Quantum List Decoding from Quantumly Corrupted Codewords for Classical Block Codes of Polynomially Small Rate
(Extended Abstract)

Tomoyuki Yamakami

Department of Computer Software, University of Aizu
90 Kami-Iawase, Tsuruga, Ikki-machi, Fukushima 965-8580, Japan

Abstract

Our task of quantum list decoding for a classical block code is to recover from a given quantumly corrupted codeword a short list containing all messages whose codewords have high "presence" in this quantumly corrupted codeword. All known families of efficiently quantum list decodable codes, nonetheless, have exponentially-small message rate. We show that certain generalized Reed-Solomon codes concatenated with Hadamard codes of polynomially-small rate and constant codeword alphabet size have efficient quantum list decoding algorithms, provided that target codewords should have relatively high presence in a given quantumly corrupted codeword.

Keywords: error-correcting code, quantum list decoding, quantum computation, quantumly corrupted codeword

1 Introduction

Classical list decoding, which was rooted in the late 1950s by Elias [3] and Wozencraft [18], has drawn significant attention since Sudan's [15] discovery of an efficient list decoding algorithm for Reed-Solomon codes beyond its "traditional" error-correction radius. List decoding has since then found useful applications to cryptography as well as complexity theory (see, e.g., a survey article [16]).

Quantum list decoding dealing with classical block codes first arose in connection to quantum hardcore functions in a seminal paper by Kawachi and Yamakami [12] (following an early result of Adcock and Cleve [1] on biased oracles) in the so-called *implicit-input explicit-output model*, in which we wish to output a list of messages with oracle access to a quantum encoding procedure which produces a quantum superposition of corrupted codewords. This model differs from the conventional error-correction model between a sender and a receiver through a noisy channel. In contrast, we are given a (possibly) faulty quantum algorithm (known as a *quantum-computationally corrupted codeword* or *quantumly corrupted codeword*) which encodes a classical message to a certain quantum state representing a quantum corruption of the correct codeword. It is in general hard to recover the original message from such a quantumly corrupted codeword; however, we may be able to produce a reasonably small list that contains all messages whose codewords are close proximity to the given quantumly corrupted codeword. This closeness is scaled by the notion of *presence*, which expresses the average probability of obtaining each block of the target codeword from the quantumly corrupted codeword. (See [12] for an intuition behind this notion.) This is the primary purpose of quantum list decoding. A natural question is: what types of classical block codes are efficiently quantum list decodable?

There are known families of block codes that are efficiently quantum list decodable with arbitrary presence. The first known example is Hadamard codes. In classical list decoding, Goldreich and Levin [5] showed the classical list decodability of the binary Hadamard codes and subsequently Goldreich, Rubinfeld, and Sudan [6] gave a general list decoding algorithm for the q-ary Hadamard codes. Concerning quantum list decoding, Adcock and Cleve [1] essentially proved that the binary Hadamard codes are quantum list decodable in polynomial time. For the q-ary Hadamard codes, a fast quantum list decoding algorithm was recently given by Kawachi and Yamakami [12]. They also presented two additional quantum list decodable codes: *shifted Legendre symbol codes* and *pairwise equality codes*. All these codes, nonetheless, have *exponentially-small rate*, where the (message) rate of a code is a ratio of message length and codeword's block length.

This paper is motivated by the question of whether there exists a family of efficiently quantum list decodable codes of polynomially-small rate and constant codeword alphabet size, because such a code family finds useful applications to quantum complexity theory (an example will be seen in Section 5). Natural candidates are well-studied Reed-Solomon codes. They have relatively large rate; however, they usually have large alphabet size. A standard way to build a code of large rate but small alphabet size is to concatenate two codes of good properties. We claim that concatenating generalized Reed-Solomon codes with Hadamard codes gives the desired codes, assuming that the generalized Reed-Solomon codes are efficiently quantum list decodable. This claim is proven by employing in Section 3 a technique of constructing a "quantum reduction" between two quantumly corrupted codewords. Note that this technique requires no *soft information*, which is a key ingredient in the classical case of [7, 8].

Are the generalized Reed-Solomon codes *efficiently* quantum list decodable? A direct and simple approach toward their quantum list decoding is an application of the polynomial reconstruction algorithm of Guruswami and Sudan [7]. When codeword presence in a quantumly corrupted codeword is relatively high, we can show in Section 4 how to construct a quantum list decoding algorithm for the generalized Reed-Solomon codes. As the presence becomes lower, however, it seems harder to solve efficiently the quantum list decoding problem for the generalized

Reed-Solomon codes, because its efficient list decoding leads to the unexpected consequence that every NP-problem can be efficiently solved on a quantum computer with high success probability. There is also a direct connection between quantum list decodability of the generalized Reed-Solomon codes and quantum solvability of two classical problems: the *noisy polynomial interpolation problem* (NPIP) [13] and the *bounded distance vector problem* (BDVP).

To a certain type of application, our quantum list decoding algorithm for the aforementioned concatenated code is still applicable. Our example is the *QCMA search problem*, in which we want to find a classical witness of polynomial size that forces a given polynomial-time quantum algorithm to accept with high probability. We show in Section 5 that solving this search problem on average implies solving it in worst case.

Finally, we make a brief discussion on the notion of *local quantum list decoding* based on an implicit-input implicit-output model where an outcome of a list decoder is a list of *descriptions* of quantum circuit list-decoders. Similar to the classical case of [17], we can apply our quantum list decoder for the generalized Reed-Solomon codes to do local quantum list decoding for Reed-Müller codes from quantumly corrupted codewords. As an immediate consequence, we can prove the so-called *hardness amplification* of quantum circuits, following the argument of [17].

2 Foundations of Quantum List Decoding

This section explains basic notions and notation concerning quantum list decoding. Throughout this paper, let $\mathbb{N}$ denote the set of all nonnegative integers and set $\mathbb{N}^+ = \mathbb{N} - \{0\}$. For any positive integers m, n with $m \leq n$, let $[m,n]_{\mathbb{Z}}$ denote the set $\{m, m+1, m+2, \ldots, n\}$ and let $[n]$ be short for $[1,n]_{\mathbb{Z}}$ if $n \geq 1$.

2.1 Classical Block Codes

We briefly explain classical block (error-correcting) codes, which are objects of our interest. Roughly speaking, a *code* is a set of strings of the same length over a finite alphabet Σ and each string of a code is indexed by a message and is called a *codeword*. In this paper, we are mostly focused on a *family of codes*, each of which corresponds to a different message length n in $\mathbb{N}$. Such a code family is in general specified by a series $(\Sigma_n, I_n, \Gamma_n)$ of *message space* Σ_n, *index set* I_n, and *code alphabet* Γ_n for each *message length* n (which serves as a "basis parameter" in this paper).

As standard in complexity theory, a code C is viewed as a function that, for each message length n, maps $\Sigma_n \times I_n$ to Γ_n. Let $N(n) = |\Sigma_n|$ and $q(n) = |\Gamma_n|$. It is convenient to assume that $\Sigma_n = (\Sigma'_n)^n$ so that n actually represents the *length* of messages in Σ_n over the message alphabet Σ'_n; in this case, $n = \lceil \log_{|\Sigma'_n|} N(n) \rceil$ for each $n \in \mathbb{N}$. By abbreviating $C(x,y)$ as $C_x(y)$, we treat $C_x(\cdot)$ as a function mapping I_n to Γ_n and is called a *codeword*, where the *block length* $M(n)$ of such a codeword is $|I_n|$. For simplicity, we often assume that $I_n = \{0, 1, \ldots, M(n)-1\}$ so that each element of I_n 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* $(\Gamma_n)^{M(n)}$ of dimension $M(n)$. We mainly work on a finite field and we often regard Γ_n as the finite field $\mathbb{F}_{q(n)}$ $(= \mathrm{GF}(q(n)))$ of order $q(n)$.

The *(message) rate* of C is defined to be the ratio $n/M(n)$. 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. In contrast, $\Delta(C_x, C_y)$ denotes the *relative (Hamming) distance* $d(C_x, C_y)/M(n)$. The above-described code is simply called a $(M(n), n)_{q(n)}$-code* (or $(M(n), n, d(n))$-code if the minimal distance $d(n)$ of the code of message length n is emphasized). We may drop a length parameter n from both subscript and argument place whenever we discuss a set of codewords with a "fixed" n.

Hadamard Codes HAD. Let n be any message length, used as a parameter, and let q be any prime number. A q-ary Hadamard code family $\mathrm{HAD}^{(q)} = \{\mathrm{HAD}^{(q,n)}\}_{n \in \mathbb{N}}$ consists of $(q^n, n, q^n - q^{n-1})_q$-codes obtained as follows. For each message $x = (x_1, x_2, \ldots, x_n)$ in $(\mathbb{F}_q)^n$, let $\mathrm{HAD}^{(q,n)}_x(r) = \sum_{i=1}^n x_i r_i \bmod q$, where $r = (r_1, r_2, \ldots, r_n) \in (\mathbb{F}_q)^n$.

(Normalized) Generalized Reed-Solomon Codes GRS. Let q be any prime and let k, n be any positive integers with $n \leq k \leq q$. A (normalized) generalized Reed-Solomon code family $\mathrm{GRS} = \{\mathrm{GRS}^{(k,n,q)}\}_{n,k \in \mathbb{N}}$ consists of all $(k, n, k-n+1)_q$-codes obtained as follows. Let $x = (x_1, x_2, \ldots, x_n) \in (\mathbb{F}_q)^n$ be any message and let D_k be a set of k distinct elements (called *code locators*) in $\mathbb{F}_q$. Let $\mathrm{GRS}^{(k,n,q)}_x(r) = \sum_{i=1}^n x_i r^{i-1} \bmod q$ be the polynomial of degree at most $n-1$ for each $r \in D_k$.

2.2 Quantumly Corrupted Codewords and Codeword Presence

We are mostly concerned with a quantum corruption that occurs during a quantum procedure of encoding messages into codewords. The process of such a quantum corruption can be described as a certain type of unitary map. Formally, a *quantum-computationally corrupted codeword* (or *quantumly corrupted codeword*) is a unitary operator $\tilde{O}$, with two fixed function parameters $l(n)$ and $m(n)$ mapping $\mathbb{N}$ to $\mathbb{N}$, that satisfies the following condition: for any three strings $r \in \Sigma^n$, $s \in \Sigma^{l(n)}$, and $t \in \Sigma^{m(n)}$, there exists a unit vector $|\phi_{r,z}\rangle$ of length $m(n)$ such that

$$\tilde{O}|r\rangle|s\rangle|t\rangle = \sum_z \alpha_{r,z}|r\rangle|s \oplus z\rangle|t \oplus \phi_{r,z}\rangle,$$

where the notation $|t \oplus \phi_{r,z}\rangle$ is shorthand for $\sum_{w \in \Sigma^{m(n)}} \langle w|\phi_{r,z}\rangle |t \oplus w\rangle$ and $\oplus$ is the bitwise XOR. The *presence* of codeword C_x in $\tilde{O}$, denoted $\mathrm{Pre}_{\tilde{O}}(C_x)$, is the average probability of obtaining the correct values $C_x(r)$ over all indices $r \in I_n$; namely, $\mathrm{Pre}_{\tilde{O}}(C_x) = \frac{1}{M} \sum_r |\alpha_{r,C_x(r)}|^2$. See [12] for an intuition behind these notions.

We further expand the notions of presence and distance. Let n be any message length. Define W_n to be the set of all vectors $w = (w_{r,z})_{r,z} \in [0,1]^{q(n)M(n)}$ (which is viewed as a "measured" quantumly corrupted codeword) such that $\sum_{z \in [0,q(n)-1]_{\mathbb{Z}}} w_{r,z} = 1$ for each index $r \in [0, M(n)-1]_{\mathbb{Z}}$. Notice that $\sum_r \sum_z w_{r,z} = M(n)$ for any $w \in W_n$. Next, consider the set V_n of all codewords $a = (a_r)_r \in ([0, q(n)-1]_{\mathbb{Z}})^{M(n)}$. We embed this codeword a into W_n in the following way. Define $v(a) = (\delta^{(a)}_{r,z})_{r,z} \in$

*In some literature, the notation $(M(n), \Gamma_n)_{q(n)}$ is used instead.

$\{0,1\}^{q(n)M(n)}$, where $\delta_{r,z}^{(a)} = 1$ if $a(r) = z$ and 0 otherwise. Moreover, for any code (i.e., a subset of V_n) $C^{(n)}$, let $v(C^{(n)}) = \{v(a) \mid a \in C^{(n)}\}$. Finally, we obtain $v(V_n) \subseteq W_n$.

First, we expand the notion of presence. For any $a \in V_n$ and any vector $w \in W_n$, define $\mathrm{Pre}_w(a) = \frac{1}{M(n)}\langle v(a)|w\rangle$, where $\langle\cdot|\cdot\rangle$ denotes the standard inner product. Second, we expand the notion of the (Hamming) distance. For any pair $v, w \in W_n$, define $d(v,w) = M(n) - \langle v|w\rangle$. This new definition clearly expands the standard notion of the distance $d(\cdot,\cdot)$ because, for any $a, b \in V_n$, we have

$$d(v(a), v(b)) = M(n) - \langle v(a)|v(b)\rangle) = d(a,b).$$

Notice that, for any $a \in V_n$ and any vector $w \in W_n$,

$$\mathrm{Pre}_w(a) = \frac{\langle v(a)|w\rangle}{M(n)} = 1 - \frac{d(v(a),w)}{M(n)}.$$

2.3 Presence Versus Minimal Distance

A relatively good upper bound on the value of presence is shown in [12] by following a geometric method of Guruswami and Sudan [9], who gave a q-ary extension of Johnson bound. Let C be any $(M(n), n, d(n))_{q(n)}$-code family with message space Σ_n and define $P_{q(n)}(M(n), d(n), \varepsilon(n))$ as $\sup_{\tilde{O}} \{|\{x \in \Sigma_n \mid \mathrm{Pre}_{\tilde{O}}(C_x) \geq \varepsilon(n)\}|\}$, where "sup" is taken over all quantumly corrupted word $\tilde{O}$ for C.

Lemma 2.1 [12] *Let n be any message length. Let $(\varepsilon(n), q(n), d(n), M(n))$ satisfy the inequality $\varepsilon(n) > \ell(n)$, where $\ell(n)$ equals $1/q(n) + (1-1/q(n))\sqrt{1-(d(n)/M(n))\,(q(n)/(q(n)-1))}$. Assume that C is an $(M(n), n, d(n))_{q(n)}$-code family. The value $P_{q(n)}(M(n), d(n), \varepsilon(n))$ is upper-bounded by $\min\left\{M(n)(q(n)-1), \frac{d(n)(1-1/q(n))}{d(n)(1-1/q(n))+M(n)\varrho(n)}\right\}$, where $\varrho(n) = (\varepsilon(n) - 1/q(n))^2 - (1-1/q(n))^2$. In case where $\varepsilon(n) = \ell(n)$, it holds that $P_{q(n)}(M(n), d(n), \varepsilon(n)) \leq 2M(n)(q(n)-1) - 1$.*

To derive an asymptotic bound from this lemma, we introduce $QL^{poly}(\lambda)$, which indicates the minimal possible presence for a family of quantum list decodable codes of minimal relative distance λ having only a polynomial-size message list. Let $C = \{C^{(n)}\}_{n\in\mathbb{N}}$ be any $(M(n), n, d(n))_{q(n)}$-code family. For each pair $w \in W_n$ and $\varepsilon \in [0,1]$, set $E(w,\varepsilon) = \{a \in V_n \mid \mathrm{Pre}_w(a) \geq \varepsilon\}$. For any $n \in \mathbb{N}$, let $presence(C,l)(n)$ denote $\min\{\varepsilon \in \mathbb{R}^{\geq 0} \mid \forall w \in W_n[|E(w,\varepsilon) \cap C^{(n)}| \leq l]\}$ and define $Pre(C,l) = \limsup_n\{\frac{presence(C,l)(n)}{M(n)}\}$. Moreover, for any function set $\mathcal{F}$, we define $Pre(C,\mathcal{F}) = \inf_{l\in\mathcal{F}}\{Pre(C,l)\}$. For any function l and any value λ, let $QL_l(\lambda) = \inf_{C:\Delta(C)\geq\lambda}\{Pre(C,l)\}$, where $\Delta(C) = \liminf_n\{\Delta(C^{(n)})\}$. For each constant $c \in \mathbb{N}$, let $QL_c^{poly}(\lambda) = \sup_a QL_{l_a}(\lambda)$, where $l_a(n) = an^c$. Finally, $QL^{poly}(\lambda)$ is set to be $\limsup_{c\to\infty} QL_c^{poly}(\lambda)$.

From Lemma 2.1 follows the next proposition.

Proposition 2.2 *Let $\lambda \in [0,1]$ be any minimal relative distance. It holds that $QL_c^{poly}(\lambda) \geq 1/q + (1-1/q)\,(1 - \lambda/(1-1/q) + \lambda/an^c(1-1/q))^{1/2}$ and thus, $QL^{poly}(\lambda) \geq 1/q + (1-1/q)\,(1-\lambda(1-1/q))^{1/2}$.*

Proof. Consider the case where the upper bound given in Lemma 2.1 is at most an^c. For readability, we omit the parameter "n" in the following calculation. We then obtain the inequality

$$\frac{d\,(1-1/q)}{d\,(1-1/q) + M\varrho} \leq an^c,$$

which is equivalent to

$$M\left(\varepsilon - \frac{1}{q}\right)^2 \geq \frac{d\,(1-1/q)}{an^c} - d\left(1-\frac{1}{q}\right) + M\left(1-\frac{1}{q}\right)^2.$$

The term $|\varepsilon - 1/q|$ is thus lower-bounded by

$$\left(\frac{d\,(1-1/q)}{Man^c} - \frac{d\,(1-1/q)}{M} + \left(1-\frac{1}{q}\right)^2\right)^{1/2}.$$

Assuming that $\varepsilon \geq 1/q$, the proposition follows immediately from the relation $\lambda = d/M$. □

It is still open whether the equality $QL^{poly}(\lambda) = 1/q + (1-1/q)\,(1-\lambda(1-1/q))^{1/2}$ holds.

2.4 Implicit-Input Explicit-Output Model

List decoding has been modeled in several different ways in the past literature. This paper chiefly uses the model that takes quantumly corrupted codewords implicitly as an oracle and outputs hidden messages explicitly. Upon this *implicit-input explicit-output model*, the *quantum list decoding problem* (QLDP) for a code C is described in the following fashion. First, let C be any $(M(n), n, d(n))_{q(n)}$-code family with message space Σ_n and let $\mathcal{O}$ be any set of quantumly corrupted codewords for C. Take a *bias parameter* $\varepsilon(n)$.

ε-Quantum List Decoding Problem (ε-QLDP) for Code C w.r.t. $\mathcal{O}$

- Input: a message length n and a value $1/\varepsilon(n)$.
- Implicit Input: an oracle $\tilde{O} \in \mathcal{O}$ representing a quantumly corrupted codeword for C.
- Output: a list of messages including all messages $x \in \Sigma_n$ that satisfy the inequality $\mathrm{Pre}_{\tilde{O}}(C_x) \geq 1/q(n) + \varepsilon(n)$. For convenience, we refer to such a list as a *valid list* for the ε-QLDP.

Our goal is to solve this ε-QLDP using quantum computation with oracle access to a quantumly corrupted codeword in $\mathcal{O}$ with success probability at least $\delta(n)$, which is given as a *confidence parameter*. Now, let us introduce the notion of quantum list decoding algorithm that works with bias ε and confidence δ.

Definition 2.3 (quantum list decoding) Let C be any code family, let $\varepsilon(n)$ be any bias parameter, and let $\delta(n)$ be any confidence parameter. A *quantum list decoding algorithm* (or a quantum list decoder) for C with bias ε and confidence δ is a quantum algorithm $\mathcal{A}$ that solves the ε-QLDP for C with success probability at least $\delta(n)$. If $\mathcal{A}$ also runs in time polynomial in $(n, 1/\varepsilon(n), 1/\delta(n))$, it is called a *polynomial-time quantum list decoding algorithm* for C.

The *list size* of a quantum list decoding algorithm refers to the maximal size of a valid list produced by the algorithm.

Remark: In certain applications, list size plays a crucial role. For instance, if a quantum list decoder produces a valid list L with probability at least $\delta(n)$, it is possible to specify a hidden message x *uniquely* with

the same success probability with help of "advice" of $\log_{|\Sigma|}|L|$ size over message alphabet Σ.

In the rest of this subsection, we discuss a simple connection between one-way functions and the QLDPs. To begin with, we introduce the notion of a one-way function of the strong form, which we preferably call *super one-way*.

Definition 2.4 (quantum super one-wayness) A function f is called *quantum super one-way* if (i) there exists a polynomial-time quantum algorithm $\mathcal{A}$ such that $\mathcal{A}|x\rangle|0\rangle = |x\rangle|f(x)\rangle|\phi_x\rangle$ for a certain quantum state $|\phi_x\rangle$ and (ii) for any positive polynomial p and any polynomial-time quantum algorithm $\mathcal{B}$, the probability that $\mathcal{B}|f(x)\rangle|\phi_x\rangle$ outputs x is at most $1/p(n)$.

Remark: The "standard" one-wayness requires that $\mathcal{B}|f(x)\rangle$ outputs x with negligible probability whereby the information $|\phi_x\rangle$ is *hidden* from the adversary $\mathcal{B}$ who tries to invert f. Our new notion indicates that $\mathcal{B}$ hardly outputs x even though $|\phi_x\rangle$ is given besides $f(x)$ as supplemental information.

A typical example of a quantum super one-way function is a *quantum one-way permutation* because, for a permutation, we can replace $|\phi_x\rangle$ in Definition 2.4 with $|0^m\rangle$ by uncomputing a deterministic procedure that computes $f(x)$ from x.

Lemma 2.5 *No polynomial-time quantum list decodable code with polynomially-small confidence is quantum super one-way.*

Proof. Let f be a quantum super one-way function with its *length function* $m(n) \in n^{O(1)}$ (i.e., $|f(x)| = m(|x|)$). Consider an $(m(n), n, d(n))_{q(n)}$-code C and let $C_x(r)$ denote the rth bit $(f(x))_r$ of $f(x)$.

Take a polynomial-time quantum algorithm $\mathcal{A}$ computing C and assume that $\mathcal{A}|x\rangle|r\rangle|0^{m(n)}\rangle|0^m\rangle = |x\rangle|r\rangle|C_x(r)\rangle|\phi_x\rangle$ for a certain quantum state $|\phi_x\rangle$. Fix x arbitrarily and define $\tilde{O}|r\rangle|s\rangle|t\rangle = |r\rangle|s \oplus C_x(r)\rangle|t \oplus \phi_x\rangle$ for each pair (s,t) of strings. Toward a contradiction, assume that C has a polynomial-time quantum list decoder $\mathcal{B}$ with polynomially-small confidence. Without loss of generality, we can assume that $\mathrm{Prob}_{\mathcal{B}}[\mathcal{B}^{\tilde{O}}(0^n) = x] \geq 1/p(n)$ for a certain fixed positive polynomial p. Convert this $\mathcal{B}$ to an algorithm that inverts f as follows. On input $|f(x)\rangle|\phi_x\rangle$, where $y \in \mathrm{range}(f)$, run $\mathcal{B}$. Whenever $\mathcal{B}$ makes an oracle call with a query $|r\rangle|s\rangle|t\rangle$, generate its answer $|r\rangle|s \oplus (f(x))_r\rangle|t \oplus \phi_x\rangle$ from the input information. Finally, output an outcome of $\mathcal{B}$. This implies that f is not quantum super one-way, a contradiction. □

3 Codes of Polynomially-Small Rate

A family of polynomial-time classical list decodable codes of polynomially-small rate and binary codeword alphabet finds numerous applications in the fields of cryptography and complexity theory (see, e.g., [16]). Since all known efficiently quantum list decodable code families have exponentially-small rate, it is natural to ask whether there is any quantum list decodable code of polynomially-small rate and small alphabet size for any given bias parameter.

3.1 Concatenated Codes

A standard way of building a family of classical block codes of polynomially-small rate and small codeword alphabet size is to concatenate two codes of good properties: for instance, a generalized Reed-Solomon code and a Hadamard code. We can build a similar code under the assumption that the generalized Reed-Solomon codes are efficiently quantum list decodable for a certain bias value.

We first explain Forney's [4] notion of *concatenated codes*. Let us consider two codes $C^{(1)}$ and $C^{(2)}$ such that $C^{(1)}$ is an $(M_1, n_1, d_1)_{q^{n_2}}$-code and $C^{(2)}$ is an $(M_2, n_2, d_2)_q$-code. Let $x = (x_1, x_2, \ldots, x_{n_1})$ be any message of length n_1, where each x_i is taken from Σ^{n_2} over a q-letter alphabet Σ. Since x_i can be expressed as a n_2-letter string, x can be viewed as a string of total length $n_1 n_2$ over a q-letter alphabet. The code $C = C_2 \odot C_1$, given by the inner code $C^{(2)}$ concatenated with the outer code $C^{(1)}$, is defined as $C(x, r, s) = C^{(2)}(C^{(1)}(x, r), s)$. This concatenated code C is an $(M_1 M_2, n_1 n_2, d)_q$-code, where d satisfies $d \geq d_1 d_2$, where $d_1 d_2$ is called the *design distance*.

For our purpose, we choose the concatenated code $C^{GRS\text{-}H}[n, q, \theta]$ explained in [8].

Concatenated Code $C^{GRS\text{-}H}[n, q, \theta]$. This is the concatenated code obtained by a certain generalized Reed-Solomon code as an outer code with a Hadamard code as an inner code. Following [8], we choose three parameters (q, n, θ) with $n, q \in \mathbb{N}$ and $\theta \in [0, 1]$ such that $n \geq 1$, $q \geq 2$, $n = mq^m\theta$, and $q^m\theta \in \mathbb{N}$ for a certain number $m \in \mathbb{N}$. Here, we use the $(q^m, q^m\theta, (1-\theta)q^m + 1)_{q^m}$ generalized Reed-Solomon code $\mathrm{GRS}^{(q^m, q^m\theta, q^m)}$ as an outer code and the $(q^m, m, (1-1/q)q^m)_q$ Hadamard code $\mathrm{HAD}^{(q,m)}$ as an inner code. The desired code $C^{GRS\text{-}H}[n, q, \theta] = \{C^{GRS\text{-}H}[n, q, \theta]_x\}_x$ is the collection of all concatenated codes defined by $C^{GRS\text{-}H}[n, q, \theta]_x(r, r') = \mathrm{HAD}^{(q,m)} \odot \mathrm{GRS}^{(q^m, q^m\theta, q^m)}$. This concatenated code is a $(q^{2m}, n, d)_q$-code, where $d \geq (1-1/q)(1-\theta)q^{2m}$ (design distance). We have the bound $\frac{\log(1/\theta)}{\log q} \leq m \leq n$, which further implies that $q^m \leq \frac{n \log q}{\theta \log(1/\theta)}$. Therefore, as far as $\theta = O(1/p(n))$ and $q = O(2^{p(n)})$ for a certain polynomial p, q^m is upper-bounded by $O(n^2 p(n)^2)$.

Now, we claim that $C^{GRS\text{-}H}[n, q, \theta]$ is quantumly list decodable for an appropriate choice of parameters (n, q, θ), assuming that the generalized Reed-Solomon codes are quantumly list decodable for a specific bias parameter.

Lemma 3.1 *Let $(q, n, \theta, m, \varepsilon, \varepsilon', \delta)$ satisfy the following conditions: $n, m, q \in \mathbb{N}^+$, $\theta, \varepsilon, \varepsilon', \delta \in [0, 1]$, $q \geq 2$, $q^m\theta \in \mathbb{N}$, $n = mq^m\theta$, and $\varepsilon^2 \geq \frac{(q-1)^3}{q^2}(q^{-2m} + \varepsilon')$. If the $(q^m, q^m\theta, (1-\theta)q^m + 1)_{q^m}$ generalized Reed-Solomon code has a quantum list decoder with bias ε' and confidence δ running in time polynomial in $(n, q, 1/\varepsilon', 1/\delta, 1/\theta)$, then $C^{GRS\text{-}H}[n, q, \theta]$ has a quantum list decoding algorithm with bias ε and confidence δ running in time polynomial in $(n, q, 1/\varepsilon', 1/\delta, 1/\theta)$.*

In this lemma, the value δ of the confidence of the generalized Reed-Solomon code is transferred to the concatenated code $C^{GRS\text{-}H}[n, q, \theta]$. The proof of the lemma is given in the subsequent subsection.

3.2 Quantum Reduction Technique

For the proof of Lemma 3.1, we wish to construct a "quantum reduction" between two quantumly corrupted codewords. It is useful to describe such a reduction, say, from $\tilde{O}$ to $\tilde{O}'$, as a quantum algorithm that, on each input $|r\rangle|s\rangle|t\rangle$, computes the outcome

$\tilde{O}'|r\rangle|s\rangle|t\rangle$ by making oracle calls to $\tilde{O}$. This can be seen as a strong form of well-known *Turing reduction* between two languages.

As a key lemma, we show a general result concerning the q-ary Hadamard code used as an inner code for an arbitrary outer code C. Now, let C be any $(q^m, n)_{q^m}$-code, which is treated as a function $C(x, r)$ mapping from $(\mathbb{F}_{q^m})^n \times (\mathbb{F}_q)^m$ to $(\mathbb{F}_q)^m$. The concatenated code $D = \mathrm{HAD}^{(q)} \odot C$ therefore satisfies that

$$D(x, r, s) = C(x, r) \cdot s \mod q$$

for $r \in (\mathbb{F}_q)^m$ and $s \in (\mathbb{F}_q)^m$. Our goal is to construct a quantum reduction between quantumly corrupted codewords $\tilde{O}_C$ and $\tilde{O}_D$ associated with C and D, respectively. For any unitary transform U, we conveniently say that a quantum algorithm $\mathcal{A}$ *realizes* U if, for any basis state $|r\rangle$, $\mathcal{A}$ on input $|r\rangle$ produces the state $U|r\rangle$ exactly.

We have the following key lemma on the code D.

Lemma 3.2 *Let C and D be the codes given as above and let $\tilde{O}_D$ be any quantumly corrupted codeword for D. There exist a polynomial-time quantum algorithm $\mathcal{B}$ and a quantumly corrupted codeword $\tilde{O}_C$ for C such that*

1. $\mathrm{Pre}_{\tilde{O}_C}(C_x) \geq \frac{1}{q^m} + \frac{q^2}{(q-1)^3}\left(\mathrm{Pre}_{\tilde{O}_D}(D_x) - \frac{1}{q}\right)^2 - \frac{1}{q^{2m}}$; *and*
2. *$\mathcal{B}$ realizes $\tilde{O}_C$ with access to $\tilde{O}_D$ as an oracle.*

From the above lemma, Lemma 3.1 follows easily. We quickly sketch its proof.

Proof of Lemma 3.1. Let $(q, n, \theta, m, \varepsilon, \varepsilon', \delta)$ be the parameters given in the lemma. For simplicity, write $M = q^m$. Assume that the $(M, M\theta, (1-\theta)M + 1)_M$ generalized Reed-Solomon code has a polynomial-time quantum list decoder $\mathcal{A}$ with bias ε' and confidence δ. Let $\tilde{O}$ be any quantumly corrupted codeword for $C^{GRS\text{-}H}[n, q, \theta]$. We want to find all messages x that satisfy the inequality $\mathrm{Pre}_{\tilde{O}}(C^{GRS\text{-}H}[n, q, \theta]_x) \geq 1/q + \varepsilon$. By Lemma 3.2, we can reduce $\tilde{O}$ to another quantumly corrupted codeword $\tilde{O}_C$ for the outer code $\mathrm{GRS}^{(M,M\theta,M)}$ with the following presence condition:

$$\mathrm{Pre}_{\tilde{O}}\left(\mathrm{GRS}_x^{(M,M\theta,M)}\right) \geq \frac{1}{M} + \frac{q^2\varepsilon^2}{(q-1)^3} - \frac{1}{M^2} \geq \frac{1}{M} + \varepsilon',$$

where the last inequality follows from the bound $\varepsilon^2 \geq \frac{(q-1)^3}{q^2}(1/M^2 + \varepsilon')$. By running a quantum list decoder for the $\mathrm{GRS}^{(M,M\theta,M)}$, we obtain a list that contains all messages x satisfying $\mathrm{Pre}_{\tilde{O}}(\mathrm{GRS}_x^{(M,M\theta,M)}) \geq 1/M + \varepsilon'$ with the desired probability. □

The proof of our key lemma (Lemma 3.2) is much more involved. We note that a simple approach using the following relation

$$C_x(r) = D_x(r, s^{(1)})D_x(r, s^{(2)}) \cdots D_x(r, s^{(m)}),$$

where $s^{(i)} = 0^{i-1}10^{l-i}$, does not give the desired presence value for C_x.

Proof of Lemma 3.2. Let C be any $(q^m, n)_{q^m}$-code and let D be the concatenated code $\mathrm{HAD}^{(q)} \odot C$. Assume that, for any $r, s \in (\mathbb{F}_q)^m$, $\tilde{O}_D|r, s\rangle|0\rangle|0^d\rangle = \sum_{z\in\mathbb{F}_q} \alpha_{r,s,z}|r, s\rangle|z\rangle|\phi_{r,s,z}\rangle$. The desired quantumly corrupted codeword $\tilde{O}_C$ can be realized by the following quantum algorithm using $\tilde{O}_D$ as an oracle.

Quantum Algorithm $\mathcal{B}$:

(1) Starting with $|r\rangle|0\rangle|0^{d+1}\rangle$ (a general case is similar), move the last register to the left-most location and then generate the state $(1/\sqrt{q-1})\sum_{k\in[q]}|k\rangle|r\rangle|0\rangle|0^d\rangle$.
(2) Fix k for the meantime and generate the state $q^{-m/2}\sum_{s\in(\mathbb{F}_q)^m}|k\rangle|r\rangle|s\rangle|0^d\rangle$.
(3) Apply $\tilde{O}_D$ to the first three registers. This step transforms the previous state into $\frac{1}{q^{m/2}}\sum_s\sum_{z\in\mathbb{F}_q}\alpha_{r,s,z}|k\rangle|r\rangle|s\rangle|z\rangle|\phi_{r,s,z}\rangle$.
(4) Encode the content of the fourth register into the "phase" together with the information on k, i.e., $\frac{1}{q^{m/2}}\sum_s\sum_z\omega_q^{k\cdot z}\alpha_{r,s,z}|k\rangle|r\rangle|s\rangle|z\rangle|\phi_{r,s,z}\rangle$. This process is known as the *phase encoding*.
(5) Apply the inverse of $\tilde{O}_D$. The resulted state $|\psi'_k\rangle$ can be expressed as $\sum_s\sum_z\beta_{k,r,s,z}|k\rangle|r\rangle|s\rangle|0\rangle|0^d\rangle + |k\rangle|\Delta_{k,r}\rangle$ with certain amplitudes $\beta_{k,r,s,z}$ and a certain vector $|\Delta_{k,r}\rangle$ whose last two registers contain no $|0\rangle|0^d\rangle$. The amplitude $\beta_{k,r,s,z}$ is calculated as

$$\begin{aligned}\beta_{k,r,s,z} &= (\langle k|\langle r|\langle s|\langle 0|\langle 0^d|)(\tilde{O}_D)^{-1}|\psi'_k\rangle \\ &= \frac{1}{q^{m/2}}\omega_q^{k\cdot z}|\alpha_{r,s,z}|^2.\end{aligned}$$

Note that $q^{-(2m+1)} \leq \sum_{s,z}|\beta_{k,r,s,z}|^2 \leq q^{-m}$ because

$$\frac{1}{q^{m+1}}\left(\sum_{s,z}|\alpha_{r,s,z}|^2\right)^2 \leq \sum_{s,z}|\alpha_{r,s,z}|^4 \leq \sum_{s,z}|\alpha_{r,s,z}|^2.$$

Therefore, our state $|\psi'_k\rangle$ is written in the form

$$\frac{1}{q^{m/2}}\sum_s\sum_z\omega_q^{k\cdot z}|\alpha_{r,s,z}|^2|k\rangle|r\rangle|s\rangle|0\rangle|0^d\rangle + |k\rangle|\Delta_{k,r}\rangle.$$

What is the norm of $|\Delta_{k,r}\rangle$? Since $\sum_{s,z}|\beta_{k,r,s,z}|^2 + \||\Delta_{k,r}\rangle\|^2 = 1$, the squared norm of $|\Delta_{k,r}\rangle$ satisfies $1 - q^{-m} \leq \||\Delta_{k,r}\rangle\|^2 \leq 1 - q^{-(2m+1)}$.
(6) If the last two registers contain $|0\rangle|0^d\rangle$, multiply the content s of the third register by k to obtain $k \cdot s$; otherwise, do nothing. Note that $k\cdot s$ is in $(\mathbb{F}_q)^m$ since so is s.
(7) Similarly, exactly when $|0\rangle|0^d\rangle$ is in the last two registers, apply the inverse Fourier transform $(F_q^{-1})^m$ over $\mathbb{F}_q$ to the second register. This produces the state $|\psi''_k\rangle = \sum_{w\in(\mathbb{F}_q)^m}\gamma_{k,r,w}|k\rangle|r\rangle|w\rangle|0\rangle|0^d\rangle + |k\rangle|\Delta_{k,r}\rangle$, where $\gamma_{k,r,w}$ is the complex number defined by $\gamma_{k,r,w} = \frac{1}{q^m}\sum_s\sum_z\omega_q^{k(z-w\cdot s)}|\alpha_{r,s,z}|^2$.
(8) Prepare two new registers $|0\rangle|0\rangle$ for $|\Delta_{k,r}\rangle$ and then generate $q^{-m/2}\sum_{w\in(\mathbb{F}_q)^m}|r\rangle|w\rangle$ so that we have the state $q^{-m/2}\sum_{w\in(\mathbb{F}_q)^m}|k\rangle|r\rangle|w\rangle \otimes |\Delta_{k,r}\rangle$.
(9) Finally, output the state

$$\frac{1}{\sqrt{q-1}}\sum_{k\in[q-1]}\sum_{w\in(\mathbb{F}_q)^m}\gamma_{k,r,w}|r\rangle|w\rangle|k\rangle|0\rangle|0^d\rangle + \frac{1}{\sqrt{q^m(q-1)}}\sum_{k\in[q-1]}\sum_{w\in(\mathbb{F}_q)^m}|r\rangle|w\rangle|k\rangle|\Delta_{k,r}\rangle.$$

This ends the description of $\mathcal{B}$.

To complete the proof, we need to evaluate the value of the presence of C_x in $\tilde{O}_C$, i.e., $\mathrm{Pre}_{\tilde{O}_C}(C_x) = \frac{1}{q^m(q-1)} \sum_{r\in\mathbb{F}_{q^m}, k\in[q-1]} \left(|\gamma_{k,r,C_x(r)}|^2 + q^{-m}\||\Delta_{k,r}\rangle\|^2\right)$. Note that $\sum_z |\alpha_{r,s,z}|^2 = 1$ for each pair (r,s). Recall that $\mathrm{Pre}_{\tilde{O}_D}(D_x) = q^{-2m}\sum_{r,s\in(\mathbb{F}_q)^m} |\alpha_{r,s,D_x(r,s)}|^2$. It thus follows that, for each $k \in [q-1]$,

$$\frac{1}{q^m}\sum_{r\in\mathbb{F}_{q^m}} |\gamma_{k,r,C_x(r)}|^2 \;\geq\; \frac{1}{q^{4m}}\left|\sum_{r,s} |\alpha_{r,s,D_x(r,s)}|^2 + \chi_k\right|^2$$
$$= \left(\mathrm{Pre}_{\tilde{O}_D}(D_x) + \mathrm{Re}(\chi_k)\right)^2 + \left(\mathrm{Im}(\chi_k)\right)^2,$$

where $\chi_k = q^{-2m}\sum_{r,s}\sum_{z\neq D_x(r,s)} \omega_q^{k(z-D_x(r,s))}|\alpha_{r,s,z}|^2$. An argument similar to [12] shows that, for a certain $k \in [q-1]$, $\mathrm{Re}(\chi_k) \geq -\frac{1}{q-1}\left(1 - \mathrm{Pre}_{\tilde{O}_D}(D_x)\right)$. Hence,

$$\frac{1}{q^m}\sum_{r\in\mathbb{F}_{q^m}} |\gamma_{k,r,C_x(r)}|^2 \geq \left|\frac{q}{q-1}\left(\mathrm{Pre}_{\tilde{O}_D}(D_x) - \frac{1}{q}\right)\right|^2.$$

Therefore, $\mathrm{Pre}_{\tilde{O}_C}(C_x)$ is lower-bounded by

$$\frac{1}{q-1}\left(\frac{q}{q-1}\right)^2\left(\mathrm{Pre}_{\tilde{O}_D}(D_x) - \frac{1}{q}\right)^2 + \frac{1}{q^m}\left(1 - \frac{1}{q^m}\right).$$

This completes the proof of Lemma 3.2. □

Lemma 3.2 gives a fast quantum reduction from $\tilde{O}_D$ to $\tilde{O}_C$. By contrast, there also exists a quantum reduction from $\tilde{O}_C$ to $\tilde{O}_D$ with the following conditions.

Lemma 3.3 *Let $\tilde{O}_C$ be any quantumly corrupted codeword for C. There exist a polynomial-time quantum algorithm $\mathcal{A}$ and a quantumly corrupted codeword $\tilde{O}_D$ for D such that*

1. $\mathrm{Pre}_{\tilde{O}_D}(D_x) = 1/q + (1-1/q)\,\mathrm{Pre}_{\tilde{O}_C}(C_x)$*; and*
2. *$\mathcal{A}$ realizes $\tilde{O}_D$ with oracle access to $\tilde{O}_C$.*

Proof Sketch. Given $\tilde{O}_C$, the following quantum algorithm $\mathcal{A}$ realizes the desired $\tilde{O}_D$.

Quantum Algorithm $\mathcal{A}$:

(1) Start with the state $|r\rangle|s\rangle|0^l\rangle|0^d\rangle|0^l\rangle$.
(2) Change the register order to obtain the state $|r\rangle|0^l\rangle|0^d\rangle|s\rangle|0^l\rangle$.
(3) Invoke $\tilde{O}_C$. Assume that we obtain the state $|\psi_1\rangle = \sum_{z\in\mathbb{F}_{q^m}} \alpha_{r,z}|r\rangle|z\rangle|\phi_{r,z}\rangle|s\rangle|0^l\rangle$.
(4) Compute deterministically $z\cdot s \bmod q$ from (s,z) to obtain $|\psi_2\rangle = \sum_z \alpha_{r,z}|r\rangle|z\rangle|\phi_{r,z}\rangle|s\rangle|z\cdot s \bmod q\rangle|\phi'_{s,z}\rangle$, where $|\phi'_{s,z}\rangle$ is the garbage produced while simulating the deterministic computation in a reversible fashion.
(5) Change the register order so that we obtain $|\psi_3\rangle = \sum_z \alpha_{r,z}|r\rangle|s\rangle|z\cdot s \bmod q\rangle|z\rangle|\phi_{r,z}\rangle|\phi'_{s,z}\rangle$.

It is not difficult to evaluate the value $\mathrm{Pre}_{\tilde{O}_D}(D_x)$ using $\mathrm{Pre}_{\tilde{O}_C}(C_x)$. ■

4 Complexity of generalized Reed-Solomon Codes

We turn our interest to the question of whether the generalized Reed-Solomon codes are efficiently quantum list decodable against a given bias parameter. We point out that a classical approach works well when the bias is relatively large; however, for smaller bias, there seems little hope in search of an efficient quantum list decoder. We also show that the generalized Reed-Solomon codes have natural connections to the *noisy polynomial interpolation problem* (NPIP) of Naor and Pinkas [13] and a lattice problem, which we call the *bounded distance vector problem* (BDVP).

4.1 A Direct and Simple Approach

A direct and simple approach toward the quantum list decoding of the $(q,n,q-n+1)_q$ generalized Reed-Solomon codes is the use of the Guruswami-Sudan polynomial reconstruction algorithm [7]. This approach works well after performing measurement on all oracle answers when bias is relatively large.

Lemma 4.1 *Let $n,q \in \mathbb{N}$ and $\varepsilon,\varepsilon',\delta \in (0,1)$ satisfy the conditions: $2 \leq n \leq q$, $n-2 \leq q\varepsilon' \leq q-1$, and $\varepsilon' + \left(1 - \frac{1}{q} - \varepsilon'\right)\sqrt{\frac{n-1}{1+q\varepsilon'}} < \varepsilon \leq 1 - \frac{1}{q}$. There exists a quantum list decoding algorithm for the $(q,n,q-n+1)_q$ generalized Reed-Solomon codes with bias ε and confidence δ running in time polynomial in $(n,q,1/\delta,1/(1-\delta))$.*

Proof. Choose numbers $n,q \in \mathbb{N}$ and $\varepsilon,\varepsilon',\delta \in (0,1)$ to satisfy the premise of the lemma. Let $\tilde{O}$ be any quantumly corrupted codeword for the $\mathrm{GRS}^{(q,n,q)}$. Now, we want to find all messages x satisfying the inequality $\mathrm{Pre}_{\tilde{O}}(\mathrm{GRS}_x^{(q,n,q)}) \geq 1/q + \varepsilon$. Fix such a message x arbitrarily in the following argument.

Let $A_{\varepsilon'} = \{r \in \mathbb{F}_q \mid |\alpha_{r,\mathrm{GRS}_x^{(q,n,q)}(r)}|^2 \geq 1/q + \varepsilon'\}$. It easily follows that $|A_{\varepsilon'}| \geq (1-\gamma_{\varepsilon,\varepsilon'})q$, where $\gamma_{\varepsilon,\varepsilon'} = \frac{1-1/q-\varepsilon}{1-1/q-\varepsilon'}$, because we have

$$\frac{1}{q} + \varepsilon \leq \mathrm{Pre}_{\tilde{O}}(\mathrm{GRS}_x^{(q,n,q)}) \leq \frac{|A_{\varepsilon'}|}{q} + \frac{|\mathbb{F}_q - A_{\varepsilon'}|}{q}\left(\frac{1}{q} + \varepsilon'\right).$$

Initially, set r to be 0. Using $\tilde{O}$ as an oracle, we iterate the following procedure by incrementing r by one. First, we make a query on r to the oracle T times, where T is the minimal integer satisfying

$$T \geq \left(\frac{q}{1+q\varepsilon'} - 1\right)\log\frac{q}{(1+q\varepsilon')(1-\delta^{1/q})}.$$

Notice that $1 - \delta^{1/q} \geq (1-\delta)/q > 0$ since $\delta < 1$. After receiving each answer from $\tilde{O}$, we perform a measurement on the computational basis over $\mathbb{F}_q$ and store a pair (r,y) if y is a result of this measurement. Since there are at most $q/(1+q\varepsilon')$ values y with $|\alpha_{r,y}|^2 \geq 1/q + \varepsilon'$, the probability P_r of obtaining all such y's is bounded by

$$P_r \geq 1 - \frac{q}{1+q\varepsilon'}\cdot\left(1 - \frac{1}{q} - \varepsilon'\right)^T \geq \delta^{1/q},$$

where the last inequality follows from the choice of T. After the qth iteration, we can store at most $q^2/(1+q\varepsilon')$ points. Let $S_{\varepsilon'}$ be the set of all stored points. The probability that $S_{\varepsilon'}$ contains all the points (r,y) that satisfy $|\alpha_{r,y}|^2 \geq 1/q + \varepsilon'$ is at least $\prod_{r\in\mathbb{F}_q} P_r \geq \left(\delta^{1/q}\right)^q = \delta$.

Lastly, we should find all univariate polynomials p of degree at most $n-1$ that lie on at least $|A_{\varepsilon'}|$ points in $S_{\varepsilon'}$. For this purpose, we run the well-known Guruswami-Sudan polynomial reconstruction

algorithm. Guruswami and Sudan [7] gave a deterministic algorithm $\mathcal{A}$ that solves in time polynomial in $(m, \log q)$ the following *polynomial reconstruction problem*: on input of integers m, n', t and m points $\{(x_i, y_i)\}_{i\in[m]} \subseteq \mathbb{F}_q \times \mathbb{F}_q$, find all univariate polynomials p of degree at most n' which lie on at least t points, provided that $t > \sqrt{mn'}$.

The choice of our parameters implies that

$$|A_{\varepsilon'}| \geq (1 - \gamma_{\varepsilon,\varepsilon'})q > \sqrt{\frac{q^2(n-1)}{1+q\varepsilon'}} \geq \sqrt{(n-1)|S_{\varepsilon'}|}.$$

Therefore, the Guruswami-Sudan algorithm correctly produces a list[†] that includes all the polynomials p of degree at most $n-1$ that satisfy $|\alpha_{r,p(r)}|^2 \geq 1/q + \varepsilon'$ for at least $(1-\gamma_{\varepsilon,\varepsilon'})q$ indices r. Hence, the list also includes all messages x for which $\mathrm{Pre}_{\tilde{O}}(\mathrm{GRS}_x^{(q,n,q)}) \geq 1/q + \varepsilon$. □

Combining the above lemma with Lemma 3.1, we obtain the proposition below.

Proposition 4.2 *Let $(q, n, \theta, m, \varepsilon, \delta)$ satisfy the conditions: $m, n, q \in \mathbb{N}^+$, $\varepsilon, \delta, \theta \in [0,1]$, $q \geq 2$, $q^m\theta \in \mathbb{N}$, $n = mq^m\theta$, $2\theta < 1 + q^{-m}$, and $\varepsilon^2 > t^2(\theta - q^{-m}) + \frac{1}{t}(1-q^{-m}) - q^{-m} + q^{2m}$, where $t = \left(\frac{q^m-1}{2(q^m\theta-1)}\right)^{1/3}$. The concatenated code $C^{GRS\text{-}H}[n, q, \theta]$ has a quantum list decoder with bias ε and confidence δ running in time polynomial in $(n, q, 1/\varepsilon, 1/\delta, 1/(1-\delta))$.*

To use the Guruswami-Sudan algorithm in the proof of Lemma 4.1, we make the bias ε relatively large. Is there any other way to list decode the generalized Reed-Solomon codes from a quantumly corrupted codeword even for relatively small bias? We can show in the next proposition that an *efficient* quantum list decoder for the generalized Reed-Solomon codes with arbitrary bias and high confidence can be used to solve all NP-problems *efficiently* on a quantum computer with high success probability.

Proposition 4.3 *Let $t(n)$ be any function from $\mathbb{N}$ to $\mathbb{N}$ with $t(n) \geq n$ for all $n \in \mathbb{N}$. If there exists a quantum list decoder for the generalized Reed-Solomon codes with arbitrary bias and confidence $2/3$ running in $t(n)$ time, then every NP-problem can be solved by a certain quantum algorithm with success probability at least $2/3$ in $n^{O(1)}t(n)$ time.*

Proof. We want to give a reduction from a certain NP-complete problem to the QLDP with a specific quantumly corrupted codeword. To make our proof simple, we use the following restricted form of the interpolation problem discussed in [6].

Constrained Interpolation Problem (CIP)

- Input: three numbers $d, e, m \in \mathbb{N}$, a prime q, a set $A = \{(x_1, y_1), \ldots, (x_m, y_m)\}$ of m points in $\mathbb{F}_q \times \mathbb{F}_q$, given in binary.
- Condition: $d_A(x_1) = 1$ and $d_A(x_i) = 2$ for any $i \in [2, m]_{\mathbb{Z}}$, where $d_A(x) = |\{y \mid (x, y) \in A\}|$.
- Question: is there any univariate polynomial p of degree at most d such that $p(x_1) = y_1$ and $p(x_i) = y_i$ for at least e different i's?

This problem is clearly in NP and is also proven to be NP-hard[‡] [6]. Now, let $d, e, m \in \mathbb{N}$, let q be a prime, and let $A = \{(x_1, y_1), \ldots, (x_m, y_m)\}$ be any set of m points in $\mathbb{F}_q \times \mathbb{F}_q$. Define D as the set $\{x_1, \ldots, x_m\}$ of code locators and write $\ell = |D|$. Note that $\ell = (m-1)/2$ by the given condition.

Using A, we define a quantumly corrupted codeword $\tilde{O}$ of the form $\tilde{O}|x\rangle|s\rangle|t\rangle = \sum_{y\in\mathbb{F}_q} \alpha_{x,y}|x\rangle|y \oplus s\rangle|t\rangle$ for every $x \in \mathbb{F}_q$. Let (x, y) be any point in $\mathbb{F}_q \times \mathbb{F}_q$. If $(x, y) \in A$, let $\alpha_{x,y} = 1/\sqrt{d_A(x)}$; otherwise, let $\alpha_{x,y} = 0$. Finally, let $\varepsilon = \varepsilon(e, m, q) = \frac{e+2}{2\ell} - \frac{1}{q}$. Note that $\varepsilon > 0$ since $\ell \leq q$.

Now, we claim the following: a polynomial p of degree d passes on at least e points in A as well as the point (x_1, y_1) if and only if the presence of p in $\tilde{O}$ satisfies

$$\frac{1}{|D|}\sum_{x\in D} \mathrm{Pre}_{\tilde{O}}(p) \geq \frac{1}{\ell} + \frac{1}{\ell}\cdot\frac{e}{2} = \frac{1}{q} + \varepsilon.$$

Therefore, solving the CIP can be reduced to solving the ε-QLDP with $\tilde{O}$. Note that it takes only quantum polynomial time to *realize* $\tilde{O}$ from the set A (which is given as an input). Applying a $t(n)$-time quantum list decoder for the ε-QLDP with confidence $2/3$, we obtain a valid list of polynomials p. The list size is at most $t(n)$. Since the list may contain illegitimate polynomials, we need to check if each p passes on at least $e+1$ different points in A including (x_1, y_1). This quantum algorithm solves the CIP with success probability at least $2/3$. □

Since the inclusion NP $\subseteq$ BQP seems unlikely, there is little hope to find a "polynomial-time" quantum list decoder for the generalized Reed-Solomon code with relatively small bias.

4.2 Noisy Polynomial Interpolation Problem

We point out that quantum list decoding of the generalized Reed-Solomon code is closely related to the *noisy polynomial interpolation problem*[§] introduced by Naor and Pinkas [13].

Noisy Polynomial Interpolation Problem (NPIP)

- Input: three numbers $k, m, n \in \mathbb{N}$, a prime q, n distinct points $\{x_1, x_2, \ldots, x_n\}$ in $\mathbb{F}_q$, and n sets $S_1, \ldots, S_n$, each of which consists of exactly m elements from $\mathbb{F}_q$.
- Promise: there exists a *unique* polynomial p of degree at most k such that, for each $i \in [n]$, there exists exactly one element $y \in S_i$ satisfying $p(x_i) = y$.
- Output: the hidden polynomial p.

Naor and Pinkas used the NPIP as an intractable assumption for a cryptographic primitive, called *oblivious polynomial evaluation*. Now, we prove the following.

Proposition 4.4 *If the generalized Reed-Solomon codes are quantum list decodable with arbitrary bias and confidence $2/3$, then there exists a quantum algorithm that solves the NPIP with probability at least $2/3$.*

Proof. Take n distinct elements $X = \{x_1, \ldots, x_n\}$ and n sets $S_1, \ldots, S_n$ of m elements each. Assume that the promise of the NPIP holds with a unique polynomial, say, p of degree at most k. We set the

[†] Actually, to obtain an output of a unique list, we need to repeat the above process.

[‡] This fact is observed by examining the reduction constructed in [6] from the subset sum problem.

[§] This name is actually taken from the paper by Bleichenbacher and Nguyen [2].

bias ε to be $\frac{n}{q}(1/m - 1/q)$ and let $S = \bigcup_{i\in[m]} S_i$. Note that $k, m, n \le q$.

Let us define a quantumly corrupted codeword $\tilde{O}$ as follows. For any element x in X, say $x = x_i$ for a certain $i \in [m]$, let $\tilde{O}|x_i\rangle|s\rangle|t\rangle = \frac{1}{\sqrt{m}} \sum_{y\in S_i} \delta_{i,y}|x_i\rangle|s \oplus y\rangle|t\rangle$, where $\delta_{i,y} = 1$ if $y \in S_i$ and 0 otherwise. For the other elements x outside of X, let $\tilde{O}|x\rangle|s\rangle|t\rangle = \frac{1}{\sqrt{q}} \sum_{y\in\mathbb{F}_q} |x\rangle|s \oplus y\rangle|t\rangle$. We claim that the unique polynomial p satisfies the condition $\mathrm{Pre}_{\tilde{O}}(p) \ge 1/q+\varepsilon$. Since $|X| = n$ and $|\mathbb{F}_q - X| = q-n$, it follows that

$$\begin{aligned}\mathrm{Pre}_{\tilde{O}}(p) &= \frac{1}{q}\sum_{x\in\mathbb{F}_q} |\alpha_{x,y}|^2 = \frac{1}{q}\sum_{x\in X}\frac{1}{m} + \frac{1}{q}\sum_{x\notin X}\frac{1}{q} \\ &= \frac{1}{q}\left(\frac{n}{m} + \frac{q-n}{q}\right) = \frac{1}{q} + \frac{n}{q}\left(\frac{1}{m} - \frac{1}{q}\right).\end{aligned}$$

Hence, we conclude that $\mathrm{Pre}_{\tilde{O}}(p) \ge 1/q + \varepsilon$.

Now, consider the ε-QLDP for the $\mathrm{GRS}^{(n,k,q)}$ with $\tilde{O}$. By our assumption, there exists a quantum list decoder $\mathcal{A}$ that solves this ε-QLDP with high confidence. To apply this $\mathcal{A}$ to find the hidden polynomial p, we need to *realize* $\tilde{O}$ from the given inputs $(x_1, \ldots, x_n, S_1, \ldots, S_n)$. This is done by generating the state $\tilde{O}|x_i\rangle|s\rangle|t\rangle$ as follows: choose y in S_i randomly and then generate the amplitude $\delta_{i,y}/\sqrt{m}$. Therefore, we can solve the NPIP with high success probability. □

4.3 Bounded Distance Vector Problem

To construct a quantum list decoder for the generalized Reed-Solomon code against relatively small bias, it suffices to give a quantum algorithm to the following lattice problem.

Bounded Distance Vector Problem (BDVP)

- Input: m basis vectors $b_1, b_2, \ldots, b_m \in \mathbb{Z}^n$ and a radius $\xi \in \mathbb{Q}$.
- Oracle: given a vector $v \in \mathbb{Z}^n$, returns the value $\|v\|^2 = \sum_{j\in[n]} \lambda_j^2 v_j^2$, where $v = (v_1, \ldots, v_n)$ and $\lambda = (\lambda_j)_j \in [0,1]^n$ is a weight vector.
- Output: a list that contains all vectors v in the lattice L spanned by $\{b_1, b_2, \ldots, b_m\}$, satisfying $\|v\|^2 \le \xi$.

Proposition 4.5 *If there exists a quantum algorithm that solves the BDVP with probability at least* $2/3$*, then there exist quantum list decoders for the generalized Reed-Solomon codes with arbitrary bias and confidence* $2/3$*.*

Proof. The following argument is owing to [2]. We want to construct an efficient quantum reduction to the BDVP from the QLDP for the $(M, n, M-n+1)_q$ generalized Reed-Solomon code. This proves the proposition.

Fix a set $D_M = \{x_1, x_2, \ldots, x_M\}$ of M distinct code locators in $\mathbb{F}_q$ and consider the product set $D_M \times \mathbb{F}_q = \{(x_i, z_j) \mid i \in [M], j \in [q]\}$. Let ε be any bias and assume that a quantumly corrupted codeword $\tilde{O}$ for the generalized Reed-Solomon code satisfies $\tilde{O}|x_i\rangle|s\rangle|t\rangle = \sum_{j\in[q]} \alpha_{i,j}|x_i\rangle|s \oplus z_j\rangle|t \oplus \phi_{i,j}\rangle$. The *(special) Lagrange interpolation polynomials* corresponding to D_M are $L_i(x) = \prod_{j\in[M]-\{i\}} \frac{x-x_j}{x_i-x_j}$ in $\mathbb{F}_q[x]$, which is of degree $M-1$, for each $i \in [M]$. Note that every $L_i(x)$ satisfies the following property: $L_i(x_i) = 0$ and $L_i(x_j) = 0$ if $j \ne i$. Assume that $L_i(x) = \sum_{k=1}^{M} c_{ik}x^{k-1}$ for certain constants $c_{ik} \in \mathbb{F}_q$.

Let $a = (a_1, a_2, \ldots, a_n) \in (\mathbb{F}_q)^n$ be any message and let $p_a(x) = \sum_{k=1}^{n} a_k x^{k-1}$ be its codeword, i.e., the polynomial over $\mathbb{F}_q$ of degree at most $n-1$. Now, we assume that $\mathrm{Pre}_{\tilde{O}}(p_a) \ge 1/q + \varepsilon$. Note that p_a satisfies the Lagrange's interpolation formula:

$$\begin{aligned}p_a(x) &= \sum_{i=1}^{M} p_a(x_i)L_i(x) = \sum_{i=1}^{M}\sum_{j=1}^{q} \delta_{ij}^{(a)} z_j L_i(x) \\ &= \sum_{k=1}^{M}\left(\sum_{i=1}^{M}\sum_{j=1}^{q}\delta_{ij}^{(a)} z_j c_{ik}\right) x^{k-1},\end{aligned}$$

where $\delta_{ij}^{(a)} = 1$ if $p_a(x_i) = z_j$ and 0 otherwise. Note that $\sum_{j=1}^{q} \delta_{ij}^{(a)} = 1$ for each fixed i and a. Let $\delta^{(a)} = (\delta_{ij}^{(a)})_{ij} \in \mathbb{Z}^{qM}$ be our *target vector*. We define the set L as the collection of all vectors $d = (d_{ij})_{ij} \in \mathbb{Z}^{qM}$ such that

1. $\forall i, i' \in [M]\left[\sum_{j=1}^{q} d_{ij} = \sum_{j=1}^{q} d_{i'j}\right]$; and
2. $\forall k \in [n+1, M]_{\mathbb{Z}}\left[\sum_{i=1}^{M}\sum_{j=1}^{q} d_{ij} z_j c_{ik} = 0 \bmod q\right]$.

It is not difficult to show that L forms a lattice. Notice that the target vector $\delta^{(a)}$ belongs to L. A set of basis vectors $\{b_1, b_2, \ldots, b_m\}$ for L can be found easily (see, e.g., [2]).

Next, we define a weight vector $\lambda = (\lambda_{ij})_{ij} \in [0,1]^{qM}$ as follows: for each point (x_i, z_j), let $\lambda_{i,j} = \sqrt{1 - |\alpha_{x_i,z_j}|^2}$. The *weighted norm* $\|d\|$ of a vector $d = (d_{ij})_{ij} \in L$ is thus calculated as $\|d\| = \sqrt{\sum_{i,j} d_{ij}^2 \lambda_{ij}^2} = \sqrt{\sum_{i,j} d_{ij}^2 (1 - |\alpha_{x_i,z_j}|^2)}$. Therefore, the square of the weighted norm of $\delta^{(a)}$ equals

$$\begin{aligned}\|\delta^{(a)}\|^2 &= \sum_{ij}\left(\delta_{ij}^{(a)}\right)^2\left(1 - |\alpha_{x_i,p_a(x_i)}|^2\right) \\ &= M\left(1 - \mathrm{Pre}_{\tilde{O}}(p_a)\right).\end{aligned}$$

By taking the radius $\xi = M(1 - 1/q - \varepsilon)$, it follows that $\|\delta^{(a)}\|^2 \le \xi$ iff $\mathrm{Pre}_{\tilde{O}}(p_a) \ge 1/q + \varepsilon$.

To solve the QLDP, we first compute a basis vectors $b_1, \ldots, b_m$ and a radius ξ. We then solve the BDVP using the weight vector (given by an oracle). Let $v_1, \ldots, v_k$ be the resulted list of vectors in L. For each v_i, find $a_i \in (\mathbb{F}_q)^n$ such that $v_i = \delta^{(a_i)}$ by solving a set of linear equations. □

5 Quantum Search Problems

We present an example of how to use Proposition 4.2. Our example here is a QCMA search problem. Set our alphabet Σ to be $\{0,1\}$ in this section. A *QCMA search problem* is a triplet (L, M, p), where L is a language, M is a polynomial-time quantum algorithm taking inputs from $\Sigma^* \times \Sigma^*$, and p is a polynomial, with the following two requirements:

1. for every $x \in L$, there exists a witness $y \in \Sigma^{p(|x|)}$ such that $\mathrm{Prob}_M[M(x,y) = 1] \ge 2/3$; and
2. for every $x \notin L$, $\mathrm{Prob}_M[M(x,y) = 0] \ge 2/3$ holds for any string $y \in \Sigma^{p(|x|)}$.

A *solution function* f for the search problem (L, M, p) satisfies that (i) for every $x \in L$, $\mathrm{Prob}_M[M(x, f(x)) = 1] \ge 2/3$ and $|f(x)| = p(|x|)$ and (ii) for every $x \notin L$, $f(x) = \perp$ (a special symbol). Moreover, QCMA

denotes the class consisting of all languages L over the alphabet Σ such that there exist a polynomial-time quantum algorithm M and a polynomial p for which (L, M, p) is a QCMA search problem.

Proposition 5.1 *Let s be any positive polynomial. The following two statements are equivalent.*

1. *For every QCMA search problem, there exist its solution function g and a polynomial-time quantum algorithm $\mathcal{A}$ such that, for every x, $\mathrm{Prob}_{\mathcal{A},i}[\mathcal{A}(x,1^i) = (g(x))_i] \geq 1/2 + 1/s(|x|)$.*
2. *For every QCMA search problem, there exist its solution function f and a polynomial-time quantum algorithm $\mathcal{B}$ such that, for every x, $\mathrm{Prob}_{\mathcal{B}}[\mathcal{B}(x) = f(x)] \geq 2/3$.*

An immediate corollary is stated as follows.

Corollary 5.2 *Assuming that* QCMA $\neq$ BQP*, for every positive polynomial pair (p, p') with $p'(n) > p(n)$ for all $n \in \mathbb{N}$, there exists a QCMA search problem $\mathcal{P}$ that satisfies the following: for any solution function f for $\mathcal{P}$, no polynomial-time quantum algorithm finds strings y, on each input x of length n, with probability at least $1 - \frac{2p(n)}{p'(n)(p(n)+2)}$ such that the relative distance $\Delta(y, f(x))$ is at most $1/2 - 1/p(n)$.*

Proof. Assume that QCMA $\neq$ BQP. Assume also that, for every QCMA search problem, there exist its solution function f and a polynomial-time quantum algorithm $\mathcal{A}$ that finds a string y, on each input x, with probability at least $1 - \frac{2p(n)}{p'(n)(p(n)+2)}$ with $\Delta(y, f(x)) \leq 1/2 - 1/p(n)$.

Consider the following algorithm $\mathcal{B}$: on input $(x, 1^i)$, run $\mathcal{A}$ on input x and then output the ith bit of its outcome. The success probability of $\mathcal{B}$ is lower-bounded by

$$\begin{aligned}
&\mathrm{Prob}_{\mathcal{B},i}[\mathcal{B}(x,1^i) = (f(x))_i] \\
&\geq \left(1 - \frac{2p(n)}{p'(n)(p(n)+2)}\right)(1 - \max\{\Delta(y, f(x)))\}) \\
&= \frac{1}{2} + \frac{1}{p(n)} - \frac{1}{p'(n)}.
\end{aligned}$$

Now, choose a polynomial s satisfying that $1/s(n) \leq 1/p(n) - 1/p'(n)$ for all $n \in \mathbb{N}$. By Proposition 5.1, we have a polynomial-time quantum algorithm that computes a certain solution function with probability at least 3/4. This means that QCMA is included in BQP, a contradiction. □

Finally, we give the proof of Proposition 5.1.

Proof of Proposition 5.1. Let s be any positive polynomial. Take two positive polynomials q, t and a $(t(n), n)_2$-code family C that is polynomial-time classically list decodable and has a polynomial-time quantum list decoder D with bias $1/s(t^{-1}(n))$ and confidence 2/3, producing a list of size at most $q(n)$, where n is message length. Without loss of generality, we can assume that $t(n) \geq n$ for all $n \in \mathbb{N}$.

The implication (2) $\Rightarrow$ (1) is trivial. Next, we assume (1) and want to show (2). Let $\mathcal{P} = (L, M, p)$ be any QCMA search problem. Assume also that $p(n) \geq n$ for all $n \in \mathbb{N}$. Note that a standard *majority vote technique* can reduce the bounded error probability of a quantum algorithm exponentially small (without changing the witness size) by polynomially-many repetitions. Therefore, we can assume from (1) that

1. for every $x \in L$, there exists a witness $y \in \Sigma^{p(|x|)}$ such that $\mathrm{Prob}_M[M(x,y) = 1] \geq 1 - 2^{-r(|x|)}$; and
2. for every $x \notin L$ and for every $y \in \Sigma^{p(|x|)}$, we have $\mathrm{Prob}_M[M(x,y) = 0] \geq 1 - 2^{-r(|x|)}$,

where $r(n) = t(p(n)) + 3$ and M is a certain polynomial-time quantum algorithm that depends on (p, r, L).

Now, we define another QCMA search problem $\mathcal{P}'$ as follows. Let C_y denote the codeword, to which y is encoded, of block length $t(|y|)$. Consider the quantum algorithm M' that behaves as follows.

> On input (x, z), first run the classical list decoding algorithm in polynomial time to produce with probability at least 5/6 a list S of candidates for C using z as a classically corrupted codeword (or a received word). Next, check if $z = C_y$ for a certain $y \in S$. If there is no such y, reject immediately. Assuming $z = C_y$, run $M(x, y)$ and outputs its outcome.

Let $\mathcal{P}' = (L, M', p)$. We then claim that $\mathcal{P}'$ is a QCMA search problem. Take any $n \in \mathbb{N}$ and any $x \in \Sigma^n$. Consider the case where $x \in L$. Since there exists a witness $y \in \Sigma^{p(n)}$, the corresponding codeword $z = C_y$ forces M' to accept (x, z) with probability at least $\frac{5}{6}(1 - 2^{-r(|x|)}) \geq 2/3$. For the other case where $x \notin L$, let z be any string in $\Sigma^{t(p(n))}$. If $z \neq C_y$ for all $y \in S$, then M' accepts (x, z) with probability $\leq 1/6$. On the contrary, if $z = C_y$ for a certain $y \in S$, then M' accepts (x, z) with probability $\leq \frac{5}{6} 2^{-r(|x|)} \leq 1/3$.

Again, by the majority vote technique, we can reduce the error probability of M' to $2^{-r(n)}$. Abusing the notation, we use M' to denote this new algorithm. By our assumption (1), there exist a solution function g for $\mathcal{P}'$ and a polynomial-time quantum algorithm $\mathcal{A}$ such that, for every $x \in \Sigma^n$,

$$\mathcal{A}(x, 1^i) = \alpha_{x,i,0}|i\rangle|0\rangle|\phi_{x,0}\rangle + \alpha_{x,i,1}|i\rangle|1\rangle|\phi_{x,1}\rangle,$$

where $\||\phi_{x,b}\rangle\| = 1$ for any choice $b \in \{0, 1\}$, and $\mathrm{Prob}_{\mathcal{A},i}[\mathcal{A}(x, 1^i) = (g(x))_i] \geq 1/2 + 1/s(n)$.

We fix an arbitrary x and, for the meantime, we omit subscript x. Let us define the oracle $\tilde{O}$ as follows:

$$\tilde{O}|i\rangle|0\rangle|0\rangle = \alpha_{i,0}|i\rangle|0\rangle|\phi_{i,0}\rangle + \alpha_{i,1}|i\rangle|1\rangle|\phi_{i,1}\rangle.$$

If there exists a string y satisfying $C_y = g(x)$, then the presence of C_y in $\tilde{O}$ is

$$\begin{aligned}
\mathrm{Pre}_{\tilde{O}}(C_y) &= \frac{1}{p(n)} \sum_i |\alpha_{i,C_y(i)}|^2 \\
&= \frac{1}{p(n)} \sum_i |\alpha_{i,(g(x))_i}|^2 \geq \frac{1}{2} + \frac{1}{s(n)}.
\end{aligned}$$

Recall that D produces a list of size at most $t(n)$ for message length n. We assume the standard order in $\Sigma^{p(n)}$. Consider the following algorithm $\mathcal{B}$.

> On input x ($n = |x|$), run D using $\tilde{O}$ as an oracle to produce a list S' of $t(p(n))$ candidates (since the message size is $p(n)$), which include the above y (if $x \in L$), with probability $\geq 1 - 2^{-r(n)}$. Run $M'(x, z)$ sequentially for all $z \in S'$ in order. Output the first $z \in S'$ such that $M'(x, z)$ outputs 1. If there is no such z, output $\perp$.

Let $f(x)$ be the minimal string z in S' such that (i) $\mathrm{Prob}_{M'}[M'(x, z) = 1] \geq 1 - 2^{-r(n)}$ and (ii) for all

$z' < z$ in S', $\mathrm{Prob}_{M'}[M'(x,z')=0] \geq 1-2^{-r(n)}$. The probability that $\mathcal{B}(x)$ outputs $f(x)$ is at least $\left(1-2^{-r(n)}\right)^{t(p(n))} \geq 1-2^{-r(n)+t(p(n))-1} \geq 3/4$. This guarantees that we obtain $f(x)$ with probability at least $3/4$. □

6 Further Discussion

In the previous sections, we have used the model of implicit inputs and explicit outputs. When the running time of a quantum list decoder is limited to sublinear, it becomes impossible to explicitly output a list of messages. Instead, we may allow a quantum list decoder to produces a list of "oracle quantum circuits," each of which output each block element of a specific message with oracle access to a quantumly corrupted codeword. Such a model is called an *implicit-output model*. We briefly discuss a realm of quantum list decoding on this implicit-input implicit-output model.

Let us introduce the notion of local quantum list decoding, analogous to local list decoding.

Definition 6.1 Let C be any $(M(n), n, d(n))_{q(n)}$-code family with message alphabet Σ. We say that C is *locally quantum list decodable* with bias ε and confidence δ if there exists a quantum algorithm $\mathcal{A}$ such that, for any message length $n \in \mathbb{N}$ (given in binary, not in unary), any $\tilde{O}$ for C, and any $x \in \Sigma^n$ with $\mathrm{Pre}_{\tilde{O}}(C_x) \geq 1/q + \varepsilon(n)$, the following happens with probability at least $3/4$:

1. $\mathcal{A}(n)$ outputs a list of descriptions of oracle quantum circuits $D_1, D_2, \ldots, D_\ell$; and
2. there exists an index $j \in [\ell]$ such that, for every $i \in [n]$, $D_j^{\tilde{O}}(i)$ outputs x_i with probability at least $\delta(n)$

Similar to $C^{GRS\text{-}H}$, we can define the concatenated code $C^{RM\text{-}H}$ using an appropriate Reed-Müller code and a proper Hadamard code. Following an argument of [17], we can easily prove that, using Lemmas 3.2 and 4.1, the code $C^{RM\text{-}H}$ is efficiently locally quantum list decodable with polynomially-small bias and confidence $2/3$. Hence, we can conclude:

Lemma 6.2 *There exists a code family of polynomially-small rate and constant codeword alphabet size that are efficiently locally quantum list decodable with confidence $2/3$ for polynomially-small bias.*

An immediate consequence of this lemma is the hardness amplification of quantum circuits, again following an argument of [17].

Corollary 6.3 *There exists a constant $d > 0$ for which the following is true. Let $\varepsilon \in (0,1)$ and let f be any Boolean function from $\{0,1\}^{k(n)}$. If no quantum circuit of size s computes f with probability at least δ, then there exists a Boolean function g mapping $\{0,1\}^{\ell \circ k(n)}$ with $\ell(n) \in O(n)$ such that no quantum circuit C of size $s' = (k(n)/\varepsilon)^d \cdot s$ satisfies $\mathrm{Prob}_{C,x}[C(x) = g(x)] \geq 1/2 + \varepsilon$, where $C(x)$ denotes the random variable indicating the observed outcome bit of C on input x.*

7 Concluding Remarks and Open Problems

The theme of this paper is an exploration of quantum list decodable code families of polynomially-small rate and constant codeword alphabet size. We have shown that certain generalized Reed-Solomon codes concatenated with Hadamard codes achieving such requirement are efficiently quantum list decodable when the bias of presence is relatively large. Even with such large bias, this helps us show the local quantum list decodability of Reed-Müller codes. Notice that a core part of the proofs of these results heavily relies on classical list decoding algorithms of [7, 17]. Among codes of polynomially-small rate, is there any code whose quantum list decoding algorithm is in essence different from its classical one? Is there any quantum list decodable code that is not even classically list decodable? Does a generalized Reed-Solomon code have a subexponential-time quantum list decoder against arbitrary bias? Another important open problem is to find useful applications of quantum list decoding to a wide range of quantum information processing.

Acknowledgements: The author thanks Akinori Kawachi for a discussion on quantum cryptography and Igor Shparlinski for a pointer to reference [2].

References

[1] M. Adcock and R. Cleve. A quantum Goldreich-Levin theorem with cryptographic applications. In *Proc. 19th STACS 2002*. LNCS Vol.2285, pp.323–334, 2002.

[2] D. Bleichenbacher and P. Q. Nguyen. Noisy polynomial interpolation and noisy Chinese remaindering. In *Proc. EUROCRYPT 2000*, LNCS Vol.1807, pp.53–69, 2000.

[3] P. Elias. List decoding for noisy channels. *WESCON Convention Record*, Part 2, Institute of Radio Engineers, pp.94–104, 1957.

[4] G. D. Forney. *Concatenated Codes*, MIT Press, Cambridge, MA, 1966.

[5] O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In *Proc. 21st ACM STOC'89*, pp.25–32, 1989.

[6] O. Goldreich, R. Rubinfeld, and M. Sudan. Learning polynomials with queries: the highly noisy case. *Proc. 36th IEEE FOCS'95*, pp.294–303, 1995.

[7] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45, 1757–1767, 1999.

[8] V. Guruswami and M. Sudan. List decoding algorithms for certain concatenated codes. In *Proc. 32nd ACM STOC 2000*, pp.181–190, 2000.

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

[10] M. Kearns, R. Schapire, and L. Sellie. Towards efficient agnostic learning. In *Proc. 5th ACM COLT*, ACM Press, pp.341–352, 1992.

[11] J. Katz and L. Trevisan. On the efficiency of local decoding procedures for error-correcting codes. *Proc. 32nd ACM STOC 2000*, pp.80–86, 2000.

[12] A. Kawachi and T. Yamakami. Quantum hardcore functions by complexity-theoretical quantum list decoding. In *Proc. 33rd ICALP 2006*, LNCS Vol.4052, pp.216–227, 2006. See also ArXiv.org quant-ph/0602088 and ECCC Report TR06-020.

[13] M. Naor and B. Pinkas. Oblivious transfer and polynomial evaluation. In *Proc. 31st ACM STOC'99*, pp.245–254, 1999.

[14] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *J. SIAM* 8, 300-304, 1960.

[15] M. Sudan. Decoding of Reed-Solomon codes beyond the error-correction bound. *J. Complexity*, 13 (1997), 180–193.

[16] M. Sudan. List decoding: Algorithms and applications. *SIGACT News*, Vol.31, pp.16–27, 2000.

[17] M. Sudan, L. Trevisan, and S. Vadhan. Pseudorandom generators without the XOR lemma. *J. Comput. System Sci.*, 62, 236–266, 2001.

[18] J. M. Wozencraft. List decoding. Quarterly Progress report. Research Laboratory of Electronics, MIT, Vol.48, pp.90–95, 1958.