

Amplitude Amplification and Applications

Peter Høyer (hoyer@cpsc.ucalgary.ca)

University of Calgary

Department of Computer Science

Calgary, Alberta

T2N 1N4, Canada

Abstract.

Not only is amplitude amplification a beautiful mathematical statement about quantum algorithmics, it is also a very general, intuitive and useful concept. Next to the quantum Fourier transform, it is probably the most used tool in quantum algorithms. For any quantum state constructible by an algorithm, amplitude amplification provides us with a method for driving that state into another more desirable state.

Amplitude amplification generalizes ideas used in Grover's algorithm, as presented on Tuesday by Alain Tapp. In Grover's algorithm, we start with an initial state $|0\rangle$ and then drive that state to the desirable state $|x\rangle$ for which $F(x) = 1$, as described in Tapp's abstract. We start by reconsidering those ideas, and recast them in terms of amplitude amplification. We then discuss some of the many applications of amplitude amplification, including determining whether or not a given function is one-to-one.