A Deterministic Reduction for the Gap Minimum Distance Problem

Qi Cheng and Daqing Wan

***Abstract*—Determining the minimum distance of a linear code is one of the most important problems in algorithmic coding theory. The exact version of the problem was shown to be NP-complete in [15]. In [9], the gap version of the problem was shown to be NP-hard for any constant factor under a randomized reduction. It was shown in the same paper that the minimum distance problem is not approximable in randomized polynomial time to the factor $2^{\log^{1-\epsilon} n}$ unless $NP \subseteq RTIME(2^{polylog(n)})$. In this paper, we derandomize the reduction and thus prove that there is no deterministic polynomial time algorithm to approximate the minimum distance to any constant factor unless $P = NP$. We also prove that the minimum distance is not approximable in deterministic polynomial time to the factor $2^{\log^{1-\epsilon} n}$ unless $NP \subseteq DTIME(2^{polylog(n)})$. As the main technical contribution, for any constant $2/3 < \rho < 1$, we present a deterministic algorithm that given a positive integer s, runs in time $poly(s)$ and constructs a code $\mathcal{C}$ of length $poly(s)$ with an explicit Hamming ball of radius $\rho d(\mathcal{C})$, such that the projection at the first s coordinates sends the codewords in the ball surjectively onto a linear subspace of dimension s, where $d(\mathcal{C})$ denotes the minimum distance of $\mathcal{C}$. The codes are obtained by concatenating Reed-Solomon codes with Hadamard codes.**

***Index Terms*—Coding theory, NP-complete, approximation algorithm, minimum distance problem.**

I. Introduction

In the theory of computational complexity, a (Karp) reduction from a language A to another language B is a transformation f, such that $x \in A$ if and only if $f(x) \in B$. After the fundamental work of Cook [8], polynomial time reductions are systematically used to identify complete problems for classes of computational problems. As there is still no separation between P and many supposedly larger classes such as $PSPACE$, we rely on reductions to order the intractability of computational problems.

Ideally, one would like reductions to be deterministic, but sometimes deterministic reductions are hard to find, in which case randomized reductions become useful. In general, a randomized reduction is a randomized algorithm which maps strings in A to strings in B with high probability, and maps strings not in A to strings not in B with high probability. The probability in the randomized reductions is over the random coins in the reduction and not over the inputs. For example, no deterministic reduction from a NP-complete problem has been found for the shortest vector problem of integer lattices in L_2 norm, but it was shown to be NP-hard by Ajtai [1] in 1998 under a randomized reduction. His work was later refined in [5], [12] to show the hardness of approximating the shortest vector problem, again under randomized reductions. In those reductions, for any positive integer s, a gadget is constructed which includes an integer lattice of dimension $poly(s)$, a ball of radius less than the length of shortest vectors but containing many lattice points and a linear map which sends the lattice points in the ball *onto* $\{0,1\}^s$. Randomized algorithms have to be deployed to find the center of the ball and the surjective linear map. Derandomizing the reductions is a long standing open problem in computational complexity. This can be done conditionally [12] assuming certain smooth number conjecture which is unfortunately hopeless to be proven at present.

The shortest vector problem of integer lattices corresponds to the minimum distance problem of linear codes in coding theory. A linear code $\mathcal{C}$ of length n and rank k over a finite field $\mathbf{F}_q$ is a k-dimensional linear subspace of $\mathbf{F}_q^n$. It is usually represented by a (generating) matrix in $\mathbf{F}_q^{n\times k}$, whose column vectors form a base of the code. For two vectors $\mathbf{x}, \mathbf{y}$ in $\mathbf{F}_q^n$, the Hamming distance $d(\mathbf{x}, \mathbf{y})$ is defined to be the number of positions where these two vectors differ. The minimum distance of the code, denoted by $d(\mathcal{C})$, is defined to be the minimum Hamming distance between any two distinct codewords. It equals the minimum weight of nonzero codewords. The distance of a vector $\mathbf{x} \in \mathbf{F}_q^n$ to the code $\mathcal{C}$, denoted by $d(\mathbf{x}, \mathcal{C})$, is defined to be $\min_{\mathbf{y}\in\mathcal{C}} d(\mathbf{x}, \mathbf{y})$. A Hamming ball with center $\mathbf{c} \in \mathbf{F}_q^n$ and radius r, denoted by $\mathcal{B}(\mathbf{c}, r)$, is defined to be the set of vectors within distance r from $\mathbf{c}$, namely,

$$\mathcal{B}(\mathbf{c}, r) = \{\mathbf{x} \in \mathbf{F}_q^n | d(\mathbf{x}, \mathbf{c}) \le r\}.$$

The minimum distance problem of linear codes was proven to be NP-complete [15] in 1997 under a deterministic reduction. Approximating the minimum distance of a linear code was proved to be NP-hard [9] for any constant factor, under a randomized reduction. More precisely the reduction in [9] is *a reverse unfaithful random reduction*, which maps YES instances of an NP-complete problem to YES instances in the gap version of the minimum distance problem with high probability and always maps NO instances to NO instances.

The research was done while the authors were visiting the Center for Advanced Study of Tsinghua University. We thank Professor Xiaoyun Wang and her group for the hospitality. The second author would also like to thank the Institute of Mathematics at the Chinese Academy of Sciences for its hospitality. The preliminary version of this paper appeared in the Proceedings of the 41st ACM Symposium on Theory of Computing (STOC 2009).

Qi Cheng is with School of Computer Science, University of Oklahoma, Norman, OK73019, Email: qcheng@cs.ou.edu. His research is partially supported by NSF grant CCF-0830524 and CCF-0830522.

Daqing Wan is with Department of Mathematics, University of California, Irvine, CA 92697-3875, Email: dwan@math.uci.edu. His research is partially supported by NSF.

Definition 1.1: For a prime power q and $\gamma \geq 1$, an instance of the Gap Minimum Distance Problem $GapMDP_{q,\gamma}$ is a linear code $\mathcal{C}$ over $\mathbf{F}_q$, given by its generating matrix, and an integer t such that

- it is a YES instance if $d(\mathcal{C}) \leq t$;
- it is a NO instance if $d(\mathcal{C}) > \gamma t$,

A related problem, the Relatively Near Codeword Problem, was also proved to be NP-hard by a randomized reduction.

Definition 1.2: For a prime power q, real number $\rho > 0$ and $\gamma \geq 1$, an instance of the Gap Relatively Near Codeword Problem $GapRNC^{(\rho)}_{q,\gamma}$ is a linear code $\mathcal{C}$ of length n over $\mathbf{F}_q$, given by its generating matrix, a vector $\mathbf{v} \in \mathbf{F}_q^n$ and a positive integer t such that $t \leq \rho d(\mathcal{C})$

- it is a YES instance if $d(\mathbf{v}, \mathcal{C}) \leq t$;
- it is a NO instance if $d(\mathbf{v}, \mathcal{C}) > \gamma t$,

The reduction in [9] adopted some ideas in the work on the shortest vector problem [1], [12], and used randomness in a similar way in two steps:

- For certain codes, a randomized algorithm finds the center of a Hamming ball which has a radius smaller than the minimum distance by a constant factor less than 1 but contains subexponentially many codewords.
- Randomness is needed to find a linear map which sends the codewords in the Hamming ball **onto** a linear subspace of given dimension.

In both places, it was proved that random objects satisfy the required properties with high probability. More precisely it was proved in [9]

Proposition 1.3: (A rephrasing of Lemma 15 in [9]) Let q be a prime power and $1/2 < \rho < 1$ be a constant. There exists a randomized algorithm that given an integer s, runs in time $poly(s)$ and constructs a linear code $\mathcal{C}$ over $\mathbf{F}_q$ of length $n = poly(s)$, a vector $\mathbf{w} \in \mathbf{F}_q^n$ and a linear map τ from $\mathbf{F}_q^n$ to $\mathbf{F}_q^s$ such that with probability at least $1 - 1/q^{-s}$

$$\tau(\mathcal{B}(\mathbf{w}, \rho d(\mathcal{C})) \cap \mathcal{C}) = \mathbf{F}_q^s.$$

Sometimes a random object possesses a certain property but it is hard to construct an object with the property in a deterministic manner. It is a recurring theme in combinatorics and algorithm design, and poses a challenge for the derandomization research. It is related to the P vs. RP problem, one of the central questions on computational complexity.

Like the exact version of the shortest vector problem in L_2 norm, the gap version for lattices was proved to be NP-hard to any constant factor under randomized reductions in [11], [10]. It is interesting to contrast these problems with the inhomogeneous versions, namely, the closest vector problems in L_2 norm for integer lattices and the maximum likelihood decoding problems for linear codes. Both problems were known to be NP-complete since the early eighties [14], [4], and there are inapproximability results under deterministic reductions [2]. Their homogeneous versions turn out to be significantly harder to study.

A. Our results

The work in [9] left open a problem whether a deterministic reduction can be found to prove the NP-completeness of the gap version of the minimum distance problem. In this paper, we answer the question affirmatively. We start by defining Reed-Solomon codes.

Notation 1.4: Suppose f is a function defined over a field F and let S be a subset of F. We use $(f)_{x \in S}$ to denote the vector $(f(C_1), f(C_2), \cdots, f(C_s))$, where $C_1, C_2, \cdots, C_s$ is a prefixed ordering of elements in S.

Definition 1.5: Let q be a prime power. The (extended) Reed-Solomon code of dimension k, denoted by $RS[q,k]$, consists of all the vectors $(f(x))_{x \in \mathbf{F}_q}$ where $f \in \mathbf{F}_q[x]$ is a polynomial of degree at most $k-1$.

It is well-known that the minimum distance of $RS[q,k]$ is $q - k + 1$. Let ρ be a real number in $(1/2, 1)$. By an averaging argument, one can show that for Reed-Solomon codes of rate approaching one, there exist Hamming balls of radius ρd containing subexponentially codewords, where d is the distance of the code. In [7], we show that for $\rho \in (2/3, 1)$, such Hamming balls can be found in a deterministic manner. Continuing this line of research, in this paper, we present a deterministic reduction from an NP-complete problem to the Gap Minimum Distance Problem for any constant factor, and to the Gap Relatively Near Codeword Problem with $\rho > 2/3$, thus finalizing the NP-completeness proofs of both problems. We achieve this by an in-depth study of codewords inside balls constructed in [7], as the balls are explicit and more information is available to us. As a result, we show that in fact, for a certain code over $\mathbf{F}_q$ that is a concatenation of a Reed-Solomon code over $\mathbf{F}_{q^e}$ with a Hadamard code, a suitable *projection* is enough to send the codewords in the balls surjectively onto a linear subspace. This essentially derandomizes Lemma 15 in [9] (Proposition 1.3) with $\rho > 2/3$. Our main technical contribution is the following theorem.

Theorem 1.6: Let q be a prime power and $2/3 < \rho < 1$ be a constant. There exists a deterministic algorithm that given an integer s, runs in time $poly(s)$ and constructs a linear code $\mathcal{C}$ over $\mathbf{F}_q$ of length $n = poly(s)$, and a vector $\mathbf{w} \in \mathbf{F}_q^n$ such that

$$\pi_{1,2,\cdots,s}(\mathcal{B}(\mathbf{w}, \rho d(\mathcal{C})) \cap \mathcal{C}) = \mathbf{F}_q^s,$$

where $\pi_{i_1,i_2,\cdots,i_j}$ denotes the projection at coordinates $i_1, i_2, \cdots, i_j$.

Since a Hamming ball of radius r contains at most

$$\sum_{0 \leq i \leq r} \binom{n}{i} (q-1)^i < (r+1)(n(q-1))^r < (poly(s))^r$$

many codewords, the above projection shows that the Hamming ball $\mathcal{B}(\mathbf{w}, \rho d(\mathcal{C}))$ contains at least q^s many codewords, thus has radius at least $\Omega(s/\log s)$. As pointed out in [9], we can then deduce the following corollaries from Theorem 1.6.

Corollary 1.7: The minimum distance problem cannot be approximated by a deterministic polynomial time algorithm to any constant factor greater than one unless $NP = P$. It is not approximable by a deterministic polynomial time algorithm to the factor $2^{\log^{1-\epsilon} n}$ unless $NP \subseteq DTIME(2^{polylog(n)})$.

Corollary 1.8: For any $\rho > 2/3$, any prime power q and any $\gamma \geq 1$, the Gap Relatively Near Codeword Problem $GapRNC^{(\rho)}_{q,\gamma}$ is NP-complete.

B. Technique overview

Let q be a fixed prime power. Let $\mathbf{h}(x)$ be a monic polynomial over $\mathbf{F}_{q^e}$ of degree $h \geq 2$. Given $f(x) \in \mathbf{F}_{q^e}[x]$ and an integer $g > h$ with $\deg(f) < g$ and $\gcd(f(x), \mathbf{h}(x)) = 1$, we denote by $T_{\mathbf{h},g}(f)$ the set of monic polynomials $t(x) \in \mathbf{F}_{q^e}[x]$ of degree $g-h$, such that $f(x) + t(x)\mathbf{h}(x)$ can be factored completely into g distinct linear factors in $x + \mathbf{F}_{q^e}$. Finding a good lower bound for the cardinality of $T_{\mathbf{h},g}(f)$ lies at the heart of this work for the following reasons:

- The cardinality of the set is equal to the number of codewords inside a Hamming ball of radius $q^e - g$ and centered at a vector easily obtained from f and $\mathbf{h}$.
- Related problems such as counting primes or smooth numbers in arithmetic progressions, and counting irreducible polynomials which are congruent to $f(x)$ modulo $\mathbf{h}(x)$, have been well-studied. Classical mathematical tools, e.g. the Weil character sum bound, have been developed to tackle this type of problems.

For example, we proved in the paper [6] that if

$$g = (2+\epsilon)h \quad \text{and} \quad q^e = h^{\Omega(1/\epsilon)},$$

then for every nonzero $f(x)$ of degree less than h, $|T_{\mathbf{h},g}(f)| \geq q^{g/2}$. By a duality argument, we can obtain a similar bound for $T_{\mathbf{h},q^e-g}(f)$. This allows us to construct deterministically Hamming balls containing many codewords in Reed-Solomon codes $RS[q^e, q^e - g - h]$ of rate approaching 1, of which the ratio between the radius and the distance, i.e. $\frac{g}{g+h}$, falls in $(2/3, 1)$.

Remark 1.9: For $\rho \in (1/2, 2/3]$, one can also show by an averaging argument that there exist Hamming balls of radius ρd containing many codewords for some Reed-Solomon codes of distance d. However, to deterministically find such a Hamming ball requires substantially new ideas, as our proof does not work if $g/h < 2$.

Based on the above results and a standard technique of concatenating codes, we reduce Theorem 1.6 to show that under certain conditions, $T_{\mathbf{h},g}(f)$ is not only nonempty, but also fairly big. More precisely we will prove that for any small subset S of $\mathbf{F}_{q^e}$ of cardinality s, and any $\mathbf{F}_q$-linear surjective map τ from $\mathbf{F}_{q^e}$ to $\mathbf{F}_q$, if we evaluate polynomials in $T_{\mathbf{h},g}(f)$ at elements in S to produce

$$\{(t(x))_{x\in S} | t \in T_{\mathbf{h},g}(f)\} \subseteq (\mathbf{F}_{q^e})^s,$$

and then apply the linear map τ on the set, we get the full linear space $\mathbf{F}_q^s$. Note that the cardinality of $T_{\mathbf{h},g}(f)$ must be greater than q^s. To prove the statement, we will use the Weil bound in the residue class ring $\mathbf{F}_{q^e}[x]/(\mathbf{h}(x)\prod_{c\in S}(x-c))$. Though this ring is not a field, the powerful Weil bound can be applied without much change. Together with an inclusion-exclusion sieving argument, one can then show the desired property of $T_{\mathbf{h},g}(f)$ if q^e is polynomial in s, and $g = (2+\epsilon)h$. This gives us favorable parameters for our present coding theory applications.

II. Mathematical preparation

To simplify the notations, we shall replace q^e with q in this section. Let $\mathbf{h}(x) \in \mathbf{F}_q[x]$ have degree $h > 1$. For an integer $g > h$, and $f(x) \in \mathbf{F}_q[x]$ of degree less than g, we use $T_{\mathbf{h},g}(f)$ to denote the set of monic polynomials $t(x) \in \mathbf{F}_q[x]$ of degree $g-h$, such that $f(x) + t(x)\mathbf{h}(x)$ can be factored completely as a product of g distinct factors in $x + \mathbf{F}_q$. In our earlier paper [6], we proved that under certain conditions on q, h and g, $|T_{\mathbf{h},g}(f)| > 0$ if $\mathbf{h}$ is irreducible and f is not a zero polynomial. The main purpose of this section is to generalize this result. We prove that under the same conditions on q, h and g, $|T_{\mathbf{h},g}(f)| > 0$ if f is invertible in $\mathbf{F}_q[x]/(\mathbf{h}(x))$. Note that $\mathbf{h}(x)$ may be a reducible polynomial.

Theorem 2.1: Let $\mathbf{h}(x) \in \mathbf{F}_q[x]$ be a non-zero polynomial of degree $h > 1$. Assume that

$$q > \max(g^2, h^{2+\frac{4}{\epsilon}}),\ g \geq (2+\epsilon)(h+1)$$

for some constant $\epsilon > 0$. Then, every element β in the multiplicative residue group $(\mathbf{F}_q[x]/\mathbf{h}(x))^*$ can be written as

$$\beta = \prod_{j=1}^{g}(x - v_j),$$

where $v_j \in \mathbf{F}_q$ are distinct.

By expanding the linear product, the existence of such v_j's can be reduced to the existence of an $\mathbf{F}_q$-rational point of a rather complicated higher dimensional quasi-projective variety defined over $\mathbf{F}_q$, involving many elementary symmetric functions. If this variety is absolutely irreducible (which is often not easy to prove), then one can apply an effective Lang-Weil estimate to obtain the existence of many $\mathbf{F}_q$-rational points if q is sufficiently large. This approach would result in poor parameters for coding theory applications as one needs to assume that q is very large (exponentially large compared to other parameters). For coding theory applications, one needs q to grow only polynomially with other parameters. We shall keep the compact form of the above problem and reduce it to the estimate of various partial character sums along a line in the residue class ring $\mathbf{F}_q[x]/\mathbf{h}(x)$, which is not a field. Via class field theory over function fields, one finds that such partial sums along a line can be interpreted as complete character sums on the affine line, and thus one can use Weil's bound for character sums to get a good estimate.

Proof: Let $\phi(\mathbf{h})$ denote the number of the elements in the group $(\mathbf{F}_q[x]/\mathbf{h}(x))^*$. It is clear that $\phi(\mathbf{h}) < q^h$. Let G be the complex character group of the multiplicative group $(\mathbf{F}_q[x]/\mathbf{h}(x))^*$. If $\chi \in G$, then χ can be extended to a multiplicative map on the full residue class ring $\mathbf{F}_q[x]/\mathbf{h}(x)$ by defining $\chi(\alpha) = 0$ for non-invertible elements α in $\mathbf{F}_q[x]/\mathbf{h}(x)$. If χ is non-trivial, then Weil's character sum bound on the affine line can be simply stated as:

$$|\sum_{v\in\mathbf{F}_q}\chi(x-v)| \leq (h-1)\sqrt{q},$$

see [16] for a fuller exposition of this estimate and its various incarnations.

Let $N_g(\beta)$ denote the number of ordered g-tuple $(v_1, ..., v_g) \in \mathbf{F}_q^g$ with distinct coordinates such that $\beta = \prod_{j=1}^{g}(x - v_j)$. The sum

$$\sum_{\chi\in G}\chi(\alpha)$$

is either $\phi(\mathbf{h})$ or 0 depending on whether α is 1 or not. Thus, we obtain the counting formula

$$N_g(\beta) = \frac{1}{\phi(\mathbf{h})} \sum_{\substack{v_j \in \mathbf{F}_q, \text{distinct} \\ 1 \le j \le g}} \sum_{\chi \in G} \chi(\frac{(x-v_1)\cdots(x-v_g)}{\beta}). \tag{1}$$

Applying the principle of inclusion-exclusion sieving and the inequality $\phi(\mathbf{h}) < q^h$, we deduce

$$N_g(\beta) > \frac{1}{q^h}\{(\sum_{\substack{v_j \in \mathbf{F}_q \\ 1 \le j \le g}} - \sum_{\substack{v_i = v_j \\ 1 \le i < j \le g}}) \sum_{\chi \in G} \chi(\frac{(x-v_1)\cdots(x-v_g)}{\beta})\}$$

$$= \frac{1}{q^h} \sum_{\chi \in G}\{(\sum_{\substack{v_j \in \mathbf{F}_q \\ 1 \le j \le g}} - \sum_{\substack{v_i = v_j \\ 1 \le i < j \le g}})\chi(\frac{(x-v_1)\cdots(x-v_g)}{\beta})\}.$$

The sum over the trivial character in the above formula gives us the main term for $N_g(\beta)$

$$\frac{q^g - \binom{g}{2} q^{g-1}}{q^h}.$$

Using the Weil bound for non-trivial characters to obtain the error term, we have

$$\begin{aligned} N_g(\beta) &> \frac{q^g - \binom{g}{2} q^{g-1}}{q^h} - (1 + \binom{g}{2})(h-1)^g q^{g/2} \\ &= q^{g/2}\left((q - \binom{g}{2}) q^{g/2-1-h} \right. \\ &\quad \left. -(1 + \binom{g}{2})(h-1)^g\right). \end{aligned}$$

In order for $N_g(\beta) > 0$, it suffices to have

$$q - \binom{g}{2} > 1 + \binom{g}{2},\ q^{g/2-1-h} > (h-1)^g.$$

If $q > g^2$, then the first inequality holds. If $q > h^{2+\frac{4}{\epsilon}}$ and $h < \frac{g}{2+\epsilon} - 1$, then

$$\begin{aligned} q^{g/2-1-h} &> (h^{2+\frac{4}{\epsilon}})^{(\frac{g}{2}-1-\frac{g}{2+\epsilon}+1)} \\ &= h^g > (h-1)^g. \end{aligned}$$

This concludes the proof of the theorem. ∎

III. The gadget

In this section, we apply the result of the previous section with $\mathbf{F}_q$ replaced by $\mathbf{F}_{q^e}$. We showed that the set $T_{\mathbf{h},g}(f)$ is not empty under a certain condition on q^e, g and h if $\deg(f) < g$ and $\gcd(f(x), \mathbf{h}(x)) = 1$. In the section, we first show that the set and its dual $T_{\mathbf{h},q^e-g}(f)$ are fairly large in the sense that if we evaluate the polynomials in the sets at a small subset S of $\mathbf{F}_{q^e}$ of cardinality s, then we will get almost all the vectors in $(\mathbf{F}_{q^e})^s$. We reduce the problem to prove that $|T_{\mathbf{h}',g}(f')| > 0$ for some suitable $\mathbf{h}'(x)$ and $f'(x)$ dependent on $\mathbf{h}(x), f(x)$ and S.

Theorem 3.1: Let q be a prime power and $e \ge 2, h \ge 2$ and s be positive integers. Let $S = \{C_1, \cdots, C_s\}$ be a subset of $\mathbf{F}_{q^e}$ of cardinality s and define

$$\pi(x) = \prod_{i=1}^{s}(x - C_i).$$

Let $\mathbf{h}(x) \in \mathbf{F}_{q^e}[x]$ be a monic polynomial of degree h over $\mathbf{F}_{q^e}$ that has no roots in $\mathbf{F}_{q^e}$ and is relatively prime to $\pi(x)$. If

$$q^e > \max((g-s)^2, (h+s)^{2+\frac{4}{\epsilon}}),\ g - s \ge (2+\epsilon)(h+s+1),$$

for some positive integer g and some constant $\epsilon > 0$, then for any $f(x) \in \mathbf{F}_{q^e}[x]$ of degree less than $h+s$ that is relatively prime to $\mathbf{h}(x)\pi(x)$,

$$\begin{aligned} &\{\mathbf{v} \in \mathbf{F}_{q^e}^s | d(\mathbf{v}, (-f(x)/\mathbf{h}(x))_{x \in S}) = s\} \\ \subseteq\ &\{(t(x))_{x \in S} | t(x) \in T_{\mathbf{h}(x), q^e - g}(f)\}. \end{aligned}$$

Proof: For any vector $\mathbf{v} = (v_1, v_2, \cdots, v_s)$ such that

$$d(\mathbf{v}, (-f(x)/\mathbf{h}(x))_{x \in S}) = s,$$

we have $f(C_i) + v_i \mathbf{h}(C_i) \neq 0$, where C_i is the i-th element in the prefixed order of S. Write

$$t(x) = t_1(x) + \pi(x) t_2(x),$$

where $t_1(x) \in \mathbf{F}_{q^e}[x]$ is the unique polynomial of degree smaller than s such that $t_1(C_i) = v_i$ for all $1 \le i \le s$, and $t_2 \in \mathbf{F}_{q^e}[x]$ is a monic polynomial of degree $q^e - g - h - s$, to be determined. Thus, $t(x)$ always satisfies the interpolation $t(C_i) = v_i$ for $1 \le i \le s$.

To prove the theorem, it suffices to show that the congruence

$$f(x) + t_1(x)\mathbf{h}(x) \equiv \prod_{i=1}^{q^e - g} (x - u_i) \pmod{\pi(x)\mathbf{h}(x)},\ u_i \in \mathbf{F}_{q^e}$$

has solutions with the u_i's being distinct. Now, the condition that $\gcd(f(x), \mathbf{h}(x)) = 1$ and the conditions $f(C_i) + v_i \mathbf{h}(C_i) \neq 0$ for all i imply that

$$(f(x) + t_1(x)\mathbf{h}(x), \pi(x)\mathbf{h}(x)) = 1.$$

This also implies that any solution automatically satisfies $u_i \notin S$. One could try to apply the character sum estimate in Theorem 2.1 to the above congruence, but the number $q^e - g$ of linear factors is too large and this would result in poor (useless) parameters. To get around this difficulty, we shall use the "dual" version of the above congruence, which will have a much smaller number of linear factors.

Let

$$W(x) = \prod_{a \in \mathbf{F}_{q^e} - S} (x - a).$$

This is a polynomial in $\mathbf{F}_{q^e}[x]$ relatively prime to $\pi(x)\mathbf{h}(x)$. Dividing $W(x)$ by the above desired congruence, we are reduced to showing that the dual congruence

$$\frac{W(x)}{f(x) + t_1(x)\mathbf{h}(x)} \equiv \prod_{j=1}^{g-s}(x - v_j) \pmod{\pi(x)\mathbf{h}(x)},\ v_j \in \mathbf{F}_{q^e}$$

has solutions with the v_j's being distinct. This dual congruence now has only $g - s$ linear factors. It does have solutions by Theorem 2.1 under the condition

$$q^e > \max((g-s)^2, (h+s)^{2+\frac{4}{\epsilon}}),\ g - s \ge (2+\epsilon)(h+s+1).$$

The theorem is proved. ∎

We now present a deterministic algorithm that given a positive integer s, constructs a linear code $\mathcal{C}$ over $\mathbf{F}_q$, and a

Hamming ball of radius $\rho d(\mathcal{C})$, where $2/3 < \rho < 1$, such that the projection at the first s coordinates maps the codewords inside the Hamming ball surjectively onto $\mathbf{F}_q^s$. The algorithm runs in time $poly(s)$.

Lemma 3.2: Let q be a prime power. Let $2/3 < \rho < 1$ be a constant. There exists a deterministic algorithm that, given an integer $s \geq 2$, constructs a Reed-Solomon code $\mathcal{C}'$ over $\mathbf{F}_{q^e}$ and a received word $\mathbf{w}' \in \mathbf{F}_{q^e}^{q^e}$ such that

- $e = O(\log_q s)$;
- Let A be an element in $\mathbf{F}_{q^e}$ satisfying $\mathbf{F}_q[A] = \mathbf{F}_{q^e}$. Such an A, or more precisely, its minimum polynomial, can be found in deterministic time $poly(qe)$ [13]. For any $(a_1, a_2, \cdots, a_s) \in \mathbf{F}_q^s$, there exist elements $(b_1, b_2, \cdots, b_s) \in \mathbf{F}_q^s$ and $(u_1, u_2, \cdots, u_{q^e-s}) \in \mathbf{F}_{q^e}^{q^e-s}$ such that

$$\begin{aligned} & (b_1A + a_1, b_2A + a_2, \cdots, b_sA + a_s, u_1, \cdots, u_{q^e-s}) \\ \in \quad & \mathcal{C}' \cap \mathcal{B}(\mathbf{w}', \rho d(\mathcal{C}')); \end{aligned}$$

- the minimum distance of $\mathcal{C}'$ is greater than s^2.

Proof: Set $h = s^2$ and $g = \lfloor \frac{\rho h}{1-\rho} \rfloor$. We have

$$\lim_{s\to\infty} \frac{g-s}{h+s+1} = \frac{\rho}{1-\rho} > 2.$$

Thus when s is large enough, we can find a positive constant ϵ, e.g.

$$\epsilon = (\frac{\rho}{1-\rho} - 2)/2 = \frac{3\rho - 2}{2 - 2\rho},$$

so that $g - s \geq (2+\epsilon)(h+s)$. Let e be the least positive integer such that

$$q^e > \max((g-s)^2, (h+s)^{2+\frac{4}{\epsilon}}).$$

It is easy to verify that $e = O(\log_q s)$. Let $C_1, C_2, \cdots, C_{q^e}$ be a natural ordering of elements in $\mathbf{F}_{q^e}$. Now consider the Reed-Solomon code $\mathcal{C}' = RS[q^e, q^e - g - h + 1]$. Find a monic irreducible polynomial $\mathbf{h}(x)$ of degree h over $\mathbf{F}_{q^e}$, which can be done in deterministic time $poly(qeh)$ [13]. Let

$$\mathbf{w}' = (-1/\mathbf{h}(C_1), -1/\mathbf{h}(C_2), \cdots, -1/\mathbf{h}(C_{q^e})).$$

For any $(a_1, a_2, \cdots, a_s) \in \mathbf{F}_q^s$, we can find $(b_1, b_2, \cdots, b_s) \in \mathbf{F}_q^s$ such that

$$1 + (b_iA + a_i)\mathbf{h}(C_i) \neq 0$$

for all $1 \leq i \leq s$. According to Theorem 3.1, taking $f(x) = 1$, there exists a polynomial $t(x)$ of degree $q^e - g - h$, such that

- $1 + t(x)\mathbf{h}(x)$ can be completely split into distinct factors in $x + \mathbf{F}_{q^e}$;
- $t(C_i) = b_iA + a_i$ for some b_i, $1 \leq i \leq s$;

This means that

$$(t(C_1), \cdots, t(C_{q^e}))$$

is a codeword, and it shares at least $q^e - g$ many coordinates with $\mathbf{w}'$. Therefore it is a codeword in the Hamming ball $\mathcal{B}(\mathbf{w}', g)$. The ratio between the radius of the Hamming ball $\mathcal{B}(\mathbf{w}', g)$ and the minimum distance of the Reed-Solomon code is

$$\frac{g}{d(\mathcal{C})} = \frac{g}{g+h} \leq \rho.$$

■

The code we construct above is a Reed-Solomon code, and thus its field size cannot be fixed. Next we use the idea of concatenation with a Hadamard code to obtain a code in a fixed field. An element in $\mathbf{F}_{q^e}$ can be represented uniquely as $a_0 + a_1A + \cdots + a_{e-1}A^{e-1}$ with $a_i \in \mathbf{F}_q$ for all $0 \leq i \leq e-1$. Define the map

$$\phi : \mathbf{F}_{q^e} \to \mathbf{F}_q^{q^e}$$

by sending $a_0 + a_1A + \cdots + a_{e-1}A^{e-1}$ to a vector in $\mathbf{F}_q^{q^e}$ that consists of evaluations of the multilinear polynomial

$$a_0x_0 + a_1x_1 + \cdots + a_{e-1}x_{e-1} \tag{2}$$

at all the points in $\mathbf{F}_q^e$. Without loss of generality, we assume that the first position of $\phi(a_0 + a_1A + \cdots + a_{e-1}A^{e-1})$ is the evaluation of (2) at $(1, 0, \cdots, 0)$, so

$$\pi_1(\phi(a_0 + a_1A + \cdots + a_{e-1}A^{e-1})) = a_0.$$

It is easy to see that $d(\phi(u), \phi(v)) = q^{e-1}(q-1)$ if $u \neq v$, because two distinct hyperplanes of dimension e intersect at a hyperplane of dimension $e-1$. We extend ϕ to vectors over $\mathbf{F}_{q^e}$ by letting ϕ act on each coordinate, namely,

$$\phi(v_1, v_2, \cdots, v_n) = (\phi(v_1), \phi(v_2), \cdots, \phi(v_n)),$$

where $v_i \in \mathbf{F}_{q^e}$ for $1 \leq i \leq n$.

Proof: (of Theorem 1.6): Let $\mathcal{C}'$ be the code constructed in Lemma 3.2. We define a code

$$\mathcal{C}'' = \{(\phi(v_1), \phi(v_2), \cdots, \phi(v_{q^e}))|(v_1, v_2, \cdots, v_{q^e}) \in \mathcal{C}'\}.$$

It is easy to verify that $\mathcal{C}''$ is a linear code of length $(q^e)^2$ and minimum distance $q^{e-1}(q-1)d(\mathcal{C}')$. Let $\mathbf{w}'' = \phi(\mathbf{w}')$. For any $(a_1, a_2, \cdots, a_s) \in \mathbf{F}_q^s$, there exists $(b_1, b_2, \cdots, b_s) \in \mathbf{F}_q^s$ such that a codeword $\mathbf{c}'$ in $\mathcal{B}(\mathbf{w}', \rho d(\mathcal{C}'))$ has $a_i + Ab_i$ as the i-th coordinates for $1 \leq i \leq s$. Then $\mathbf{c}'' = \phi(\mathbf{c}')$ is a codeword in the ball $\mathcal{B}(\mathbf{w}'', \rho d(\mathcal{C}''))$, and

$$\pi_{1,1+q^e,1+2q^e\cdots,1+(s-1)q^e}(\mathbf{c}'') = (a_1, a_2, \cdots, a_s).$$

Therefore, rearranging the coordinates of $\mathcal{C}''$ and $\mathbf{w}''$ will produce a code $\mathcal{C}$ and $\mathbf{w}$ satisfying the requirements. ■

IV. The reduction

In this section we reduce the gap maximum likelihood decoding problem with a large factor to the gap minimum distance problem with the factor close to $3/2$. Though the idea is adopted from [9], we include a proof here for completeness. To boost the gap from $3/2$ to any constant, one applies the standard technique of using tensor product codes. For details see [9].

Definition 4.1: For a prime power q and a real constant $\gamma > 1$, an instance of the gap maximum likelihood decoding problem $GapMLP_{q,\gamma}$ is a linear code $\mathcal{C}$, given by its generating matrix, a received word $\mathbf{v}$ and an integer t, such that

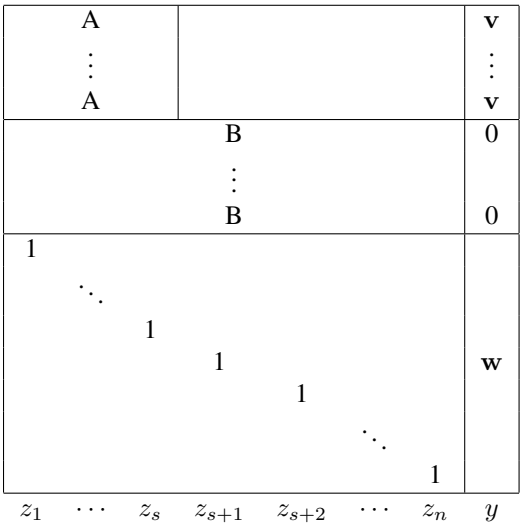
- it is a YES instance if $d(\mathbf{v}, \mathcal{C}) \leq t$;
- it is a NO instance if $d(\mathbf{v}, \mathcal{C}) > \gamma t$.

The following theorem was proved in [2].

Theorem 4.2: For any prime power q and constant $\gamma > 1$, there is a polynomial time deterministic reduction from 3SAT to $GapMLP_{q,\gamma}$.

Theorem 4.3: Let q be a prime power. There exists a deterministic polynomial time reduction from the gap maximum likelihood decoding problem over $\mathbf{F}_q$ with factor γ to the gap version of the minimum distance problem of linear codes with factor $\gamma' = 3/2 + O(1/\gamma)$.

Proof: Given an instance of the gap maximum likelihood decoding problem $(\mathcal{C}, \mathbf{v}, t)$, let $A \in \mathbf{F}_q^{l\times s}$ be the generator matrix for $\mathcal{C}$. Set $s' = \max(s, \gamma t)$, and let B be the *parity check matrix* for the code $\mathcal{C}_1$ constructed in Theorem 1.6 with input s', and let $\mathbf{w}$ be the center of the Hamming ball with many codewords. Denote the length of $\mathcal{C}_1$ by n and $d(\mathcal{C}_1)$ by d. Note that $d \geq (s')^2 \geq (\gamma t)^2$ and the matrix B has size $poly(s')$. Let $\mathcal{C}_2$ be the code with the following generator matrix M:



where the number of A's is $\lceil \frac{d}{\gamma t} \rceil$ and the number of B's is d. Now consider a nonzero codeword $\mathbf{c}$ generated by the column vectors of M with $z_1, \cdots, z_n, y$ as the coefficients.

$$\mathbf{c} = (\overbrace{A(z_1, z_2, \cdots, z_s)^T, \cdots}^{\lceil d/(\gamma t)\rceil}, \overbrace{B(z_1, z_2, \cdots, z_n)^T, \cdots}^{d}, \overbrace{z_1, z_2, \cdots, z_n}^{\lceil d/(\gamma t)\rceil}) + y(\overbrace{\mathbf{v}, \cdots}^{}, 0, \cdots, \mathbf{w})$$

If the gap maximum likelihood decoding problem is YES instance, then there exists a vector $(z_1, \cdots, z_s) \in \mathbf{F}_q^s$ such that

$$d(A(z_1, \cdots, z_s)^T, \mathbf{v}) \leq t.$$

According to Theorem 1.6, we can find $(z_{s+1}, \cdots, z_n) \in \mathbf{F}_q^{n-s}$ so that $(z_1, \cdots, z_n)$ is a codeword of $\mathcal{C}_1$ in the Hamming ball centered at $\mathbf{w}$ and of radius $2d/3$. Let $y = -1$. We can verify that the weight of $\mathbf{c}$ is at most

$$2d/3 + t\lceil d/(\gamma t)\rceil = (2/3 + O(1/\gamma))d.$$

Now assume that the gap maximum likelihood decoding problem is a NO instance. We want to show that $\mathbf{c}$ has a weight at least d. If $y = 0$, then $z_1, \cdots, z_n$ cannot be all zeros. If $(z_1, \cdots, z_n) \notin \mathcal{C}_1$, then

$$B(z_1, z_2, \cdots, z_n)^T \neq 0,$$

so the weight of $\mathbf{c}$ is at least d, as there are d many B's. If $(z_1, \cdots, z_n) \in \mathcal{C}_1$, then its weight is at least d, so is the weight of $\mathbf{c}$.

If $y \neq 0$, w.l.o.g, assume that $y = -1$. Then the weight of $\mathbf{c}$ would be at least $\gamma t\lceil \frac{d}{\gamma t} \rceil \geq d$.

In summary, the ratio of the minimum distance of $\mathcal{C}_2$ at NO instance of $GapMLP_{q,\gamma}$ over the minimum distance at YES instance is at least

$$\frac{d}{(2/3 + O(1/\gamma))d} = 3/2 + O(1/\gamma).$$

■

V. Concluding remarks and open problems

The gap minimum distance problem was proved to be NP-hard in [9] under a randomized reduction. It left open the question whether the reduction can be derandomized. In this paper, we settle the problem affirmatively and thus finalize the proof of the NP completeness of the gap minimum distance problem to any constant factor. Recently Austrin and Khot have found a new solution to this problem [3].

Although the idea in Ajtai and Micciancio's work on the shortest vector problem in L_2 norm inspired the results on the gap minimum distance problem, the reduction for the latter problem is now derandomized. In contrast, finding a deterministic reduction for the NP-completeness of the corresponding lattice problem, even for the exact version, remains open. We hope that some of the ideas in this paper can contribute to the ultimate solution of the corresponding lattice problem. Another interesting open problem is to prove Theorem 1.6 for $1/2 < \rho \leq 2/3$.

References

[1] Miklos Ajtai. The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract). In *Proc. 30th ACM Symp. on Theory of Computing*, pages 10–19, 1998.

[2] Sanjeev Arora, Laszlo Babai, Jacques Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes and systems of linear equations. *Journal of Computer and System Sciences*, 54:317–331, 1997.

[3] Per Austrin and Subhash Khot. A simple deterministic reduction for the gap minimum distance of code problem. In *Proceedings of the 38th International Colloquium on Automata, Languages and Programming*, volume 6755 of *Lecture Notes in Computer Science*, pages 474–485. Springer-Verlag, 2011.

[4] Elwyn R. Berlekamp, Robert J. McEliece, and Henk C. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions of Information Theory*, 24(3):384–386, 1978.

[5] J.-Y. Cai and A. Nerurkar. Approximating the svp to within a factor $(1 + 1/dim^{\epsilon})$ is NP-hard under randomized reductions. *J. of Comput. Syst. Sci.*, 59(2):221–239, 1999.

[6] Qi Cheng and Daqing Wan. On the list and bounded distance decodability of Reed-Solomon codes. *SIAM Journal on Computing*, 37(1):195–209, 2007. Special Issue on FOCS 2004.

[7] Qi Cheng and Daqing Wan. Complexity of decoding positive-rate Reed-Solomon codes. In *Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP)*, volume 5125 of *Lecture Notes in Computer Science*. Springer-Verlag, 2008.

[8] Stephen Cook. The complexity of theorem proving procedures. In *Proc. 3rd ACM Symp. on Theory of Computing*, pages 151–158, 1971.

[9] Ilya Dumer, Daniele Micciancio, and Madhu Sudan. Hardness of approximating the minimum distance of a linear code. *IEEE Transactions on Information Theory*, 49(1):22–37, 2003.

[10] Ishay Haviv and Oded Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. In *Proc. 39th ACM Symp. on Theory of Computing*, pages 469–477, 2007.

[11] Subhash Khot. Hardness of approximating the shortest vector problem in lattices. *Journal of ACM*, 52(5):789–808, 2005.

[12] D. Micciancio. The shortest vector problem is NP-hard to approximate to within some constant. *SIAM J. on Computing*, 30(6):2008–2035, 2001.

[13] Victor Shoup. New algorithms for finding irreducible polynomials over finite fields. *Mathematics of Computation*, 54:435–447, 1990.
[14] P. van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical report, Mathematische Instituut, University of Amsterdam, 1981.
[15] Alexander Vardy. The intractability of computing the minimum distance of a code. *IEEE Trans. Inform. Theory*, 43(6):1757–1766, 1997.
[16] Daqing Wan. Generators and irreducible polynomials over finite fields. *Mathematics of Computation*, 66(219):1195–1212, 1997.