The Quantum Fourier Transform and a Comparison with the Fast Fourier Transform

Peter Young

(Dated: November 2, 2019)

I. INTRODUCTION

This handout introduces the quantum Fourier transform (QFT), which is at the heart of Shor's algorithm for period finding, and hence for factoring. The appendices make a detailed comparison with the (classical) Fast Fourier Transform(FFT). The FFT is not part of the course so if you are not interested in this comparison you can ignore the appendices.

II. QUANTUM FOURIER TRANSFORM (QFT) FOR $N = 4$

In this section we describe a simple example, that of $N = 4$ states, i.e. $n = 2$ qubits.

Firstly, a reminder about notation. A state of n qubits is labeled either by a single n-bit integer, x say, or by the values of the individual qubits x_i, which form the binary representation of x. As an example, the four computational basis states for two qubits are

$$\begin{aligned} |0\rangle_2 &\equiv |00\rangle\,, \\ |1\rangle_2 &\equiv |01\rangle\,, \\ |2\rangle_2 &\equiv |10\rangle\,, \\ |3\rangle_2 &\equiv |11\rangle\,, \end{aligned} \tag{1}$$

To prevent any ambiguity, we will, when necessary, indicate the number of qubits in a state by a subscript, e.g. $|x\rangle_n$ has n qubits so x will be an n-bit integer, whose bits indicate the state of the individual qubits.

We now describe the Quantum Fourier Transform (QFT) for $n = 2$ qubits.

In the Quantum Fourier Transform (QFT) one starts from an initial state $|x\rangle_2 \equiv |x_1 x_0\rangle$ in the computational basis and generates the following superposition

$$|\psi_x\rangle_2 = \frac{1}{2}\sum_{y=0}^{3} \exp\left[2\pi i x y/2^2\right]\ |y\rangle_2, \tag{2}$$

where $|y\rangle_2 \equiv |y_1 y_0\rangle$. Note this has the same structure as a standard Fourier Transform, but here we are performing a change of basis of a quantum system, rather than transforming a set of data. The

$|\psi_x\rangle_2$ form a basis just as the $|x\rangle_2$ form a basis because one can show that they are orthonormal, i.e.

$$ {}_2\langle\psi_{x_1}|\psi_{x_2}\rangle_2 = \delta_{x_1,x_2}\,. \tag{3}$$

Noting that $y = y_0 + 2y_1$ and $x = x_0 + 2x_1$ we can simplify the argument of the exponential:

$$\frac{2\pi i x y}{2^2} = \frac{2\pi i (x_0 + 2x_1)(y_0 + 2y_1)}{2^2} = 2\pi i \left\{ y_0 \left(\frac{x_0}{4} + \frac{x_1}{2} \right) + y_1 \left(\frac{x_0}{2} + x_1 \right) \right\}. \tag{4}$$

Now $\exp(2\pi i y_1 x_1) = 1$ so the factor $y_1 x_1$ above can be neglected. Hence Eq. (2) becomes

$$|\psi_x\rangle_2 = \left(\frac{1}{\sqrt{2}} \sum_{y_0=0}^{1} \exp\left[2\pi i y_0 \left(\frac{x_0}{4} + \frac{x_1}{2} \right) \right] \right) \left(\frac{1}{\sqrt{2}} \sum_{y_1=0}^{1} \exp\left[2\pi i y_1 \frac{x_0}{2} \right] \right) |y_1 y_0\rangle. \tag{5}$$

Next we will explain how to perform the operations in Eq. (5) using quantum gates.

Consider the second factor on the RHS of Eq. (5), which involves a sum over y_1. The exponential is 1 for $y_1 = 0$ and is -1 for $y_1 = 1$ provided $x_0 = 1$. This functionality is provided by a Hadamard gate H,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{6}$$

so

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,, \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,, \end{aligned} \tag{7}$$

Recall that in terms of components

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0, \end{pmatrix}\,, \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}\,. \tag{8}$$

More compactly, we can write

$$H|x_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_0}|1\rangle\right) = \frac{1}{\sqrt{2}} \sum_{y_1=0}^{1} (-1)^{x_0 y_1} |y_1\rangle = \frac{1}{\sqrt{2}} \sum_{y_1=0}^{1} \exp[2\pi i y_1 x_0/2] |y_1\rangle\,, \tag{9}$$

where we denote by y_1 the dummy variable to be summed over (coming from the effects of the Hadamard) in order to correspond with the second factor on the RHS of Eq. (5). We therefore see that the second factor on the RHS of Eq. (5) is generated by the Hadamard gate shown in Fig. 1.

What about the first factor on the RHS of Eq. (5) which involves y_0? There are two pieces in the exponential. The one involving $2\pi i y_0 x_1/2$ can be dealt with by a Hadamard, similar to Fig. 1

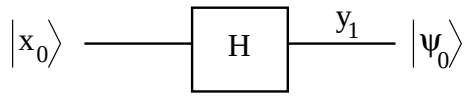

FIG. 1: The output from the Hadamard gate is $|\psi_0\rangle = \frac{1}{\sqrt{2}}(|y_1{=}0\rangle + (-1)^{x_0}|y_1{=}1\rangle)$. This can be expressed as $\frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}(-1)^{x_0 y_1}|y_1\rangle = \frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}\exp[2\pi i y_1 x_0/2]|y_1\rangle$. Recall that x_0 takes a fixed value 0 or 1.

but with the left hand qubit being x_1 and the right hand qubit being labeled by y_0. However, the piece involving $2\pi i y_0 x_0/4$ is different. It induces a phase shift of $e^{i\pi/2}$ for $y_0 = 1$ provided that x_0 is also 1. This requires a controlled phase gate. We define a phase gate R_d by[1]

$$R_d = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/2^d} \end{pmatrix} . \tag{10}$$

Acting on $|0\rangle, R_d$ makes no change while acting on $|1\rangle, R_d$ changes the phase by $\pi/2^d$. Note that R_0 is just the Z gate. Here we need R_1.

The exponential in the first term on the RHS of Eq. (5) can be generated by a Hadamard followed by a controlled R_1 gate as shown for the top qubit in Fig. 2. Note that the R_1 phase gate on the upper qubit is controlled by the lower qubit. Including the Hadamard on the lower qubit, Fig. 2 generates both factors on the RHS of Eq. (5).

To make sure we understand we understand what is happening in the circuit in Fig. 2 we now write down the state at each of the steps shown in the figure. After the first Hadamard the state is

$$|\phi_1\rangle_2 = \frac{1}{\sqrt{2}}\sum_{y_0=0}^{1} e^{2\pi i y_0 x_0/2}|y_0 x_0\rangle, \tag{11a}$$

where we denote by y_0 the dummy variable that is summed over in order to agree with Eq. (5). After the controlled-R_1 gate we have

$$|\phi_2\rangle_2 = \frac{1}{\sqrt{2}}\sum_{y_0=0}^{1} e^{2\pi i y_0 x_0/2}\, e^{2\pi i y_0 x_1/4}|y_0 x_0\rangle. \tag{11b}$$

The final state after the Hadamard on the lower qubit is therefore

$$|\psi'_x\rangle_2 = \left(\frac{1}{\sqrt{2}}\sum_{y_0=0}^{1} e^{2\pi i y_0 x_0/2}\, e^{2\pi i y_0 x_1/4}\right)\left(\frac{1}{\sqrt{2}}\sum_{y_1=0}^{1} e^{2\pi i y_1 x_0/2}\right)|y_0 y_1\rangle. \tag{11c}$$

[1] This is the definition of R_d given in Vathsan's book, and I find it convenient. Some other authors adopt a slightly different definition with $e^{2\pi i/2^d}$ instead of $e^{\pi i/2^d}$.

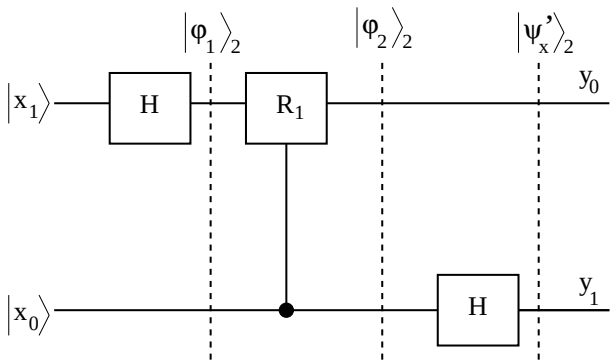

FIG. 2: The initial state on the left is the single quantum state $|x\rangle_2 \equiv |x_1 x_0\rangle$ in the computational basis. The final state on the right is the superposition $|\psi_x'\rangle_2 = (1/2)\sum_{y=0}^{3} \exp(2\pi i xy/2^2)|y_0 y_1\rangle$, which is almost $|\psi_x\rangle_2$, the QFT of $|x\rangle_2 \equiv |x_1 x_0\rangle$ given in Eq. (5), except that the order of the bits in the final state is the reverse of what it should be according to Eq. (5). This can be corrected by a swap gate as shown in Fig. 3. Note the controlled-R_1 phase gate. The general phase gate R_d is defined in Eq. (10).

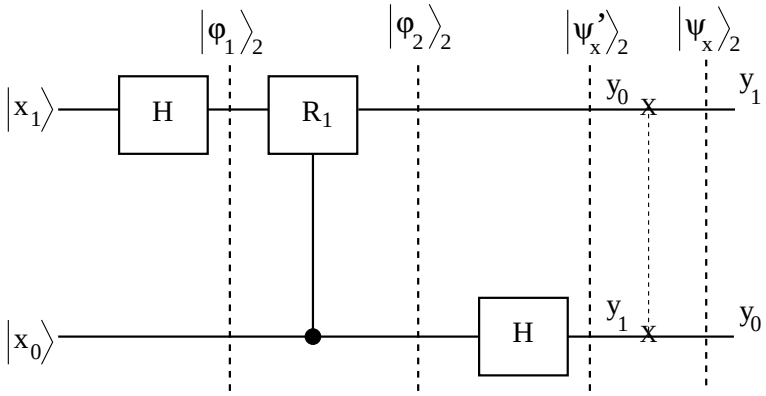

FIG. 3: The same as Fig. 2 but with the addition of a swap gate on the right (the dashed line with crosses at the ends). The final state is now precisely $|\psi_x\rangle_2 = (1/2)\sum_{y=0}^{3} \exp(2\pi i xy/2^2)|y_1 y_0\rangle$, the QFT given in Eq. (5).

$|\psi_x'\rangle$ is almost the desired QFT in Eq. (5), except that the order of the qubits on in the final state on the right has been reversed. This can be compensated for by adding a swap gate on the right as shown in Fig. 3. Hence Fig. 3 displays the circuit to implement the QFT for 2 qubits written out in Eq. (5).

We now make an extremely important point. We have shown the QFT for a fixed basis state x (in the computational basis) inputted to the left of the circuit diagrams. However, since the circuit is linear (because quantum mechanics is linear) the circuit will act *in parallel* on a linear superposition of basis states. This is where the power of the QFT lies.

III. QFT WITH THREE OR MORE QUBITS

With three qubits the QFT, analogous to Eq. (5) is

$$|\psi_x\rangle_3 = \frac{1}{\sqrt{8}} \sum_{y=0}^{7} \exp[2\pi i x y/2^3] |y\rangle_3 \tag{12}$$

$$= \left(\frac{1}{\sqrt{2}} \sum_{y_0=0}^{1} \exp\left[2\pi i y_0 \left(\frac{x_0}{8} + \frac{x_1}{4} + \frac{x_2}{2}\right)\right] \right) \left(\frac{1}{\sqrt{2}} \sum_{y_1=0}^{1} \exp\left[2\pi i y_1 \left(\frac{x_0}{4} + \frac{x_1}{2}\right)\right] \right) \times \left(\frac{1}{\sqrt{2}} \sum_{y_2=0}^{1} \exp\left[2\pi i y_2 \frac{x_0}{2}\right] \right) |y_2 y_1 y_0\rangle. \tag{13}$$

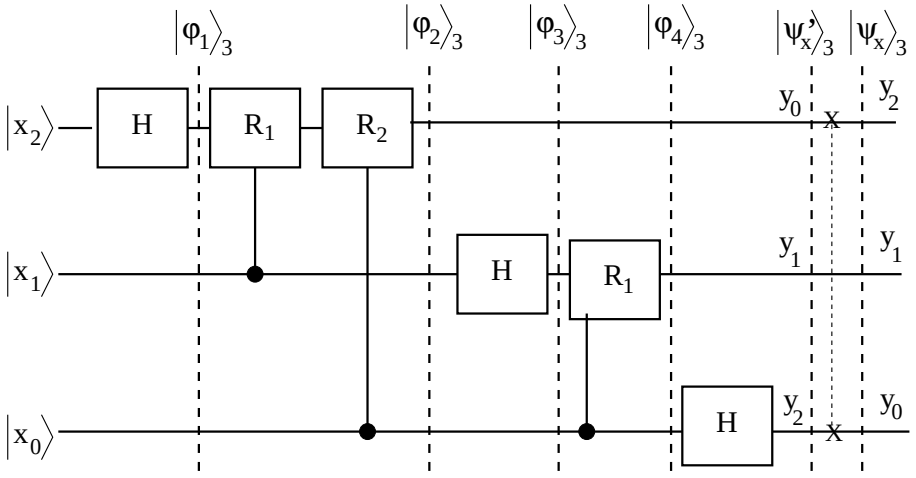

FIG. 4: Circuit diagram for performing the QFT with $n = 3$ qubits. It generates the transformation shown in Eq. (13). The phase gates, R_d, are defined in Eq. (10). The dashed line with crosses at the ends indicates a swap gate between qubits 0 and 2. This serves to reverse the order of the qubits.

Following along the lines in the previous section, the circuit diagram which will perform this is shown in Fig. 4. To make sure we understand this circuit we will write down the state at each stage indicated on the figure. (Although these expressions look rather complicated is useful to make the effort to understand them. In particular, you will appreciate why the order of the qubits

is reversed in $|\psi'_x\rangle_3$.)

$$|\phi_1\rangle_3 = \left(\frac{1}{\sqrt{2}}\sum_{y_0=0}^{1}\exp\left[2\pi i y_0\left(\frac{x_2}{2}\right)\right]\right)|y_0x_1x_0\rangle, \tag{14a}$$

$$|\phi_2\rangle_3 = \left(\frac{1}{\sqrt{2}}\sum_{y_0=0}^{1}\exp\left[2\pi i y_0\left(\frac{x_0}{8}+\frac{x_1}{4}+\frac{x_2}{2}\right)\right]\right)|y_0x_1x_0\rangle, \tag{14b}$$

$$|\phi_3\rangle_3 = \left(\frac{1}{\sqrt{2}}\sum_{y_0=0}^{1}\exp\left[2\pi i y_0\left(\frac{x_0}{8}+\frac{x_1}{4}+\frac{x_2}{2}\right)\right]\right)\left(\frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}\exp\left[2\pi i y_1\left(\frac{x_1}{2}\right)\right]\right)|y_0y_1x_0\rangle, \tag{14c}$$

$$|\phi_4\rangle_3 = \left(\frac{1}{\sqrt{2}}\sum_{y_0=0}^{1}\exp\left[2\pi i y_0\left(\frac{x_0}{8}+\frac{x_1}{4}+\frac{x_2}{2}\right)\right]\right)\left(\frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}\exp\left[2\pi i y_1\left(\frac{x_0}{4}+\frac{x_1}{2}\right)\right]\right)|y_0y_1x_0\rangle, \tag{14d}$$

$$|\psi'_x\rangle_3 = \left(\frac{1}{\sqrt{2}}\sum_{y_0=0}^{1}\exp\left[2\pi i y_0\left(\frac{x_0}{8}+\frac{x_1}{4}+\frac{x_2}{2}\right)\right]\right)\left(\frac{1}{\sqrt{2}}\sum_{y_1=0}^{1}\exp\left[2\pi i y_1\left(\frac{x_0}{4}+\frac{x_1}{2}\right)\right]\right)\times\left(\frac{1}{\sqrt{2}}\sum_{y_2=0}^{1}\exp\left[2\pi i y_2\frac{x_0}{2}\right]\right)|y_0y_1y_2\rangle. \tag{14e}$$

$|\psi'_x\rangle$ is almost the desired QFT in Eq. (13), except that the order of the qubits on in the final state on the right has been reversed. This can be compensated for by adding a swap gate between qubits 1 and 3. Hence $|\psi_x\rangle$ in the figure is the desired QFT for 3 qubits given in Eq. (13).

Comparing with the case for two qubits shown in Fig. 3, and that for three qubits in Fig. 4, the generalization to an arbitrary number of qubits, where

$$|\psi_x\rangle_n = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}\exp[2\pi i xy/2^n]|y\rangle_n \tag{15}$$

can be deduced and is shown in Fig. 5. Note that the controlled phase gate between qubits x_i and x_j is $R_{|i-j|}$, which makes the structure fairly simple.

For an n-qubit QFT one needs n Hadamard gates. The number of controlled phase gates is $1+2+\cdots+n-1 = n(n-1)/2$. Also $[n/2]$ swaps are required, where $[k]$ denotes the largest integer less than or equal to k. The circuit therefore provides an algorithm for performing the QFT in $O(n^2)$ steps. By contrast the FFT requires $O(n2^n)$ steps which is exponentially greater.

However, we cannot obtain the 2^n Fourier amplitudes from the QFT since a measurement will just give one of the basis states with a probability proportional to the square of the absolute value of its Fourier amplitude. The QFT can, however, give useful information if the

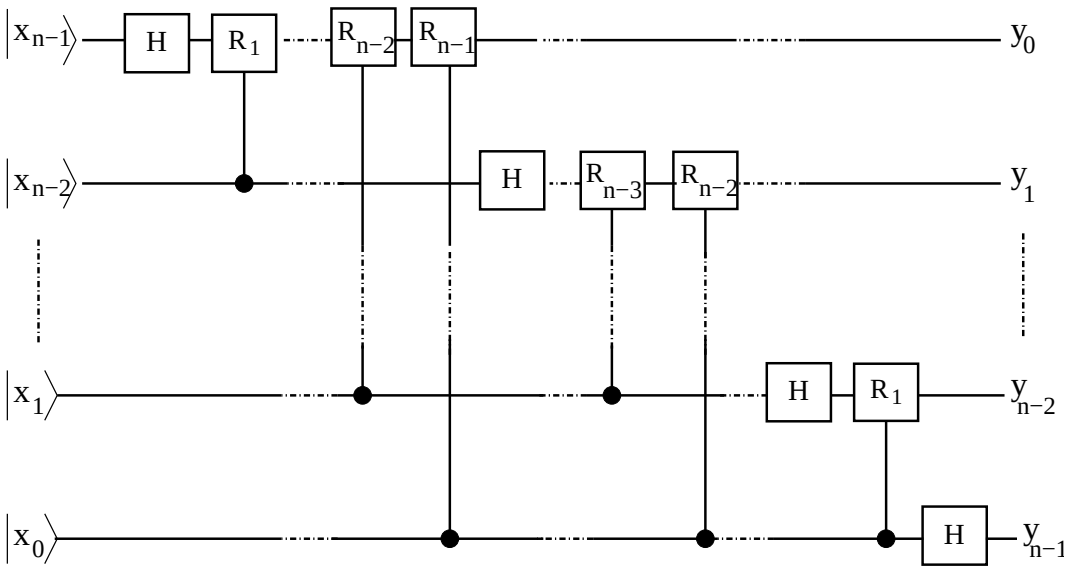

FIG. 5: Circuit diagram for performing the QFT with an arbitrary number of qubits. For clarity the final swaps are not shown, so the input states on the left, x_i, and the output states on the right, y_i, are in opposite order. Note that the controlled phase gate between qubits x_i and x_j is $R_{|i-j|}$, which makes the structure fairly simple.

input state is a linear combination $\sum_x a_x|x\rangle$ where the a_x are periodic in x with some period r. As we shall see in the handout *Shor's Algorithm for Period Finding on a Quantum Computer*, `https://young.physics.ucsc.edu/150/shor.pdf`, the Fourier amplitudes are then strongly peaked at multiples of $2^n/r$, so there is a high probability of getting a value for y at, or close to, a multiple of $2^n/r$, from which it turns out that one can deduce r with high probability. Hence the QFT is useful for period finding.

As we saw in the handout *Using Period Finding to Factor an Integer*, period finding can be used to factor integers. If one could factor large integers, one would be able to decode messages sent down the internet which have been encoded with the standard RSA encryption method. We discussed RSA encryption in the handout *RSA (Rivest-Shamir-Adleman) Encryption*, `https://young.physics.ucsc.edu/150/rsa.pdf`.

Appendix A: Fast Fourier Transform (FFT) for $N = 4$

For comparison with the QFT we write out the Fast Fourier Transform (FFT) for $N = 4$. The Fourier transform for this case is

$$y_0 = \tfrac{1}{2}\,(\,x_0 + x_1 + x_2 + x_3)\;, \tag{A1a}$$

$$y_1 = \tfrac{1}{2}\,\big(\,x_0 + ix_1 + i^2x_2 + i^3x_3\big)\;, \tag{A1b}$$

$$y_2 = \tfrac{1}{2}\,\big(\,x_0 + i^2x_1 + x_2 + i^2x_3\,\big)\;, \tag{A1c}$$

$$y_3 = \tfrac{1}{2}\,\big(\,x_0 + i^3x_1 + i^2x_2 + ix_3\,\big)\;, \tag{A1d}$$

where the x_j are the original data, the y_j are the Fourier transformed data, and we have used that

$$\exp(2\pi i/4) = i\,. \tag{A2}$$

To evaluate Eqs. (A1) efficiently, the FFT proceeds recursively. We firstly define Fourier transforms of length 2:

$$u_0 = \tfrac{1}{\sqrt{2}}(x_0 + x_2) \qquad = \tfrac{1}{\sqrt{2}}(x_0 + i^{2k}x_2)\;(k=0)\,, \tag{A3a}$$

$$u_1 = \tfrac{1}{\sqrt{2}}(x_1 + x_3) \qquad = \tfrac{1}{\sqrt{2}}(x_1 + i^{2k}x_3)\;(k=0)\,, \tag{A3b}$$

$$u_2 = \tfrac{1}{\sqrt{2}}(x_0 - x_2) \qquad = \tfrac{1}{\sqrt{2}}(x_0 + i^{2k}x_2)\;(k=1)\,, \tag{A3c}$$

$$u_3 = \tfrac{1}{\sqrt{2}}(x_1 - x_3) \qquad = \tfrac{1}{\sqrt{2}}(x_1 + i^{2k}x_3)\;(k=1)\,, \tag{A3d}$$

$$\tag{A3e}$$

Pairs of quantities in Eqs. (A3) are combined to form the Fourier Transform in Eqs. (A1):

$$y_0 = \tfrac{1}{\sqrt{2}}(u_0 + u_1) \qquad = \tfrac{1}{\sqrt{2}}(u_0 + i^{k}u_1)\;(k=0)\,, \tag{A4a}$$

$$y_1 = \tfrac{1}{\sqrt{2}}(u_2 + i\,u_3) \qquad = \tfrac{1}{\sqrt{2}}(u_2 + i^{k}u_3)\;(k=1)\,, \tag{A4b}$$

$$y_2 = \tfrac{1}{\sqrt{2}}(u_0 - u_1) \qquad = \tfrac{1}{\sqrt{2}}(u_0 + i^{k}u_1)\;(k=2)\,, \tag{A4c}$$

$$y_3 = \tfrac{1}{\sqrt{2}}(u_2 - iu_3) \qquad = \tfrac{1}{\sqrt{2}}(u_2 + i^{k}u_3)\;(k=3)\,, \tag{A4d}$$

$$\tag{A4e}$$

Let's check that this works by evaluating y_1. We have

$$y_1 = \tfrac{1}{\sqrt{2}}\,(u_2 + i\,u_3)\;, \tag{A5a}$$

$$= \tfrac{1}{2}\,(\,x_0 - x_2 + i(x_1 - x_3)\,) = \tfrac{1}{2}\,\big(\,u_0 + ix_1 + i^2x_2 + i^3x_3\big)\;, \tag{A5b}$$

$$\tag{A5c}$$

which agrees with Eq. (A1b).

It is instructive to write the linear transformations in Eqs. (A1), (A3), and (A4) in matrix form. Equation (A1) is written in matrix formulation as

$$\vec{y} = U\vec{x}\,, \tag{A6}$$

where

$$U = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & i^2 & i^3 \\ 1 & i^2 & 1 & i^2 \\ 1 & i^3 & i^2 & i \end{pmatrix}. \tag{A7}$$

Equation (A3) in matrix form is

$$\vec{u} = U_1\vec{x}\,, \tag{A8}$$

where

$$U_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & i^2 & 0 \\ 0 & 1 & 0 & i^2 \end{pmatrix}. \tag{A9}$$

Equation (A4) in matrix form is

$$\vec{y} = U_2\vec{u}\,, \tag{A10}$$

where

$$U_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & i \\ 1 & i^2 & 0 & 0 \\ 0 & 0 & 1 & i^3 \end{pmatrix}. \tag{A11}$$

With some matrix manipulations one can verify that

$$U = U_2\,U_1\,, \tag{A12}$$

as required. (I used *Mathematica*.)

Appendix B: Comparison between FFT and the QFT for $N = 4$

The QFT is generated by the unitary matrix U in Eq. (A7). The classical FFT is written as the product of two sparse matrices, $U = U_2 U_1$, see Eq. (A12), where U_1 is given in Eq. (A9) and U_2 is given in Eq. (A11). We will now see that there is a close connection between the FFT and the QFT, in particular, that the transformations U_1 and U_2 correspond to different parts of the diagram in Fig. 3.

The swap gate interchanges states $|1\rangle$ and $|2\rangle$, see Eq. 1, so it has the matrix representation

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} . \tag{B1}$$

The Hadamard gate acting on the lower qubit of Fig. 3 was shown in Eq. (9). Including now also the (unchanged) upper qubit, the matrix representation of the transformation induced by this gate is

$$H_l = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} . \tag{B2}$$

The Hadamard on the upper qubit has a similar representation, except that the two qubits have been interchanged, i.e.

$$H_u = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} . \tag{B3}$$

The controlled R_1 phase gate gives a multiplicative factor of i if y_0 and x_0 are both 1, i.e. state $|3\rangle$. Hence

$$R_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix} . \tag{B4}$$

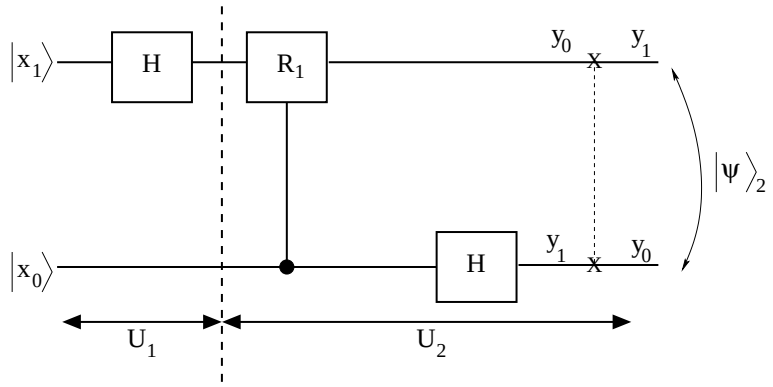

FIG. 6: The same as Fig. 3 but also showing the correspondence with the breakup of the FFT into two operations $U = U_2U_1$, see Eqs. (B6).

The total effect of the quantum circuit in Fig. 3, reading from left to right on the circuit, is given by the matrix product $SH_lR_1H_u$. Note that one reads from from right to left in a product of operators because the operators act on the right. It can be confusing that the direction of time in the circuit diagram is opposite to that in an expression of operators. Multiplying these out these matrices using *Mathematica* one gets the expected result,

$$SH_lR_1H_u = U\,, \tag{B5}$$

where U is the Fourier transform, shown in Eq. (A7). Recall that S is the swap, H_l is the Hadamard on the lower qubit, R_1 is the controlled phase gate, and H_u is the Hadamard on the upper qubit. Hence the gates in the quantum circuit in Fig. 3 do indeed affect a Fourier transform for 2 qubits.

In the FFT we decomposed U into a product of two sparse matrices, $U = U_2U_1$, see Eq. (A12). We can also make a connection between the individual matrices U_2 and U_1 of the FFT and the individual matrices S, H_l, H_u and R_1 of the QFT. One finds

$$U_1 = H_u\,, \tag{B6a}$$

$$U_2 = SH_lR_1\,. \tag{B6b}$$

The first is obtained by inspection and the second I checked with *Mathematica*. Hence the first operation U_1 in the FFT for $N = 4$ corresponds, in the QFT, to the Hadamard on the upper qubit in Fig. 3, while the second operation U_2 in the FFT corresponds to the remaining operations in the QFT: the controlled phase gate on the upper qubit, the Hadamard on the lower qubit, and the swap. This breakup is shown in Fig. 6.

To conclude this section, we have seen that there is close connection between the breakup used in the FFT and that used in the QFT. This should not be a surprise. In the FFT we iteratively

divide the FT into two FTs of half the length, while in the QFT we have a binary representation of the states and treat each bit in turn, so clearly there is a connection. For $N = 4$, this connection is expressed in Eqs. (B6).

Appendix C: Comparison of FFT and QFT for $N = 8$

In this appendix we show how the breakup of the FFT for $N = 8$ is related to the circuit for the QFT. Our final result will be Fig. 7, which is the analog of Fig. 6 for $N = 4$.

As shown in the handout entitled *The Fast Fourier Transform* `https://young.physics.ucsc.edu/150/FFT.pdf` the FFT for $N = 8$ can be written as

$$U^{(8)} = U_3^{(8)}\, U_2^{(8)}\, U_1^{(8)} \tag{C1}$$

where

$$U^{(8)} = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}, \tag{C2}$$

$$U_1^{(8)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & \omega^4 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \omega^4 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \omega^4 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega^4 \end{pmatrix}, \tag{C3}$$

$$U_2^{(8)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & \omega^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & \omega^2 \\ 1 & 0 & \omega^4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & \omega^4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & \omega^6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & \omega^6 \end{pmatrix}, \tag{C4}$$

and

$$U_3^{(8)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & \omega & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \omega^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega^3 \\ 1 & \omega^4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & \omega^5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \omega^6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega^7 \end{pmatrix}. \tag{C5}$$

One can verify by doing the matrix multiplication (using *Mathematica* helps) that Eq. (C1) is satisfied.

One can see from Fig. 4 that the QFT can be written as[2]

$$U^{(8)} = S_{02}^{(8)}\, H_l^{(8)}\, R_{1,m}^{(8)}\, H_m^{(8)}\, R_{2,u}^{(8)}\, R_{1,u}^{(8)}\, H_u^{(8)}\,, \tag{C6}$$

[2] Recall that we work from right to left in operator equations like Eq. (C6) but from left to right in circuit diagrams such as Fig. 4.

in a fairly obvious notation, where

$$S_{02}^{(8)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \tag{C7}$$

$$H_l^{(8)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}, \tag{C8}$$

$$R_{1,m}^{(8)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & i & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & i \end{pmatrix}, \tag{C9}$$

$$H_m^{(8)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{pmatrix}, \tag{C10}$$

$$R_{2,u}^{(8)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega \end{pmatrix}, \tag{C11}$$

$$R_{1,u}^{(8)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & i \end{pmatrix}, \tag{C12}$$

$$H_u^{(8)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & -1 \end{pmatrix}, \tag{C13}$$

One may verify Eq. (C6) using *Mathematica*. Note that S_{02} swaps qubits 0 and 2, as required to reverse the order of the qubits.

Can we make a connection between the individual matrices, $U_1^{(8)}, U_2^{(8)}$, and $U_3^{(8)}$, in the FFT, Eq. (C1), and the individual matrices, $S_{02}^{(8)}, H_l^{(8)}, R_{1,m}^{(8)}, H_m^{(8)}, R_{2,u}^{(8)}, R_{1,u}^{(8)}$, and $H_u^{(8)}$, in the QFT, Eq. (C6)?

One immediately sees that $U_1^{(8)} = H_u^{(8)}$. However to make a connection between the other parts of the FFT, $U_2^{(8)}$ and $U_3^{(8)}$, we introduce the swap operator between qubits 1 and 2:

$$S_{12}^{(8)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \tag{C14}$$

We also need to realize that we can move the R_2 gate in Fig. 4 to the right as long as it does not cross the Hadamard on the lowest qubit (since this is the control qubit). Hence we can also write Eq. (C6) as

$$U^{(8)} = S_{02}^{(8)}\, H_l^{(8)}\, R_{1,m}^{(8)}\, R_{2,u}^{(8)}\, H_m^{(8)}\, R_{1,u}^{(8)}\, H_u^{(8)}\,, \tag{C15}$$

where we have moved $R_{2,u}^{(8)}$ to the *left*. We then find that

$$U_1^{(8)} = H_u^{(8)}\,, \tag{C16a}$$

$$U_2^{(8)} = S_{12}^{(8)}\, H_m^{(8)}\, R_{1,u}^{(8)}, \tag{C16b}$$

$$U_3^{(8)} = S_{02}^{(8)}\, H_l^{(8)}\, R_{1,m}^{(8)}\, R_{2,u}^{(8)}\, S_{12}^{(8)}\,, \tag{C16c}$$

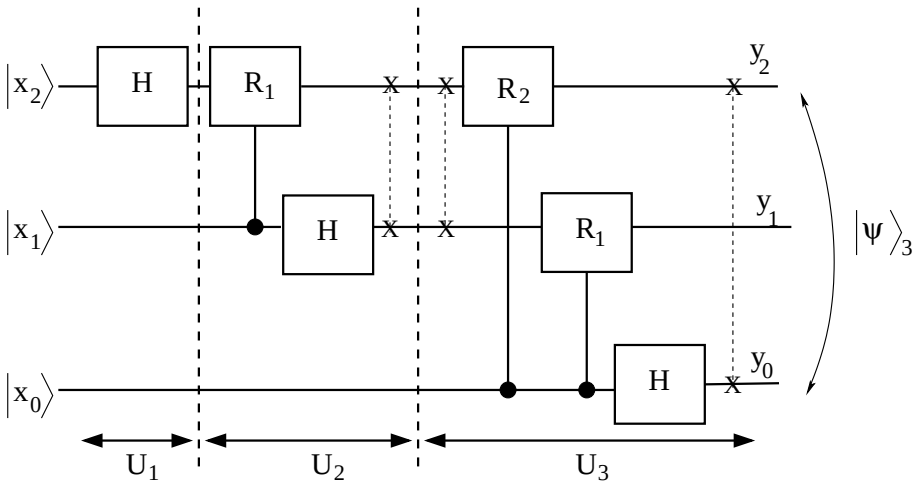

FIG. 7: Like Fig. 4 except that the R_2 gate has been moved to the right of the Hadamard on the middle qubit (which has no effect) and that a pair of reversals of the order of qubits 1 and 2 have been added (which also has no effect). The reversal is accomplished by a swap gate. Note that the final reversal of the order of all three qubits (on the right of the diagram) is also accomplished by a single swap gate. The correspondence with the breakup of the FFT ($U = U_3U_2U_1$) is indicated, see Eqs. (C16). To see this correspondence it is necessary to include the pair of reversals of the order of qubits 1 and 2.

which agrees with Eqs. (C15) and (C1) since $\left(S_{12}^{(8)}\right)^2$ is the identity (swapping twice makes no change). This breakup is shown in Fig. 7. Apart from the reversals of qubit order, the correspondence between the QFT and the FFT is straightforward to see.

Following the structure of Fig. 6 for two qubits, and Fig. 7 for three qubits the generalization to four qubits is shown in Fig. 8. The correspondence with the FFT is clear, the only complication being that, in order to show the correspondence, pairs of reversals of the order of the qubits (which cancel each other out) have to be introduced, with one reversal being in one stage of the FFT and the other reversal in the next stage of the FFT. Reading Fig. 8 from left to right, the first reversal pair reverses qubits 2 and 3 (which needs a single swap gate between qubits 2 and 3), the next reversal reverses qubits 1, 2 and 3 (which only needs a single swap gate between qubits 1 and 3), and the last reversal (not a pair because this is the last one so there is no additional stage to compensate it) reverses all 4 qubits (which needs two swap gates, one between qubits 0 and 3 and the other between qubits 1 and 2).

We see that there is a close parallel between the breakup of the FFT and circuit of the QFT. The details are slightly complicated because one needs reversals of the order of the qubits to make the correspondence precise. Note that Fig. 1 in `https://arxiv.org/pdf/1005.3730.pdf` is related to the results presented here.

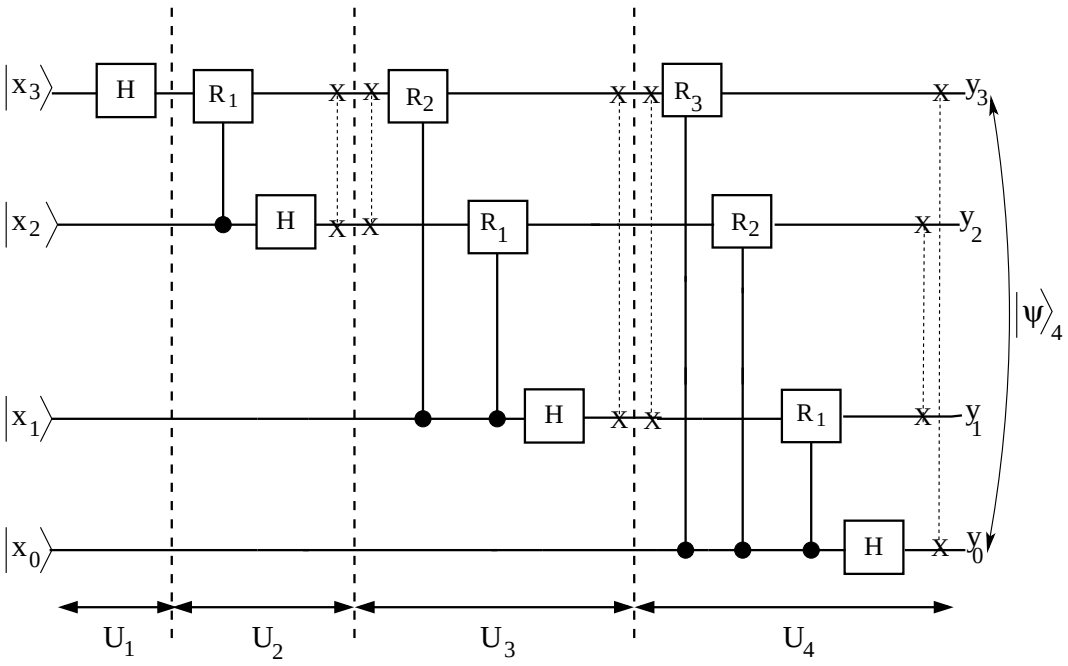

FIG. 8: The generalization of Figs. 7 and 6 to the case of four qubits. The correspondence with the breakup of the FFT ($U = U_4U_3U_2U_1$) is indicated.