Measurement Error in KSV Phase Estimation

Paul Pham

May 23, 2012

In this note, we provide a detailed calculation for the error in phase estimation due to Kitaev, Shen, and Vyalyi (KSV) where projective measurement is used instead of a coherent measurement. We show an increase from $2\sqrt{\epsilon}$ to $\sqrt{2}\sqrt[4]{\epsilon}$. The use of projective measurement is to offload many trigonometric operations onto a classical controller instead of doing them reversibly on a quantum computer. The cost of projective measurement is leaving garbage qubits in the ancillae of the target register, but this is a constant amount relative to the size of circuits we may wish to compile using the KSV procedure. Our goal is to show that this increase in error by a square root factor is negligible and may be preferrable in realistic implementations.

To begin with, we review (coherent) measurement operators as a generalization of controlled quantum operators, and then we further extend them to the case of approximately measuring functions on orthogonal basis decompositions where there are garbage bits left over in an ancillary register which must be uncomputed. Next, we calculate the error of this approximate measurement with ancillae. Then, we show how this general measurement procedure corresponds to estimating the phase of the modular multiplication operator used in Shor's factoring algorithm. Finally, we show that the error only increases by a square root factor when we projectively measure the garbage in the ancillae instead of coherently simulating the measurement.

1 Measurement Operators

First we introduce some preliminary definitions related to measurement.

A very common quantum operation entangles the results of one register (called the *target*) based on the value of another register (called the *control*). The most basic case of this is CNOT, or $\Lambda(X)$, operator, which operates on a control register of one qubit and a target register of one qubit.

$$\Lambda(X)\,|y,z\rangle \to |y,z\oplus y\rangle \tag{1}$$

We have two ways of describing how CNOT is measuring in this case. We can say CNOT is *measuring with respect to the decomposition* of the control

registers, namely the computational basis, in that the operation on the target register (flipping the bit) depend on decomposing the control register in the basis $\{0,1\}$. We can also say that CNOT is *measuring a function* $f : \{0,1\} \to \{0,1\}$ which in this case is simply the copy operator, $f(x) = x$. We can rewrite the equation above as:

$$\Lambda(X) \left|y, z\right\rangle \to \left|y, z \oplus f(y)\right\rangle \tag{2}$$

However, we know that the distinction between control and target registers often depends on a particular basis. For example, we can flip the direction of control and target in the CNOT case by conjugating both qubits with Hadamard operators. The general characteristic of measurement operators is that they are entangling, and that they can encode information about one register in another in a very general way. From the point of view of measurement, we call the control register the *object*, as in the state we are trying to measure, and the target register is the *instrument*, as in the state that we transform according to projecting the measurement object in some orthogonal decomposition.

Let's begin with a simple but more general case of a measuring operator W which operates on a space decomposed into the subsystems $\mathcal{N}$ (the measurement object) and $\mathcal{K}$ (the measurement instrument) according to the orthogonal decomposition $\mathcal{N} = \bigoplus_j \mathcal{L}_j$, so-called because each of the $\mathcal{L}_j$ are pairwise orthogonal subspaces. W will perform a different unitary operator U_j on the subsystem $\mathcal{K}$ depending on the projection of $\mathcal{N}$ into each $\mathcal{L}_j$.

$$W = \sum_{j \in \Omega} \Pi_{\mathcal{L}_j} \otimes U_j \tag{3}$$

An interesting fact about this definition of measurement operators is that approximativeness is preserved. If each unitary U_j is replaced with another unitary $\tilde{U}_j$ that approximates it with precision δ, then the new measuring operator $\tilde{W}$ also approximates the original W with the precision δ.

This precision is defined in terms of the inner product between any state $\left|\zeta\right\rangle$ operated on by W and by $\tilde{W}$. We can decompose $\left|\zeta\right\rangle$ into two subsystems $\left|\psi\right\rangle$ and $\left|\phi\right\rangle$ corresponding to the spaces $\mathcal{N}$ and $\mathcal{K}$ above. We will use this fact later.

$$\left\langle\zeta\right| W^\dagger \tilde{W} \left|\zeta\right\rangle = \left\langle\psi\right| \otimes \left\langle\phi\right| W^\dagger \tilde{W} \left|\psi\right\rangle \otimes \left|\phi\right\rangle = \sum_{j \in \Omega} \left(\left\langle\psi\right| \Pi_{\mathcal{L}_j} \left|\psi\right\rangle \otimes \left\langle\phi\right| U_j^\dagger \tilde{U}_j \left|\phi\right\rangle \right) \leq \delta \tag{4}$$

2 Operators That Measure a Function

We now introduce the idea that an operator can measure a function from the indices of the measurement object space $\mathcal{N}$ to the measurement instrument

space $\mathcal{K}$ with respect to some fixed orthogonal decompositions of these spaces.

$$\mathcal{N} = \bigotimes_{j \in \Omega} \qquad \mathcal{K} = \bigotimes_{y \in \Delta} \qquad f : \Omega \to \Delta \tag{5}$$

Saying that an operator Y is measuring with respect to a fixed orthogonal decomposition Ω is equivalent to saying that Y measures the function f, which need not even be reversible. The simplest, but not the most general, form of such an operator projects the first subsystem $\mathcal{N}$ into a subspace $\mathcal{L}_j$ and performs the corresponding operation $Q_{f(j)}$ on the second subsystem $\mathcal{K}$. In Equation 6, we define Y as the sum of these projectors, and our notation means it operates on the space of $\mathcal{N}$ tensored with $\mathcal{K}$.

$$Y = \sum_{j \in \Omega} \Pi_{\mathcal{L}_j} \otimes Q_{f(j)} : \mathcal{N} \otimes \mathcal{K} \tag{6}$$

3 Measurement Operators with Ancillae

However, this is not the most general case of a measurement operator. We make *three extensions* here which require cascading two rounds of measurement through an ancillary register. We now define a new composite measurement operator $\tilde{Y}$ on this space with three subsystems corresponding to the input register $\mathcal{N}$, the intermediate ancillary register $\mathcal{B}^N$, and a final output register $\mathcal{K}$ which approximates Y from Equation 6.

$$\tilde{Y} : \mathcal{N} \otimes \mathcal{B}^N \otimes \mathcal{K} \tag{7}$$

We will build up to an operational definition of $\tilde{Y}$ later, but first we must motivate what it must achieve.

In the first round, we measure with our object in $\mathcal{N}$ and our instrument in $\mathcal{B}^N$. Here we allow for garbage, which is our first extension, described in 3.1. In the second round, we measure with our object being the instrument of the first round, in $\mathcal{B}^N$, and our instrument is in $\mathcal{K}$. Here we allow for operations other than just copying from $\mathcal{B}^N$ to $\mathcal{K}$, which is our second extension, described in 3.2. Finally, instead of implementing our ideal Y directly, we allow ourselves, and quantify what it means, to approximate it as $\tilde{Y}$.

3.1 First Extension: Measurement with Garbage

To motivate why we need this new composite measurement Y instead of just using W directly from the previous section, let's consider the problem of garbage. In general, only some of the information computed by W into its target register $\mathcal{K}$ above may be useful, but we generate some garbage qubits

(say, to make the operation reversible). To be concrete, let's say that we have the following:

$$W : \mathcal{N} \otimes \mathcal{B}^N = \sum_{j \in \Omega} \Pi_{\mathcal{L}_j} \otimes U_j \qquad U_j : \mathcal{B}^N \to \mathcal{B}^N \qquad U_j \left|0\right\rangle = \sum_{y,z} c_{y,z}(j) \left|y, z\right\rangle \tag{8}$$

where $y \in \mathbb{B}^m$ represents the useful part of the result, $z \in \mathbb{B}^{N-m}$ is garbage, and the complex weights $c_{y,z} \in \mathbb{C}$ are functions of the index of the orthogonal decomposition of $\mathcal{N}$, the number j. In many cases, we would like to uncompute this garbage in order to use space efficiently. We can do this using an uncomputing trick due to Charlie Bennett [1] by first running an operation U which may produce garbage, copying out the useful part of the result to a second register, and finally running $U^\dagger$ to uncompute the input register.

Now we will give a more concrete definition for Y in terms of W and the operation V which simply copies a state $|\psi\rangle \in \mathcal{B}^N$ from the ancillary register to a state $|\phi\rangle \, in \mathcal{K}$ in the output register using bitwise CNOTs, or bitwise addition modulo 2^n for an n-qubit register. Then $Y = W^{-1}VW$, where W is our operator from above which computes a function with garbage, V is our copy operation, and W^{-1} uncomputes the original function and it garbage. We make this more rigorous in Equation 11.

$$Y = WVW^{-1} : \mathcal{N} \otimes \mathcal{B}^N \otimes \mathcal{K} \tag{9}$$

$$W = \sum_{j \in \Omega} \Pi_{\mathcal{L}_j} \otimes U_j \otimes I_{mathcalK} \tag{10}$$

$$V : |x\rangle \otimes |y\rangle \otimes |z\rangle \to |x\rangle \otimes |y\rangle \otimes |z \oplus y\rangle \tag{11}$$

3.2 Second Extension: Measurement with a Non-Copy Operation

Our notion of measurement with garbage is still not the most general it could be. For example, there is no reason why the decomposition of $\mathcal{K}$ has to be the same as that for $\mathcal{B}^N$ or $\mathcal{N}$, or why we are limited to strictly copying the useful output from $\mathcal{B}^N$ into $\mathcal{K}$. We don't need to limit the function f measured by W to be invertible. Furthermore, for practical reasons, there may be a more efficient way of encoding the useful part of f's output, or we may need to do further processing on it as part of the algorithm we want to run.

To allow this, in this section, we allow an arbitrary orthogonal decomposition $\mathcal{K} = \bigotimes_{y \in \Delta} \mathcal{M}_y$. This is the same as allowing V to be an arbitrary sum of projectors onto $\{\mathcal{M}_y\}$ and corresponding unitary operators Q_y on $\mathcal{K}$.

$$V = \sum_{y \in \Delta} I_{\mathcal{N}} \otimes Q_y \otimes \Pi_{\mathcal{M}_y} \tag{12}$$

3.3 Third Extension: Approximate Measurement

We can now allow a very general form of measurement which allows garbage, non-copying uncomputation, and finally, approximating a function. We will explain this last feature in this section.

We review that in the last two subsections we have been building up a composite measurement operator $\tilde{Y} = W^{-1}VW$ which consists of these two operations on a space with three subsystems.

$$W = \sum_{j \in \Omega} \Pi_{\mathcal{L}_j} \otimes R_j \otimes I_{\mathcal{K}} \qquad V = \sum_{y \in \Delta} I_{\mathcal{N}} \otimes \Pi_{\mathcal{M}_y} \otimes Q_y \tag{13}$$

We now reveal that $\tilde{Y}$ approximates Y from Equation 6. What does this mean? It means that the conditional probabilities of getting a given output index $y \in \Delta$ given an input index $j \in \Omega$, namely $P(y \mid j) = \left\langle 0^N \right| R_j^\dagger \Pi_{\mathcal{M}_y} R_j \left| 0^N \right\rangle$ satisfies Equation 15.

$$P(f(j) \mid j) \quad \geq \quad 1 - \epsilon \tag{14}$$

$$\sum_{y \neq f(j)} P(y \mid j) \quad < \quad \epsilon \tag{15}$$

References

[1] Charles Bennett: Logical Reversibility of Computation. *Atomic Energy*, (November), 1973.