Solution 3.3

All we have to do is to write

$$y_{j_1\dots j_N} = y_j = \frac{1}{2^{N/2}} \sum_{k=0}^{D-1} e^{2\pi i j k/D} x_k$$

= $\frac{1}{2^{N/2}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_N=0}^{1} x_{k_1\dots k_N} \prod_{l=1}^{N} e^{2\pi i k_l 0.j_{N-l+1}\dots j_N}$
= $\frac{1}{2^{N/2}} \sum_{k_N=0}^{1} e^{2\pi i k_N 0.j_1\dots j_N} \cdots \sum_{k_2=0}^{1} e^{2\pi i k_2 0.j_{N-1} j_N} \sum_{k_1=0}^{1} e^{2\pi i k_1 0.j_N} x_{k_1\dots k_N} .$

The final expression invites us to do the DFT one bit label at a time. To see this, define the lth partial transform iteratively by

$$\begin{aligned} x_{k_{l+1}\dots k_N; j_N\dots j_{N-l+1}} &= \sum_{k_l=0}^{1} e^{2\pi i k_l 0.j_{N-l+1}\dots j_N} x_{k_l\dots k_N; j_N\dots j_{N-l+2}} \\ &= x_{0k_{l+1}\dots k_N; j_N\dots j_{N-l+2}} + e^{2\pi i 0.j_N\dots j_{N-l+1}} x_{1k_{l+2}\dots k_N; j_{N-l+2}\dots j_N} \;, \end{aligned}$$

with $x_{k_1...k_N} \equiv x_{k_1...k_N}$ and $x_{j_N...j_1} = 2^{N/2} y_{j_1...j_N}$. For l = 1, this partial transform is the far right (first) sum in the final expression:

$$x_{k_2\dots k_N;j_N} = \sum_{k_1=0}^{1} e^{2\pi i k_1 0.j_N} x_{k_1\dots k_N;} = x_{0k_2\dots k_N} + e^{2\pi i 0.j_N} x_{1k_2\dots k_N}$$

For l = N, we get the far left (final) sum, which finishes off the DFT:

$$2^{N/2}y_{j_1\dots j_N} = x_{;j_N\dots j_1} = \sum_{k_N=0}^1 e^{2\pi i k_N 0.j_1\dots j_N} x_{k_N;j_N\dots j_2} = x_{0;j_N\dots j_2} + e^{2\pi i 0.j_1\dots j_N} x_{1;j_N\dots j_2} \ .$$

The partial transforms do the DFT one bit label at a time. The whole DFT is obtained by doing the l = 1 partial transform, followed by the l = 2 partial transform, on up to the l = N partial transform. At the end we have to reverse the order of the bit labels (this is akin to the SWAPs at the end of the QFT) and divide by $2^{N/2}$.

Each partial transform requires $O(2^N)$ multiplications; there being N partial transforms, the whole DFT gets done with $O(N2^N)$ multiplications. If the input amplitudes factor, i.e., $x_{j_1...j_N} = x_{j_1} \cdots x_{j_N}$, then the partial transforms can all be done independently and the DFT can be done with $O(N^2)$ multiplications. This is a very special case for a DFT, but it is exactly what happens in the QFT, since we are transforming basis states, which do have the required (tensor) product structure.