Exercises for Quantum Information
Sheet 4 — Discrete Fourier Transform

0. For $g, h \in \mathbb{Z}_{r_1} \times ... \times \mathbb{Z}_{r_m}$ show that $\chi^{-1}(g) = \chi(g)^*$ and $\chi_g(h) = \chi_h(g)$.

Solution. Let χ be any character of G. Since G is finite, every $g \in G$ has finite order, say $g^r = e$. Hence

$$\chi(g)^r = \chi(g^r) = \chi(e) = 1.$$

So $\chi(g)$ is an r-th root of unity, in particular $|\chi(g)| = 1$. Therefore

$$\chi(g)^{-1} = \overline{\chi(g)} = \chi(g)^*.$$

This proves

$$\chi^{-1}(g) = \chi(g)^*.$$

Now write

$$g = (g_1, \ldots, g_m), \qquad h = (h_1, \ldots, h_m) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_m}.$$

With the convention from the notes,

$$\chi_g(h) = \exp\left(2\pi i \sum_{j=1}^{m} \frac{g_j h_j}{r_j}\right).$$

Since multiplication in $\mathbb{C}$ and in the exponent is commutative,

$$\chi_g(h) = \exp\left(2\pi i \sum_{j=1}^{m} \frac{g_j h_j}{r_j}\right) = \exp\left(2\pi i \sum_{j=1}^{m} \frac{h_j g_j}{r_j}\right) = \chi_h(g).$$

Hence $\chi_g(h) = \chi_h(g)$. □

1. Show that DFT and DFT^{-1} are complex conjugate.

Solution. Let $G = \{g_1, \ldots, g_n\}$. From the notes,

$$[\mathrm{DFT}]_{k,\ell} = \frac{1}{\sqrt{n}} \chi_{g_k}(g_\ell)^*.$$

By the previous exercise,

$$\chi_{g_k}(g_\ell) = \chi_{g_\ell}(g_k),$$

so

$$[\mathrm{DFT}]_{k,\ell} = [\mathrm{DFT}]_{\ell,k}.$$

Thus DFT is symmetric:

$$\mathrm{DFT}^T = \mathrm{DFT}\,.$$

Also, DFT is unitary, hence

$$\mathrm{DFT}^{-1} = \mathrm{DFT}^* = \overline{\mathrm{DFT}}^T.$$

Since $\mathrm{DFT}^T = \mathrm{DFT}$, we get

$$\mathrm{DFT}^{-1} = \overline{\mathrm{DFT}}.$$

Equivalently, DFT and DFT^{-1} are complex conjugate matrices. □

2. Describe the canonical basis and the basis of characters of the space of functions from G to $\mathbb{C}$, where:

   - $G = \mathbb{Z}_2 \times \mathbb{Z}_3$,
   - $G = \mathbb{Z}_9$,
   - $G = \mathbb{Z}_3 \times \mathbb{Z}_3$.

   Compute DFT and IFT matrices for all the cases described above.

   Solution. In every case, the canonical basis of the space of functions $G \to \mathbb{C}$ is

   $$\{b_g\}_{g\in G}, \qquad b_g(x) = \delta_{g,x}.$$

   The orthonormal basis of characters is

   $$\left\{ \frac{1}{\sqrt{|G|}} \chi_h \right\}_{h\in G}.$$

   We now write these explicitly in each case. The matrices depend on the order of the group elements, so we fix a natural order in each example.

   (a) $G = \mathbb{Z}_2 \times \mathbb{Z}_3$**.**

   Take the order

   $$(0,0), (0,1), (0,2), (1,0), (1,1), (1,2).$$

   The canonical basis is

   $$b_{(a,b)}(x,y) = \delta_{a,x}\delta_{b,y}.$$

   The characters are indexed by $(u,v) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ and have the form

   $$\chi_{(u,v)}(a,b) = \exp\left(2\pi i \left(\frac{ua}{2} + \frac{vb}{3}\right)\right) = (-1)^{ua}\,\omega^{vb}, \qquad \omega = e^{2\pi i/3}.$$

   Hence the basis of characters is

   $$\left\{ \frac{1}{\sqrt{6}} \chi_{(u,v)} \;:\; (u,v) \in \mathbb{Z}_2 \times \mathbb{Z}_3 \right\}.$$

Using the same order for rows and columns, the inverse Fourier matrix is

$$\mathrm{IFT}_{\mathbb{Z}_2\times\mathbb{Z}_3} = \frac{1}{\sqrt{6}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & \omega & \omega^2 & -1 & -\omega & -\omega^2 \\ 1 & \omega^2 & \omega & -1 & -\omega^2 & -\omega \end{pmatrix}.$$

By the previous exercise,

$$\mathrm{DFT}_{\mathbb{Z}_2\times\mathbb{Z}_3} = \overline{\mathrm{IFT}_{\mathbb{Z}_2\times\mathbb{Z}_3}},$$

i.e. it is obtained by replacing ω with ω^2.

(b) $G = \mathbb{Z}_9$**.**

Take the order

$$0, 1, \ldots, 8.$$

The canonical basis is

$$b_j(x) = \delta_{j,x}, \qquad j, x \in \mathbb{Z}_9.$$

The characters are indexed by $t \in \mathbb{Z}_9$:

$$\chi_t(x) = \eta^{tx}, \qquad \eta = e^{2\pi i/9}.$$

So the basis of characters is

$$\left\{\frac{1}{3}\,\chi_t\right\}_{t=0}^{8}.$$

The inverse Fourier matrix is the usual 9×9 Fourier matrix:

$$[\mathrm{IFT}_{\mathbb{Z}_9}]_{t,x} = \frac{1}{3}\,\eta^{tx}, \qquad t, x = 0, \ldots, 8.$$

Equivalently,

$$\mathrm{IFT}_{\mathbb{Z}_9} = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \eta & \eta^2 & \eta^3 & \eta^4 & \eta^5 & \eta^6 & \eta^7 & \eta^8 \\ 1 & \eta^2 & \eta^4 & \eta^6 & \eta^8 & \eta & \eta^3 & \eta^5 & \eta^7 \\ 1 & \eta^3 & \eta^6 & 1 & \eta^3 & \eta^6 & 1 & \eta^3 & \eta^6 \\ 1 & \eta^4 & \eta^8 & \eta^3 & \eta^7 & \eta^2 & \eta^6 & \eta & \eta^5 \\ 1 & \eta^5 & \eta & \eta^6 & \eta^2 & \eta^7 & \eta^3 & \eta^8 & \eta^4 \\ 1 & \eta^6 & \eta^3 & 1 & \eta^6 & \eta^3 & 1 & \eta^6 & \eta^3 \\ 1 & \eta^7 & \eta^5 & \eta^3 & \eta & \eta^8 & \eta^6 & \eta^4 & \eta^2 \\ 1 & \eta^8 & \eta^7 & \eta^6 & \eta^5 & \eta^4 & \eta^3 & \eta^2 & \eta \end{pmatrix}.$$

Again,

$$\mathrm{DFT}_{\mathbb{Z}_9} = \overline{\mathrm{IFT}_{\mathbb{Z}_9}}.$$

(c) $G = \mathbb{Z}_3 \times \mathbb{Z}_3$**.**

Take the order

$$(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2).$$

The canonical basis is

$$b_{(a,b)}(x,y) = \delta_{a,x}\delta_{b,y}.$$

The characters are indexed by $(u,v) \in \mathbb{Z}_3 \times \mathbb{Z}_3$:

$$\chi_{(u,v)}(a,b) = \omega^{ua+vb}, \qquad \omega = e^{2\pi i/3}.$$

Thus the basis of characters is

$$\left\{ \frac{1}{3}\,\chi_{(u,v)} \ : \ (u,v) \in \mathbb{Z}_3 \times \mathbb{Z}_3 \right\}.$$

Using the same order for rows and columns,

$$\mathrm{IFT}_{\mathbb{Z}_3\times\mathbb{Z}_3} = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\ 1 & 1 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\ 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & 1 & \omega \\ 1 & \omega^2 & \omega & \omega & 1 & \omega^2 & \omega^2 & \omega & 1 \\ 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega \\ 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & 1 \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 & \omega & 1 & \omega^2 \end{pmatrix}.$$

Therefore

$$\mathrm{DFT}_{\mathbb{Z}_3\times\mathbb{Z}_3} = \overline{\mathrm{IFT}_{\mathbb{Z}_3\times\mathbb{Z}_3}},$$

i.e. again one just replaces ω with ω^2.

This completes the description of both bases and of the DFT / IFT matrices in all three cases. □

3. Are there some special relations between DFT and IFT matrices for $\mathbb{Z}_2^m$?

Solution. Yes. For $G = \mathbb{Z}_2^m$, every component has modulus 2, so for

$$g = (g_1, \ldots, g_m), \qquad h = (h_1, \ldots, h_m) \in \mathbb{Z}_2^m$$

we get

$$\chi_g(h) = \exp\left(2\pi i \sum_{j=1}^{m} \frac{g_j h_j}{2} \right) = (-1)^{g_1h_1+\cdots+g_mh_m} = (-1)^{g\cdot h}.$$

Thus all character values are real and equal to ± 1. Hence

$$\mathrm{DFT} = \mathrm{IFT} = \frac{1}{\sqrt{2^m}}\big((-1)^{g\cdot h}\big)_{g,h\in\mathbb{Z}_2^m}.$$

So in this case the Fourier matrix is

- real,
- symmetric,

- orthogonal,
- equal to its own inverse.

In particular,

$$\mathrm{DFT}^{-1} = \mathrm{DFT} = \mathrm{IFT}, \qquad \mathrm{DFT}^2 = I.$$

This is exactly the Walsh–Hadamard matrix:

$$\mathrm{DFT}_{\mathbb{Z}_2^m} = H^{\otimes m}.$$

□

4. Construct a circuit computing IFT for $\mathbb{Z}_8$ explicitly.

Solution. Here $8 = 2^3$, so we work with three qubits. Write

$$|k\rangle = |k_1 k_2 k_3\rangle, \qquad k = 4k_1 + 2k_2 + k_3, \qquad \frac{k}{8} = \frac{k_1}{2} + \frac{k_2}{4} + \frac{k_3}{8}.$$

From the formula in the notes,

$$\mathrm{IFT}\,|k_1 k_2 k_3\rangle = \frac{|0\rangle + e^{2\pi i(0.k_3)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i(0.k_2 k_3)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i(0.k_1 k_2 k_3)}|1\rangle}{\sqrt{2}}.$$

Therefore we need the phase gates

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/4} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \qquad R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/8} \end{pmatrix}.$$

As in the notes, the output appears in reversed order, so we first swap the first and third qubits. Then the circuit for $\mathrm{IFT}_{\mathbb{Z}_8}$ is:

(from left to right) $\quad \mathrm{SWAP}_{1,3}, \quad H_3, \quad \Lambda_{2\to 3}(R_2), \quad \Lambda_{1\to 3}(R_3), \quad H_2, \quad \Lambda_{1\to 2}(R_2), \quad H_1.$

In words:

(a) swap qubits 1 and 3;
(b) apply H to qubit 3;
(c) apply controlled-R_2 from qubit 2 to qubit 3;
(d) apply controlled-R_3 from qubit 1 to qubit 3;
(e) apply H to qubit 2;
(f) apply controlled-R_2 from qubit 1 to qubit 2;
(g) apply H to qubit 1.

This is exactly the 3-qubit inverse quantum Fourier transform, i.e. the circuit computing IFT for $\mathbb{Z}_8$. □