CORR 2003-02

Exact quantum Fourier transforms and discrete logarithm algorithms

Michele Mosca and Christof Zalka

Abstract We show how the quantum fast Fourier transform (QFFT) can be made exact for arbitrary orders (first for large primes). For most quantum algorithms only the quantum Fourier transform of order 2^n is needed, and this can be done exactly. Kitaev [9] showed how to approximate the Fourier transform for any order. Here we show how his construction can be made exact by using the technique known as "amplitude amplification". Although unlikely to be of any practical use, this construction e.g. allows to make Shor's discrete logarithm quantum algorithm exact. Thus we have the first example of an exact non black box fast quantum algorithm, thereby giving more evidence that "quantum" need not be probabilistic.

We also show that in a certain sense the family of circuits for the exact QFFT is uniform. Namely the parameters of the gates can be calculated efficiently.