Quantum Computation **(CMU 18-859BB, Fall 2015)**

Lecture 6: Boolean Fourier Analysis and Simon's Algorithm

September 28, 2015

Lecturer: John Wright *Scribe: Vikesh Siddhu*

1 Short Summary

Today we will cover the Fourier transform over $\mathbb{Z}_2^n$. Fourier transformation can be viewed as a change of basis transformation. Functions expressed in this basis can make certain patterns in a function more evident. In quantum computing, we frequently perform a Fourier transform. Given its ability to reveal some pattern in the function, it's in some sense at the heart of various quantum algorithms and we will specifically see its role in Deutsch-Josza algorithm [DJ92], Grover's algorithm [Gro96] and Simon's Problem [Sim94].

2 Fourier Transform over $\mathbb{Z}_2^n$

We will show that a Fourier Transform essentially

- Is a change of basis
- Makes it easy to find certain patterns in the function
- In quantum computing parlance it can be computed using $H^{\otimes n}$.

Consider a set of functions $\{\delta_y(x)\}_{y\in\{0,1\}^n}$ with the property that

$$\delta_y(x) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{else} \end{cases}$$

This set of functions constitute a basis for any function $g(x) : \{0,1\}^n \mapsto \mathbb{C}$ (for example $g(x) = (-1)^{f(x)}$ where $f : \{0,1\}^n \mapsto \{0,1\}$), in the sense that we can expand any $g(x)$ as follows

$$g(x) = \sum_{y\in\{0,1\}^n} g(y)\delta_y(x) \tag{1}$$

quite generally the coefficients of $\delta_y(x)$ are called expansion coefficients, in the case at hand they take the value $g(y)$ (the actual value of the function at y). The representation of the function $g(x)$ in equation (1) is called the *standard* representation.

We may represent the function $g(x)$ as a column vector with 2^n rows, such that the $(i,1)^{\text{th}}$ entry $i \in \{0,1\}^n$ is $g(i)$ i.e.

$$g \equiv \begin{bmatrix} g(0^n) \\ g(0^{n-1}1) \\ . \\ . \\ . \\ . \\ g(1^n) \end{bmatrix}$$

In this representation δ_y is the column vector with 0's everywhere except the y^{th} position where we have a 1.

By expressing a function in the standard basis we may not be able to observe certain patterns as efficiently as we would like. For e.g. in the Deutsch-Josza problem, classical algorithms sample the function in the standard basis and we need $\frac{n}{2}+1$ samplings before we can decide whether the function is balanced or all-zero.

2.1 Fourier/Parity basis

2.1.1 Definitions

Let $\sigma, X \in \mathbb{F}_2^n$ then

$$\begin{aligned} \sigma.X &\equiv \sum_{i=1}^{n} \sigma_i X_i && (2) \\ &= \bigoplus_{i:\sigma_i=1} X_i && (3) \end{aligned}$$

where $\bigoplus$ is additional mod 2. Equation (3) allows us to interpret $\sigma.X$ as the parity of the bits in X where $\sigma_i = 1$ i.e. the parity of a subset of the entries in X. We may also consider the ± version of the parity function.

$$\begin{aligned} (-1)^{\sigma.X} &= \begin{cases} 1 & \text{if } \sigma.X = 0 \\ -1 & \text{if } \sigma.X = 1 \end{cases} && (4) \\ &= \prod_{i:\sigma_i=1} (-1)^{X_i} && (5) \\ &\equiv \chi_\sigma(X) && (6) \end{aligned}$$

Where the final equality introduced the $\chi_\sigma(X)$ function which is called the *Fourier characteristic.*

Example 2.1. $\sigma = 0^n \equiv \mathbf{0}$ *then* $\sigma.X = \mathbf{0}.X = 0$ *which gives*

$$\chi_{\mathbf{0}}(X) = (-1)^{\sigma.X} = (-1)^0 = 1$$

We define the Fourier basis as $\{\chi_\sigma\}_{\sigma \in \mathbb{F}_2^n}$ whose elements may be represented as column vectors

$$\chi_\sigma = \begin{bmatrix} \chi_\sigma(0^n) \\ \chi_\sigma(0^{n-1}1) \\ . \\ . \\ . \\ . \\ \chi_\sigma(1^n) \end{bmatrix}$$

2.1.2 Properties

In order to show $\{\chi_\sigma\}_{\sigma \in \mathbb{F}_2^n}$ is a basis we show

(i) χ_σ are orthogonal

(ii) χ_σ are 2^n in number

The second condition follows from the definition of our set of functions. The first can be restated as follows

$$\sum_{X \in \{0,1\}^n} \chi_\sigma(X)\chi_\gamma(X) = \begin{cases} 0 & \text{if } \sigma \neq \gamma \\ 2^n & \text{if } \sigma = \gamma \end{cases}$$

alternatively

$$\frac{1}{2^n} \sum_{X \in \{0,1\}^n} \chi_\sigma(X)\chi_\gamma(X) = \begin{cases} 0 & \text{if } \sigma \neq \gamma \\ 1 & \text{if } \sigma = \gamma \end{cases} \tag{7}$$

We can also write the lhs in equation (7) as $\mathbb{E}_X[\chi_\sigma(X)\chi_\gamma(X)]$ where $X \in$ uniform $\{0,1\}^n$. Finally the condition (i) can be restated as follows.

$$\underset{X \in \text{uniform } \{0,1\}^n}{\mathbb{E}_X}[\chi_\sigma(X)\chi_\gamma(X)] = \begin{cases} 0 & \text{if } \sigma \neq \gamma \\ 1 & \text{if } \sigma = \gamma \end{cases} \tag{8}$$

Before we show equation (8) we compute $\underset{X \in \text{uniform } \{0,1\}^n}{\mathbb{E}_X}[\chi_\sigma(X)]$,

(i) Case 1: Assume $\sigma \neq \mathbf{0}$ then

$$\begin{aligned} \underset{X \in \text{uniform } \{0,1\}^n}{\mathbb{E}_X}[\chi_\sigma(X)] &= \underset{X \in \text{uniform } \{0,1\}^n}{\mathbb{E}_X}[(-1)^{\sigma.X}] && (9) \\ &= \underset{X \in \text{uniform } \{0,1\}^n}{\mathbb{E}_X}[\prod_{i:\sigma_i=1}(-1)^{X_i}] && (10) \\ &= \prod_{i:\sigma_i=1} \underset{X \in \text{uniform } \{0,1\}^n}{\mathbb{E}_X}[(-1)^{X_i}] && (11) \\ &= \prod_{i:\sigma_i=1} \frac{1}{2}[(-1)^1 + 1^0] && (12) \\ &= 0 && (13) \end{aligned}$$

The first and second equality follow from the definition, the third follows from the fact the all X_i's are from a *i.i.d* source, the fourth come from taking the expectation over uniform random $X_i \in \{0,1\}$, the final one from basic algebra.

(ii) Case 2: $\sigma = \mathbf{0}$ then it is easy to see

$$\mathop{\mathbb{E}_X}_{X \in \text{uniform } \{0,1\}^n}[\chi_\sigma(X)] = \mathop{\mathbb{E}_X}_{X \in \text{uniform } \{0,1\}^n}[(-1)^{\mathbf{0}.X}] = \mathop{\mathbb{E}_X}_{X \in \text{uniform } \{0,1\}^n}[(-1)^0] = 1$$

hence

$$\mathop{\mathbb{E}_X}_{X \in \text{uniform } \{0,1\}^n}[\chi_\sigma(X)] = \begin{cases} 1 & \text{if } \sigma = 0 \\ 0 & \text{else} \end{cases} \tag{14}$$

We now compute $\mathop{\mathbb{E}_X}_{X \in \text{uniform } \{0,1\}^n}[\chi_\sigma(X)\chi_\gamma(X)]$ which is given by

$$\begin{aligned} \mathop{\mathbb{E}_X}_{X \in \text{uniform } \{0,1\}^n}[\chi_\sigma(X)\chi_\gamma(X)] &= \mathop{\mathbb{E}_X}_{X \in \text{uniform } \{0,1\}^n}[\prod_{i:\sigma_i=1}(-1)^{X_i}\prod_{i:\gamma_i=1}(-1)^{X_i}] && (15) \\ &= \mathop{\mathbb{E}_X}_{X \in \text{uniform } \{0,1\}^n}[\prod_{i:\sigma_i \oplus \gamma_i = 1}(-1)^{X_i}] && (16) \\ &= \mathop{\mathbb{E}_X}_{X \in \text{uniform } \{0,1\}^n}[\chi_{\sigma\oplus\gamma}(X)] && (17) \\ &= \begin{cases} 1 & \text{if } \sigma \oplus \gamma = 0 \\ 0 & \text{else} \end{cases} && (18) \end{aligned}$$

Here $\oplus$ refers to the entrywise XOR. The first equality follows from definition, the second can be obtained by a direct calculation or by studying simple examples like $\sigma = 0101\ldots$ and $\gamma = 0011\ldots$ and observing the pattern, the final equality follows from equation (14). $\sigma \oplus \gamma = 0$ implies $\sigma = \gamma$ this gives the desired result of equation (8). Consequently we have verified conditions (i) and (ii)

2.2 Change of Basis view

We can represent any function $g(X) : \{0,1\}^n \mapsto \mathbb{C}$ in the Fourier basis i.e. we may write

$$g(X) = \sum_{\gamma \in \mathbb{F}_n^2} \hat{g}(\gamma)\chi_\gamma(X) \tag{19}$$

where

Claim 2.2.

$$\hat{g}(\sigma) = \mathop{\mathbb{E}_X}_{X \in \mathit{uniform}\ \{0,1\}^n}[\chi_\sigma(X)g(X)] \tag{20}$$

Proof.

$$\begin{aligned}
\mathbb{E}_X[\chi_\sigma g(X)] &= \mathbb{E}_X[\sum_{\gamma\in\mathbb{F}_n^2} \hat{g}(\gamma)\chi_\sigma(X)\chi_\gamma(X)] && (21)\\
&= \sum_{\gamma\in\mathbb{F}_n^2} \hat{g}(\gamma)\mathbb{E}_X[\chi_\sigma(X)\chi_\gamma(X)] && (22)\\
&= \hat{g}(\sigma) && (23)
\end{aligned}$$

where the final equality follows from equation (8). □

Let us see a few examples

Example 2.3. *What is $\hat{g}(\mathbf{0})$?*

$$\hat{g}(\mathbf{0}) = \mathbb{E}_X[\chi_{\mathbf{0}}(X)g(x)] = \mathbb{E}_X[1.g(x)] = \mathbb{E}_X[g(x)] \tag{24}$$

Example 2.4. *Let $g(X) = (-1)^{f(X)}$ where $f(X) = \sigma.X$, then what is the Fourier representation of $g(X)$.*

$$\begin{aligned}
g(X) &= (-1)^{\sigma.X} && (25)\\
&= 1.\chi_\sigma(X) + \sum_{\gamma\neq\sigma} 0.\chi_\gamma(X) && (26)
\end{aligned}$$

which gives

$$\hat{g}(\gamma) = \begin{cases} 1 & \mathit{if}\, \gamma = \sigma \\ 0 & \mathit{else} \end{cases} \tag{27}$$

If $f(X) \approx \sigma.X$ with probability $1-\epsilon$ where ϵ is a small positive number then

$$\hat{g}(\gamma) = \mathop{\mathbb{E}_X}_{X\in uniform\,\{0,1\}^n}[\chi_\sigma(X)(-1)^{f(x)}] \approx 1-\epsilon$$

2.3 Implementation with Hadamard

In quantum circuits the Fourier transform of a set of qubits is implemented by a Hadamard transformation on the set. Specifically

Claim 2.5. *For $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_X g(X)\,|X\rangle$ where $N \equiv 2^n$*

$$H^{\otimes n}\,|\psi\rangle = \sum_\gamma \hat{g}(\gamma)\,|\gamma\rangle \tag{28}$$

Proof.

$$H^{\otimes n}|\psi\rangle = \frac{1}{\sqrt{N}}\sum_X g(X)H^{\otimes n}|X\rangle \tag{29}$$

What is the coefficient of $|\gamma\rangle = |\gamma_1\gamma_2\dots\gamma_n\rangle$ in equation (29)? We may write

$$H^{\otimes n}|011\dots\rangle = (\frac{|0\rangle+|1\rangle}{\sqrt{2}})\otimes(\frac{|0\rangle-|1\rangle}{\sqrt{2}})\otimes(\frac{|0\rangle-|1\rangle}{\sqrt{2}})\dots$$

The coefficient of $|000\dots0\rangle$ is $\frac{(-1)^0}{2^{n/2}}$, the coefficient of $|010\dots0\rangle$ is $\frac{(-1)^{0+1+0\dots}}{2^{n/2}}$, the coefficient of $|110\dots0\rangle$ is $\frac{(-1)^{0+1+0\dots}}{2^{n/2}}$. In general the coefficient of $|\gamma_1\gamma_2\dots\gamma_n\rangle$ is accumulated as follows, for each $\gamma_i = 0$ we get $(-1)^0$, for each $\gamma_i = 1$ we get a $(-1)^{X_i}$, the general coefficient of $|\gamma_1\gamma_2\dots\gamma_n\rangle$ is a product of the accumulated coefficients which can be written as

$$= \frac{1}{2^{n/2}}(-1)^{\bigoplus_{i:\gamma_i=1}X_i} \tag{30}$$

$$= \frac{1}{2^{n/2}}(-1)^{\gamma.X} \tag{31}$$

continuing the calculation from equation (29) we may write

$$H^{\otimes n}|\psi\rangle = \frac{1}{\sqrt{N}}\sum_X g(X)\sum_\gamma \frac{1}{\sqrt{N}}(-1)^{\gamma.X}|\gamma\rangle \tag{32}$$

$$= \sum_\gamma \frac{1}{N}\sum_X g(X)(-1)^{\gamma.X}|\gamma\rangle \tag{33}$$

$$= \sum_\gamma \underset{X\in\text{uniform }\{0,1\}^n}{\mathbb{E}_X}[g(X)\chi_\gamma]|\gamma\rangle \tag{34}$$

$$= \sum_\gamma \hat{g}(\gamma)|\gamma\rangle \tag{35}$$

□

It is worth noting that $H.H = \mathbb{I}$ and hence $H^{\otimes n}H^{\otimes n} = \mathbb{I}_n$. An immediate consequence of this is for $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_X g(X)|X\rangle$ we my write

$$|\psi\rangle = H^{\otimes n}H^{\otimes n}|\psi\rangle \tag{36}$$

$$|\psi\rangle = H^{\otimes n}[H^{\otimes n}\frac{1}{\sqrt{N}}\sum_X g(X)|X\rangle] \tag{37}$$

$$|\psi\rangle = H^{\otimes n}\sum_\gamma \hat{g}(\gamma)|\gamma\rangle \tag{38}$$

The final equality implies that we can invert the Fourier transform by simply acting $H^{\otimes n}$.

2.4 Use in Quantum Algorithms

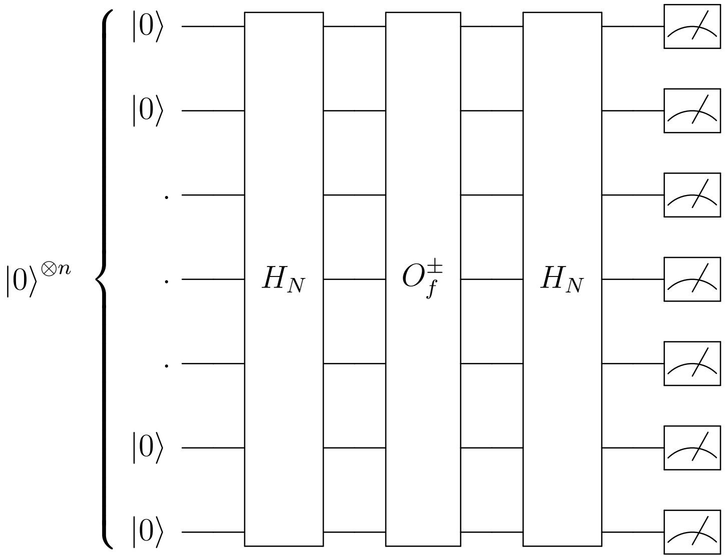
2.4.1 Deutsch-Josza algorithm

In this problem we are given a function $f : \{0,1\}^n \mapsto \{0,1\}$ with the promise that

1. Either f is always 0

2. Or f is balanced (0 and 1 with equal probability)

The goal is to find which of the two is true. The Deutsch-Josza algorithm proceeds by applying the following circuit.



Where $H_N \equiv H^{\otimes n}$ where $N = 2^n$, the $O_f^{\pm}$ is the ± version of the oracle for the function f. After the measurement, if we get $|0\rangle^n$ we say condition (1) is true, else we say condition (2) is true.

One way to see why this procedure is essentially extracting information about the pattern in the function f as revealed by the Fourier transform is as follows. Set

$$g(X) = (-1)^{f(X)}$$

then the above circuit produces the Fourier transform of $g(X)$, observe

$$\begin{aligned}
|0\rangle^{\otimes n} \xrightarrow{H_N} \frac{1}{\sqrt{N}} \sum_{X \in \{0,1\}^n} |X\rangle \xrightarrow{O_f^{\pm}} \frac{1}{\sqrt{N}} \sum_{X \in \{0,1\}^n} (-1)^{f(X)} |X\rangle \\
= \frac{1}{\sqrt{N}} \sum_{X \in \{0,1\}^n} g(X) |X\rangle \xrightarrow{H_N} \sum_{\gamma} \hat{g}(\gamma) |\gamma\rangle
\end{aligned}$$

hence the output is the Fourier transform of the function $g(X)$. We notice that

$$\begin{aligned}\hat{g}(\mathbf{0}) &= \mathbb{E}_X[g(X)] = \mathbb{E}_X[(-1)^{f(X)}] \\ &= \begin{cases} 1 & \text{if condition 1 is true} \\ 0 & \text{if condition 2 is true} \end{cases}\end{aligned}$$

Hence the probability of the outcome $|0\rangle^{\otimes n}$ which is $|\hat{g}(\mathbf{0})|^2$ essentially tells us which of the conditions 1 or 2 is true.

2.4.2 Grover's Algorithm

One key component of the Grover's algorithm is the diffusion operator (D) whose action on a state $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_X g(X) |X\rangle$ is given by

$$D|\psi\rangle = \frac{1}{\sqrt{N}} \sum_X (2\mu - g(X)) |X\rangle \tag{39}$$

where $\mu = \mathbb{E}_X[g(X)]$. The circuit that does the job is easy to see once we do the Fourier analysis,

$$\begin{aligned} g(X) &= \sum_\gamma \hat{g}(\gamma)\chi_\gamma(X) && (40) \\ &= \hat{g}(\mathbf{0})\chi_{\mathbf{0}}(X) + \sum_{\gamma \neq \mathbf{0}} \hat{g}(\gamma)\chi_\gamma(X) && (41) \\ &= \mathop{\mathbb{E}_X}_{X \in \text{uniform } \{0,1\}^n} [g(X)]\chi_{\mathbf{0}}(X) + \sum_{\gamma \neq \mathbf{0}} \hat{g}(\gamma)\chi_\gamma(X) && (42) \\ & && (43) \end{aligned}$$

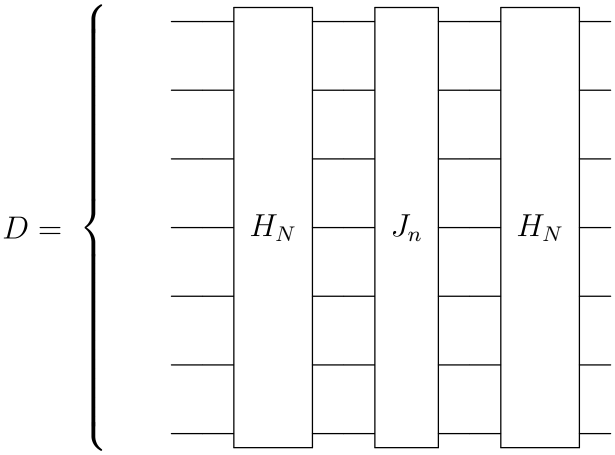
We can define a function $g'(X)$ such that

$$\begin{aligned} g'(X) &\equiv \mathop{\mathbb{E}_X}_{X \in \text{uniform } \{0,1\}^n} [g(X)]\chi_{\mathbf{0}}(X) - \sum_{\gamma \neq \mathbf{0}} \hat{g}(\gamma)\chi_\gamma(X) && (44) \\ &= \mu\chi_{\mathbf{0}}(X) - (g(X) - \mu\chi_{\mathbf{0}}(X)) && (45) \\ &= 2\mu\chi_{\mathbf{0}}(X) - g(X) && (46) \end{aligned}$$

We wish to replace $g(X)$ with $g'(X)$. Which can be done by taking an input and going to the Fourier basis, then putting a $-$ sign in front of all states that are not $\mathbf{0}$ and then returning from the Fourier basis. If we define

$$J_n |x\rangle = \begin{cases} |x\rangle & \text{if } x = \mathbf{0} \\ -|x\rangle & \text{else} \end{cases} \tag{47}$$

The the circuit that does the job can be written as follows.

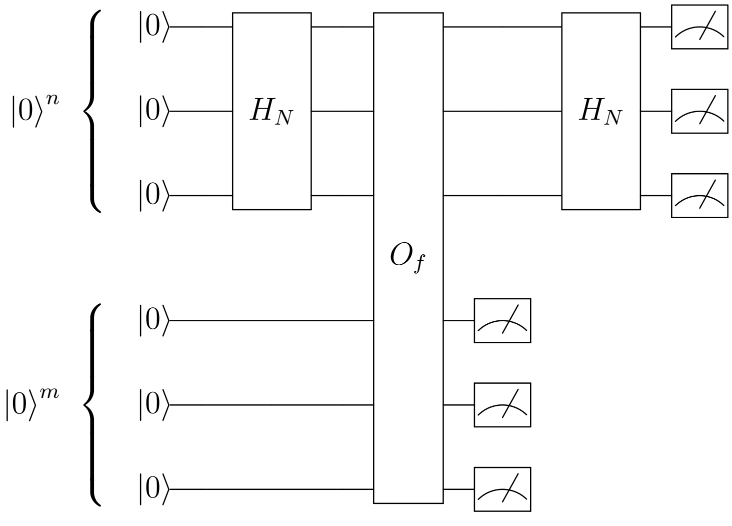


2.4.3 Simon's Problem

Simon's Problem is the precursor to the period finding algorithm which is a precursor to Shor's factorization. It utilizes quantum Fourier transform in a non-trivial way. The problem can be described as follows

- **Given**: $f : \{0,1\}^n \mapsto \{0,1\}^n$
- **Promise**:
  - (i) f is 2 to 1
  - (ii) $f(X) = f(X \otimes s)$ for some $s \in \{0,1\}^n$ and $s \neq \mathbf{0}$
- **Goal**: Find s

From last lecture, we note that classically this would take $O(\sqrt{N})$ queries and the quantum version takes $O(\log N)$ queries. We now proceed to explain the quantum circuit that does the job. Consider the circuit given below, $n+m$ wires come in (only 3 are shown schematically),



Here O_f is the oracle that acts such that

$$sO_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$$

The state in the circuit changes as follows

$$|0\rangle^n |0\rangle^m \xrightarrow{H_N} \frac{1}{\sqrt{N}} \sum_x |x\rangle |0\rangle^m \xrightarrow{O_f} \frac{1}{\sqrt{N}} \sum_x |x\rangle |f(x)\rangle \tag{48}$$

Once we perform the measurement on the lower m qubits we get some value y. The conditional quantum state of the first n qubits is

$$|\psi\rangle_y = \frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle) \tag{49}$$

where $y = f(x)$. Then by applying the final Hadamard gates we get

$$\begin{aligned} H_N |\psi\rangle_y &= \frac{1}{\sqrt{2N}}(\sum_{\gamma\in\{0,1\}^n} (-1)^{\gamma.x} |\gamma\rangle + \sum_{\gamma\in\{0,1\}^n} (-1)^{\gamma.(x\oplus s)} |\gamma\rangle) && (50)\\ &= \frac{1}{\sqrt{2N}} \sum_{\gamma\in\{0,1\}^n} (-1)^{\gamma.x}[1 + (-1)^{\gamma.s}] |\gamma\rangle && (51)\\ &= \frac{1}{\sqrt{2N}} \sum_{\gamma\in\{0,1\}^n} |\gamma\rangle \begin{cases} 2(-1)^{\gamma.s} & \text{if } \gamma.s = 0 \\ 0 & \text{if } \gamma.s = 1 \end{cases} && (52)\\ &= \sqrt{\frac{2}{N}} \sum_{\gamma\in\{0,1\}^n, \gamma.s=0} (-1)^{\gamma.s} |\gamma\rangle && (53) \end{aligned}$$

The final measurement gives a uniformly random γ_i such that $\gamma_i.s = 0$. By doing a large enough number of runs of the circuit i.e. by getting many different γ_i's we may recover s. But how many γ_i's do we need? $n - 1$ linearly independent ones, here's why.

After $n - 1$ runs we'll get γ_i's which satisfy

$$\begin{aligned} \gamma_1.s &= 0 \\ \gamma_2.s &= 0 \\ &\dots \\ \gamma_n.s &= 0 \end{aligned} \tag{54}$$

We make two claims

(i) If the γ_i's are linearly independent, then this system of linear equations fully determines s

(ii) With constant probability, running the Simon circuit will output $n - 1$ linearly independent γ_i's

The above two claims imply, that we have a constant probability of success, which as we have seen, is good enough.

We prove claim (i) by noticing that each linearly independent γ_i cuts down the number of possibilities for s by half. So after $n-1$ equations, there are $2^{n-1}/2^n = 2$ possibilities for s, one of whom is $\mathbf{0}$ which is ruled out assuming that s is non-trivial, hence s is given by the other possibility.

To show (ii), let's first consider the subspace of $\mathbb{F}_2^n$

$$s^{\perp} := \{\gamma | \gamma.s = 0\}$$

This subspace has dimension $n-1$ since it is defined by a single linear equality, and thus the subspace contains 2^{n-1} distinct vectors.

The easiest way to prove (ii) is to show that γ_2 is linearly independent from γ_1 with high probability, then showing that γ_3 is linearly independent from γ_1,γ_2 with high probability, and so forth. So, let's suppose that $\gamma_1, \ldots \gamma_k$ are linearly independent. Then what's the probability that γ_{k+1} is linearly independent from them? i.e.:

$$\begin{aligned}\mathbf{Pr}[\gamma_1, \ldots \gamma_{k+1}\text{are linearly independent}] &= 1 - \mathbf{Pr}[\gamma_{k+1}\text{is in the span of}\gamma_1, \ldots \gamma_k] \\ &= 1 - \frac{2^k}{2^{n-1}}\end{aligned}$$

The last line follows because there are 2^{n-1} possibilities in $s^{\perp}$ for γ_{k+1}, and 2^k of them are in the span of $\gamma_1, \ldots, \gamma_k$. Now, the probability that $\gamma_1, \ldots, \gamma_{n-1}$ are all linearly independent is what we get when we multiply the quantities we just got here for $k = 0, \ldots, n-2$ (the $k = 0$ case gives the probability that γ_1 is not $\mathbf{0}$), i.e.

$$\left(1 - \frac{1}{2^{n-1}}\right)\left(1 - \frac{1}{2^{n-2}}\right) \ldots \left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{2}\right) = \prod_{i=1}^{n-1}\left(1 - \frac{1}{2^i}\right) \tag{55}$$

To analyze this product, we note that $(1-a)(1-b) \geq (1-(a+b))$ when $a, b \in [0,1]$. Applying this inequality to every term but the $(1 - \frac{1}{2})$ term, we get

$$\prod_{i=1}^{n-1}\left(1 - \frac{1}{2^i}\right) \geq \left(1 - \left(\frac{1}{2^{n-1}} + \frac{1}{2^{n-2}} \cdots \frac{1}{2^2}\right)\right) . \frac{1}{2} \geq \frac{1}{4} \tag{56}$$

Thus, Simon's algorithm succeeds with probability at least $\frac{1}{4}$, and this probability can be improved via repetition.

References

[DJ92] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 439(1907):553–558, 1992.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. ACM.

[Sim94] Daniel R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26:116–123, 1994.