Quantum Computation

oliverobrien111

July 2021

1 Lecture 1

1.1 Review of Shor's algoirthm/quantum period finding algorithm

Polynomial time hierarchy:// Computation with input of size n, and we are interested in the number of steps/gates (classical or quantum). When we say $O(poly(n))$ steps we regard this as an "efficent computation".

Shor's algorithm solves the factoring problem:
Given an integer N needing $O(logN)$ bits, we want to find a non-trival factor in $O(polyn)$ time.

The best known classical algorithm (number sieve): $e^{O(n^{\frac{1}{3}}(\log n)^{\frac{1}{3}})}$
Shor's alogrithm takes $O(n^3)$

1.1.1 Quantum factoring algorithm (summary)

1. First, convert factoring into periodicity determination. Given N, choose $a < N$ s.t. a is coprime (this is easy classically can be seen in part II lecture notes). Consider $f : \mathbb{Z} \to \mathbb{Z}_N$ $f(x) = a^x \mod N$. **Euler's Theorem**: if f is periodic with period r, then it is called 'order of $a \mod N$'.

2. In order to find r we need a quantum implementation of f. We are always workingon finite size registers so restricting $x \in \mathbb{Z}$ to $x \in \mathbb{Z}_M$ (for some large enough M): $f : \mathbb{Z}_M \to \mathbb{Z}_N$. f will no longer be exactly preriodic but this would have neglible effect if M is sufficently large e.g. $M = O(N^2)$

3. Using the classical theory of continued fractions. Define Hilbert spaces $\mathcal{H}_M \to \{|i\rangle\}_{i\in\mathbb{Z}_M}, \mathcal{H}_N \to \{|i\rangle\}_{i\in\mathbb{Z}_N}$.

4. $|x\rangle \to |f(x)\rangle$ is not generally a valid quantum operator, so we make it a unitary operation which can be implemented:

$$U_f : \mathcal{H}_M \otimes \mathcal{H}_N \to \mathbb{H}_M \otimes \mathbb{H}_N$$

$$U_f : |i\rangle |k\rangle \rightarrow |i\rangle |k + f(i)\rangle$$

5. if $x \rightarrow f(x)$ can be classically computed in $O(poly(m))$ time ($m = \log M$)), then U_f can be implemented in poly(m) time quantumly too

6. We will sometimes view U_f as a black box/oracle and we will count the number of times the algorithm invokes the oracle.

7. Back to facotoring to get r we'll use the quantum algorithm for periodicity determination:

8. Given an oracle U_f with the promise that f is periodic of some unknown period $r \in \mathbb{Z}_N$ so that $f(x + r) = f(x)$ and f is one-to-one in this period (for all $0 \leq x_1 < x_2 < r f(x_1) \neq f(x_2)$)

9. To find r in $O(polyn)$ with any persecribed success probability $1 - \epsilon$ we use the following alogirthm:

   - Step 1: Create the state

   $$\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle |0\rangle$$

   - Step 2: Apply U_f to get

   $$\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle |f(i)\rangle$$

   - Step 3: Measure the 2nd register to get y. By the born rule the first register collapses to all those i: $f(i) = y$ i.e. $i = x_0, x_0 + r, x_o + 2r, ..., x_0 + (A - 1)r$, $0 \leq x_0 < r$.

     Discard the second register to get the following state:

   $$|per\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle$$

     If we measure $|per\rangle$ in computation basis we will get a value of one of these states $x_0 + jr$ for uniformly random j. This only gives us a random element of $\mathbb{Z}_M$ with no information about r.

   - Step 4: Apply quantum fourier transform mod M (QFT). Lets recap what QFT does:

   $$|x\rangle \rightarrow \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \omega^{xy} |y\rangle, \forall x \in \mathbb{Z}_M, \omega = e^{2\pi i/M}$$

This can be implement in $O(m^2)$ time and gives state:

$$QFT\,|per\rangle = \frac{1}{\sqrt{MA}}\sum_{j=0}^{A-1}\sum_{y=0}^{M-1}\omega^{(x_0+jr)y}\,|y\rangle = \frac{1}{\sqrt{MA}}\sum_{y=0}^{M-1}\omega^{x_0 y}\left[\sum_{j=0}^{A-1}\omega^{jry}\,|y\rangle\right]$$

The square brackets will be:

$$\begin{cases} A & \text{if } y = KA = k\frac{M}{r}, x = 0, 1, ..., r-1 \\ 0 & \text{otherwise} \end{cases}$$

So gives final state:

$$QFT\,|per\rangle = \sqrt{\frac{A}{M}}\sum_{k=0}^{A-1}\omega^{x_0 k\frac{N}{r}}\,|k\frac{M}{r}\rangle$$

Now the random shift x_0 only appears in the phase not in the ket labels. So now the measurement probabilities will be indepedant of x_0. When we measure this we get some value $c = \frac{k_0 M}{r}$ with k_0 uniformly random in range $0 \leq k_0 < r$

$$\frac{k_0}{r} = \frac{c}{M}$$

As c and M are known, and k_0 is unknown but random in the given range. We want to find r and so we recall several classical facts.

Co-primality Theorem: The number of integers less than r that are coprime to r grows with $O(\frac{r}{\log\log r})$

Therefore, the probability of k_0 being coprime to r is $O(\frac{1}{\log\log r})$.

Lemma: If a single trial has success probability p then if one repeats it M^* times, for any $0 < 1-\epsilon < 1$. We get probability of at least one success in M^* trails is greater than $1-\epsilon$ if $M^* = \frac{-\log\epsilon}{p}$. i.e. roughly $O(1/p)$ trials suffice to achieve probability of success $> 1-\epsilon$

- After step 4 cancel $\frac{c}{M}$ down to an irredicible algorithm $\frac{a}{b}$ there is an efficent algorithm ($O(polyn)$) for this. This will give us r as denominator b if k_0 is coprime to r with probablity $O(\frac{1}{\log\log r})$. So check b value by computing $f(0)$ and $f(b)$ and $b = r \iff f(0) = f(b)$.

  By repeating this process $M^* = O(\log\log r)$ times this will give us r with any desired probability $1-\epsilon$. Since $r < M$ the whole algorithm takes $O(polym)$ time!

10. From learning the period r we can use number theory to find a factor of N

1.1.2 Further insights to QFT

Now lets think about the implications of QFT. What does applying quantum fourier transform really achieve?

Lets consider a function: $f : \mathbb{Z}_M \to \mathbb{Z}_N$ with period $r \in \mathbb{Z}_M$, $A = \frac{M}{r}$. Define:

$$R = \{0, r, 2r, 3r, ..., (A-1)r\} < \mathbb{Z}_M$$

$$|R\rangle = \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |kr\rangle$$

$$|per\rangle = |x_0 + R\rangle = \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |x_0 + rk\rangle$$

The problem was this random shift x_0 when measuring $|per\rangle$. For each $x_0 < \mathbb{Z}_M$ consider a mapping $k \to k + x_0$. "Shift by x_0". It is a 1-1 invertible map, and can define a unitary version $U(x_0)$ on $\mathcal{H}_M$: $U(x_0)|k\rangle = |k + x_0\rangle$.

$$|x_0 + R\rangle = U(x_0)|R\rangle$$

Since $(\mathbb{Z}_M, +)$ is an abelian group $U(x_0)U(x_1) = U(x_0 + x_1) = U(x_1)U(x_0)$. So all $U(x_i)$ commute as operators on $\mathcal{H}_M$. Therefore they have an orthonomal basis of common eigenvectors $\{|\chi_k\rangle\}_{k\in\mathbb{Z}_M}$. These are called shift invariant states as $U(x_0)|\chi_k\rangle = \omega(x_0, k)|\chi_k\rangle$ for all $x_0, k \in \mathbb{Z}_M$ with the important caveat that $|\omega(x_0, k)| = 1$.

Consider $|R\rangle$ written in $\{|\chi_r\rangle\}$ basis:

$$|R\rangle = \sum_{k=0}^{M-1} a_k |\chi_k\rangle$$

a_k only depend on r not on x_0. Then:

$$|per\rangle = U(x_0)|R\rangle = \sum_{k=0}^{M-1} a_k \omega(x_0, k)|\chi_k\rangle$$

Here it can be seen that the probability of measuring k is

$$prob(k) = |a_k \omega(x_0, k)|^2 = |a_k|^2$$

So this is all indepedant of x_0 and depends only on r. So measuring in this basis gives us some information about r. So one can think of QFT as the unitary mapping that rotates χ basis into the standard computational basis. So can define QFT as:

$$QFT|\chi_k\rangle = |k\rangle$$

How do these mysterious shift invariant states look?

1.1.3 Explicit form of shift invariant shapes

$$|\chi_k\rangle = \frac{1}{\sqrt{M}} \sum_{l=0}^{M-1} e^{-2\pi i l \frac{k}{M}} |l\rangle$$

$$U(x_0)|\chi_k\rangle = 1\sqrt{M} \sum_{l=0}^{M-1} e^{-2\pi i l \frac{k}{M}} |l + x_0\rangle = 1\sqrt{M} \sum_{\tilde{l}=0}^{M-1} e^{-2\pi i (\tilde{l} - x_0) \frac{k}{M}} |\tilde{l}\rangle = e^{2\pi i k \frac{x_0}{M}} |\chi_k\rangle$$

giving eigenvalue: $\omega(x_0, k) = e^{2\pi i k \frac{x_0}{M}}$. From this we could reconstruct the basis of QFT:

$$[QFT]_{kl} = \frac{1}{\sqrt{M}} e^{2\pi i \frac{kl}{M}}$$

2 Lecture 3

2.1 Hidden Subgroup Problem

Let G be a finite group of size $|G|$. We are given an oracle $f : G \to X$ with X just some set. We are promised there is a subgroup $K < G$ s.t.

f is constant on (left) cosets of K in G

f is distinct on distinct cosets

Problem: 'Determine' the 'hidden subgroup' K (e.g. output a set of generators or sample uniformly from elements of K)

We want to solve in time $O(poly(\log |G|))$ (efficent algorithm) with anuy consitent probability $1 - \epsilon$. **Examples of problems that can be cast as HSP** Periodicity finding $f : \mathbb{Z}_M \to X$ periodic, period r 1-1 in period

$$G = \mathbb{Z}_M, K = \{0, r, 2r, ..., (A-1)r\} < G$$

Discrete Logarithm Problem: p - prime number, $\mathbb{Z}_p^*$ group of integers with multiplication mod p, $g \in \mathbb{Z}_p^*$ to be a generator (or primitive root mod p). If $\mathbb{Z}_p^* = \{g^0, g^1, ..., g^{r-2}\}$ and we have $g^{p-1} = 1$ (mod p). Fact: These always exist for p is prime. Any $x \in \mathbb{Z}_p^*$ can be written as $x = g^y$ for some $y \in \mathbb{Z}_{p-1}$, $y = \log_g x$ is called the discrete log of x to base g. Discrete log problem is given a generator g, $x \in \mathbb{Z}_p^*$ we want to compute $y = \log_g x$. To express this as the HSP:

$$f : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$$

$$f(a, b) = g^a x^{-b} \mod p = g^{a-yb} \mod p$$

Can check if $f(a_1, b_1) = f(a_2, b_2) \iff (a_1, b_1) = (a_2, b_2) + \lambda(y, 1), \in \mathbb{Z}_{p-1}$:

$$G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$$

$$K = \{\lambda(y, 1) : \lambda \in \mathbb{Z}_{p-1}\} < G$$

Then f is constant and distinct on cosets of K and generator $(y, 1)$ of K gives $y = \log_g x$

Graph Problems:
So we can solve problems like those above where G is abelian, but we can also solve graph problems.

Consdier graph $A = (V, E)$, $|V| = n$ lets say that the graph is undirected and there is at most one edge between any two vertices. Vertices here are labelled by numbers from 1 to n.

Lets define an adjacency matrix M_A: $[M_a]_{ij} = \begin{cases} 1 & \iff (i,j) \\ 0 & \text{otherwise} \end{cases}$. The permuation group of $[n]$, $|P_n| = n!, \log|P_n| \sim O(n \log n)$. Define a group of automorphisms of group A which is a set of permuations with the following property: $\pi \in P_n$ s.t. $\forall i, j (i, j)$ is an edge in $A \iff (\pi(i), \pi(j))$ is also an edge in A.

An associated HSP (the case of non-abelian G):

$$G = P_n, X = \text{set of all labelled graphs on } n \text{vertices}$$

For any $A \in X$, define $f_A : G \to X$, $f_A(\pi) =$"A with vertex labels permuted by π"

$$K = Aut(A)$$

(Check $f(K)$ is constant and disctint on cosets of $Aut(A)$)

Applications:
If we can sample uniformly from K, then we can solve Graph Isomorphism problem (GI).This has a number of different applications in areas of computer science. Two labelled graphs A and B with n vertices are isomorphic if there is a 1-1 map (i.e. permutation) $\pi[n] \to [n]$ s.t. $\forall i, j \in [n](i, j)$ is an edge in $A \iff (\pi(i), \pi(j))$ is an edge in B. The GI problem is given to graphs A and B and deciding if they are isomorphic. This can be represented as a non-abealian HSP. There is no known poly(m) time classical algorithm to solve this problem, so GI is clearly in NP but not believed to be NP-complete (a class of problems such that every problem in NP can be reduced to an NP-complete problem these are the hardest NP problems). In 2017, L Babai presented a quasi-polynomial algorithm for GI runtime $n^O(\log n)^2)$. This ranks in between polynomial runtime and exponential algorithms.

3 Lecture 4

Quantum algorithm for finite abelian HSPs - Generalisation of period-finding algorithm
Write our abelian group $(G, +)$ additively

Construction of shift-invariant states and Fourier transform for G.
Representations of abelian G:
Consdier the mapping $\chi : G \to \mathbb{C}^* = \mathbb{C} - \{0\}$ with multiplication that satisfies:

$$\chi(g_1 + g_2) = \chi(g_1)\chi(g_2), \forall g_1, g_2 \in G$$

χ is a group homomorphism from G to $\mathbb{C}^*$. Such χ's are called irreducible representations of G. They have the following properties: **Theorem 1**:
1) any value $\chi(g)$ is a $|G|$-th root of unity ($\chi \in\to S^1$ the unit circle)
2) Schur's lemma (orthogonality): If χ_i, χ_j satisfy (HOM) then

$$\frac{1}{|G|}\sum_{g\in G} \chi_i(g)\bar{\chi_j}(g) = \delta_{ij}$$

There are always exactly $|G|$ different functions χ satisfying (HOM).

Examples: $\chi(g) = 1, \forall g \in G$ is an irrep/ called a trival irrep
Label the trivial irrep as χ_0, $0 \in G$. Then for any other irrep $\chi \neq \chi_0$ orthonality to χ_0 gives:

$$\sum_{g\in G} \chi(g) = 0 \text{ if } \chi \neq \chi_0$$

Going back to constructing shift-invariant states

3.0.1 Shift-invariant states

Consider a state space $\mathcal{H}_G, dim\mathcal{H}_G = |G|$ wtih basis $\{|g\rangle\}_{g\in G}$. Now introduce shift operators $U(k)$ for $k \in G$ defined as follows:

$$U(k) : |g\rangle \to |g + k\rangle, g, k \in G$$

All shift operators commute so there exists a simultaneous eigenbasis.
For each $\chi_k, k \in G$:

$$|\chi_k\rangle = \frac{1}{\sqrt{|G|}}\sum_{g\in G} \bar{\chi_k}(g) |g\rangle$$

By thereom 1 $\{\chi_k\}$ form an orthonormal basis.

$$U(g) |\chi_k\rangle = \chi_k(g) |\chi_k\rangle$$

Proof:

$$U(g) |\chi_k\rangle = \frac{1}{\sqrt{|G|}}\sum_{h\in G} \bar{\chi_k}(h) |h + g\rangle$$

$$\{h' = h + g\} = \frac{1}{\sqrt{|G|}}\sum_{h'\in G} \bar{\chi_k}(h' - g) |h'\rangle$$

using HOM $\chi_k(-g) = \chi_k(g)^{-1} = \bar{\chi}_k(g) \implies \chi_k(\bar{h'} - g) = \bar{\chi}_k(h')\bar{\chi}_k(-g) = \bar{\chi}_k(h')\chi_k(g)$. Therefore,

$$U(g)\,|\chi_k\rangle = \frac{1}{\sqrt{|G|}} \sum_{h' \in G} \chi_k(g)\bar{\chi}_k(h')\,|h'\rangle = \chi_k(g)\,|\chi_k\rangle$$

So $|\chi_k\rangle$'s form a common eigenbasis

Introduce Fourier transform QFT for a group G
- consider a unitary mapping on $\mathcal{H}_G$ mapping $|\chi_k\rangle$ basis to $|g\rangle$ basis

$$QFT\,|\chi_g\rangle = |g\rangle\,, \forall g \in G$$

$$QFT^{-1}\,|g\rangle = |\chi_g\rangle$$

k-th column of QFT^{-1} in $|g\rangle$ basis is mode of components of $|\chi_k\rangle$:

$$[QFT^{-1}]_{gk} = \frac{1}{\sqrt{|G|}}\bar{\chi_k}(g)$$

Example: $G = \mathbb{Z}_M$L
Check $\chi_a(b) = e^{\frac{2\pi iab}{M}}, a, b \in \mathbb{Z}_M$ satsifies HOM and has its irreps labelled by $a \in \mathbb{Z}_M$ with $\chi_0(b) = 1 \forall b \in \mathbb{Z}_m$.

$$G = \mathbb{Z}_{M_1} \times ... \times \mathbb{Z}_{M_r}$$

$$(a_1, ..., a_r) = g_1, (b_1, ..., b_r) = g_2$$

$$\chi_{g_1}(g_2) = e^{2\pi i(\frac{a_1 b_1}{M_1} + ... + \frac{a_r b_r}{M_r}}$$

This satifies HOM and our $QFT_G = QFT_{M_1} \otimes ... \otimes QFT_{M_r}$ on $\mathcal{H}_G = \mathcal{H}_{M_1} \otimes ... \otimes \mathcal{H}_{M_r}$.

This second example is exhaustive since we have a classification theroem:
Classification theorem: Any fintie abelian group G is isomorphic to a direct product of the form $G = \mathbb{Z}_{M_1} \otimes ... \otimes \mathbb{Z}_{M_r}$. So M_1 can be taken in a form $p_1^{s_1}, ...p_r^{s_r}$.

3.0.2 Quantum algorithm

$$f : G \to X$$

with hidden subgroup K and cosets $k = 0 + k, g_2 + k, ...g_m + k$, $m = \frac{|G|}{|K|}$. we will work on $\mathcal{H}_{|G|} \otimes \mathcal{H}_{|X|}$,$\{|g\rangle\,|x\rangle\}_{g \in G, x \in X}$.

Create a state $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle\,|0\rangle$
$Apply$U$_f$ and $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle\,|f(g)\rangle$

Measure the second register to get $f(g_0)$. The first register will not give the coset state:

$$|g_0 + k\rangle = \frac{1}{\sqrt{|k|}} \sum_{k \in K} |g_0 + k\rangle = U(g_0)\,|K\rangle$$

apply QFT and measure to get a result $g \in G$

4 Lecture 6

We can write $|K\rangle$ in the shift-invariant basis $\{\chi_g\}_{g \in G}$

$$|K\rangle = \sum_g a_g\,|\chi_g\rangle$$

$$|g_0 + K\rangle = U(g_0)\,|K\rangle = \sum_g a_g \chi_g(g_0)\,|\chi_g\rangle$$

as $QFT\,|\chi_g\rangle = |g\rangle$ so after we apply QFT

$$prob(g) = |a_g \chi_g(g_0)|^2 = |a_g|^2, |\chi_g(g_0)| = 1$$

$$QFT\,|K\rangle = \frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|K|}} \sum_{l \in G} (\sum_{k \in K} \chi_l(k)\,|l\rangle)$$

$\sum_{k \in K} \chi_l(k)\,|l\rangle$ involves irreps χ_l of G restricted to subgroup $K < G$, and each such object is itself an irrep in K. Hence we have the following relation:

$$\sum_{k \in K} \chi_l(k) = \begin{cases} |k| & if\,\chi_l \text{ restricts to the trival irrep of K} \\ 0 & \text{otherwise} \end{cases}$$

$$QFT\,|K\rangle = \sqrt{\frac{|K|}{|G|}} \sum_{l \in G} |l\rangle$$

Then a measurement gives a uniformly random choice of l s.t. $\chi_l(k) = 1$.
If k has generators $k_1, ..., k_n$ where $M = O(\log(K)) = O(\log|G|)$. Then the output of a measurement gives us $\chi_l(k) = 1 \forall i$.

It can be shown that if $O(\log(|G|)$ values of l chosen uniformly at random then with probability $> \frac{2}{3}$ they will suffice to determine a generating set for k via the equations $\chi_l(k) = 1$.

Example: $G = \mathbb{Z}_{M_1} \times ... \times \mathbb{Z}_{M_l}$
$l = (l_1, ..., l_q) \in G$, $g = (b_1, ..., b_q) \in G$ gives $\chi_l(g) = e^{2\pi i(\frac{l_1 b_1}{M_1} + ... + \frac{l_q b_q}{M_q}}$
For $k = (k_1, ..., k_q) \in K$ with $\chi_l(k) = 1 \implies \frac{l_1 k_1}{M_1} + ... + \frac{l_q k_q}{M_q} = 0 mod 1$. This is a homogenous linear equation on k and $O(\log(k))$ such equations determine k as null space.

4.0.1 Remarks on HSP for non-abelian groups G

Now we will consider multiplicative shifts. As before we can generate a bunch of coset states but it is curious to investigate what breaks down.

$$|g_0K\rangle = \frac{1}{\sqrt{|K|}} \sum_{k \in K} |g_0k\rangle \,, g_0 \in G \text{ is chosen randomly}$$

The real problem with QFT construction is that there is no good basis of shift invariant states. This is because $U(g_0)$ don't commute.

Construction of non-abelian QFT
Consider a d-dimensional representation of G and a group homomorphism $\chi : G \to U(d)$
χ is irreducible if no subset of $\mathbb{C}^d$ is left invariant by all matrices $\chi(g), g \in G$. (i.e. we cannot simulatenoulsy block-diagonalize all of $\chi(g)$'s by a simple basis change)
Let's define a complete set of irreps. It is a set $\chi_1, ..., \chi_m$ s.t. that any irrep is unitarily equivalent to one of them. e.g. $\chi \sim \chi' = V\chi CV^{-1}, V \in U(d)$
Example: G is abelian , all irreps have $d = 1$, since all $\chi(g)$ commute. Theorem(non-abelian analogue of Theorem 1) (consullt Fulton and Hardes "Representation Theory" fo more information)
If $d_1, ..., d_m$ are the dimensions of a complete set of irreps $\chi_1, ..., \chi_M$ then:
1) $d_1^2 + ... + d_m^2 = |G|$
2) $\chi_{i,jk}(g)$ is (j, k) th matrix entry of $\chi_i(g)$ then by Schur orthogonality:

$$\sum_g \chi_{i,jk}(g)\bar{\chi}_{i',j'k'}(g) = |G|\delta ii'\delta_{jj'}\delta kk'$$

Now if we look at the states that correspond to these irreps $\chi_{i,jk} = \sum_g \in G\bar{\chi}_{i,jk}(g)\,|g\rangle$ they form an orthonormal basis.
QFT on G is defined to be a unitary rotation between two basis of $\{\chi_{i,jk}\}$ basis $\to \{|g\rangle\}_{g\in G}$.
These takes $|\chi_{i,jk}\rangle$ are not shift-invariant for all $U(g_0)$ so this implies that measuring coset state $|g_0k\rangle$ in the $\{|\chi\rangle\}$ basis results in an output distribution that is not independant of g_0.
A "partial" shift-invariance survives. Consider a measuremnt M_{rep} on $|g_0k\rangle$ this measurement will only distinguish the irreps (i values) and not all (i, j, k)'s. the outcome i will be associated with d_i^2 dimensional orthogonal subspaces that are spanned by $\{\chi_{i,jk}\}_{j,k=1}^{d_i}$.
Then $\chi_i(g_1g_2) = \chi_i(g_1)\chi_i(g_2) \implies$ the output distribution of i values is indeed independant of g_0.