Quantum Computation - Lecture 05 - Quantum Fourier Transform

Mateus de Oliveira Oliveira

TCS-KTH

December 3, 2012

- Quantum Fourier transform over $\mathbb{Z}_n$
- QFT for abelian groups,
- Hidden subgroup problem for abelian groups
- QFT for general groups

- Quantum Fourier Transform over $\mathbb{Z}_N$:

$$QFT_N|x\rangle = \sum_{y=0}^{N-1} e^{\frac{2\pi ixy}{N}}|y\rangle$$

- Quantum Fourier Transform over $\mathbb{Z}_N$:

$$QFT_N|x\rangle = \sum_{y=0}^{N-1} e^{\frac{2\pi ixy}{N}} |y\rangle$$

- Recall that any abelian group G is isomorphic to the direct sum of cyclic groups:

$$G = \bigoplus_{j=1}^{k} \mathbb{Z}_{N_j}$$

- Quantum Fourier Transform over $\mathbb{Z}_N$:

$$QFT_N|x\rangle = \sum_{y=0}^{N-1} e^{\frac{2\pi ixy}{N}}|y\rangle$$

- Recall that any abelian group G is isomorphic to the direct sum of cyclic groups:

$$G = \bigoplus_{j=1}^{k} \mathbb{Z}_{N_j}$$

- Quantum fourier transform over G:

$$QFT|x_1\rangle|x_2\rangle...|x_k\rangle \rightarrow (QFT_{N_1}|x_1\rangle)(QFT_{N_2}|x_2\rangle)...(QFT_{N_k}|x_k\rangle)$$

- Quantum Fourier Transform over $\mathbb{Z}_N$:

$$QFT_N|x\rangle = \sum_{y=0}^{N-1} e^{\frac{2\pi ixy}{N}}|y\rangle$$

- Recall that any abelian group G is isomorphic to the direct sum of cyclic groups:

$$G = \bigoplus_{j=1}^{k} \mathbb{Z}_{N_j}$$

- Quantum fourier transform over G:

$$QFT|x_1\rangle|x_2\rangle...|x_k\rangle \rightarrow (QFT_{N_1}|x_1\rangle)(QFT_{N_2}|x_2\rangle)...(QFT_{N_k}|x_k\rangle)$$

- $$= \frac{1}{\sqrt{N_1 N_2 \cdot N_k}} \sum_{y_1 y_2 ... y_k} e^{\sum_{j=1}^{k} \frac{2\pi i x_j y_j}{N_j}} |y_1\rangle|y_2\rangle...|y_k\rangle$$

- Simplifying the notation: If $G = \oplus_{j=1}^{k} \mathbb{Z}_j$ then set

- Simplifying the notation: If $G = \oplus_{j=1}^{k} \mathbb{Z}_j$ then set
  - $g = (g_1, g_2, ..., g_k)$, $x = (x_1, x_2, ..., x_k)$, $y = (y_1, y_2, ..., y_k)$

- Simplifying the notation: If $G = \oplus_{j=1}^{k} \mathbb{Z}_j$ then set
  - $g = (g_1, g_2, ..., g_k)$, $x = (x_1, x_2, ..., x_k)$, $y = (y_1, y_2, ..., y_k)$
  - $\chi_y(g) = e^{\sum_{j=1}^{k} \frac{2\pi i g_j y_j}{N_j}} |y\rangle$

- Simplifying the notation: If $G = \oplus_{j=1}^{k} \mathbb{Z}_j$ then set
  - $g = (g_1, g_2, ..., g_k)$, $x = (x_1, x_2, ..., x_k)$, $y = (y_1, y_2, ..., y_k)$
  - $\chi_y(g) = e^{\sum_{j=1}^{k} \frac{2\pi i g_j y_j}{N_j}} |y\rangle$
- Then QFT can be written as:

$$QFT|g\rangle = \frac{1}{\sqrt{|G|}} \sum_{y \in G} \chi_y(g)|y\rangle$$

- Simplifying the notation: If $G = \oplus_{j=1}^{k} \mathbb{Z}_j$ then set
  - $g = (g_1, g_2, ..., g_k)$, $x = (x_1, x_2, ..., x_k)$, $y = (y_1, y_2, ..., y_k)$
  - $\chi_y(g) = e^{\sum_{j=1}^{k} \frac{2\pi i g_j y_j}{N_j}} |y\rangle$
- Then QFT can be written as:

$$QFT|g\rangle = \frac{1}{\sqrt{|G|}} \sum_{y \in G} \chi_y(g)|y\rangle$$

- and its inverse:

$$QFT^{-1}|g\rangle = \frac{1}{\sqrt{|G|}} \sum_{y \in G} \overline{\chi_y(g)}|y\rangle$$

- Superposition of the elements of a Coset:

- Superposition of the elements of a Coset:
- Define $|Hg\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |hg\rangle$

- Superposition of the elements of a Coset:
- Define $|Hg\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |hg\rangle$
- $$QFT|Hg\rangle = \frac{1}{\sqrt{H}} \sum_{h \in H} \frac{1}{\sqrt{|G|}} \sum_{y \in G} \chi_y(hg)|y\rangle$$

- Superposition of the elements of a Coset:
- Define $|Hg\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |hg\rangle$
- $$QFT|Hg\rangle = \frac{1}{\sqrt{H}} \sum_{h \in H} \frac{1}{\sqrt{|G|}} \sum_{y \in G} \chi_y(hg)|y\rangle$$
- $$= \frac{1}{\sqrt{|H||G|}} \sum_{y \in G} \chi_y(g) \left[\sum_{h \in H} \chi_y(h) \right] |y\rangle$$

- Define

$$H^{\perp} = \{y \in G | (\forall h \in H) \sum_{j=1}^{k} \frac{y_j h_j}{N_j} \in \mathbb{Z}\}$$

- Define
$$H^{\perp} = \{y \in G | (\forall h \in H) \sum_{j=1}^{k} \frac{y_j h_j}{N_j} \in \mathbb{Z}\}$$
- Exercise: If G is an Abelian group and H is an abelian subgroup of G then $H^{\perp}$ is an abelian subgroup of G.

- Define

$$H^{\perp} = \{y \in G | (\forall h \in H) \sum_{j=1}^{k} \frac{y_j h_j}{N_j} \in \mathbb{Z}\}$$

- Exercise: If G is an Abelian group and H is an abelian subgroup of G then $H^{\perp}$ is an abelian subgroup of G.
- Exercise:

$$\sum_{h \in H} \chi_y(h) = \begin{cases} |H| & \text{if } y \in H^{\perp} \\ = 0 & \text{otherwise.} \end{cases}$$

- Define

$$H^{\perp} = \{y \in G | (\forall h \in H) \sum_{j=1}^{k} \frac{y_j h_j}{N_j} \in \mathbb{Z}\}$$

- Exercise: If G is an Abelian group and H is an abelian subgroup of G then $H^{\perp}$ is an abelian subgroup of G.
- Exercise:

$$\sum_{h \in H} \chi_y(h) = \begin{cases} |H| & \text{if } y \in H^{\perp} \\ = 0 & \text{otherwise.} \end{cases}$$

- Plugging this exercise in the equation:

$$QFT|Hg\rangle = \frac{1}{\sqrt{|H||G|}} \sum_{y \in G} \chi_y(g) \left[\sum_{h \in H} \chi_y(h) \right] |y\rangle$$

- Define

$$H^{\perp} = \{y \in G | (\forall h \in H) \sum_{j=1}^{k} \frac{y_j h_j}{N_j} \in \mathbb{Z}\}$$

- Exercise: If G is an Abelian group and H is an abelian subgroup of G then $H^{\perp}$ is an abelian subgroup of G.
- Exercise:

$$\sum_{h \in H} \chi_y(h) = \begin{cases} |H| & \text{if } y \in H^{\perp} \\ = 0 & \text{otherwise.} \end{cases}$$

- Plugging this exercise in the equation:

$$QFT|Hg\rangle = \frac{1}{\sqrt{|H||G|}} \sum_{y \in G} \chi_y(g) \left[\sum_{h \in H} \chi_y(h) \right] |y\rangle$$

- we have:

$$QFT|Hg\rangle = \sqrt{\frac{|H|}{|G|}} \sum_{y \in H^{\perp}} \chi_y(g)|y\rangle$$

- Create a uniform superposition of all elements of G:

$$|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle$$

- Create a uniform superposition of all elements of G:

$$|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle$$

- Apply the black box function:

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |f(x)\rangle$$

- Create a uniform superposition of all elements of G:

$$|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle$$

- Apply the black box function:

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |f(x)\rangle$$

- Measure the second register: Then for some element $g \in G$ the first register collapses to $|Hg\rangle$

- Create a uniform superposition of all elements of G:

$$|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle$$

- Apply the black box function:

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |f(x)\rangle$$

- Measure the second register: Then for some element $g \in G$ the first register collapses to $|Hg\rangle$
- Apply the inverse fourier quantum fourier transform:

$$\sqrt{\frac{|H|}{|G|}} \sum_{y \in H^{\perp}} \overline{\chi_y(g)} |y\rangle$$

- Create a uniform superposition of all elements of G:

$$|G\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle$$

- Apply the black box function:

$$\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle |f(x)\rangle$$

- Measure the second register: Then for some element $g \in G$ the first register collapses to $|Hg\rangle$
- Apply the inverse fourier quantum fourier transform:

$$\sqrt{\frac{|H|}{|G|}} \sum_{y \in H^{\perp}} \overline{\chi_y(g)} |y\rangle$$

- Measuring the first register we have an uniform $y \in H^{\perp}$

- Fact: Any group on n elements can be generated by a set of $O(\log n)$ elements.

- Fact: Any group on n elements can be generated by a set of $O(\log n)$ elements.
- Exercise: After measuring $O(\log n)$ y's with constant probability we have indeed a set of generators for $H^{\perp}$.

- Fact: Any group on n elements can be generated by a set of $O(\log n)$ elements.
- Exercise: After measuring $O(\log n)$ y's with constant probability we have indeed a set of generators for $H^{\perp}$.
- Repeating the anterior procedure $O(\log n)$ times we get a sequence $\langle y_1, y_2, ..., y_{O(\log n)} \rangle$

- Fact: Any group on n elements can be generated by a set of $O(\log n)$ elements.
- Exercise: After measuring $O(\log n)$ y's with constant probability we have indeed a set of generators for $H^{\perp}$.
- Repeating the anterior procedure $O(\log n)$ times we get a sequence $\langle y_1, y_2, ..., y_{O(\log n)} \rangle$
- Exercise (analogous to Simon's problem): Finding a set of generators for $H^{\perp}$. We can find a set of generators for $H = (H^{\perp})^{\perp}$

- Let V be a finite dimensional vector space. Then $U(V)$ denotes the group of unitary linear tranformations on V.

- Let V be a finite dimensional vector space. Then $U(V)$ denotes the group of unitary linear tranformations on V.
- A representation ρ of a finite group G is a homomorphism $\rho : G \rightarrow U(V)$ where V is a finite d_ρ-dimensional vector space over $\mathbb{C}$ with an inner product.

- Let V be a finite dimensional vector space. Then $U(V)$ denotes the group of unitary linear tranformations on V.
- A representation ρ of a finite group G is a homomorphism $\rho : G \to U(V)$ where V is a finite d_ρ-dimensional vector space over $\mathbb{C}$ with an inner product.
- Fixing an orthonormal basis for V each $\rho(g)$ may be realized as a $d_\rho \times d_\rho$ unitary matrix.

- Let V be a finite dimensional vector space. Then $U(V)$ denotes the group of unitary linear tranformations on V.
- A representation ρ of a finite group G is a homomorphism $\rho : G \to U(V)$ where V is a finite d_ρ-dimensional vector space over $\mathbb{C}$ with an inner product.
- Fixing an orthonormal basis for V each $\rho(g)$ may be realized as a $d_\rho \times d_\rho$ unitary matrix.
- In that case say that ρ is a matrix representation of G.

- Let V be a finite dimensional vector space. Then $U(V)$ denotes the group of unitary linear tranformations on V.
- A representation ρ of a finite group G is a homomorphism $\rho : G \to U(V)$ where V is a finite d_ρ-dimensional vector space over $\mathbb{C}$ with an inner product.
- Fixing an orthonormal basis for V each $\rho(g)$ may be realized as a $d_\rho \times d_\rho$ unitary matrix.
- In that case say that ρ is a matrix representation of G.
- Define the function $\rho_{ij}(g) = [\rho(g)]_{ij}$.

- Let V be a finite dimensional vector space. Then $U(V)$ denotes the group of unitary linear tranformations on V.
- A representation ρ of a finite group G is a homomorphism $\rho : G \to U(V)$ where V is a finite d_ρ-dimensional vector space over $\mathbb{C}$ with an inner product.
- Fixing an orthonormal basis for V each $\rho(g)$ may be realized as a $d_\rho \times d_\rho$ unitary matrix.
- In that case say that ρ is a matrix representation of G.
- Define the function $\rho_{ij}(g) = [\rho(g)]_{ij}$.
- Since ρ is a homomorphism $\rho(gh) = \rho(g)\rho(h)$. Then $\rho_{ij}(gh) = \sum_j \rho_{ik}(g)\rho_{kj}(h)$.

- Irreducible representation: There is no unitary U such that $U\rho U^{\dagger}$ is block diagonal.

- Irreducible representation: There is no unitary U such that $U\rho U^\dagger$ is block diagonal.
- Two representations ρ and σ are equivalent if they differ only in a change of basis. In other words, there is a fixed U such that $\sigma(g) = U^\dagger \rho(g) U$ for every $g \in G$.

- Irreducible representation: There is no unitary U such that $U\rho U^\dagger$ is block diagonal.
- Two representations ρ and σ are equivalent if they differ only in a change of basis. In other words, there is a fixed U such that $\sigma(g) = U^\dagger \rho(g) U$ for every $g \in G$.
- A finite group G has a finite number of irreducible representations equal to the number of its conjugacy classes.

- Irreducible representation: There is no unitary U such that $U\rho U^\dagger$ is block diagonal.
- Two representations ρ and σ are equivalent if they differ only in a change of basis. In other words, there is a fixed U such that $\sigma(g) = U^\dagger \rho(g) U$ for every $g \in G$.
- A finite group G has a finite number of irreducible representations equal to the number of its conjugacy classes.
- $\hat{G}$ denotes a set containing exactly one representation of each equivalence class.

- Irreducible representation: There is no unitary U such that $U\rho U^\dagger$ is block diagonal.
- Two representations ρ and σ are equivalent if they differ only in a change of basis. In other words, there is a fixed U such that $\sigma(g) = U^\dagger \rho(g) U$ for every $g \in G$.
- A finite group G has a finite number of irreducible representations equal to the number of its conjugacy classes.
- $\hat{G}$ denotes a set containing exactly one representation of each equivalence class.
- The set of all entries of all matrices in $\hat{G}$ form a $|G|$ dimensional vector space of complex valued functions on G. In other words, a basis to the space of functions $f : G \to \mathbb{C}$.

- Irreducible representation: There is no unitary U such that $U\rho U^\dagger$ is block diagonal.
- Two representations ρ and σ are equivalent if they differ only in a change of basis. In other words, there is a fixed U such that $\sigma(g) = U^\dagger \rho(g) U$ for every $g \in G$.
- A finite group G has a finite number of irreducible representations equal to the number of its conjugacy classes.
- $\hat{G}$ denotes a set containing exactly one representation of each equivalence class.
- The set of all entries of all matrices in $\hat{G}$ form a $|G|$ dimensional vector space of complex valued functions on G. In other words, a basis to the space of functions $f : G \to \mathbb{C}$.
- Therefore $\sum_{\rho \in \hat{G}} d_\rho^2 = G$.

- Fourier Transform of f at ρ: Let $f : G \to \mathbb{C}$ and $\rho : G \to U(V)$ be a matrix representation of G. Then the Fourier transform of f at ρ, denoted by $\hat{f}(\rho)$ is the matrix

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{|G|}} \sum_{g \in G} f(g)\rho(g)$$

.

- Fourier Transform of f at ρ: Let $f : G \to \mathbb{C}$ and $\rho : G \to U(V)$ be a matrix representation of G. Then the Fourier transform of f at ρ, denoted by $\hat{f}(\rho)$ is the matrix

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{|G|}} \sum_{g \in G} f(g)\rho(g)$$

.

- The collection $\{\hat{f}(\rho)\}_{\rho \in \hat{G}_B}$ is called the Fourier Transform of f.

- Fourier Transform of f at ρ: Let $f : G \to \mathbb{C}$ and $\rho : G \to U(V)$ be a matrix representation of G. Then the Fourier transform of f at ρ, denoted by $\hat{f}(\rho)$ is the matrix

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{|G|}} \sum_{g \in G} f(g)\rho(g)$$

.

- The collection $\{\hat{f}(\rho)\}_{\rho \in \hat{G}_B}$ is called the Fourier Transform of f.
- In this way, f is mapped into $|\hat{G}|$ matrices of varying dimensions.

- Fourier Transform of f at ρ: Let $f : G \to \mathbb{C}$ and $\rho : G \to U(V)$ be a matrix representation of G. Then the Fourier transform of f at ρ, denoted by $\hat{f}(\rho)$ is the matrix

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{|G|}} \sum_{g \in G} f(g)\rho(g)$$

.

- The collection $\{\hat{f}(\rho)\}_{\rho \in \hat{G}_B}$ is called the Fourier Transform of f.
- In this way, f is mapped into $|\hat{G}|$ matrices of varying dimensions.
- The total number of entries in these matrices is $\sum d_\rho^2 = |G|$.

- Fourier Transform of f at ρ: Let $f : G \to \mathbb{C}$ and $\rho : G \to U(V)$ be a matrix representation of G. Then the Fourier transform of f at ρ, denoted by $\hat{f}(\rho)$ is the matrix

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{|G|}} \sum_{g \in G} f(g)\rho(g)$$

.

- The collection $\{\hat{f}(\rho)\}_{\rho \in \hat{G}_B}$ is called the Fourier Transform of f.
- In this way, f is mapped into $|\hat{G}|$ matrices of varying dimensions.
- The total number of entries in these matrices is $\sum d_\rho^2 = |G|$.
- The fourier transform is linear in f.

- Inner product for complex valued functions: $\langle f_1, f_2 \rangle = \frac{1}{|G|} f_1(g) f_2(g)^*$

- Inner product for complex valued functions: $\langle f_1, f_2 \rangle = \frac{1}{|G|} f_1(g) f_2(g)^*$
- For any pair of matrix representations $\rho, \sigma \in \hat{G}_B$ the corresponding irreducible matrix elements are orthogonal according to the inner product defined as follows

- Inner product for complex valued functions: $\langle f_1, f_2 \rangle = \frac{1}{|G|} f_1(g) f_2(g)^*$
- For any pair of matrix representations $\rho, \sigma \in \hat{G}_B$ the corresponding irreducible matrix elements are orthogonal according to the inner product defined as follows
- $\langle [\rho(\cdot)]_{ij}, [\sigma(\cdot)]_{kl} \rangle = 0$ if $\rho \neq \sigma$

- Inner product for complex valued functions: $\langle f_1, f_2 \rangle = \frac{1}{|G|} f_1(g) f_2(g)^*$
- For any pair of matrix representations $\rho, \sigma \in \hat{G}_B$ the corresponding irreducible matrix elements are orthogonal according to the inner product defined as follows
- $\langle [\rho(\cdot)]_{ij}, [\sigma(\cdot)]_{kl} \rangle = 0$ if $\rho \neq \sigma$
- $\langle [\rho(\cdot)]_{ij}, [\sigma(\cdot)]_{kl} \rangle = \frac{1}{d_\rho \delta_{ik} \delta_{jl}}$ if $\rho = \sigma$

- Computing the Fourier transform with respect to a choice of $\hat{G}$ is equivalent to the change of basis from the basis defined by the point masses to the irreducible matrix representations determined by $\hat{G}$.

- Computing the Fourier transform with respect to a choice of $\hat{G}$ is equivalent to the change of basis from the basis defined by the point masses to the irreducible matrix representations determined by $\hat{G}$.
- The inverse of this is given by:

- Computing the Fourier transform with respect to a choice of $\hat{G}$ is equivalent to the change of basis from the basis defined by the point masses to the irreducible matrix representations determined by $\hat{G}$.
- The inverse of this is given by:
- $$f(s) = \sum_{\rho \in \hat{G}} \sqrt{\frac{d_\rho}{|G|}} tr(\rho(s)\hat{f}(\rho)^{-1})$$

- Rewriting the fourier transform in quantum notation:

$$QFT|g\rangle = \frac{1}{\sqrt{|G|}} \sum_{\rho \in \hat{G}} \sqrt{d_\rho} \sum_{i,j=1}^{d_\rho} \rho_{i,j}(g)|\rho, i, j\rangle$$