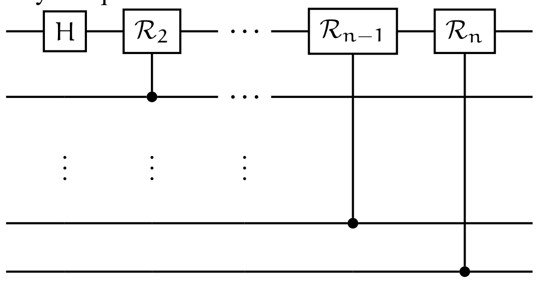
RSA and DFT

Problem 1. (20 pts) Let us practice with the RSA cryptosystem.

(a) My number n is 171352770689 and encryption key $e = 58787$. Using the encoding given by the correspondence $A \leftrightarrow 11, B \leftrightarrow 12, \ldots, Z \leftrightarrow 36$, send me a short message (the plaintext must be meaningful and contain at least six letters, each five letter block should be converted to the corresponding 10-digit number, the last block can contain any $0 < k \leq 5$ number of letters and is converted to an at most 10-digit number).

(b) Using the programs (http://tsvboris.pythonanywhere.com/IntrotoCryptography), find the factorization of n and my decryption exponent d. A grateful student sent me a message $'52284131866|29526308836'$. Hope it is something good. Let me know (decrypt the message).

Problem 2. (30 pts) Let $t \in \{1, \dots, n\}$, define $\mathcal{R}_t = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^t} \end{pmatrix}$ and let $U_1 \in U_n(\mathbb{C})$ be the unitary operator given by the quantum circuit



Compute (in the standard basis)

(a) $U_1(|00\dots0\rangle)$

(b) $U_1(|010\dots0\rangle)$

(c) $U_1(|011\dots1\rangle)$

(d) $U_1(|0y_2\dots y_n\rangle)$

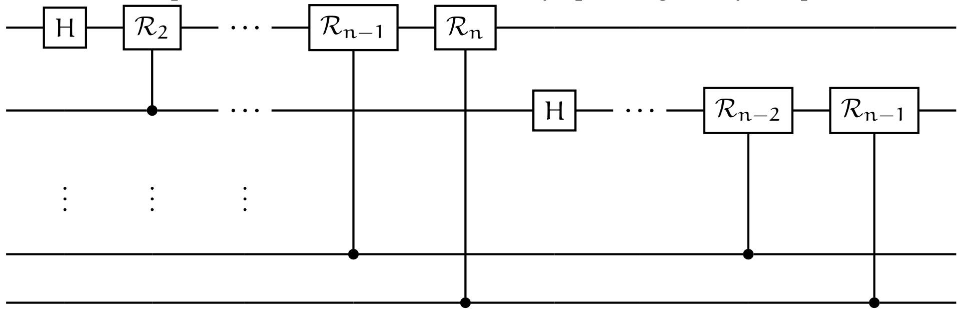
(e) $U_1(|10\ldots0\rangle)$

(f) $U_1(|110\ldots0\rangle)$

(g) $U_1(|11\ldots1\rangle)$

(h) $U_1(|1y_2\ldots y_n\rangle)$

Problem 3. (20 pts) Let $U_2 \in U_n(\mathbb{C})$ be the unitary operator given by the quantum circuit



Compute (in the standard basis)

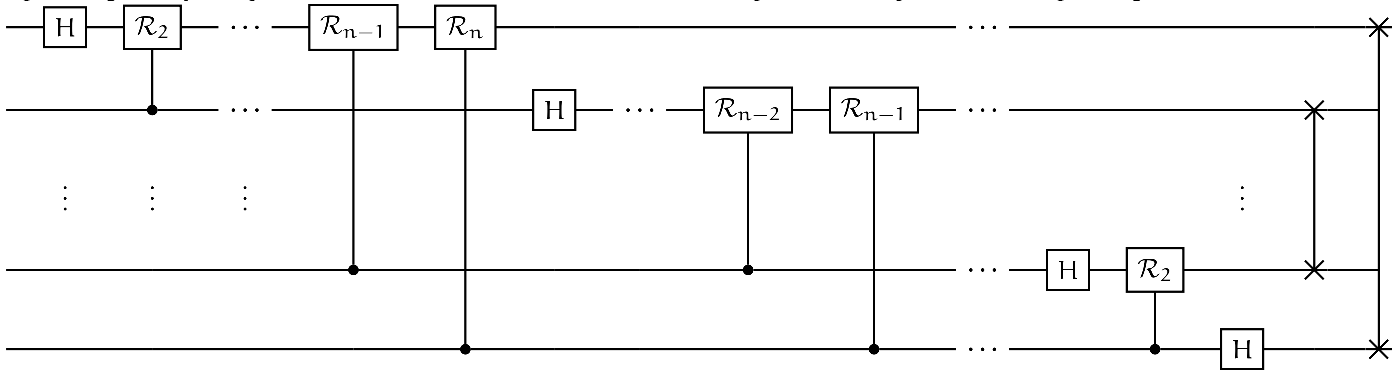
(a) $U_2(|00y_3 \ldots y_n\rangle)$

(b) $U_2(|01y_3 \ldots y_n\rangle)$

(c) $U_2(|10y_3 \ldots y_n\rangle)$

(d) $U_2(|11y_3 \ldots y_n\rangle)$

Problem 4. (30 pts) The goal of this exercise is to produce a quantum circuit for DFT. Let $U \in U_n(\mathbb{C})$ be the unitary operator given by the quantum circuit (here $\times$—$\times$ stands for the transposition (swap) of the corresponding elements)



(a) Compute $U(y)$ in the standard basis for an element $y = |y_1 y_2 \dots y_n\rangle$ with $y_i \in \mathbb{B}$.

(b) Show that $\mathsf{FT}(y) = U(y)$ for any element $y = |y_1 y_2 \dots y_n\rangle$ of the standard basis of $(\mathbb{C}^2)^{\otimes n}$.

(c) Conclude that $\mathsf{FT}(y)$ is realized by the quantum circuit above for any state vector $y \in (\mathbb{C}^2)^{\otimes n}$.[1]

[1] **Hint:** use (b) and linearity of unitary operators.