Lecture 7: Verification for n-qubit Hamiltonians

Tuesday, November 10, 2020 9:51 AM

1 - Computational assumptions

2 - Protocol

3 - Completeness

4 - Soundness

5 - Construction of function family

---

1 Comp assumptions.

$$\mathcal{F} = \left\{ f_{pk} : \{0,1\}^m \to \{0,1\}^m \right\}_\lambda$$

F.1 $\forall pk$, • f_{pk} is 2-to-1
• f_{pk} can be efficiently evaluated

F.2 Adaptive hardcore bit: ~~trapdoor~~ hard to find (x, d) s.t. $d \cdot (x_0 + x_1) = 0$
where $\{x_0, x_1\} = f_{pk}^{-1}\{f_{pk}(x)\}$
$d \neq 0^m$

F.3 exists trapdoor td that allows efficient inversion

F.4 preimages of y are $x_0 = (0, x'_0)$
$x_1 = (1, x'_1)$

F.5 Collapsing

$\mathcal{A}$ $\xleftarrow{pk}$ C
$pk \leftarrow GEN(1^\lambda)$

prepare $|\phi\rangle = \sum_x \alpha_x |x\rangle$
$x \in$ domain of f_{pk}

$\xrightarrow{|b\rangle}$ 1. Evaluate f_{pk} on $|\phi\rangle$

$\to \sum_x \alpha_x |x\rangle |f(x)\rangle$

2. Measure image reg.
$\rightarrow (\alpha_{x_0}|x_0\rangle + \alpha_{x_1}|x_1\rangle)|y\rangle$

$\xleftarrow{G_b}$

3. Randomly send back either
$G_0 = (\alpha_0|x_0\rangle + \alpha_1|x_1\rangle)(\quad)^\dagger$
or
$G_1 = |\alpha_0|^2 |x_0\rangle\langle x_0| + |\alpha_1|^2 |x_1\rangle\langle x_1|$

has to guess b' st $b' = b$?

$\xrightarrow{b' \in \{0,1\}}$

Def $\mathcal{F}$ is collapsing if no QPT $\mathcal{A}$ can win in game w.p. $> \frac{1}{2} + \text{negl}(\lambda)$

Rk
- this implies collision-resistance:
  $\mathcal{A}$: prepare $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_1\rangle)$
- this implies that $\mathcal{A}$ cannot distinguish $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_1\rangle)$ from $\frac{1}{\sqrt{2}}(|x_0\rangle - |x_1\rangle)$

---

2. Protocol

λ, $H_C = -\sum_{i \neq j} \frac{J_{ij}}{2}(G_{x_i} G_{x_j} + G_{z_i} G_{z_j})$

$(pk_i, td_i) \leftarrow GEN(1^\lambda)$ $\quad i = 1 \dots n$

$\xrightarrow{pk_1, \dots, pk_n}$

Prepare $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$

For each $i \in \{1, \dots, n\}$:
- Prepare $\frac{1}{\sqrt{2^m}} \sum_x |x\rangle$
- Evaluate f_{pk_i} on i-th qubit of $|\psi\rangle$ +
- Measure outcome to get $y_i \in \{0,1\}^m$

$\xleftarrow{y_1, \dots, y_n}$

$i \neq j \leftarrow_R \{1, \dots, n\}$
$c \leftarrow_R \{0,1\}$

$\xrightarrow{c}$

measure in comp. basis to get $x_1, \dots, x_n$

$c = 0$

$\xleftarrow{x_1, \dots, x_n}$

check $\forall i$ $f_{pk_i}(x_i) = y_i$
if not, ABORT.
o/w set $\gamma = \binom{n}{2} \cdot J_{ij} \cdot (-1)^{b(x_i)} (-1)^{b(x_j)}$

(1st bit of x_i)

$c = 1$ $\quad\leftarrow d_1, \dots, d_n$

measure in Hadamard basis to get $d_1, \dots, d_n$

$$V = \left(\frac{1}{2}\right) J_{ij} (-1)^{d_i \cdot (x_{0,i} + x_{1,i})} (-1)^{d_j \cdot (x_{0,j} + x_{1,j})}$$

$d_i \cdot (x_{0,i} + x_{1,i})$: preimages of y_i; $d_j \cdot (x_{0,j} + x_{1,j})$: preimages of y_j

---

th **Completeness**: For any H_C and any $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ there exists a QPT P s.t.

(a) P is acc. wp 1 (no ABORT)

(b) $E[\gamma] = \langle \psi | H_C | \psi \rangle$

Soundness: For any H_C and any QPT prover P s.t. P is acc wp 1, there exists a $\rho \in \text{Dens}((\mathbb{C}^2)^{\otimes n})$ s.t. $E[\gamma] = \text{Tr}(H_C \rho)$

Rk:

- Soundness can be extended to $P_r(\text{ABORT}) < \frac{1}{2}$.
- Typically, protocol is run N times sequentially. Can also run in parallel.
- Gives us a delegated computation protocol. Can show that P "must have prepared ρ"

Completeness

Prover prepares $|\psi\rangle = \sum_{z \in \{0,1\}^n} \alpha_z |z\rangle$

encode in $|y\,|\,\Phi\rangle = \left(\sum_{z \in \{0,1\}^n} \alpha_z \; |z_1, z_1'\rangle |z_2, z_2'\rangle \cdots |z_n, z_n'\rangle \right) |y_1, \dots, y_n\rangle$

($z_1 \in \{0,1\}$, $z_1' \in \{0,1\}^{m-1}$; $|z_1, z_1'\rangle$: preimage of y_i)

W_y: $\alpha_0 |0\rangle + \alpha_1 |1\rangle \longrightarrow (\alpha_0 |x_0\rangle + \alpha_1 |x_1\rangle) |y_1\rangle$

$|0\rangle \longrightarrow |x_0\rangle$

$|1\rangle \longrightarrow |x_1\rangle$

$$\alpha_0|0\rangle + \alpha_1|1\rangle \longrightarrow \frac{1}{\sqrt{2^{m-1}}}\sum_x \left(\alpha_0|0\rangle|x\rangle + \alpha_1|1\rangle|x\rangle\right)$$

Eval f

$$\longrightarrow \frac{1}{\sqrt{2^{m-1}}}\sum_x \left(\alpha_0|0\rangle|x\rangle|f(0,x)\rangle + \alpha_1|1\rangle|x\rangle|f(1,x)\rangle\right)$$

meas $\to y$.

$$\longrightarrow \alpha\left(\alpha_0|0,x_0'\rangle + \alpha_1|1,x_1'\rangle\right)$$

(x_0, x_1)

---

3. Soundness

A - Definition of "extracted qubits" e

single-qubit case:

$$Z = \sum_x (-1)^{b(x)}|x\rangle\langle x|$$

$$X = \sum_d (-1)^{d\cdot(x_0+x_1)}$$ M_d

pair applied by P on challenge $c=1$.

V: prover's ancilla space

$$V: \quad H_x \otimes H_p \longrightarrow \mathbb{C}^2 \otimes H'$$

$$|\psi\rangle \longrightarrow \frac{1}{2}\sum_{P\in\{I,X,Z,XZ\}} (I\otimes\sigma_p\otimes P)|\phi^+\rangle|\psi\rangle$$

($|\phi^+\rangle$: EPR pair.)

We showed:

if $\{Z,X\}=0$

$$\begin{array}{ccc} H & \xrightarrow{V} & \mathbb{C}^2\otimes H' \\ {\scriptstyle Z}\downarrow & & \downarrow{\scriptstyle \sigma_Z\otimes I} \\ {\scriptstyle X}\downarrow & & \downarrow{\scriptstyle \sigma_X\otimes I}. \\ H & \xrightarrow[V]{} & \mathbb{C}^2\otimes H' \end{array}$$

Lemma Suppose $\{X(a) : a\in\{0,1\}^n\}$, $\{Z(b) : b\in\{0,1\}^n\}$ are observables on H.

Then

$$V: \quad H \longrightarrow (\mathbb{C}^2)^{\otimes n}\otimes H'$$

$$|\psi\rangle \longmapsto \frac{1}{2^n}\sum_{a,b\in\{0,1\}^n} \left(I\otimes\sigma_x(a)\sigma_z(b)\otimes X(a)Z(b)\right)|\phi^+\rangle^{\otimes n}|\psi\rangle$$

is an isometry.

$$\sigma_x(a) = \sigma_{x,1}^{a_1}\otimes\sigma_{x,2}^{a_2}\otimes\cdots\otimes\sigma_{x,n}^{a_n}$$

Def: let $\mathcal{C}$ be the state of the first n qubits of $V|\psi\rangle$. Call $\mathcal{C}$ "extracted qubits".

where $$Z(b) = \sum_{x_1,\dots,x_n} (-1)^{b_1\cdot b(x_1)} \cdots (-1)^{b_n\cdot b(x_n)} |x_1\rangle\langle x_1| \otimes \cdots |x_n\rangle\langle x_n|$$

$$X(a) = \sum_{d_1,\dots,d_n} (-1)^{a_1\cdot d_1\cdot(x_{0,1}+x_{0,1})} \cdots (-1)^{a_n d_n\cdot(x_{0,n}+x_{1,n})} M_{d_1,\dots,d_n}$$

Hard prover

W $\quad$ V

$|0\rangle \longrightarrow |x_0\rangle \longrightarrow |0\rangle$

$|1\rangle \longrightarrow |x_1\rangle \longrightarrow |1\rangle$

$|\psi\rangle$

$|\psi\rangle \longmapsto |\Phi\rangle \longrightarrow |\psi\rangle$

$Tr(H_c\,\mathcal{C})$?

$\underbrace{G_{x,i}G_{x,j}}$ $\quad$ $\underbrace{G_{z,i}G_{z,j}}$

$G_x(a)$ $\quad$ $G_z(b_i+b_j)$

$a = e_i + e_j$

Lemma 1 Assume $X(a)$, $Z(b)$ are observables and $X(a)X(a') = X(a+a')$ $\forall a,a'$.

Then:

$\forall b$, $\quad Tr(G_z(b)\,\mathcal{C}) = \langle\psi|Z(b)|\psi\rangle$

$\forall a$, $\quad Tr(G_x(a)\,\mathcal{C}) = \frac{1}{2^n}\sum_{b\in\{0,1\}^n}(-1)^{a\cdot b}\langle\psi|Z(b)X(a)Z(b)|\psi\rangle$

if x,z anti-commute $\Rightarrow \langle\psi|X(a)|\psi\rangle$

Pf: Calculation. $\quad G_x(a)G_z(b) = (-1)^{a\cdot b} G_z(b)G_x(a)$

Lemma 2 Suppose P succeeds w.p. 1 in protocol and "does not break F.2 and F.5"

Then:

- If $b = e_i + e_j$ then $Tr(G_z(b)\,\mathcal{C}) = E\,(-1)^{b(x_i)}(-1)^{b(x_j)}$ (computed by the verifier in case $c=0$)
- If $a = e_i + e_j$ then $Tr(G_x(a)\,\mathcal{C}) \approx E\,(-1)^{d_i\cdot(x_{0,i}+x_{1,i})}$ $d_i\cdot(x_{0,i}+x_{1,i})$

• If $a = e+g$ then $\mathrm{Tr}(G_x(a)|e\rangle) \approx$ (up to $\mathrm{negl}(\lambda)$) $E (-1)^{d_i \cdot (x_{0,i}+x_{1,i})} \cdot (-1)^{d_j \cdot (x_{0,j}+x_{1,j})}$

Pf Use lemma 1

$$\mathrm{Tr}(G_x(a)|e\rangle) = \frac{1}{2^n} \sum_{b \in \{0,1\}^n} \langle \psi | Z(b) X(a) Z(b) | \psi \rangle$$

$\langle \psi |$ $\quad$ $|\psi\rangle$

to show $\approx$ $\quad$ $\langle \psi | X(a) | \psi \rangle$

Collapsing $\Rightarrow$ $|\psi\rangle \approx Z(b)|\psi\rangle$

$\Rightarrow$ $|\langle \psi | X(a) | \psi \rangle - \langle \psi | Z(b) X(a) Z(b) | \psi \rangle|$ small

---

Proof of soundness:

Let P succeed w.p. 1

Let e be the "x extracted qubits".

$$\mathrm{Tr}(H_C e) = -\sum_{i \neq j} \frac{\pi_{ij}}{2} \left(\mathrm{Tr}(G_{z_i} G_{z_j} e) + \mathrm{Tr}(G_{x_i} G_{x_j} e) \right)$$

definition of H_C

$$\approx_{\mathrm{negl}(\lambda)} -\sum_{i \neq j} \frac{\pi_{ij}}{2} \left((-1)^{b(x_i)} (-1)^{b(x_j)} + (-1)^{d_i \cdot (x_0 + x_1)_i} (-1)^{d_j \cdot (x_0 + x_1)_j} \right)$$

lemma 2

$$= E[V]$$

by definition of V

4- Construction of claw-free family $\mathcal{F}$

~~$f(x) = f(x+s) \quad x, s \in \mathbb{Z}_2^n$~~

~~$f(x) = Ax \quad A \in \mathbb{F}_2^{n \times n}$ s.t. $\mathrm{rk}(A) = n-1$~~

Learning with Errors (LWE) assumption (Regev, 2005)

n, m, q integers.

n, m, q integers.

χ : distr on $\mathbb{Z}_q$.

LWE assumption:

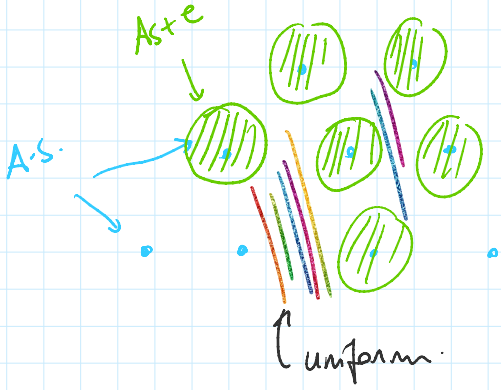
$$\{ (A, As+e) \text{ where } A \leftarrow_R \mathbb{Z}_q^{m \times n},\ s \leftarrow_R \{0,1\}^n,\ e \leftarrow \chi^m \}$$

comp indistinguishable $\rightarrow \simeq$

$$\{ (A, u) \text{ where } A \leftarrow_R \mathbb{Z}_q^{m \times n},\ u \leftarrow_R \mathbb{Z}_q^m \}$$

Typically, χ is discrete gaussian on $\mathbb{Z}_q$ centered at 0 with variance αq $0 < \alpha \ll 1$

$m \gg n \log q$ ($\Rightarrow$ s is uniquely recoverable from $(A, As+e)$ in principle.)



Construction of $\mathcal{F}$:

$pk = (A, As+e)$ where $A \leftarrow_R \mathbb{Z}_q^{m \times n}$, $s \leftarrow_R \{0,1\}^n$, $e \leftarrow \chi^m$

$f_{pk}(b, x')$ where $b \in \{0,1\}$, $x' \in \mathbb{Z}_q^n$

$f_{pk}(0, x') = Ax' + e_0$ $\quad e_0 \sim (\chi')^m$

$f_{pk}(1, x') = Ax' + (As+e) + e_1$ $\quad e_1 \sim (\chi')^m$

$= A(x'+s) + e + e_1$.

When do we have $f_{pk}(0, x_0') \simeq f_{pk}(1, x_1')$

$Ax_0' + e_0 \simeq A(x_1' + s) + e + e_1$

$$A x_0' + e_0 \simeq A(x_1' + s) + e + e_1$$

$$\Rightarrow \underbrace{A x_0' = A(x_1' + s)}_{\Rightarrow\ y_0' = x_1' + s.} \quad \text{and} \quad e_0 \simeq e + e_1$$