数理解析研究所講究録
1489 巻 2006 年 114-120

Complexity-Theoretical Quantum List Decoding and Applications to Quantum Hardcore Functions

Akinori Kawachi *
(河内 亮周)

Tomoyuki Yamakami †
(山上 智幸)

Abstract— We present three new quantum hardcore functions for any quantum one-way function. We also give a "quantum" solution to Damgård's question (CRYPTO'88) on his pseudorandom generator by proving the quantum hardcore property of his generator, which has been unknown to have the classical hardcore property. Our technical tool is quantum list-decoding of "classical" error-correcting codes (rather than "quantum" error-correcting codes), which is defined on the platform of computational complexity theory and cryptography (rather than information theory). In particular, we give a simple but powerful criterion that makes a polynomial-time computable code (seen as a function) a quantum hardcore for any quantum one-way function. On their own interest, we also give quantum list-decoding algorithms for codes whose associated quantum states (called codeword states) are "almost" orthogonal using the technique of pretty good measurement.

Keywords: quantum hardcore, quantum one-way, quantum list-decoding, codeword state, phase orthogonal, presence, Johnson bound

1 Introduction: From Hardcore to List-Decoding

Background: Modern cryptography heavily relies on computational hardness and pseudorandomness. One of its key notions is a *hardcore* bit of a one-way function—a bit that can be completely determined by the information available to the adversary but still looks random to any feasible adversary. A hardcore function transforms the onewayness into pseudorandomness by generating such hardcore bits of a given one-way function. Such a hardcore function is a crucial element of constructing a pseudorandom generator as well as a bit commitment protocol from a one-way permutation. A typical example is the inner product mod 2 function $\mathrm{GL}_x(r)$ of Goldreich and Levin [12], computing the bitwise inner product modulo two $\langle x, r\rangle$, which constitutes a hardcore bit for any (strong) one-way function. [1] Since $\mathrm{GL}_x(r)$ equals the rth bit of the codeword $\mathrm{HAD}_x^{(2)} = (\langle x, 0^n\rangle, \langle x, 0^{n-1}1\rangle, \cdots, \langle x, 1^n\rangle)$ of message x of a binary Hadamard code, Goldreich and Levin essentially gave a polynomial-time list-decoding algorithm for this Hadamard code. In the recent literature, list-decoding has kept playing a key role in a general construction of hardcores [2, 17].

Thirteen years later, the "quantum" hardcore property (i.e., a hardcore property against feasible quantum adversary) of $\mathrm{GL}_x(\cdot)$ was shown by Adcock and Cleve [1], who implicitly gave a simple and efficient quantum algorithm that list-decodes x for the binary Hadamard code by exploiting the robust nature of a quantum algorithm of Bernstein and Vazirani [6]. The simplicity of the proof of Adcock and Cleve can be best compared to the original proof of Goldreich and Levin, who employed a rather complicated algorithm with powerful techniques: self-correction property of the aforementioned Hadamard code and pairwise independent sampling. This highlights a significant role of robust quantum computation in list-decoding (and thus hardcores); however, it has been vastly unexplored until our work except for a quantum decoder of Barg and Zhou [5] for the simplex code. No other quantum hardcore has been proven so far. The efficiency of robust quantum algorithms with access to biased oracles has been also discussed in a different context [3, 7, 18].

Our Major Contributions: As our main result, we present three new quantum hardcore functions, $\mathrm{HAD}^{(q)}$, SLS^p, and PEQ (see Section 5 for their definition), for any (strongly) quantum one-way function, the latter two of which are not yet known to be hardcores in a classical setting (see [13]). In particular, we prove the quantum hardcore property of Damgård's pseudorandom generator [8]. This gives a "quantum" solution to his question of whether his generator has the classical hardcore property (this is also listed as an open problem in [13]). Our proof technique exploits quantum list-decodability of classical error-correcting codes (rather than quantum error-correcting codes). For our purpose, we formulate the notion of *complexity-*

* Department of Mathematical and Computing Sciences, Tokyo Institute of Technology. W8-55, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan. kawachi@is.titech.ac.jp.

† ERATO-SORST Quantum Computation and Information Project, Japan Science and Technology Agency, 5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan. yamakami@qci.jst.go.jp

[1] Literally speaking, this statement is slightly misleading. To be more accurate, such a hard-core function concerns only the one-way function of the form $f'(x, r) = (f(x), r)$ with $|r| = poly(|x|)$ induced from an arbitrary strong one-way function f. See, e.g., [11] for a detailed discussion.

theoretical quantum list-decoding to conduct message-recovery from quantum-computational error rather than information-theoretical error which is usually associated with transmission error. This notion naturally expands the classical framework of list-decoding. Our goal is to give fast quantum list-decoding algorithms for the aforementioned codes.

Proving the quantum hardcore property of a given code C (seen as a function) corresponds to solving the *quantum list-decoding problem* (QLDP) for C via direct access to a *quantum-computationally (or quantumly) corrupted word*, which is given as a black-box oracle. The task of a quantum list-decoder is simply to list all message candidates whose codewords match the quantumly-corrupted word within a certain error rate bound.

The key notion of this paper is a specific quantum state, called a *(k-shuffled) codeword state*, which embodies the full information on a given codeword. Note that similar states have appeared in several quantum algorithms in the literature [6, 9, 14, 20]. In our key lemmas, we show (i) how to generate such a codeword state from *any* (even adversarial) quantumly corrupted word and (ii) how to convert a *codeword-state decoder* (i.e., a quantum algorithm that recovers a message x from a codeword state given as an input) to a quantum list-decoding algorithm working with a quantumly corrupted word. The robust construction made in the course of our proofs also provides a useful means, known as "hardness" reduction, which is often crucial in the security proof of a quantum cryptosystem. Moreover, using pretty good measurement [10, 16], we present a quantum list-decoding algorithm for any code whose codeword states are "almost" orthogonal.

Further Implications: Classical list-decodable codes have provided numerous applications in the theory of classical computational complexity, including proving hardcores for any one-way function, hardness amplification, and derandomization (see, e.g., [19]). Because our formulation of quantum list-decoding naturally extends classical one, classical list-decoding algorithms (e.g., for Reed-Solomon codes) work in our quantum setting as well. This will make our quantum list-decoding a powerful tool in quantum complexity theory and quantum computational cryptography.

2 Quantum Hardcore Functions

We begin with the notion of a quantum one-way function, which naturally expands the classical notion of one-way function. The notion has been studied in the recent literature.

Definition 2.1 A function f from $\{0,1\}^*$ to $\{0,1\}^*$ is called *(strongly) quantum one-way* if (i) there exists a polynomial-time deterministic algorithm G computing f and (ii) for any polynomial-time quantum algorithm A, for any positive polynomial p, and for any sufficiently large n, $\Pr_{x\in\{0,1\}^n,\mathcal{A}}[f(\mathcal{A}(f(x),1^n)) = f(x)] < 1/p(n)$, where x is uniformly distributed over $\{0,1\}^n$ and the subscript $\mathcal{A}$ is a random variable determined by measuring the final state of A on the computational basis. We consider only *length-regular* (i.e., $|f(x)| = l(|x|)$ for length function $l(n)$) one-way functions.

For any quantum one-way function f, the notation f' denotes the function induced from f by the scheme: $f'(x,r) = (f(x),r)$ for all $x,r \in \{0,1\}^*$ with $|r| = poly(|x|)$. Note that f' is also a quantum one-way function. Throughout this paper, we deal only with quantum one-way function of this form in direct connection to quantum hardcores.

The standard definition of a hardcore function h from $\{0,1\}^n$ to $\{0,1\}^{l(n)}$ is given in terms of the indistinguishability between $h(x)$ and a truly random variable over $\{0,1\}^{l(n)}$. Although a hardcore predicate (i.e., a hardcore function of output length $l(n) = 1$) is usually defined using the notion of *nonapproximability* instead of indistinguishability, it is well-known that both notions coincide for hardcore functions of output length $O(\log n)$ (see Excise 31 in [11]). In this paper, we conveniently define our quantum hardcores in terms of nonapproximability.

Definition 2.2 Let f be any length-regular function. A polynomial-time computable function h with length function $l(n)$ is called a *quantum hardcore* of f if, for any polynomial-time quantum algorithm $\mathcal{A}$, for any polynomial p, and for any sufficiently large n,

$$\left| \Pr_{x\in\{0,1\}^n,\mathcal{A}}[\mathcal{A}(f(x),1^n) = h(x)] - 1/2^{l(n)} \right| < 1/p(n),$$

where x is uniformly distributed over $\{0,1\}^n$ and the subscript $\mathcal{A}$ is a random variable determined by measuring the final state of A on the computational basis.

3 How to Prove Quantum Hardcores

We outline our argument of proving quantum hardcore functions for any quantum one-way function. To prove new quantum hardcores, we exploit the notion of quantum list-decoding as a technical tool. Our approach toward list-decoding is, however, *complexity-theoretical* in nature rather than information-theoretical. Our main objects of quantum list-decoding are "classical" codes and codewords, which are manipulated in a quantum fashion. Generally speaking, a *code* is a set of strings of the same length over a finite alphabet Σ. Each string is indexed by a message and is called a *codeword*. A *code family* is specified by a series $(\Gamma_n, I_n, \Sigma_n)$ of message space Γ_n, index set I_n, and code alphabet Σ_n for each length parameter n. For simplicity, let $\Gamma^* = \bigcup_{n\in\mathbb{N}} \Gamma_n$.

Usually, a code (family) C consists of codewords C_x for each message $x \in \Gamma^*$. As standard in computational complexity theory, we view the code C as a function that, for each *message length* n (which serves as a *basis parameter* in this paper), maps $\Gamma_n \times I_n$ to Σ_n. Let $N(n) = |\Gamma_n|$ and $q(n) = |\Sigma_n|$. It is convenient to assume that $\Gamma_n \subseteq (\Sigma_n)^n$ so that n actually represents the *length* of a message. By abbreviating $C(x, y)$ as $C_x(y)$, we also treat $C_x(\cdot)$ as a function mapping I_n to Σ_n. Denote by $M(n)$ the *block length* $|I_n|$ of codeword C_x. We simply set $I_n = \{0, 1, \ldots, M(n)-1\}$, each element of which can be expressed in $\lceil \log_2 M(n) \rceil$ bits. We freely identify C_x with the vector $(C_x(0), C_x(1), \cdots, C_x(M(n) - 1))$ in the *ambient space* $(\Sigma_n)^{M(n)}$ of dimension $M(n)$. We often work on a finite field and it is convenient to regard Σ_n as the finite field $\mathbb{F}_{q(n)}$ of numbers $0, 1, \ldots, q(n) - 1$. The *(Hamming) distance* $d(C_x, C_y)$ between two codewords C_x and C_y is the number of non-zero components in the vector $C_x - C_y$. The *minimal distance* $d(C)$ of a code C is the smallest distance between any pair of distinct codewords in C. The above-described code is simply called a $(M(n), n)_{q(n)}$-code[2] (or $(M(n), n, d(n))$-code if $d(n)$ is emphasized). We often drop a length parameter n from subscript and argument place whenever we discuss a set of codewords with a "fixed" n (for instance, $\Gamma = \Gamma_n$ and $M = M(n)$).

Now, we wish to prove that a code $C(x, r)$ (seen as a function) is indeed a quantum hardcore for any quantum one-way function of the form $f'(x, r) = (f(x), r)$ with $|r| = poly(|x|)$. First, we assume to the contrary that there exists a feasible quantum algorithm $\mathcal{A}$ that approximates $C_x(r)$ from input $(f(x), r)$ with probability $\geq 1/q(n) + \varepsilon(n)$. To be more precise, the outcome of $\mathcal{A}$ on input (y, r), where $r \in I_n$ and $y = f(x)$ for a certain $x \in \Gamma_n$, is of the form:

$$\mathcal{A}(y, r) = \alpha_{y,r,C_x(r)}|r\rangle|C_x(r)\rangle|\phi_{y,r,C_x(r)}\rangle + \sum_{s \in \Sigma_n - \{C_x(r)\}} \alpha_{y,r,s}|r\rangle|s\rangle|\phi_{y,r,s}\rangle$$

for certain amplitudes $\alpha_{y,r,s}$ and ancilla quantum states $|\phi_{x,r,s}\rangle$, where the second register corresponds to the output of the algorithm. For each fixed y, the algorithm $\mathcal{A}_y(\cdot) =_{def} \mathcal{A}(y, \cdot)$ gives rise to the (unitary) oracle $\tilde{O}_{\mathcal{A}_y}$ defined by the maps:

$$\tilde{O}_{\mathcal{A}_y}|r\rangle|u\rangle|t\rangle = \sum_{s \in \Sigma} \alpha_{y,r,s}|r\rangle|u \oplus s\rangle|t \oplus \phi_{y,r,s}\rangle$$

for any strings (r, u, t), where $\oplus$ is the bitwise XOR and the notation $|t \oplus \phi_{y,r,s}\rangle$ denotes the quantum state $\sum_{v:|v|=|t|}\langle v|\phi_{y,r,s}\rangle|t \oplus v\rangle$. This oracle $\tilde{O}_{\mathcal{A}_y}$ describes *computational error* (not transmission error) occurring during the computation of C_x. This type of erroneous quantum computation is similar to the computational errors (e.g., [1, 3, 4, 18]) dealt with in quantum computational cryptography and quantum algorithm designing. Remember that $\tilde{O}_{\mathcal{A}_y}$ may choose amplitudes $\{\alpha_{y,r,s}\}_{r,s}$ adversely, not favorably.

Similar to the notion of a classically *received word* in coding theory, we introduce our terminology concerning an oracle which represents a "quantum-computationally" corrupted word.

Definition 3.1 Fix $n \in \mathbb{N}$. We say that an oracle $\tilde{O}$ *represents a quantum-computationally (or quantumly) corrupted word* if $\tilde{O}$ satisfies $\tilde{O}|r\rangle|u\rangle|t\rangle = \sum_{s \in \Sigma} \alpha_{r,s}|r\rangle|u \oplus s\rangle|t \oplus \phi_{r,s}\rangle$ for certain unit vectors $|\phi_{r,s}\rangle$ depending only on (r, s). For convenience, we identify a quantumly corrupted word with its representing oracle.

To lead to the desired contradiction, we wish to invert f by "decoding" x from the quantumly corrupted word $\tilde{O}$. Notice that the entity $(1/M(n)) \sum_{r \in I_n} |\alpha_{r,C_x(r)}|^2$ yields the probability of $\mathcal{A}$'s computing $C_x(\cdot)$ correctly on average. This entity also indicates "closeness" between a codeword C_x and its quantumly corrupted word $\tilde{O}$. In classical list-decoding, for any given oracle $\tilde{O}$ that represents a *received word* and for any error bound e, we need to output a list that include all messages x such that the relative (Hamming) distance between codeword C_x and its received word $\tilde{O}$ is at most $1 - e$ (i.e., $\Pr_{r \in I_n}[\tilde{O}(r) = C_x(r)] \geq 1 - e$). By setting $p_{r,s} = 1$ if $\tilde{O}(r) = s$ and 0 otherwise, the behavior of $\tilde{O}$ can be viewed in a unitary style as $\tilde{O}|r\rangle|0\rangle = \sum_{r \in I_n} p_{r,s}|r\rangle|s\rangle$. The aforementioned entity $(1/M(n)) \sum_{r \in I_n} |\alpha_{r,C_x(r)}|^2$ equals the relative distance, $\Pr_{r \in I_n}[\tilde{O}(r) = C_x(r)]$, in a classical setting. For our convenience, we name this entity the *presence* of C_x in $\tilde{O}$ and denote it by $\mathrm{Pre}_{\tilde{O}}(C_x)$. The requirement for the error rate of classical list-decoding is rephrased as $\mathrm{Pre}_{\tilde{O}}(C_x) \geq 1 - e$.

Here, we formulate a quantum version of a classical list-decoding problem using our notions of quantumly corrupted words and presence. Let $C = \{C_x\}_{x \in \Gamma^*}$ be any $(M(n), n, d(n))_{q(n)}$-code.

QUANTUM LIST DECODING PROBLEM (QLDP) FOR CODE C

> INPUT: a message length n, an error bias ε, and a confidence parameter δ.
>
> IMPLICIT INPUT: an oracle $\tilde{O}$ representing a quantumly corrupted word.
>
> OUTPUT: with success probability at least $1 - \delta$, a list of messages that include all messages $x \in \Gamma_n$ such that $\mathrm{Pre}_{\tilde{O}}(C_x) \geq 1/q(n) + \varepsilon$; that is, codewords C_x have "slightly" higher presence in $\tilde{O}$ than the average.

For any given quantumly corrupted word $\tilde{O}$, how many messages x satisfy the required inequality $\mathrm{Pre}_{\tilde{O}}(C_x) \geq 1/q(n) + \varepsilon$? An upper bound on the number of such

[2] In some literature, the notation $(M(n), N(n))_{q(n)}$ is used instead.

messages directly follows from a nice argument of Guruswami and Sudan [15], who gave a q-ary extension of Johnson bound using a geometric method.

Lemma 3.2 Let n be any message length. Let $\varepsilon(n)$, $q(n)$, $d(n)$, and $M(n)$ satisfy that $\varepsilon(n) > \ell(n) =_{def} (1 - 1/q(n))\sqrt{1 - d(n)/M(n)(1 + 1/(q(n) - 1))}$. For any $(M(n), n, d(n))_{q(n)}$-code C and for any quantumly corrupted word $\tilde{O}$, there are at most $J(n) =_{def}$

$$\min\left\{M(n)(q(n)-1), \frac{d(n)(1-1/q(n))}{d(n)(1-1/q(n)) + M(n)\varepsilon(n)^2 - M(n)(1-1/q(n))^2}\right\}$$

messages $x \in \Gamma_n$ such that $\mathrm{Pre}_{\tilde{O}}(C_x) \geq 1/q(n) + \varepsilon(n)$. If $\varepsilon(n) = \ell(n)$, then the above bound is replaced by $2M(n)(q(n) - 1) - 1$.

The proof of Lemma 3.2 is obtained by an adequate modification of the proof in [15]. As a simple example, consider the $(q^n, n, q^n - q^{n-1})_q$ Hadamard code $\mathrm{HAD}^{(q)} = \{\mathrm{HAD}_x^{(q)}\}_{x\in\Gamma_n}$. Lemma 3.2 guarantees that, for any quantumly corrupted word $\tilde{O}$, there are only at most $(1 - 1/q)^2/\varepsilon(n)^2$ messages x that satisfy the inequality $\mathrm{Pre}_{\tilde{O}}(\mathrm{HAD}_x^{(q)}) \geq 1/q + \varepsilon(n)$.

Definition 3.3 Let C be any code. Any quantum algorithm $\mathcal{A}$ that solves the QLDP for C is called a *quantum list-decoding algorithm* for C. If $\mathcal{A}$ further runs in time polynomial in $(n, 1/\varepsilon, 1/\delta)$, it is called a *polynomial-time quantum list-decoding algorithm* for C.

To complete our argument (which we started at the beginning of this section), assume that there exists a polynomial-time quantum list-decoding algorithm that solves the QLDP for $C_x(\cdot)$. Such a list-decoder may output with high probability all possible candidates x' of required presence. Since we can check that $x' \in f^{-1}(x)$ in polynomial time, the list-decoder gives rise to a polynomial-time quantum algorithm that inverts f with high probability. Clearly, this contradicts the quantum one-wayness of f. Therefore, we obtain the following key theorem that bridges between quantum hardcores and quantum list-decoding.

Theorem 3.4 Let $C = \{C_x\}_{x\in\Gamma^*}$ be any $(M(n), n, d(n))_{q(n)}$-code, which is also polynomial-time computable, where $\log_2 M(n) \in n^{O(1)}$ and $\log_2 q(n) \in n^{O(1)}$. If there exists a polynomial-time quantum list-decoding algorithm for C for any sufficiently large number n, then $C(x, r)$ is a quantum hardcore function for any quantum one-way function of the form $f'(x, r) = (f(x), r)$ with $|x| = \lceil \log_2 |\Gamma_n| \rceil$ and $|r| = \lceil \log_2 M(n) \rceil$.

4 How to Construct Quantum List-Decoding Algorithms

Due to Theorem 3.4, it suffices to solve the QLDP for any given candidate of quantum hardcore functions. Our goal is now to find a way to construct a polynomial-time quantum list-decoder for a wide range of codes. Classically, however, it seems hard to design such list-decoding algorithms in general. Nevertheless, the robust nature of quantum computation enables us to prove that, if we have a decoding algorithm $\mathcal{A}$ from a unique quantum state (called a *codeword state*), then we can construct a list-decoding algorithm by calling $\mathcal{A}$ as a black-box oracle. The notion of such codeword states plays our central role as a technical tool in proving new quantum hardcores in Section 5.

Hereafter, we assume the arithmetic (multiplication, addition, subtraction, etc.) on the finite field $\mathbf{F}_q$ (of numbers $0, 1, \ldots, q - 1$), where q is a prime. Denote by ω_q the complex number $e^{2\pi i/q}$.

Definition 4.1 Let $C = \{C_x\}_{x\in\Gamma_n}$ be any $(M(n), n)_{q(n)}$-code and let k be any number in $\mathbf{F}_{q(n)}$. A *k-shuffled codeword state* for codeword C_x that encodes a message $x \in \Gamma_n$ is the quantum state

$$|C_x^{(k)}\rangle = \frac{1}{\sqrt{M(n)}} \sum_{r\in I_n} \omega_{q(n)}^{k\cdot C_x(r)} |r\rangle.$$

In particular when $k = 1$, we write $|C_x\rangle$ instead of $|C_x^{(1)}\rangle$.

Remark: Codeword states for binary codes have appeared implicitly in several important quantum algorithms. For instance, Grover's search algorithm [14] produces such a codeword state after the first oracle call. In the quantum algorithms of Bernstein and Vazirani [6], of Deutch and Jozsa [9], and of van Dam, Hallgren, and Ip [20], such codeword states were generated to obtain their desired results.

We consider how to generate the k-shuffled codeword state $|C_x^{(k)}\rangle$ for each q-ary codeword C_x with access to a quantumly corrupted word $\tilde{O}$. Note that it is easy to generate $|C_x\rangle$ from the oracle O_{C_x} that represents C_x *without* any corruption (behaving as the "standard" oracle). Here, we claim that there is a generic quantum algorithm that generates codeword states for any q-ary code C. For convenience, write $\mathbf{F}_q^+ = \mathbf{F}_q - \{0\}$ throughout this paper.

Lemma 4.2 There exists a quantum algorithm $\mathcal{A}$ that, for any quantumly corrupted word $\tilde{O}$, for any message $x \in \Gamma_n$, and for any $k \in \mathbf{F}_q^+$, generates the quantum state $|\psi_k\rangle = \kappa_x^{(k)}|k\rangle|C_x^{(k)}\rangle|\tau\rangle + |\Lambda_x^{(k)}\rangle$ from the initial state $|\psi_k^{(0)}\rangle = |k\rangle|0^{\lceil \log_2 M(n)\rceil}\rangle|0\rangle|0^{l(n)}\rangle$ with only two queries to $\tilde{O}$ and $\tilde{O}^{-1}$, where $|\tau\rangle$ is a fixed basis vector, and $\kappa_x^{(k)}$ is a complex number, and $|\Lambda_x^{(k)}\rangle$ is a vector satisfying $(\langle k|\langle C_x^{(k)}|\langle\tau|)|\Lambda_x^{(k)}\rangle = 0$ with the following condition:

for every $x \in \Gamma_n$, there exists a number $k \in \mathbb{F}_q^+$ with the inequality $|\kappa_x^{(k)}| \geq (q/(q-1))\left|\mathrm{Pre}_{\tilde{O}}(C_x) - 1/q\right|$.

Isolating all individual messages x in Lemma 4.2 simultaneously requires a certain type of "orthogonality," which we call *phase-orthogonality*.

Definition 4.3 A code $C = \{C_x\}_{x\in\Gamma_n}$ is called *k-shuffled phase-orthogonal* if, for any distinct messages $x, y \in \Gamma_n$, $\langle C_x^{(k)}|C_y^{(k)}\rangle = 0$. If $\langle C_x^{(k)}|C_y^{(k)}\rangle = 0$ holds for every number $k \in \mathbb{F}_q^+$, the code C is simply called *phase-orthogonal*.

Note that phase-orthogonality for a binary code, in particular, is naturally induced from the standard *inner product* of two codewords when we translate their binary symbols $\{0, 1\}$ into $\{+1, -1\}$.

It is not difficult to prove that, for any pair (C_x, C_y) of codewords in a given $(M(n), n, d(n))_{q(n)}$-code C, we have $|\langle C_x|C_y\rangle| \geq 1 - 2 \cdot d(C_x, C_y)/M(n)$. In particular, a binary code C satisfies that $\langle C_x|C_y\rangle = 1 - 2 \cdot d(C_x, C_y)/M(n)$.

Assume that $\{C_x\}_{x\in\Gamma_n}$ is a phase-orthogonal code. Such orthogonality makes it possible to prove the following theorem using Lemma 4.2.

Theorem 4.4 Let $\{C_x\}_{x\in\Gamma_n}$ be any phase-orthogonal code. There exists a quantum algorithm $\mathcal{A}$ that, starting with $|\phi^{(0)}\rangle = |0\rangle|0^{\lceil \log_2 M(n)\rceil}\rangle|0\rangle|0^{l(n)}\rangle$ with any quantumly corrupted word $\tilde{O}$, $\mathcal{A}$ makes only two queries to $\tilde{O}$ and $\tilde{O}^{-1}$ and generates the state $|\psi'\rangle = (1/\sqrt{q-1})\sum_{k\in\mathbb{F}_q^+} \sum_{x\in\Gamma_n} \kappa_x^{(k)}|k\rangle|C_x^{(k)}\rangle|\tau\rangle + |\Lambda'\rangle$, such that, for every message $x \in \Gamma_n$, there exists a number $k \in \mathbb{F}_q^+$ satisfying $|\kappa_x^{(k)}| \geq (q/(q-1))\left|\mathrm{Pre}_{\tilde{O}}(C_x) - 1/q\right|$, where $(\langle k|\langle C_x^{(k)}|\langle\tau|)|\Lambda'\rangle = 0$ for any $k \in \mathbb{F}_q^+$.

Now, we give the proof of our key lemma, Lemma 4.2. Notice that Lemma 4.2 is true for any $q(n)$-ary code. The binary case ($q = 2$) was implicit in [1]; however, our argument for the general $q(n)$-ary case is more involved because of the introduction of "k-shuffledness."

Proof Sketch of Lemma 4.2. First, we describe our codeword-state generation algorithm $\mathcal{A}$ in detail. Fix $x \in \Gamma_n$ and $k \in \mathbb{F}_q^+$ and let $m = \lceil \log_2 M(n)\rceil$.

(1) Start with the initial state: $|\psi_k^{(0)}\rangle = |k\rangle|0^m\rangle|0\rangle|0^{l'}\rangle$.
(2) Apply the Fourier transformation $(F_q)^{\otimes m}$ over $\mathbb{F}_q$ to the second register. We then obtain the superposition $|\psi_k^{(1)}\rangle = (1/\sqrt{M})\sum_{r\in I_n}|k\rangle|r\rangle|0\rangle|0^{l'}\rangle$.
(3) Invoke $\tilde{O}$ using the last three registers. The resulting state is $|\psi_k^{(2)}\rangle = (1/\sqrt{M})\sum_{r\in I_n}\sum_{z\in\mathbb{F}_q} \alpha_{r,z}|k\rangle|r\rangle|z\rangle|\phi_{r,z}\rangle$.
(4) Encode the information on the first and the third resisters into "phase" so that we obtain the state $|\psi_k^{(3)}\rangle = (1/\sqrt{M})\sum_{r\in I_n}\sum_{z\in\mathbb{F}_q} \omega_q^{k\cdot z}\alpha_{r,z}|k\rangle|r\rangle|z\rangle|\phi_{r,z}\rangle$.
(5) Apply $\tilde{O}^{-1}$ to the last three registers. Let $|\psi_k^{(4)}\rangle$ be the resulting state $(I \otimes \tilde{O}^{-1})|\psi_k^{(3)}\rangle$.
(6) The state $|\psi_k^{(4)}\rangle$ can be expressed in the form $\kappa_x^{(k)}|k\rangle|C_x^{(k)}\rangle|\tau\rangle + |\Lambda_x^{(k)}\rangle$, where $|\tau\rangle = |0\rangle|0^{l'}\rangle$ and $(\langle k|\langle C_x^{(k)}|\langle\tau|)|\Lambda_x^{(k)}\rangle = 0$. The amplitude $\kappa_x^{(k)}$ equals $\mathrm{Pre}_{\tilde{O}}(C_x) + (1/M)\sum_{r\in I_n} \sum_{z:z\neq C_x(r)} \omega_q^{k(z-C_x(r))}|\alpha_{r,z}|^2$.

The non-trivial part of the lemma is to prove the lower-bound of $|\kappa_x^{(k)}|$. For each $j \in \mathbb{F}_q$, let $\beta_j = (1/M)\sum_{r\in I_n}|\alpha_{r,C_x(r)+j}|^2$. By letting $\chi_x^{(k)} = \sum_{j\in\mathbb{F}_q^+}\omega_q^{k\cdot j}\beta_j$, κ_x can be expressed as $\kappa_x^{(k)} = \mathrm{Pre}_{\tilde{O}}(C_x) + \mathrm{Re}(\chi_x^{(k)}) + \mathrm{Im}(\chi_x^{(k)})$. To estimate $|\kappa_x^{(k)}|$, it thus suffices to prove that, for each $x \in \Gamma_n$, there exists a number $k \in \mathbb{F}_q^+$ such that $\mathrm{Re}(\chi_x^{(k)}) \geq -(1/(q-1))(1 - \mathrm{Pre}_{\tilde{O}}(C_x))$. Since $|\kappa_x^{(k)}|^2 = (\mathrm{Pre}_{\tilde{O}}(C_x) + \mathrm{Re}(\chi_x^{(k)}))^2 + (\mathrm{Im}(\chi_x^{(k)}))^2$, the lemma immediately follows.

To complete the proof, we employ an "adversary" argument. Now, assume that our adversary has cleverly chosen $\tilde{O}$ to make $|\kappa_x^{(k)}|^2$ the smallest for every $k \in \mathbb{F}_q^+$. We argue that the adversary's best choice is to set $\beta_j = \hat{\beta}/(q-1)$ for all $j \in \mathbb{F}_q^+$, where $\hat{\beta} = \sum_{j\in\mathbb{F}_q^+}\beta_j$. This follows directly from the claim below. We omit the proof of the claim due to space limitation. Let $\hat{\chi}_x = \sum_{k\in\mathbb{F}_q^+}\chi_x^{(k)}$.

Claim 1
1. $\hat{\chi}_x = -\hat{\beta}$.
2. For his best strategy, the adversary can be assumed to have chosen $\{\beta_j\}_{j\in\mathbb{F}_q^+}$ so that $\beta_j = \beta_{q-j}$ for any $j \in \mathbb{F}_q^+$ and $\mathrm{Im}(\chi_x^{(k)}) = 0$.

Since $\beta_j = \hat{\beta}/(q-1)$ for all $j \in \mathbb{F}_q^+$ and $\hat{\beta} = 1 - \beta_0$, it easily follows that $\mathrm{Re}(\chi_x^{(k)}) \geq -(1/(q-1))(1 - \mathrm{Pre}_{\tilde{O}}(C_x))$, as required. □

The following theorem shows how to convert a *codeword-state decoder* (i.e., a quantum algorithm that decodes x from $|C_x^{(k)}\rangle$ for any k) into a quantum list-decoder. This complements Theorem 4.4.

Theorem 4.5 Let $C = \{C_x\}_{x\in\Gamma_n}$ be any phase-orthogonal $(M(n), n, d(n))_{q(n)}$-code. Let $k \in \mathbb{F}_q^+$ and $M'(n) \geq 0$. Let U_n be any quantum algorithm that, for each fixed $x \in \Gamma_n$, decodes x from a k-shuffled codeword state $|C_x^{(k)}\rangle \in \mathcal{H}_{M(n)}$ with probability $\geq 1 - \xi(n)$. Let V_n be any quantum algorithm that generates a quantum state $|\tilde{C}\rangle$ consisting of a $\lceil \log_2 M(n)\rceil$-qubit approximation of the codeword state together with ancilla $\lceil \log_2 M'(n)\rceil$ qubits generated from a quantumly corrupted word $\tilde{O}$ with success probability $\eta(n)$. Assume that $|(\langle C_x^{(k)}|\langle 0^{\lceil \log_2 M'(n)\rceil}|)|\tilde{C}\rangle| \geq \zeta(n)$ for every $x \in \Gamma_n$ satisfying $\mathrm{Pre}_{\tilde{O}}(C_x) \geq 1/q(n) + \varepsilon(n)$. If $\xi(n) < \zeta^2(n)/2$, then there exists a quantum list-decoding algorithm W_n for C of list size at most

$$\lceil (\eta(n)(\zeta^2(n)/2 - \xi(n)))^{-1}(\log_2 J(n) + \log_2(1/\delta))\rceil,$$

where $J(n)$ is from Lemma 3.2. Moreover, if U_n and V_n are polynomial-time computable and $(\zeta^2(n)/2) - \xi(n)$ and $\eta(n)$ are polynomially-bounded functions, then W_n is a polynomial-time quantum list-decoding algorithm for C.

Proof Sketch. Given (n, ε, δ) and $\tilde{O}$ as input, the following algorithm solves the QLDP for each fixed $n \in \mathbb{N}$. Let $m = \lceil \log_2 M(n) \rceil$ and $m' = \lceil \log_2 M'(n) \rceil$.

(1) Run algorithm V_n to obtain the state $|\tilde{C}\rangle$ with probability at least η.
(2) Apply algorithm U_n to the first m qubits of $|\tilde{C}\rangle$ as well as an appropriate number of ancilla qubits, say c. We then obtain the state $U_n|\tilde{C}\rangle|0^c\rangle$.
(3) Measure the obtained state and add its measured result to the list of message candidates.
(4) Repeat Steps (1)–(3) $\lceil (\log_2 J(n) + \log_2(1/\delta))/e \rceil$ times and output the list, where $e = \eta(1-\xi-\sqrt{1-\zeta^2}) \geq \eta(n)(\zeta^2(n)/2 - \xi(n))$.

We next claim the following, whose proof is omitted due to space limitation. Let $B_\varepsilon^{(k)} = \{x \in \Gamma_n \mid \mathrm{Pre}_{\tilde{O}}(C_x^{(k)}) \geq 1/q + \varepsilon\}$.

Claim 2 1. The probability that x is observed when measuring the quantum state obtained after Step (2) on the computational basis is at least e.

2. If we perform Steps (1)–(3) $\lceil e^{-1}(\log_2 |B_\varepsilon^{(k)}| + \log_2 (1/\delta)) \rceil$ times, then we obtain a list that includes all messages in $B_\varepsilon^{(k)}$ with probability at least $1-\delta$.

Since $|B_\varepsilon^{(k)}| \leq J(n)$, we obtain the desired list of message candidates at Step (4) with probability at least $1 - \delta$ by the above claim. □

At the end of this section, we show a general theorem, in which "almost phase-orthogonal" codes are quantumly list-decodable. Our argument uses the notion of pretty-good measurement (known also as square-root measurement or least-squared measurement) [10, 16].

Theorem 4.6 let $k \in \mathbb{F}_q$ and let C be any $(M(n), n, d(n))_q$ code such that there exists a constant $\xi \in [0, 1/2]$ satisfying $|\langle C_x^{(k)} | C_y^{(k)} \rangle| \leq \xi$ for any distinct pair $x, y \in \Gamma_n$. Let S be the matrix of the form $(|C_0^{(k)}\rangle, |C_1^{(k)}\rangle, \ldots, |C_{N-1}^{(k)}\rangle)$. If $\xi < 2\varepsilon^2$ and $\mathrm{rank}(S) = N$, then there exists a quantum list-decoding algorithm for C.

Proof Sketch. From Lemma 4.2 and Theorem 4.5, it suffices to construct a unitary operator U whose success probability $|\langle z|U|C_z\rangle|^2$ of decoding z from $|C_z\rangle$ is at least $1 - \xi$ whenever $|\langle C_x | C_y \rangle| \leq \xi$ for any distinct $x, y \in \Gamma$ and $\mathrm{rank}(S) = N$.

We want to design U following an argument of pretty good measurement [10, 16]. Note that, since $\mathrm{rank}(S) = N$, the matrices $S^\dagger S$ and $SS^\dagger$ share the same eigenvalues, say $\lambda_0, \ldots, \lambda_{N-1}$. Perform singular-value decomposition and we obtain $S = PTQ$ for M- and N-dimensional unitary operators P and Q, respectively, and a diagonal matrix $T = \mathrm{diag}(\sqrt{\lambda_0}, \sqrt{\lambda_1}, \ldots, \sqrt{\lambda_{N-1}}, 0, \ldots, 0)$. We therefore have $\langle z|_M US|z\rangle_N = \langle z|_M UPTQ|z\rangle_N$, where $|z\rangle_M$ and $|z\rangle_N$ are respectively an M-dimensional and an N-dimensional vectors.

The desired matrix U is defined as $U = RP^\dagger$, where $R = \begin{pmatrix} Q^\dagger & 0 \\ 0 & I \end{pmatrix}$. It immediately follows that $\langle z|_M US|z\rangle_N = \langle z|_M RTQ|z\rangle_N = \langle z|_N Q^\dagger T' Q|z\rangle_N$ with the diagonal matrix $T' = \mathrm{diag}(\sqrt{\lambda_0}, \sqrt{\lambda_1}, \ldots, \sqrt{\lambda_{N-1}})$. The success probability of decoding z from $|C_z^{(k)}\rangle$ is therefore lower-bounded by $|\langle z|Q^\dagger T' Q|z\rangle|^2 \geq |\lambda_{\min}|$, where $\lambda_{\min}$ denotes $\min\{|\lambda_1|, |\lambda_2|, \ldots, |\lambda_{N-1}|\}$.

The remaining task is to prove the following claim.

Claim 3 $|\lambda_{\min}| \geq 1 - \xi$.

We omit the proof of this claim due to space limitation. This completes the proof. □

5 New Quantum Hardcore Functions

Finally, as our main result, we present three new quantum hardcore functions, two of which are unknown to be classically hardcores. We explain them as codes and give polynomial-time list-decoding algorithms for them. From Lemma 4.2 and Theorem 4.5, we only need to build their codeword-state decoders.

Proposition 5.1 There exist polynomial-time quantum list-decoding algorithms for the following codes: letting $p(n), q(n)$ be any functions from $\mathbb{N}$ to the primes,

1. The *$q(n)$-ary Hadamard code* $\mathrm{HAD}^{(q)}$ with $q(n) \in n^{O(1)}$, whose codeword is defined as $\mathrm{HAD}_x^{(q)}(r) = \sum_{i=0}^{2^n-1} x_i \cdot r_i \bmod q(n)$.

2. The *shifted Legendre symbol code* SLS^p, which is a $(p(n), n)_2$-code with $n = \lceil \log p(n) \rceil$, whose codeword is defined by the Legendre symbol[3] as $\mathrm{SLS}_x^p(r) = 1$ if $(\frac{x+r}{p(n)}) = -1$, and $\mathrm{SLS}_x^p(r) = 0$ otherwise.

3. The *pairwise equality code* PEQ for even $n \in \mathbb{N}$, which is a $(2^n, n)_2$-code, whose codeword is $\mathrm{PEQ}_x(r) = \oplus_{i=0}^{n/2} \mathrm{EQ}(x_i x_{i+1}, r_i r_{i+1})$, where EQ denotes the equality predicate.

Combining Proposition 5.1 and Theorem 3.4, we obtain the quantum hardcore property of all the aforementioned codes.

Theorem 5.2 The functions $\mathrm{HAD}^{(q)}$, SLS^p, and PEQ are all quantum hardcore functions for any quantum

[3] For any odd prime p. let $(\frac{x}{p}) = 0$ if $p|x$, $(\frac{x}{p}) = 1$ if $p \nmid x$ and x is a quadratic residue modulo p. and $(\frac{x}{p}) = -1$ otherwise.

one-way function of the form $f'(x,r) = (f(x),r)$ with $|r| = poly(|x|)$, where f is an arbitrary quantum one-way function.

Remark: Damgård [8] introduced the so-called *Legendre generator*, which produces a bit sequence whose rth bit equals $\mathrm{SLS}^p(r)$. He asked if his generator possesses the classical hardcore property. (This is also listed as an open problem in [13].) Our result proves the "quantum" hardcore property of Damgård's generator for any quantum one-way function.

Proof Sketch of Proposition 5.1. It suffices to provide a codeword-state decoder for each given codeword.

(1) To decode x from the codeword state $|\mathrm{HAD}^{(q)}\rangle$, we simply apply the Fourier transformation $F_{q(n)}$ over $\mathbb{F}_{q(n)}$ and then extract x deterministically.

(2) Our codeword-state decoder is obtained by an appropriate modification of a quantum algorithm of van Dam, Hallgren, and Ip [20].

(3) Consider the *circulant Hadamard transformation* H_C:

$$H_C =_{def} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} = F_4^{-1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} F_4,$$

where F_4 is the quantum Fourier transformation over $\mathbb{F}_4$. We can obtain x from the codeword state $|\mathrm{PEQ}_x\rangle$ by applying $U = H_C^{\otimes n/2}$. □

References

[1] M. Adcock and R. Cleve. A quantum Goldreich-Levin theorem with cryptographic applications. In *Proc. STACS 2002*, LNCS 2285, pages 323–334. Springer, 2002.

[2] A. Akavia, S. Goldwasser, and S. Safra. Proving hard-core predicates using list decoding. In *Proc. FOCS 2003*, pages 146–157, 2003.

[3] A. Ambainis, K. Iwama, A. Kawachi, R. H. Putra, and S. Yamashita. Robust quantum algorithms for oracle identification. Available at http://arxiv.org/abs/quant-ph/0411204, 2004.

[4] A. Atici and R. Servedio. Improved bounds on quantum learning algorithms. To appear in *Quantum Information Processing*. Available also at http://arxiv.org/abs/quant-ph/0411140.

[5] A. Barg and S. Zhou. A quantum decoding algorithm for the simplex code. In *Proc. Allerton Conference on Communication, Control and Computing*, 1998. Available at http://citeseer.ist.psu.edu/barg98quantum.html.

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

[7] H. Buhrman, I. Newman, H. Röhrig, and R. de Wolf. Robust quantum algorithms and polynomials. In *Proc. STACS 2003*, LNCS 3404, pages 593–604, 2003.

[8] I. B. Damgård. On the randomness of Legendre and Jacobi sequences. In *Proc. CRYPTO '88*, LNCS 403, pages 163–172, 1988.

[9] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. In *Proc. Roy. Soc. London*, A, volume 439, pages 553–558, 1992.

[10] Y. C. Eldar and G. D. Forney, Jr. On quantum detection and the square-root measurement. *IEEE Trans. Inform. Theory*, 47(3):858–872, 2001.

[11] O. Goldreich. *Foundations of Cryptography: Basic Tools*, 2001.

[12] O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In *Proc. STOC '89*, pages 25–32, 1989.

[13] M. I. González Vasco and M. Näslund. A survey of hard core functions. In *Proc. Workshop on Cryptography and Computational Number Theory*, pages 227–256. Birkhauser, 2001.

[14] L. K. Grover. Quantum Mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. 79(2), pages 325–328, 1997.

[15] V. Guruswami and M. Sudan. Extensions to the Johnson bound. Manuscript, 2000. Available at http://theory.csail.mit.edu/ madhu/.

[16] P. Hausladen and W. K. Wootters. A 'pretty good' measurement for distinguishing quantum states. *J. Mod. Opt.*, 41:2385–2390, 1994.

[17] T. Holenstein, U. M. Maurer, and J. Sjödin. Complete classification of bilinear hard-core functions. In *Proc. CRYPTO 2004*, LNCS 3152, pages 73–91, 2004.

[18] P. Høyer, M. Mosca, and R. de Wolf. Quantum search on bounded-error inputs. In *Proc. ICALP 2003*, LNCS 2719, pages 291–299, 2003.

[19] M. Sudan. List decoding: Algorithms and applications. *SIGACT News*, 31(1):16–27, 2000.

[20] W. van Dam, S. Hallgren, and L. Ip. Quantum algorithms for some hidden shift problems. In *Proc. SODA 2003*, pages 489–498, 2003.