Quantum Information Theory

Prof. John Schliemann
Dr. Paul Wenk

Tue. H33 13pm c.t. & **Thu.** H34, 3pm c.t.
Mon. 12pm c.t., H33

Sheet 8

---

1 Period Finding .... [10P]

One important application of the QFT is in Shoer's factorization algorithm. Assume a system consisting of two 3-qubit systems which are an input register ($|\mathrm{In}\rangle$) and an output register ($|\mathrm{Out}\rangle$). The computational basis of each 3-qubit system is the orthogonal basis $\{|0\rangle \equiv |000\rangle, |1\rangle \equiv |001\rangle \ldots, |7\rangle \equiv |111\rangle\}$.

(a) Let the initial input register be

$$|\mathrm{In}\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle \ . \tag{1}$$

Following the lecture, we apply now U_f on the total initial state,

$$|\psi\rangle = U_f \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle\,|0\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x, f(x)\rangle \ , \tag{2}$$

with $f(x)$ a periodic, non-constant function satisfying $f(x+2) = f(x)$. Show that if we measure the first register after we applied the QFT to it, we are left with only two distinct results. This is a direct consequence of the periodicity.

(b) Now, we generalize the above result to a system with each register being an N-qubit system and $f(x)$ having a period of P. Further, assume we apply the procedure corresponding to (a). Let the outcome of a measurement of the first register after this procedure be ξ. Show that

$$\xi \in \left\{0,\ \frac{1\cdot 2^N}{P},\ \frac{2\cdot 2^N}{P}, \ldots, \frac{(P-1)\cdot 2^N}{P}\right\} \quad \text{with} \quad 2^N/P \in \mathbb{N}\ . \tag{3}$$

Hint: Say you have an arbitrary function $g(x)$ and you want to calculate $\sum_x g(x)$. How to rewrite this sum into two sums $\sum_{l,k} g(kP+l)$? Apply this separation to use the periodicity to simplify the expression.

2 Factorization Algorithm .... [6P]

In the lecture a prime factoring algorithm has been presented. Apply this algorithm to $N = 35$. To simplify it: Choose in the first step a random m where the order is less than 10.

3 RSA Cryptosystem .... [5P]

Show in thin mini-example how the RSA cryptosystem works by encrypting the message "13" with $N = pq = 15$ and the random number $e = 3$ and decoding it again.

4 Josephson Junction . . . . [12P]

One possible building block for the realization of quantum computers are Josephson junctions. Here, we would like to derive the Hamiltonian describing the Josephson junction starting with the Josephson equations

$$\frac{\mathrm{d}Q}{\mathrm{d}t} = -I_{\text{ext}} + I_c \sin(\phi) \;, \tag{4}$$

$$\frac{\mathrm{d}\phi}{\mathrm{d}t} = -\frac{2e}{\hbar} V \;, \tag{5}$$

where $Q = -2eN = CV$, $-e$ the electron charge, $\phi = \theta_2 - \theta_2$ the difference in the phases of the order parameters, N the number of Cooper pairs, I_c the critical current and I_{ext} the external current.

(a) Write down the Euler-Lagrange equation which follows from the Josephson equations and deduce the Lagrangian L. *Hint: Recall that the electrostatic energy is given by $CV^2/2$.*

(b) Write down the classical Hamiltonian function. What is the meaning of the conjugate momentum π to ϕ?

(c) By imposing the canonical commutation relation $[\pi, \phi] = \hbar/i$ show that we end up with the Hamiltonian

$$H = -\frac{E_C}{2} \frac{\mathrm{d}^2}{\mathrm{d}\phi^2} - E_J \cos(\phi) - E_J \frac{I_{\text{ext}}}{I_c} \phi \;. \tag{6}$$

(d) What are the general solutions of Eq. (6) if $I_{\text{ext}} = 0$?