1 Fourier Transformations and Simon's Algorithm

1.1 Definitions

We are going to give a fairly general overview on Fourier-Transforms applied to quantum computations.

To do this, we start out with an abelian Group G which for our purposes is finite. Let $*_G$ denote the group operation of G. Then we obtain a complex vector-space V in the following way: Take the elements of G as a basis for V and let $v \in V$ be the formal complex linear combinations of these basis elements, which we denote

$$v = \sum_{g \in G} \alpha_g |g\rangle (\alpha \in C).$$

Clearly the dimension of V is the group order of G ($dimV = |G|$).
We can turn V into an algebra (called the group algebra of G and denoted CG) by defining a multiplication among elements of V:
Multiplication by an element of the basis:

$$(\sum_{g \in G} \alpha_g |g\rangle) * |g'\rangle = \sum_{g \in G} \alpha_g |g *_G g'\rangle$$

extending this linearly in the obvious way.
Let's assume that V has an inner product so that $\{|g\rangle : g \in G\}$ is an orthonormal basis. Then we want to define the **Fourier Transform (FT)** of V as a linear transformation having the following property:

- *FT maps $\{|g\rangle\}$ to an orthonormal basis $\{|\Psi_g\rangle\}$*
- *the new basis is G-invariant, i.e. if*

$$FT : |v\rangle \rightarrow |\Psi_v\rangle = \sum_{g \in G} \beta_g |\Psi_g\rangle$$

$$FT : |v\rangle * |g\rangle \rightarrow |\Psi_{v*g}\rangle = \sum_{g \in G} \beta'_g |\Psi_g\rangle$$

  then $|\beta_g| = |\beta'_g| \; \forall g \in G$ i.e. the probability-distribution on the new basis is invariant under the group-action of G.

Thus we have the following properties of the Fourier-basis $\{|\Psi_g\rangle\}$:

(1) Multiplication of $|v\rangle \in V$ by $|g\rangle$ changes the components of $|v\rangle$ by a factor of magnitude 1 (G-invariance).

(2) A basis-element $|g\rangle$ of V has components of equal magnitude in the Fourier-basis.

(3) We can chose an element of the Fourier-basis - $|\Psi_0\rangle$ - such that every $|g\rangle$ has component exactly $\beta_0 = \frac{1}{\sqrt{|G|}}$ (i.e. via possibly multiplication by a constant phase we can have a direction with phase 1 in the Fourier-basis).

(4) The uniform superposition $(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle)$ is mapped to $|\Psi_0\rangle$, i.e. the other components cancel out.

(5) The identitiy in G, $|e\rangle$ is mapped to $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |\Psi_g\rangle$.

(6) **Behaviour on Cosets** Let $H \leq G$ be a subgroup of G. Let $g'H = \{g' * h : h \in H\}$ be a coset of H. Then the Fourier-Tansformation treats all cosets of H similarly in the sens that the images of **FT** of uniform superpositions on the coset $g'H$ for all cosets of H have components differing only by a phase-factor, i.e. the magnitudes of the components do not depend on the specific coset of H chosen:

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |g' * h\rangle \rightarrow \sum_{g \in G} \alpha_g |\Psi_g\rangle$$

and $|\alpha_g|$ is independent of the choice of g'.

1.2 Example

Let's study the Fourier-Transform in the vector-space of the group $G = Z_n^2 = Z_2 \otimes \cdots \otimes Z_2$. The group-operation $*_G$ is componentwise addition mod 2, which we will denote $+$ here. Let V be the group-vectorspace CG of G, i.e. all complex linear combinations of elements of G. Define an "inner-product" on V in the following way on basis elements $|x\rangle$, $|y\rangle$ of V:

$$|x\rangle \cdot |y\rangle = \sum_{i=1}^{n} x_i \cdot y_i \ (mod\ 2)$$

and extending it linearly. (This is not a "real" inner-product since $x \cdot x = 0$ does not necessarily imply that $x = 0$.) Now define our Fourier-Transform to be the following map of V into V (we have encountered it earlier as the Hadamard-Transformation):

$$|x\rangle \to |\Psi_x\rangle = \frac{1}{2^{n/2}} \sum_{u \in G} (-1)^{u \cdot x} |u\rangle.$$

Claim: This transformation is G-invariant.
Proof: Let's compute it:

$$|v\rangle = (\sum_{x \in G} \alpha_x |x\rangle) \to \frac{1}{2^{n/2}} \sum_{u \in G} (\sum_{x \in G} (-1)^{x \cdot u} \alpha_x)\, |u\rangle \qquad (*)$$

$$|v\rangle * |y\rangle = (\sum_{x \in G} \alpha_x |x\rangle) * |y\rangle = \sum_{x \in G} \alpha_x |x+y\rangle \to \frac{1}{2^{n/2}} \sum_{u \in G} (\sum_{x \in G} (-1)^{(x+y) \cdot u} \alpha_x)\, |u\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{u \in G} (\sum_{x \in G} (-1)^{x \cdot u} (-1)^{y \cdot u} \alpha_x)\, |u\rangle = \frac{1}{2^{n/2}} \sum_{u \in G} (-1)^{y \cdot u} (\sum_{x \in G} (-1)^{x \cdot u} \alpha_x)\, |u\rangle$$

The last expression is equal to the r.h.s. of $(*)$ except for a y-dependent phase. □

1.3 Revisiting Simon's Algorithm

Let's review Simon's algorithm under the aspect of Fourier-Transformations. We look at a slightly modified version where we only have on case, namely where we have as input for Simon's algorithm a reversible circuit C_f computing $f : Z_2^n \to Z_2^n$ such that

- *f is two-to-one and there exists u such that $f(x) = f(x+u)$ for all $x \in Z_2^n$.*

Simon's algorithm finds u. Our group G here is Z_2^n, the subgroup $H = \{0, u\}$ of order $|H| = 2$. The function f is constant on cosets of H.
Now, when we perform the first **FT** (i.e. in this case the Hadamard-Transformation) we get a uniform superposition on the whole group G. Inputting this to the circuit C_f we get a uniform superposition on all the cosets of H, together with our initial uniform superposition on G, namely the total output of C_f will be:

$$\frac{1}{2^{n/2}} \sum_{x \in Z_2^n} |x\rangle \otimes |f(x)\rangle$$

To continue in our analysis we need to define **Fourier-Transformations on tensor products:**
Let $G = H \times K$ be the direct product of two groups H and K. Let $\{|\sigma_h\rangle : h \in H\}$ be the Fourier-basis for H and $\{|\tau_k\rangle : k \in K\}$ be the Fourier-basis for K.
Claim: $\{|\sigma_h\rangle \otimes |\tau_k\rangle : h \in H, k \in K\}$ is a Fourier-basis for G.
Proof: We only have to show G-invariance: But multiplication of an element of $H \times K$ by an element (h', k') amounts to first multiplying by (h', e) (e_K being the identity in K), which changes the components in the Fourier-basis by a factor of magnitude 1 and after that multiplying by (e_H, k') which again changes the components by a factor of magnitude one. $\square$

Let's apply this to Fourier-transform a uniform H-superposition tensored with an element of K (without loss of generality let this be e_K, the identity in K):

$$\frac{1}{\sqrt{|H|}} \sum_{h \in h} (h, e) \quad \to \quad \frac{1}{\sqrt{|K|}} \sum_{k \in K} |\sigma_0\rangle \otimes |\tau_k\rangle.$$

Identifying the basis elements $|\tau_k\rangle$ with elements in K, which is possible in the case of the group $G = Z_2^n$, we see, that the **FT** maps a uniform superposition on a subgroup H to a uniform superposition on the other subgroup K.
More specifically let H be a normal subgroup and K be the quotient-group G/H. Then we have $G = H \times G/H$ and the **FT** maps a uniform H-superposition to a uniform G/H-superposition!
Returning to Simon's algorithm this means that the last **FT** (Hadamard-Transformation) - after safe-storage of $|f(x)\rangle$ - gives us a uniform superposition on the subgroup $K = G/H = Z_2^n/\{0, u\}$. But all elements $|y\rangle$ of K then have the property that $y \cdot u = 0$ which we use to determine u, performing the algorithm several times.

1.4 Generalisation of Simon's Algorithm - Fourier-Transformations on Z_q

We can generalise Simon's algorithm to the group Z_q and problems where we are given as input for Simon's algorithm a reversible circuit C_f computing $f : Z_q \to Z_q$ such that

- *f is k-to-one and there exists a cyclic subgroup $H \leq G$ of order $|H| = k$ generated by an element $u \in G$ such that f is constant on cosets of H.*

We want Simon's algorithm to find a generator u of H.
To study this problem we need to find out what the Fourier-basis of $G = Z_q$ looks like.
The group operation on our cyclic group $G = Z_q$ is addition modulo q, denoted by $+$ here. Let $\{|a\rangle : a = 0 \ldots q-1\}$ be the basis for the group-vectorspace CG. Define $\omega = e^{2\pi i/q}$ to be the $q-th$ primitive root of unity. Then we have the following **identities for** ω:

$$1 + \omega + \omega^2 + \cdots + \omega^{q-1} = 0$$
$$1 + \omega^j + \omega^{2j} + \cdots + \omega^{(q-1)j} = 0 \quad if \quad j \not\equiv 0 \pmod q$$
$$1 + \omega^j + \omega^{2j} + \cdots + \omega^{(q-1)j} = q \quad if \quad j \equiv 0 \pmod q$$

stemming from the fact that ω is a root of $\frac{X^q-1}{X-1} = X^{q-1}+X^{q-2}+\cdots+X+1$.
Claim: A Fourier-basis for $G = Z_q$ is given by

$$\{|\Psi_k\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \omega^{k*a} |a\rangle : k = 0 \ldots q-1\}$$

and the Fourier-Transformation maps $|k\rangle \to |\Psi_k\rangle$.
Proof: We only have to show G-invariance, it is sufficient to see this on the basis elements and then to extend linearly.

$$|k\rangle * |k'\rangle = |k+k'\rangle \quad \to \quad |\Psi_{k+k'}\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \omega^{(k+k')*a} |a\rangle$$

$$= \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \omega^{k'*a} \omega^{k*a} |a\rangle.$$

But $|\omega^{k'*a}| = 1$ so this has the same amplitudes as $|\Psi_k\rangle$. $\square$
The basis element $|0\rangle$ then gets mapped by FT to $|\Psi_0\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle$, i.e. to the uniform superposition over all basis elements of our vector-space CG.

To implement the generalised Simon's algorithm now we use the same circuit as before replacing the Hadamard parts of the circuit by Fourier-Transformation circuits. (We assume that the basis elements $|a\rangle$ are represented in binary.)

Thus the input to C_f is a uniform superposition of all elements of G. After measuring $|f(x)\rangle$ (or - equivalently - safe-storing it) the input to the last **FT** circuit is a uniform superposition of the k elements of a coset $v + H$

of $H = \{1, u, 2u, \ldots, (k-1)u\}$ (all the $|x\rangle$ which got mapped to this actual $f(x)$), i.e.:

$$\frac{1}{\sqrt{k}} \sum_{m=0}^{k-1} |a * u + v\rangle \quad \rightarrow \quad \frac{1}{\sqrt{k}} \sum_{m=0}^{k-1} (\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} \omega^{(mu+v)*a} |a\rangle)$$

$$= \frac{1}{\sqrt{kq}} \sum_{a=0}^{q-1} \omega^{v*a} (\sum_{m=0}^{k-1} \omega^{m*u*a}) |a\rangle.$$

Now the inner sum is $(\sum_{m=0}^{k-1} \omega^{m*u*a}) = (\sum_{m=0}^{k-1} \omega'^{m*a})$ where $\omega' = \omega^u$ is a $\frac{q}{u} - th$ primitive root of unity. Using the second of our identities established above this sum is 0 whenever $a \not\equiv 0 \ (mod \ \frac{q}{u})$ and is equal to $\frac{q}{u}$ whenever $a \equiv \frac{q}{u}$. So the output of **FT** becomes:

$$\frac{1}{\sqrt{kq}} \sum_{r=0}^{\frac{q}{k}-1} (\frac{q}{u} \, |r * \frac{q}{u}\rangle = \sqrt{\frac{q}{k}} \sum_{r=0}^{\frac{q}{k}-1} (\frac{q}{u}) \, |r * \frac{q}{u}\rangle.$$

Measuring now gives $|r * \frac{q}{u}\rangle$ for a random r between 0 and $\frac{q}{k} - 1$. Repeating the whole process of the generalised Simon's algorithm and taking $g.c.d.'s$ of the results gives $\frac{q}{u}$ with very high probability and thus u can be determined efficiently.

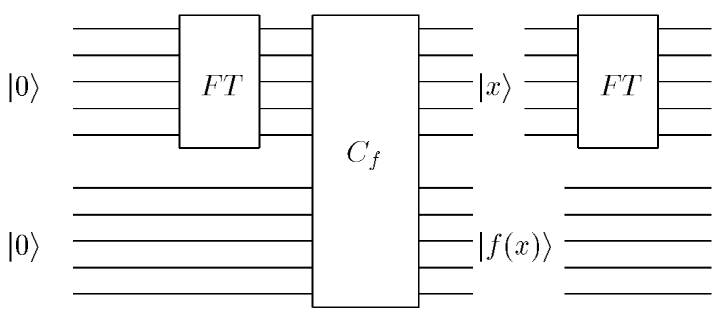

Figure 1: Generalised Simon's circuit