

1. Suppose you are given quantum circuits C_i for computing the Fourier transform mod n_i for $i = 1$ to k where the n_i are pairwise relatively prime. Give a quantum circuit for computing the Fourier transform mod N where $N = n_1 \cdot n_2 \cdots n_k$. Bound the size of the resulting circuit in terms of N and the sizes of the given circuits C_i .
2. Let $a|q$ and $b|q$. What is the Fourier transform mod q of the uniform superposition on all $0 \leq x < q$ such that $a|x$ or $b|x$.
3. Recall the experiment demonstrating Bell inequality violations: Alice and Bob share entanglement and on input bits a and b output bits x_A and x_B such that $a \cdot b = x_A + x_B \pmod{2}$ with probability greater than $3/4$.
 - Show that if Alice and Bob could output x_A and x_B satisfying the above condition with certainty, then Bob could reconstruct a without any communication from Alice, thus achieving superluminal communication.
Hint: suppose Bob sets his input b to be a superposition of $|0\rangle$ and $|1\rangle$.
 - Now consider the generalization where the inputs a and b are numbers mod N , and Alice and Bob output x_A and $x_B \pmod{N}$ such that $a \cdot b = x_A + x_B \pmod{N}$. Prove that if Alice and Bob can achieve this with certainty then Bob can reconstruct a without any communication from Alice.
4. Suppose there are K solutions in the table of N items. Analyze the running time of Grover's algorithm for picking a uniformly random solution among the K possibilities.
Now give a quantum algorithm for finding the minimum element in a list of N numbers.
5. Suppose you are given a 2^k -to-1 function $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ such that there exist n -bit strings a_1, \dots, a_k , such that for all $x \in \{0, 1\}^n$ and for $1 \leq i \leq k$, $f(x + a_i) = f(x)$. What information about the a_i 's can we hope to reconstruct from f ? Cast this as an instance of the hidden subgroup problem. What is the underlying group G . What is the hidden subgroup H ? Work out the details of the algorithm (including the classical reconstruction).