Information and Computation
ACADEMIC PRESS

John H. Reif, On the Impossibility of Interaction-Free Quantum Sensing for Small I/O Bandwidth, Published in *Information and Computation*, Jan 2000, pp. 1-20.

On the Impossibility of Interaction-Free Quantum Sensing for Small I/O Bandwidth[1]

John Reif

Computer Science Department, Duke University, Durham, North Carolina 27708-0129
E-mail: reif@cs.duke.edu

A method for (*nearly*) *interaction-free measurement* (*IFM*) specifies the design of a quantum optical sensing system that is able to determine with arbitrarily high likelihood if an obstructing body has been inserted into the system, without moving or modifying its optical components, and uses at most an arbitrarily small multiplicative factor of the input intensity to do the sensing when the obstructing body is present. Kwiat *et al.* (1995, *Phys. Rev. Lett.* **74**, 4763–4766) have given a method for IFM. We give a precise mathematical formulation of IFM and as an example, we use this formulation to specify the IFM method of Kwiat *et al.* We similarly define (*nearly*) *interaction-free sensing* (*IFS*), except that we impose an upper bound on the intensity to do the sensing (which again is an arbitrarily small multiplicative factor of the input intensity) whether or not the obstructing body is present. A quantum optical method for IFS (but not IFM) may be used to do I/O with bandwidth reduced by an arbitrarily small multiplicative factor of the bandwidth required for conventional optical or electronic I/O methods (i.e., without using quantum effects). We prove that there is no method for IFS with unitary transformations. Hence we conclude that I/O bandwidth can not be significantly reduced by such quantum methods for sensing. This is one of relatively few known proofs of the non-existence of a class of quantum devices (e.g., for instantaneous communication and EPR) and apparently the first for a quantum device relevant to computational I/O bandwidth. We use an interesting proof method, where we first show that no unitary transformation can do *quantum amplification detection*: that is, significantly increase the amplitude on detection of a small amplitude basis state. Then we show that the existence of a method for IFS implies a unitary quantum amplification detection method, which is impossible.

---

[1] A postscript preprint of this paper is online at http://www.cs.duke.edu/~reif/paper/quantum.ps. Supported by Grants NSF/DARPA CCR-9725021, CCR-96-33567, and NSF IRI-9619647 and ARO Contract DAAH-04-96-1-0448. A postscript version of this paper is at http://www.cs.duke.edu/~reif/paper/qsense/qsense.ps.

1. INTRODUCTION

1.1. Quantum Sensing Systems

A (*quantum optical*) *sensing system* is a quantum optical system that is able to determine if an obstructing body has been inserted into the system, without moving or modifying the optical components (e.g., components such as mirrors and lenses) during sensing. If the obstructing body has been inserted into the system, then it is always inserted in the same way, forming obstructions in the same locations. Such a sensing system should be *explicitly specified* by providing unitary matrices (which may be infinite dimensional) defining the unique unitary transformations done by the sequence of individual quantum optic components comprising the sensing system. For any ε, ε_0, $\varepsilon_1 > 0$, where $0 < \varepsilon_0$ and $0 < \varepsilon$, $\varepsilon_1 < 1$, let an $(\varepsilon, \varepsilon_0, \varepsilon_1)$-*sensing system* be a quantum optical sensing system that provides output that determines, with likelihood $\geqslant 1 - \varepsilon$, if an obstructing body has been inserted into the system, and furthermore, if the obstructing body is not present uses at most a multiplicative factor ε_0 of the input intensity to do sensing (note that ε_0 may be above 1 if repeated sensing is done when the obstructing body is not present), and otherwise if the obstructing body is present, sends at most a multiplicative factor ε_1 of the input intensity into the obstructing body.

A method for (*nearly*) *interaction-free measurement* (*IFM*) specifies for any arbitrarily small ε, ε_1, for $0 < \varepsilon$, $\varepsilon_1 < 1$, the design of an $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system for some $\varepsilon_0 > 0$. Elitzur and Vaidman [EV93] gave an (1/2, 1/2, 1/2)-sensing system. Kwiat *et al.*, [KWZ95] (see also [KWZ96]) gave an ingenious method for IFM, using the "quantum Zeno effect" to do the sensing in multiple stages. Their $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system was experimentally demonstrated [KWZ95] up to moderate ε_1 and ε.

Kwiat *et al.* [KWZ96] claim applications of their IFM method to photography. However, the definition of IFM imposes no upper bound on ε_0; that is, there is no required upper bound on the intensity to do the sensing if the obstructing body is not present. In particular, the $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system of [KWZ95] for IFM allowed for arbitrarily small ε, $\varepsilon_1 > 0$, with $\varepsilon = O(\varepsilon_1)$, but required ε_0 to grow as c/ε_1 for a constant $c \geqslant 1/2$. Hence to achieve small ε_1, their IFM method requires large ε_0 (for example, for $\varepsilon_1 = 1/1000$, their IFM method requires $\varepsilon_0 > 500$). This growth in ε_0 appears to be (but had not been proved to be) unavoidable using techniques based on the quantum Zeno effect. Thus IFM can have applications such as photography only in the quite restricted case where the sensing can be repeatedly done when the obstructing body is not present (e.g., transmissive photography with a large number of repeated transmissions).

1.2. I/O Bandwidth Applications of Quantum Sensing

The recent interest in quantum effects by computer scientists has centered on the use of quantum parallelism for cryptography (see [BBE92] for a survey) to quickly solve problems (e.g., factoring large numbers [S94, S97]) otherwise considered intractable in conventional models of computation. However, the existence of a device for IFS may have major applications in computer science that would conceivably outstrip even those quantum computing applications. The I/O bandwidth is a critical issue for many computer systems, including:

- memory systems, such as for disk and tape drives,
- pad-limited VLSI systems, and
- communication systems on bandwidth limited parallel networks.

For I/O bandwidth applications, we can associate 1 with the case where the obstructing body is present and associate 0 with the case where the obstructing body is not present. The I/O bandwidth is determined by the total amplitude of the sensed bits, where the cost of sensing a bit is charged the same, whether or not it is 0 or 1. Since IFM provides only bounds on the sensing used to detect 1 but provides no bound on the sensing used to detect 0, IFM does not seem to be useful for decreasing I/O bandwidth. Thus there remained the question of designing a sensing system with also small ε_0.

A method for (*nearly*) *interaction-free sensing* (*IFS*) specifies the design of an $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system for arbitrarily small ε, ε_0, $\varepsilon_1 > 0$. A quantum optical method for IFS may be used to do I/O, where the receiver uses the sensing system to obtain the data from the sender. As discussed at the end of Section 4, IFS allows reduction of the bandwidth by a multiplicative factor of $\max(\varepsilon_0, \varepsilon_1)$ of the bandwidth required for conventional methods (i.e., without using quantum effects) for optical or electronic I/O.

1.3. Our Results

We provide a precise mathematical definition of a quantum sensing system, specifying how the sequence of unitary transformations, corresponding to optical components and sensing, are to be composed (the previous papers on IFM did not do this explicitly), and so formulate the IFM and IFS problems in mathematical terms. As an example, we briefly explain how the experimental quantum optical system of [KWZ95] for IFM can be described in our mathematical formulation for a quantum sensing system, and further explain why it is not an IFS system.

Our paper resolves the question of existence of IFS by a proof that there is no $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system using unitary transformations (which may be infinite dimensional), if $\varepsilon_0 < \min(1, (\sqrt{1-\varepsilon} - \sqrt{\varepsilon})^2)/2$. This condition holds for any given $\varepsilon < 1/2$ and sufficiently small ε_0, so there is no method for IFS with unitary transformations. This is one of relatively few known proofs of the non-existence of a class of quantum devices (e.g., for instantaneous communication and EPR). The only known previous negative result relevant to computational I/O bandwidth was that of Holevo [H73] (also see Fuchs and Caves [FC94]), who proved that quantum methods cannot increase the bandwidth for transmission of classical information.

We use an interesting proof method. We first show that no unitary transformation can do *quantum amplification detection*[2]: that is, significantly increase the amplitude on detection of a small amplitude basis state.

Our proof then assumes, for the sake of contradiction, the existence of a method for IFS for appropriate choice of parameters $\varepsilon, \varepsilon_0$, and proceeds by transforming the given $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system into a single unitary transformation that does quantum amplification detection, which we have already proved cannot be done.

1.4. Organization of This Paper

In Section 1, we discuss previous work, our new results, and the organization of our paper. In Section 2, we give preliminary definitions. In Section 3, we prove that amplification detection of quantum amplitudes is generally not possible by use of unitary transformations. In Section 4, we give a precise mathematical definition of a quantum sensing system, and in particular of IFM and IFS. As an example, we use our definition to describe the IFM method of [KWZ95]. We also discuss applications of IFS to decreasing I/O bandwidth. In Section 5, we show that IFS implies a method for quantum amplification detection. Hence we conclude that IFS cannot be done by use of unitary transformations. Section 6 concludes the paper. In the Appendix (Section 7), we give a proof of the initialization of certain unitary transformations for our simulation of sensing.

2. PRELIMINARY DEFINITIONS

The *magnitude* of a complex number z is denoted $|z|$ and the *intensity* the square of its magnitude. Hereafter in this paper, we assume a fixed orthonormal basis to describe the states via superpositions. We use the term *basis state* to denote a member of this particular chosen orthonormal basis, and use the *Dirac notation* $|s\rangle$ to designate a basis state. Each quantum system considered in this paper is assumed to have a (possibly infinite) set of basis states S. At a given time, the *superposition state* of the quantum system is a linear superposition of basis states given by a mapping α from S to the complex numbers, such that $1 = \sum_{|s\rangle \in S} |\alpha(s)|^2$, that is, the intensities of the amplitudes of all the elements of S sum to 1. Each basis state $|s\rangle \in S$ is thus assigned by α a complex number $\alpha(s)$ which we call its *amplitude*. The *Dirac sum notation* $\sum_{|s\rangle \in S} \alpha(s)\, |s\rangle$ is used to denote a linear superposition of basis states. The sum $\sum_{|s\rangle \in S} |\alpha(s)|^2$ of the intensities of the amplitudes

[2] Brassard *et al.* [BH98, BHT98] show that quantum amplification is possible if a small amplitude basis state always exists, whereas in quantum amplification detection as defined here, we also need to detect that a small amplitude basis state does not exist. Note also that the term quantum amplification has other definitions in other distinct contexts (e.g., quadrature amplification and photon number amplification) but the relation of quantum amplification and the uncertainty relation seems to have been well worked out in those other contexts only in the case where we do not also need to detect that a small amplitude basis state does not exist.

of the elements of S remain invariant due to the application of a unitary transformation.[3]

As in the IFM apparatus of the paper [KWZ95], we assume that the observation of the final output of the quantum system triggers a quantum projection (also sometimes known as a quantum collapse) to a single output basis state, chosen with probability equal to the intensity of its output amplitude. (This assumption does not limit the generality of our results, since Bernstein and Vazirani [B93, BV97] showed that all observation operations can be pushed to the end of the computation, by repeated use of a quantum XOR gate construction.)

3. QUANTUM AMPLIFICATION DETECTION IS NOT POSSIBLE

3.1. Definition of Quantum Amplification Detection

Fix some real $\mathscr{A}$, β, β', for $0<\beta$, $\beta'<1$ and $1<\mathscr{A}\leqslant 1/\beta$. Let a *quantum* $(\mathscr{A}, \beta, \beta')$*-amplification* system be a unitary transformation defined as follows:

- There are distinguished basis states $|s_{POWER}\rangle$, $|s_{TEST}\rangle$ initially with amplitudes a_{POWER}, a_{TEST}, respectively, and we assume that all other elements in S initially have amplitude 0. In Dirac notation, the initial superposition state is $a_{POWER}\,|s_{POWER}\rangle + a_{TEST}\,|s_{TEST}\rangle$.
- There is also a distinguished basis state $|s_{OUTPUT}\rangle$; let a_{OUTPUT} be the amplitude of $|s_{OUTPUT}\rangle$ on output.
- We require that any quantum $(\mathscr{A}, \beta, \beta')$-amplification system satisfy the following restrictions:

— If $a_{POWER}=1$ and $a_{TEST}=0$ (so the initial superposition state is $1\,|s_{POWER}\rangle$), then $|a_{OUTPUT}|\leqslant\sqrt{\beta'}$. Hence in this case, if we observe the basis state of the system on output to be $|s\rangle$, $\text{Prob}(s_{OUTPUT}=s)\leqslant\beta'$.

— If $a_{POWER}=\sqrt{1-\beta}$ and $a_{TEST}=\sqrt{\beta}$ (so the initial superposition state is $\sqrt{1-\beta'}\,|s_{POWER}\rangle+\sqrt{\beta}\,|s_{TEST}\rangle$), then $|a_{OUTPUT}|\geqslant\sqrt{\mathscr{A}\beta}$. Hence in this case, if we observe the basis state of the system on output to be $|s\rangle$, $\text{Prob}(s_{OUTPUT}=s)\geqslant\mathscr{A}\beta$.

For example, a quantum $(\mathscr{A}, \beta, \beta)$-amplification system essentially amplifies, by a factor $\mathscr{A}$, the likelihood of observing a given basis state.

3.2. Impossibility of Quantum Amplification Detection

THEOREM 3.1. *There is no unitary transformation that does quantum* $(\mathscr{A}, \beta, \beta')$*-amplification, if*

$$|\sqrt{\mathscr{A}}-\sqrt{(1-\beta)\,\beta'/\beta}|>1,$$

for $0<\beta$, $\beta'<1$ *and* $1<\mathscr{A}\leqslant 1/\beta$.

[3] For example, a class of unitary matrices, known as *permutation matrices*, have exactly one 1 on every row and column, with all other entries 0. Also, the following 2×2 unitary matrices are sometimes known as *rotation matrices*: $\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}$. We will frequently use their generalization to arbitrary size unitary matrices that have a submatrix which is a rotation matrix applied to a pair of basis states, and with the remaining portion of the transformation being an identity map on the other basis states.

Proof. Given the linear property of unitary transformations, $a_{OUTPUT} = c_1 a_{POWER} + c_2 a_{TEST}$, for fixed constants c_1, c_2. By the definition of a quantum $(\mathscr{A}, \beta, \beta')$-amplification system, we have:

- If $a_{POWER} = 1$ and $a_{TEST} = 0$ then $|a_{OUTPUT}| \leqslant \sqrt{\beta'}$, so $c_1 = a_{OUTPUT}/a_{POWER} = a_{OUTPUT}$ and $|c_1| \leqslant \sqrt{\beta'}$.
- Also, if $a_{POWER} = \sqrt{1-\beta}$ and $a_{TEST} = \sqrt{\beta}$, then $|a_{OUTPUT}| \geqslant \sqrt{\mathscr{A}\beta}$, so

$$\begin{aligned}|c_2| &= |(a_{OUTPUT} - c_1 a_{POWER})/a_{TEST}| \\ &\geqslant |(\sqrt{\mathscr{A}\beta} - \sqrt{\beta'(1-\beta)})/\sqrt{\beta}| = |\sqrt{\mathscr{A}} - \sqrt{(1-\beta)\,\beta'/\beta}|.\end{aligned}$$

- On the other hand, if we set $a_{POWER} = 0$ and $a_{TEST} = 1$, then

$$|a_{OUTPUT}| = |c_1 a_{POWER} + c_2 a_{TEST}| = |c_2| \geqslant |\sqrt{\mathscr{A}} - \sqrt{(1-\beta)\,\beta'/\beta}|.$$

Thus, the output intensity is $\geqslant |a_{OUTPUT}| > 1$ if $|\sqrt{\mathscr{A}} - \sqrt{(1-\beta)\,\beta'/\beta}| > 1$. We have set the summed intensity of the input amplitudes of all basis states to be 1 and have shown that the output intensity can be > 1 for these settings of β, $\mathscr{A}$. So we conclude that for these settings, there is no unitary transformation that does quantum $(\mathscr{A}, \beta, \beta')$-amplification. ∎

There are many amplitudes for $\mathscr{A}$, β, β' such that $|\sqrt{\mathscr{A}} - \sqrt{(1-\beta)\,\beta'/\beta}| > 1$. Let $\beta^*(\mathscr{A})$ be the minimum real where $0 < \beta^* < 1$ and $|\sqrt{\mathscr{A}} - \sqrt{1-\beta^*}| > 1$. Thus, there is no unitary transformation that does quantum $(\mathscr{A}, \beta, \beta)$-amplification, for $0 < \beta^*(\mathscr{A}) \leqslant \beta$. Note, for example, since $\sqrt{1-\beta} \leqslant 1$, there is unitary transformation that does quantum $(4, \beta, \beta)$-amplification for any $0 < \beta < 1$.

4. QUANTUM SENSING SYSTEMS

Informally, a (*quantum optical*) *sensing system* is a quantum optical system that is able to determine if an obstructing body has been inserted at a given location into the system. One of the contributions of our paper is a mathematically precise definition of this concept and of interaction-free sensing. This section shows that any given quantum sensing system can be precisely specified by a sequence of unitary transformations of its individual quantum optical components.

4.1. A Precise Specification of a Quantum Sensing System

We will first give a terse, but complete, definition of an $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system. This definition will be motivated and explained in the subsection to follow.

DEFINITION. An $(\varepsilon, \varepsilon_0, \varepsilon_1)$-*sensing system*, for $0 < \varepsilon_0$ and $0 < \varepsilon_1$, $\varepsilon \leqslant 1$, is a sequence of n unitary transformations $U_1, \ldots, U_{n+1}$ over the amplitudes of a basis state set S such that:

FIG. 1. The unitary maps applied in case CLEAR.

• S contains as a subset distinguished basis states $\{|s_{INITIAL}\rangle, |s_{OUTPUT}\rangle\} \cup \{|s_{sense,\,j}\rangle, |s_{absorb,\,j}\rangle \mid j=1, ..., n\}$.

• For $j=1, ..., n+1$, each U_j provides an identity map on the basis states $|s_{absorb,\,1}\rangle, ..., |s_{absorb,\,n}\rangle$.

• For $j=1, ..., n$, each P_j is a unitary permutation that maps the basis states $|s_{sense,\,j}\rangle$ and $|s_{absorb,\,j}\rangle$ into each other (thereby interchanging the amplitudes of $|s_{sense,\,j}\rangle$ and $|s_{absorb,\,j}\rangle$), and provides an identity mapping on all the other elements of S.

• In the initial superposition, the amplitude of $|s_{INITIAL}\rangle$ is 1 and the amplitude of all other elements of S is 0.

• Case CLEAR (see Fig. 1):

— If we apply the sequence of unitary maps U_j, for $j=1, ..., n+1$, then the intensity of the final amplitude of $|s_{OUTPUT}\rangle$ is $\leqslant \varepsilon$, and

— the sum $\sum_{j=1}^{n} |\sigma_j|^2$ is upper bounded by ε_0, where each σ_j is the amplitude of $|s_{sense,\,j}\rangle$ just before the jth stage.

• Case OBSTRUCTION (see Fig. 2):

— If we apply the sequence of unitary maps U_j immediately followed by P_j, for $j=1, ..., n$, and finally apply U_{n+1}, then the intensity of the final amplitude of $|s_{OUTPUT}\rangle$ is $\geqslant 1-\varepsilon$.

— The sum $\sum_{j=1}^{n} |\sigma'_j|^2$ is upper bounded by ε_1, where each σ'_j is the amplitude of $|s_{sense,\,j}\rangle$ just before the jth stage.

4.2. Comparison between IFS and IFM

Recall that we have defined IFM and IFS as follows:

• A method for Ifs provides for the design of an $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system, given for any arbitrarily small ε, ε_0, $\varepsilon_1 > 0$ (e.g., by appropriately choosing a large enough number of sensing stages n). Observe that IFM imposes:

— an upper bound on ε_1 (that is, there is no upper bound on the intensity to do the sensing if the obstructing body is present), but

— no upper bound on ε_0 (that is, there is no upper bound on the intensity to do the sensing if the obstructing body is not present).

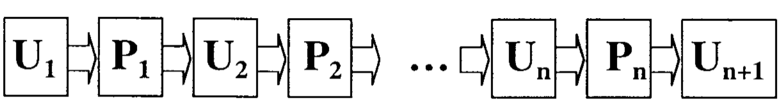

FIG. 2. The unitary maps applied in case OBSTRUCTION.

File: 643J 288007 . By:XX . Date:23:08:00 . Time:13:30 LOP8M. V8.B. Page 01:01
Codes: 3089 Signs: 1886 . Length: 52 pic 10 pts, 222 mm

• A method for IFM provides for the design of an $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system for some $\varepsilon_0 > 0$, for any arbitrarily small ε, $\varepsilon_1 > 0$. In contrast, observe that IFS imposes:

— an upper bound on both ε_1 and ε_0 (that is, there is an upper bound on the intensity to do the sensing whether or not the obstructing body is present).

4.3. *Physical Explanation of Our Definition of a Quantum Sensing System*

This subsection will provide a detailed physical explanation of our terse mathematical definition of an $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system, as given in Subsection 4.1 (and this will be followed in the next subsection by an example of how it can used to model an experimental quantum optical system). Each part of our definition will be motivated and precisely formulated from the perspective of our intended quantum optical sensing applications of IFS, in particular to decreasing the input/output (I/O) bandwidth. (Also, more recently, Gacs [G98] has developed a similar mathematical formulation of sensing systems.)

The State Set S and Their Initial Amplitudes. We assume that the sensing system is always provided a single input photon, and to denote this, we use the unique, distinct *initial basis state* $|s_{INITIAL}\rangle$ of unit amplitude in the initial superposition. We assume that the optical devices of the quantum sensing system are not modified by this photon. Thus, the other basis states of the quantum sensing system simply provide the subsequent possible locations for this photon within the sensing system. We define S to be a (possibly infinite size) set of basis states, which are positions of the photon within the quantum sensing system. Let us enumerate the elements of S in some (arbitrary) fixed order. Thus, unitary transformations on the amplitudes of the elements of S can be specified by unitary matrices[4] (which will be infinite dimensional if $|S|$ is infinite).

Enumerating the elements of S in the chosen fixed order, in the initial superposition we represent the amplitudes of the basis states by a (possibly infinite) $|S|$-vector α_0, where the initial basis state $|s_{INITIAL}\rangle$ has amplitude 1 and all elements of S have amplitude 0. In Dirac notation, α_0 gives $1\ |s_{INITIAL}\rangle$.

The Unitary Transformations of the Quantum Optical Components. Any quantum optical system must be specified by a sequence of unitary transformations (i.e., unitary matrices), done by the sequence of individual quantum optical components of their system. We assume that the sensing system uses a fixed number n of sensing stages (defined by unitary permutation matrices). Strictly between each sensing stage, there are fixed unitary transformations, done by a sequence of fixed quantum optic components of the system. Thus, if an obstructing body has been inserted into the system, it does not change or modify the individual quantum optical components[5] and instead obscures the channels at specified locations between

[4] For readers not familiar with quantum systems, note that each of the unitary transformations is viewed as a unitary matrix product, with the convention of applying the sequence of unitary transformations from right to left.

[5] Note that a sensing system must not modify its optical components during sensing. Hence we cannot model the insertion of an obstructing body simply by withdrawing a corresponding mirror, for then one has modified the sensing system during observation.

consecutive quantum optical components. (Note that the obscuring object is assumed not to be a quantum object.)

For each $j = 1, ..., n$ let U_j be the unitary transformation done strictly between the $j-1$ and jth sensing stage, and for $j = n+1$ let U_j be the unitary transformation done strictly after the nth sensing stage (that is, there is no sensing done via U_j). Note that none of these unitary transformations U_j are affected by the case of insertion of an obstructing device, since there is no sensing done strictly between sensing stages. Also note that to explicitly specify the sensing system, each U_j must be further specified by a product of a sequence of unitary transformations, corresponding to the individual quantum optical components, used strictly between the $j-1$ and jth sensing stage for $1 \leqslant j \leqslant n$, or used strictly after the nth sensing stage for $j = n+1$.

The Unitary Transformations Done on Sensing Stages. We also need to specify the unitary transformations done on each sensing stage. There are two cases:

1. *CLEAR*: the obstructing body has not been inserted into the system.
2. *OBSTRUCTION*: the obstructing body has been inserted into the system.

The unitary transformations done on sensing depend on these two cases. In case OBSTRUCTION, the obstructing body is always inserted into the system in the same way, forming obstructions in the same locations.

We define a unique, distinct basis state $|s_{sense,\, j}\rangle$ to denote the case of sensing for the obstructing body at a given fixed location on the jth sensing stage. We also define a unique, distinct basis state $|s_{absorb,\, j}\rangle$ to denote the case of absorption of an input photon by an obstructing body on the jth sensing stage. In both cases CLEAR and OBSTRUCTION, the jth sensing stage does not change the amplitudes for any other elements of S other than $|s_{sense,\, j}\rangle$ and $|s_{absorb,\, j}\rangle$.

In case CLEAR (where the obstructing body has not been inserted), the jth sensing stage does not change the amplitudes of any elements of S, including $|s_{sense,\, j}\rangle$ and $|s_{absorb,\, j}\rangle$. Thus, in case CLEAR, U_j in case CLEAR for $1 \leqslant j \leqslant n$ is exactly the unitary transformation done by the sensing system done just after the $j-1$ sensing stage up to and including the jth sensing stage, and for $j = n+1$, U_j is the unitary transformation done just after the nth sensing stage. Also in case CLEAR (since the obstructing body has not been inserted), we require that the input photon can never reach an absorbing basis state $|s_{absorb,\, j}\rangle$ (whereas in case OBSTRUCTION, the input photon may possibly reach an absorbing basis state $|s_{absorb,\, j}\rangle$). Thus, we require that each U_j provide an identity map on basis states $|s_{absorb,\, 1}\rangle, ..., |s_{absorb,\, n}\rangle$.

On the other hand, the case OBSTRUCTION (where the photon is absorbed by the obstructing body on the jth sensing stage), is represented by a transition from $|s_{sense,\, j}\rangle$ to $|s_{absorb,\, j}\rangle$. This case of absorption is irrevocable and may happen only in case OBSTRUCTION. (For simplicity and since it is not used by the proposed method of [KWZ95], we do not allow a more general scheme where the obstructing body could alter the state of the photon instead of absorbing it.) Hence the jth sensing stage is given by a unitary permutation matrix P_j that maps the states $|s_{sense,\, j}\rangle$ and $|s_{absorb,\, j}\rangle$ into each other (thereby interchanging the amplitudes of

$|s_{sense,\, j}\rangle$ and $|s_{absorb,\, j}\rangle$), and provides an identity mapping on all other elements of S. Thus, case OBSTRUCTION, for $1 \leqslant j \leqslant n$, $U'_j = P_j U_j$ (that is, U_j followed by P_j) is the unitary transformation done just after the $j-1$ up to and including the jth sensing stage, and for $j = n+1$, $U'_{n+1} = U_{n+1}$ is the unitary transformation done just after the nth sensing stage.

The Input–Output Unitary Transformation. The unitary transformation by the $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system, up to and including the j stage, written in matrix notation, is $T_j = U_j U_{j-1} \cdots U_2 U_1$ in case CLEAR, and is $T'_j = U'_j U'_{j-1} \cdots U'_2 U'_1$ in case OBSTRUCTION.

We conclude that the total input–output unitary transformation is $T_{n+1} = U_{n+1} U_n \cdots U_2 U_1$ in case CLEAR, and is $T'_{n+1} = U'_{n+1} U'_n \cdots U'_2 U'_1$ in case OBSTRUCTION.

Viewing each of the unitary transformation as matrix products, we can determine the amplitudes of the elements in S just after the jth sensing stage from the vector $T_j \alpha_0$ in case CLEAR and by $T'_j \alpha_0$ in case OBSTRUCTION.

The Output Parameters of a Sensing System. The additional basis state $|s_{OUTPUT}\rangle$ is intended to indicate case OBSTRUCTION. Fix some reals $\varepsilon, \varepsilon_0, \varepsilon_1$, where $0 < \varepsilon_0$ and $0 < \varepsilon, \varepsilon_1 < 1$ (note that ε_0 may be above 1, due to repeated sensing). We formally define an $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system to be a quantum optical sensing system that (a) determines, with likelihood $\geqslant 1-\varepsilon$, if an obstructing body has been inserted at a given location into the system, and furthermore to do this, (b) sends only a fraction $\varepsilon_0, \varepsilon_1$ of the input intensity to the locations of the obstructing body in case CLEAR, OBSTRUCTION, respectively. By (a), in case CLEAR, the intensity of the amplitude of $|s_{OUTPUT}\rangle$ just after the final $(n+1)$th stage is $\leqslant \varepsilon$. Also, by (a), in case OBSTRUCTION, the intensity of the amplitude of the basis state $|s_{OUTPUT}\rangle$ just after the final $(n+1)$th stage is $\geqslant 1-\varepsilon$. Thus, the $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system provides output as follows. We make (as is done in the IFM method of [KWZ95]) an observation of the final basis state $|s\rangle$ after the final $(n+1)$th stage, triggering a quantum projection to a single basis state. Then,

- $\mathrm{Prob}(s_{OUTPUT} = s) \leqslant \varepsilon$ in case CLEAR, and
- $\mathrm{Prob}(s_{OUTPUT} = s) \geqslant 1-\varepsilon$ in case OBSTRUCTION.

By (b), in case CLEAR, $\varepsilon_0 \geqslant$ the sum, for $j = 1, ..., n$, of the intensities of the amplitude of $|s_{sense,\, j}\rangle$ just before the jth sensing stage. Also by (b), in case OBSTRUCTION, $\varepsilon_1 \geqslant$ the sum, for $j = 1, ..., n$, of the intensities of the amplitude of $|s_{sense,\, j}\rangle$ just before the jth sensing stage.

4.4. *The IFM Method of [KWZ95]*

We now briefly explain how the experimental quantum optical system of [KWZ95] for IFM can be described in our mathematical formulation of quantum sensing systems (we thank Shor for his assistance here), and also explain why it is not an IFS system.

In their system, a photon is sent through a series of optical devices in n stages of sensing (see the excellent illustrations given in [KWZ96] for a visualization of the path of the photon). S consists of the set

$$\{|s_{INITIAL}\rangle, |s_{OUTPUT}\rangle\} \cup \{|s_{sense,\, j}\rangle, |s_{absorb,\, j}\rangle \mid j = 1, ..., n\}$$

of distinguished basis states of the photon, as described in the previous subsection. (Note: the quantum optical system of [KWZ95] happens to use polarization to encode certain basis states, but the details of the actual encoding of basis states is not critical to our discussion here.) In the initial superposition, the amplitude of $|s_{INITIAL}\rangle$ is 1 and the amplitude of all other elements of S is 0. This models how a single photon initially enters the system with the basis state $|s_{INITIAL}\rangle$.

The unitary matrices U_j, defined below for $j = 1, ..., n$, model ho the system of [KWZ95] executes each stage of sensing. In particular, the photon is sent through an optical beam splitter and phase rotation filter modeled by the rotation matrix $R_\theta = \left[\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right]$, where $\theta = \frac{\pi}{2n}$. (For simplicity, at the start of the first stage the amplitude of the basis state $|s_{INITIAL}\rangle$ is exchanged with that of the basis state $|s_{OUTPUT}\rangle$.)

- U_1 is the unitary matrix which is composed as follows:

  — it applies a unitary permutation that maps the basis states $|s_{INITIAL}\rangle$ and $|s_{OUTPUT}\rangle$ into each other (thereby interchanging the amplitudes of $|s_{INITIAL}\rangle$ and $|s_{OUTPUT}\rangle$),

  — then uses R_θ to map the pair of basis states $|s_{OUTPUT}\rangle, |s_{sense,\,1}\rangle$ to the pair of basis states $|s_{OUTPUT}\rangle, |s_{sense,\,1}\rangle$ (thereby mapping the pair of amplitudes of $|s_{OUTPUT}\rangle, |s_{sense,\,1}\rangle$ to the pair of amplitudes of $|s_{OUTPUT}\rangle, |s_{sense,\,1}\rangle$), and

  — provides an identity map on all other basis states.

- For $j = 2, ..., n$ each U_j is a unitary matrix which is composed as follows:

  — it applies a unitary permutation that exchanges the basis states $|s_{sense,\, j-1}\rangle$ and $|s_{sense,\, j}\rangle$ (thereby interchanging the amplitudes of $|s_{sense,\, j-1}\rangle$ and $|s_{sense}, j\rangle$),

  — then uses R_θ to map the pair of basis states $|s_{OUTPUT}\rangle, |s_{sense,\, j}\rangle$ to the pair of basis states $|s_{OUTPUT}\rangle, |s_{sense,\, j}\rangle$ (thereby mapping the pair of amplitudes of $|s_{OUTPUT}\rangle, |s_{sense,\, j}\rangle$ to the pair of amplitudes of $|s_{OUTPUT}\rangle, |s_{sense,\, j}\rangle$), and

  — provides an identity map on all other basis states.

- U_{n+1} is the identity matrix that provides an identity map on all basis states. (Note: U_{n+1} was included in our formulation of a quantum sensing system to allow for more generality, although in this particular method U_{n+1} does nothing.)

As described in detail in the previous subsection, the P_j matrices are used to model absorption in the case of OBSTRUCTION. Again, by our definition of quantum sensing systems:

- P_j is a unitary permutation that maps the states $|s_{sense,\, j}\rangle$ and $|s_{absorb,\, j}\rangle$ into each other (thereby interchanging the amplitudes of $|s_{sense,\, j}\rangle$ and $|s_{absorb,\, j}\rangle$), and provides an identity mapping on all the other elements of S.

This completes our description of how we model the optical components of the quantum optical system of [KWZ95]. After the final stage, the amplitude of $|s_{OUTPUT}\rangle$ is observed. It is easy to verify that this is an IFM system:

- In case CLEAR:

— If we apply the sequence of unitary maps $U_1, ..., U_j$, then since $(R_\theta)^j = R_{j\theta}$, it follows that the amplitudes of $|s_{OUTPUT}\rangle$, $|s_{sense,\, j}\rangle$ are $\cos(j\theta)$, $\sin(j\theta)$. Hence, after the nth stage, the amplitude of $|s_{OUTPUT}\rangle$ is $\cos(\pi/2) = 0$, and so after we apply U_{n+1}, the intensity of the final amplitude of $|s_{OUTPUT}\rangle$ is 0. Hence, the system indicates that it has detected that there is no obstacle by outputting a photon which is not in basis state $|s_{OUTPUT}\rangle$.

- Case OBSTRUCTION:

— If we apply the sequence of unitary maps U_j immediately followed by P_j, for $j = 1, ..., n$, then after each j stage, the amplitude of $|s_{OUTPUT}\rangle$ is $(\cos\theta)^j$, and so after we finally apply U_{n+1}, the intensity of the final amplitude of $|s_{OUTPUT}\rangle$ is $(\cos\theta)^{2n} \geqslant 1 - O(1)/n$ (this holds since $\cos\theta \geqslant 1 - \theta^2/2 = 1 - c/2n^2$ for $\theta = \pi/2n$ and $c = \pi^2/4$, and so $(\cos\theta)^{2n} \geqslant (1 - c/2n^2)^{2n} \geqslant e^{-c/n} \geqslant 1 - c/n$). Hence, the system indicates that it has detected that there is an obstacle by outputting (with high likelihood) a photon in basis state $|s_{OUTPUT}\rangle$.

— The sum, for $j = 1, ..., n$, of the intensities of the amplitude of $|s_{sense,\, j}\rangle$ just before the jt sensing stage, is $\varepsilon_1 \leqslant n(\sin\theta)^2 \leqslant O(1/n)$ (since $\sin\theta \leqslant O(\theta) \leqslant O(1/n)$), which can be made arbitrarily small for a large enough n. This bounds the likelihood of absorption of the photon.

Also in case CLEAR, it is easy to verify that the sum, for $j = 1, ..., n$ of the intensities of the amplitude of $|s_{sense,\, j}\rangle$ just before the jth sensing stage, is $\varepsilon_0 = \sum_{j=1}^{n} (\sin(j\theta))^2 \geqslant c'n$, for a constant $c' > 0$. Hence, due to the repeated sensing on the stages, ε_0 grows linearly with n, and so the method of [KWZ95] is certainly not an IFS system.

However, this method of [KWZ95] is only a single quantum system. Might another quantum optical system exist that simultaneously has small ε, ε_0, and ε_1? That is impossible, since Section 5 will prove that, in fact, there can be no IFS system.

4.5. The Reduced Bandwidth for I/O

A quantum optical method for IFS may be used to do I/O, as follows. We can assume w.l.o.g. that the I/O is originally bit serial (if it is in fact k-bit parallel, then the sensing system is simply replicated k times), using a conventional optical or electronic I/O method, without the use of quantum effects. The receiver uses an $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system to obtain the data from the sender bit by bit in serial fashion. The cost of sensing a bit is charged the same, whether or not it is 0 or1. Let us also assume w.l.o.g. that the CLEAR case is used to encode the bit 0 and the OBSTRUCTION case is used to encode the bit 1. Then when we transmit a 0 bit by use of the IFS system, the probability of actually sending the 0 bit over the I/O channel (i.e., of sensing in the CLEAR case) is reduced to ε_0. Also, when we transmit a 1 bit by use of the IFS system, the probability of actually sending the 1 bit over the I/O channel (i.e., of sensing in the OBSTRUCTION case) is reduced to ε_1. Hence, the probability of sending each bit over the I/O channel is reduced by a multiplicative factor of at least $\max(\varepsilon_0, \varepsilon_1)$ by use of the sensing system. Thus I/O bandwidth is reduced by a multiplicative factor of $\max(\varepsilon_0, \varepsilon_1)$ of the bandwidth required for conventional I/O.

5. A QUANTUM SENSING SYSTEM THAT IMPLIES QUANTUM AMPLIFICATION DETECTION

5.1. *Assumptions of the Reduction*

For the sake of contradiction, we now assume an $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system, for $0 < \varepsilon_0 < 1/2$ and $0 < \varepsilon < 1$. Let σ_j be the amplitude of the basis state $|s_{sense,\,j}\rangle$ just before the jth sensing stage in the case CLEAR. By the definition of an $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system, we have $\sum_{j=1}^{n} |\sigma_j|^2 \leqslant \varepsilon_0$. Without loss of generality, we assume $\varepsilon_0 = \sum_{j=1}^{n} |\sigma_j|^2$.

5.2. *Goals of the Reduction*

We construct from the $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system a unitary transformation that does quantum $(\mathscr{A}, \beta, \beta')$-amplification, for $\mathscr{A} = (1-\varepsilon)/2\varepsilon_0$, $\beta = 1 - 1/(1 + 2\varepsilon_0(1 - 2\varepsilon_0))$, and $\beta' = (1 - 2\varepsilon_0)\,\varepsilon$. To provide the contradiction, we later further restrict ε_0, ε to provide amplitudes of $\mathscr{A}$, β, β' to those for which quantum $(\mathscr{A}, \beta, \beta')$-amplification is impossible.

5.3. *The New State Set $\hat{S}$ and Their Initial Amplitudes*

Let S be the basis set defined in Subsection 4.3. We introduce distinct new basis states $|s_{POWER}\rangle$, $|s_{TEST}\rangle$ and fix a_{POWER}, a_{TEST}, respectively, to be their initial amplitudes. We also augment the basis state set with distinct new basis states $|s_{test,\,j}\rangle$, $|s_{power,\,j}\rangle$ for each $j = 1, ..., n$, initially with amplitude 0. Thus, the new basis state set is

$$\hat{S} = S \cup \{|s_{POWER}\rangle\} \cup \{|s_{TEST}\rangle\} \cup \{|s_{power,\,j}\rangle, |s_{test,\,j}\rangle \mid 1 \leqslant j \leqslant n\}.$$

Let $\gamma = \sqrt{1 - 2\varepsilon_0}$. Let $\hat{\alpha}_0$ be an $|\hat{S}|$-vector providing the initial assignment of the amplitudes of the element so $\hat{S}$ so that $a_{POWER} = \frac{1}{\gamma}$ and $a_{TEST} = 0$. Let $\hat{\alpha}_1$ be an $|\hat{S}|$-vector providing the initial assignment of the amplitudes of the elements of $\hat{S}$ so that $a_{POWER} = \frac{1}{\gamma}$ and $a_{TEST} = \sqrt{2\varepsilon_0}$. We assume that $\hat{\alpha}_0$, $\hat{\alpha}_1$ provide amplitude 0 to all other elements of $\hat{S}$. (Note that the total input intensity in these cases is > 1; later we will lower this total input intensity to 1.) Thus, in Dirac notation, $\hat{\alpha}_0$ gives $\frac{1}{\gamma}|s_{POWER}\rangle + 0\,|s_{TEST}\rangle$, and $\hat{\alpha}_1$ gives $\frac{1}{\gamma}|s_{POWER}\rangle + \sqrt{2\varepsilon_0}\,|s_{TEST}\rangle$. Note that in $\hat{\alpha}_0$ (and also in $\hat{\alpha}_1$), the sum of the intensities of the amplitudes do not sum up to 1; but the amplitudes will later be renormalized by Lemma 5.3.

5.4. The Initialization of Unitary Transformations for Simulation of Sensing

In the Appendix (Section 7), we prove a technical lemma:

LEMMA 5.1. *For* $\varepsilon_0 < 1/2$, *there is a unitary transformation* $\hat{T}_0$ *such that in* $\hat{T}_0 \hat{\alpha}_0$, *each* $|s_{test,\, j}\rangle$ *has amplitude* σ_j, *and in* $\hat{T}_0 \hat{\alpha}_1$, *each* $|s_{test,\, j}\rangle$ *has amplitude* 0. *Furthermore, basis state* $|s_{INITIAL}\rangle$ *has amplitude* 1 *in both* $\hat{T}_0 \hat{\alpha}_0$ *and* $\hat{T}_0 \hat{\alpha}_1$.

5.5. The New Unitary Transformations between and during Sensing Stages

For each $j = 1, ..., n+1$, let U_j be the unitary transformations of the quantum optical components of the given sensing system (as defined in Subsection 4.3). Also, let $\hat{U}_j$ be derived from U_j by extending the transformation to the amplitudes of the elements of $\hat{S}$; this is done by defining the transformations on the amplitudes of $\hat{S} - S$ to be identity maps. For each $j = 1, ..., n$, let Q_j be the unitary transformation, reversing the amplitudes of basis states $|s_{sense,\, j}\rangle$, $|s_{test,\, j}\rangle$, as defined by the unitary permutation matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Let Q_j be extended to the remaining elements of $\hat{S} - \{|s_{sense,\, j}\rangle, |s_{test,\, j}\rangle\}$ by defining the transformations to be identity maps. Let M be any unitary map that does not affect basis states $|s_{sense,\, j}\rangle$, $|s_{test,\, j}\rangle$. By Lemma 5.1 and the definition of Q_j, we have:

- If initially $\frac{1}{\gamma} |s_{POWER}\rangle$ (so $a_{POWER} = \frac{1}{\gamma}$ and $a_{TEST} = 0$, as given by $\hat{\alpha}_0$), then in $Q_j M \hat{T}_0 \hat{\alpha}_0$ the amplitude of $|s_{sense,\, j}\rangle$ is σ_j.
- If initially $\frac{1}{\gamma} |POWER\rangle + \sqrt{2\varepsilon_0}\, |s_{TEST}\rangle$ (so $a_{POWER} = \frac{1}{\gamma}$ and $a_{TEST} = \sqrt{2\varepsilon_0}$, as given by $\hat{\alpha}_1$), then in $Q_j M \hat{T}_0 \hat{\alpha}_1$, the amplitude of $|s_{sense,\, j}\rangle$ is 0.

Thus, we have shown:

PROPOSITION 5.1. *The amplitude of* $|s_{sense,\, j}\rangle$ *is* σ_j *in* $Q_j M \hat{T}_0 \hat{\alpha}_0$ *and is* 0 *in* $Q_j M \hat{T}_0 \hat{\alpha}_1$.

5.6. The New Total Input–Output Unitary Transformation

The composition of the new total unitary transformations up to the jth stage gives

$$\hat{T}_j = Q_j \hat{U}_j Q_{j-1} \hat{U}_{j-1} \cdots Q_2 \hat{U}_2 Q_1 \hat{U}_1 \hat{T}_0.$$

This can be recursively defined as $\hat{T}_j = Q_j \hat{U}_j \hat{T}_{j-1}$. Thus, the total input–output unitary transformation due to the new unitary transformations is

$$\hat{T}_{n+1} = \hat{U}_{n+1} Q_n \hat{U}_n Q_{n-1} \hat{U}_{n-1} \cdots Q_2 \hat{U}_2 Q_1 \hat{U}_1 \hat{T}_0.$$

5.7. Proof of the Simulation of Quantum Amplification Detection

LEMMA 5.2. *Let* $S' = S - \{|s_{absorb,\,j}\rangle \mid 1 \leqslant j \leqslant n\}$. *Then* $\hat{T}_j \hat{\alpha}_0$ *provides the same amplitude to the elements of* S' *as does* $T_j \alpha_0$, *and also* $\hat{T}_j \hat{\alpha}_j$ *provides the same amplitude to the elements of* S' *as does* $T'_j \alpha_0$.

Proof. We provide a proof by induction on j.

Recall from Subsection 4.3 that the unitary transformation by the $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system, up to and including the j stage, can be recursively defined as $T_j = U_j T_{j-1}$ in case CLEAR, and $T'_j = U'_j T'_{j-1}$ in case OBSTRUCTION, where T_0, T'_0 are the identity map, and $U'_j = P_j U_j$, and where P_j is a unitary permutation matrix defined in Subsection 4.3 that interchanges states $|s_{sense,\,j}\rangle$ and $|s_{absorb,\,j}\rangle$ (thereby interchanging the amplitudes of $|s_{sense,\,j}\rangle$ and $|s_{absorb,\,j}\rangle$), and provides an identity mapping on all elements of $\hat{S}$ except $|s_{sense,\,j}\rangle$ and $|s_{absorb,\,j}\rangle$. Also recall that α_0 is defined in Subsection 4.3 to be the input amplitudes of basis states of the sensing system in both the case CLEAR and OBSTRUCTION.

The basis case holds by Lemma 5.1. For our induction hypothesis, we assume that $\hat{T}_{j-1}\hat{\alpha}_0$ provides the same amplitude to the elements of S' as does $T_{j-1}\alpha_0$, and also that $\hat{T}_{j-1}\hat{\alpha}_1$ provides the same amplitude to the elements of S' as does $T'_{j-1}\alpha_0$. By definition, $\hat{T}_j\hat{\alpha}_0 = \hat{U}_j \hat{T}_{j-1}\hat{\alpha}_0$ provides the same amplitude to the elements of S' as does $U_j T_{j-1}\alpha_0$, and also $\hat{T}_j\hat{\alpha}_1 = \hat{U}_j \hat{T}_{j-1}\hat{\alpha}_1$ provides the same amplitude to the elements of S' as does $U_j T'_{j-1}\alpha_0$. Then the definition of Q_j and $\hat{T}_j = Q_j \hat{U}_j \hat{T}_{j-1}$.

- Proposition 5.1 ensures that from $\hat{T}_j\hat{\alpha}_0$, the application of mapping Q_j provides the amplitude σ_j to $|s_{sense,\,j}\rangle$, which is the same as in $T_j\alpha_0$;
- Proposition 5.1. also ensures that in $\hat{T}_j\hat{\alpha}_1$, the application of mapping Q_j sets the amplitude of $|s_{sense,\,j}\rangle$ to 0, which is the same as in $T'_j\alpha_0$; and
- furthermore, the amplitude of no other elements of S' is modified.

Hence we have that $\hat{T}_j\hat{\alpha}_0$ provides the same amplitude to the elements of S' as does $T_j\alpha_0$, and also that $\hat{T}_j\hat{\alpha}_1$ provides the same amplitude to the elements of S' as does $T'_j\alpha_0$. ∎

5.8. Renormalization of the Amplitudes

LEMMA 5.3. *Suppose that the unitary transformations* U_j, $j = 1, ..., n+1$, *define an* $(\varepsilon, \varepsilon_0, \varepsilon_1)$*-sensing system. Let* $\mathscr{A} = (1-\varepsilon)/2\varepsilon_0$, $\beta = 1 - 1/(1 + 2\varepsilon_0(1-2\varepsilon_0))$, *and* $\beta' = (1-2\varepsilon_0)\,\varepsilon$. *Then unitary transformation* $\hat{T}_{n+1}$ *is a quantum* $(\mathscr{A}, \beta, \beta')$*-amplification system.*

Proof. We need to renormalize the initial amplitude vectors for $\hat{T}_{n+1}$ so that the total input intensity in each case is 1.

Recall that $\hat{\alpha}_0$ gives $\frac{1}{\gamma}\,|s_{POWER}\rangle + 0\;|s_{TEST}\rangle$, that it provides the initial assignment of the amplitudes of the elements of $\hat{S}$ so that $a_{POWER} = \frac{1}{\gamma}$, for $\gamma = \sqrt{1-2\varepsilon_0}$, and $a_{TEST} = 0$. Let $\bar{\alpha}_0$ be an $\hat{S}$-vector providing the initial assignment of the amplitudes of the elements in $\hat{S}$ so that $a_{POWER} = 1$ and $a_{TEST} = 0$, and provides amplitude 0 to all other elements in $\hat{S}$. In Dirac notation, $\bar{\alpha}_0$ gives $1\;|s_{POWER}\rangle + 0\;|s_{TEST}\rangle$. In the case CLEAR for the $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system, by definition it produces output

$T_{n+1}\alpha_0$ where the intensity of the output amplitude of basis state $|s_{OUTPUT}\rangle$ is $\leqslant \varepsilon$. Lemma 5.2 implies that $\hat{T}_{n+1}\hat{\alpha}_0$ provides the same output amplitude to $|s_{OUTPUT}\rangle$ as does $T_{n+1}\alpha_0$, so in $\hat{T}_{n+1}\hat{\alpha}_0$ the intensity of the output amplitude of basis state $|s_{OUTPUT}\rangle$ is also $\leqslant \varepsilon$. By linearity, $\hat{T}_{n+1}\bar{\alpha}_0$ provides a factor $\gamma = \sqrt{1-2\varepsilon_0}$ less to the output amplitude of $|s_{OUTPUT}\rangle$, so the intensity is a factor $\gamma^2 = 1-2\varepsilon_0$ less. Thus, in $\hat{T}_{n+1}\bar{\alpha}_0$, the intensity of the output amplitude of basis state $|s_{OUTPUT}\rangle$ is $\leqslant (1-2\varepsilon_0)\,\varepsilon = \beta'$.

Also, recall that $\hat{\alpha}_1$ gives $\frac{1}{\gamma}|s_{POWER}\rangle + \sqrt{2\varepsilon_0}\,|s_{TEST}\rangle$, and that it provides the initial assignment of the amplitudes of the elements of $\hat{S}$ so that $a_{POWER} = \frac{1}{\gamma}$ and $a_{TEST} = \sqrt{2\varepsilon_0}$. To renormalize, we decrease the amplitudes by a factor of $\lambda = 1/\sqrt{1/\gamma^2 + 2\varepsilon_0}$. Note that $\lambda = \gamma\sqrt{1-\beta}$, where $\beta = 1 - 1/(1+2\varepsilon_0(1-2\varepsilon_0))$, and observe that $\lambda\sqrt{2\varepsilon_0} = \sqrt{\beta}$. We let $\bar{\alpha}_1$ be an $\hat{S}$-vector providing the initial assignment of the amplitudes of the elements of $\hat{S}$ so that $a_{POWER} = \lambda/\gamma = \sqrt{1-\beta}$ and $a_{TEST} = \lambda\sqrt{2\varepsilon_0} = \sqrt{\beta}$, and provides 0 amplitude to all other elements of $\hat{S}$. In Dirac notation, $\bar{\alpha}_1$ gives $\sqrt{1-\beta}\,|s_{POWER}\rangle + \sqrt{\beta}\,|s_{TEST}\rangle$. In the case OBSTRUCTION for the $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system, by definition it produces output $T'_{n+1}\alpha_0$ where the intensity of the output amplitude of basis state $|s_{OUTPUT}\rangle$ is $\geqslant 1-\varepsilon$. Lemma 5.2 implies that $\hat{T}_{n+1}\hat{\alpha}_1$ provides the same output amplitude for $|s_{OUTPUT}\rangle$ as does $T'_{n+1}\alpha_0$. Thus, in $\hat{T}_{n+1}\hat{\alpha}_1$ the intensity of the output amplitude of basis state $|s_{OUTPUT}\rangle$ is also $\geqslant 1-\varepsilon$. By linearity, $\hat{T}_{n+1}\bar{\alpha}_1$ provides output amplitude that is a factor λ less than $\hat{T}_{n+1}\hat{\alpha}_1$, and so has intensity λ^2 less. Thus, in $\hat{T}_{n+1}\bar{\alpha}_1$ the intensity of the output amplitude of basis state $|s_{OUTPUT}\rangle$ is $\geqslant (1-\varepsilon)\,\lambda^2 = (1-\varepsilon)\,\beta/(2\varepsilon_0) = \mathscr{A}\beta$, since $\lambda^2 = \beta/(2\varepsilon_0)$ and $\mathscr{A} = (1-\varepsilon)/2\varepsilon_0$. Hence $\hat{T}_{n+1}$ is a unitary transformation that does quantum $(\mathscr{A}, \beta, \beta')$-amplification. ∎

5.9. *Proof That Nearly Interaction-Free Sensing is Not Possible*

By Theorem 3.1, there is no unitary transformation that does quantum $(\mathscr{A}, \beta, \beta')$-amplification, if

$$\left|\sqrt{\mathscr{A}} - \sqrt{(1-\beta)\,\beta'/\beta}\right| > 1$$

for $0 < \beta$, $\beta' < 1$ and $1 < \mathscr{A} \leqslant 1/\beta$. Set $\mathscr{A} = (1-\varepsilon)/2\varepsilon_0$, $\beta = 1 - 1/(1+2\varepsilon_0(1-2\varepsilon_0))$, and $\beta' = (1-2\varepsilon_0)\,\varepsilon$. Note that $(1-\beta)/\beta = 1/2\varepsilon_0(1-2\varepsilon_0)$, so $(1-\beta)\,\beta'/\beta = \varepsilon/2\varepsilon_0$. By Lemma 5.3, there is no $(\varepsilon, \varepsilon_0, \varepsilon_1)$-sensing system if $|\sqrt{\mathscr{A}} - \sqrt{(1-\beta)\,\beta'/\beta}| = |\sqrt{(1-\varepsilon)/2\varepsilon_0} - \sqrt{\varepsilon/2\varepsilon_0}| > 1$. Solving for ε_0, for $\varepsilon_0 < 1/2$, we obtain the condition:

THEOREM 5.1. *If* $\varepsilon_0 < \min(1, (\sqrt{1-\varepsilon} - \sqrt{\varepsilon})^2)/2$ *there is no* $(\varepsilon, \varepsilon_0, \varepsilon_1)$*-sensing system using unitary transformations* (*which may be infinite dimensional*).

COROLLARY 5.1. *There is no* $(\varepsilon, \varepsilon_0, \varepsilon_1)$*-sensing system using unitary transformations, for* $\varepsilon < 1/2$ *and sufficiently small* ε_0. *Thus, there is no method for IFS using unitary transformations.*

6. CONCLUSION

Our research was motivated by the potential applications of IFS to lower the I/O bandwidth in computer systems and related applications in complexity theory.

There are some further possible extensions of our work. In this paper, we have assumed that a quantum projection (also sometimes known as a quantum collapse) is done after the final nth sensing stage, via observation of the output basis state. This suffices to provide a disproof of IFS, which is the main goal of our paper. However, Bernstein and Vazirani [BV93, BV97] showed that all observation operations can be pushed to the end of the computation, by repeated use of a quantum XOR gate construction. Thus implies that our proof extends to allow a quantum projection to be done on earlier stages as well, thus ruling out an even larger class of proposals for IFS.

For simplicity in our formulation, we assumed that the entering photon was either absorbed or not absorbed by the apparatus, and do not allow for a more general scheme where the obstructing body could alter the state of the photon instead of absorbing it. (Such a scheme was not used by the IFM method of [KWZ95].) It is an open question whether this scheme is of benefit, or whether our impossibility proof techniques can be extended to this scheme.

Subsequent to this paper, two interesting (but less direct) possible alternative proofs of our impossibility result for quantum amplification detection have been suggested to us. One of these alternative proofs would use a reduction from a well-known result that proves that instantaneous communication is not possible by a quantum system. This alternative proof would show that if quantum amplification detection were possible, then it would enable instantaneous communication across arbitrarily large distances. Another alternative proof would use a reduction to EPR.

APPENDIX

The Initialization of Unitary Transformations for Simulation of Sensing

7.1. Quantum Coin Flips

Let $\varepsilon_0 = \sum_{j=1}^{n} |\sigma_j|^2$. Let u be an n-vector which has 1 at its first entry and 0 on the other entries. Let u' be an n-vector which has amplitude $u'_j = \sigma_j/\sqrt{\varepsilon_0}$, for each $j = 1, ..., n$. The vector u can be mapped to the vector u' by a well-known unitary transformation known in theoretical computer science as a *weighted quantum coin flip* [G96], which we denote by F. For example, in the case $n = 2$, F is a rotation matrix:

$$F = \frac{1}{\sqrt{\sigma_1^2 + \sigma_2^2}} \begin{bmatrix} \sigma_1 & -\sigma_2 \\ \sigma_2 & \sigma_1 \end{bmatrix}.$$

For general $n > 2$, the weighted quantum coin flip can be constructed by a series of appropriately defined 2×2 weighted quantum coin flips.

7.2. Proof of Lemma 5.1.

Proof. We have defined $\hat{\alpha}_\ell$ to give the initial amplitudes of the basis states, where ℓ is either 0 or 1 depending on the input. In the following, we will define transformations W_0, W'_0, W_j, for $0 < j \leq n$. We define unitary transformation $\hat{T}_0$ to be a composition (written in matrix form and applied from right to left) $\hat{T}_0 = W_{n+1} W_n \cdots W_1 W'_0 W_0$ of unitary transformations defined below.

We have already defined a_{POWER}, a_{TEST} to be the initial amplitudes of basis states $|s_{POWER}\rangle$, $|s_{TEST}\rangle$ as given in $\hat{\alpha}_\ell$. It will be useful to introduce notation for the amplitudes of other basis states after those specified transformations. For $j = 1, ..., n$, let

- $a_{test,\,j}$ be the amplitude of $|s_{test,\,j}\rangle$ in $W_0 \hat{\alpha}_\ell$,
- $a_{power,\,j}$ be the amplitude of $|s_{power,\,j}\rangle$ in $W'_0 W_0 \hat{\alpha}_\ell$, and
- $a'_{test,\,j}$ be the amplitude of $|s_{test,\,j}\rangle$ in $\hat{T}_0 \hat{\alpha}_\ell$.

Also, we define $a_{INITIAL}$ to be the amplitude of basis state $|s_{INITIAL}\rangle$ in $W'_0 W_0 \hat{\alpha}_\ell$, which will be the same as in $\hat{T}_0 \hat{\alpha}_\ell$.

Definition of W_0. Let w_0 be the following unitary transformation:

1. First permute the amplitude of $|s_{TEST}\rangle$ and $|s_{test,\,1}\rangle$, by use of the unitary permutation submatrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

2. Then apply the weighted quantum coin flip F defined above on the basis states $(|s_{test,\,1}\rangle, |s_{test,\,2}\rangle, ..., |s_{test,\,n}\rangle)$, so that in $W_0 \hat{\alpha}_0$, each $|s_{test,\,j}\rangle$ now has amplitude $a_{test,\,j} = (\sigma_j / \sqrt{\varepsilon_0})\, a_{TEST}$.

3. W_0 does not affect any other elements of $\hat{S}$.

Definition of W'_0. Let $\gamma' = \sqrt{1 - \gamma^2 2\varepsilon_0}$. Note that $\gamma^2 2\varepsilon_0 < 1$ since we have assumed $\varepsilon_0 < 1/2$. Also note that $(\gamma/\gamma')^2 < 1$ since we have defined $\gamma^2 = 1 - 2\varepsilon_0 < 1 - 2\varepsilon_0 + 4\varepsilon_0^2 = 1 - (1 - 2\varepsilon_0)\, 2\varepsilon_0 = (\gamma')^2$. Let W'_0 be the following unitary transformation:

1. First apply the unitary rotation matrix transformation

$$\begin{bmatrix} \gamma' & -\sqrt{2\varepsilon_0}\,\gamma \\ \sqrt{2\varepsilon_0}\,\gamma & \gamma' \end{bmatrix}$$

on the amplitudes of $|s_{POWER}\rangle$, $|s_{power,\,1}\rangle$ (note that these basis states initially had amplitude a_{POWER}, 0, respectively), so that $|s_{POWER}\rangle$ now has amplitude $\gamma' a_{POWER}$ and $|s_{power,\,1}\rangle$ now has amplitude $(\sqrt{2\varepsilon_0}\,\gamma)\, a_{POWER}$.

2. Then apply the unitary rotation matrix transformation

$$\begin{bmatrix} \sqrt{1 - (\gamma/\gamma')^2} & -\gamma/\gamma' \\ \gamma/\gamma' & \sqrt{1 - (\gamma/\gamma')^2} \end{bmatrix}$$

on the amplitudes of $|s_{POWER}\rangle$, $|s_{INITIAL}\rangle$ (note that these basis states initially had amplitude $\gamma' a_{POWER}$, 0, respectively), so that $|s_{INITIAL}\rangle$ now has amplitude γa_{POWER}.

3. Then apply the weighted quantum coin flip F defined above on the basis states $(|s_{power,1}\rangle, |s_{power,2}\rangle, ..., |s_{power,n}\rangle)$, so that after applying W'_0, each $|s_{power,j}\rangle$ now has amplitude $a_{power,j} = (\sigma_j/\sqrt{\varepsilon_0})(\sqrt{2\varepsilon_0}\,\gamma a_{POWER}) = \sigma_j(\sqrt{2}\,\gamma a_{POWER})$.

4. W'_0 does not affect any other elements of $\hat{S}$.

Definition of W_j. For $j = 1, ..., n$ let W_j be the unitary transformation from the amplitudes of basis states $|s_{power,j}\rangle$, $|s_{test,j}\rangle$ to those of $|s_{power,j}\rangle$, $|s_{test,j}\rangle$ defined by the unitary rotation submatrix

$$\frac{1}{\sqrt{2}}\begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix},$$

and W_j does not affect any other elements of $\hat{S}$.

Note that since the amplitude of $|s_{POWER}\rangle$ is not changed by W_0, it has the same initial amplitude $a_{POWER} = \frac{1}{\gamma}$ in $W_0\hat{\alpha}_\ell$ as in $\hat{\alpha}_\ell$. So in $W'_0 W_0 \hat{\alpha}_\ell$, basis state $|s_{INITIAL}\rangle$ has amplitude $a_{INITIAL} = a_{POWER}(\gamma/\gamma')\,\gamma' = 1$. Since the amplitude of $|s_{POWER}\rangle$ is not change in the subsequent transformations W_j, basis state $|s_{INITIAL}\rangle$ also has amplitude $a_{INITIAL} = 1$ in both $\hat{T}_0\hat{\alpha}_0$ and $\hat{T}_0\hat{\alpha}_1$.

We have shown that each $|s_{test,j}\rangle$ has amplitude $a_{test,j} = (\sigma_j/\sqrt{\varepsilon_0})\,a_{TEST}$ in $W'_0 W_0 \hat{\alpha}_\ell$. Also, since $a_{POWER} = \frac{1}{\gamma}$, in $W'_0 W_0 \hat{\alpha}_\ell$ each $|s_{power,j}\rangle$ has amplitude $a_{power,j} = \sigma_j(\sqrt{2}\,\gamma a_{POWER}) = \sqrt{2}\,\sigma_j$. The amplitude of the basis state $|s_{test,j}\rangle$ after transformation $W_j \cdots W_1 W'_0 W_0$ is $a'_{test,j} = 1/\sqrt{2}(a_{power,j} - a_{test,j})$, which is the same as its amplitude after transformation $\hat{T}_0\hat{\alpha}_0$. Hence we have:

- If $a_{POWER} = \frac{1}{\gamma}$ and $a_{TEST} = 0$ (as given by $\hat{\alpha}_0$), then $a_{power,j} = \sqrt{2}\,\sigma_j$ and $a_{test,j} = 0$. Thus, in $\hat{T}_0\hat{\alpha}_0$, each $|s_{test,j}\rangle$ has amplitude $a'_{test,j} = 1/\sqrt{2}(a_{power,j} - 0) = 1/\sqrt{2}(\sqrt{2}\,\sigma_j - 0) = \sigma_j$.
- Also, if $a_{POWER} = \frac{1}{\gamma}$ and $a_{TEST} = \sqrt{2\varepsilon_0}$ (as given by $\hat{\alpha}_1$), then $a_{power,j} = \sqrt{2}\,\sigma_j$ and $a_{test,j} = \sqrt{2}\,\sigma_j$. Thus, in $\hat{T}_0\hat{\alpha}_1$, each $|s_{test,j}\rangle$ has amplitude $a'_{test,j} = 1/\sqrt{2}(a_{power,j} - a_{test,j}) = 1/\sqrt{2}(\sqrt{2}\,\sigma_j - \sqrt{2}\,\sigma_j) = 0$.

ACKNOWLEDGMENTS

Giles Brassard, Peter Shor, Zheng Zao, and the referees provided many very useful suggestions for improvements to this paper. K. Redding provided considerable aid in preparation of the paper.

Received September 26, 1997; final manuscript received July 18, 1999

REFERENCES

[BBE92] Bennett, C. H., Brassard, G., and Ekert, A. K. (Oct. 1992), Quantum cryptography, *Sci. Amer*. 50–57.

[BV93] Bernstein, E., and Vazirani, U. (1993), Quantum complexity Theory, *in* "Proceedings, 25th ACM Symposium on the Theory of Computation," pp. 11–20, Assoc. Comput. Mach., New York.

[BV97] Bernstein, E., and Vazirani, U. (1997), Quantum complexity theory, *SIAM J. Comput.* **26**(5), 1411–1473.

[BHT98] Brassard, G., Hoyer, P., and Tapp, A. (May 1998), Quantum counting, *in* "Proceedings 25th Colloquium on Automata, Languages, and Programming, Aalborg, Denmark."

[BH98] Brassard, G., and Hoyer, P. (1997), An exact quantum polynomial-time algorithm for Simon's problem, *in* "Proceedings Fifth Israeli Symposium on theory of Computing and Systems (ISCS'97)." [Online preprint quant-ph/9704027]

[EV93] Elitzur, A. C., and Vaidman, L. (1993), Quantum mechanical interaction-free measurement, *Found. Phys.* **23**(7), 987–997.

[FC94] Fuchs, C., and Caves, C. (1994), Ensemble-dependent bounds for accessible information in quantum mechanics, *Phys. Rev. Lett.* **73**, 3047–3050.

[G98] Gacs, P. (1998), Quantum zeno effect without collapse, to appear; postscript preprint http://www.cs.bu.edu/ftp/gacs/papers/bomb.ps.Z.

[G96] Grover, L. K. (May, 1996), A fast quantum mechanical algorithm for database search, *in* "Proceedings, Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA," pp. 212–219.

[H73] Holevo, A. S. (1973), Some estimates of the information transmitted by quantum communication channels, *Problemy Peredachi Informatsii* **9**, 3–11. [English translation in *Problems Inform. Transmission* (*USSR*) **9**, 177–183 (1973)]

[KWZ95] Kwiat, P. G., Weinfurter, H., Herzog, T., Zeilinger, A., and Kasevich, M. A. (1995), Interaction-free measurement, *Phys. Rev. Lett.* **74**, 4763–4766.

[KWZ96] Kwiat, P. G., Weinfurter, H., and Zeilinger, A. (Nov. 1996), Quantum seeing in the dark, *Sci. Amer.*

[S94] Shor, P. W. (Nov. 1994), Algorithms for quantum computation: Discrete logarithms and factoring, *in* "35th Annual IEEE Symposium on Foundations of Computer Science, Santa Fe, New Mexico," pp. 124–134.

[S94] Shor, P. W. (1997), Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* **26**, 1484.

[SKC96] Steinberg, A. M., Kwiat, P. G., and Chiao, R. Y. (1996), Quantum optical tests of the foundations of physics, *in* "AIP Atomic, Molecular, and Optical Physics Handbook" (G. W. F. Drake *et al.*, Eds.), Chap. 77 Am. Inst. of Phys., New York.