On the Power of Quantum Fingerprinting [*]

[Extended Abstract]

Andrew Chi-Chih Yao
Computer Science Department
Princeton University
Princeton, NJ 08544
yao@cs.princeton.edu

ABSTRACT

In the simultaneous message model, two parties holding n-bit integers x, y send messages to a third party, the *referee*, enabling him to compute a boolean function $f(x, y)$. Buhrman et al [3] proved the remarkable result that, when f is the equality function, the referee can solve this problem by comparing short "quantum fingerprints" sent by the two parties, i.e., there exists a quantum protocol using only $O(\log n)$ bits. This is in contrast to the well-known classical case for which $\Omega(n^{1/2})$ bits are provably necessary for the same problem even with randomization. In this paper we show that short quantum fingerprints can be used to solve the problem for a much larger class of functions. Let $R^{||,pub}(f)$ denote the number of bits needed in the classical case, assuming in addition a common sequence of random bits is known to all parties (the *public coin* model). We prove that, if $R^{||,pub}(f) = O(1)$, then there exists a quantum protocol for f using only $O(\log n)$ bits. As an application we show that $O(\log n)$ quantum bits suffice for the bounded Hamming distance function, defined by $f(x, y) = 1$ if and only if x and y have a constant Hamming distance d or less.

Categories and Subject Descriptors

F.1 [**Theory of Computation**]: Computation by Abstract Devices

General Terms

Theory

Keywords

Quantum protocol, computational complexity, communication complexity, public coin, simultaneous message model

1. INTRODUCTION

In the simultaneous message model (see Kushilevitz ad Nisan [4]), two parties A, B holding n-bit strings x, y send messages a_x, b_y to a third party, called the *referee*, who wishes to compute a boolean function $f(x, y)$. In the randomized setting, a *protocol* specifies the probability distributions of a_x, b_y, and an $M \times M$ boolean *referee matrix* D, such that for all x, y, the probability of $D(a_x, b_y) = f(x, y)$ exceeds $1 - \epsilon$, where $0 < \epsilon \leq 1/3$ is a fixed constant. (The choice of ϵ affects the complexity only by a multiplicative constant.) Let $R^{||}(f)$ be the minimum number of bits (i.e., $\lceil \log_2 M \rceil$) needed by any such protocol.

Buhrman et al [3] extended the above model to the quantum setting, in which A, B send quantum states $|u_x>, |v_y>$ in a Hilbert space of dimension M, and the referee makes a decision based on some measurement on the the received combined state $|u_x> \otimes |v_y>$. They proved the remarkable result that, when f is the equality function, the referee can solve this problem by comparing short "quantum fingerprints" sent by the two parties, i.e., there is a quantum protocol using only $\lceil \log_2 M \rceil = O(\log n)$ qbits. This is in contrast to the classical case for which it is well known (Ambainis [1], Babai and Kimmel [2], Newman and Szegedy [6]) that $\Theta(n^{1/2})$ bits are necessary and sufficient for the equality function.

In this paper we show that short quantum fingerprints can be used to solve a much larger class of functions. To fix the notation, let $Q^{||}(f)$ denote the minimum number of qbits communicated by any quantum protocol. The error probability is bounded by a fixed constant $0 < \epsilon \leq 1/3$.

Consider the *public coin* version (see Kushilevitz ad Nisan [4]) of the (classical) simultaneous message model, in which a common random bit sequence ξ is known to both A and B. In this model, A sends a (deterministic) message $a_{x,\xi}$, B sends a (deterministic) message $b_{y,\xi}$, and the referee makes the decision $D(a_{x,\xi}, b_{y,\xi})$ using a boolean matrix D. Let $R^{||,pub}(f)$ denote the minimum number of bits needed by any protocol in the public coin model. Our main result (Theorem 1) shows that the complexity in the quantum model is closely related to that in the (classical) public coin model.

Let $f_1, f_2, f_3, \cdots$ be a sequence of functions where $f_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$.

Theorem 1 If $R^{||,pub}(f_n) = O(1)$, then $Q^{||}(f_n) = O(\log n)$.

One can regard the result of Buhrman [3] as a special case of Theorem 1, as the equality function has complexity $O(1)$ in the public coin model (see [4]). Let $HAM_n^{(d)}$ denote the

[*]This research was supported in part by the National Science Foundation grant CCR-9820855

STOC'03, June 9–11, 2003, San Diego, California, USA.
Copyright 2003 ACM 1-58113-674-9/03/0006 ...$5.00.

boolean function such that $HAM_n^{(d)}(x,y) = 1$ if and only if the two n-bit strings x and y have Hamming distance at most d. As an application of Theorem 1, we show that, for any fixed d, $R^{||,pub}(HAM_n^{(d)}) = O(1)$, and hence by Theorem 1 the problem $HAM_n^{(d)}$ can be solved with $O(\log n)$-qbit quantum fingerprints.

Theorem 2 $R^{||,pub}(HAM_n^{(d)}) = O(d^2)$.

Corollary For any fixed d, $Q^{||}(HAM_n^{(d)}) = O(\log n)$.

In Theorem 1, the term $O(\log n)$ hides a large constant. It says that, if $R^{||,pub}(f_n) \leq c$, then $Q^{||}(f_n) = 2^{O(c)} \log n$. It is natural to ask whether one may achieve $Q^{||}(f_n) = O(R^{||,pub}(f_n) \cdot \log n)$ or better. (For comparison, note that it is known ([2, 4, 6]) that $R^{||}(f_n) = O(R^{||,pub}(f_n) \cdot n^{1/2})$.) The next theorem is a partial result in this direction.

Let M be any positive integer. Call two $M \times M$ real matrices G, G' *isomorphic*, if they differ only by the naming of rows and columns, i.e., $G' = PGQ$ for some permutation matrices P, Q. (Regard any G as a weighted bipartite graph with vertex set $[M] \times [M]$, and with weight $G(i,j)$ associated with edge (i,j). Then G, G' are isomorphic if and only if their associated weighted graphs are isomporhic.) Let $\mathcal{F}_M$ be the set of all $M \times M$ real positive semidefinite matrices F with only non-negative entries. Let $\mathcal{G}_M$ be the set of all G isomorphic to at least some $F \in \mathcal{F}_M$. For any $M \times M$ matrix K, define its *convex width*, $w(K)$, as the smallest integer k for which K can be expressed as the sum of k matrices in $\mathcal{G}_M$.

Theorem 3 Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a boolean function, and $\mathcal{A}$ is a protocol that computes f in the public coin model using an $M \times M$ referee matrix D. Then $Q^{||}(f) = O(w(D)^5(1 + \log w(D)) \cdot (\log_2 M + \log n))$.

Note that $w(D) \leq M$, and thus Theorem 3 can be regarded as an extension of Theorem 1. The rest of the paper is devoted to the proof of the above theorems. Some open problems are discussed in the last section.

2. PRELIMINARIES

We review some material in [3]. Let H be a Hilbert space. The Hilbert space $H \otimes H$ can be decomposed into two orthogonal subspaces V^+, V^-, called the *symmetric* subspace and the *anti-symmetric* subspace. Subspace V^+ is generated by the set of all states of the form $|u> \otimes |v> + |v> \otimes |u>$ for all $|u>, |v> \in H$; and V^- is generated by all states of the form $|u> \otimes |v> - |v> \otimes |u>$. Consider the measurement $\mathcal{M}_H$ corresponding to the above decomposition, with "+" and "-" as the possible outcomes. Buhrman et al observed that the following simple fact is very useful.

Fact 1 Perform measurement $\mathcal{M}_H$ on the state $|u> \otimes |v>$. The probability of observing the result "-" is equal to $(1 - |<u|v>|^2)/2$.

Let $E : \{0,1\}^n \to \{0,1\}^N$, where $N = O(n)$, be an error correcting code such that $E(x)$ and $E(y)$ have Hamming distance greater than $0.4N$ for any distinct x, y. Let $E_i(x)$ be the i-th bit of $E(x)$. For each $x \in \{0,1\}^n$, let

$$|u_x> = \frac{1}{N^{1/2}} \sum_{1 \leq i \leq N} |i, E_i(x)> .$$

Note that $|<u_x|u_y>| = 1$ if $x = y$, and otherwise $|<u_x|u_y>| < 0.6$. By Fact 1, this implies that if one performs the measurement $\mathcal{M}_H$ on $|u_x> \otimes |u_y>$, the probability of seeing "-" is equal to 0 if $x = y$, and otherwise is at least $(1 - 0.6^2)/2 = 0.32$.

We now describe Buhrman et al's quantum protocol. Parties A, B send k copies of $|u_x>$, $|u_y>$ to the referee. The referee performs the measurement $\mathcal{M}_H$ on each of the k copies of $|u_x> \otimes |u_y>$, and declare $x = y$ if and only if "-" is absent in the outcomes of all k experiments. The error probability of this protocol is easy to analyze. It is always correct if $x = y$. If $x \neq y$, the error probability is less than $(1 - 0.32)^k$, which can be made arbitrarily small by taking a large enough constant k.

For our purpose, we need to extend their method to obtain an estimate of $|<u|v>|$. As before, we perform measurement $\mathcal{M}_H$ on k copies of $|u> \otimes |v>$. Let k' be the number of times the answer "-" comes up. Define the output η as $(1 - \frac{2k'}{k})^{1/2}$ if $k' \leq k/2$, and 0 otherwise. Let $\Delta = \eta - |<u|v>|$. The proof of the following lemma is given in the Appendix.

Lemma 1 For any $\beta > 0$, $\Pr\{|\Delta| > \beta\} < 2e^{-k\beta^4/32}$.

3. PROOF OF THEOREM 1

Fix the error probability at $\epsilon = 1/10$. Let c be a positive constant such that $R^{||,pub}(f_n) \leq c$ for all n. Consider a public coin protocol computing f_n using c communication bits. Let $[M] = \{1, 2, \cdots, M\}$ be the message space where $M = 2^c$, and let $D : [M] \times [M] \to \{0,1\}$ be the referee matrix (D may depend on n). It is well known (Newman [5]) that we can assume that the public random string is uniformly chosen from a set of $L = O(n)$ strings $\xi_1, \xi_2, \cdots, \xi_L$. Let $a_i(x) \in [M], b_i(y) \in [M]$ be the messages sent by A, B to the referee when ξ_i is the public string chosen. By definition,

$$|f(x,y) - \frac{1}{L} \sum_{1 \leq i \leq L} D(a_i(x), b_i(y))| < \epsilon. \qquad (1)$$

Our plan is to construct a quantum protocol with error probability bounded by 1/3, using $2^{O(c)} \log n$ communication qbits. Define the Hilbert space $H = \mathbf{C}^M \otimes \mathbf{C}^L$, where $\mathbf{C}$ is the set of complex numbers. For each $x, y \in \{0,1\}^n$, associate vectors in H

$$\begin{aligned} |u_x> &= \frac{1}{L^{1/2}} \sum_{1 \leq i \leq L} |a_i(x)> \otimes |i>, \\ |v_y> &= \frac{1}{L^{1/2}} \sum_{1 \leq i \leq L} |b_i(y)> \otimes |i> . \end{aligned}$$

Let $A_t(x)$ be the set of $i \in [L]$ satisfying $a_i(x) = t$, and $B_t(y)$ be the set of $i \in [L]$ satisfying $a_i(y) = t$.

Definition 1 For each $1 \leq t \leq M$, let

$$\begin{aligned} |u_{x,t}> &= \sum_{i \in A_t(x)} |i>, \\ |v_{y,t}> &= \sum_{i \in B_t(y)} |i> . \end{aligned}$$

Note that the vectors $|u_{x,t}>, 1 \leq t \leq M$ are mutually orthogonal, and $\sum_{1 \leq t \leq M} |||u_{x,t}>||^2 = L$. Similar statements hold for the $|v_{y,t}>$'s. It is clear that

$$\begin{aligned} |u_x> &= \frac{1}{L^{1/2}} \sum_{1 \leq t \leq M} |t> |u_{x,t}>, \\ |v_y> &= \frac{1}{L^{1/2}} \sum_{1 \leq t \leq M} |t> |v_{y,t}> . \qquad (2) \end{aligned}$$

Lemma 2

$$\frac{1}{L}\sum_{1\leq i\leq L} D(a_i(x),b_i(y)) = \sum_{1\leq t,t'\leq M} D(t,t')\frac{< u_{x,t}|v_{y,t'} >}{L}.$$

The proof of Lemma 2 follows easily from the fact that $< u_{x,t}|v_{y,t'} >= |A_{x,t}\cap B_{y,t'}|$.

If we can estimate the quantity $\frac{<u_{x,t}|v_{y,t'}>}{L}$ for each pair t,t', up to an additive term ϵ/M^2, then Lemma 2 allows us to estimate $\frac{1}{L}\sum_{1\leq i\leq \ell} D(a_i(x),b_i(y))$ up to an additive term ϵ. By Equation (1), this means we can accurately decide whether $f(x,y)$ is 1 or 0.

Let $t,t'\in\{1,2,\cdots,M\}$. Let $k=64(M^2/\epsilon)^4\log_e(M^2/\epsilon)$.

Lemma 3 By performing unitary transformations and quantum measurements on k copies of $|u_x > \otimes|v_y >$, one can obtain a random output rational number η such that

$$\Pr\{|\eta - \frac{< u_{x,t}|v_{y,t'} >}{L}| > \frac{\epsilon}{M^2}\} < \frac{\epsilon}{M^2}.$$

For the moment, assume that we have proved Lemma 3. Consider the following quantum protocol. Parties A, B send kM^2 copies of $|u_x >$, $|v_y >$ to the referee. For each of the M^2 pairs $(t,t')\in[M]\times[M]$, the referee then obtains an estimate $\eta_{x,y}(t,t')$ of the quantity $\frac{<u_{x,t}|v_{y,t'}>}{L}$ for every t,t', using k of these copies and the quantum procedure provided by Lemma 3. The referee then declares $f(x,y)=1$ if and only if $\sum_{t,t'}\eta_{x,y}(t,t')>1/2$.

We now analyze the protocol. From Lemma 3 we conclude that, with probability at least $1-M^2\frac{\epsilon}{M^2}=1-\epsilon$,

$$|\eta_{x,y}(t,t') - \frac{< u_{x,t}|v_{y,t'} >}{L}| \leq \frac{\epsilon}{M^2},$$

for all t,t'. By Equation (1) and Lemma 2, we conclude that, for any $x,y\in\{0,1\}^n$, the probability is at least $1-\epsilon$ for the following inequality to hold:

$$\begin{aligned}
& |f(x,y) - \sum_{t,t'}\eta_{x,y}(t,t')| \\
\leq\ & |f(x,y) - \frac{1}{L}\sum_{1\leq i\leq L} D(a_i(x),b_i(y))| \\
& + \sum_{1\leq t,t'\leq M} D(t,t')|\frac{< u_{x,t}|v_{y,t'} >}{L} - \eta_{x,y}(t,t')| \\
\leq\ & \epsilon + M^2\frac{\epsilon}{M^2} \\
=\ & 2\epsilon \\
=\ & 1/5.
\end{aligned}$$

Note that this last inequality implies the following: $f(x,y)=1$ if and only if $\sum_{t,t'}\eta_{x,y}(t,t')>1/2$. Therefore, the probability for the referee to make the correct decision is at least $1-\epsilon>2/3$. This proves Theorem 1, as the protocol uses $O(M^{10}(\log M)\cdot(\log M+\log n))$ qbits.

It remains to prove Lemma 3. For each of the k copies of $|u_x > \otimes|v_y >$, do the following. First apply a unitary transformation to $|u_x > \otimes|v_y >$ to obtain $|u'_x > \otimes|v'_y >$, where

$$|u'_x > = \frac{1}{L^{1/2}}(|0 > \otimes|t > |u_{x,t} > + \sum_{\tau\neq t}|0 > \otimes|\tau > |u_{x,\tau} >),$$

$$|v'_y > = \frac{1}{L^{1/2}}(|0 > \otimes|t > |v_{y,t'} > + \sum_{\tau\neq t}|1 > \otimes|\tau > |v_{y,\tau} >).$$

(Strictly speaking, we need to enlarge the Hilbert space H to $\mathbf{C}\otimes H$ in order to accommodate $|u'_x >$ and $|v'_y >$.) Note that $< u'_x|v'_y >= \frac{<u_{x,t}|v_{y,t'}>}{L}$. We have thus reduced the problem to the estimation of $< u'_x|v'_y >$ from k copies of $|u'_x > \otimes|v'_y >$. By Lemma 1, this problem can be solved by performing measurements $\mathcal{M}_H$. Choose $\beta=\epsilon/M^2$, and $k=64(M^2/\epsilon)^4\log_e(M^2/\epsilon)$ in Lemma 1. Lemma 3 then follows from the probability estimate in Lemma 1.

4. PROOF OF THEOREM 2

We give a protocol in the public coin model using γd^2 communication bits, where $\gamma=10^4$. We then prove that the probability for the referee to be correct is at least 2/3.

The random public string consists of a sequence of $\gamma d^2 n$ random bits, each of which is generated independently with probability $p=1/(2d)$ to be a 1. Write this string as $z_1,z_2,\cdots,z_{\gamma d^2}$ where each z_i is an n-bit string. Party A sends the referee the string $a=a_1a_2\cdots a_{\gamma d^2}$ where a_i is the inner product of $x\cdot z_i$ mod 2. Similarly, Party B sends the referee the string $b=b_1b_2\cdots b_{\gamma d^2}$ where b_i is the inner product of $y\cdot z_i$ mod 2. The referee decides that $HAM_n^{(d)}(x,y)=1$ if and only if the Hamming distance between a and b is less than $\gamma d^2/2-q\gamma d^2$ where

$$q=((1-\frac{1}{d})^d+(1-\frac{1}{d})^{d+1})/4.$$

Let $c_i=a_i+b_i$. The Hamming distance between a and b is the number of 1's among $c_1,c_2,\cdots,c_{\gamma d^2}$.

Lemma 4 Assume that the Hamming distance between x and y is k. Then each c_i is an independent random variable with probability α_k being 1, where

$$\alpha_k=\frac{1}{2}-\frac{1}{2}(1-\frac{1}{d})^k.$$

To prove Lemma 4, note that $c_i=1$ if and only if $z_i\cdot(x\oplus y)=1$. That is, $c_i=1$ if and only if among the k bit positions in which x and y differ, z_i has an odd number of its bits equal to 1. Therefore, c_i is a random bit with probability β_k to be 1, where $\beta_k=\sum_{\substack{0\leq i\leq k\\ i:odd}}\binom{k}{i}p^i(1-p)^{k-i}$. Let $g_k(x)=(px+(1-p))^k=\sum_{0\leq i\leq k}\binom{k}{i}(px)^i(1-p)^{k-i}$. It is easy to see that $\beta_k=\frac{1}{2}(g_k(1)-g_k(-1))=1/2-(1-\frac{1}{d})^k/2=\alpha_k$. This proves Lemma 4.

Note that α_k is an increasing function of k. By Lemma 4, we have reduced the analysis of the protocol to the following problem. We have a coin with a fixed but unknown probability s to yield result 1 when it is tossed. We want to distinguish the case $s\leq\alpha_d$ from the case $s\geq\alpha_{d+1}$, by observing $c_1,c_2,\cdots,c_{\gamma d^2}$, the result of a sequence of γd^2 independent tosses of the coin. We adopt the rule that we declare $s\leq\alpha_d$ if and only if the number of 1's is less than $\gamma d^2/2-q\gamma d^2$. To prove Theorem 2, we only need to show that the probability of making the correct decision is greater than 2/3.

This is now just a routine calculation in elementary statistics, and we only give an informal argument here. For a given s, the probability distribution of the number of 1's is centered around its expected value $N_s=s\gamma d^2$ with a standard deviation $\sigma\approx(s\gamma d^2)^{1/2}\leq 100d$. In our decision rule, the cutoff point $\gamma d^2/2-q\gamma d^2$ is exactly the midpoint between N_{α_d} and $N_{\alpha_{d+1}}$. Since $N_{\alpha_{d+1}}-N_{\alpha_d}=\gamma d^2(\alpha_{d+1}-\alpha_d)=\gamma d^2\cdot(1-\frac{1}{d})^d/(2d)\geq 2000d$, the cutoff point is at least 10 standard deviations away from both N_{α_d} and $N_{\alpha_{d+1}}$. Thus, the choice of this cutoff point offers very reliable discrimination between the hypothesis $s \leq \alpha_d$ and $s \geq \alpha_{d+1}$.

5. PROOF OF THEOREM 3

Fix the error probability at $\epsilon = 1/10$. Given a protocol using referee matrix D in the public coin model, we would like to construct a quantum protocol using $O(w(D)^5(1 + \log w(D)) \cdot (\log_2 M + \log n))$ qbits.

We adopt the notation developed in the proof of Theorem 1. The goal is for A and B to send the appropriate states to the referee, so that he can estimate accurately the quantity

$$J = \sum_{1\leq t,t'\leq M} D(t,t')\frac{< u_{x,t}|v_{y,t'} >}{L},$$

which is approximately $f(x,y)$ by (1) and Lemma 2. By assumption, $D = \sum_{1\leq \ell\leq w(D)} G_\ell$ where $G_\ell \in \mathcal{G}_M$. Therefore,

$$\begin{aligned}\sum_{1\leq t,t'\leq M} & D(t,t')\frac{< u_{x,t}|v_{y,t'} >}{L} \\ &= \sum_{1\leq \ell\leq w(D)} (\sum_{1\leq t,t'\leq M} G_\ell(t,t')\frac{< u_{x,t}|v_{y,t'} >}{L}).(3)\end{aligned}$$

Note that each G_ℓ is a matrix with all its entries being real numbers between 0 and 1 (inclusive). The next proposition offers a quantum protocol to estimate J through Equation (3).

Proposition 1 Let $G \in \mathcal{G}_M$ be a matrix with all entries ≤ 1 . Then there is a quantum protocol using $O(w(D)^4(1 + \log w(D)) \cdot (\log_2 M + \log n))$ qbits such that the referee can output (probabilistically) a rational number η satisfying the following condition:

$$\Pr\{|\eta - \sum_{1\leq t,t'\leq M} G(t,t')\frac{< u_{x,t}|v_{y,t'} >}{L}| > \frac{\epsilon}{w(D)}\} < \frac{\epsilon}{w(D)}.$$

Similar to the discussions in Section 3, the referee can apply Proposition 1 to $G = G_\ell$ for each $1 \leq \ell \leq w(D)$ to obtain an output $\eta_\ell(x,y)$. He then declares $f(x,y) = 1$ if and only if the value $\sum_{1\leq\ell\leq w(D)} \eta_\ell(x,y)$ exceeds 1/2. In exactly the same way as in Section 3, one can prove that this quantum protocol satisfies the requirements of Theorem 3.

It remains to prove Proposition 1. Without loss of generality, we can assume that $G \in \mathcal{F}_M$. Since G differs from some $G' \in \mathcal{F}_M$ only in the naming of its rows and columns, any quantum protocol satisfying the specification of Proposition 1 G' can be made to work for G.

Since G is a real semidefinite matrix, there exist a real diagonal matrix $\Lambda = (\delta_{t,t'}\lambda_t)$ with only non-negative entries and a real orthogonal matrix $R = (r_{t,t'})$ such that $G = R\Lambda R^{-1}$. Note that R^{-1} is equal to R^T, the transpose of R.

We will define a set of fingerprints $|u''_x >, |v''_y >$ in $\mathbf{C} \otimes \mathbf{C}^M \otimes \mathbf{C}^L$ such that $< u''_x|v''_y >= \sum_{1\leq t,t'\leq M} G(t,t')\frac{<u_{x,t}|v_{y,t'}>}{L}$. This immediately leads to a quantum protocol for proving Theorem 3, since A, B can send the referee sufficiently many copies of $|u''_x >, |v''_y >$, so that the referee can estimate $< u''_x|v''_y >$ within the specification required by Proposition 1. Applying Lemma 1 with $\beta = \epsilon/w(D)$, we see that k copies are sufficient where $k = (4w(D)/\epsilon)^4 \log_e((1 + w(D))/\epsilon)$.

Let

$$\begin{aligned}|u'_{x,s} > &= \sum_{1\leq t\leq M} r_{t,s}|u_{x,t} >, \\ |v'_{y,s} > &= \sum_{1\leq t\leq M} r_{t,s}|v_{y,t} > .\end{aligned}$$

Definition 2 For any $x, y \in \{0,1\}^n$, let

$$\begin{aligned}|u'_x > &= \frac{1}{L^{1/2}}\sum_{1\leq s\leq M} (\lambda_s)^{1/2}|s > |u'_{x,s} >, \\ |v'_y > &= \frac{1}{L^{1/2}}\sum_{1\leq s\leq M} (\lambda_s)^{1/2}|s > |v'_{y,s} > .\end{aligned}$$

Lemma 5 For each $x, y \in \{0,1\}^n$,

$$< u'_x|v'_y >= \sum_{1\leq t,t'\leq M} G(t,t')\frac{< u_{x,t}|v_{y,t'} >}{L}.$$

Furthermore, $\||u'_x > \| \leq 1$ and , $\||v'_y > \| \leq 1$.

Proof of Lemma 5 Let U be the $M \times L$ matrix whose t-th row is the vector $|u_{x,t} >$ represented in the basis $\{|1 >, |2 >, \cdots, |L >\}$ (see Definition 1). Let U' be the $M \times L$ matrix whose t-th row is the vector $|u'_{x,t} >$ represented in the basis $\{|1 >, |2 >, \cdots, |L >\}$. Then $U' = R^T U$ and $U = RU'$.

Similarly, define V, V' as the matrices associated with $\{|v_{y,t} >\}$, $\{|v'_{y,t} >\}$. Then $V' = R^T V$ and $V = RV'$.

Observe that

$$\begin{aligned}< u'_x|v'_y > &= \frac{1}{L}\sum_{1\leq s\leq M} \lambda_s < u'_{x,s}|v'_{y,s} > \\ &= \frac{1}{L}Tr(U'^T \Lambda V') \\ &= \frac{1}{L}Tr((RU')^T R\Lambda R^{-1}(RV')) \\ &= \frac{1}{L}Tr(U^T G V) \\ &= \sum_{1\leq t,t'\leq M} G(t,t')\frac{< u_{x,t}|v_{y,t'} >}{L}.\end{aligned}$$

This proves the first assertion in Lemma 5.

Exactly the same manuipulation gives

$$\||u'_x > \|^2 =< u'_x|u'_x >= \sum_{1\leq t,t'\leq M} G(t,t')\frac{< u_{x,t}|u_{x,t'} >}{L}.$$

Using the fact that $< u_{x,t}|u_{x,t'} >= 0$ for $t \neq t'$ (see Definition 1), we have $\||u'_x > \|^2 = \sum_{1\leq t\leq M} G(t,t)\frac{<u_{x,t}|u_{x,t}>}{L} \leq \sum_{1\leq t\leq M} \frac{<u_{x,t}|u_{x,t}>}{L} = 1$. Similarly, one obtains $\||v'_y > \|^2 \leq 1$. This proves Lemma 5.

For any $x, y \in \{0,1\}^n$, define $0 \leq \theta_x, \psi_y \leq \pi/2$ such that $\cos\theta_x = \|u'_x\|$ and $\cos\psi_y = \|v'_y\|$.

The final fingerprints can now be defined as vectors in $\mathbf{C} \otimes \mathbf{C}^M \otimes \mathbf{C}^L$. Let $|\kappa >, |\kappa' >$ be any two fixed mutually orthogonal unit vectors in $\mathbf{C}^M \otimes \mathbf{C}^L$.

Definition 3 For any $x, y \in \{0,1\}^n$, let

$$\begin{aligned}|u''_x > &= |0 > \otimes|u'_x > + \sin\theta_x|1 > \otimes|\kappa >, \\ |v''_y > &= |0 > \otimes|v'_y > + \sin\psi_y|1 > \otimes|\kappa' > .\end{aligned}$$

It it easy to check that $|u''_x >, |v''_y >$ are unit vectors, and that $< u''_x|v''_y >=< u'_x|v'_y >$. By Lemma 5 we have then $< u''_x|v''_y >= \sum_{1\leq t,t'\leq M} G(t,t')\frac{<u_{x,t}|v_{y,t'}>}{L}$. This completes the proof of Proposition 1, and hence Theorem 3.

6. DISCUSSIONS

The quantum protocol constructed in the proof of Theorem 1 uses $O(M^{10}(\log M)(\log M+\log n)) = 2^{O(c)} \log n$ qbits, where $M = 2^c$ and c is the number of bits needed in the classical public coin simultaneous message model. Theorem 3 gives an improvement to $O(M^5(\log M)(\log M+\log n))$, since $w(D) \leq M$ for any D.

A further improvement can be made to give $O(M^4(\log M+\log n))$ (but is still $2^{O(c)} \log n$). Let $F \subseteq [M] \times [M]$ be the set of (t,t') with $f(t,t') = 1$, and F' be the complement of F. Costruct quantum fingerprints

$$\begin{aligned} |u_x> &= \frac{1}{(LM)^{1/2}}(\sum_{(t,t')\in F} |00>\otimes|t,t'>|u_{x,t}> \\ &\quad + \sum_{(t,t')\in F'} |01>\otimes|t,t'>|u_{x,t}>), \\ |v_y> &= \frac{1}{(LM)^{1/2}}(\sum_{(t,t')\in F} |00>\otimes|t,t'>|v_{y,t'}> \\ &\quad + \sum_{(t,t')\in F'} |10>\otimes|t,t'>|v_{y,t'}>). \end{aligned}$$

One can verify that $|u_x>, |v_y>$ are unit vectors, and that $| < u_x|v_y > | \geq (1-\epsilon)/M$ if $f(x,y) = 1$, and $\leq \epsilon/M$ if $f(x,y) = 0$. The can be exploited easily to give an $O(M^4(\log M) \cdot (\log M + \log n))$-qbit quantum protocol. We remark that a similar improvement can be made to the number of qbits needed in Theorem 3 (to $O(w(D)^4(1+\log w(D))(\log_2 M + \log n)))$.

We conclude with some open problems concerning the power of quantum fingerprinting.

1. Is it true that $Q^{||}(f) = O(R^{||,pub}(f) \cdot \log n)$? It is even conceivable that $Q^{||}(f) = O(R^{||,pub}(f) + \log n)$.

2. Is there some converse to Theorem 1? For example, is it possible that any function f with $Q^{||}(f) = O(\log n)$ must satisfy $R^{||,pub}(f) = O(1)$? Is it possible that any function f with $Q^{||}(f) = O(\log n)$ must satisfy $R^{||}(f) = O(n^{1-\epsilon})$? (Recall that $R^{||}(f)$ is the complexity in the basic (no public coin) model.)

3. Can one improve the bound $R^{||,pub}(HAM_n^{(d)}) = O(d^2)$ given in Theorem 2? Can one get better bounds, as a function of n and d, on $Q^{||}(HAM_n^{(d)})$?

4. Develop lower bound techniques for $Q^{||}(f)$. As a first step, one may restrict the class of quantum protocols to those based on estimating $| < u_x|v_y > |$. This gives rise to interesting questions on the embedding of graphs in vector spaces. For example, a bipartite graph $G = ([N] \times [N], E)$ is said to have a (d, δ_1, δ_2)-*threshold embedding*, if there exist two mappings ϕ, ψ from the set $[N]$ to the set of all unit vectors in $\mathbf{C}^d$ such that (a) $| < \phi(x)|\psi(y) > | \geq \delta_1$ if $(x,y) \in E$, and (b) $| < \phi(x)|\psi(y) > | \leq \delta_2$ if $(x,y) \notin E$. Can one characterize those G for which there is a $(\text{poly}(\log N), \delta_1, \delta_2)$ threshold embedding where $\delta_1 > \delta_2 \geq 0$ are fixed constants? This is closely related to the question of characterization of functions f with $Q^{||}(f) = O(\log n)$.

7. ACKNOWLEDGMENTS

We thank Yaoyun Shi for valuable suggestions for improving the presentation of the paper, including the $O(M^4(\log M)\cdot(\log M+\log n))$-qbit quantum protocol mentioned in Section 6.

8. REFERENCES

[1] A. Ambainis. Communication complexity in a 3-computer model. *Algorithmica*, 16:298–301, 1996.

[2] L. Babai and P. Kimmel. Randomized simultaneous messages. In *Proc. 12th IEEE Symp. on Computational Complexity*, pages 239–246. IEEE, 1997.

[3] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.

[4] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, Cambridge, UK, 1997.

[5] I. Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39:67–71, 1991.

[6] I. Newman and M. Szegedy. Public vs. private coin flips in one round communication games. In *Proc. 28th ACM Symp. on Theory of Computing*, pages 561–570. ACM, 1996.

APPENDIX

Proof of Lemma 1

Recall that η is defined to be $(1-\frac{2k'}{k})^{1/2}$ if $k' \leq k/2$, and 0 otherwise; $\Delta = \eta - | < u|v > |$. We will prove that, for any $\beta > 0$,

$$\Pr\{|\Delta| > \beta\} < 2e^{-k\beta^4/32}.$$

Let $q = (1 - | < v|w > |^2)/2$. By Chernoff's Inequality, for any $\xi > 0$, we have

$$\Pr\{|\frac{k'}{k} - q| > \xi\} < 2e^{-2k\xi^2}.$$

Choose $\xi = \beta^2/8$. Then with probability at least $1-2e^{-2k\xi^2} = 1-2e^{-k\beta^4/32}$, we have

$$-\xi \leq \frac{k'}{k} - \frac{1 - | < u|v > |^2}{2} \leq \xi. \tag{4}$$

To prove Lemma 1, we only need to prove that (6) implies $|\Delta| \leq \beta$.

If $| < u|v > | < \beta/2$, then the leftmost inequality in (6) implies

$$1 - \frac{2k'}{k} \leq | < u|v > |^2 + 2\xi < \frac{\beta^2}{2}.$$

From the definition of η, we conclude then $0 \leq \eta \leq \beta$, and hence $-\beta \leq -| < u|v > | \leq \eta - | < u|v > | \leq \beta$. Therefore, $|\Delta| \leq \beta$ is true in this case.

We now consider the other case: $| < v|w > | \geq \beta/2$. Observe that (6) implies

$$| \, \eta^2 - | < u|v > |^2 \, | \leq 2\xi,$$

leading to

$$|\Delta| = | \, \eta - | < u|v > | \, | \leq \frac{2\xi}{| < u|v > |} \leq 2\frac{\beta^2}{8}\frac{2}{\beta} = \frac{\beta}{2}.$$

This completes the proof of Lemma 1.