The Quantum Decoding Problem

André Chailloux, Jean-Pierre Tillich

The Quantum Decoding Problem

André Chailloux[1] and Jean-Pierre Tillich[1]
Inria de Paris, {andre.chailloux,jean-pierre.tillich}@inria.fr

Abstract

One of the founding results of lattice based cryptography is a quantum reduction from the Short Integer Solution problem to the Learning with Errors problem introduced by Regev. It has recently been pointed out by Chen, Liu and Zhandry that this reduction can be made more powerful by replacing the learning with errors problem with a quantum equivalent, where the errors are given in quantum superposition. In the context of codes, this can be adapted to a reduction from finding short codewords to a quantum decoding problem for random linear codes.

We therefore consider in this paper the quantum decoding problem, where we are given a superposition of noisy versions of a codeword and we want to recover the corresponding codeword. When we measure the superposition, we get back the usual classical decoding problem for which the best known algorithms are in the constant rate and error-rate regime exponential in the codelength. However, we will show here that when the noise rate is small enough, then the quantum decoding problem can be solved in quantum polynomial time. Moreover, we also show that the problem can in principle be solved quantumly (albeit not efficiently) for noise rates for which the associated classical decoding problem cannot be solved at all for information theoretic reasons.

We then revisit Regev's reduction in the context of codes. We show that using our algorithms for the quantum decoding problem in Regev's reduction matches the best known quantum algorithms for the short codeword problem. This shows in some sense the tightness of Regev's reduction when considering the quantum decoding problem and also paves the way for new quantum algorithms for the short codeword problem.

Contents

1 Introduction

1.1 General context

Error correcting codes which appeared first as the fundamental tool to transmit information reliably through a noisy channel [Sha48] have found their way outside this kind of applications, such as for instance in average case complexity [Lev87], or when locally testable codes were found to be the combinatorial core for probabilistically checkable proofs (PCP) [Din07]. Another important application domain for error correction is cryptography with Shamir's secret sharing scheme [Sha79], authentication protocols [Ste93], pseudorandom generators [FS96], signature schemes [Ste93], or public-key encryption schemes [McE78, Ale11, MTSB12]. Contrarily to the applications in reliable communication, data storage, or application in complexity theory where finding suitable families of structured codes is the problem that has to be addressed, many of these applications in cryptography deal with *random linear* codes, and more precisely take advantage of the hardness of decoding a generic linear code.

The decoding problem corresponds to decoding the k-dimensional vector space $\mathscr{C}$ (*i.e.*, the code) generated by the rows of a randomly generated $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ (which is called a *generating matrix* of the code) :

$$\mathscr{C} \stackrel{\triangle}{=} \left\{ \boldsymbol{u}\mathbf{G} \colon \boldsymbol{u} \in \mathbb{F}_q^k \right\}. \tag{1}$$

Here $\mathbb{F}_q$ denotes the finite field with q elements. In the decoding problem, we are given the noisy codeword $\boldsymbol{c} + \boldsymbol{e}$ where $\boldsymbol{c}$ belongs to $\mathscr{C}$ and we are asked to find the original codeword $\boldsymbol{c}$.

Problem 1 ($\mathrm{DP}(q, n, k, f)$)**.** *The decoding problem with positive integer parameters q, n, k and a probability distribution f on $\mathbb{F}_q^n$ is defined as:*

- *Input:* $(\mathbf{G}, \boldsymbol{c} + \boldsymbol{e})$ *where* $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ *and* $\boldsymbol{u} \in \mathbb{F}_q^k$ *are sampled uniformly at random over their domain - which generates a random codeword* $\boldsymbol{c} = \boldsymbol{u}\mathbf{G}$ *- and* $\boldsymbol{e}$ *is sampled from the distribution* f*.*
- *Goal: from* $(\mathbf{G}, \boldsymbol{c} + \boldsymbol{e})$*, find* $\boldsymbol{c}$*.*

This problem for random codes has been studied for a long time and despite many efforts on this issue, the best algorithms are exponential in the codelength n for natural noise distributions f in the regime where k is linear in n and the rate $R \stackrel{\triangle}{=} \frac{k}{n}$ bounded away from 0 and 1 [Pra62, Ste88, Dum89, MMT11, BJMM12, MO15, CDMT22].

The most common noise distribution studied in this context is the uniform distribution over the errors of fixed Hamming weight t, but there are also other distributions, like in the binary case ($q = 2$) the i.i.d Bernoulli distribution model which is frequently found in the Learning Parity with Noise problem (LPN) [GGR98]. When the number of samples of the LPN problem is fixed, this is exactly the decoding problem defined above where n is equal to the number of available LPN samples. When the number of samples in LPN is unlimited, this can be viewed as a decoding problem where we might add on the fly as many columns in $\mathbf{G}$ as we need (and as many corresponding positions in $\boldsymbol{u}\mathbf{G} + \boldsymbol{e}$). The LWE problem in its standard form [Reg05] is a slight variation on the input alphabet, it is $\mathbb{Z}_q$ rather than the finite field $\mathbb{F}_q$ and as in LPN, the number of samples is often assumed to be unlimited. The noise distribution is frequently the discrete Gaussian distribution in this case.

The fact that in LPN, n can grow unlimited with a fixed value of k and a fixed noise distribution can only make the problem simpler than the decoding problem. Interestingly enough, there are now algorithms solving the LPN problem like the Blum-Kalai-Wasserman algorithm [BKW03] which solve the problem with only subexponential complexity of the form $2^{O\left(\frac{k}{\log k}\right)}$ whereas no algorithm with such a complexity is known for $n = O(k)$ (all known algorithms have exponential

complexity in this case). Note that as soon as $n = \Omega\left(k^{1+\varepsilon}\right)$ for any absolute constant $\varepsilon > 0$, the best known algorithm [Lyu05] is somewhat in between, namely $2^{O\left(\frac{k}{\log\log k}\right)}$ and consists in building many new LPN samples from the original pool of samples. In terms of the decoding problem given above, this consists in adding artificially new columns to the generator matrix $\mathbf{G}$ given above by summing a small number of columns of $\mathbf{G}$ (together with the relevant positions of $\boldsymbol{u}\mathbf{G} + \boldsymbol{e}$) to artificially enlarge the value of n and then solve the new decoding problem for this larger matrix. In our work, we will only be interested in the linear regime setting *i.e.* $k = \Theta(n)$.

It should be added here that the LWE problem has proved much more versatile than LPN for building cryptographic primitives. Indeed, it does not only allow to build cryptosystems from it [Reg05], but also allows to obtain advanced cryptographic functionalities such as fully homomorphic encryption [BV11] or attribute-based encryption [GVW13] for instance. It should also be mentioned that three out of the four signature schemes, public key encryption schemes or key establishment protocols supposed to resist to a quantum computer which were selected by the NIST for standardization are based on the hardness of this problem (see `https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022`).

While the security of many code-based cryptosystems relies on the hardness of the decoding problem, it can also be based on finding a "short" codeword (as in [MTSB12] or in [AHI+17, BLVW19, YZW+19] to build collision resistant hash functions), a problem which is stated as follows.

Problem 2 (SCP(q, n, k, w))**.** *The short codeword problem with parameters $q, n, k, w \in \mathbb{N}$ is defined as:*

- *Given:* $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ *which is sampled uniformly at random,*
- *Find:* $\boldsymbol{c} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$ *such that* $\mathbf{H}\boldsymbol{c}^\intercal = \mathbf{0}$ *and the weight* $|\boldsymbol{c}|$ *of* $\boldsymbol{c}$ *satisfies* $|\boldsymbol{c}| \leq w$*.*

Here we are looking for a non-zero codeword $\boldsymbol{c}$ of weight $\leq w$ in the k-dimensional code $\mathscr{C}$ defined by the so-called parity-check matrix $\mathbf{H}$, namely[1] :

$$\mathscr{C} \stackrel{\triangle}{=} \left\{\boldsymbol{c} \in \mathbb{F}_q^n \colon \mathbf{H}\boldsymbol{c}^\intercal = \vec{0}\right\}.$$

The weight function which is generally used here is the Hamming weight, *i.e.* for a vector $\boldsymbol{x} = (x_1, \cdots, x_n) \in \mathbb{F}_q^n$, its Hamming weight is defined as

$$|\boldsymbol{x}| \stackrel{\triangle}{=} \#\{i \in [\![1, n]\!] : x_i \neq 0\}.$$

We will only deal with this weight here. The lattice version of this problem is called the Short Integer Solution (SIS) problem. It consists in replacing the finite field $\mathbb{F}_q$ by $\mathbb{Z}_q$ and using as weight function the euclidean weight $\sqrt{\sum_{i=1} x_i^2}$ (and by representing the elements in $\mathbb{Z}_q$ as $\{-\lfloor (q-1)/2 \rfloor, \cdots, 0, \cdots, \lceil (q-1)/2 \rceil\}$). It was introduced in the seminal work [Ajt96] and used there to build a family of one-way functions based on the difficulty of this problem. What made this problem so attractive is that it was shown there to be as hard on average as a worst case short lattice vector problem.

Decoding and looking for short codewords are problems that have been conjectured to be extremely close. They have been studied for a long time, and the best algorithms for solving these two problems are the same, namely Information Set Decoding algorithms [Pra62, Ste88, Dum89, MMT11, BJMM12, MO15, BM17]. A reduction from decoding to the problem of finding short

[1]The short codeword problem is usually defined by picking a random parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ and not a random generating matrix $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ but the differences are minor (see for example [Deb23]) and one could also define this problem via the generating matrix of a code as we did for the decoding problem.

codewords is known but in an LPN context [AHI+17, BLVW19, YZW+19, DR22]. However, until recently and even in an LPN context, no reduction was known in the other direction before [DRT23] which gave a quantum reduction from SCP to DP which followed the path of the breakthrough result of [Reg05] which reduced the problem of sampling short lattice vectors to LWE. Note that the reduction [Reg05] was not classical but quantum. Later on, it was shown in [SSTX09] that the quantum reduction technique of Regev allows to reduce quantumly SIS to LWE, and this kind of reduction also applies to structured versions of these problems, namely Ideal-SIS can be reduced to Ideal-LWE.

There is a fundamental difficulty of reducing the search of low weight codewords to decoding a linear code which is due to the fact that the nature of these two problems is very different. Decoding concentrates on a region of parameters where there is typically just one solution, whereas finding low weight codewords concentrates on a region of parameters where there are many solutions (and typically an exponential number of solutions). This makes these problems inherently very different. This was also the case for the reduction of SIS to LWE and the fact that we can have a reduction from one to another by looking for quantum reductions instead of classical reductions was really a breakthrough at that time.

It is also worthwhile to notice that all these problems, DP, LPN, LWE, SCP, SIS are all widely believed to be hard also for a quantum computer. The best quantum algorithms for solving these problems have not changed much the picture, the complexity exponent gets essentially only reduced by a constant factor when compared to the best classical algorithms achieving this task, see for instance [Ber10, BJLM13, KT17, LMvdP15, Laa16, CL21]. Indeed, as explained above, most public-key cryptosystems and digital signature schemes that are being standardized right now by the NIST are based on the presumed hardness of LWE, and there are also alternate fourth round finalists of the competition [ABC+22, AAB+22b, AAB+22a] which are based on the hardness of binary DP.

1.2 Regev's quantum reduction and follow-up work

Regev's quantum reduction[Reg05] is at the core of complexity reductions for these problems, which with [Ajt96] essentially started lattice-based cryptography. His approach when rephrased in the coding context is based on the following observation. Suppose that we were able to construct a quantum superposition $\sqrt{\frac{1}{Z}}\sum_{\boldsymbol{c}\in\mathcal{C}}\sum_{\boldsymbol{e}\in\mathbb{F}_q^n}\sqrt{f(e)}|\boldsymbol{c}+\boldsymbol{e}\rangle$ of noisy codewords of a code $\mathcal{C}$ of dimension k over $\mathbb{F}_q$, for a normalization factor Z. If we would apply the quantum Fourier transform on such a state, then because of the periodicity property of such a state we would get a superposition concentrating solely on the codewords of the dual $\mathcal{C}^\perp$ of $\mathcal{C}$, that is $\frac{1}{\sqrt{Z}}\sum_{\boldsymbol{c}^\perp\in\mathcal{C}^\perp}\sqrt{\widehat{f}(\boldsymbol{c}^\perp)}|\boldsymbol{c}^\perp\rangle$. Here $\widehat{f}$ is the (classical) Fourier transform of f that we will properly define in the technical part of the paper. Recall that the dual code is defined as

Definition 1 (dual code)**.** *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$, i.e. a k-dimensional subspace of $\mathbb{F}_q^n$ for some k and n. The dual code $\mathcal{C}^\perp$ is an $(n-k)$ dimensional subspace of $\mathbb{F}_q^n$ defined by*

$$\mathcal{C}^\perp \stackrel{\triangle}{=} \{\boldsymbol{d}\in\mathbb{F}_q^n : \boldsymbol{d}\cdot\boldsymbol{c}=0,\ \forall \boldsymbol{c}\in\mathcal{C}\},$$

where $\boldsymbol{x}\cdot\boldsymbol{y}=\sum_i x_i y_i$ stands for the inner product between the vectors $\boldsymbol{x}$ and $\boldsymbol{y}$.

Now, we can expect that if f concentrates on fairly small weights, then $\widehat{f}$ would also concentrate on rather small weights and therefore we would have a way of sampling low weight (dual) codewords and solve SCP for the dual code. The point is now that $\sqrt{\frac{1}{Z}}\sum_{\boldsymbol{c}\in\mathcal{C}}\sum_{\boldsymbol{e}\in\mathbb{F}_q^n}\sqrt{f(e)}|\boldsymbol{c}+\boldsymbol{e}\rangle$ could be obtained by solving the DP problem on states that are easy to construct. This is the main idea of Regev's reduction. More precisely, the whole algorithm works as follows

Step 1. Creation of the tensor product of a uniform superposition of codewords and a quantum superposition of noise

$$|\phi_1\rangle = \sqrt{\frac{1}{q^k}} \sum_{\boldsymbol{c}\in\mathcal{C}} |\boldsymbol{c}\rangle \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} \sqrt{f(e)}|\boldsymbol{e}\rangle.$$

Step 2. Entangling the codeword with the noise by adding the first register to the second one and then swapping the two registers

$$|\phi_2\rangle = \sqrt{\frac{1}{q^k}} \sum_{\boldsymbol{c}\in\mathcal{C}} \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} \sqrt{f(e)}|\boldsymbol{c}+\boldsymbol{e}\rangle|\boldsymbol{c}\rangle.$$

Step 3. Disentangling the two registers by decoding $\boldsymbol{c}+\boldsymbol{e}$ and therefore finding $\boldsymbol{c}$ which allows to erase the second register

$$|\phi_2\rangle = \sqrt{\frac{1}{Z}} \sum_{\boldsymbol{c}\in\mathcal{C}} \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} \sqrt{f(e)}|\boldsymbol{c}+\boldsymbol{e}\rangle|\boldsymbol{0}\rangle.$$

(The different normalizing factor Z arises when the above decoding procedure is imperfect and we condition on measuring $\boldsymbol{0}$ in the last register.)

Step 4. Applying the quantum Fourier transform on the first register and get

$$\frac{1}{\sqrt{Z}} \sum_{\boldsymbol{d}\in\mathcal{C}^\perp} \sqrt{\widehat{f}(\boldsymbol{d})}|\boldsymbol{d}\rangle|\boldsymbol{0}\rangle$$

Step 5. Measure the first register and get some $\boldsymbol{d}$ in $\mathcal{C}^\perp$.

This approach is at the heart of the quantum reductions obtained in [Reg05, SSTX09, DRT23]. It is also a crucial ingredient in the paper [YZ22] proving verifiable quantum advantage by constructing - among other things - one-way functions that are even collision resistant against classical adversaries but are easily invertible quantumly. In [Reg05, SSTX09, DRT23], the crucial erasing/disentangling step is performed with the help of a *classical* decoding algorithm. Indeed any (classical or quantum) algorithm that can recover $\boldsymbol{c}$ from $\boldsymbol{c}+\boldsymbol{e}$ can be applied coherently to erase the last register in step 3[2] .

A key insight observed in [CLZ22] is that it is actually enough to recover $|\boldsymbol{c}\rangle$ from the state $\sum_{\boldsymbol{e}\in\mathbb{F}_q^n} \sqrt{f(\boldsymbol{e})}|\boldsymbol{c}+\boldsymbol{e}\rangle$ so we are given a superposition of all the noisy codewords $\boldsymbol{c}+\boldsymbol{e}$ and not a fixed one. This means we have to solve the following problem

Problem 3 (QDP(q,n,k,f))**.** *The quantum decoding problem with positive integer parameters q,n,k and a probability distribution f on $\mathbb{F}_q^n$ is defined as:*

- *Input: Take $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ and $\boldsymbol{u} \in \mathbb{F}_q^k$ sampled uniformly at random over their domain. Let $\boldsymbol{c} = \boldsymbol{u}\mathbf{G}$ and $|\psi_{\boldsymbol{c}}\rangle \stackrel{\triangle}{=} \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} \sqrt{f(e)}|\boldsymbol{c}+\boldsymbol{e}\rangle$. The (quantum) input to this problem is $(\mathbf{G}, |\psi_{\boldsymbol{c}}\rangle)$.*
- *Goal: given $(\mathbf{G}, |\psi_{\boldsymbol{c}}\rangle)$, find $\boldsymbol{c}$.*

[2]Indeed, having such an algorithm means we can construct the unitary $U : |\boldsymbol{c}+\boldsymbol{e}\rangle|0\rangle \to |\boldsymbol{c}+\boldsymbol{e}\rangle|\boldsymbol{c}\rangle$. Applying the inverse of this unitary will give the erasure operation.

It's not clear a priori whether this is helpful or not. If one measures the state $|\psi_{\boldsymbol{c}}\rangle$ then one recovers a noisy codeword and we are back to the classical decoding problem.

However, having improvements by directly solving the (LWE variant of the) above problem has been proposed in [CLZ22] where a polynomial time quantum algorithm based on Regev's approach solving SIS is proposed for the l_∞ norm (and not the euclidean norm as is standard there) for extremely high rate codes. Here the decoding problem is obtained by measuring the qudits in an appropriate basis allowing to rule out certain values for the code-symbols, and then they use the Arora-Ge algorithm [AG11] for recovering completely the codeword by solving an algebraic system which for the parameters that are considered there, is of polynomial complexity. Despite the fact that the parameters of the SIS problem are highly degenerate, no efficient classical algorithm performing this task is known. This paper puts forward the S-LWE and the C-LWE problems. Informally the first problem is the one we solve in Step 3 above and the second one is just to create directly the uniform superposition of noisy codewords obtained at Step 3.

1.3 Contributions

Our work has 2 starting points. First, the quantum reduction of [DRT23] between the short codeword problem and the decoding problem in the regime relevant for code-based cryptography *i.e.* a constant code rate $\frac{k}{n}$ and constant error rate. Then, the key insight of [CLZ22] that one requires to solve the quantum decoding problem in the above reduction which can make it more efficient. Instead on focusing too much on the reduction, our aim is first to study here the quantum decoding problem for its own sake. Indeed, the problem is already interesting as a quantum generalization of the decoding problem and the fact it is used in the above reduction creates strong motivation for studying it.

In this work, we focus only on the Bernoulli noise of parameter p. This means we consider the error function

$$f(\boldsymbol{e}) = (1-p)^{n-|\boldsymbol{e}|}\left(\frac{p}{q-1}\right)^{|\boldsymbol{e}|}.$$

which in turn means that for any $\boldsymbol{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$, we can rewrite

$$|\psi_{\boldsymbol{c}}\rangle \stackrel{\triangle}{=} \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} \sqrt{f(\boldsymbol{e})}|\boldsymbol{c}+\boldsymbol{e}\rangle = \bigotimes_{i=1}^{n}\left(\sqrt{1-p}|c_i\rangle + \sum_{\alpha\in\mathbb{F}_q^*}\sqrt{\frac{p}{q-1}}|c_i+\alpha\rangle\right).$$

For this Bernoulli noise with parameter p, the associated quantum decoding problem is written $\mathrm{QDP}(q,n,k,p)$. We show that indeed, the complexity of the quantum decoding problem significantly differs from its classical counterpart. Our contributions can be summarized as

A polynomial time algorithm for QDP **when the noise is low enough (but still of constant rate).** We will show that the quantum problem QDP defined here is probably much easier than its classical counterpart DP. Indeed, for fixed rate $R \stackrel{\triangle}{=} \frac{k}{n}$ only exponential-time algorithms are known for DP for natural noise models, for instance the Bernoulli i.i.d model where $q = 2$, $\Pr(e_i = 1) = p$ for which all algorithms solving it are exponential for p in $(0, 1)$. This is not the case for the associated QDP problem, where we will show that by using Unambiguous State Discrimination (USD) together with linear algebra we can solve the problem in *polynomial time* up to some limiting value of p which is strictly between 0 and 1 for a fixed rate R. We generalize this result for any q by generalizing existing bounds on USD and also present an algorithm for partial binary unambiguous state discrimination which could be of independent interest.

A problem which can be solved above capacity. There is an information theoretic limit for *any algorithm* solving classically or quantumly the classical decoding problem DP. When the rate exceeds the capacity of the noisy channel specified by f (and if this is an i.i.d. noise) then above the capacity of the noisy channel it is just impossible to solve with say polynomial error probability the decoding problem just because there are exponentially many candidates at least as likely as the right candidate. The problem becomes intractable just because of this reason. For instance in the Bernoulli model above, the rate $R = k/n$ has to be smaller than $1 - h(p)$ where $h(x)$ is the binary entropy function, $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. Somewhat surprisingly, it turns out that we can go above the Shannon capacity for the QDP problem. Moreover, with the help of the Pretty Good Measurement (PGM) we can fully characterize the noise range where the problem is tractable.

Applying QDP **solvers in Regev's reduction.** Both algorithms (the one using USD and the other one based on PGM) can be applied to sample small weight dual codewords and solve SCP. By applying the quantum reduction steps above, together with our polynomial time solving QDP we obtain non-zero codewords of relative weight $\omega \stackrel{\triangle}{=} w/n$ satisfying $\omega \leq \frac{(q-1)(1-R)}{q}$. Interestingly enough, this is precisely the smallest weight that can be reached by the best known polynomial time algorithm, namely a minor variant of the Prange algorithm [Pra62]. On the other hand, we will show that there is no hope to have a proper general reduction of SCP to QDP, by providing examples showing that we can solve QDP in a certain noise regime and still get nothing useful for SCP after using it in Regev's reduction. However, we can adapt the PGM to still have some small codewords up to the tractability bound. Our examples really show that we have to analyze properly the state that we have at Step 3. of the reduction on a case by case basis.

We now perform a detailed description of our contributions.

1.3.1 Using USD as a means of improving quantum algorithms for QDP

The binary setting. Our first idea, which extends naturally the work of [CLZ22] is to apply USD for the quantum decoding problem. We first consider the binary setting, *i.e.* $q = 2$. This means the states $|\Psi_{\boldsymbol{c}}\rangle = \sum_{\boldsymbol{e}\in\mathbb{F}_2^n} \sqrt{f(\boldsymbol{e})}|\boldsymbol{c}+\boldsymbol{e}\rangle$ for which we want to recover $\boldsymbol{c}$ are of the form

$$|\Psi_{\boldsymbol{c}}\rangle = \bigotimes_{i=1}^{n} \sqrt{1-p}|c_i\rangle + \sqrt{p}|1-c_i\rangle.$$

Consider a fixed coordinate i for which we have the state $\sqrt{1-p}|c_i\rangle + \sqrt{p}|1-c_i\rangle$ which we call $|\psi^p_{c_i}\rangle$. By measuring this state in the computational basis we get c_i wp. $1-p$ and $1-c_i$ wp. p. This measurement is actually the measurement that distinguishes best $|\psi_0\rangle$ and $|\psi_1\rangle$.

Another measurement of interest is unambiguous state discrimination. Here, the goal is not to distinguish optimally between $|\psi^p_0\rangle$ and $|\psi^p_1\rangle$ but to make sure that our guess is always correct but allowing for some abort. In this setting, we have the following

Proposition 1 (Unambiguous state discrimination)**.** *For any $p \in [0,1]$, there exists a quantum measurement that on input $|\psi^p_{c_i}\rangle$ outputs c_i wp. $1 - 2\sqrt{p(1-p)}$ and outputs $\perp$ otherwise.*

Using this measurement, the probability of guessing correctly c_i is always smaller than $1-p$ for $p \leq \frac{1}{2}$. However, we know exactly when we succeed in guessing c_i. This will be extremely useful for decoding. Indeed, if we recover k values of c_i we recover the complete codeword $\boldsymbol{c}$ with good probability by linear algebra by using the fact that $\boldsymbol{c} = \boldsymbol{m}\mathbf{G}$ with $\mathbf{G} \in \mathbb{F}_2^{k\times n}$. This will lead to

Theorem 1. *Let $R \in [0,1]$. For any $p < \left(\frac{R}{2}\right)^{\perp}$, there exists a quantum algorithm that solves $\mathrm{QDP}(2, n, \lfloor Rn \rfloor, p)$ wp. $1 - 2^{-\Omega(n)}$ in time $\mathsf{poly}(n)$. Here for a real number $x \in [0,1]$, $x^{\perp}$ stands for $\frac{1-2\sqrt{x(1-x)}}{2}$.*

Interpretation as changing the noise channel and partial unambiguous state discrimination. A nice interpretation of the above algorithm is that when the error is in quantum superposition, one can use quantum measurements to change the noise model. For example in the above, if we are given $|\psi_{c_i}\rangle = \sqrt{1-p}|c_i\rangle + \sqrt{p}|1-c_i\rangle$ then

- One can measure in the computational basis to obtain c_i that has been flipped wp. p.
- One can use unambiguous state discrimination in which case c_i has been erased wp. $2\sqrt{p(1-p)}$.

What we show in Theorem 1 is that the second strategy is actually much more powerful for recovering the codeword $\boldsymbol{c}$. A natural question to ask is whether this can further be generalized to other measurements.

In this work, we actually generalize Unambiguous State Discrimination as follows: given $|\psi_{c_i}\rangle$, the measurement will sometimes output $\perp$ but it can also fail with some small probability. We prove the following

Proposition 2 (Partial Unambiguous State Discrimination)**.** *Let $p, s \in [0, \frac{1}{2})$ with $s \leq p$ and let $u = \frac{p^{\perp}}{s^{\perp}}$. There exists a quantum measurement that when applied to $|\psi_{c_i}\rangle = \sqrt{1-p}|c_i\rangle + \sqrt{p}|1-c_i\rangle$ outputs c_i wp. $u(1-s)$, $(1-c_i)$ wp. us and $\perp$ wp. $1-u$.*

Notice that this generalizes both the standard measurement (by taking $s = p$) and unambiguous state discrimination (by taking $s = 0$ which gives $u = 2p^{\perp}$). This seems a very natural way of generalizing Unambiguous State Discrimination but is not something we have found in the literature and could be of independent interest. We can use this measurement not to provide new polynomial time algorithm but rather to give a reduction between different Quantum Decoding problems, which we detail in the full text.

The general setting. The unambiguous state discrimination approach works in the q-ary setting as well. A difficulty here is that optimal unambiguous state discrimination is not known in general for more than 2 states, but in certain situations where we have a symmetric set of states [CB98] we know how to perform optimal USD. This would apply in our case case where q is prime. We have generalized sligthly the approach of [CB98] to be able to apply it to any finite field size q. We get finally a result very similar to the binary case

Theorem 2. *Let $R \in [0,1]$. For any $p < \left(\frac{(q-1)R}{q}\right)^{\perp}$, there exists a quantum algorithm that solves $\mathrm{QDP}(q, n, \lfloor Rn \rfloor, p)$ wp. $1 - 2^{-\Omega(n)}$ in time $\mathsf{poly}(n)$.*

Here we have used a notation which "generalizes" the $p^{\perp}$ notation used in the binary setting.

Notation 1. *For a real number $x \in [0,1]$, $x^{\perp}$ stands for $\frac{\left(\sqrt{(1-x)(q-1)} - \sqrt{x}\right)^2}{q}$.*

This quantity depends on q which will be clear from the context. Note that when $q = 2$ we get $\frac{1-2\sqrt{x(1-x)}}{2}$ which coincides with the one given in the binary case.

1.3.2 Determining exactly the tractability of the quantum decoding problem

We are now interested in the tractability of $\mathrm{QDP}(q,n,k,p)$ meaning when is it possible from an information theoretic perspective to solve this problem. In order to study this problem, a fundamental quantity is $\delta_{\min}(R)$ defined below, sometimes referred to as the Gilbert-Varshamov distance

Notation 2. *Let $R \in [0,1]$. We define $\delta_{\min}(R) \stackrel{\triangle}{=} h_q^{-1}(1-R)$, where $h_q(x) \stackrel{\triangle}{=} -(1-x)\log_q(1-x) - x\log_q\left(\frac{x}{q-1}\right)$. h_q is a bijection from $x \in \left[0, \frac{q-1}{q}\right]$ to $[0,1]$ and we define $h_q^{-1} : [0,1] \to \left[0, \frac{q-1}{q}\right]$ st. $h_q^{-1}(h_q(x)) = x$ for $x \in \left[0, \frac{q-1}{q}\right]$.*

For the classical setting, it is well understood that $\mathrm{DP}(q,n,k,p)$ is not tractable when $p > \delta_{\min}(\frac{k}{n})$, meaning that even an unbounded algorithm will solve the problem wp. $o(1)$.

We would like now to understand what happens in the quantum setting. Techniques based on (partial) unambiguous state discrimination will not work in the regime $p > \delta_{\min}(R)$. Since we are only interested in the tractability of the problem, we can consider optimal quantum algorithms for discriminating between the states $|\Psi_{\boldsymbol{c}}\rangle = \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} \sqrt{f(\boldsymbol{e})}|\boldsymbol{c}+\boldsymbol{e}\rangle$ where f accounts for the Bernoulli noise of parameter p. This problem can be addressed by using the *Pretty Good Measurement* (PGM) which has turned out to be a very useful tool in quantum information. If we define $\mathrm{P}_{\mathrm{PGM}}$ as the probability that the pretty good measurement succeeds in solving our problem and define $\mathrm{P}_{\mathrm{OPT}}$ as the maximal probability that any measurement succeeds, we have [BK02, Mon06]

$$\mathrm{P}_{\mathrm{OPT}}^2 \leq \mathrm{P}_{\mathrm{PGM}} \leq \mathrm{P}_{\mathrm{OPT}}.$$

This means that if the problem is tractable then $\mathrm{P}_{\mathrm{OPT}} = \Omega(1)$ which implies $\mathrm{P}_{\mathrm{PGM}} = \Omega(1)$. On the other hand, if the problem is intractable then $\mathrm{P}_{\mathrm{OPT}} = o(1)$ which implies $\mathrm{P}_{\mathrm{PGM}} = o(1)$. In conclusion, in order to study the tractability of the quantum decoding problem, it is enough to look at the PGM associated with the problem of distinguishing the states $\{|\Psi_{\boldsymbol{c}}\rangle\}$. We show the following

Theorem 3. *Let $R \in (0,1)$.*

- *For $p < (\delta_{\min}(1-R))^{\perp}$, $\mathrm{QDP}(q,n,\lfloor Rn \rfloor,p)$ can be solved using the PGM wp. $P_{PGM} = \Omega(1)$ hence the problem is tractable.*
- *For $p > (\delta_{\min}(1-R))^{\perp}$, $\mathrm{QDP}(q,n,\lfloor Rn \rfloor,p)$, the probability that the PGM solves this problem is $P_{PGM} = o(1)$ hence the problem is intractable.*

The pretty good measurement associated to this distinguishing problem actually has a a lot of structure. It is actually a projective measurement on an orthonormal basis corresponding which can be seen as a Fourier basis involving the shifted dual codes of the code $\mathcal{C}$ we are working on.

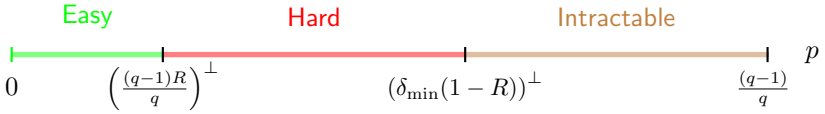
Comparing the complexity of the decoding problem and the quantum decoding problem With this full characterization, we compare the hardness, and tractability of the classical and quantum decoding problems. For $p = 0$, we have of course a polynomial time algorithm to solve $\mathrm{DP}(q,n,\lfloor Rn \rfloor,0)$. For $0 < p \leq \delta_{\min}(R)$, the problem is tractable and the best known classical or quantum algorithms run in time $2^{\Omega(n)}$. For $p > \delta_{\min}(R)$, we know the problem is intractable. In the quantum setting, we obtain a very different picture. A comparison of these results is presented in Figures 1 and 2 where we use the following terminology

- Easy: there exists an algorithm that runs in time $\mathsf{poly}(n)$.
- Hard: the best known algorithm runs in time $2^{\Omega(n)}$, but there could potentially be more efficient algorithms.

- Intractable: we know that any (even unbounded) algorithm can solve the problem wp. at most $o(1)$.

Figure 1: Hardness and tractability of the decoding problem $\mathrm{DP}(q, n, \lfloor Rn \rfloor, p)$, for any fixed $R \in [0, 1]$, as a function of p.

Figure 2: Hardness and tractability of the quantum decoding problem $\mathrm{QDP}(q, n, \lfloor Rn \rfloor, p)$, for any fixed $R \in [0, 1]$, as a function of p.



This gives a proper characterization of the difficulty of the Quantum Decoding Problem. In our next contribution, we will apply them in Regev's quantum reduction in order to derive some results for the short codeword problem. As we will show, the results from Figure 2 will match exactly our knowledge for the short codeword problem.

1.3.3 Using our algorithms in Regev's reduction

We are now interested in solving the short codeword problem using Regev's reduction and the algorithms we described in the previous section. The known hardness of the short codeword problem is summarized in the figure below

Figure 3: Hardness and tractability of the short codeword problem $\mathrm{SCP}(q, n, \lfloor Rn \rfloor, p)$ for a fixed $R \in (0, 1)$, as a function of p.

For our coding context, the only known reduction is the following

Proposition 3 ([DRT23], informal)**.** *Fix integers $n, q \geq 2$ as well as parameters $R, p \in (0, 1)$ st. $p \leq \delta_{\min}(R)$. From any quantum algorithm that solves $DP(q, n, \lceil (1-R)n \rceil, p)$ with high probability, there exists a quantum algorithm that solves $SCP(q, n, \lfloor Rn \rfloor, p^{\perp})$ with high probability where recall that $p^{\perp} = \frac{\left(\sqrt{(1-p)(q-1)} - \sqrt{p}\right)^2}{q}$.*

How can we characterize the efficiency of this reduction? Let us consider the best algorithms for $\mathrm{DP}(q, n, \lceil (1-R)n \rceil, p^{\perp})$ and see what algorithms does it give for $\mathrm{SCP}(q, n, \lfloor Rn \rfloor, p)$. We obtain the following result, summarized in Figure 4. We can see that the obtained algorithm for the short decoding problem is significantly worse[3] than best known algorithm for this problem (see Figure 3). But in the light of our previous results, this is understandable, Regev's reduction actually requires

[3]One can check that we always have $(\delta \min(1-R))^{\perp} \geq \delta_{\min}(R)$.

to solve the quantum decoding problem and we just showed that it is much simpler than the decoding problem. If we could directly use the above proposition with our algorithms, we would obtain the following results, summarized in Figure 5.

Figure 4: On the top, best known (classical or quantum) algorithms for $\mathrm{DP}(q, n, \lceil (1-R)n \rceil, p)$. On the bottom, complexity of a quantum algorithm for $\mathrm{SCP}(q, n, \lceil Rn \rceil, p)$ that uses the best algorithm for $\mathrm{DP}(q, n, \lceil (1-R)n \rceil, p)$ and then uses Proposition 3

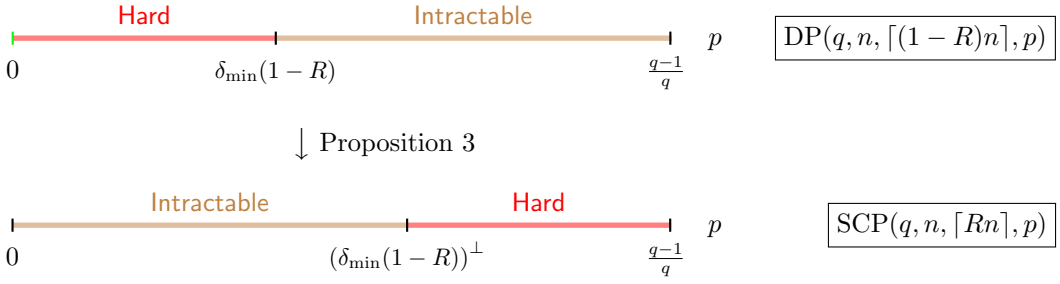
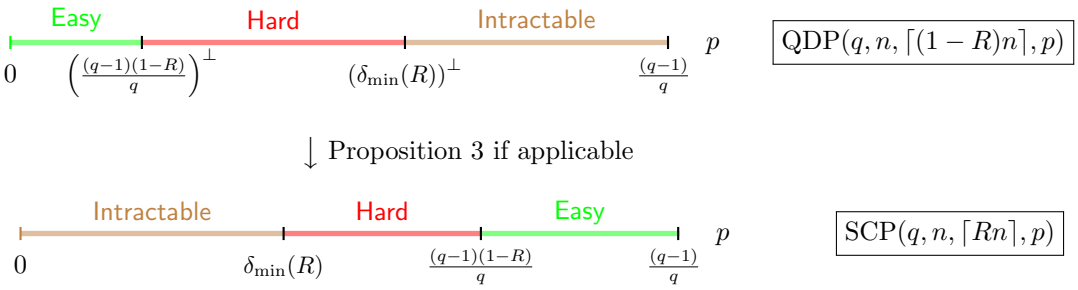


Figure 5: On the top, our quantum algorithms for $\mathrm{QDP}(q, n, \lceil (1-R)n \rceil, p)$. On the bottom, complexity of a quantum algorithm for $\mathrm{SCP}(q, n, \lceil Rn \rceil, p)$ that would use our algorithms $\mathrm{QDP}(q, n, \lceil (1-R)n \rceil, p)$ and then Proposition 3 when applicable



Here, if we could apply Proposition 3 with our algorithms, we would recover exactly the same complexities as the best known algorithms for SCP[4]. However, it's not clear whether this is the case. What we do is that for each of our algorithms, we try to perform Regev's reduction and see what we obtain. We show the following:

- If we take our polynomial time algorithms involving unambiguous state discrimination for the quantum decoding problem in Regev's reduction, we can find in quantum polynomial time small codewords down to Prange's bound, *i.e.* down to $\frac{(1-R)(q-1)}{q}$ (the Easy zone in Figure 3). The bound $\left(\frac{(1-q)(1-R)}{q}\right)^{\perp}$ comes from bounds on quantum unambiguous state discrimination and it is quite remarkable that after the quantum reduction, it corresponds exactly to Prange's bound where the short codeword problem is easy.
- If we use our algorithm involving the Pretty Good Measurement in Regev's reduction, the following happens:

[4]We say we recover the same complexities only in the sense that we recover the areas which are easy,hard,intractable. We're not claiming that within these areas, the running times are exactly the same.

1. If we apply the PGM directly, we will most often be in regimes where we measure $\mathbf{0}$ in the final step so we will not be able to solve the Short Codeword problem.
2. We can slightly tweak the PGM so that we can solve the corresponding short codeword problem for all the regimes where it is tractable (the Hard zone in Figure 3).
3. We also show another example where we can slightly tweak the PGM but where the reduction utterly fails, meaning that the state we obtain after Step 4 is $|\perp\rangle$, so measuring will give absolutely no information about a small dual codeword. This shows that there is no hope to perform a generic reduction (*i.e.* a generalization of Proposition 3) between the quantum decoding problem and the short codeword problem with this method.

These results show that, while it is impossible to have a generic reduction from QDP to SCP with this method, it is - at least for our examples - possible to find algorithms for QDP that will give results according to Figure 5, and recover the areas where the problem is easy and where it is tractable. This can be seen as quite a surprise since our bounds on QDP essentially come from information theory and best known bounds on SCP comes from classical coding theory and seem unrelated at first.

2 Preliminaries

2.1 Notations and basic probabilities

Sets, finite field. The finite field with q elements is denoted by $\mathbb{F}_q$. $\mathbb{Z}_q$ denotes the ring of integers modulo q. The cardinality of a finite set $\mathcal{E}$ is denoted by $|\mathcal{E}|$. The set of integers $\{a, a+1, \cdots, b\}$ between the integers a and b is denoted by $[\![a, b]\!]$. For a positive integer n, $[n]$ denotes $[\![1, n]\!]$. $x \leftarrow S$ means that x is sampled uniformly from the set S.

Vector and matrices. For a Hermitian matrix $\mathbf{M}$ we write that $\mathbf{M} \succeq 0$ when $\mathbf{M}$ is positive semi-definite. Vectors are row vectors as is standard in the coding community and $\boldsymbol{x}^\intercal$ denotes the transpose of a vector or a matrix. In particular, vectors will always be denoted by bold small letters and matrices with bold capital letters. For a subset $J \subseteq [n]$ of positions of the vector $\boldsymbol{x} = x_1, \ldots, x_n$, $\boldsymbol{x}_J = (x_j)_{j \in J}$ denotes the vector formed by the entries indexed by J. For a matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ and a subset of columns $J \subseteq [n]$, $\mathbf{G}_J \in \mathbb{F}_q^{k \times |J|}$ denotes the submatrix formed by its columns indexed by J.

Lemma 1 (Hoeffding's inequality)**.** *Let $X_1, \ldots, X_n$ be independent random Bernoulli variables with parameter p. We have*

$$\Pr[\sum_{i=1}^{n} X_i \leq pn - \alpha\sqrt{n}] \leq 2^{-2\alpha^2}.$$

2.2 Random linear codes

2.2.1 Basic properties

For a vector $\boldsymbol{x} = x_1, \ldots, x_n \in \mathbb{F}_q^n$, we define the Hamming weight $|\boldsymbol{x}| = |\{i : x_i \neq 0\}|$. For $q, n, w \in \mathbb{N}^*$ with $q \geq 2$, we define the (Hamming) sphere of radius w as $S_w^{q,n} = \{\boldsymbol{x} \in \mathbb{F}_q^n : |\boldsymbol{x}| = w\}$. A code $\mathcal{C}$ can be specified by a generating matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, in which case $\mathcal{C} = \{\boldsymbol{u}\mathbf{G} : \boldsymbol{u} \in \mathbb{F}_q^k\}$ or via a parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{n \times (n-k)}$, in which case $\mathcal{C} = \{\boldsymbol{y} : \mathbf{H}\boldsymbol{y}^\intercal = \mathbf{0}\}$.

(André: Si ces quantités suivantes ne sont pas utilisées ici, peut-être les mettre directement dans la section correspondante aux propriétés avancées sur les codes aléatoires.)

Definition 2 (q-ary entropy)**.** *We define the q-ary entropy $h_q : [0,1] \to [0,1]$ s.t. $h(x) = -x \log\left(\frac{x}{q-1}\right) - (1-x)\log(1-x)$ if $x \in (0,1)$ and $h_q(0) = h_q(1) = 0$.*

h_q is increasing for $x \in [0, \frac{q-1}{q}]$ and deceasing for $x \in [\frac{q-1}{q}, 1]$. Moreover, $h_q(\frac{q-1}{q}) = 1$.

Definition 3 (Inverse q-ary entropy)**.** *h_q is a bijection from $\left[0, \frac{q-1}{q}\right]$ to $[0,1]$ and we define $h_q^{-1} : [0,1] \to \left[0, \frac{q-1}{q}\right]$ s.t. $h_q^{-1}(h_q(x)) = x$ for $x \in \left[0, \frac{q-1}{q}\right]$.*

Definition 4 (Relative Gilbert-Varshamov distance)**.** *The (relative) Gilbert-Varshamov distance for q-ary codes $\delta_{\min}(R,q)$ corresponding to the rate R is defined as $\delta_{\min}(R,q) = h_q^{-1}(1-R)$.*

Definition 5 (Relative maximum weight)**.** *The (relative) maximum weight for q-ary code $\delta_{\max}(R,q)$ is defined as the unique solution x in $[\frac{q-1}{q}, 1]$ of $h_q(x) = R$ if it exists. If such an x does not exist, we just write $\delta_{\max}(R,q) = \perp$.*

$\delta_{\min}(R,q)$ corresponds to the typical asymptotic relative minimum distance of a random linear code over $\mathbb{F}_q$ of rate R, whereas the second quantity (when it is not $\perp$) is equal to the typical asymptotic relative maximum distance. Generally q will be clear from the context and we will drop the dependency in q and simply write $\delta_{\min}(R)$ and $\delta_{\max}(R)$.

Definition 6 (Inverse of a full rank matrix)**.** *Let $k < n$ and $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ be a matrix of full rank k. We define the pseudo-inverse $\mathbf{G}^{-1} \in \mathbb{F}_q^{n \times k}$ as a matrix satisfying $\forall \boldsymbol{u} \in \mathbb{F}_q^k$, $(\boldsymbol{u}\mathbf{G}) \cdot \mathbf{G}^{-1} = \boldsymbol{u}$.* **[jp: Cette matrice n'est pas unique, j'ai changé "inverse" en "pseudo-inverse" et "the" par "a".]**

Proposition 4. *Let $m \geq k$ and let $G \leftarrow {\mathbb{F}_q}^{k \times m}$. We have*

$$\Pr[\mathrm{rank}(G) = k] \geq 1 - q^{k-m}.$$

Proposition 5. *Let $\boldsymbol{c} = \boldsymbol{s}\mathbf{G}$ for some $\boldsymbol{s} \in \mathbb{F}_q^k$ and $G \in \mathbb{F}_q^{k \times n}$. Let $J \subseteq [n]$ s.t. G_J is of rank k. Then we have $\boldsymbol{c} = \boldsymbol{c}_J \mathbf{G}_J^{-1} \mathbf{G}$.*

Proof. Notice that $\boldsymbol{c}_J = \boldsymbol{s}\mathbf{G}_J$. If $\mathbf{G}_J$ is of full rank k then $\mathbf{G}_J^{-1}$ is well defined and $\boldsymbol{c}_J \mathbf{G}_J^{-1} = \boldsymbol{s}\mathbf{G}_J\mathbf{G}_J^{-1} = \boldsymbol{s}$. From there, we conclude $\boldsymbol{c}_J\mathbf{G}_J^{-1}\mathbf{G} = \boldsymbol{s}\mathbf{G} = \boldsymbol{c}$. □

2.2.2 Classical and quantum decoding problems

Before defining our coding problem, we define the Bernoulli error distributions that we will use.

Definition 7. *For $q \in \mathbb{N}^*$, with $q \geq 2$ and $\omega \in [0,1]$, we define the Bernoulli probability function $b_q : F_q \to \mathbb{R}$ satisfying $b_q(0) = 1 - w$ and $b_q(i) = \frac{w}{q-1}$ for $i \neq 0$.*

Definition 8. *For $q \in \mathbb{N}^*$, with $q \geq 2$ and $\omega \in [0,1]$ we define the distribution $\mathcal{B}(q,\omega)$ sampled as follows: pick x w.p. $b_q(x)$, return x.*

We now define the Bernoulli distribution on vectors on F_q^n where each coordinate is taken according to $\mathcal{B}(q,\omega)$.

Definition 9. *For $q, n \in \mathbb{N}^*$, $\omega \in [0,1]$, with $q \geq 2$ we define the distribution $\mathcal{B}(q,n,\omega)$ sampled as follows: for $i \in \{1,\ldots,n\}$, $x_i \leftarrow \mathcal{B}(q,\omega)$, return $\boldsymbol{x} = x_1,\ldots,x_n$. Notice that sampling from $\mathcal{B}(q,n,\omega)$ is equivalent to the following sampling procedure: pick $\boldsymbol{x}$ w.p. $\left(\frac{\omega}{q-1}\right)^{|\boldsymbol{x}|}(1-\omega)^{n-|\boldsymbol{x}|}$, return $\boldsymbol{x}$.*

What we are interested here is the decoding problem as it arises in cryptography, but we will describe it here by using the langage of information theory. We have a message $\boldsymbol{m} \in F_q^k$ which is encoded via a generating matrix $\mathbf{G} \in F_q^{k \times n}$. The encoded message $\boldsymbol{m}\mathbf{G}$ is sent through a channel and an error $\boldsymbol{e}$ occurs. The receiver gets the message $\boldsymbol{m}\mathbf{G}+\boldsymbol{e}$ and his goal is to recover $\boldsymbol{m}$. Notice that the receiver also knows the generating matrix $\mathbf{G}$ so his goal is, given $\mathbf{G}$ and $\boldsymbol{y} = \boldsymbol{m}\mathbf{G}+\boldsymbol{e}$, to recover $\boldsymbol{m}$.

The way we model the error is that $\boldsymbol{e}$ is sampled from the Bernoulli distribution $\mathcal{B}(q,n,\omega)$ for some chosen ω. Note that there are other choices for the error model that can be of interest that we discuss in the next section. We first define the distribution of input/solution to our decoding problem.

Definition 10. *For $q,n,k \in \mathbb{N}^*$, with $q \geq 2$, for $\omega \in [0,1]$, we define the distribution $\boxed{\mathcal{D}(q,n,k,\omega)}$ sampled as follows: $\mathbf{G} \leftarrow \{0,1\}^{k\times n}$, $\boldsymbol{m} \leftarrow \mathbb{F}_q^k$, $\boldsymbol{c} = \boldsymbol{m}\mathbf{G}$, $\boldsymbol{e} \leftarrow \mathcal{B}(q,n,\omega)$, $\boldsymbol{y} = \boldsymbol{c}+\boldsymbol{e}$, return $(\mathbf{G},\boldsymbol{y},\boldsymbol{c})$.*

We can now define our classical decoding problem

Definition 11. *For $q,n,k \in \mathbb{N}^*$, with $q \geq 2$, for $\omega \in [0,1]$, the decoding problem $\boxed{DP(q,n,k,\omega)}$ is the following. We sample $(\mathbf{G},\boldsymbol{y},\boldsymbol{c}) \leftarrow \mathcal{D}(q,n,k,\omega)$ and the goal is, given only $(\mathbf{G},\boldsymbol{y})$, to recover $\boldsymbol{c}$.*

Another problem of interest is finding short codewords.

Definition 12. *For $q,n,k \in \mathbb{N}$ with $q \geq 2$ and $\omega \in (0,1)$, the short codeword problem $\boxed{SCP(q,n,k,\omega)}$ is the following. We sample $\mathbf{H} \leftarrow \mathbb{F}_q^{n\times(n-k)}$ and the goal is, given $\mathbf{H}$, to find $\boldsymbol{c} \in \mathbb{F}_q^n \backslash \{\mathbf{0}\}$ st. $\mathbf{H}\boldsymbol{c}^\intercal = \mathbf{0}$ and $|\boldsymbol{c}| \leq \omega n$.*

We now consider the quantum decoding problem. Now, instead of choosing a random error $\boldsymbol{e}$ from $\mathcal{B}(q,n,\omega)$ and constructing $\boldsymbol{y} = \boldsymbol{c}+\boldsymbol{e}$, we construct a quantum state that is a superposition of all these noisy codewords. This motivates the following definition for the input/solution distribution.

Definition 13. *For $q,n,k \in \mathbb{N}^*$, with $q \geq 2$ and $\omega \in [0,1]$, we define the distribution $\boxed{\mathcal{D}_{\mathcal{Q}}(q,n,k,\omega)}$ sampled as follows: $\mathbf{G} \leftarrow \{0,1\}^{k\times n}$, $\boldsymbol{m} \leftarrow \mathbb{F}_q^k, \boldsymbol{c} = \boldsymbol{m}\mathbf{G}$, $|\psi_{\boldsymbol{c}}\rangle = \sum_{\boldsymbol{e}\in F_q^n} \sqrt{\omega^{|\boldsymbol{e}|}(1-\omega)^{n-|\boldsymbol{e}|}}|\boldsymbol{c}+\boldsymbol{e}\rangle$, return $(\mathbf{G},|\psi_{\boldsymbol{c}}\rangle,\boldsymbol{c})$.*

From there, we define our quantum decoding problem.

Definition 14. *For $q,n,k \in \mathbb{N}^*$, with $q \geq 2$, for $\omega \in [0,1]$, the decoding problem $\boxed{\mathrm{QDP}(q,n,k,\omega)}$ is the following. We sample $(\mathbf{G},|\psi_{\boldsymbol{c}}\rangle,\boldsymbol{c}) \leftarrow \mathcal{D}_{\mathcal{Q}}(q,n,k,\omega)$ and the goal is, given only $(\mathbf{G},|\psi_{\boldsymbol{c}}\rangle)$, to recover $\boldsymbol{c}$.*

The above definition can be generalized to any probability function $P : \mathbb{F}_q^n \to \mathbb{R}$ by considering the state $|\psi_{\boldsymbol{c}}\rangle = \sum_{\boldsymbol{e}\in F_q^n} \sqrt{P(\boldsymbol{e})}|\boldsymbol{c}+\boldsymbol{e}\rangle$. Moreover, and this is specific to the quantum setting, this can be generalized to any function $f : \mathbb{F}_q^n \to \mathbb{C}$ with $\|f\|_2 = 1$ by considering the state $|\psi_{\boldsymbol{c}}\rangle = \sum_{\boldsymbol{e}\in F_q^n} f(\boldsymbol{e})|\boldsymbol{c}+\boldsymbol{e}\rangle$. This is what motivates the following definitions.

Definition 15. *For $q,n,k \in \mathbb{N}^*$, with $q \geq 2$, for $f : \mathbb{F}_q^n \to \mathbb{C}$ with $\|f\|_2 = 1$, we define the distribution $\boxed{\mathcal{D}_{\mathcal{Q}}(q,n,k,f)}$ sampled as follows: $\mathbf{G} \leftarrow \{0,1\}^{k\times n}$, $\boldsymbol{m} \leftarrow \mathbb{F}_q^k, \boldsymbol{c} = \boldsymbol{m}\mathbf{G}$, $|\psi_{\boldsymbol{c}}\rangle = \sum_{\boldsymbol{e}\in F_q^n} f(\boldsymbol{e})|\boldsymbol{c}+\boldsymbol{e}\rangle$, return $(\mathbf{G},|\psi_{\boldsymbol{c}}\rangle,\boldsymbol{c})$.*

Definition 16. *For $q,n,k \in \mathbb{N}^*$, with $q \geq 2$, for $f : \mathbb{F}_q^n \to \mathbb{C}$ with $\|f\|_2 = 1$, the decoding problem $\boxed{\mathrm{QDP}(q,n,k,f)}$ is the following. We sample $(\mathbf{G},|\psi_{\boldsymbol{c}}\rangle,\boldsymbol{c}) \leftarrow \mathcal{D}_{\mathcal{Q}}(q,n,k,f)$ and the goal is, given only $(\mathbf{G},|\psi_{\boldsymbol{c}}\rangle)$, to recover $\boldsymbol{c}$.*

2.2.3 Punctured codes and Prange's algorithm

We will use in what follows the notion of punctured and shortened code.

Definition 17 (Punctured and shortened code)**.** *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code over $\mathbb{F}_q$ of length n. Let $J \subseteq [n]$ be a subset of code positions. The punctured code $\mathcal{C}_J$ with respect to J is defined as $\mathcal{C}_J = \{\boldsymbol{c}_J : \boldsymbol{c} \in \mathcal{C}\}$. The shortened code C^J with respect to J is defined as $\mathcal{C}^J = \{\boldsymbol{c}_J : \boldsymbol{c} \in \mathcal{C},\ \boldsymbol{c}_{[n]\setminus J} = \mathbf{0}\}$ (i.e. the set of codewords of $\mathcal{C}$ where we keep only the positions in J and which are zero outside J).*

It is readily seen that these two operations commute when taking the dual

Lemma 2. *For any linear code $\mathcal{C}$ and any subset J of positions of this code*

$$\begin{aligned} (\mathcal{C}_J)^\perp &= \left(\mathcal{C}^\perp\right)^J \\ \left(\mathcal{C}^J\right)^\perp &= \left(\mathcal{C}^\perp\right)_J . \end{aligned}$$

A variation of the Prange algorithm. We recall here a result which is essentially folklore in coding theory, namely that there is a probabilistic polynomial time algorithm for finding short codewords in a random linear code of dimension k and length n over $\mathbb{F}_q$ which produces short codewords of weight $\left\lfloor \frac{(q-1)(n-k)}{q} \right\rfloor$. It simply uses linear algebra. For this, consider a parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ of $\mathcal{C}$ and run $\Theta\left(\sqrt{n}\right)$ times the following procedure

1. Choose uniformly at random subset J of k positions of $\mathcal{C}$. Let $\bar{J} = [n] \setminus J$.
2. If $\mathbf{H}_{\bar{J}}$ is not of rank $n-k$, abort and else choose $\boldsymbol{c}$ on J as a random vector of Hamming weight 1.
3. Find the remaining entries of $\boldsymbol{c}$ by solving the linear system
$$\mathbf{H}_{\bar{J}} \boldsymbol{c}_{\bar{J}}{}^\intercal = -\mathbf{H}_J \boldsymbol{c}_J{}^\intercal$$
4. If $|\boldsymbol{c}| = \left\lfloor \frac{(q-1)(n-k)}{q} \right\rfloor$ output $\boldsymbol{c}$.

The rationale behind this algorithm is that the expected weight of such a $\boldsymbol{c}$ is $1 + \frac{(q-1)(n-k)}{q}$ and that it can be proved that it takes the right weight with probability $\Omega\left(\frac{1}{\sqrt{n}}\right)$. Note that all the known (be they classical or quantum) algorithms that produce asymptotically relative weights $\omega < \frac{(1-q)(1-R)}{q}$ where $R = \frac{k}{n}$ is the code rate have exponential complexity.

2.3 Distinguishing quantum states

Proposition 6 (Helstrom's measurement)**.** *Let $|\psi_0\rangle, |\psi_1\rangle$ be 2 quantum pure states s.t. $|\langle\psi_0|\psi_1\rangle| = u$. There exists a quantum projective measurement $\Pi = \{\Pi_0, \Pi_1\}$ s.t. $\forall c \in \{0,1\}$, $\mathrm{tr}(\Pi_c |\psi_c\rangle\langle\psi_c|) = \frac{1}{2} + \frac{\sqrt{1-u^2}}{2}$.*

In the above measurement, the measurement gives the correct answer w.p. $\frac{1}{2} + \frac{\sqrt{1-u^2}}{2}$ and gives the opposite answer w.p. $\frac{1}{2} - \frac{\sqrt{1-u^2}}{2}$. Another measurement of interest is the one arising in the context of unambiguous state discrimination. Here we allow the measurement to answer "I don't know" (which corresponds to outcome 2). What we require from the measurement is that if the measurement does not answer 2 then it always answers the correct value. The optimal unambiguous measurement is given by the proposition below.

Proposition 7 (Unambiguous State Discrimination)**.** *Let $|\psi_0\rangle, |\psi_1\rangle$ be 2 quantum pure states s.t. $|\langle\psi_0|\psi_1\rangle| = u$. There exists a POVM $F = \{F_0, F_1, F_2\}$ s.t. $\forall c \in \{0,1\}, \mathrm{tr}(F_c|\psi_c\rangle\langle\psi_c|) = 1-u$ and $\mathrm{tr}(F_2|\psi_c\rangle\langle\psi_c|) = u$.*

The optimal unambiguous measurement is not known when there are more than 2 states. We present a detailed analysis of USD with q states in Section 4.1, where we give known results and also provide some new ones.

The final measurement of interest is the Pretty Good Measurement, which is a generic measurement to distinguish n quantum states.

Definition 18 (Pretty Good Measurement)**.** *Consider an ensemble $\{|\psi_i\rangle\}_{i\in[n]}$ of n quantum pure states. The Pretty Good Measurement associated to this ensemble is the POVM $\{M_i\}_{i\in[n]}$ with*

$$M_i = \rho^{-\frac{1}{2}}|\psi_i\rangle\langle\psi_i|\rho^{-\frac{1}{2}} \quad \text{given} \quad \rho = \sum_{i\in[n]} |\psi_i\rangle\langle\psi_i|.$$

One can easily check that each $M_i \succcurlyeq 0$ and that $\sum_i M_i = \rho^{-\frac{1}{2}}\rho\rho^{-\frac{1}{2}} = I$.

Proposition 8. *[BK02, Mon06] Consider an ensemble $\{|\psi_i\rangle\}_{i\in[n]}$ of n quantum pure states and $\{M_i\}_{i\in[n]}$ the associated pretty good measurement. We consider the setting where i is chosen at random and we want to recover i from $|\psi_i\rangle$. Let P_{PGM} be the probability of success using the PGM and P_{OPT} be the optimal success probability. This means*

$$P_{PGM} = \frac{1}{n}\sum_i \mathrm{tr}\left(|\psi_i\rangle\langle\psi_i|M_i\right)$$
$$P_{OPT} = \max_{\{N_i\}} \frac{1}{n}\sum_i \mathrm{tr}(|\psi_i\rangle\langle\psi_i|N_i)$$

where the maximum is over all POVMs $\{N_i\}_{i\in[n]}$. We have

$$P_{PGM} \leq P_{OPT} \leq \sqrt{P_{PGM}}.$$

2.4 The classical and quantum Fourier transform on $\mathbb{F}_q^n$

In this article, we will use the quantum Fourier transform on $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is the finite field $\mathbb{F}_q$.

Definition and basic properties. It is based on the characters of the group $(\mathbb{F}_q^n, +)$ which are defined as follows (for more details see [LN97, Chap 5, S1], in particular a description of the characters in terms of the trace function is given in [LN97, Ch. 5, S1, Th. 5.7]).

Definition 19. *Fix $q = p^s$ for a prime integer p and an integer $s \geq 1$. The characters of $\mathbb{F}_q$ are the functions $\chi_y : \mathbb{F}_q \to \mathbb{C}$ indexed by elements $y \in \mathbb{F}_q$ defined as follows*

$$\begin{aligned} \chi_y(x) &\stackrel{\triangle}{=} e^{\frac{2i\pi\,\mathrm{tr}(x\cdot y)}{p}}, \quad \text{with} \\ \mathrm{tr}(a) &\stackrel{\triangle}{=} a + a^p + a^{p^2} + \cdots + a^{p^{s-1}}. \end{aligned}$$

where the product $x \cdot y$ corresponds to the product of elements in $\mathbb{F}_q$. We extend the definition to vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$ as follows:

$$\chi_{\boldsymbol{y}}(\boldsymbol{x}) \stackrel{\triangle}{=} \Pi_{i=1}^n \chi_{y_i}(x_i).$$

When q is prime, we have $\chi_y(x) = e^{\frac{2i\pi xy}{q}}$. In the case where q is not prime, the above definition is not necessarily easy to handle for computations. Fortunately, characters have many desirable properties that we can use for our calculations.

Proposition 9. *The characters $\chi_{\boldsymbol{y}} : \mathbb{F}_q^n \to \mathbb{C}$ have the following properties*

1. *(Group Homomorphism). $\forall \boldsymbol{y} \in \mathbb{F}_q^n$, $\chi_{\boldsymbol{y}}$ is a group homomorphism from $(\mathbb{F}_q^n, +)$ to $(\mathbb{C}, \cdot)$ meaning that $\forall \boldsymbol{x}, \boldsymbol{x}' \in \mathbb{F}_q^n$, $\chi_{\boldsymbol{y}}(\boldsymbol{x} + \boldsymbol{x}') = \chi_{\boldsymbol{y}}(\boldsymbol{x}) \cdot \chi_{\boldsymbol{y}}(\boldsymbol{x}')$.*
2. *(Symmetry). $\forall \boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$, $\chi_{\boldsymbol{y}}(\boldsymbol{x}) = \chi_{\boldsymbol{x}}(\boldsymbol{y})$*
3. *(Orthogonality of characters). The characters are orthogonal functions meaning that $\forall \boldsymbol{x}, \boldsymbol{x}' \in \mathbb{F}_q^n$, $\sum_{\boldsymbol{y} \in \mathbb{F}_q^n} \chi_{\boldsymbol{y}}(\boldsymbol{x})\overline{\chi_{\boldsymbol{y}}(\boldsymbol{x}')} = q^n \delta_{\boldsymbol{x},\boldsymbol{x}'}$. In particular $\sum_{\boldsymbol{y} \in \mathbb{F}_q^n} |\chi_{\boldsymbol{y}}(\boldsymbol{x})|^2 = q$ and $\forall \boldsymbol{x} \in \mathbb{F}_q^n \setminus \{0\}$, $\sum_{\boldsymbol{y} \in \mathbb{F}_q^n} \chi_{\boldsymbol{y}}(\boldsymbol{x}) = 0$.*

Notice that these imply some other properties on characters. For instance $\chi_{\boldsymbol{y}}(\boldsymbol{0}) = 1$ or $|\chi_{\boldsymbol{y}}(\boldsymbol{x})| = 1$ for any $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$. The orthogonality of characters, allows to define a unitary transform which is is nothing but the classical or the quantum Fourier transform on $\mathbb{F}_q^n$.

Definition 20. *For a function $f : \mathbb{F}_q^n \to \mathcal{C}$, we define the (classical) Fourier transform $\hat{f}$ as*

$$\widehat{f}(\boldsymbol{x}) = \frac{1}{\sqrt{q^n}} \sum_{\boldsymbol{y} \in \mathbb{F}_q^n} \chi_{\boldsymbol{x}}(\boldsymbol{y}) f(\boldsymbol{y}).$$

The quantum Fourier transform QFT *on $\mathbb{F}_q^n$ is the quantum unitary satisfying $\forall \boldsymbol{x} \in \mathbb{F}_q^n$,*

$$\mathrm{QFT}\,|\boldsymbol{x}\rangle \quad = \quad \frac{1}{\sqrt{q^n}} \sum_{\boldsymbol{y} \in \mathbb{F}_q^n} \chi_{\boldsymbol{x}}(\boldsymbol{y}) |\boldsymbol{y}\rangle.$$

We will also write $|\widehat{\psi}\rangle \stackrel{\triangle}{=} \mathrm{QFT}\,|\psi\rangle$.

Note that when $|\psi\rangle = \sum_{\boldsymbol{x} \in \mathbb{F}_q^n} f(\boldsymbol{x})|\boldsymbol{x}\rangle$ we have

$$|\widehat{\psi}\rangle = \sum_{\boldsymbol{x} \in \mathbb{F}_q^n} \widehat{f}(\boldsymbol{x})|\boldsymbol{x}\rangle.$$

The Fourier transform can also be viewed as expressing the coefficients of a state in the Fourier basis $\left\{|\widehat{\boldsymbol{x}}\rangle, \boldsymbol{x} \in \mathbb{F}_q^n\right\}$ as shown by

Fact 1. *Let $|\psi\rangle = \sum_{\boldsymbol{y} \in \mathbb{F}_q^n} f(\boldsymbol{y})|\boldsymbol{y}\rangle$, then*

$$|\psi\rangle = \sum_{\boldsymbol{x} \in \mathbb{F}_q^n} \widehat{f}(-\boldsymbol{x})|\widehat{\boldsymbol{x}}\rangle.$$

This follows on the spot from the fact that if $|\psi\rangle = \sum_{\boldsymbol{x} \in \mathbb{F}_q^n} c_{\boldsymbol{x}}|\widehat{\boldsymbol{x}}\rangle$, then

$$c_{\boldsymbol{x}} = \langle \widehat{\boldsymbol{x}}|\psi\rangle = \frac{1}{\sqrt{q^n}} \sum_{\boldsymbol{y} \in \mathbb{F}_q^n} \overline{\chi_{\boldsymbol{x}}(y)} f(y) = \widehat{f}(-\boldsymbol{x}).$$

Translations amount to multiplication by a phase in the Fourier basis. It will be convenient for what follows to bring in the shift and phase operators which are defined by

Definition 21 (shift and phase operators)**.** *For $\boldsymbol{b}$ in $\mathbb{F}_q^n$, let $X_{\boldsymbol{b}}$ be the shift operator $X_{\boldsymbol{b}}|\boldsymbol{x}\rangle = |\boldsymbol{x}+\boldsymbol{b}\rangle$ and $Z_{\boldsymbol{b}}$ be the phase operator $Z_{\boldsymbol{b}} = \chi_{\boldsymbol{x}}(\boldsymbol{b})|\boldsymbol{x}\rangle$.*

The main properties of the Fourier transform follow from the fact that the characters are the common eigenbasis of all shift operators (and therefore all convolution operators). In the quantum setting, this amounts to the fact that the quantum states $\{|\widehat{\boldsymbol{x}}\rangle, \boldsymbol{x} \in \mathbb{F}_q^n\}$ form an eigenbasis of the shift operators as shown by

Proposition 10. *We have for all $\boldsymbol{b}$ in $\mathbb{F}_q^n$ that $|\widehat{\boldsymbol{x}}\rangle$ is an eigenstate of $X_{\boldsymbol{b}}$ associated to the eigenvalue $\chi_{\boldsymbol{x}}(-\boldsymbol{b})$ and*

$$X_{\boldsymbol{b}} \cdot \mathrm{QFT} = \mathrm{QFT} \cdot Z_{-\boldsymbol{b}} \tag{2}$$

$$\mathrm{QFT} \cdot X_{\boldsymbol{b}} = Z_{\boldsymbol{b}} \cdot \mathrm{QFT}\,. \tag{3}$$

Proof. Let $\boldsymbol{x} \in \mathbb{F}_q^n$. We observe that

$$\begin{aligned} X_{\boldsymbol{b}} \cdot \mathrm{QFT}\,|\boldsymbol{x}\rangle &= \frac{1}{\sqrt{q^n}} \sum_{\boldsymbol{y}\in\mathbb{F}_q^n} \chi_{\boldsymbol{x}}(\boldsymbol{y})|\boldsymbol{y}+\boldsymbol{b}\rangle \\ &= \frac{1}{\sqrt{q^n}} \sum_{\boldsymbol{y}\in\mathbb{F}_q^n} \chi_{\boldsymbol{x}}(\boldsymbol{y}-\boldsymbol{b})|\boldsymbol{y}\rangle \\ &= \chi_{\boldsymbol{x}}(-\boldsymbol{b}) \frac{1}{\sqrt{q^n}} \sum_{\boldsymbol{y}\in\mathbb{F}_q^n} \chi_{\boldsymbol{x}}(\boldsymbol{y})|\boldsymbol{y}\rangle \\ &= \mathrm{QFT} \cdot Z_{-\boldsymbol{b}}|\boldsymbol{x}\rangle. \end{aligned}$$

This computation shows that $|\widehat{\boldsymbol{x}}\rangle = \mathrm{QFT}\,|\boldsymbol{x}\rangle$ is an eigenstate of the shift operator $X_{\boldsymbol{b}}$ associated to the eigenvalue $\chi_{\boldsymbol{x}}(-\boldsymbol{b})$. The other equality follows from this and the symmetry property 2 of Proposition 9 which implies that

$$\mathrm{QFT}^\dagger = \overline{\mathrm{QFT}} \tag{4}$$

where by $\overline{M}$ we mean the (complex) conjugate operator of the operator M which is defined by $\overline{M} \triangleq \sum_{x,y} \overline{M_{x,y}}|x\rangle\langle y|$ when $M = \sum_{x,y} M_{x,y}|x\rangle\langle y|$. (2) namely implies that

$$\mathrm{QFT}^\dagger \cdot X_{\boldsymbol{b}}^\dagger = Z_{-\boldsymbol{b}}^\dagger \cdot \mathrm{QFT}^\dagger$$

This in turn means that

$$\overline{\mathrm{QFT}} \cdot X_{-\boldsymbol{b}} = Z_{\boldsymbol{b}} \cdot \overline{\mathrm{QFT}},$$

or equivalently

$$\overline{\overline{\mathrm{QFT}} \cdot X_{-\boldsymbol{b}}} = \overline{Z_{\boldsymbol{b}} \cdot \overline{\mathrm{QFT}}}$$

which gives

$$\mathrm{QFT} \cdot X_{-\boldsymbol{b}} = Z_{-\boldsymbol{b}} \cdot \mathrm{QFT},$$

and therefore proving (3). □

We will focus on the following quantum states $|\psi\rangle = \sqrt{1-\tau}|0\rangle + \sum_{\alpha\in\mathbb{F}_q^*} \sqrt{\frac{\tau}{q-1}}|\alpha\rangle$ associated to a q-ary channel of crossover probability τ. Indeed, when we measure such a quantum state, we namely get an element of $\mathbb{F}_q$ which can be viewed as a sample of an error output by such a channel. The quantum Fourier transform applied to such states yields a state of the same form, since it is readily verified that

Lemma 3. *Let $\tau \in [0, \frac{q-1}{q}]$ and $|\psi\rangle = \sqrt{1-\tau}|0\rangle + \sum_{\alpha\in\mathbb{F}_q^*} \sqrt{\frac{\tau}{q-1}}|\alpha\rangle$. We have*

$$\mathrm{QFT}\,|\psi\rangle = \sqrt{1-\tau^\perp}|0\rangle + \sum_{\alpha\in\mathbb{F}_q^*} \sqrt{\frac{\tau^\perp}{q-1}}|\alpha\rangle$$

with $\tau^\perp = \frac{\left(\sqrt{(q-1)(1-\tau)}-\sqrt{\tau}\right)^2}{q}$.

Proof. We write

$$\begin{aligned}\mathrm{QFT}\,|\psi\rangle &= \sqrt{\frac{1-\tau}{q}} \sum_{y\in\mathbb{F}_q} |y\rangle + \sqrt{\frac{\tau}{q(q-1)}} \sum_{y\in\mathbb{F}_q} \sum_{\alpha\in\mathbb{F}_q^*} \chi_\alpha(y)|y\rangle \\ &= \left(\sqrt{\frac{1-\tau}{q}} + \sqrt{\frac{q\tau}{q-1}}\right)|0\rangle + \sum_{y\in\mathbb{F}_q^*} \left(\sqrt{\frac{1-\tau}{q}} - \sqrt{\frac{\tau}{q(q-1)}}\right)|y\rangle\end{aligned}$$

where in the last equality we used the fact that for $y \neq 0$, we have $\sum_{\alpha\in\mathbb{F}_q} \chi_\alpha(y) = \sum_{\alpha\in\mathbb{F}_q} \chi_y(\alpha) = 0$ (by using first the symmetry property and then the orthogonality property of characters of Proposition 9). This implies that $\sum_{\alpha\in\mathbb{F}_q^*} \chi_\alpha(y) = -\chi_0(y) = -1$. In order to conclude, notice that

$$\sqrt{\frac{\tau^\perp}{q-1}} = \frac{\sqrt{(q-1)(1-\tau)}-\sqrt{\tau}}{\sqrt{q(q-1)}} = \sqrt{\frac{1-\tau}{q}} - \sqrt{\frac{\tau}{q(q-1)}}$$

which means we can rewrite $\mathrm{QFT}\,|\psi\rangle = \sqrt{1-\tau^\perp}|0\rangle + \sum_{y\in\mathbb{F}_q^*} \sqrt{\frac{\tau^\perp}{q-1}}$. □

We will also need to describe how the quantum Fourier transform acts on shifts of $|\psi\rangle$

Lemma 4. *Let $\tau \in [0, \frac{q-1}{q}]$, $b \in \mathbb{F}_q$ and denote by $|\psi_b\rangle$ the state $X_b|\psi\rangle$ where $|\psi\rangle \stackrel{\triangle}{=} \sqrt{1-\tau}|0\rangle + \sum_{\alpha\in\mathbb{F}_q^*} \sqrt{\frac{\tau}{q-1}}|\alpha\rangle$. We have*

$$\begin{aligned}|\psi_b\rangle &= \sqrt{1-\tau}|b\rangle + \sum_{\alpha\neq b} \sqrt{\frac{\tau}{q-1}}|\alpha\rangle \\ \mathrm{QFT}\,|\psi_b\rangle &= \sqrt{1-\tau^\perp}|0\rangle + \sum_{\alpha\in\mathbb{F}_q^*} \chi_\alpha(b)\sqrt{\frac{\tau^\perp}{q-1}}|\alpha\rangle.\end{aligned}$$

Proof. The first point follows right away from the definition of these quantities, whereas the second point follows on the spot from Fact 10 and the previous lemma:

$$\begin{aligned}\mathrm{QFT}\,|\psi_b\rangle &= \mathrm{QFT}\cdot X_b|\psi\rangle \\ &= Z_b \cdot \mathrm{QFT}\,|\psi\rangle \quad \text{(by Fact 10)} \\ &= Z_b\left(\sqrt{1-\tau^\perp}|0\rangle + \sum_{\alpha\in\mathbb{F}_q^*} \sqrt{\frac{\tau^\perp}{q-1}}|\alpha\rangle\right) \quad \text{(by Lemma 3)} \\ &= \sqrt{1-\tau^\perp}|0\rangle + \sum_{\alpha\in\mathbb{F}_q^*} \chi_\alpha(b)\sqrt{\frac{\tau^\perp}{q-1}}|\alpha\rangle.\end{aligned}$$

□

Applying the quantum Fourier transform on periodic states. Regev's reduction applies to states which are periodic. In our case, they will be of the form $\frac{1}{\sqrt{Z}}\sum_{\boldsymbol{c}\in\mathcal{C}}\sum_{\boldsymbol{e}\in\mathbb{F}_q^n} f(\boldsymbol{e})|\boldsymbol{c}+\boldsymbol{e}\rangle$ where Z is some normalizing constant, $\mathcal{C}$ some linear code of length n over $\mathbb{F}_q$ and f some function from $\mathbb{F}_q^n$ to $\mathbb{C}$. This state can be written as $\frac{1}{\sqrt{Z}}\sum_{\boldsymbol{x}\in\mathbb{F}_q^n} g(\boldsymbol{x})|\boldsymbol{x}\rangle$ where $g(\boldsymbol{x})=\sum_{\boldsymbol{c}\in\mathcal{C}} f(\boldsymbol{x}-\boldsymbol{c})$. We clearly have in this case $g(\boldsymbol{x}+\boldsymbol{c})=g(\boldsymbol{x})$ for any $\boldsymbol{x}\in\mathbb{F}_q^n$ and any $\boldsymbol{c}\in\mathcal{C}$. For such states, we have the following

Proposition 11. *Consider a function $f:\mathbb{F}_q^n\mapsto\mathbb{C}$. We have for all linear codes $\mathcal{C}\subseteq\mathbb{F}_q^n$:*

$$\mathrm{QFT}\left(\frac{1}{\sqrt{Z}}\sum_{\boldsymbol{c}\in\mathcal{C}}\sum_{\boldsymbol{e}\in\mathbb{F}_q^n} f(\boldsymbol{e})|\boldsymbol{c}+\boldsymbol{e}\rangle\right)=\frac{|\mathcal{C}|}{\sqrt{Z}}\sum_{\boldsymbol{y}\in\mathcal{C}^\perp}\widehat{f}(\boldsymbol{y})|\boldsymbol{y}\rangle$$

where Z is some normalizing constant.

Proof. The proposition follows from the following computation

$$\begin{aligned}
\mathrm{QFT}\left(\frac{1}{\sqrt{Z}}\sum_{\boldsymbol{c}\in\mathcal{C}}\sum_{\boldsymbol{e}\in\mathbb{F}_q^n} f(\boldsymbol{e})|\boldsymbol{c}+\boldsymbol{e}\rangle\right) &= \frac{1}{\sqrt{Z}}\sum_{\boldsymbol{e}\in\mathbb{F}_q^n} f(\boldsymbol{e})\sum_{\boldsymbol{c}\in\mathcal{C}}\sum_{\boldsymbol{x}\in\mathbb{F}_q^n}\chi_{\boldsymbol{y}}(\boldsymbol{c}+\boldsymbol{e})|\boldsymbol{y}\rangle\\
&= \frac{1}{\sqrt{Z}}\sum_{\boldsymbol{e}\in\mathbb{F}_q^n} f(\boldsymbol{e})\sum_{\boldsymbol{y}\in\mathbb{F}_q^n}\chi_{\boldsymbol{y}}(\boldsymbol{e})|\boldsymbol{y}\rangle\sum_{\boldsymbol{c}\in\mathcal{C}}\chi_{\boldsymbol{y}}(\boldsymbol{c})\\
&= \frac{|\mathcal{C}|}{\sqrt{Z}}\sum_{\boldsymbol{e}\in\mathbb{F}_q^n}\chi_{\boldsymbol{y}}(\boldsymbol{e})f(\boldsymbol{e})\sum_{\boldsymbol{y}\in\mathcal{C}^\perp}|\boldsymbol{y}\rangle \qquad (5)\\
&= \frac{|\mathcal{C}|}{\sqrt{Z}}\sum_{\boldsymbol{y}\in\mathcal{C}^\perp}\widehat{f}(\boldsymbol{y})|\boldsymbol{y}\rangle
\end{aligned}$$

where (5) follows from a slight generalization of (3) of Proposition 9, namely that

$$\begin{aligned}
\sum_{\boldsymbol{c}\in\mathcal{C}}\chi_{\boldsymbol{y}}(\boldsymbol{c}) &= |C| \text{ if } \boldsymbol{y}\in\mathcal{C}^\perp\\
&= 0 \text{ otherwise,}
\end{aligned}$$

which follows by a similar reasoning by noticing that $\mathcal{C}^\perp$ can be vieved as the set of trivial characters acting on $\mathcal{C}$:

$$\{\boldsymbol{y}\in\mathbb{F}_q^n:\chi_{\boldsymbol{y}}(\boldsymbol{c})=1,\ \forall\boldsymbol{c}\in\mathcal{C}\}=\mathcal{C}^\perp.$$

□

3 Algorithms for the binary quantum decoding problem

3.1 Quantum polynomial time algorithm using unambiguous state discrimination

We present our first quantum algorithm that directly uses unambiguous state discrimination.

Theorem 4. *Let $R\in(0,1)$. For any $\omega<\left(\frac{R}{2}\right)^\perp\stackrel{\triangle}{=}\frac{1}{2}-\sqrt{\frac{R}{2}(1-\frac{R}{2})}$, there exists a quantum algorithm that solves* $\mathrm{QDP}(2,n,\lfloor Rn\rfloor,\omega)$ *w.p.* $1-2^{-\Omega(n)}$.

Proof. We fix R, ω, as well as $n \in \mathbb{N}$ and $k = \lfloor Rn \rfloor$. We consider an instance of $QDP(2, R, k, \omega)$ so we have a random matrix $\mathbf{G} \leftarrow \{0,1\}^{k \times n}$, $\boldsymbol{c} = \boldsymbol{m}\mathbf{G}$ for a randomly chosen $\boldsymbol{m} \leftarrow \{0,1\}^k$ and the state $|\Psi_{\boldsymbol{c}}\rangle = \bigotimes_{i=1}^n |\psi_{c_i}^\omega\rangle$ where $|\psi_{c_i}^\omega\rangle = \sqrt{1-\omega}|c_i\rangle + \sqrt{\omega}|1-c_i\rangle$. We consider the following algorithm for solving our Quantum Decoding Problem

Quantum algorithm for QDP using USD

1. Start from $|\Psi_{\boldsymbol{c}}\rangle = \bigotimes_{i=1}^n |\psi_{c_i}^\omega\rangle$. Notice that $|\langle\psi_0^\omega|\psi_1^\omega\rangle| = 2\sqrt{\omega(1-\omega)}$.
2. Perform the optimal unambiguous measurement from Proposition 7 on each qubit of $|\Psi_{\boldsymbol{c}}\rangle$ in order to guess c_i, which can be done w.p. $p = 1 - |\langle\psi_0^\omega|\psi_1^\omega\rangle| = 1 - 2\sqrt{\omega(1-\omega)} \triangleq 2\omega^\perp$. Let $J \subseteq [n]$ be the set of indices where this measurement succeeds. The algorithm recovers here $\boldsymbol{c}_J$.
3. If $G_J \in \{0,1\}^{k \times |J|}$ is of rank k, recover $\boldsymbol{c}$ from $\boldsymbol{c}_J$ by computing $\boldsymbol{c}_J G_J^{-1} G$.

Let $p = 2\omega^\perp$. Since $\omega < \left(\frac{R}{2}\right)^\perp$, we have $2\omega^\perp > R$ and there exists an absolute constant $\gamma > 0$ s.t. $p = R + \gamma$. Let X_i be the random variable s.t. $X_i(i \in J) = 1$ and $X_i(i \notin J) = 0$. The X_i are independent random Bernoulli variables with parameter p. Using Hoeffding's inequality, we first compute

$$P_1 = \Pr\left[|J| \geq k + \frac{\gamma n}{2}\right] \geq \Pr\left[\sum_{i=1}^n X_i \geq pn - \frac{\gamma n}{2}\right] \geq 1 - 2^{-\frac{\gamma^2 n}{2}}$$

Then, using Proposition 4 we compute

$$P_2 = \Pr\left[\text{rank}(G_J) = k \,\middle|\, |J| \geq k + \frac{\gamma n}{2}\right] \geq 1 - 2^{-\gamma n}.$$

Notice that the algorithm recovers $\boldsymbol{c}_J$ so from Proposition 5, if $\text{rank}(G_J) = k$ then the algorithm successfully recovers $\boldsymbol{c}$. If we define P_{Succ} to be the probability of success of the algorithm, we therefore have

$$P_{Succ} \geq \Pr[\text{rank}(G_J) = k] \geq P_1 P_2 \geq 1 - 2^{-\Omega(n)}.$$

□

Using complex phases. It is also possible to put complex phases in front of the error. This means we consider the states

$$|\Psi_{\boldsymbol{c}}\rangle = \bigotimes_{i=1}^n \sqrt{1-\omega}|c_i\rangle + \sqrt{\omega}e^{i\theta}|1-c_i\rangle.$$

Interesting phenomena appear and we refer to Appendix A for a full analysis.

3.2 Reduction between quantum decoding problems in the binary setting

The above algorithm is interesting as it presents an polynomial time algorithm for the quantum decoding problem in a regime where its classical counterpart requires - with our current knowledge - an exponential classical or quantum algorithm. However, it completely fails when $\omega > \left(\frac{R}{2}\right)^\perp$ and the best algorithm for $\text{QDP}(2, n, \lfloor Rn \rfloor, \omega)$ is still by first measuring and then solving $\text{DP}(2, n, \lfloor Rn \rfloor, \omega)$. Is there a way to improve the best algorithms $\text{QDP}(2, n, \lfloor Rn \rfloor, \omega)$ by using ideas of the previous section? The answer is yes. Instead of using USD, we use what we call partial Unambiguous State Discrimination. Our measurement will still abort with some probability but

when it does not abort, we still allow a small probability failure but which will typically be smaller than if we used Helstrom's measurement. With this technique we can actually show a general reduction theorem for QDP.

Theorem 5. *Let $R \in (0,1)$. Let $\omega \in [0, \frac{1}{2})$ and $\omega' \in [0, \frac{1}{2})$ satisfying: $\omega' \leq \omega$ and $\frac{\omega^\perp}{(\omega')^\perp} > R$. Let any $p > \frac{\omega^\perp}{(\omega')^\perp}$. Let also $k = \lfloor Rn \rfloor$. Then $\mathrm{QDP}(2, n, k, \omega) \preccurlyeq \mathrm{QDP}(2, \lfloor pn \rfloor, k, \omega')$ meaning that if we have an algorithm that solves $\mathrm{QDP}(2, \lfloor pn \rfloor, k, \omega')$, we can use it to solve $\mathrm{QDP}(2, n, k, \omega)$.*

In order to prove our theorem, we first present our partial unambiguous state discrimination protocol. As a special case, we obtain our previous algorithm by taking $\omega' = 0$ (the theorem can then be applied when $R < 2\omega^\perp$).

3.2.1 Partial unambiguous state discrimination

We define $|\psi_b^\omega\rangle = \sqrt{1-\omega}|b\rangle + \sqrt{\omega}|1-b\rangle$. Recall that $\langle\psi_0^\omega|\psi_1^\omega\rangle = 2\sqrt{\omega(1-\omega)} = 1 - 2\omega^\perp$. Fix $\omega, \omega' \in (0, \frac{1}{2})$ with $\omega' \leq \omega$. We use the following lemma

Lemma 5. *Let $\alpha = \sqrt{\frac{\omega^\perp}{(\omega')^\perp}}$ and $\beta = \sqrt{1-\alpha^2}$. There exists a unitary U operation acting on $\mathrm{span}\{|0\rangle, |1\rangle, |2\rangle\}$ s.t.*

$$U|\psi_0^\omega\rangle = \alpha|\psi_0^{\omega'}\rangle + \beta|2\rangle$$
$$U|\psi_1^\omega\rangle = \alpha|\psi_1^{\omega'}\rangle + \beta|2\rangle$$

Proof. **[jp: J'enleve le proof sketch, la preuve en appendice est trop longue et n'est pas plus convaincante que le calcul ici.]** With the choice of α that was made the hermitian product $\langle\psi_0^\omega|\psi_1^\omega\rangle$ and their image is preserved. As a matter of fact

$$\langle\psi_0^\omega|\psi_1^\omega\rangle = 2\sqrt{\omega(1-\omega)} = 1 - 2\omega^\perp. \tag{6}$$

Now, if we let $|\psi_b'\rangle \triangleq \alpha|\psi_b^{\omega'}\rangle + \beta|2\rangle$ for $b \in \{0,1\}$, then we have

$$\begin{aligned}
\langle\psi_0'|\psi_1'\rangle &= |\alpha|^2\langle\psi_0^{\omega'}|\psi_1^{\omega'}\rangle + |\beta|^2 \\
&= |\alpha|^2(1 - 2\,(\omega')^\perp) + |\beta|^2 \quad (\text{ by (6)}) \\
&= 1 - 2|\alpha|^2\,(\omega')^\perp \quad (\text{by using } |\beta|^2 = 1 - |\alpha|^2) \\
&= 1 - 2\omega^\perp \qquad (\text{with our choice of } \alpha).
\end{aligned}$$

By definition of β, $|\psi_0'\rangle$ and $|\psi_1'\rangle$ are both of norm 1. This together with the equality $\langle\psi_0^\omega|\psi_1^\omega\rangle = \langle\psi_0'|\psi_1'\rangle$ we just proved shows that U as defined above preserves the hermitian product on $\mathrm{span}\{\psi_0^\omega, \psi_1^\omega\} = \mathrm{span}\{|0\rangle, |1\rangle\}$. It suffices to choose $U|2\rangle$ of norm 1 and orthogonal to both $|\psi_0'\rangle$ and $|\psi_1'\rangle$ to obtain a unitary transform since by construction it preserves the hermitian product on $\mathrm{span}\{|0\rangle, |1\rangle, |2\rangle\}$. □

Proposition 12. *Let $\omega, \omega' \in (0, \frac{1}{2})$ with $\omega' < \omega$. There exists a quantum measurement s.t. when it is applied on $|\psi_b^\omega\rangle$, the resulting state is $|\psi_b^{\omega'}\rangle$ w.p. $\frac{\omega^\perp}{(\omega')^\perp}$ and $|2\rangle$ w.p. $1 - \frac{\omega^\perp}{(\omega')^\perp}$.*

Proof. Start from $|\psi_b^\omega\rangle$ and apply the unitary U from Lemma 5. Then, perform the two outcomes projective measurement $\{(|0\rangle\langle 0| + |1\rangle\langle 1|), |2\rangle\langle 2|\}$ on the state $U|\psi_b^\omega\rangle = \alpha|\psi_b^{\omega'}\rangle + \beta|2\rangle$. We obtain the first outcome w.p. $|\alpha|^2 = \frac{\omega^\perp}{(\omega')^\perp}$ and the resulting state is $|\psi_b^{\omega'}\rangle$ and the second outcome w.p. $|\beta|^2$ and the resulting outcome is $|2\rangle$. □

Unambiguous state discrimination can be seen as a special case of this operation by taking $\omega' = 0$, which gives $\alpha = \sqrt{2\omega^\perp}$ and the probability of success is $\alpha^2 = 2\omega^\perp = 1 - \langle\psi_0^\omega|\psi_1^\omega\rangle$.

3.2.2 Proof of Theorem 5

In order to prove Theorem 5, one can just apply the algorithm of Section 3.1 in a similar fashion. We take any $\omega, \omega' \in (0, \frac{1}{2})$ with $\omega' \leq \omega$ and $\frac{\omega^\perp}{(\omega')^\perp} > R$. We also fix $p > \frac{\omega^\perp}{(\omega')^\perp}$

We want to solve $\mathrm{QDP}(2, n, k, \omega)$ using an algorithm that solves $\mathrm{QDP}(2, \lfloor pn \rfloor, k, \omega')$. We start from $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ as well as $|\psi_{\boldsymbol{c}}\rangle = \bigotimes_{i=1}^n |\psi_{c_i}^{\omega}\rangle$. We consider the following algorithm

Quantum algorithm for QDP using partial USD

1. Perform the quantum measurement of Proposition 12 on each register of $|\psi_{\boldsymbol{c}}\rangle$. Let $J \subseteq [n]$ be the set of indices where this measurement succeeds *i.e.* where we obtain $|\psi_{c_i}^{\omega'}\rangle$. By discarding the indices not in J, we obtain
$$|\phi_{\boldsymbol{c}_J}\rangle = \bigotimes_{i \in J} |\psi_{c_i}^{\omega'}\rangle.$$
2. Notice that $\boldsymbol{c}_J \in \mathcal{C}_J$ and recovering $\boldsymbol{c}_J$ from $|\phi_{\boldsymbol{c}_J}\rangle$ is a quantum decoding problem on $\mathcal{C}_J$, more precisely an instance of $\mathrm{QDP}(2, |J|, k, \omega')$. As long as $|J| \geq \lfloor pn \rfloor$, we use our $\mathrm{QDP}(q, n, \lfloor pn \rfloor, \omega')$ (by potentially removing excess coordinates if necessary if $|J| > \lfloor pn \rfloor$) to recover $\boldsymbol{c}_J$.
3. We recover $\boldsymbol{c}$ from $\boldsymbol{c}_J$ by computing $\boldsymbol{c}_J \mathbf{G}_J^{-1} \mathbf{G}$.

By definition, we recover $\boldsymbol{c}_J$. We just have to bound the probability to recover $\boldsymbol{c}$. Notice that in Step 1, we have from Proposition 12 that the measurement will succeed w.p. $\frac{\omega^\perp}{(\omega')^\perp} > p > R$ for each index. As in Section 3.1, this implies that with overwhelming probability, $|J| \geq \lfloor pn \rfloor$ which in turn implies that we can recover $\boldsymbol{c}$ from $\boldsymbol{c}_J$ with overwhelming probability.

3.2.3 Interpretation of the above as changing the noise model

In this section, we show how performing (partial) unambiguous state discrimination on a state $|\psi_b\rangle = \sqrt{1-\omega}|b\rangle + \sqrt{\omega}|1-b\rangle$ can be seen as a way to change the noise model applied on the bit b. We first define different notions of noisy channels in the binary setting.

Definition 22. *For a bit b, an error probability ω and abort probability p, we define the distributions of the Binary Symmetric Channel $BSC(b, \omega)$, of the Binary Erasure Channel $BEC(b, p)$ and of the Binary Symmetric with Errors and Erasures Channel $BSEEC(b, \omega, p)$ sampled as follows:*

$$\begin{aligned} BSC(b, \omega) &: \text{ return } b \text{ wp. } (1-\omega) \text{ and } (1-b) \text{ wp. } \omega. \\ BEC(b, p) &: \text{ return } b \text{ wp. } (1-p) \text{ and } \perp \text{ wp. } p. \\ BSEEC(b, \omega, p) &: \text{ return } b \text{ wp. } (1-p)(1-\omega), (1-b) \text{ wp. } (1-p)\omega \text{ and } \perp \text{ wp. } p. \end{aligned}$$

For a bit b, flipping it w.p. ω can be seen as passing b through a binary symmetric channel $BSC(\omega)$. Having this error in superposition means that we have access to the quantum state. Our results can be interpreted as follows

Proposition 13. *From $|\psi_b\rangle = \sqrt{1-\omega}|b\rangle + \sqrt{\omega}|1-b\rangle$ it is possible to:*

1. *Generate $y \leftarrow BSC(b, \omega)$ simply by measuring $|\psi_b\rangle$.*

2. *Generate* $y \leftarrow BEC(b, 1-2\omega^{\perp})$ *by performing unambiguous state discrimination on* $|\psi_b\rangle$.

3. *Generate* $y \leftarrow BSEEC(b, (\frac{\omega^{\perp}}{1-p})^{\perp}, p)$ *for any abort probability* $p \in [0, 1-2\omega^{\perp}]$*, by performing partial unambiguous state discrimination on* $|\psi_b\rangle$.

Notice that the third case generalizes the 2 first cases by respectively taking $p = 0$ and $p = 1-2\omega^{\perp}$. This shows the advantage of having the noise in quantum superposition. It is possible to change the noise from the one coming from a Binary Symmetric Channel to the one coming from a Binary Erasure Channel or a Binary Symmetric with Errors and Erasures Channel.

4 Polynomial time algorithm for QDP in the q-ary setting

As we saw in the previous section, unambiguous state discrimination is crucial for polynomial time algorithm for QDP. While this task is very well understood in the binary case, we do not have any general formula in the q-ary setting. Fortunately, the states we consider will have enough structure so that we can fully characterize the optimal unambiguous state discrimination algorithm. We first present this characterization, which is essentially a generalization of the work of [CB98]. We then use this unambiguous state discrimination in the q-ary setting to derive our quantum algorithm for QDP in the q-ary setting, in the same spirit as what we did in Section 3.1.

4.1 Unambiguous state discrimination in the q-ary setting

Definition 23. *An unambiguous state discrimination measurement associated to some states* $|\psi_0\rangle, \ldots, |\psi_{N-1}\rangle$ *is a POVM* $\{E_0, \ldots, E_{N-1}, E_F\}$ *(where* E_F *stands for the failure outcome) s.t.*

$$\forall i, j \neq i \in [\![0, N-1]\!],\ \mathrm{tr}(E_i|\psi_j\rangle\langle\psi_j|) = 0.$$

To such a POVM, we associate the quantities $P_j \stackrel{\triangle}{=} \mathrm{tr}(E_j|\psi_j\rangle\langle\psi_j|)$ *(the probability of correctly guessing* j *when given* $|\psi_j\rangle$*, as well as the average success probability* $\overline{P_D} \stackrel{\triangle}{=} \frac{1}{N}\sum_{j=0}^{N-1} P_j$.

The optimal unambiguous measurement is not known when there are more than 2 states, however it is known in a case where the states we want to distinguish are linearly independent, have the same *a priori* probabilities and are symmetric in the following sense [BKMH97]

Definition 24 (symmetric states)**.** *A set* $\{|\psi_0\rangle, \cdots, |\psi_{N-1}\rangle\}$ *in a Hilbert space* $\mathcal{H}$ *of dimension* N *is symmetric if and only if there exists a unitary transformation* U *of order* N *on* $\mathcal{H}$ *such that for any* i *and* j *in* $[\![0, N-1]\!]$ *we have* $|\psi_j\rangle = U^{j-i}|\psi_i\rangle$.

In such a case, the optimal unambiguous measurement is known [CB98]

Proposition 14 (Unambiguous State Discrimination of Symmetric States)**.** *Let* $\{|\psi_0\rangle, \cdots, |\psi_{N-1}\rangle\}$ *be a set of* N *symmetric states associated to a unitary transform* U*. Let* $\{E_0, \ldots, E_{N-1}, E_F\}$ *be any unambiguous state discrimination measurement associated to these states and let* P_j *and* $\overline{P_D}$ *be the associated success probabilities.* $\overline{P_D}$ *always satisfies*

$$\overline{P_D} \leq N \min_{r \in [\![0, N-1]\!]} |c_r|^2, \tag{7}$$

where c_r *are the coordinates of* $|\psi_0\rangle$ *in the eigenbasis* $\{|\gamma_r\rangle, r \in [\![0, N-1]\!]\}$ *of* U*, i.e.* $|\psi_0\rangle = \sum_{i=0}^{N-1} c_r|\gamma_r\rangle$*. There is a POVM which meets* (7) *with equality.*

A corollary of this result is obtained by taking the Hilbert space of dimension a prime number p and take U as the shift operator $U|x\rangle = |x+1\rangle$ where addition is performed in $\mathbb{F}_p$. It is easy to verify that in this case, the maximal average probability of discrimination $\overline{P_D}^{\max}$ is given by

$$\overline{P_D}^{\max} = p \min_{r \in \mathbb{F}_p} |\widehat{f}(r)|^2$$

when $|\psi_0\rangle = \sum_{e \in \mathbb{F}_p} f(e)|e\rangle$. This is a consequence of the fact that an eigenbasis of U is given by $\{|\widehat{x}\rangle, x \in \mathbb{F}_p\}$ (this is implied by Proposition 10) and from

$$|\psi_0\rangle = \sum_{x \in \mathbb{F}_p} \widehat{f}(-x)|\widehat{x}\rangle.$$

The last equation follows from Fact 1. We will actually use and prove a slightly more general result, where in particular the dimension of the Hilbert space is not prime anymore (in which case we can not apply Proposition 14)

Proposition 15. *Let $|\psi\rangle = \sum_{\boldsymbol{y} \in \mathbb{F}_q^n} f(\boldsymbol{y})|\boldsymbol{y}\rangle$ for some function $f : \mathbb{F}_q^n \to \mathbb{C}$ s.t. $\|f\|_2 = 1$ and for $\boldsymbol{b} \in \mathbb{F}_q^n$, let $|\psi_{\boldsymbol{b}}\rangle \stackrel{\triangle}{=} X_{\boldsymbol{b}}|\psi\rangle$. When the states $|\psi_{\boldsymbol{b}}\rangle$ are all linearly independent, unambiguous state discrimination of the states $\{|\psi_{\boldsymbol{b}}\rangle,\ \boldsymbol{b} \in \mathbb{F}_q^n\}$ is possible and has a maximal average probability of discrimination given by*

$$\overline{P_D}^{max} = q^n \min_{\boldsymbol{x} \in \mathbb{F}_q^n} |\widehat{f}(\boldsymbol{x})|^2.$$

The proof of this statement borrows many ideas from [CB98]. Before giving it, we have to recall a few points (see [CB98, S II] for more details) about unambiguous state discrimination.

Unambiguous state discrimination of linearly independent states. Let $\mathcal{H}$ be the Hilbert space spanned by the $|\psi_{\boldsymbol{b}}\rangle$'s for $\boldsymbol{b}$ ranging over $\mathbb{F}_q^n$. An optimal (leading to the maximal average probability of discrimination) POVM $\{E_{\boldsymbol{b}}, \boldsymbol{b} \in \mathbb{F}_q^n\} \cup \{E_F\}$ distinguishing unambiguously all the $|\psi_{\boldsymbol{b}}\rangle$, where $E_{\boldsymbol{b}}$ detects unambiguously $|\psi_{\boldsymbol{b}}\rangle$ for all $\boldsymbol{b}$ in $\mathbb{F}_q^n$, can be chosen of the form

$$E_{\boldsymbol{b}} = \frac{P_{\boldsymbol{b}}}{|\langle \psi_{\boldsymbol{b}}^{\perp} | \psi_{\boldsymbol{b}} \rangle|^2} |\psi_{\boldsymbol{b}}^{\perp}\rangle\langle\psi_{\boldsymbol{b}}^{\perp}| \tag{8}$$

where $P_{\boldsymbol{b}}$ is the probability of detecting $|\psi_{\boldsymbol{b}}\rangle$ given that the input state was of this form and the $\{|\psi_{\boldsymbol{b}}^{\perp}\rangle,\ \boldsymbol{b} \in \mathbb{F}_q^n\}$ are the reciprocal states of the $|\psi_{\boldsymbol{b}}\rangle$'s. $|\psi_{\boldsymbol{b}}^{\perp}\rangle$ is the state (unique up to a irrelevant phase) which belongs to $\mathcal{H}$ and is orthogonal to all other $|\psi_{\boldsymbol{a}}\rangle$ for $\boldsymbol{a}$ ranging over $\mathbb{F}_q^n \setminus \{\boldsymbol{b}\}$. The average probability of discrimination is then

$$\overline{P_D} = \frac{1}{q^n} \sum_{\boldsymbol{b} \in \mathbb{F}_q^n} P_{\boldsymbol{b}}.$$

Let

$$E_D \stackrel{\triangle}{=} \sum_{\boldsymbol{b} \in \mathbb{F}_q^n} E_{\boldsymbol{b}}$$

Since $E_D + E_F = \mathbb{1}$ and E_F should be a positive semi-definite operator, it is readily verified that an optimum POVM (i.e. one that gives the maximum average probability of discrimination) has necessarily its maximum eigenvalue $\lambda_{\max}(E_D)$ equal to 1. From these considerations, we see that if we bring in $\mathbf{A}_{\boldsymbol{b}} \stackrel{\triangle}{=} \frac{1}{|\langle \psi_{\boldsymbol{b}}^{\perp} | \psi_{\boldsymbol{b}} \rangle|^2} |\psi_{\boldsymbol{b}}^{\perp}\rangle\langle\psi_{\boldsymbol{b}}^{\perp}|$ then the problem of maximizing $\overline{P_D}$ is nothing but the problem of maximizing $\frac{1}{q^n} \sum_{\boldsymbol{b} \in \mathbb{F}_q^n} P_{\boldsymbol{b}}$ given that $0 \leq P_{\boldsymbol{b}} \leq 1$ for all $\boldsymbol{b}$ in $\mathbb{F}_q^n$ and $\mathbb{1} - \sum_{\boldsymbol{b} \in \mathbb{F}_q^n} P_{\boldsymbol{b}} \mathbf{A}_{\boldsymbol{b}} \succeq 0$

(*i.e.* is a positive semi-definite matrix). No general solution to this problem is known, with the notable exception of the symmetric states case given above and our case given in Proposition 15. An averaging argument can be used in such a case to show that actually in the optimal solution all the P_j can be chosen to be equal which makes the optimization trivial.

An averaging argument. The proof of Proposition 14 of [CB98] relies essentially on an averaging argument which is used to show that there is an optimal POVM that satisfies a certain kind of invariance relation and whose individual discrimination probabilities are all the same. We show that a similar result also holds in our case

Lemma 6. *Assume that an optimal POVM is* $\{E_{\boldsymbol{b}}, \boldsymbol{b} \in \mathbb{F}_q^n\} \cup \{E_F\}$. *Denote by* $\overline{P_D}^{max}$ *its average probability of discrimination. Define for all* $\boldsymbol{b}$ *in* $\mathbb{F}_q^n$, $E_{\boldsymbol{b}}^{ave} \triangleq \frac{1}{q^n} \sum_{\boldsymbol{a} \in \mathbb{F}_q^n} X_{\boldsymbol{a}} E_{\boldsymbol{b}-\boldsymbol{a}} X_{-\boldsymbol{a}}$. *We also let* $E_D^{ave} \triangleq \sum_{\boldsymbol{b} \in \mathbb{F}_q^n} E_{\boldsymbol{b}}^{ave}$ *and* $E_F^{ave} \triangleq \mathbb{1} - E_D^{ave}$. *Then* $\{E_{\boldsymbol{b}}^{ave}, \boldsymbol{b} \in \mathbb{F}_q^n\} \cup \{E_F^{ave}\}$ *is also an optimal POVM that satisfies for all* $\boldsymbol{a}$ *in* $\mathbb{F}_q^n$ *the invariance relation* $X_{\boldsymbol{a}} E_{\boldsymbol{b}}^{ave} X_{-\boldsymbol{a}} = E_{\boldsymbol{b}}^{ave}$. *Moreover for this new POVM, the discrimination probability* $P_{\boldsymbol{b}}^{ave} \triangleq \langle \psi_{\boldsymbol{b}} | E_{\boldsymbol{b}}^{ave} | \psi_{\boldsymbol{b}} \rangle$ *of* $|\psi_{\boldsymbol{b}}\rangle$ *is equal to the maximal average discrimination probability* $\overline{P_D}^{max}$ *for all* $\boldsymbol{b}$ *in* $\mathbb{F}_q^n$.

Proof. Clearly for all $\boldsymbol{a}$ in $\mathbb{F}_q^n$, the POVM $\{X_{\boldsymbol{a}} E_{\boldsymbol{b}} X_{-\boldsymbol{a}}, \boldsymbol{b} \in \mathbb{F}_q^n\} \cup \{X_{\boldsymbol{a}} E_F X_{-\boldsymbol{a}}\}$ gives an unambiguous discrimination for the set of states $\{|\psi_{\boldsymbol{b}}\rangle, \boldsymbol{b} \in \mathbb{F}_q^n\}$. We call this POVM, the original POVM shifted by $\boldsymbol{a}$. However now the operator $X_{\boldsymbol{a}} E_{\boldsymbol{b}} X_{-\boldsymbol{a}}$ detects the state $|\psi_{\boldsymbol{a}+\boldsymbol{b}}\rangle$. Let $P_{\boldsymbol{b}}$ be the discrimination probability of $|\psi_{\boldsymbol{b}}\rangle$ by the operator $E_{\boldsymbol{b}}$, that is $P_{\boldsymbol{b}} = \langle \psi_{\boldsymbol{b}} | E_{\boldsymbol{b}} | \psi_{\boldsymbol{b}} \rangle$ and $P_{\boldsymbol{b}}^{\boldsymbol{a}}$ be the discrimination probability of the same state, but this time by the POVM $\{X_{\boldsymbol{a}} E_{\boldsymbol{b}} X_{-\boldsymbol{a}}, \boldsymbol{b} \in \mathbb{F}_q^n\} \cup \{X_{\boldsymbol{a}} E_F X_{-\boldsymbol{a}}\}$. Since $|\psi_{\boldsymbol{b}}\rangle$ is now detected by $X_{\boldsymbol{a}} E_{\boldsymbol{b}-\boldsymbol{a}} X_{-\boldsymbol{a}}$, we have for all $\boldsymbol{b}$ and $\boldsymbol{a}$ in $\mathbb{F}_q^n$

$$P_{\boldsymbol{b}}^{\boldsymbol{a}} = P_{\boldsymbol{b}-\boldsymbol{a}}. \tag{9}$$

From these considerations, we clearly see that $E_{\boldsymbol{b}}^{\text{ave}} = \frac{1}{q^n} \sum_{\boldsymbol{a} \in \mathbb{F}_q^n} X_{\boldsymbol{a}} E_{\boldsymbol{b}-\boldsymbol{a}} X_{-\boldsymbol{a}}$ detects $|\psi_{\boldsymbol{b}}\rangle$ with probability $P_{\boldsymbol{b}}^{\text{ave}} = \frac{1}{q^n} \sum_{\boldsymbol{a} \in \mathbb{F}_q^n} P_{\boldsymbol{b}-\boldsymbol{a}} = \overline{P}_D$. However, we also have to show that $\{E_{\boldsymbol{b}}^{\text{ave}}, \boldsymbol{b} \in \mathbb{F}_q^n\} \cup \{E_F^{\text{ave}}\}$ defines a POVM. All the $E_{\boldsymbol{b}}^{\text{ave}}$ are clearly positive semi-definite, it remains to check that $E_F^{\text{ave}} \triangleq \mathbb{1} - E_D^{\text{ave}}$ is also positive semi-definite. For this, we observe that

$$\begin{aligned} E_D^{\text{ave}} &\triangleq \sum_{\boldsymbol{b} \in \mathbb{F}_q^n} E_{\boldsymbol{b}}^{\text{ave}} \\ &= \frac{1}{q^n} \sum_{\boldsymbol{b} \in \mathbb{F}_q^n} \sum_{\boldsymbol{a} \in \mathbb{F}_q^n} X_{\boldsymbol{a}} E_{\boldsymbol{b}-\boldsymbol{a}} X_{-\boldsymbol{a}} \\ &= \frac{1}{q^n} \sum_{\boldsymbol{b} \in \mathbb{F}_q^n} \sum_{\boldsymbol{a} \in \mathbb{F}_q^n} X_{\boldsymbol{a}} E_{\boldsymbol{b}} X_{-\boldsymbol{a}} \\ &= \frac{1}{q^n} \sum_{\boldsymbol{a} \in \mathbb{F}_q^n} X_{\boldsymbol{a}} E_D X_{-\boldsymbol{a}} \end{aligned}$$

where $E_D \triangleq \sum_{\boldsymbol{b} \in \mathbb{F}_q^n} E_{\boldsymbol{b}}$. By convexity of the maximum eigenvalue on the space of Hermitian operators on $\mathcal{H}$ we have

$$\lambda_{\max}(E_D^{\text{ave}}) \leq \frac{1}{q^n} \sum_{\boldsymbol{a} \in \mathbb{F}_q^n} \lambda_{\max}(E_D^{\boldsymbol{a}}) \tag{10}$$

where $E_D^{\boldsymbol{a}} = \sum_{\boldsymbol{b} \in \mathbb{F}_q^n} X_{\boldsymbol{a}} E_D X_{-\boldsymbol{a}}$. The shifted POVM by $\boldsymbol{a}$ is indeed a POVM and we have therefore $\lambda_{\max}(E_D^{\boldsymbol{a}}) \leq 1$. This together with (10) shows that $\lambda_{\max}(E_D^{\text{ave}}) \leq 1$ and that therefore $E_F^{\text{ave}} = \mathbb{1} - E_D^{\text{ave}}$ is indeed positive semi-definite. □

Choosing the appropriate basis. The appropriate basis which simplifies a lot the computation is the common diagonalization basis of all the $X_{\boldsymbol{b}}$'s. It is given by the "character" basis $\{|\widehat{\boldsymbol{x}}\rangle, \boldsymbol{x} \in \mathbb{F}_q^n\}$ (see Proposition 10) and we have

$$X_{\boldsymbol{b}}|\widehat{\boldsymbol{x}}\rangle = \chi_{\boldsymbol{x}}(-\boldsymbol{b})|\widehat{\boldsymbol{x}}\rangle. \tag{11}$$

From this, we deduce that for all $\boldsymbol{b}$ in $\mathbb{F}_q^n$ we have

$$X_{\boldsymbol{b}} = \sum_{\boldsymbol{x}\in\mathbb{F}_q^n} \chi_{\boldsymbol{x}}(-\boldsymbol{b})|\widehat{\boldsymbol{x}}\rangle\langle\widehat{\boldsymbol{x}}| \tag{12}$$

If we express $|\psi_{\mathbf{0}}\rangle$ in this basis, we obtain

$$|\psi_{\mathbf{0}}\rangle = \sum_{\boldsymbol{x}\in\mathbb{F}_q^n} c_{\boldsymbol{x}}|\widehat{\boldsymbol{x}}\rangle$$

then all the other ones are given by

$$|\psi_{\boldsymbol{b}}\rangle = X_{\boldsymbol{b}}|\psi_{\mathbf{0}}\rangle = \sum_{\boldsymbol{x}\in\mathbb{F}_q^n} c_{\boldsymbol{x}}\chi_{\boldsymbol{x}}(-\boldsymbol{b})|\widehat{\boldsymbol{x}}\rangle. \tag{13}$$

It is readily verified that the reciprocal states are given by

$$|\psi_{\boldsymbol{b}}^{\perp}\rangle = \frac{1}{\sqrt{Z}} \sum_{\boldsymbol{x}\in\mathbb{F}_q^n} \frac{1}{\overline{c_{\boldsymbol{x}}}}\chi_{\boldsymbol{x}}(-\boldsymbol{b})|\widehat{x}\rangle \tag{14}$$

where $Z = \sum_{\boldsymbol{x}\in\mathbb{F}_q^n} |c_{\boldsymbol{x}}|^{-2}$. Indeed, we observe that for any $\boldsymbol{a}$ and $\boldsymbol{b}$ in $\mathbb{F}_q^n$ we have

$$\langle\psi_{\boldsymbol{a}}^{\perp}|\psi_{\boldsymbol{b}}\rangle = \frac{1}{\sqrt{Z}} \sum_{\boldsymbol{x}\in\mathbb{F}_q^n} \overline{\chi_{\boldsymbol{x}}(-\boldsymbol{a})}\chi_{\boldsymbol{x}}(-\boldsymbol{b}) = \frac{1}{\sqrt{Z}} \sum_{\boldsymbol{x}\in\mathbb{F}_q^n} \chi_{\boldsymbol{x}}(\boldsymbol{a}-\boldsymbol{b}) = \frac{q^n}{\sqrt{Z}}\delta(\boldsymbol{a},\boldsymbol{b}) \tag{15}$$

where $\delta(\boldsymbol{x},\boldsymbol{y})$ is the Kronecker function which is equal to 1 iff $\boldsymbol{x} = \boldsymbol{y}$ and to 0 otherwise.

We have now all the tools we need to prove Proposition 15.

Proof of Proposition 15. From Lemma 6 we can choose the $E_{\boldsymbol{b}}$ of the optimal POVM as

$$E_{\boldsymbol{b}} = \frac{\overline{P_D}}{|\langle\psi_{\boldsymbol{b}}^{\perp}|\psi_{\boldsymbol{b}}\rangle|^2}|\psi_{\boldsymbol{b}}^{\perp}\rangle\langle\psi_{\boldsymbol{b}}^{\perp}|. \tag{16}$$

By (15) we know that $|\langle\psi_{\boldsymbol{b}}^{\perp}|\psi_{\boldsymbol{b}}\rangle|^2 = \frac{q^{2n}}{Z}$, and therefore by plugging this expression in (16) and using (13) and (14) we obtain

$$\begin{aligned}
E_{\boldsymbol{b}} &= \frac{Z}{q^{2n}}\frac{\overline{P_D}}{Z} \sum_{\substack{\boldsymbol{x}\in\mathbb{F}_q^n \\ \boldsymbol{y}\in\mathbb{F}_q^n}} \frac{1}{\overline{c_{\boldsymbol{x}}}c_{\boldsymbol{y}}}\chi_{\boldsymbol{x}}(-\boldsymbol{b})\overline{\chi_{\boldsymbol{y}}(-b)}|\widehat{\boldsymbol{x}}\rangle\langle\widehat{\boldsymbol{y}}| \\
&= \frac{\overline{P_D}}{q^{2n}} \sum_{\substack{\boldsymbol{x}\in\mathbb{F}_q^n \\ \boldsymbol{y}\in\mathbb{F}_q^n}} \frac{1}{\overline{c_{\boldsymbol{x}}}c_{\boldsymbol{y}}}\chi_{\boldsymbol{b}}(-\boldsymbol{x})\chi_{\boldsymbol{b}}(\boldsymbol{y})|\widehat{\boldsymbol{x}}\rangle\langle\widehat{\boldsymbol{y}}| \\
&= \frac{\overline{P_D}}{q^{2n}} \sum_{\substack{\boldsymbol{x}\in\mathbb{F}_q^n \\ \boldsymbol{y}\in\mathbb{F}_q^n}} \frac{1}{\overline{c_{\boldsymbol{x}}}c_{\boldsymbol{y}}}\chi_{\boldsymbol{b}}(\boldsymbol{y}-\boldsymbol{x})|\widehat{\boldsymbol{x}}\rangle\langle\widehat{\boldsymbol{y}}|
\end{aligned}$$

From this we infer that

$$\begin{aligned} E_D &= \sum_{\boldsymbol{b}\in\mathbb{F}_q^n} E_{\boldsymbol{b}} \\ &= \frac{\overline{P_D}}{q^{2n}} \sum_{\boldsymbol{b}\in\mathbb{F}_q^n} \sum_{\substack{\boldsymbol{x}\in\mathbb{F}_q^n \\ \boldsymbol{y}\in\mathbb{F}_q^n}} \frac{1}{\overline{c_{\boldsymbol{x}}} c_{\boldsymbol{y}}} \chi_{\boldsymbol{b}}(\boldsymbol{y}-\boldsymbol{x}) |\widehat{\boldsymbol{x}}\rangle\langle\widehat{\boldsymbol{y}}| \\ &= \frac{\overline{P_D}}{q^{2n}} \sum_{\substack{\boldsymbol{x}\in\mathbb{F}_q^n \\ \boldsymbol{y}\in\mathbb{F}_q^n}} \sum_{\boldsymbol{b}\in\mathbb{F}_q^n} \frac{1}{\overline{c_{\boldsymbol{x}}} c_{\boldsymbol{y}}} \chi_{\boldsymbol{b}}(\boldsymbol{y}-\boldsymbol{x}) |\widehat{\boldsymbol{x}}\rangle\langle\widehat{\boldsymbol{y}}| \\ &= \frac{\overline{P_D}}{q^n} \sum_{\boldsymbol{x}\in\mathbb{F}_q^n} \frac{1}{|c_{\boldsymbol{x}}|^2} |\widehat{\boldsymbol{x}}\rangle\langle\widehat{\boldsymbol{x}}|, \end{aligned}$$

where in the last line we used that $\sum_{\boldsymbol{b}\in\mathbb{F}_q^n} \chi_{\boldsymbol{b}}(\boldsymbol{y}-\boldsymbol{x}) = q^n \delta(\boldsymbol{x},\boldsymbol{y})$ by Proposition 9. Since the $|\widehat{\boldsymbol{x}}\rangle\langle\widehat{\boldsymbol{x}}|$'s form an orthonormal set of projectors we have that $\lambda_{\max}(E_D) = \frac{\overline{P_D}}{q^n \min_{\boldsymbol{x}\in\mathbb{F}_q^n} |c_{\boldsymbol{x}}|^2}$. From the fact that we should have $\lambda_{\max}(E_D) \leq 1$ in order E_F to be positive semi-definite, we have

$$\overline{P_D} \leq q^n \min_{\boldsymbol{x}\in\mathbb{F}_q^n} |c_{\boldsymbol{x}}|^2.$$

Clearly the optimum is attained when we have equality here and therefore

$$\begin{aligned} \overline{P_D}^{\max} &= q^n \min_{\boldsymbol{x}\in\mathbb{F}_q^n} |c_{\boldsymbol{x}}|^2 \\ &= q^n \min_{\boldsymbol{x}\in\mathbb{F}_q^n} |\widehat{f}(\boldsymbol{x})|^2 \end{aligned}$$

where we used Fact 1 for the last point which gives $c_{\boldsymbol{x}} = \widehat{f}(-\boldsymbol{x})$. □

Remark 1. *It is readily seen that the two crucial ingredients of the proof are that (i) we can take an "average" of an optimal solution to show that there is an optimal solution where all states are discriminated with the same probability, (ii) a basis which simplifies the computation. (i) holds in a more general case where the set of states is of the form $\{U|\psi\rangle, U \in G\}$ where G is a finite group of unitaries. On top of that, (ii) holds for instance if the group G is Abelian, the nice basis is then provided by the common diagonalization basis of the U's. It other words, it is straightforward to generalize Proposition 14 in the case where the set of states is of the form $\{U|\psi\rangle, U \in G\}$ where G is a finite Abelian group.*

4.2 Quantum polynomial time algorithm for QDP in the q-ary setting

The goal of the previous subsection was to extend unambiguous state discrimination to our q-ary setting. When we apply Proposition 15 in our case we obtain

Proposition 16 (Unambiguous state discrimination, q-ary case)**.** *Let $\omega \leq \frac{q-1}{q}$. For each $a \in \mathbb{F}_q$, we define $|\psi_a\rangle = \sqrt{1-\omega}|a\rangle + \sum_{b\neq a} \sqrt{\frac{\omega}{q-1}}|b\rangle$. There exists a POVM $\{\{E_a\}_{a\in\mathbb{F}_q}, E_F\}$ s.t.*

$$\begin{aligned} \forall a \in \mathbb{F}_q,\ \operatorname{tr}(E_a|\psi_a\rangle\langle\psi_a|) &\stackrel{\triangle}{=} P_{usd} = \frac{q\cdot\omega^{\perp}}{q-1} \\ \forall a, b \neq a \in \mathbb{F}_q,\ \operatorname{tr}(E_b|\psi_a\rangle\langle\psi_a|) &= 0 \end{aligned}$$

Notice that since $\{\{E_a\}_{a\in\mathbb{F}_q}, E_F\}$ is a POVM, this implies for each $a \in \mathbb{F}_q$ $\mathrm{tr}(E_F|\psi_a\rangle\langle\psi_a|) = 1 - \mathrm{P_{usd}} = 1 - \frac{q\cdot\omega^\perp}{q-1}$

Proof. We define $|\psi\rangle = \sum_{x\in\mathbb{F}_q} f(x)|x\rangle$ with $f(0) = \sqrt{1-\omega}$ and $f(x) = \sqrt{\frac{\omega}{q-1}}$ for $x \in \mathbb{F}_q^*$. With this definition, $|\psi_a\rangle = X_a|\psi\rangle$. As computed in Lemma 3, we have

$$\widehat{f}(0) = \sqrt{1-\omega^\perp} \quad ; \quad \widehat{f}(y) = \sqrt{\frac{\omega^\perp}{q-1}} \ \text{ for } y \in \mathbb{F}_q^*.$$

with $\omega^\perp = \frac{\left(\sqrt{(q-1)(1-\omega)}-\sqrt{\omega}\right)^2}{q}$. One can check that for $\omega \in [0, \frac{q-1}{q}]$, we have $\hat{f}(0) \geq \hat{f}(y)$ for $y \in \mathbb{F}_q^*$. We use Proposition 15 with $n = 1$ to immediately get

$$\mathrm{P_{usd}} = q \cdot \min_y |\hat{f}(y)|^2 = \frac{q\cdot\omega^\perp}{q-1}$$

□

It also turns that this operation can be implemented efficiently in poly-log time (in q) as shown by

Proposition 17. *Consider the unitary U acting on $|\psi_a\rangle|0\rangle$ as*

$$U|\widehat{0}\rangle|0\rangle = |\widehat{0}\rangle\left(u|0\rangle + \sqrt{1-u^2}|1\rangle\right) \qquad \text{with } u = \sqrt{\frac{\omega^\perp}{(1-\omega^\perp)(q-1)}}$$
$$U|\widehat{\alpha}\rangle|0\rangle = |\widehat{\alpha}\rangle|0\rangle \qquad \forall \alpha \in \mathbb{F}_q^*$$

With our choice of function f, the above unambiguous state discrimination quantum measurement can be done by applying U on $|\psi_\alpha\rangle|0\rangle$ and and then measuring the output state in the computational basis. This can be done in time $O(\mathsf{polylog}(q))$.

Proof. Let us start the proof by writing $|\psi_\alpha\rangle$ in the Fourier basis $\{\widehat{x},\ x \in \mathbb{F}_q\}$. This can be done by observing that

$$\begin{aligned}
|\psi_\alpha\rangle &= X_\alpha|\psi\rangle \\
&= X_\alpha \cdot \mathrm{QFT}\cdot\mathrm{QFT}^\dagger|\psi\rangle \\
&= X_\alpha \cdot \mathrm{QFT}\left(\sqrt{1-\omega^\perp}|0\rangle + \sum_{\gamma\in\mathbb{F}_Q^*}\sqrt{\frac{\omega^\perp}{q-1}}|\gamma\rangle\right) \text{ (by Lemma 3 and } \left(\omega^\perp\right)^\perp = \omega) \\
&= \mathrm{QFT}\cdot Z_{-\alpha}\left(\sqrt{1-\omega^\perp}|0\rangle + \sum_{\gamma\in\mathbb{F}_Q^*}\sqrt{\frac{\omega^\perp}{q-1}}|\gamma\rangle\right) \text{ (by Lemma 4)} \\
&= \mathrm{QFT}\left(\sqrt{1-\omega^\perp}|0\rangle + \sum_{\gamma\in\mathbb{F}_Q^*}\chi_{-\alpha}(\gamma)\sqrt{\frac{\omega^\perp}{q-1}}|\gamma\rangle\right) \\
&= \sqrt{1-\omega^\perp}|\widehat{0}\rangle + \sum_{\gamma\in\mathbb{F}_Q^*}\chi_{-\alpha}(\gamma)\sqrt{\frac{\omega^\perp}{q-1}}|\widehat{\gamma}\rangle.
\end{aligned}$$

Applying U on $|\psi_\alpha\rangle|0\rangle$, we obtain

$$|\phi'_\alpha\rangle := U|\Psi_\alpha\rangle|0\rangle = \left(u\sqrt{1-\omega^\perp}|\widehat{0}\rangle + \sum_{\gamma\in\mathbb{F}_q^*}\chi_{-\alpha}(\gamma)\sqrt{\frac{\omega^\perp}{q-1}}|\widehat{\gamma}\rangle\right)|0\rangle + \sqrt{1-u^2}\sqrt{1-\omega^\perp}|\widehat{0}\rangle|1\rangle.$$

Notice that $u\sqrt{1-\omega^\perp} = \sqrt{\frac{\omega^\perp}{q-1}}$ and that $|\alpha\rangle = \frac{1}{\sqrt{q}}\sum_{\gamma\in\mathbb{F}_q}\chi_{-\alpha}(\gamma)|\widehat{\gamma}\rangle$ (by Fact 1). From there, we can rewrite

$$|\phi'_\alpha\rangle = \sqrt{\frac{q\omega^\perp}{q-1}}|\alpha\rangle|0\rangle + \sqrt{1-u^2}\sqrt{1-\omega^\perp}|\widehat{0}\rangle|1\rangle.$$

We now measure all the qubits in the computational basis. If the last qubit is 0, the measurement outputs the value α in the first register. If the last qubit is 1, we output Fail. The measurement succeeds and outputs the correct value α w.p. $\frac{q\omega^\perp}{q-1}$. The time to perform U is essentially the time to perform two Quantum Fourier Transforms so U can be efficiently computed in time $O(\mathsf{polylog}(q))$, the whole measurement can be done in time $O(\mathsf{polylog}(q))$. □

We can now present our polynomial time algorithm in the q-ary setting:

Theorem 6. *Let $R > 0$ and $\omega \in (0, \frac{q-1}{q})$ satisfying $\frac{q\cdot\omega^\perp}{q-1} > R$. There exists a quantum algorithm that solves $\mathrm{QDP}(q, n, \lfloor Rn\rfloor, \omega)$ in time $\mathsf{poly}(n, \log(q))$.*

Proof. We fix $R > 0, k = \lfloor Rn\rfloor$ and $\omega \in (0, \frac{q-1}{q})$ satisfying $\frac{q\omega_\perp}{q-1} > R$. We are given a random generating matrix $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ with associated code $\mathcal{C}$ as well as a state $|\psi_{\boldsymbol{c}}\rangle = \bigotimes_{i=1}^n |\psi_{c_i}\rangle$ for a randomly chosen $\boldsymbol{c} \in \mathcal{C}$, where

$$|\psi_{c_i}\rangle = \sqrt{1-\omega}|c_i\rangle + \sum_{x\neq c_i}\sqrt{\frac{\omega}{q-1}}|x\rangle.$$

As in Section 3.1, we consider the following algorithm.

Quantum algorithm for QDP using q-ary USD

1. Perform the optimal unambiguous measurement given in Proposition 16 from Proposition 7 on each register i in order to guess c_i, which can be done w.p. $\mathrm{P}_{\mathrm{usd}} = \frac{q\omega^\perp}{q-1}$. Let $J \subseteq [n]$ be the set of indices where this measurement succeeds. The algorithm recovers here $\boldsymbol{c}_J$.
2. If $G_J \in \mathbb{F}_q^{k\times|J|}$ is of rank k, recover $\boldsymbol{c}$ from $\boldsymbol{c}_J$ by computing $\boldsymbol{c}_J G_J^{-1} G$.

By our choice of ω, we have $\mathrm{P}_{\mathrm{usd}} > R$ which means that there exists an absolute constant $\gamma > 0$ s.t. $\mathrm{P}_{\mathrm{usd}} = R + \gamma$. This in turn implies that the success probability of this algorithm is $1 - o(1)$, using the same arguments as in Section 3.1. □

5 (In)tractability of the quantum decoding problem

In this section we provide a full characterization of the tractability of $\mathrm{QDP}(q, n, k, \omega)$. We show that the problem is tractable *i.e.* there exists a quantum algorithm that solves the problem w.p. $1 - o(1)$ (as $n \to +\infty$ and $q = \Omega(1)$) for any absolute constant $\omega < (\delta_{\min}(q, 1-k/n))^\perp$. We will

simplify the notation as alluded in Subsection 2.1 and write from now on just $\delta_{\min}(1-k/n)$ instead of $\delta_{\min}(q, 1-k/n)$. Moreover, R denotes in the whole section the rate $\frac{k}{n}$ of the code we decode:

$$R \stackrel{\triangle}{=} k/n.$$

Notice here that we do not put here any restriction on the running time of the algorithm. On the other hand, we show that the problem is intractable *i.e.* all quantum algorithms solve the problem w.p. at most $o(1)$ for any absolute constant $\omega > (\delta_{\min}(1-R))^{\perp}$.

In order to prove our results, we will focus on a single quantum algorithm: the one that performs a pretty good measurement. Recall that in the quantum decoding problem, we have to recover $\boldsymbol{c}$ from $|\psi_{\boldsymbol{c}}\rangle = \sum_{\boldsymbol{e}} \sqrt{(\frac{\omega}{q-1})^{|\boldsymbol{e}|}(1-\omega)^{n-|\boldsymbol{e}|}}|\boldsymbol{c}+\boldsymbol{e}\rangle$. In order to prove our results, we will focus on a single quantum algorithm performing the pretty good measurement on the Fourier transforms of these states. For the tractability result, we show that the PGM recovers $\boldsymbol{c}$ w.p. $1-o(1)$. For the intractability result, we show that the PGM recovers $\boldsymbol{c}$ w.p. $o(1)$. But we know from Proposition 8 that this implies that any quantum algorithm will recover $\boldsymbol{c}$ w.p. $o(1)$ hence the intractability result.

We first study the PGM for any error function f and then apply our results to $f(\boldsymbol{e}) = \sqrt{(\frac{\omega}{q-1})^{|\boldsymbol{e}|}(1-\omega)^{n-|\boldsymbol{e}|}}$ in order to show our (in)tractability results.

5.1 Computing the PGM associated to the quantum decoding problem

We fix a generating matrix $\mathbf{G}$ and an associated code $\mathcal{C}$. In order to study our PGM, we define the shifted dual codes of $\mathcal{C}$

$$\mathcal{C}_{\boldsymbol{s}}^{\perp} \stackrel{\triangle}{=} \{\boldsymbol{x} \in \mathbb{F}_q^n : \mathbf{G}\boldsymbol{x}^{\intercal} = \boldsymbol{s}\}$$

Notice that $\mathcal{C}_{\mathbf{0}}^{\perp} = \mathcal{C}^{\perp}$ where $\mathcal{C}^{\perp}$ is the dual code of $\mathcal{C}$. For each shifted dual code $\mathcal{C}_{\boldsymbol{s}}^{\perp}$, we fix an element $u_{\boldsymbol{s}} \in \mathcal{C}_{\boldsymbol{s}}^{\perp}$. We have $\mathcal{C}_{\boldsymbol{s}}^{\perp} = \{u_{\boldsymbol{s}} + \boldsymbol{d} : \boldsymbol{d} \in \mathcal{C}^{\perp}\}$. This means that for all $\boldsymbol{c}$ in $\mathcal{C}$ and all $\boldsymbol{y}$ in $\mathcal{C}_{\boldsymbol{s}}^{\perp}$

$$\chi_{\boldsymbol{c}}(\boldsymbol{y}) = \chi_{\boldsymbol{c}}(u_{\boldsymbol{s}})$$

Moreover, for any $\boldsymbol{s}, \boldsymbol{s}'$ in $\mathbb{F}_q^k$ s.t. $\boldsymbol{s}' \neq \boldsymbol{s}$, since $u_{\boldsymbol{s}} + u_{\boldsymbol{s}'} \notin \mathcal{C}^{\perp}$, we have

$$\sum_{\boldsymbol{c} \in \mathcal{C}} \chi_{\boldsymbol{c}}(u_{\boldsymbol{s}} + u_{\boldsymbol{s}'}) = 0 \tag{17}$$

Now fix any error function $f : \mathbb{F}_q^n \to \mathbb{C}$ s.t. $\|f\|_2 = 1$, and consider the states $|\psi_{\boldsymbol{c}}\rangle = \sum_{\boldsymbol{e} \in \mathbb{F}_q^n} f(\boldsymbol{e})|\boldsymbol{c}+\boldsymbol{e}\rangle$. The goal is to recover $\boldsymbol{c}$. Actually, we will start from $|\widehat{\psi_{\boldsymbol{c}}}\rangle = \mathrm{QFT}\,|\psi_{\boldsymbol{c}}\rangle$ instead of $|\psi_{\boldsymbol{c}}\rangle$ and apply the Pretty Good Measurement on the ensemble of states $\{|\widehat{\psi_{\boldsymbol{c}}}\rangle\}$. The distinguishing problem is equivalent since applying QFT is a unitary operation. We first define the states

$$|W_{\boldsymbol{s}}\rangle \stackrel{\triangle}{=} \sum_{\boldsymbol{y} \in \mathcal{C}_{\boldsymbol{s}}^{\perp}} \hat{f}(\boldsymbol{y})|\boldsymbol{y}\rangle \quad \text{(not normalized)}$$
$$|\widetilde{W_{\boldsymbol{s}}}\rangle \stackrel{\triangle}{=} \frac{|W_{\boldsymbol{s}}\rangle}{\||W_{\boldsymbol{s}}\rangle\|}$$

as well as $n_{\boldsymbol{s}} \stackrel{\triangle}{=} \||W_{\boldsymbol{s}}\rangle\| = \sqrt{\sum_{\boldsymbol{y} \in \mathcal{C}_{\boldsymbol{s}}^{\perp}} |\hat{f}(\boldsymbol{y})|^2}$. We first write $|\widehat{\psi_{\boldsymbol{c}}}\rangle$ in the $\{|W_{\boldsymbol{s}}\rangle\}$ basis.

Lemma 7. $|\widehat{\psi_{\boldsymbol{c}}}\rangle = \sum_{\boldsymbol{s} \in \mathbb{F}_q^k} \chi_{\boldsymbol{c}}(u_{\boldsymbol{s}})|W_{\boldsymbol{s}}\rangle$.

Proof. We write

$$\begin{aligned}|\widehat{\psi_{\boldsymbol{c}}}\rangle &= \frac{1}{\sqrt{q^n}} \sum_{\boldsymbol{y},\boldsymbol{e}\in\mathbb{F}_q^n} \chi_{\boldsymbol{c}+\boldsymbol{e}}(\boldsymbol{y}) f(\boldsymbol{e}) |\boldsymbol{y}\rangle \\ &= \frac{1}{\sqrt{q^n}} \sum_{\boldsymbol{s}\in\mathbb{F}_q^k} \sum_{\boldsymbol{x}\in\mathcal{C}_{\boldsymbol{s}}^\perp} \chi_{\boldsymbol{c}}(\boldsymbol{x}) \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} \chi_{\boldsymbol{e}}(\boldsymbol{x}) f(\boldsymbol{e}) |\boldsymbol{x}\rangle \\ &= \sum_{\boldsymbol{s}\in\mathbb{F}_q^k} \chi_{\boldsymbol{c}}(u_{\boldsymbol{s}}) \sum_{\boldsymbol{x}\in\mathcal{C}_{\boldsymbol{s}}^\perp} \hat{f}(\boldsymbol{x}) |\boldsymbol{x}\rangle = \sum_{\boldsymbol{s}\in\mathcal{C}_{\boldsymbol{s}}^\perp} \chi_{\boldsymbol{c}}(u_{\boldsymbol{s}}) |W_{\boldsymbol{s}}\rangle.\end{aligned}$$

□

We can now explicit the PGM associated to the states $|\widehat{\psi_{\boldsymbol{c}}}\rangle$.

Proposition 18. *The PGM associated to the ensemble of states $\{|\widehat{\psi_{\boldsymbol{c}}}\rangle\}_{\boldsymbol{c}\in C}$ is the projective measurement $\{|Y_{\boldsymbol{c}}\rangle\langle Y_{\boldsymbol{c}}|\}_{\boldsymbol{c}\in\mathcal{C}}$ where $|Y_{\boldsymbol{c}}\rangle = \frac{1}{\sqrt{q^k}} \sum_{\boldsymbol{s}\in\mathbb{F}_q^k} \chi_{\boldsymbol{c}}(u_{\boldsymbol{s}}) |\widetilde{W_{\boldsymbol{s}}}\rangle$.*

Proof. We write the PGM $\{M_{\boldsymbol{c}}\}$ associated to the states $|\widehat{\psi_{\boldsymbol{c}}}\rangle$ using Definition 18.

$$M_{\boldsymbol{c}} = \rho^{-1/2} |\widehat{\psi_{\boldsymbol{c}}}\rangle\langle\widehat{\psi_{\boldsymbol{c}}}| \rho^{-1/2} \quad \text{given } \rho = \sum_{\boldsymbol{c}\in\mathbb{F}_q^k} |\widehat{\psi_{\boldsymbol{c}}}\rangle\langle\widehat{\psi_{\boldsymbol{c}}}|$$

We now write

$$\rho = \sum_{\boldsymbol{c}\in\mathcal{C}} |\widehat{\psi_{\boldsymbol{c}}}\rangle\langle\widehat{\psi_{\boldsymbol{c}}}| = \sum_{\boldsymbol{c}\in\mathcal{C}} \sum_{\boldsymbol{s},\boldsymbol{s}'\in\mathbb{F}_q^k} \chi_{\boldsymbol{c}}(u_{\boldsymbol{s}} - u_{\boldsymbol{s}'}) |W_{\boldsymbol{s}}\rangle\langle W_{\boldsymbol{s}'}| = q^k \sum_{\boldsymbol{s}\in\mathbb{F}_q^k} |W_{\boldsymbol{s}}\rangle\langle W_{\boldsymbol{s}}|$$

where we use Equation 17 as well as $\chi_{\boldsymbol{c}}(\boldsymbol{0}) = 1$ for the last equality. Using the fact that the $|W_{\boldsymbol{s}}\rangle$ are pairwise orthogonal (since they have disjoint support in the computational basis), the $|\widetilde{W_{\boldsymbol{s}}}\rangle\langle\widetilde{W_{\boldsymbol{s}}}|$'s are pairwise orthogonal projectors and we have

$$\rho = q^k \sum_{\boldsymbol{s}\in\mathbb{F}_q^k} n_{\boldsymbol{s}}^2 |\widetilde{W_{\boldsymbol{s}}}\rangle\langle\widetilde{W_{\boldsymbol{s}}}| \quad \text{hence} \quad \rho^{-1/2} = \frac{1}{\sqrt{q^k}} \sum_{\boldsymbol{s}\in\mathbb{F}_q^k} \frac{1}{n_{\boldsymbol{s}}} |\widetilde{W_{\boldsymbol{s}}}\rangle\langle\widetilde{W_{\boldsymbol{s}}}|$$

and

$$\rho^{-1/2} |\widehat{\psi_{\boldsymbol{c}}}\rangle = \frac{1}{\sqrt{q^k}} \sum_{\boldsymbol{s}\in\mathbb{F}_q^k} \chi_{\boldsymbol{c}}(u_{\boldsymbol{s}}) |\widetilde{W_{\boldsymbol{s}}}\rangle := |Y_{\boldsymbol{c}}\rangle. \tag{18}$$

Here $|Y_{\boldsymbol{c}}\rangle$ is a pure state of norm 1. Also, notice that these states are pairwise orthogonal. So $M_{\boldsymbol{c}} = |Y_{\boldsymbol{c}}\rangle\langle Y_{\boldsymbol{c}}|$ and the PGM is just the projective measurement $\{|Y_{\boldsymbol{c}}\rangle\langle Y_{\boldsymbol{c}}|\}_{\boldsymbol{c}\in\mathcal{C}}$. □

Finally, we can explicit the probability that the PGM succeeds on the states $|\widehat{\psi_{\boldsymbol{c}}}\rangle$.

Proposition 19. *The PGM succeeds to recover $\boldsymbol{c}$ from $|\widehat{\psi_{\boldsymbol{c}}}\rangle$ w.p. $\frac{1}{q^k}\left(\sum_{\boldsymbol{s}\in\mathbb{F}_q^k} n_{\boldsymbol{s}}\right)^2$.*

Proof. From the previous proposition, the PGM we use is the projective measurement $\{|Y_{\boldsymbol{c}}\rangle\langle Y_{\boldsymbol{c}}|\}_{\boldsymbol{c}\in\mathcal{C}}$ with $|Y_{\boldsymbol{c}}\rangle = \frac{1}{\sqrt{q^k}} \sum_{\boldsymbol{s}\in\mathbb{F}_q^k} \chi_{\boldsymbol{c}}(u_{\boldsymbol{s}}) |\widetilde{W_{\boldsymbol{s}}}\rangle$. For each $\boldsymbol{c} \in \mathcal{C}$, we write using Lemma 7 as well as the expression of $|Y_{\boldsymbol{c}}\rangle$ the probability $p_{\boldsymbol{c}}$ that this measurement succeeds

$$p_{\boldsymbol{c}} \stackrel{\triangle}{=} |\langle Y_{\boldsymbol{c}}|\widehat{\psi_{\boldsymbol{c}}}\rangle|^2 = \frac{1}{q^k} \left| \sum_{\boldsymbol{s}} \langle\widetilde{W_{\boldsymbol{s}}}|W_{\boldsymbol{s}}\rangle \right|^2 = \frac{1}{q^k} \left(\sum_{\boldsymbol{s}\in\mathbb{F}_q^k} n_s \right)^2 \tag{19}$$

which immediately gives us the result. □

Remark 2. *Since $\widehat{|\psi_{\boldsymbol{c}}\rangle}$ is of norm 1, we have immediately from Lemma 7 that $\sum_{\boldsymbol{s}\in\mathbb{F}_q^k} n_{\boldsymbol{s}}^2 = 1$. In the case where all the norms are equal, we have $n_{\boldsymbol{s}} = \sqrt{q^{-k}}$ which gives indeed $P_{PGM} = 1$. On the other hand, if these norms are highly unbalanced the probability that the PGM succeeds is very low.*

5.2 (In)tractability results

5.2.1 First computations and probabilistic arguments on random codes

We go back to our quantum decoding problem. Our error function corresponds to the q-ary symmetric channel so $f(\boldsymbol{e}) = \left(\sqrt{1-\omega}\right)^{n-|\boldsymbol{e}|}\left(\sqrt{\frac{\omega}{q-1}}\right)^{|\boldsymbol{e}|}$ we have (see Lemma 3)

$$\hat{f}(\boldsymbol{y}) = (\sqrt{1-\omega^{\perp}})^{n-|\boldsymbol{y}|}\left(\sqrt{\frac{\omega^{\perp}}{q-1}}\right)^{|\boldsymbol{y}|},$$

with $\omega^{\perp} = \frac{\left(\sqrt{(q-1)(1-\omega)}-\sqrt{\omega}\right)^2}{q}$. For a fixed $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ and associated code $\mathcal{C}$ (we will not make this dependency explicit in the notation to simplify it), we define

$$\begin{aligned} n_{\boldsymbol{s},\mathcal{C}} &\stackrel{\triangle}{=} \| \sum_{\boldsymbol{y}\in\mathcal{C}_{\boldsymbol{s}}^{\perp}} \hat{f}(\boldsymbol{y})|\boldsymbol{y}\rangle \| \\ a_{\boldsymbol{s},\mathcal{C}}(t) &\stackrel{\triangle}{=} \left|\{\boldsymbol{y}\in\mathcal{C}_{\boldsymbol{s}}^{\perp} : |\boldsymbol{y}| = t\}\right| \end{aligned}$$

We also define $S(t) \stackrel{\triangle}{=} \frac{(q-1)^t\binom{n}{t}}{q^k}$. Notice that $n_{\boldsymbol{s},\mathcal{C}}$ corresponds exactly to $n_{\boldsymbol{s}}$ defined in the previous section but we made the dependency in $\mathcal{C}$ explicit. Our goal is to compute the success probability of the PGM on average on $\mathbf{G}$ so using Proposition 19, we want to bound the quantity

$$\mathrm{P}_{\mathrm{PGM}} = \mathsf{E}_{\mathbf{G}}\left[\frac{1}{q^k}\left(\sum_{\boldsymbol{s}\in\mathbb{F}_q^k} n_{\boldsymbol{s},\mathcal{C}}\right)^2\right].$$

We first write

$$n_{\boldsymbol{s},\mathcal{C}}^2 = \sum_{y\in\mathcal{C}_{\boldsymbol{s}}^{\perp}} |\hat{f}(\boldsymbol{y})|^2 = \sum_{t=0}^{n} a_{\boldsymbol{s},\mathcal{C}}(t)\left(\frac{\omega^{\perp}}{q-1}\right)^t (1-\omega^{\perp})^{n-t} \tag{20}$$

and recall from Remark 2 that $\sum_{\boldsymbol{s}\in\mathbb{F}_q^k} n_{\boldsymbol{s},\mathcal{C}}^2 = 1$. We see that to compute P_{PGM}, we have to say something about the terms $a_{\boldsymbol{s}}(t,\mathcal{C})$. We first have the following, which was proven for example in [Deb23]:

Proposition 20. $\forall t \neq 0,\ \mathsf{E}_{\mathbf{G}}\left[a_{\boldsymbol{s}}(t,\mathcal{C})\right] = S(t)$.

But the expected value will not be enough. We will need concentration bounds coming from the second moment technique

Proposition 21 (Second moment technique, Proposition 3 from [Deb23])**.** *Fix any $\boldsymbol{s}\in\mathbb{F}_q^k$ and $t\in[\![1,n]\!]$. For any $\varepsilon > 0$, we have*

$$\Pr_{G}\left[|a_{\boldsymbol{s},\mathcal{C}}(t) - S(t)| \geq \varepsilon S(t)\right] \leq \frac{q-1}{\varepsilon^2 S(t)}.$$

In particular, take $\varepsilon = S(t)^{-1/3}$, we have

$$\Pr_G\left[a_{\boldsymbol{s},\mathcal{C}}(t) \leq S(t)(1-\frac{1}{S(t)^{1/3}})\right] \leq \frac{q-1}{S(t)^{1/3}}.$$

We can now observe two things

1. From the above proposition combined with Equation 20, we have that when $S(t)$ is exponential, which happens when $t = \gamma n$ with $\gamma \in (\delta_{\min}(1-R), \delta_{\max}(1-R))$

$$n^2_{\boldsymbol{s},\mathcal{C}} \approx \sum_{t=\lfloor \delta_{\min}(1-R)n \rfloor}^{\lceil \delta_{\max}(1-R)n \rceil} S(t)\left(\frac{\omega^\perp}{q-1}\right)^t (1-\omega^\perp)^{n-t}. \tag{21}$$

2. In order to estimate the above sum, first notice that

$$\sum_{t=0}^{n} S(t)\left(\frac{\omega^\perp}{q-1}\right)^t (1-\omega^\perp)^{n-t} = \frac{1}{q^k}\sum_{t=0}^{n}\binom{n}{t}(\omega^\perp)^t(1-\omega^\perp)^{n-t} = \frac{1}{q^k}. \tag{22}$$

   But the above sum is actually the cumulative sum of the binomial distribution with parameters n and $\omega^\perp$. It concentrates around the weight $n\omega^\perp$. This is formalized by the following proposition

Proposition 22. *For any absolute constant $\varepsilon > 0$,*

$$\sum_{t=\lfloor(\omega^\perp-\varepsilon)n\rfloor}^{\lceil(\omega^\perp+\varepsilon)n\rceil} S(t)\left(\frac{\omega^\perp}{q-1}\right)^t (1-\omega^\perp)^{n-t} = \frac{1}{q^k}\left(1-o(1)\right). \tag{23}$$

We now have all the tools for our (in)tractability proofs. The main idea is the following: when $t = \omega n$ with $\omega < \delta_{\min}(1-R)^\perp$, we have $\omega^\perp \in (\delta_{\min}(1-R), \delta_{\max}(1-R))$ and so we can combine Equations 21,23 to show that for most $\mathbf{G}$, $n^2_{\boldsymbol{s},\mathcal{C}} = \frac{1}{q^k}(1-o(1))$. On the other hand, when $\omega > \delta_{\min}(1-R)^\perp$, we have $\omega^\perp \notin (\delta_{\min}(1-R), \delta_{\max}(1-R))$ and so we can combine Equations 21,22,23 to show that for most $\mathbf{G}$, $n^2_{\boldsymbol{s},\mathcal{C}} = o(1)$. The next sections will make these arguments formal and show how this allows us to conclude.

5.2.2 Tractability

We use the notations previously defined in Section 5.2.1. ω will be considered as a fixed constant in $(0,1)$. Our main claim is the following

Proposition 23. *If $\omega < (\delta_{\min}(1-R))^\perp$ then $P_{PGM} = \frac{1}{q^k}\mathsf{E}_{\mathbf{G}}\left[\left(\sum_{\boldsymbol{s}\in\mathbb{F}_q^k} n_{\boldsymbol{s},\mathcal{C}}\right)^2\right] = 1-o(1)$.*

Proof. Using (20) we know that $n^2_{\boldsymbol{s},\mathcal{C}} = \sum_{t=0}^{n} a_{\boldsymbol{s},\mathcal{C}}(t)\left(\frac{\omega^\perp}{q-1}\right)^t (1-\omega^\perp)^{n-t}$. Since $\omega < (\delta_{\min}(1-R))^\perp$, we have $\omega^\perp > \delta_{\min}(1-R)$ so we fix $\delta > 0$ s.t. $\omega^\perp - \delta > \delta_{\min}(1-R)$. We therefore write

$$n^2_{\boldsymbol{s},\mathcal{C}} \geq \sum_{t=\lfloor(\omega^\perp-\delta)n\rfloor}^{\lfloor(\omega^\perp+\delta)n\rfloor} a_{\boldsymbol{s},\mathcal{C}}(t)\left(\frac{\omega^\perp}{q-1}\right)^t (1-\omega^\perp)^{n-t}.$$

We define $t_0 = \lfloor(\omega^\perp - \delta)n\rfloor$ and $t_1 = \lfloor(\omega^\perp + \delta)n\rfloor$. Recall that $a_{\boldsymbol{s},\mathcal{C}}(t)$ is typically close to $S(t)$ as shown by Lemma 21. This gives for $t \in \left(\lfloor(\omega^\perp - \delta)n\rfloor, \lfloor(\omega^\perp + \delta)n\rfloor\right)$

$$\begin{aligned}\Pr_G\left[a_{\boldsymbol{s},\mathcal{C}}(t) \le S(t)(1 - \frac{1}{S(t_0)^{1/3}})\right] &\le \Pr_G\left[a_{\boldsymbol{s},\mathcal{C}}(t) \le S(t)(1 - \frac{1}{S(t)^{1/3}})\right] \\ &\le \frac{q-1}{S(t)^{1/3}} \le \frac{q-1}{S(t_0)^{1/3}}.\end{aligned}$$

and

$$\Pr_G\left[\forall t \in [\![t_0, t_1]\!],\ a_{\boldsymbol{s},\mathcal{C}}(t) \ge S(t)(1 - \frac{1}{S(t_0)^{1/3}})\right] \ge 1 - \frac{(q-1)(t_1 - t_0 + 1)}{S(t_0)^{1/3}}$$

This implies

$$\Pr_G\left[n^2_{\boldsymbol{s},\mathcal{C}} \ge \sum_{t=t_0}^{t_1} S(t)(1 - S(t_0)^{-1/3})\left(\frac{\omega^\perp}{q-1}\right)^t (1-\omega^\perp)^{n-t}\right] \ge 1 - \frac{(q-1)(t_1 - t_0 + 1)}{S(t_0)^{1/3}}. \quad (24)$$

We have

$$\begin{aligned}\sum_{t=t_0}^{t_1} S(t)(1 - S(t_0)^{-1/3})\left(\frac{\omega^\perp}{q-1}\right)^t (1-\omega^\perp)^{n-t} &= (1 - S(t_0)^{-1/3})\sum_{t=t_0}^{t_1} S(t)\left(\frac{\omega^\perp}{q-1}\right)^t (1-\omega^\perp)^{n-t} \\ &= \frac{(1 - S(t_0)^{-1/3})}{q^k} K(n)\end{aligned}$$

where $K(n) \triangleq \sum_{t=t_0}^{t_1} \binom{n}{t} \left(\omega^\perp\right)^t (1-\omega^\perp)^{n-t}$ and $K(n) = 1 - o(1)$ as n tends to infinity by Proposition 22. By plugging this equality in the left-hand side of (24) we obtain

$$\Pr_G\left[n_{\boldsymbol{s},\mathcal{C}} \ge \sqrt{\frac{1 - S(t_0)^{-1/3}}{q^k} K(n)}\right] \ge 1 - \frac{(q-1)(t_1 - t_0)}{S(t_0)^{1/3}}.$$

Since $t_0 = \lfloor(\omega^\perp - \delta)n\rfloor$ with $\delta_{\min}(1-R) < (\omega^\perp - \delta) < \delta_{\max}(1-R)$, we have $S(t_0) = q^{\Omega(n)}$ which implies

$$\begin{aligned}\mathsf{E}_G[n_{\boldsymbol{s},\mathcal{C}}] &\ge \sqrt{\frac{1 - S(t_0)^{-1/3}}{q^k} K(n)} \cdot \Pr_G\left[n_{\boldsymbol{s},\mathcal{C}} \ge \sqrt{\frac{1 - S(t_0)^{-1/3}}{q^k} K(n)}\right] \\ &\ge \sqrt{\frac{1 - S(t_0)^{-1/3}}{q^k} K(n)} \cdot \left(1 - \frac{(q-1)(t_1 - t_0)}{S(t_0)^{1/3}}\right) \\ &= \frac{1}{\sqrt{q^k}}\left(1 - o(1)\right)\end{aligned}$$

which gives

$$\mathsf{E}_G[\sum_{\boldsymbol{s}\in\mathbb{F}_q^k} n_{\boldsymbol{s},\mathcal{C}}] \ge \sqrt{q^k}(1 - o(1)) \quad (25)$$

In order to conclude, we use Jensen's inequality $\mathsf{E}_G(X^2) \ge (\mathsf{E}_G(X))^2$ and Equation 25 to get

$$P_{PGM} = \frac{1}{q^k}\mathsf{E}_G\left[\left(\sum_{\boldsymbol{s}\in\mathbb{F}_q^n} n_{\boldsymbol{s},\mathcal{C}}\right)^2\right] \ge \frac{1}{q^k}\left(\mathsf{E}_G\left[\sum_{\boldsymbol{s}\in\mathbb{F}_q^k} n_{\boldsymbol{s},\mathcal{C}}\right]\right)^2 \ge 1 - o(1)$$

□

5.2.3 Intractability

Again, we use the same notation as in the previous sections with a fixed $\omega \in (0,1)$. We show that if ω is too large then $P \stackrel{\triangle}{=} \mathsf{E}_{\mathbf{G}}(\mathrm{P}_{\mathrm{PGM}})$ is an $o(1)$ as shown by

Theorem 7. *Let $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ be a random generating matrix and $\mathcal{C}$ be the associated code. Let $\omega > (\delta_{\min}(1-R))^{\perp}$ and let the states $|\psi_{\boldsymbol{c}}\rangle = \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} f(\boldsymbol{e})|\boldsymbol{c}+\boldsymbol{e}\rangle$ with*

$$f(\boldsymbol{e}) = \sqrt{\left(\frac{\omega}{q-1}\right)^{|\boldsymbol{e}|}(1-\omega)^{n-|\boldsymbol{e}|}}.$$

The pretty good measurement distinguishes the states $|\psi_{\boldsymbol{c}}\rangle$ w.p. $P = o(1)$.

Again, we will heavily build on the expression of $n_{\boldsymbol{s},\mathcal{C}}$ given by (20) in terms of the $a_{\boldsymbol{s},\mathcal{C}}(t)$'s. The proof is based on the following steps

Step 1. Let us start by giving an upper-bound on $a_{\boldsymbol{s},\mathcal{C}}(t)$ which holds with probability close to 1 for large values of K

Lemma 8. *For any $K > 0$, any t in $[\![1,n]\!]$ and any $\boldsymbol{s} \in \mathbb{F}_q^k$, we have $\Pr_{\mathbf{G}}\left[a_{\boldsymbol{s},\mathcal{C}}(t) \geq K\cdot S(t)\right] \leq \frac{1}{K}$ which directly implies*

$$\Pr_{\mathbf{G}}\left[a_{\boldsymbol{s},\mathcal{C}}(t) \leq K\cdot S(t)\right] \geq 1 - \frac{1}{K}. \tag{26}$$

Proof. This is just Markov's inequality $\Pr_{\mathbf{G}}\left[a_{\boldsymbol{s},\mathcal{C}}(t) \leq K\mathsf{E}_{\mathbf{G}}(a_{\boldsymbol{s},\mathcal{C}}(t))\right] \leq \frac{1}{K}$ by recalling that $\mathsf{E}_{\mathbf{G}}(a_{\boldsymbol{s},\mathcal{C}}(t)) = S(t)$. □

A rather immediate corollary of this result is that

Corollary 1. *For any $\delta > 0$, $\boldsymbol{s}$ in $\mathbb{F}_q^k$ and t in $[\![1,n]\!] \setminus [(\delta_{\min}(1-R)-\delta)n, (\delta_{\max}(1-R)+\delta)n]$, we have with probability $1-q^{-\Omega(n)}$ that $a_{\boldsymbol{s},\mathcal{C}}(t) = 0$.*

Proof. In such a case we have $S(t) = q^{-\Omega(n)}$, since $S(t) \leq q^{n(h_q(t/n)-k/n)}$ and we use Lemma 8 with $K = \frac{1}{\sqrt{S(t)}}$ to obtain

$$\Pr_{\mathbf{G}}\left[a_{\boldsymbol{s},\mathcal{C}}(t) \leq \sqrt{S(t)}\right] \geq 1 - \sqrt{S(t)} = 1 - q^{-\Omega(n)}.$$

We can conclude by using the fact that $a_{\boldsymbol{s},\mathcal{C}}(t)$ is an non negative integer so if $a_{\boldsymbol{s},\mathcal{C}}(t) \leq \sqrt{S(t)} < 1$ then necessarily $a_{\boldsymbol{s},\mathcal{C}}(t) = 0$. □

Step 2. The previous results allow to show that

Lemma 9. *Let $\omega > (\delta_{\min}(1-R))^{\perp}$. There exists an $\varepsilon > 0$ such that for any $\boldsymbol{s} \in \mathbb{F}_q^k$ which is non zero we have*

$$\Pr_{\mathbf{G}}\left[n_{\boldsymbol{s},\mathcal{C}} \geq q^{-k/2-\varepsilon n}\right] = q^{-\Omega(n)}.$$

Proof. Let us recall (20)

$$n_{\boldsymbol{s},\mathcal{C}}^2 = \sum_{y\in\mathcal{C}_{\boldsymbol{s}}^{\perp}} |\hat{f}(\boldsymbol{y})|^2 = \sum_{t=0}^{n} a_{\boldsymbol{s},\mathcal{C}}(t)\left(\frac{\omega^{\perp}}{q-1}\right)^t (1-\omega^{\perp})^{n-t}.$$

By using Corollary 1 and $a_{\boldsymbol{s},\mathcal{C}}(0) = 0$ for $\boldsymbol{s} \neq 0$, we obtain that for any absolute constant $\delta > 0$,

$$\forall \boldsymbol{s} \in F_q^k \backslash \{\mathbf{0}\},\ \Pr_{\mathbf{G}}\left[n_{\boldsymbol{s},\mathcal{C}}^2 = \sum_{t=\lfloor(\delta_{\min}-\delta)n\rfloor}^{\lceil(\delta_{\max}+\delta)n\rceil} a_{\boldsymbol{s},\mathcal{C}}(t) \left(\frac{\omega^\perp}{q-1}\right)^t (1-\omega^\perp)^{n-t} \right] \geq 1 - q^{\Omega(n)}, \tag{27}$$

where to simplify notation we simply write $\delta_{\min}$ and $\delta_{\max}$ for $\delta_{\min}(1-R)$ and $\delta_{\max}(1-R)$ respectively. Then by using Lemma 8 we also deduce that for any $\delta, \delta' > 0$,

$$\forall \boldsymbol{s} \in F_q^k \backslash \{\mathbf{0}\},\ \Pr_{\mathbf{G}}\left[n_{\boldsymbol{s},\mathcal{C}}^2 \leq \sum_{t=\lfloor(\delta_{\min}-\delta)n\rfloor}^{\lceil(\delta_{\max}+\delta)n\rceil} q^{\delta' n} S(t) \left(\frac{\omega^\perp}{q-1}\right)^t (1-\omega^\perp)^{n-t} \right] \geq 1 - q^{-\Omega(n)}$$

We observe now that

$$\sum_{t=\lfloor(\delta_{\min}-\delta)n\rfloor}^{\lceil(\delta_{\max}+\delta)n\rceil} q^{\delta' n} S(t) \left(\frac{\omega^\perp}{q-1}\right)^t (1-\omega^\perp)^{n-t} = q^{\delta' n - k} \sum_{t=\lfloor(\delta_{\min}-\delta)n\rfloor}^{\lceil(\delta_{\max}+\delta)n\rceil} p(t) \tag{28}$$

where $p(t) \stackrel{\triangle}{=} \binom{n}{t}(\omega^\perp)^t(1-\omega^\perp)^{n-t}$ is the probability that a binomial variable of parameters n and $\omega^\perp$ takes the value t. By using the fact that $\omega^\perp \leq (\delta_{\min} - \delta")n$ for some $\delta" > 0$ and the Hoeffding inequality (see Lemma 1) we deduce that for $\delta = \delta"/2$, it holds that $\sum_{t=\lfloor(\delta_{\min}-\delta)n\rfloor}^{\lceil(\delta_{\max}+\delta)n\rceil} p(t) \leq q^{-\delta''' n}$ for some $\delta''' > 0$. By choosing $\delta' < \delta'''$, we obtain that $n_{\boldsymbol{s},\mathcal{C}}$ is less than $q^{-k/2-\frac{\delta'''-\delta'}{2}n}$ with probability $1 - q^{-\Omega(n)}$. We just have to choose $\varepsilon = (\delta''' - \delta')/2$ to finish the proof. □

We are ready now to prove Theorem 7.

Proof of Theorem 7. For $\boldsymbol{s} \in \mathbb{F}_q^k$, let $G_\varepsilon(\boldsymbol{s}) = \{\mathbf{G} \in \mathbb{F}_q^{k\times n} : n_{\boldsymbol{s},\mathcal{C}} \geq q^{-k/2-\varepsilon n}\}$. Also, for $\mathbf{G} \in \mathbb{F}_q^{k\times n}$, let $S_\varepsilon(\mathbf{G}) = \{\boldsymbol{s} \neq 0 : n_{\boldsymbol{s},\mathcal{C}} \geq q^{-k/2-\varepsilon n}\}$. The previous lemma tells us that $\forall \boldsymbol{s} \neq \mathbf{0}, |G_\varepsilon(\boldsymbol{s})| = o(|G|)$ where $|G| = q^{nk}$ is the total number of possible matrices $\mathbf{G} \in \mathbb{F}_q^{k\times n}$. Now, notice that

$$\sum_{\boldsymbol{s}\neq 0} |G_\varepsilon(\boldsymbol{s})| = \left|\{(\mathbf{G}, \boldsymbol{s}) : n_{\boldsymbol{s},\mathcal{C}} \geq q^{-k/2-\varepsilon n}\}\right| = \sum_{\mathbf{G}} |S_\varepsilon(\mathbf{G})|.$$

This implies that $\sum_{G\in\mathbf{G}} |S_\varepsilon(G)| = o(|G|q^k)$ and $\mathsf{E}_{\mathbf{G}}[|S_\varepsilon(\mathbf{G})|] = o(q^k)$. Now fix $\mathbf{G} \in \mathbb{F}_q^{k\times n}$. We write

$$\left(\sum_{\boldsymbol{s}\in\mathbb{F}_q^n} n_{\boldsymbol{s},\mathcal{C}}\right)^2 = \left(n_{\mathbf{0},\mathcal{C}} + \sum_{\boldsymbol{s}\in S_\varepsilon(\mathbf{G})} n_{\boldsymbol{s},\mathcal{C}} + \sum_{\boldsymbol{s}\notin S_\varepsilon(\mathbf{G})} n_{\boldsymbol{s},\mathcal{C}}\right)^2 \leq 3n_{\mathbf{0},\mathcal{C}}^2 + 3\left(\sum_{\boldsymbol{s}\in S_\varepsilon(\mathbf{G})} n_{\boldsymbol{s},\mathcal{C}}\right)^2 + 3\left(\sum_{\boldsymbol{s}\notin S_\varepsilon(\mathbf{G})} n_{\boldsymbol{s},\mathcal{C}}\right)^2 \tag{29}$$

$$\leq 3n_{\mathbf{0},\mathcal{C}}^2 + 3|S_\varepsilon(\mathbf{G})| \sum_{\boldsymbol{s}\neq\mathbf{0}} n_{\boldsymbol{s},\mathcal{C}}^2 + 3\left(q^{k/2-\varepsilon n}\right)^2 \tag{30}$$

$$\leq 3|S_\varepsilon(\mathbf{G})| + o(q^k) \tag{31}$$

Here (29) follows from the inequality $(x+y+z)^2 \leq 3x^2 + 3y^2 + 3z^2$ (which can be proved by noticing that $3x^2 + 3y^2 + 3z^2 - (x+y+z)^2 = (x-y)^2 + (y-z)^2 + (x-z)^2$). (30) follows from the Cauchy-Schwartz inequality and (31) is a consequence of $\sum_{\boldsymbol{s}\in\mathbb{F}_q^k} n_{\boldsymbol{s},\mathcal{C}}^2 = 1$ which also gives $n_{\mathbf{0},\mathcal{C}}^2 \leq 1$. In order to conclude, we write

$$P = \mathsf{E}_{\mathbf{G}}\left[\frac{1}{q^k}\left(\sum_{\boldsymbol{s}\in F_q^k} n_{\boldsymbol{s},\mathcal{C}}\right)^2\right] \leq \frac{1}{q^k}\left(3\mathsf{E}_{\mathbf{G}}[|S_\varepsilon(\mathbf{G})|] + o(q^k)\right) = o(1).$$

□

6 From the quantum decoding problem to the short codeword problem

In this section, we show how to apply our algorithm for the quantum decoding problem into Regev's reduction in order to obtain quantum algorithms for the short codeword problem.

We fix $n, k', q \in \mathbb{N}$ with $q \geq 2$ as well as $\omega' \in (0,1)$. We start from a random instance $\mathbf{G}' \in \mathbb{F}_q^{k' \times n}$ of $\mathrm{SCP}(q, n, k', \omega')$. Let $\mathcal{C}'$ be the code associated to $\mathbf{G}'$ and $\mathcal{C} = (\mathcal{C}')^\perp$ the dual code of $\mathcal{C}'$. The idea will be to solve a quantum decoding problem associated to $\mathcal{C}$, *i.e.* from the state $|\psi_{\boldsymbol{c}}\rangle \triangleq \sum_{\boldsymbol{e} \in \mathbb{F}_q^n} f(\boldsymbol{e}) |\boldsymbol{c} + \boldsymbol{e}\rangle$ where $\boldsymbol{c}$ belongs to $\mathcal{C}$, we want to recover $\boldsymbol{c}$. Then we apply the quantum Fourier transform and measure in the computational basis to obtain a short codeword of $\mathcal{C}'$. We also define $k = n - k'$ and

$$\omega \triangleq (\omega')^\perp = \frac{\left(\sqrt{(q-1)(1-\omega')} - \sqrt{\omega'}\right)^2}{q} \quad ; \quad f(\boldsymbol{e}) \triangleq \left(\sqrt{\frac{\omega}{q-1}}\right)^{|\boldsymbol{e}|} \left(\sqrt{1-\omega}\right)^{n-|\boldsymbol{e}|}$$

Recall also, using $\omega^\perp = \omega'$ that

$$\widehat{f}(\boldsymbol{y}) = \left(\sqrt{\frac{\omega'}{q-1}}\right)^{|\boldsymbol{y}|} \left(\sqrt{1-\omega'}\right)^{n-|\boldsymbol{y}|}.$$

Remark. We use this notation k', ω' so that the problem we reduce to is a $\mathrm{QDP}(q, n, k, \omega)$ with a generating matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$. This allows us to keep notation consistent with the previous section but be aware that the Short Codeword problem we are solving is on $\mathcal{C}' = \mathcal{C}^\perp$.

6.1 Regev's reduction for codes

We now describe Regev's reduction for codes. As we will see, this does not necessarily give a reduction from the short codeword problem to the quantum decoding problem because of the small error in the quantum decoding algorithm. We consider the formulation of this reduction from [SSTX09] and adapted in [DRT23] in the context of codes.

We first construct

$$|\Omega_0\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c} \in \mathcal{C}} \sum_{\boldsymbol{e} \in \mathbb{F}_q^n} f(\boldsymbol{e}) |\boldsymbol{c}\rangle |\boldsymbol{e}\rangle$$

and add $\boldsymbol{c}$ to the second register to obtain

$$|\Omega_1\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c} \in \mathcal{C}} |\boldsymbol{c}\rangle |\psi_{\boldsymbol{c}}\rangle, \qquad \text{where } |\psi_{\boldsymbol{c}}\rangle = \sum_{\boldsymbol{e} \in \mathbb{F}_q^n} f(\boldsymbol{e}) |\boldsymbol{c} + \boldsymbol{e}\rangle.$$

The idea is then to recover $\boldsymbol{c}$ from $|\psi_{\boldsymbol{c}}\rangle$ using an algorithm for the quantum decoding problem. If this can be done perfectly, we can actually use this algorithm to erase the first register and obtain the state

$$|\Omega_2\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c} \in \mathcal{C}} |\psi_{\boldsymbol{c}}\rangle.$$

We then apply the Quantum Fourier Transform on this state to get

$$|\widehat{\Omega_3}\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c} \in \mathcal{C}} |\widehat{\psi_{\boldsymbol{c}}}\rangle = \sqrt{|\mathcal{C}|} \sum_{\boldsymbol{y} \in \mathcal{C}'} \widehat{f}(\boldsymbol{y}) |\boldsymbol{y}\rangle.$$

This follows from Proposition 11. Finally, we measure this state in the computational basis and hope to find a small codeword.

The algorithm can be summarized by

Algorithm of the quantum reduction.

Initial state preparation :		$\|\Omega_0\rangle = \frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} f(\boldsymbol{e})\|\boldsymbol{c}\rangle\|\boldsymbol{e}\rangle$
adding $\boldsymbol{c}$ to $\boldsymbol{e}$:	$\mapsto$	$\|\Omega_1\rangle = \frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} f(\boldsymbol{e})\|\boldsymbol{c}\rangle\|\boldsymbol{c}+\boldsymbol{e}\rangle = \frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \|\boldsymbol{c}\rangle\|\psi_{\boldsymbol{c}}\rangle$
decoding and erasing 1st register	$\mapsto$	$\|\Omega_2\rangle = \frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \|\boldsymbol{0}\rangle\|\psi_{\boldsymbol{c}}\rangle$
QFT on the 2nd register:	$\mapsto$	$\|\Omega_3\rangle = \frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \|\boldsymbol{0}\rangle\|\widehat{\psi_{\boldsymbol{c}}}\rangle = \sqrt{\|\mathcal{C}\|} \sum_{\boldsymbol{y}\in\mathcal{C}'} \widehat{f}(\boldsymbol{y})\|\boldsymbol{0}\rangle\|\boldsymbol{y}\rangle$
measuring the whole state:	$\mapsto$	$\|\boldsymbol{0}\rangle\|\boldsymbol{y}\rangle$ (where $\boldsymbol{y} \in \mathcal{C}' = \mathcal{C}^\perp$)

There are a two issues that can make the above algorithm not work as we want:

- The quantum decoding problem used in order to go from $|\Omega_1\rangle$ to $|\Omega_2\rangle$ does not work perfectly in many cases. Even if we have an algorithm which works w.p. $1 - o(1)$, this can greatly change the state $|\Omega_3\rangle$ that we have at the end[5]. This also means we have to explicit each time our quantum decoding procedure and analyze thoroughly the resulting state.
- Even if we obtain exactly the state $\sqrt{|\mathcal{C}|}\sum_{\boldsymbol{y}\in\mathcal{C}'} \widehat{f}(\boldsymbol{y})|\boldsymbol{y}\rangle$ we want, for values of ω' which are too large, this algorithm will actually always output $\boldsymbol{y} = \boldsymbol{0}$ but we want a small non-zero codeword so our algorithm will not work.

In this section, we show that our algorithms (or slight variants of our algorithms) can be successfully used in Regev's reduction in order to solve the Short Codeword Problem despite the above shortcomings. We show the following:

1. If we take our polynomial time algorithms for the quantum decoding problem (Section 4) we can find in quantum polynomial time small codewords down to Prange's bound, *i.e.* down to $\frac{(n-k')(q-1)}{q} = \frac{k(q-1)}{q}$. Notice however, that our algorithm obtains a state $|\Omega_2\rangle$ very far from the theoretical state $|\Omega_2\rangle = \frac{1}{\sqrt{|\mathcal{C}|}}\sum_{\boldsymbol{c}\in\mathcal{C}} |\psi_{\boldsymbol{c}}\rangle$, but we still show how to obtain a small codeword in $\mathcal{C}$ after performing QFT and measuring.
2. If we consider the tractability regime and if we take the Pretty Good Measurement associated to the states $|\widehat{\psi_{\boldsymbol{c}}}\rangle$, we show that we actually exactly get the state $|\Omega_2\rangle$ we are looking for (up to a normalization factor). We then look at this PGM and 2 variants:
   (a) If we finish the analysis with the PGM, we will most often be in regimes where we measure $\boldsymbol{0}$ in the final step so we will not be able to solve the Short Codeword problem.
   (b) We can slightly tweak the PGM so that it will give us a short codeword down to the tractability bound.

[5]This seems counterintuitive at first as we would expect the final state to be ε-close to the ideal state if the quantum decoding succeeds w.p. $1-\varepsilon$. However, we are in regimes where an ideal quantum decoder does not exist so such continuity arguments will not hold. As it will appear in our analysis, it is possible to slightly tweak the measurements used in the Quantum Decoding Problem and greatly change the outcome state.

(c) We also show another example where we can slightly tweak the PGM but where the reduction utterly fails, meaning that the state we obtain before measuring is $|\perp\rangle$. This shows that there is no hope to perform generic reduction between the quantum decoding problem and the short codeword problem with this method.

6.2 The quantum reduction with unambiguous state discrimination

We first show how to use our quantum polynomial time algorithms for the quantum decoding in Regev's reduction. We first construct

$$|\Omega_1\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c}\in\mathcal{C}} |\boldsymbol{c}\rangle|\psi_{\boldsymbol{c}}\rangle, \qquad \text{where } |\psi_{\boldsymbol{c}}\rangle = \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} f(\boldsymbol{e})|\boldsymbol{c}+\boldsymbol{e}\rangle.$$

We then apply unambiguous state discrimination measurement on $|\psi_{\boldsymbol{c}}\rangle = \bigotimes_{i=1}^n |\psi_{c_i}\rangle$. Recall that by using the version of unambiguous state discrimination presented in Proposition 17 for each i, we perform a unitary U on the i^{th} register of $|\Omega_1\rangle$ that does the following for each $c_i \in \mathbb{F}_q$:

$$U|\psi_{c_i}\rangle|0\rangle = \sqrt{\mathrm{p_{usd}}}|c_i\rangle|0\rangle + \sqrt{1-\mathrm{p_{usd}}}\widehat{|0\rangle}|1\rangle.$$

Here

$$\mathrm{p_{usd}} = q\cdot\frac{\omega^\perp}{q-1} = \frac{q}{q-1}\omega'. \tag{32}$$

After applying this (coherent) USD, we obtain the state

$$\begin{aligned}|\Omega_2\rangle &= \frac{1}{\sqrt{|\mathcal{C}|}}\sum_{\boldsymbol{c}\in\mathcal{C}}\left(|\boldsymbol{c}\rangle\otimes\left(\bigotimes_{i=1}^n \sqrt{\mathrm{p_{usd}}}|c_i\rangle|0\rangle + \sqrt{1-\mathrm{p_{usd}}}\widehat{|0\rangle}|1\rangle\right)\right)\\ &= \frac{1}{\sqrt{|\mathcal{C}|}}\sum_{\boldsymbol{c}\in\mathcal{C}}|\boldsymbol{c}\rangle\sum_{J\subseteq[n]}\beta_J|\widetilde{\boldsymbol{c}}_J\rangle.\end{aligned}$$

where

$$|\widetilde{\boldsymbol{c}}_J\rangle = \bigotimes_{i=1}^n |\gamma_i\rangle \quad \text{with} \begin{cases} |\gamma_i\rangle = |c_i\rangle|0\rangle & \text{if } i\in J\\ |\gamma_i\rangle = \widehat{|0\rangle}|1\rangle & \text{otherwise}\end{cases}$$

and $\beta_J = \sqrt{(1-\mathrm{p_{usd}})^{n-|J|}(\mathrm{p_{usd}})^{|J|}}$. J here corresponds to the set of indices where the USD succeeded. Notice that one can efficiently recover J from $|\widetilde{\boldsymbol{c}}_J\rangle$ by looking at the outcome registers, so we can add it to obtain the state

$$|\Omega_3\rangle = \frac{1}{\sqrt{|\mathcal{C}|}}\sum_{\boldsymbol{c}\in\mathcal{C}}|\boldsymbol{c}\rangle\sum_{J\subseteq[n]}\beta_J|\widetilde{\boldsymbol{c}}_J\rangle|J\rangle.$$

We now measure J to obtain the state

$$|\Omega_4(J)\rangle = \frac{1}{\sqrt{|\mathcal{C}|}}\sum_{\boldsymbol{c}\in\mathcal{C}}|\boldsymbol{c}\rangle|\widetilde{\boldsymbol{c}}_J\rangle.$$

Notice that $|J|$ follows the distribution $D(\mathrm{p_{usd}})$ with $\mathrm{p_{usd}} > R$ so, there exists an absolute constant $\varepsilon > 0$, s.t. $(R+\varepsilon)n \le |J| \le (\mathrm{p_{usd}})n$ w.p. at least $\frac{1}{2} - o(1)$ (the probability that $|J| \le \mathrm{p_{usd}}n$ is at least $\frac{1}{2}$). Moreover, using the same argument as in Section 3.1, we can recover $\boldsymbol{c}$ from $\boldsymbol{c}_J$ w.p. $1-o(1)$. This means we can erase the register $\boldsymbol{c}$ in $|\Omega_4(J)\rangle$ to get

$$|\Omega_5(J)\rangle = \frac{1}{\sqrt{|\mathcal{C}|}}\sum_{\boldsymbol{c}\in\mathcal{C}}|\boldsymbol{c}_J\rangle = \frac{1}{\sqrt{|\mathcal{C}|}}\sum_{\boldsymbol{c}\in\mathcal{C}_J}|\boldsymbol{c}\rangle.$$

We apply the Fourier transform on this state to get

$$|\widehat{\Omega_5(J)}\rangle = \frac{1}{\sqrt{|(\mathcal{C}_J)^\perp|}} \sum_{\boldsymbol{y}\in(\mathcal{C}_J)^\perp} |\boldsymbol{y}\rangle.$$

By measuring this state, we get a vector $\boldsymbol{y} \in (\mathcal{C}_J)^\perp$ of weight at most $\frac{(q-1)|J|}{q} \leq \frac{(q-1)\mathrm{p}_{\mathrm{usd}} n}{q} = \omega' n$ w.p. $\Theta(1)$. Here we used (32) for the last equality. The crux is that by Lemma 2 we have

$$(\mathcal{C}_J)^\perp = (\mathcal{C}^\perp)^J.$$

In other words, we get words in $\mathcal{C}^\perp$ shortened at J, meaning dual codewords that are 0 outside J. We have therefore constructed a word $\boldsymbol{z} \in \mathcal{C}^\perp$ s.t. $\boldsymbol{z}_j = \boldsymbol{y}_j$ if $j \in J$ and $\boldsymbol{z}_j = 0$ otherwise.

In conclusion, we just proved the following

Theorem 8. *The above algorithm, that performs Regev's reduction and uses unambiguous state discrimination for the quantum decoding problem, can solve in polynomial time $SCP(q, n, k', \omega')$ for $\omega' > \frac{(q-1)k}{q} = \frac{(q-1)(n-k')}{q}$ w.p. $\Theta(1)$.*

Notice that we can repeat this algorithm to amplify the success probability. Our algorithm can go down to Prange's bound $\frac{(q-1)(n-k')}{q}$, which is the best known bound for polynomial time algorithms for the short codeword problem. The whole algorithm is summarized by:

Algorithm of the quantum reduction in the case of USD.

Initial state preparation:		$\|\Omega_0\rangle$	$=$	$\frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} f(\boldsymbol{e})\|\boldsymbol{c}\rangle\|\boldsymbol{e}\rangle$
adding $\boldsymbol{c}$ to $\boldsymbol{e}$:	$\mapsto$	$\|\Omega_1\rangle$	$=$	$\frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \sum_{\boldsymbol{e}\in\mathbb{F}_q^n} f(\boldsymbol{e})\|\boldsymbol{c}\rangle\|\boldsymbol{c}+\boldsymbol{e}\rangle = \frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \|\boldsymbol{c}\rangle\|\psi_{\boldsymbol{c}}\rangle$
applying coherent USD:	$\mapsto$	$\|\Omega_2\rangle$	$=$	$\frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \left(\|\boldsymbol{c}\rangle \otimes \left(\bigotimes_{i=1}^{n} \sqrt{\mathrm{p}_{\mathrm{usd}}}\|c_i\rangle\|0\rangle + \sqrt{1-\mathrm{p}_{\mathrm{usd}}}\widehat{|0\rangle}\|1\rangle \right) \right)$
			$=$	$\frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \|\boldsymbol{c}\rangle \sum_{J\subseteq[n]} \beta_J \|\widetilde{\boldsymbol{c}}_J\rangle$
put J in the last register using $\|\widetilde{\boldsymbol{c}}_J\rangle$	$\mapsto$	$\|\Omega_3\rangle$	$=$	$\frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \|\boldsymbol{c}\rangle \sum_{J\subseteq[n]} \beta_J \|\widetilde{\boldsymbol{c}}_J\rangle\|J\rangle$
measure J	$\mapsto$	$\|\Omega_4\rangle$	$=$	$\frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \|\boldsymbol{c}\rangle\|\widetilde{\boldsymbol{c}}_J\rangle$
erase $\boldsymbol{c}$	$\mapsto$	$\|\Omega_5\rangle$	$=$	$\frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}} \|\boldsymbol{c}_J\rangle = \frac{1}{\sqrt{\|\mathcal{C}\|}} \sum_{\boldsymbol{c}\in\mathcal{C}_J} \|\boldsymbol{c}\rangle$
QFT:	$\mapsto$	$\|\Omega_6\rangle$	$=$	$\frac{1}{\sqrt{\|(\mathcal{C}_J)^\perp\|}} \sum_{\boldsymbol{y}\in(\mathcal{C}_J)^\perp} \|\boldsymbol{y}\rangle$
measuring the whole state:	$\mapsto$			$\|\boldsymbol{y}\rangle$ (where $\boldsymbol{y} \in (\mathcal{C}_J)^\perp = (\mathcal{C}^\perp)^J \subset \mathcal{C}^\perp$)

6.3 The Quantum reduction with the Pretty Good Measurement

We now study Regev's reduction when we use the PGM for the quantum decoding problem. We consider the basis $\{|Y_{\boldsymbol{c}}\rangle\}_{\boldsymbol{c}\in\mathcal{C}}$ described in the previous section associated to the states $\{\widehat{|\psi_{\boldsymbol{c}}\rangle}\}_{\boldsymbol{c}\in\mathcal{C}}$.

We showed that

$$\forall \boldsymbol{c} \in \mathcal{C},\ \langle \widehat{\psi_{\boldsymbol{c}}} | Y_{\boldsymbol{c}} \rangle = \sqrt{\mathrm{P_{PGM}}}$$

where $\mathrm{P_{PGM}}$ is the probability that the Pretty Good Measurement succeeds. We now unfold Regev's reduction. We start from the state $|\Omega_1\rangle$ with a slight change, we apply namely immediately the QFT on the second register to get

$$|\Omega_1\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c} \in \mathcal{C}} |\boldsymbol{c}\rangle |\widehat{\psi_{\boldsymbol{c}}}\rangle$$

with $|\psi_{\boldsymbol{c}}\rangle = \sum_{\boldsymbol{e}} f(\boldsymbol{e}) |\boldsymbol{c} + \boldsymbol{e}\rangle$. We then perform coherently the PGM on the second register and write the output on the third register. This means that if we write each $|\widehat{\psi_{\boldsymbol{c}}}\rangle = \sum_{\boldsymbol{c}' \in \mathcal{C}} \alpha_{\boldsymbol{c},\boldsymbol{c}'} |Y_{\boldsymbol{c}'}\rangle$, we obtain

$$|\Omega_2\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c} \in \mathcal{C}} |\boldsymbol{c}\rangle \sum_{\boldsymbol{c}' \in \mathcal{C}} \alpha_{\boldsymbol{c},\boldsymbol{c}'} |Y_{\boldsymbol{c}'}\rangle |\boldsymbol{c}'\rangle$$

We then subtract the value of the third register in the first register to get

$$|\Omega_3\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c},\boldsymbol{c}' \in \mathcal{C}} \alpha_{\boldsymbol{c},\boldsymbol{c}'} |\boldsymbol{c} - \boldsymbol{c}'\rangle |Y_{\boldsymbol{c}'}\rangle |\boldsymbol{c}'\rangle$$

Finally, we reverse the PGM between registers 2 and 3 to obtain the state

$$|\Omega_4\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c},\boldsymbol{c}' \in \mathcal{C}} \alpha_{\boldsymbol{c},\boldsymbol{c}'} |\boldsymbol{c} - \boldsymbol{c}'\rangle |Y_{\boldsymbol{c}'}\rangle |0\rangle$$

From the discussion at the beginning of this section, we have that for any $\boldsymbol{c} \in \mathcal{C}, \alpha_{\boldsymbol{c},\boldsymbol{c}} = \sqrt{\mathrm{P_{PGM}}}$. This means we can rewrite the above state as

$$\begin{aligned} |\Omega_4\rangle &= \frac{1}{\sqrt{|\mathcal{C}|}} \left(\sum_{\boldsymbol{c}' \in \mathcal{C}} \sqrt{\mathrm{P_{PGM}}} |0\rangle |Y_{\boldsymbol{c}'}\rangle + \sum_{\boldsymbol{c},\boldsymbol{c}' \neq \boldsymbol{c}} \alpha_{\boldsymbol{c},\boldsymbol{c}'} |\boldsymbol{c} - \boldsymbol{c}'\rangle |Y_{\boldsymbol{c}'}\rangle \right) \\ &= \sqrt{\mathrm{P_{PGM}}} |0\rangle \left(\frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c} \in \mathcal{C}} |Y_{\boldsymbol{c}}\rangle \right) + \sum_{\boldsymbol{c},\boldsymbol{c}' \neq \boldsymbol{c}} \alpha_{\boldsymbol{c},\boldsymbol{c}'} |\boldsymbol{c} - \boldsymbol{c}'\rangle |Y_{\boldsymbol{c}'}\rangle. \end{aligned}$$

The next step of the reduction is to measure the first register of $|\Omega_4\rangle$. Since the states $|Y_{\boldsymbol{c}'}\rangle$ are orthogonal and of norm 1, we measure 0 w.p. $\mathrm{P_{PGM}}$ in the first register and the second register becomes

$$|\Omega_5\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c} \in \mathcal{C}} |Y_{\boldsymbol{c}}\rangle = |\widetilde{W_0}\rangle = \frac{1}{n_0} \sum_{\boldsymbol{y} \in \mathcal{C}'} \widehat{f}(\boldsymbol{y}) |\boldsymbol{y}\rangle$$

where $n_0 \stackrel{\triangle}{=} \| \sum_{\boldsymbol{y} \in \mathcal{C}'} \widehat{f}(\boldsymbol{y}) |\boldsymbol{y}\rangle \|$. We measure this final state to potentially measure a small codeword. Let $a(t) = |\{\boldsymbol{y} \in \mathcal{C}' : |\boldsymbol{y}| = t\}$. Note that this quantity corresponds to $a_{\boldsymbol{0}}(t, \mathcal{C}')$ as defined in Subsection 5.2.1. The probability $p(t)$ that the above algorithms finds a word of weight t in $\mathcal{C}'$ is

$$p(t) = \frac{1}{n_0^2} a(t) |\widehat{f}(t)|^2, \tag{33}$$

where we overload the notation $\widehat{f}$ to mean that $\widehat{f}(t) = \widehat{f}(\boldsymbol{y})$ for any $\boldsymbol{y}$ s.t. $|\boldsymbol{y}| = t$ (recall that $\widehat{f}(\boldsymbol{y})$ is constant for any of these $\boldsymbol{y}$). The issue here is that for ω' small enough, we will almost always measure 0. Indeed,

$$p_0 = \frac{|\widehat{f}(0)|^2}{n_0^2} = \frac{|\widehat{f}(0)|^2}{\sum_t a(t)|\widehat{f}(t)|^2} = \frac{|\widehat{f}(0)|^2}{|\widehat{f}(0)|^2 + \sum_{t\neq 0} a(t)|\widehat{f}(t)|^2}.$$

Here, notice that

$$|\widehat{f}(0)|^2 = (1-\omega')^n$$
$$\Pr_G\left[\sum_{t\neq 0} a(t)|\widehat{f}(t)|^2 \leq \frac{2}{q^k}\right] \geq 1 - o(1)$$

where for the last inequality, we use the concentration bounds for $a(t) = a_{\mathbf{0}}(t, \mathcal{C}')$ of Section 5.2.1. So when $\omega' < 1 - q^{-\frac{k}{n}}$, we measure 0 with high probability. This unfortunately happens quite often and it is a problem because in our short codeword problem, we want to find a small non-zero vector.

6.3.1 A counterexample that shows complete failure

We show that things can go even worse when slightly changing the measurement used. We show that instead of measuring $|\mathbf{0}\rangle$, we can measure some given state $|\perp\rangle$ orthogonal to all the $|\widetilde{W_{\boldsymbol{s}}}\rangle$. Recall from Proposition 18 that

$$|Y_{\boldsymbol{c}}\rangle = \frac{1}{\sqrt{q^k}} \sum_{\boldsymbol{s}\in\mathbb{F}_q^k} \chi_{\boldsymbol{c}}(u_{\boldsymbol{s}})|\widetilde{W_{\boldsymbol{s}}}\rangle$$

Also, the state resulting from Regev's reduction is the state $\sum_{\boldsymbol{c}\in\mathcal{C}} |Y_{\boldsymbol{c}}\rangle = |\widetilde{W_0}\rangle$. Our modified measurement can give an extra outcome which will be an $\boldsymbol{u} \in \mathbb{F}_q^n \backslash \mathcal{C}$ and we define $\mathsf{S} = \mathcal{C} \cup \{\boldsymbol{u}\}$. Let

$$|Z_{\boldsymbol{c}}\rangle \stackrel{\triangle}{=} \frac{1}{\sqrt{q^k}} \left(|\perp\rangle + \sum_{\boldsymbol{s}\neq\mathbf{0}} \chi_{\boldsymbol{c}}(u_{\boldsymbol{s}})|\widetilde{W_{\boldsymbol{s}}}\rangle \right) \quad \forall \boldsymbol{c} \in \mathcal{C}$$
$$|Z_{\boldsymbol{u}}\rangle \stackrel{\triangle}{=} |\widetilde{W_0}\rangle$$

Notice that the $|Z_{\boldsymbol{y}}\rangle$ are pairwise orthogonal and $\mathrm{span}(\{|Z_{\boldsymbol{y}}\rangle\}_{\boldsymbol{y}\in\mathsf{S}}) = \mathrm{span}(\{|\widetilde{W_{\boldsymbol{s}}}\rangle\}_{\boldsymbol{s}\in\mathbb{F}_q^k}, |\perp\rangle) = \mathrm{span}(\{|\widehat{\psi_{\boldsymbol{c}}}\rangle\}_{\boldsymbol{c}\in\mathcal{C}}, |\perp\rangle)$. This means the measurement $\{|Z_{\boldsymbol{y}}\rangle\}_{\boldsymbol{y}\in\mathsf{S}}$ will be complete when measuring any $|\widehat{\psi_{\boldsymbol{c}}}\rangle$.

Recall that $|\widehat{\psi_{\boldsymbol{c}}}\rangle = \frac{1}{\sqrt{q^k}} \sum_{\boldsymbol{s}\in\mathbb{F}_q^k} \chi_{\boldsymbol{s}}(\boldsymbol{u}_{\boldsymbol{s}})|W_{\boldsymbol{s}}\rangle$, so we have

$$\forall \boldsymbol{c} \in \mathcal{C},\ \langle\widehat{\psi_{\boldsymbol{c}}}|Z_{\boldsymbol{c}}\rangle = \frac{1}{\sqrt{q^k}} \sum_{\boldsymbol{s}\neq 0} n_s = \sqrt{\mathrm{P}_{\mathrm{PGM}}} - \frac{n_0}{\sqrt{q^k}} \geq \sqrt{\mathrm{P}_{\mathrm{PGM}}} - \frac{1}{\sqrt{q^k}}$$

This means the above measurement solves the quantum decoding problem wp. $\left(\sqrt{\mathrm{P}_{\mathrm{PGM}}} - \frac{n_0}{\sqrt{q^k}}\right)^2 \geq \left(\sqrt{\mathrm{P}_{\mathrm{PGM}}} - \frac{1}{\sqrt{q^k}}\right)^2$ which is $1 - o(1)$ as long as $P_{PGM} = 1 - o(1)$.

Now, we perform the reduction presented in Section 6.3. We just rewrite the states of the reduction

$$|\Omega_1\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c}\in\mathcal{C}} |\boldsymbol{c}\rangle|\widehat{\psi_{\boldsymbol{c}}}\rangle$$

$$|\Omega_2\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c}\in\mathcal{C}} |\boldsymbol{c}\rangle \sum_{\boldsymbol{y}\in\mathsf{S}} \beta_{\boldsymbol{c},\boldsymbol{y}}|Z_{\boldsymbol{y}}\rangle|\boldsymbol{y}\rangle \qquad \text{where } \beta_{\boldsymbol{c},\boldsymbol{y}} = \langle\widehat{\psi_{\boldsymbol{c}}}|Z_{\boldsymbol{y}}\rangle$$

$$|\Omega_3\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c}\in\mathcal{C},\boldsymbol{y}\in\mathsf{S}} \beta_{\boldsymbol{c},\boldsymbol{y}}|\boldsymbol{c}-\boldsymbol{y}\rangle|Z_{\boldsymbol{y}}\rangle|\boldsymbol{y}\rangle$$

$$|\Omega_4\rangle = \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{\boldsymbol{c}\in\mathcal{C},\boldsymbol{y}\in\mathsf{S}} \beta_{\boldsymbol{c},\boldsymbol{y}}|\boldsymbol{c}-\boldsymbol{y}\rangle|Z_{\boldsymbol{y}}\rangle|0\rangle = \left(\sqrt{P_{PGM}} - \frac{n_0}{\sqrt{q^k}}\right)|0\rangle\frac{1}{\sqrt{|\mathcal{C}|}}\sum_{\boldsymbol{c}\in\mathcal{C}}|Z_{\boldsymbol{c}}\rangle + \frac{1}{\sqrt{|\mathcal{C}|}}\sum_{\boldsymbol{c}\in\mathcal{C}}\sum_{\boldsymbol{y}\in\mathsf{S},\boldsymbol{y}\neq\boldsymbol{c}} \beta_{\boldsymbol{c},\boldsymbol{y}}|\boldsymbol{c}-\boldsymbol{y}\rangle|Z_{\boldsymbol{y}}\rangle$$

where in the last line, we use that $\beta_{\boldsymbol{c},\boldsymbol{c}} = \left(\sqrt{P_{PGM}} - \frac{n_0}{\sqrt{q^k}}\right)$ for each $\boldsymbol{c}\in\mathcal{C}$. This means that when we measure the first register, we obtain $\mathbf{0}$ w.p. $\left(\sqrt{\mathrm{P}_{\mathrm{PGM}}} - \frac{n_0}{\sqrt{q^k}}\right)^2$, and the resulting state is $|\Omega_5\rangle = \sum_{\boldsymbol{c}\in\mathcal{C}}|Z_{\boldsymbol{c}}\rangle = |\perp\rangle$ which shows that the reduction entirely fails in this case.

6.3.2 A measurement that works

Finally, we show a measurement that will make the reduction work when $\mathrm{P}_{\mathrm{PGM}} = 1 - o(1)$. The idea is similar to the one of section 6.3.1. We add an extra outcome $\boldsymbol{u}\in\mathbb{F}_q^n\backslash\mathcal{C}$ and define $\mathsf{S} = \mathcal{C}\cup\{\boldsymbol{u}\}$. We now define

$$|U_0\rangle = \frac{\sum_{\boldsymbol{y}\in\mathcal{C}':\boldsymbol{y}\neq\mathbf{0}}\widehat{f}(\boldsymbol{y})|\boldsymbol{y}\rangle}{\|\sum_{\boldsymbol{y}\in\mathcal{C}':\boldsymbol{y}\neq\mathbf{0}}\widehat{f}(\boldsymbol{y})|\boldsymbol{y}\rangle\|}$$

$$\forall\boldsymbol{c}\in\mathcal{C},\ |Z_{\boldsymbol{c}}\rangle = \frac{1}{\sqrt{q^k}}\left(|U_0\rangle + \sum_{\boldsymbol{s}\neq\mathbf{0}}\chi_{\boldsymbol{c}}(u_{\boldsymbol{s}})|\widetilde{W}_{\boldsymbol{s}}\rangle\right)$$

$$|Z_{\boldsymbol{u}}\rangle = |\mathbf{0}\rangle$$

The $|Z_{\boldsymbol{c}}\rangle$ are exactly the states $|Y_{\boldsymbol{c}}\rangle$ of the pretty good measurement but we removed the $|\mathbf{0}\rangle$ component of $|\widetilde{W}_0\rangle$. In order to make the measurement complete, we add an extra basis element $|Z_{\boldsymbol{u}}\rangle$. We therefore have a projective measurement $\{|Z_{\boldsymbol{y}}\rangle\}_{\boldsymbol{y}\in\mathsf{S}}$ Again, we have $\langle\widehat{\psi_{\boldsymbol{c}}}|Z_{\boldsymbol{c}}\rangle \geq \sqrt{\mathrm{P}_{\mathrm{PGM}}} - \frac{1}{\sqrt{q^k}}$ and independent of $\boldsymbol{c}$ so w.p. at least $\left(\sqrt{\mathrm{P}_{\mathrm{PGM}}} - \frac{1}{\sqrt{q^k}}\right)^2$, we get the state $|U_0\rangle$. Then, ff we measure this state $|U_0\rangle$, we will get a codeword of weight t w.p.

$$p(t) = \frac{a(t)|\widehat{f}(t)|^2}{\sum_{t\neq 0} a(t)|\widehat{f}(t)|^2},\ \forall t\neq 0$$

and $p(0) = 0$, where $a(t)$ is the number of codewords of weight t in $\mathcal{C}'$. Recall that

$$\widehat{f}(t) = \left(\sqrt{\frac{\omega'}{q-1}}\right)^t \left(\sqrt{1-\omega'}\right)^{n-t}.$$

and we are in the regime where $P_{PGM} = 1-o(1)$ which means that $\omega < (\delta_{\min}(1-\frac{k}{n}))^{\perp}$ and hence $\omega' > \delta_{\min}(\frac{n-k}{n}) = \delta_{\min}(\frac{k'}{n})$.

Using Proposition 22 and the expression of $\widehat{f}(t)$, as well as concentration bounds for $a(t)$, we have that for any absolute constant $\varepsilon > 0$, $\sum_{t=\lfloor(\omega'-\varepsilon)n\rfloor}^{\lfloor(\omega'+\varepsilon)n\rfloor} p(t) = 1 - o(1)$. This means we will measure a word of weight approximately $\lfloor\omega' n\rfloor$ in $\mathcal{C}'$.

Discussion. These 3 examples above show that it is very easy to slightly modify the algorithm for solving the quantum decoding problem and drastically change the result after Regev's reduction. We therefore cannot have proper reduction theorems between the quantum decoding problem and the short codeword problem but we have to analyze on a case by case basis whether an algorithm for the quantum decoding problem can be used for finding a short codeword. On the positive side of the reduction, we can summarize our results as follows:

Proposition 24. *Let $q, n, k \in \mathbb{N}$ with $q \geq 2$ and $\omega \in (0, 1)$. Let also $R = \lfloor \frac{k}{n} \rfloor$, $\omega' = \omega^{\perp}$ and $k' = n - k$.*

- *For $\omega < (\frac{q-1R}{q})^{\perp}$, there exists a quantum algorithm running in time $\mathsf{poly}(n, \log(q))$ that solves $\mathrm{QDP}(q, n, k, \omega)$ w.p. $1 - o(1)$ (Theorem 6) . Moreover, this algorithm can be used using Regev's reduction to solve SCP(q, n, k', ω') in time poly$(n, \log(q))$ (Section 6.2).*
- *For $\omega < (\delta_{\min}(1 - R))^{\perp}$, there exists a quantum algorithm (for which we don't specify the running time but which could be exponential in n) that solves $\mathrm{QDP}(q, n, k, \omega)$ w.p. $1 - o(1)$ (Proposition 23). This algorithm can be (slightly tweaked but with success probability still $1 - o(1)$) and used in Regev's reduction to solve SCP(q, n, k', ω') w.p. $\Theta(1)$ (Section 6.3.2).*

References

[AAB+22a] Carlos Aguilar Melchor, Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Santosh Ghosh, Shay Gueron, Tim Güneysu, Rafael Misoczki, Edoardo Persichetti, Jan Richter-Brockmann, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur, and Gilles Zémor. BIKE. Round 4 Submission to the NIST Post-Quantum Cryptography Call, v. 5.1, October 2022.

[AAB+22b] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jurjen Bos, Jean-Christophe Deneuville, Arnaud Dion, Philippe Gaborit, Jérôme Lacan, Edoardo Persichetti, Jean-Marc Robert, Pascal Véron, Gilles Zémor, and Jurjen Bos. HQC. Round 4 Submission to the NIST Post-Quantum Cryptography Call, October 2022. `https://pqc-hqc.org/`.

[ABC+22] Martin Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Mizoczki, Ruben Niederhagen, Edoardo Persichetti, Kenneth Paterson, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wang Wen. Classic McEliece (merger of Classic McEliece and NTS-KEM). `https://classic.mceliece.org`, November 2022. Fourth round finalist of the NIST post-quantum cryptography call.

[AG11] Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors. In Luca Aceto, Monika Henzinger, and Jiří Sgall, editors, *Automata, Languages and Programming*, volume 6755 of *LNCS*, pages 403–415. Springer Berlin Heidelberg, 2011.

[AHI+17] Benny Applebaum, Naama Haramaty, Yuval Ishai, Eyal Kushilevitz, and Vinod Vaikuntanathan. Low-complexity cryptographic hash functions. In *ITCS*, volume 67 of *LIPIcs*, pages 7:1–7:31. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017.

[Ajt96] Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 99–108. ACM, 1996.

[Ale11] Michael Alekhnovich. More on average case vs approximation complexity. *Computational Complexity*, 20(4):755–786, 2011.

[Ber10] Daniel J. Bernstein. Grover vs. McEliece. In Nicolas Sendrier, editor, *Post-Quantum Cryptography 2010*, volume 6061 of *LNCS*, pages 73–80. Springer, 2010.

[BJLM13] Daniel J. Bernstein, Stacey Jeffery, Tanja Lange, and Alexander Meurer. Quantum algorithms for the subset-sum problem. In *Post-Quantum Cryptography 2011*, volume 7932 of *LNCS*, pages 16–33, Limoges, France, June 2013.

[BJMM12] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In *Advances in Cryptology - EUROCRYPT 2012*, LNCS. Springer, 2012.

[BK02] H. Barnum and E. Knill. Reversing quantum dynamics with near-optimal quantum and classical fidelity. *Journal of Mathematical Physics*, 43(5):2097–2106, 04 2002.

[BKMH97] Masahi Ban, Keiko Kurokawa, Rei Momose, and Osamu Hirota. Optimum measurements for discrimination among symmetric quantum states and parameter estimation. *International Journal of Theoretical Physics*, 36(6):1269–1288, 1997.

[BKW03] Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM (JACM)*, 50(4):506–519, 2003.

[BLVW19] Zvika Brakerski, Vadim Lyubashevsky, Vinod Vaikuntanathan, and Daniel Wichs. Worst-case hardness for LPN and cryptographic hashing via code smoothing. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *LNCS*, pages 619–635. Springer, 2019.

[BM17] Leif Both and Alexander May. Optimizing BJMM with Nearest Neighbors: Full Decoding in $2^{2/21n}$ and McEliece Security. In *WCC Workshop on Coding and Cryptography*, September 2017.

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In Rafail Ostrovsky, editor, *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 97–106. IEEE Computer Society, 2011.

[CB98] Anthony Chefles and Stephen M. Barnett. Optimum unambiguous discrimination between linearly independent symmetric states. *Physics Letters A*, 250(4):223–229, 1998.

[CDMT22] Kevin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger, and Jean-Pierre Tillich. Statistical decoding 2.0: Reducing decoding to LPN. In *Advances in Cryptology - ASIACRYPT 2022*, LNCS. Springer, 2022.

[CL21] André Chailloux and Johanna Loyer. Lattice sieving via quantum random walks. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part IV*, volume 13093 of *Lecture Notes in Computer Science*, pages 63–91. Springer, 2021.

[CLZ22] Yilei Chen, Qipeng Liu, and Mark Zhandry. Quantum algorithms for variants of average-case lattice problems via filtering. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *LNCS*, pages 372–401. Springer, 2022.

[Deb23] Thomas Debris-Alazard. Code-based cryptography: Lecture notes, arxiv cs.cr 2304.03541, 2023.

[Din07] Irit Dinur. The PCP theorem by gap amplification. *J. ACM*, 54(3):12, 2007.

[DR22] Thomas Debris-Alazard and Nicolas Resch. Worst and average case hardness of decoding via smoothing bounds. preprint, December 2022. eprint.

[DRT23] Thomas Debris-Alazard, Maxime Remaud, and Jean-Pierre Tillich. Quantum reduction of finding short code vectors to the decoding problem. preprint (v2), June 2023. arXiv:2106.02747.

[Dum89] Il'ya Dumer. Two decoding algorithms for linear codes. *Probl. Inf. Transm.*, 25(1):17–23, 1989.

[FS96] Jean-Bernard Fischer and Jacques Stern. An efficient pseudo-random generator provably as secure as syndrome decoding. In Ueli Maurer, editor, *Advances in Cryptology - EUROCRYPT'96*, volume 1070 of *LNCS*, pages 245–255. Springer, 1996.

[GGR98] Oded Goldreich, Shafi Goldwasser, and Dana Ron. Property testing and its connection to learning and approximation. *J. ACM*, 45(4):653–750, 1998.

[GVW13] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 545–554. ACM, 2013.

[KT17] Ghazal Kachigar and Jean-Pierre Tillich. Quantum information set decoding algorithms. In *Post-Quantum Cryptography 2017*, volume 10346 of *LNCS*, pages 69–89, Utrecht, The Netherlands, June 2017. Springer.

[Laa16] Thijs Laarhoven. *Search problems in cryptography*. PhD thesis, Eindhoven University of Technology, 2016.

[Lev87] Leonid A Levin. One way functions and pseudorandom generators. *Combinatorica*, 7(4):357–363, 1987.

[LMvdP15] Thijs Laarhoven, Michele Mosca, and Joop van de Pol. Finding shortest lattice vectors faster using quantum search. *Des. Codes Cryptogr.*, 77(2-3):375–400, 2015.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[Lyu05] Vadim Lyubashevsky. The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem. In Chandra Chekuri, Klaus Jansen, José D. P. Rolim, and Luca Trevisan, editors, *Approximation, Randomization and Combinatorial Optimization, Algorithms and Techniques, 8th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2005 and 9th InternationalWorkshop on Randomization and Computation, RANDOM 2005, Berkeley, CA, USA, August 22-24, 2005, Proceedings*, volume 3624 of *Lecture Notes in Computer Science*, pages 378–389. Springer, 2005.

[McE78] Robert J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[MMT11] Alexander May, Alexander Meurer, and Enrico Thomae. Decoding random linear codes in $O(2^{0.054n})$. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 107–124. Springer, 2011.

[MO15] Alexander May and Ilya Ozerov. On computing nearest neighbors with applications to decoding of binary linear codes. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 203–228. Springer, 2015.

[Mon06] Ashley Montanaro. On the distinguishability of random quantum states. *Communications in Mathematical Physics*, 273, 07 2006.

[MTSB12] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. MDPC-McEliece: New McEliece variants from moderate density parity-check codes, 2012.

[Pra62] Eugene Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5):5–9, 1962.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93, 2005.

[Sha48] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3):379–423, 1948.

[Sha79] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[SSTX09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, volume 5912 of *LNCS*, pages 617–635. Springer, 2009.

[Ste88] Jacques Stern. A method for finding codewords of small weight. In G. D. Cohen and J. Wolfmann, editors, *Coding Theory and Applications*, volume 388 of *LNCS*, pages 106–113. Springer, 1988.

[Ste93] Jacques Stern. A new identification scheme based on syndrome decoding. In D.R. Stinson, editor, *Advances in Cryptology - CRYPTO'93*, volume 773 of *LNCS*, pages 13–21. Springer, 1993.

[YZ22] Takahashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. In *63rd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2022, Denver, CO, USA, October 31 - November 3, 2022*, pages 69–74. IEEE, 2022.

[YZW+19] Yu Yu, Jiang Zhang, Jian Weng, Chun Guo, and Xiangxue Li. Collision resistant hashing from sub-exponential learning parity with noise. In *ASIACRYPT (2)*, volume 11922 of *Lecture Notes in Computer Science*, pages 3–24. Springer, 2019.

A General phases

We consider more general error functions $f(\boldsymbol{e}) = \sqrt{1-t}^{(n-|\boldsymbol{e}|)}(e^{i\theta}\sqrt{t})^{|\boldsymbol{e}|}$ with $t \in [0, \frac{1}{2}]$ and $\theta \in [0, 2\pi)$, which means we consider the states

$$|\psi_f(\boldsymbol{c})\rangle = \sum_{\boldsymbol{e}\in\{0,1\}^n} f(\boldsymbol{e})|\boldsymbol{c}+\boldsymbol{e}\rangle = \bigotimes_{i=1}^{n} \sqrt{1-t}|c_i\rangle + e^{i\theta}\sqrt{t}|1-c_i\rangle.$$

Again, we consider unambiguous states discrimination between the following two states

$$|\zeta_0\rangle = \sqrt{1-t}|0\rangle + e^{i\theta}\sqrt{t}|1\rangle \quad ; \quad |\zeta_1\rangle = e^{i\theta}\sqrt{t}|0\rangle + \sqrt{1-t}|1\rangle.$$

We have $|\langle\zeta_0|\zeta_1\rangle| = |\sqrt{t(1-t)}(e^{i\theta} + e^{-i\theta})| = 2\sqrt{t(1-t)}|\cos(\theta)|$. From there, we have that decoding with this unambiguous measurement is possible w.h.p as long as

$$1 - 2\sqrt{t(1-t)}|\cos(\theta)| > \frac{k}{n} \tag{34}$$

Now, what do we get in the dual? Let

$$|\psi_f\rangle = \frac{1}{\sqrt{Z}} \sum_{\boldsymbol{c}\in\mathcal{C},\boldsymbol{e}\in\{0,1\}^n} f(\boldsymbol{e})|\boldsymbol{c}+\boldsymbol{e}\rangle$$

where Z is a normalizing constant. We write

$$\widehat{|\psi_f\rangle} = \frac{2^k}{\sqrt{2^n \cdot Z}} \sum_{\boldsymbol{y}\in\mathcal{C}^\perp} \hat{f}(\boldsymbol{y})|\boldsymbol{y}\rangle.$$

Moreover, we write

$$\widehat{|\zeta_0\rangle} = \frac{1}{\sqrt{2}}\left(\sqrt{1-t} + e^{i\theta}\sqrt{t}\right)|0\rangle + \frac{1}{\sqrt{2}}\left(\sqrt{1-t} - e^{i\theta}\sqrt{t}\right)|1\rangle$$
$$\widehat{|\zeta_1\rangle} = \frac{1}{\sqrt{2}}\left(\sqrt{1-t} + e^{i\theta}\sqrt{t}\right)|0\rangle - \frac{1}{\sqrt{2}}\left(\sqrt{1-t} - e^{i\theta}\sqrt{t}\right)|1\rangle$$

This means that $\hat{f}(\boldsymbol{y}) = \frac{1}{\sqrt{2}}\left(\sqrt{1-t} + e^{i\theta}\sqrt{t}\right)^{(n-|\boldsymbol{y}|)} \frac{1}{\sqrt{2}}\left(\sqrt{1-t} - e^{i\theta}\sqrt{t}\right)^{|\boldsymbol{y}|}$. The probability $p(t,\theta)$ to measure 1 on each coordinate in the above is given by

$$p(t,\theta) = \frac{1}{2}\left|\sqrt{1-t} - e^{i\theta}\sqrt{t}\right|^2 = \frac{1}{2}\left((\sqrt{1-t} - \sqrt{t}\cos(\theta))^2 + t\sin^2(\theta)\right) \tag{35}$$
$$= \frac{1}{2}\left(1 - 2\sqrt{t(1-t)}\cos(\theta)\right) \tag{36}$$

In the case Equation 34 is saturated, meaning $1 - 2\sqrt{t(1-t)}|\cos(\theta)| \approx \frac{k}{n}$, we have $p(t,\theta) = \frac{k}{2n}$ as long as $\cos(\theta) \geq 0$ (otherwise, we have the symmetric for large weights) which is Prange's bound. Notice that the above only works when Equation 34 can be saturated, so we can not take $\theta = \pi/2$ for example.