New Set of Codes for the Maximum-Likelihood Decoding Problem

Morgan Barbier

New Set of Codes for the Maximum-Likelihood Decoding Problem

M. Barbier

Abstract

The maximum-likelihood decoding problem is known to be NP-hard for general linear and Reed-Solomon codes [1, 4]. In this paper, we introduce the notion of $\mathcal{A}$-covered codes, that is, codes that can be decoded through a polynomial time algorithm $\mathcal{A}$ whose decoding bound is beyond the covering radius. For these codes, we show that the maximum-likelihood decoding problem is reachable in polynomial time in the code parameters. Focusing on binary BCH codes, we were able to find several examples of $\mathcal{A}$-covered codes, including two codes for which the maximum-likelihood decoding problem can be solved in quasi-quadratic time.

Keywords: Maximum-likelihood decoding, perfect codes, covering radius, list decoding.

1 Introduction

Berlekamp, McEliece and Van Tilborg showed in [1] that the maximum-likelihood decoding is a NP-hard problem for general linear codes. Guruswami and Vardy later proved in [4] that this problem applied to the family of Reed-Solomon codes is also NP-hard. We briefly recall below the maximum-likelihood problem.

Definition 1.1 (Maximum-likelihood decoding problem)**.** *Let $\mathcal{C}$ a linear code over $\mathbb{F}_q$ and v a $\mathbb{F}_q$-vector in the ambient space. The* maximum-likelihood decoding problem *is to find the codeword $w \in \mathcal{C}$ closest to v. Most precisely, to find $w \in \mathcal{C}$, such as*

$$d(w, v) = d(v, \mathcal{C}) = \min_{c \in \mathcal{C}} \{d(v, c)\}.$$

Clearly, if for a given code there exists an algorithm able to correct a number of errors at least equal to the covering radius, then this algorithm solves the maximum-likelihood decoding problem. We recall the covering radius definition, which is the largest distance between any vector in ambient space and the code.

Definition 1.2 (Covering radius)**.** *Let $\mathcal{C}$ a linear code over $\mathbb{F}_q$. Its ambient space is a $\mathbb{F}_q$-vector space V. Let $v \in V$, the* covering radius *R of $\mathcal{C}$ is given by*

$$R = \max_{v \in V} \{\min_{c \in \mathcal{C}} d(v, c)\}.$$

In light of Wu's recent algorithmic advances in list decoding [8], we proceed in a comparaison between covering radii and now achievable decoding bounds with such algorithm. This leads us to propose the new algorithmic notion of *$\mathcal{A}$-covered codes* for which maximum-likelihood decoding problem can be carried out in polynomial time, and provide some examples by focussing the family of binary BCH codes. We also exhibit two codes for which the maximum-likelihood decoding problem has quasi-quadratic complexity.

2 $\mathcal{A}$-covered codes

In the rest of this paper, we follow the standard notations of [2] and shall denote by R the covering radius of a code $\mathcal{C}$, and by $t \triangleq \lfloor \frac{d-1}{2} \rfloor$ its error correction capacity. We now recall the definition of a perfect code.

Definition 2.1 (Perfect code)**.** *A code $\mathcal{C}$ with capacity t and covering radius R is called a* perfect code *if and only if*

$$R = t.$$

These codes are of course very interesting from a decoding point of view since each element of their ambient spaces can be decoded. Linear perfect codes are completely classified and for each of them, we know a decoding algorithm up to $t = R$. The maximum-likelihood problem is consequently trivial for perfect codes. This very property prompts us to propose the notion of *$\mathcal{A}$-covered codes* in the context of list decoding. We first introduce the following definitions:

Definition 2.2 (List decoding algorithm)**.** *Let $\mathcal{C}$ a code and v a word in its ambient space. $\mathcal{A}$ is a* list decoding algorithm for $\mathcal{C}$ *up to $\tau_{\mathcal{A}}$ if and only if it returns all codewords $w \in \mathcal{C}$ such that $d(v, w) \leq \tau_{\mathcal{A}}$.*

Definition 2.3 (Polynomial time list decoding algorithm)**.** *Let $\mathcal{C}$ a code, n its length, v a word in its ambient space and $\mathcal{A}$ a list decoding algorithm up to $\tau_{\mathcal{A}}$. $\mathcal{A}$ is a* polynomial time list decoding algorithm *if it runs in $\mathcal{O}(f(n))$, where $f(X) \in \mathbb{R}[X]$.*

We can now present the notion of *$\mathcal{A}$-covered code*.

Definition 2.4 ($\mathcal{A}$-covered code)**.** *Let $\mathcal{C}$ a code with covering radius R and $\mathcal{A}$ a polynomial time list decoding algorithm which decodes $\mathcal{C}$ up to $\tau_{\mathcal{A}}$. $\mathcal{C}$ is an* $\mathcal{A}$-covered code *if and only if*

$$R \leq \tau_{\mathcal{A}}.$$

Remark 2.1. *Since this algorithm runs in polynomial time, the returned list is also of polynomial size.*

Proposition 2.1. *Let $\mathcal{C}$ an* $\mathcal{A}$-covered code*. The maximum-likelihood decoding problem for $\mathcal{C}$, (as given by Definition 1.1) is solvable in a time polynomial in the code parameters.*

As seen before, the notion of *$\mathcal{A}$-covered code* can be seen as a computational analogue to perfect codes, albeit in the list decoding context (see Figure 1).

Unique decoding	List decoding
Perfect code	$\mathcal{A}$-covered code
$R = t$	$R \leq \tau_{\mathcal{A}}$

Figure 1: *Perfect code vs $\mathcal{A}$-covered code*

3 Case of binary BCH codes

While still relatively recent, Wu's list decoding algorithm [8] is already regarded as a significant advance in the coding community. Compared to the Guruswami-Sudan algorithm [3], it exhibits an even better complexity. Moreover, when restricted to binary BCH codes, Wu's method allows decoding up to the binary Johnson bound $\frac{n}{2}(1-\sqrt{1-\frac{2d}{n}})$, whereas Guruswami-Sudan only reaches the smaller general Johnson bound $n(1-\sqrt{1-\frac{d}{n}})$, as shown in Figure 2.

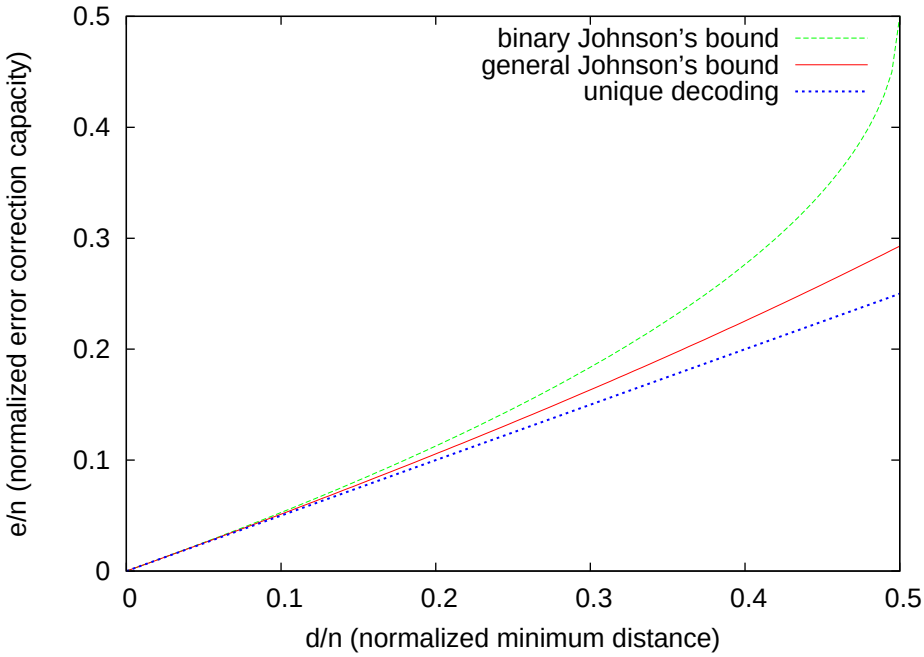

Figure 2: *General and binary Johnson's bound*

It is well known that 1-error-correcting BCH codes are perfect (these are Hamming codes) and 2-error-correcting codes are quasi-perfect [2]. Since Wu's method is a polynomial time list decoding algorithm [8], it is natural to compare their covering radii and the binary Johnson bound of other binary BCH codes. Unfortunately, classifying codes is a hard problem since it requires to compute the covering radii which usually is not an easy task [7]. Putting together and completing data from the literature [2], we still manage to obtain the list in Table 1. This table includes all primitive binary BCH codes of known covering radius. The non-primitive, Wu-covered binary BCH codes of length 17 and 23 were obtained by our own calculations.

Note that the BCH codes having 3 as their minimum distance are Hamming codes. Since those are perfect codes, the maximum-likelihood decoding problem is trivial. We also found two Reed-Muller codes of first order [5]. Since the dimensions of first order Reed-Muller codes are equal to the logarithm of their lengths, naively listing all closest codewords is already a polynomial time decoding algorithm. Hence, knowing that these codes are *Wu-covered* is of little pratical important in solving the maximum-likelihood decoding problem, since easier polynomial time methods are already available.

By contrast, the four codes $[15, 7, 5]$, $[17, 9, 5]$, $[23, 12, 7]$ and $[31, 11, 11]$ given in Table 1 do not fall into the two aforementioned families and we would expect the maximum-likelihood decoding problem to be asymptotically hard. However, the fact that they are *Wu-covered* implies that this problem is actually solvable in polynomial time only (in the code parameters).

n	k	d	R	τ	Comments
7	4	3	1	2	Hamming
15	11	3	1	1	Hamming
15	7	5	3	3	Wu-covered code
15	5	7	5	5	RM(1,4)*
17	9	5	3	3	Wu-covered code
23	12	7	3	4	Wu-covered code
31	26	3	1	1	Hamming
31	21	5	3	2	
31	16	7	5	4	
31	11	11	7	7	Wu-covered code
31	6	15	11	12	RM(1,5)*
63	57	3	1	1	Hamming
63	51	5	3	2	
63	45	7	5	3	
63	39	9	7	4	
63	36	11	9	6	

Table 1: *Table of covering radius and binary Johnson bound for some binary BCH codes.*

4 Quasi-quadratic list decoding of some binary BCH codes

Guruswami-Sudan's algorithm can decode up to Johnson's bound in polynomial time. As McEliece remarked in [6], if we accept to decode slightly less than this bound, the algorithm complexity is dramatically reduced. Under this relaxed constraint, Wu demonstrated in [8] that his algorithm runs in quasi-quadratic time.

Theorem 4.1. *Wu's list decoding algorithm decodes up to*

$$\tau = \lfloor \epsilon t + (1-\epsilon)\frac{n - n\sqrt{1-\frac{2d}{n}}}{2} \rfloor,$$

with multiplicity $m = \lfloor \epsilon^{-1} \rfloor$ *in* $\mathcal{O}(n^2 \lfloor \frac{1}{\epsilon} \rfloor^4)$.

Consequently, binary BCH codes having binary Johnson bound strictly greater than their covering radii, such as binary BCH $[31, 6, 15] = \text{RM}(1, 5)^*$ and BCH $[23, 12, 7]$, can be decoded in quasi-quadratic time up to, and including, their covering radii.

5 Conclusion

Working purely from an algorithmic point of view, we proposed a new set of codes, the $\mathcal{A}$-*covered codes*, for which we showed that the maximum-likelihood decoding problem, known as NP-hard in the general case, is solvable in polynomial time.

The main difficulty in finding such codes lies in the computation of covering radii. However there may be quite a few of those codes as we exhibited nine binary BCH codes which

are *Wu-covered codes*, of which, four constitute a new result and two can be decoded in time quasi-quadratic in code parameters.

References

[1] Berlekamp, McEliece, and Tilborg. On the inherent intractability of certain coding problem. *IEEE Trans. on Inform. Theory*, IT-24(3):384–386, May 1978.

[2] Gérard Cohen, Iiro Honkala, Simon Litsyn, and Antoine Lobstein. *Covering codes*, volume 54 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, 1997.

[3] Venkatesan Guruswami. *List Decoding of Error-Correcting Codes: Winning Thesis of the 2002 ACM Doctoral Dissertation Competition*. Lecture Notes in Computer Science. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2005.

[4] Venkatesan Guruswami and Alexander Vardy. Maximum-likelihood decoding of Reed-Solomon codes is NP-hard. In *SODA '05: Proceedings of the sixteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 470–478, Philadelphia, PA, USA, 2005. Society for Industrial and Applied Mathematics.

[5] F. J. Macwilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Mathematical Library. North Holland, January 1988.

[6] R. J. McEliece. The Guruswami-Sudan decoding algorithm for Reed-Solomon codes. Technical report, The Interplanetary Network Progress Report 42-153, April 2003. http://ipnpr.jpl.nasa.gov/progress_report/42-153/153F.pdf.

[7] A. McLoughlin. The complexity of computing the covering radius of a code. *Information Theory, IEEE Transactions on*, 30(6):800–804, November 1984.

[8] Yingquan Wu. New list decoding algorithms for Reed-Solomon and BCH codes. *IEEE Trans. Inform. Theory*, 54(8):3611–3630, 2008.