ETH Zürich, Dept. Informatik
WS 03/04

Lecturer: Jonathan Poritz

Introduction to Quantum Computation
Übung 8

16.01.2004

8.1 Convince yourself that the circuit given in class for the QFT does indeed compute the QFT.

8.2 Write out a formula for the Fourier transform in the group $G = (\mathbb{Z}_2)^n$, like the formula we had for the FT in $\mathbb{Z}_n$.

8.3 Prove *the orthogonality relations for characters of a finite Abelian group*, that is: if χ and χ' are distinct characters, then $\langle\chi|\chi'\rangle = 0$, while if n is the order of the group, then $\langle\chi|\chi\rangle = n$ for any character χ.

8.4 Working with the definition of the general Fourier transform in finite Abelian groups given in class, prove *Parseval's Identity*, that $\left\|\hat{f}\right\| = \|f\|$.

8.5 Check the formula

$$|1\rangle = \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1}|u_j\rangle$$

given in class during our work with the phase estimation algorithm.

8.6 Show that the operator

$$U(|y\rangle) = |xy(modN)\rangle$$

defined in class for $x \in \mathbb{Z}_N^*$ is unitary.

8.7 Let $N = p_1^{e_1} \dots p_k^{e_k}$ be the prime factorization of an odd number N, and x a (uniformly) randomly chosen element in $\mathbb{Z}_N^*$. Read up on the Chinese Remainder Theorem in [**S**] or [**NC**], Appendix 4. Prove that there is an isomorphism

$$\mathbb{Z}_N^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \dots \times \mathbb{Z}_{p_k^{e_k}}^*$$

What does this mean about choosing a single (uniformly) random element in the group on the left or k elements from the groups on the right?