal{M}}$$

  - Alice returns register $\mathcal{M}$ to Bob.

Translation to SDP

- Alice starts with $\rho(t)$.
- Bob sends query in $\mathcal{M}$.
- Alice now has $\tilde{\rho}(t)$ on $\mathcal{A} \otimes \mathcal{M}$, which satisfies

$$\mathrm{Tr}_{\mathcal{M}}[\tilde{\rho}(t)] = \rho(t).$$

- Alice applies $\tilde{O}$ and returns $\mathcal{M}$. Time is now $t+1$.

$$\rho(t+1) = \mathrm{Tr}_{\mathcal{M}}[\tilde{O}\tilde{\rho}\tilde{O}^{-1}]$$

where $\tilde{O} = \sum_x |x\rangle\langle x|_{\mathcal{A}} \otimes (O_x)_{\mathcal{M}}$.

Evolution of the Gram matrix

The Gram matrix can evolve according to the rule

$$\frac{dG(t)}{dt} = -i\,\mathrm{Tr}_{\mathcal{M}}[\tilde{H}\tilde{G}(t) - \tilde{G}(t)\tilde{H}]$$

for any positive operator $\tilde{G}$ on $\mathcal{A} \otimes \mathcal{M}$ satisfying

$$\mathrm{Tr}_{\mathcal{M}}[\tilde{G}(t)] = G(t),$$

where $\mathcal{A}$ is the space of hidden strings, $\mathcal{M}$ is the space of queries and

$$\tilde{H} = \sum_x |x\rangle\langle x|_{\mathcal{A}} \otimes (H_x)_{\mathcal{M}}\,.$$

Translation to SDP

- Alice starts with $\rho(t)$.
- Bob sends query in $\mathcal{M}$.
- Alice now has $\tilde{\rho}(t)$ on $\mathcal{A} \otimes \mathcal{M}$, which satisfies

$$\mathrm{Tr}_{\mathcal{M}}[\tilde{\rho}(t)] = \rho(t).$$

- Alice applies $\tilde{O}$ and returns $\mathcal{M}$. Time is now $t+1$.

$$\rho(t+1) = \mathrm{Tr}_{\mathcal{M}}[\tilde{O}\tilde{\rho}\tilde{O}^{-1}]$$

where $\tilde{O} = \sum_x |x\rangle\langle x|_{\mathcal{A}} \otimes (O_x)_{\mathcal{M}}$.

Fractional queries

Let $\tilde{O} = e^{-i\tilde{H}}$, then

- One standard query ($\Delta = 1$):

$$\rho(t+1) = \mathrm{Tr}_{\mathcal{M}}[\tilde{O}\tilde{\rho}(t)\tilde{O}^{-1}].$$

- Fraction Δ of a query:

$$\rho(t+\Delta) = \mathrm{Tr}_{\mathcal{M}}[e^{-i\Delta\tilde{H}}\tilde{\rho}(t)e^{i\Delta\tilde{H}}].$$

- Hamiltonian oracle ($\Delta \to 0$)

$$\frac{d\rho(t)}{dt} = -i\,\mathrm{Tr}_{\mathcal{M}}[\tilde{H}\tilde{\rho}(t) - \tilde{\rho}(t)\tilde{H}].$$

Returning to Oracle Interrogation...

Welcome to
Guantanamo Bay, Cuba

Symmetries of $n = 2$ case

Oracle interrogation for $n = 2$ has the following symmetries:

- Flipping bit #1.
- Flipping bit #2.
- Exchanging bit #1 and bit #2.

A symmetric Gram matrix for the problem has the form

$$G_{x,y} = f(|x \oplus y|)$$

for $x, y \in \{00, 01, 10, 11\}$.

Symmetric Gram matrix

Let $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. In the $|\pm\rangle$ basis the most general symmetric Gram matrix has the form

$$G = \begin{pmatrix} 4a_0^2 & 0 & 0 & 0 \\ 0 & 2a_1^2 & 0 & 0 \\ 0 & 0 & 2a_1^2 & 0 \\ 0 & 0 & 0 & 4a_2^2 \end{pmatrix}.$$

- Normalization: $\mathrm{Tr}\, G = 4 \longrightarrow a_0^2 + a_1^2 + a_2^2 = 1$.
- Initial condition: $a_0 = 1$, $a_1 = a_2 = 0$.
- Final condition: $a_0 = a_2 = 1/2$, $a_1 = 1/\sqrt{2}$.

Dynamics

All possible evolutions are given by

$$\frac{d}{dt}\begin{pmatrix} a_0(t) \\ a_1(t) \\ a_2(t) \end{pmatrix} = \frac{\pi}{2}\begin{pmatrix} 0 & -w_1(t) & 0 \\ w_1(t) & 0 & -w_2(t) \\ 0 & w_2(t) & 0 \end{pmatrix}\begin{pmatrix} a_0(t) \\ a_1(t) \\ a_2(t) \end{pmatrix}$$

where $w_1(t)$ and $w_2(t)$ can be chosen arbitrarily subject to the constraint $w_1^2 + w_2^2 \leq 1$.

New type of Hamiltonian problem:

- No hidden parameters.
- Restricted set of Hamiltonians.

Polar coordinates

Define θ and ϕ by

$$a_0 = \sin\theta\cos\phi, \qquad a_1 = \cos\theta, \qquad a_2 = \sin\theta\sin\phi.$$

The set of allowed velocity vectors is

$$\frac{\pi}{2}\begin{pmatrix} 0 & -w_1 & 0 \\ w_1 & 0 & -w_2 \\ 0 & w_2 & 0 \end{pmatrix}\begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = \frac{\pi}{2}\left(w_\theta e_\theta + \frac{w_\phi}{\tan\theta}e_\phi\right),$$

where e_θ, e_ϕ are the coordinate basis vectors and

$$\begin{pmatrix} w_\theta \\ w_\phi \end{pmatrix} = \begin{pmatrix} -\cos\phi & \sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}\begin{pmatrix} w_1 \\ w_2 \end{pmatrix}.$$

The local metric

The set of velocity vectors

$$\frac{\pi}{2}\left(w_\theta e_\theta + \frac{w_\phi}{\tan\theta} e_\phi\right)$$

for $w_\theta^2 + w_\phi^2 = 1$ is generated by the unit velocity vectors under the metric

$$ds^2 = \frac{4}{\pi^2}\left(d\theta^2 + \tan^2\theta d\phi^2\right).$$

Goal: find distance between $(\pi/2, 0)$ and $(\pi/4, \pi/4)$.

Recap

Hamiltonian for oracle interrogation ($n = 2$)

$$\Downarrow$$

$$\frac{d}{dt}\begin{pmatrix} a_0(t) \\ a_1(t) \\ a_2(t) \end{pmatrix} = \frac{\pi}{2}\begin{pmatrix} 0 & -w_1(t) & 0 \\ w_1(t) & 0 & -w_2(t) \\ 0 & w_2(t) & 0 \end{pmatrix}\begin{pmatrix} a_0(t) \\ a_1(t) \\ a_2(t) \end{pmatrix}$$

$$\Downarrow$$

$$ds^2 = \frac{4}{\pi^2}\left(d\theta^2 + \tan^2\theta d\phi^2\right)$$

Geodesic equations

Second order differential equations

$$\ddot{\theta} = \frac{\sin\theta}{\cos^3\theta}\,\dot{\phi}^2,$$

$$\ddot{\phi} = \frac{-2}{\sin\theta\cos\theta}\,\dot{\theta}\,\dot{\phi},$$

can be simplified to

$$\dot{\phi} = \pm\frac{\pi}{2}\frac{\tan\theta_0}{\tan^2\theta},$$

$$1 = \frac{4}{\pi^2}\dot{\theta}^2 + \frac{4\tan^2\theta}{\pi^2}\dot{\phi}^2.$$

Small worries

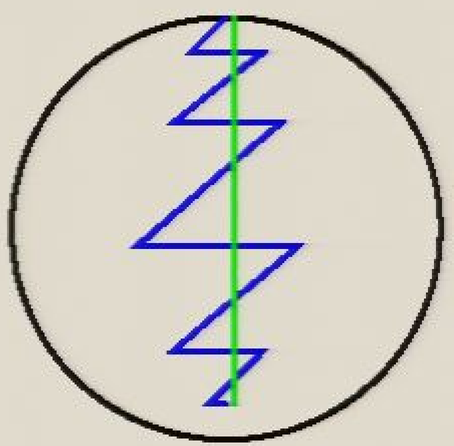
- Identification of points on the sphere by sign changes, leads to multiple possible starting and ending points.
- Must verify that geodesic solution is global minimum and not local minimum.
- Metric is poorly defined at starting point, need to start at $\theta = \pi/2 - \epsilon$.

Result

- Distance between $(\pi/2, 0)$ and $(\pi/4, \pi/4)$ is 0.9052.
- Above distance represents the query time needed to solve the $n = 2$ zero-error case of oracle interrogation with a Hamiltonian oracle.
- In the same units, the $n = 1$ case requires $T = 0.5$ query time.
- $\Longrightarrow$ Two bits can be queried with zero error faster when queried at the same time.

Summary

- Hamiltonian oracles are a potentially useful tool for proving lower bounds on unitary oracle problems.
- Hamiltonian oracles benefit from continuous equations and fractional queries.
- Hamiltonian oracles may be reduced to geometry.
- Geometry is fun.



Open problems

- Prove that all reasonable models of Hamiltonian oracles are equivalent.
- What is the relationship between Hamiltonian and Unitary oracles?
- What can be said about zero error vs. bounded error for Hamiltonian oracles?
- Prove new lower bounds (And-Or trees?)

Thank you!

Open problems

- Prove that all reasonable models of Hamiltonian oracles are equivalent.
- What is the relationship between Hamiltonian and Unitary oracles?
- What can be said about zero error vs. bounded error for Hamiltonian oracles?
- Prove new lower bounds (And-Or trees?)