Quantum fingerprinting

Harry Buhrman[*]   Richard Cleve[†]   John Watrous[†]   Ronald de Wolf[*]

Abstract

Classical fingerprinting associates with each string a shorter string (its *fingerprint*), such that, with high probability, any two distinct strings can be distinguished by comparing their fingerprints alone. The fingerprints can be exponentially smaller than the original strings if the parties preparing the fingerprints share a random key, but not if they only have access to uncorrelated random sources. In this paper we show that fingerprints consisting of *quantum* information *can* be made exponentially smaller than the original strings without any correlations or entanglement between the parties: we give a scheme where the quantum fingerprints are exponentially shorter than the original strings and we give a test that distinguishes any two unknown quantum fingerprints with high probability. Our scheme implies an exponential quantum/classical gap for the equality problem in the simultaneous message passing model of communication complexity. We optimize several aspects of our scheme.

1 Introduction

Fingerprinting can be a useful mechanism for determining if two strings are the same: each string is associated with a much shorter fingerprint and comparisons between strings are made in terms of their fingerprints alone. This can lead to savings in the communication and storage of information.

The notion of fingerprinting arises naturally in the setting of *communication complexity* (see [KN97]). The particular model of communication complexity that we consider in this paper is called the *simultaneous message passing* model, which was introduced by Yao [Yao79] in his original paper on communication complexity. In this model, two parties—Alice and Bob—receive inputs x and y, respectively, and are not permitted to communicate with one another directly. Rather they each send a message to a third party, called the *referee*, who determines the output of the protocol based solely on the messages sent by Alice and Bob. The collective goal of the three parties is to cause the protocol to output the correct value of some function $f(x, y)$ while minimizing the amount of information that Alice and Bob send to the referee.

For the *equality* problem, the function is simply

$$f(x, y) = \left\{ \begin{array}{ll} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y. \end{array} \right.$$

The problem can of course be trivially solved if Alice sends x and Bob sends y to the referee, who can then simply compute $f(x, y)$. However, the cost of this protocol is high; if x and y are n-bit strings, then a total of $2n$ bits are communicated. If Alice and Bob instead send *fingerprints* of x

and y, which may each be considerably shorter than x and y, the cost can be reduced significantly. The question we are interested in is how much the size of the fingerprints can be reduced.

If Alice and Bob share a random $O(\log n)$-bit key then the fingerprints need only be of *constant* length if we allow a small probability of error; a brief sketch of this follows. A binary error-correcting code is used, which can be represented as a function $E : \{0,1\}^n \to \{0,1\}^m$, where $E(x)$ is the codeword associated with $x \in \{0,1\}^n$. There exist error-correcting codes (Justesen codes, for instance) with $m = cn$ such that the Hamming distance between any two distinct codewords $E(x)$ and $E(y)$ (with $x \neq y$) is at least $(1-\delta)m$, where c and δ are constants. For the particular case of Justesen codes, we may choose any $c > 2$ and we will have $\delta < 9/10 + 1/(15c)$ (assuming n is sufficiently large). For further information on Justesen codes, see Justesen [Jus72] and MacWilliams and Sloane [MS77, Chapter 10]. Now, for $x \in \{0,1\}^n$ and $i \in \{1, 2, \dots, m\}$, let $E_i(x)$ denote the ith bit of $E(x)$. The shared key is a random $i \in \{1, 2, \dots, m\}$ (which consists of $\log(m) \in \log(n) + O(1)$ bits). Alice and Bob respectively send the bits $E_i(x)$ and $E_i(y)$ to the referee, who then outputs 1 if and only if $E_i(x) = E_i(y)$. If $x = y$ then $E_i(x) = E_i(y)$, so then the outcome is correct. If $x \neq y$ then the probability that $E_i(x) = E_i(y)$ is at most δ, so the outcome is correct with probability $1 - \delta$. The error probability can be reduced from δ to any $\varepsilon > 0$ by having Alice and Bob send $O(\log(1/\varepsilon))$ independent random bits of the codewords $E(x)$ and $E(y)$ to the referee. In this case, the length of each fingerprint is $O(\log(1/\varepsilon))$ bits.

One disadvantage of the above scheme is that it requires overhead in creating and maintaining a shared key. Moreover, once the key is distributed, it must be stored securely until the inputs are obtained. This is because an adversary who knows the value of the key can easily choose inputs x and y such that $x \neq y$ but for which the output of the protocol always indicates that $x = y$.

Yao [Yao79, Section 4.D] posed as an open problem the question of what happens in this model if Alice and Bob do not have a shared key. Ambainis [Amb96] proved that fingerprints of $O(\sqrt{n})$ bits suffice if we allow a small error probability (see also [KNR95, NS96, BK97]). Note that in this setting Alice and Bob still have access to random bits, but their random bits may not be correlated. Subsequently, Newman and Szegedy [NS96] proved a matching lower bound of $\Omega(\sqrt{n})$. Their result was generalized by Babai and Kimmel [BK97] to the result that the randomized and deterministic complexity can be at most quadratically far apart for *any* function in this model. Babai and Kimmel attribute a simplified proof of this fact to Bourgain and Wigderson.

We shall consider the problem where there is no shared key (or entanglement) between Alice and Bob, but the fingerprints can consist of quantum information. In Section 2, we show that $O(\log n)$-qubit fingerprints are sufficient to solve the equality problem in this setting—an exponential improvement over the $\sqrt{n}$-bound for the comparable classical case. Our method is to set the 2^n fingerprints to quantum states whose pairwise inner-products are bounded below 1 in absolute value and to use a test that identifies identical fingerprints and distinguishes distinct fingerprints with good probability. (It is possible to take the fingerprints to be nearly pairwise orthogonal, although the bound on the absolute value of the inner product between pairs of states is not directly related to the error probability of the fingerprinting method.) This gives a simultaneous message passing protocol for equality in the obvious way: Alice and Bob send the fingerprints of their respective inputs to the referee, who then executes the test to check if the fingerprints are equal or distinct. In Section 2, we also show that the fingerprints must consist of at least $\Omega(\log n)$ qubits if the error probability is bounded below 1.

In Sections 3 and 4, we consider possible improvements to the efficiency of the fingerprinting methods of Section 2. In Section 3, we investigate the number of qubits required to contain 2^n fingerprints with pairwise inner product bounded in absolute value by any $\delta < 1$. In Section 4, we consider the efficiency of tests that distinguish between k copies of pairs of indentical states and k

2

copies of pairs of states whose inner product is bounded in absolute value by any $\delta < 1$.

Finally, in Section 5 we consider a variation of fingerprinting with a shared *quantum* key, consisting of $O(\log n)$ shared Bell states (EPR-pairs). We observe that results in [BCT99] imply that errorless (i.e., exact) fingerprinting is possible with $O(\log n)$-bit classical fingerprints in a particular context where achieving the same performance with only a classical shared key requires fingerprints of length $\Omega(n)$.

We assume the reader is familiar with the basic notions of quantum computation and quantum information—for further information we refer the reader to the book by Nielsen and Chuang [NC00].

2   Quantum fingerprinting without shared keys

In this section, we show how to solve the equality problem in the simultaneous message passing model with logarithmic-length quantum fingerprints in a context where no shared key is available. The solution is quite simple and the fingerprints are exponentially shorter than in the comparable classical setting, where $\Theta(\sqrt{n})$ bit fingerprints are necessary and sufficient (see the references in the introduction). The method that we present is based on classical error-correcting codes, though in a different manner than discussed in Section 1 since no shared key is available.

Assume that for fixed $c > 1$ and $\delta < 1$ we have an error correcting code $E : \{0,1\}^n \to \{0,1\}^m$ for each n, where $m = cn$ and such that the distance between distinct codewords $E(x)$ and $E(y)$ is at least $(1 - \delta)m$. As mentioned in Section 1, a reasonable first choice of such codes are Justesen codes, which give $\delta < 9/10 + 1/(15c)$ for any chosen $c > 2$. Now, for any choice of n, we define the $(\log(m) + 1)$-qubit state $|h_x\rangle$ as

$$|h_x\rangle = \tfrac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle |E_i(x)\rangle \tag{1}$$

for each $x \in \{0,1\}^n$. Since two distinct codewords can be equal in at most δm positions, for any $x \neq y$ we have $\langle h_x | h_y \rangle \leq \delta m / m = \delta$. Thus we have 2^n different $(\log(n) + O(1))$-qubit states, and each pair of them has inner product at most δ.

The simultaneous message passing protocol for the equality problem works as follows. When given n-bit inputs x and y, respectively, Alice and Bob send fingerprints $|h_x\rangle$ and $|h_y\rangle$ to the referee. Then the referee must distinguish between the case where the two states received—call them $|\phi\rangle$ and $|\psi\rangle$—are identical or have inner product at most δ. This is accomplished with one-sided error probability by the procedure that measures and outputs the first qubit of the state

$$(H \otimes I)(\text{c-SWAP})(H \otimes I)|0\rangle|\phi\rangle|\psi\rangle.$$

Here H is the Hadamard transform, which maps $|b\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$, SWAP is the operation $|\phi\rangle|\psi\rangle \to |\psi\rangle|\phi\rangle$ and c-SWAP is the controlled-SWAP (controlled by the first qubit). The circuit for this procedure is illustrated in Figure 1. By tracing through the execution of this circuit, one can determine that the final state before the measurement is

$$\tfrac{1}{2}|0\rangle(|\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle) + \tfrac{1}{2}|1\rangle(|\phi\rangle|\psi\rangle - |\psi\rangle|\phi\rangle).$$

Measuring the first qubit of this state produces outcome 1 with probability $\frac{1}{2} - \frac{1}{2}|\langle \phi|\psi\rangle|^2$. This probability is 0 if $x = y$ and is at least $\frac{1}{2}(1 - \delta^2) > 0$ if $x \neq y$. Thus, the test determines which case holds with one-sided error $\frac{1}{2}(1 + \delta^2)$.
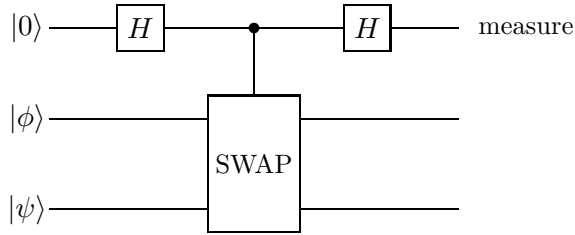
Figure 1: Circuit to test if $|\phi\rangle = |\psi\rangle$ or $|\langle\phi|\psi\rangle| \leq \delta$

The error probability of the test can be reduced to any $\varepsilon > 0$ by setting the fingerprint of $x \in \{0,1\}^n$ to $|h_x\rangle^{\otimes k}$ for a suitable $k \in O(\log(1/\varepsilon))$. From such fingerprints, the referee can independently perform the test in Figure 1 k times, resulting in an error probability below ε. In this case, the length of each fingerprint is $O((\log n)(\log(1/\varepsilon)))$.

It is worth considering what goes wrong if one tries to simulate the above quantum protocol using classical mixtures in place of quantum superpositions. In such a protocol, Alice and Bob send $(i, E_i(x))$ and $(j, E_j(y))$ respectively to the referee for *independent* random uniformly distributed $i, j \in \{1, 2, \ldots, m\}$. If it should happen that $i = j$ then the referee can make a statistical inference about whether or not $x = y$. But $i = j$ occurs with probability only $O(1/n)$—and the ability of the referee to make an inference when $i \neq j$ seems difficult. For many error-correcting codes, no inference whatsoever about $x = y$ is possible when $i \neq j$ and the lower bound in [NS96] implies that no error-correcting code enables inferences to be made when $i \neq j$ with error probability bounded below 1. The distinguishing test in Figure 1 can be viewed as a quantum operation which has no analogous classical probabilistic counterpart.

Our quantum protocol for equality in the simultaneous message model uses $O(\log n)$-qubit fingerprints for any constant error probability. Is it possible to use fewer qubits? In fact, without a shared key, $\Omega(\log n)$-qubit fingerprints are necessary. This is because any k-qubit quantum state can be specified within exponential precision with $O(k2^k)$ classical bits. Therefore the existence of a k-qubit quantum protocol implies the existence of an $O(k2^k)$-bit (deterministic) classical protocol. From this we can infer that $k \in \Omega(\log n)$.

3 Sets of pairwise-distinguishable states in low-dimensional spaces

In Section 2, we employed a particular classical error-correcting code to construct a set of 2^n quantum states with pairwise inner products below δ in absolute value. Here, we consider the question of how few qubits are sufficient for this to be accomplished for an arbitrarily small $\delta > 0$. We show that $\log n + O(\log(1/\delta))$ qubits are sufficient. While this gives somewhat better bounds than the Justesen codes discussed in Section 2, unfortunately we only have a nonconstructive proof of this fact. The proof follows.

Suppose $d \geq \frac{4n}{\delta^2 \log e}$. Then we claim there are 2^n unit vectors in $\mathbb{R}^d$ with pairwise inner product at most δ in absolute value. Consider two random vectors in v, w in $\{+1, -1\}^d/\sqrt{d}$. Suppose v and w agree in d' coordinates and disagree in $d - d'$ coordinates, then their inner product is $\langle v|w\rangle = (2d' - d)/d$. Using a Chernoff bound [AS92, Corollary A.2] we have

$$\Pr[|\langle v|w\rangle| > \delta] = \Pr[|2d' - d| > \delta d] \leq 2e^{-\delta^2 d/2}.$$

4

Now pick a set S of 2^n random vectors from $\{+1, -1\}^d/\sqrt{d}$. The probability that there are distinct $v, w \in S$ with large inner product is upper bounded by

$$
\begin{aligned}
\Pr[\exists \text{ distinct } v, w \in S \text{ with } |\langle v|w\rangle| > \delta] \quad &\leq \sum_{\text{distinct } v,w \in S} \Pr[|\langle v|w\rangle| > \delta] \\
&< \binom{2^n}{2} 2 e^{-\delta^2 d/2} < 2^{2n - \delta^2 d \log e/2}.
\end{aligned}
$$

If $d \geq 4n/\delta^2 \log e$ then this probability is < 1, which implies the existence of a set S of 2^n vectors having the right properties.

By associating $\{0, 1\}^n$ with the 2^n vectors above, we obtain fingerprints of $\log(4n/\delta^2 \log e) \in \log n + O(\log(1/\delta))$ qubits for any $\delta > 0$.

Up to constant factors, the nonconstructive method above is optimal in the following sense. Let $\delta \geq 2^{-n}$. Then an assignment of b-qubit states to all n-bit strings such that the absolute value of the inner product between any two fingerprints is at most δ, requires $b \in \Omega(\log(n/\delta))$ qubits. In order to demonstrate this, we will prove and then combine two lower bounds on b.

Firstly, the states can be used as fingerprints to solve the equality problem of communication complexity with bounded-error probability in one round of communication (Alice sends the fingerprint of her input x to Bob, who compares it with the fingerprint of his y). Therefore the known lower bound for equality implies $b \geq c \log n$ for some $c > 0$.

Secondly, pick a set of $a = 1/\delta$ different fingerprints. These are complex unit vectors $v_1, \ldots, v_a$ of dimension 2^b, whose pairwise inner products are at most δ in absolute value. Let A be the $a \times 2^b$ matrix having the conjugated vectors v_i as rows and let B be the $2^b \times a$ matrix having the v_i as columns. Consider the $a \times a$ matrix $C = AB$. Its i, j entry is $C_{ij} = \langle v_i | v_j \rangle$, so the diagonal entries of C are 1, the off-diagonal entries are at most δ in absolute value. This means that C is strictly diagonally dominant: $C_{ii} = 1 > (a - 1)\delta \geq \sum_{j \neq i} |C_{ij}|$ for all i. It is known that such a matrix has full rank [HJ85, Theorem 6.1.10.a]. This implies that the a vectors $v_1, \ldots, v_a$ are linearly independent and hence must have dimension at least a. Thus $1/\delta = a \leq 2^b$, hence $b \geq \log(1/\delta)$.

Since both lower bounds on b hold simultaneously, we have

$$
b \geq \max\{c \log n, \log(1/\delta)\} \geq \frac{c \log n + \log(1/\delta)}{2} \in \Omega(\log(n/\delta)).
$$

It should be noted that having small inner product δ is desirable but not all-important. For instance, there is a trade-off between δ and the number of copies of each state sent by Alice and Bob in the simultaneous message passing protocol for equality from the previous section in terms of the total number of qubits communicated and the resulting error bound.

4 The state distinguishing problem

Motivated by the fingerprinting scheme of Section 2, we define the *state distinguishing problem* as follows. The input consists of k copies of each of two quantum states $|\phi\rangle$ and $|\psi\rangle$ with a promise that the two states are either identical or have inner product bounded in absolute value by some given $\delta < 1$. The goal is to distinguish between the two cases with as high probability as possible.

One method for solving this problem is to use the method in Section 2, independently performing the test in Figure 1 k times, resulting in an error probability of 0 in the identical case and $(\frac{1+\delta^2}{2})^k$ otherwise. We will describe an improved method, whose error probability is approximately $\sqrt{\pi k}(\frac{1+\delta}{2})^{2k}$ (which is almost a quadratic reduction when δ is small). We also show that this is nearly optimal by proving a lower bound of $\frac{1}{4}(\frac{1+\delta}{2})^{2k}$ on the error probability.

5

The improved method for the state distinguishing problem uses registers $R_1, \ldots, R_{2k}$, which initially contain $|\phi\rangle, \ldots, |\phi\rangle, |\psi\rangle, \ldots, |\psi\rangle$ (k copies of each). It also uses a register P whose classical states include encodings of all the permutations in S_{2k}. Let 0 denote the identity permutation and let P be initialized to 0. Let F be any transformation satisfying

$$F : |0\rangle \mapsto \frac{1}{\sqrt{(2k)!}} \sum_{\sigma \in S_{2k}} |\sigma\rangle.$$

Such a transformation can easily be computed in polynomial time.

The distinguishing procedure operates as follows:

1. Apply F to register P.

2. Apply a conditional permutation on the contents of registers $R_1, \ldots, R_{2k}$, conditioned on the permutation specified in P.

3. Apply $F^\dagger$ to P and measure the final state. If P contains 0 then answer *equal*, otherwise answer *not equal*.

The state after is Step 2 is

$$\frac{1}{\sqrt{(2k)!}} \sum_{\sigma \in S_{2k}} |\sigma\rangle \sigma(|\phi\rangle \cdots |\phi\rangle |\psi\rangle \cdots |\psi\rangle)$$

(where $\sigma(|\phi\rangle \cdots |\phi\rangle |\psi\rangle \cdots |\psi\rangle)$ means we permute the contents of the $2k$ registers according to σ).

Case 1: $|\phi\rangle = |\psi\rangle$. In this case the permutation of the registers does absolutely nothing, so the procedure answers *equal* with certainty.

Case 2: Assume $|\langle \phi | \psi \rangle| < \delta$. The probability of answering *equal* is the squared norm of the vector obtained by applying the projection $|0\rangle\langle 0| \otimes I$ to the final state, which is

$$
\begin{aligned}
p_{eq} &= \left\| \frac{1}{\sqrt{(2k)!}} \sum_{\sigma \in S_{2k}} \langle 0 | F^\dagger | \sigma \rangle \sigma(|\phi\rangle \cdots |\phi\rangle |\psi\rangle \cdots |\psi\rangle) \right\|^2 \\
&= \left\| \frac{1}{(2k)!} \sum_{\sigma \in S_{2k}} \sigma(|\phi\rangle \cdots |\phi\rangle |\psi\rangle \cdots |\psi\rangle) \right\|^2 .
\end{aligned}
$$

Since $\||\eta\rangle\|^2 = \langle \eta | \eta \rangle$ for any $|\eta\rangle$ we may simplify this probability as follows:

$$
\begin{aligned}
p_{eq} &= \frac{1}{((2k)!)^2} \sum_{\sigma, \tau \in S_{2k}} \sigma((\langle \phi | \cdots \langle \phi | \langle \psi | \cdots \langle \psi |) \tau(|\phi\rangle \cdots |\phi\rangle |\psi\rangle \cdots |\psi\rangle)) \\
&= \frac{1}{((2k)!)^2} \sum_{\sigma, \tau \in S_{2k}} \langle \phi | \cdots \langle \phi | \langle \psi | \cdots \langle \psi | \sigma^{-1} \tau(|\phi\rangle \cdots |\phi\rangle |\psi\rangle \cdots |\psi\rangle) \\
&= \frac{1}{(2k)!} \sum_{\sigma \in S_{2k}} \langle \phi | \cdots \langle \phi | \langle \psi | \cdots \langle \psi | \sigma(|\phi\rangle \cdots |\phi\rangle |\psi\rangle \cdots |\psi\rangle) \\
&= \frac{(k!)^2}{(2k)!} \sum_{j=0}^{k} \binom{k}{j}^2 \delta^{2j} \\
&\le \frac{(k!)^2}{(2k)!} (1+\delta)^{2k} .
\end{aligned}
$$

The sum of binomial coefficients arises by grouping the permutations σ according to the number of registers j in the set $\{R_1, \ldots, R_k\}$ that σ causes to contain $|\psi\rangle$. We therefore have $p_{eq} \sim \sqrt{\pi k}(\frac{1+\delta}{2})^{2k}$.

We now show that the error probability cannot be less than $\frac{1}{4}(\frac{1+\delta}{2})^{2k}$ for the state distinguishing problem.[1] Consider an optimal *state distinguisher* that acts on k copies of $|\phi\rangle$ and k copies of $|\psi\rangle$ where either $|\phi\rangle = |\psi\rangle$ or $|\langle\phi|\psi\rangle| \leq \delta$. Let $|\phi_1\rangle = |\psi_1\rangle = |0\rangle$, and let $|\phi_2\rangle = \cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})|1\rangle$ and $|\psi_2\rangle = \cos(\frac{\theta}{2})|0\rangle - \sin(\frac{\theta}{2})|1\rangle$, where $\theta = \cos^{-1}(\delta)$. Clearly, $|\phi_1\rangle = |\psi_1\rangle$ and $\langle\phi_2|\psi_2\rangle = \delta$. A state distinguisher must distinguish between the state $|a\rangle = |\phi_1\rangle^{\otimes k} \otimes |\psi_1\rangle^{\otimes k}$ and the state $|b\rangle = |\phi_2\rangle^{\otimes k} \otimes |\psi_2\rangle^{\otimes k}$. We now consider the probability with which a state distinguisher can distinguish between these states. Since $\langle\phi_1|\phi_2\rangle = \langle\psi_1|\psi_2\rangle = \cos(\frac{\theta}{2})$, it follows that $\langle a|b\rangle = \cos^{2k}(\frac{\theta}{2}) = (\frac{1+\cos\theta}{2})^k = (\frac{1+\delta}{2})^k$. Now, it is known that the optimal procedure distinguishing between two states with inner product $\cos\alpha$ has error probability $\frac{1-\sin\alpha}{2} \geq \frac{1}{4}\cos^2\alpha$. (This follows from an early result of Helstrom [Hel67], which was later strengthened by Fuchs [Fuc95, Section 3.2]. A clean and self-contained derivation of this result may also be found in [Pre00].) Therefore, the state distinguisher must have error probability at least $\frac{1}{4}(\frac{1+\delta}{2})^{2k}$.

5 Errorless fingerprinting using a shared quantum key

Finally, we consider briefly the case of fingerprinting where Alice and Bob have a shared *quantum key*, consisting of $O(\log n)$ Bell states, but are required to output *classical* strings as fingerprints. Is there any sense in which a quantum key can result in improved performance over the case of a classical key? We observe that results in [BCT99] imply an improvement in the particular setting where the fingerprinting scheme must be exact (i.e., the error probability is 0) and where there is a restriction on the inputs that either $x = y$ or the Hamming distance between x and y is $n/2$ (and n is divisible by 4).

Under this restriction, any classical scheme with a shared key would still require fingerprints of length $\Omega(n)$. On the other hand, there is a scheme with a shared quantum key of $O(\log n)$ Bell states that requires fingerprints of length only $O(\log n)$ bits. See [BCT99] for details (the results are partly based on results in [BCW98, FR87]). It should be noted that if the exactness condition is relaxed to one where the error probability must be $O(1/n^c)$ (for a constant c) then there exists also a classical scheme with classical keys and fingerprints of length $O(\log n)$.

References

[Amb96]   A. Ambainis. Communication complexity in a 3-computer model. *Algorithmica*, 16(3):298–301, 1996.

---

[1]Note that this lower bound concerns a problem that is slightly more general than the problem of distinguishing *fingerprints*, because the fingerprints used in Section 2 are not arbitrary but come from a known set of only 2^n states.

[ANTV99] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Quantum dense coding and a lower bound for 1-way quantum finite automata. In *Proceedings of 31st ACM STOC*, pages 376–383, 1999. quant-ph/9804043.

[AS92] N. Alon and J. H. Spencer. *The Probabilistic Method*. Wiley-Interscience, 1992.

[BCT99] G. Brassard, R. Cleve, and A. Tapp. The cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letters*, 83(9):1874–1877, 1999. quant-ph/9901035.

[BCW98] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In *Proceedings of 30th ACM STOC*, pages 63–68, 1998. quant-ph/9802040.

[BK97] L. Babai and P. G. Kimmel. Randomized simultaneous messages: Solution of a problem of Yao in communication complexity. In *Proceedings of the 12th Annual IEEE Conference on Computational Complexity*, pages 239–246, 1997.

[CSB93] J. Conway, N. Sloane, and E. Bannai, editors. *Sphere Packings, Lattices and Groups*. Springer, second edition, 1993.

[FR87] P. Frankl and V. Rödl. Forbidden intersections. *Transactions of the American Mathematical Society*, 300(1):259–286, 1987.

[Fuc95] C. A. Fuchs. *Distinguishability and Accessible Information in Quantum Theory*. PhD thesis, University of New Mexico, Albuquerque, 1995. quant-ph/9601020.

[Hel67] C. W. Helstrom. Detection theory and quantum mechanics. *Information and Control*, 10(1):254–291, 1967.

[HJ85] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, 1985.

[Jus72] J. Justesen, A class of constructive asymptotically good algebraic codes. *IEEE Trans. Inform. Theory*, 18:652–656, 1972.

[KN97] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1997.

[KNR95] I. Kremer, N. Nisan, and D. Ron. On randomized one-round communication complexity. In *Proceedings of 27th ACM STOC*, pages 596–605, 1995.

[MS77] F. MacWilliams and N. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NS96] I. Newman and M. Szegedy. Public vs. private coin flips in one round communication games. In *Proceedings of 28th ACM STOC*, pages 561–570, 1996.

[Pre00] J. Preskill. Solutions for problem set 2, ex. 1, from course ph/229 on quantum computation. Available at http://www.theory.caltech.edu/people/preskill/ph229/#homework, 2000.

[Yao79] A. C-C. Yao. Some complexity questions related to distributive computing. In *Proceedings of 11th ACM STOC*, pages 209–213, 1979.