*Eleventh International Workshop on Algebraic and Combinatorial Coding Theory*
*June 16-22, 2008, Pamporovo, Bulgaria* *pp. 82-85*

# On complexity of decoding Reed-Muller codes within their code distance

Ilya Dumer dumer@ee.ucr.edu
University of California, Riverside, CA, USA

Grigory Kabatiansky kaba@iitp.ru
Institute for Information Transmission Problems, Moscow, RUSSIA

Cédric Tavernier cedric.tavernier@c-s.fr
Communications and Systems Le Plessis Robinson, FRANCE

**Abstract.** Recently Gopalan, Klivans, and Zuckerman proved that any binary Reed-Muller (RM) code $\mathrm{RM}(s, m)$ can be list-decoded up to its minimum distance $d$ with a polynomial complexity of order $n^3$ in blocklength $n$. The GKZ algorithm employs a new upper bound that is substantially tighter for RM codes of fixed order $s$ than the universal Johnson bound, and yields a constant number of codewords in a sphere of radius less than $d$. In this note, we modify the GKZ algorithm and show that full list decoding up to the code distance $d$ can be performed with a lower complexity order of at most $n \ln^{s-1} n$. We also show that our former algorithm yields the same complexity order $n \ln^{s-1} n$ if combined with the new GKZ bound on the list size.

## 1 Introduction

Binary Reed-Muller (RM) codes $\mathrm{RM}(s, m)$ of order $s$ have length $n = n(m)$, dimension $k = k(s, m)$, and distance $d = d(s, m)$ as follows

$$n = 2^m, \quad k = \sum_{i=0}^{s} \binom{m}{i}, \quad d = 2^{m-s}.$$

The renowned majority decoding algorithm of [1] provides bounded-distance decoding (BDD) for any code $RM(s, m)$ and corrects all errors of weight less than $d/2$ with complexity order of $kn$. Even a lower complexity order of $n \min(s, m-s)$ is required for various recursive techniques of [2], [3], and [4]. Both recursive and majority algorithms correct many error patterns beyond the BDD radius $d/2$; however, they fall short of complete error-free decoding within any given decoding radius $T \geq d/2$. Therefore, below we address *list decoding* [5] algorithms that output the list

$$L_T(\mathbf{y}) = \{\mathbf{c} \in \mathrm{RM}(s, m) : d(\mathbf{y}, \mathbf{c}) \leq T\}$$

of *all* vectors $\mathbf{c}$ of a code $\mathrm{RM}(s, m)$ located within the distance $T$ from any received vector $\mathbf{y}$.

Our study will be based on the recent algorithm obtained in [6] by Gopalan, Klivans, and Zuckerman (GKZ). The GKZ algorithm list-decodes any binary Reed-Muller (RM) code RM$(s,m)$ up to its minimum distance $d$ with a polynomial complexity of order $n^3$ in blocklength $n$. Another important advance is a new upper bound on the list size that is substantially tighter than the universal Johnson bound for codes RM$(s,m)$, and yields a constant number of RM-codewords in any sphere of radius less than $d$. More precisely, let

$$\delta_s = \frac{d(s,m)}{n(m)} = 2^{-s},\ T(s,m,\epsilon) = n(\delta_s - \epsilon)$$

be the relative distance of RM$(s,m)$ and the decoding radius of interest. Here we take any $\epsilon \in (0, \delta_s)$. Also, let $\chi(s,m,\epsilon)$ be the maximum number of binary operations required by GKZ algorithm to design the list $L_T(\mathbf{y})$ and let

$$l(s,m,\epsilon) = \max_{\mathbf{y}} |L_T(\mathbf{y})| \tag{1}$$

be the largest possible number of codewords in a sphere of radius $T(s,m,\epsilon)$. We will use the new upper bound

$$l(s,m,\epsilon) \leq 2(2^{s+5}\epsilon^{-2})^{4s} \tag{2}$$

discovered in [6]. This bound also leads to a new list decoding algorithm [6] that outputs the list $L_T(\mathbf{y})$ with complexity

$$\chi(s,m,\epsilon) = O(n^3 l^s(s,m,\epsilon)) = O(\epsilon^{-8s^2} n^3)$$

In the following, we simplify the GKZ algorithm and prove

**Theorem 1** *For any received vector* $\mathbf{y}$, *RM codes RM*$(s,m)$ *can be list-decoded within the decoding radius* $(2^{-s} - \epsilon)n$ *with complexity*

$$\chi^{(1)}(s,m,\epsilon) = O(\epsilon^{-18} n \ln^{s-1} n) + O(\epsilon^{8-16s} n \ln n) \tag{3}$$

*Also, consider our former recursive algorithm [7] that has the same complexity order* $n \ln^{s-1} n$ *in blocklength* $n$ *but was used in [7] to decode within the Johnson bound. In fact, this algorithm is restricted only by the correspomding list size. Namely, it is shown in [7] that complexity* $\chi^{(2)}(s,m,\epsilon)$ *of the algorithm* $\Psi_{s,m,\epsilon}$ *satisfies recursion*

$$\chi^{(2)}(s,m,\epsilon) \leq m(\chi^{(2)}(s-1,m-1,\epsilon) + cn\epsilon^{-1} l(s,m,\epsilon/2) l(s-1,m-1,\epsilon)) \tag{4}$$

*Thus, we can now extend the decoding radius to code distance* $d$ *using the GKZ bound (2). As initial step of our recursion (4), we can also use the list decoding algorithm [8] of RM*$(1,m)$ *codes, which has linear complexity* $O(n \ln^2(\epsilon^{-1}))$

*within radius $T(1,m,\epsilon)$. This combination of estimates (2) and (4) shows that the former algorithm $\Psi_{s,m,\epsilon}$ decodes within the radius $(2^{-s}-\epsilon)n$ with complexity*

$$\chi^{(2)}(s,m,\epsilon)=O(\chi^{(1)}\epsilon^{-1})$$

*In the next section, we briefly outline a modification of the GKZ algorithm that gives Theorem 1.*

## 2 Error-free list decoding of RM codes

We shall use the well known Plotkin construction of RM-codes [9] which represents any codeword $\mathbf{f}\in \mathrm{RM}(s,m)$ as the vector $\mathbf{u},\mathbf{u}+\mathbf{v}$, where $\mathbf{u}\in \mathrm{RM}(s,m-1)$ and $\mathbf{v}\in \mathrm{RM}(s-1,m-1)$. Let a received vector $\mathbf{y}$ be decomposed into two halves $\mathbf{y}'$ and $\mathbf{y}''$, which can be considered as the corrupted versions of some vectors $\mathbf{u}$ and $\mathbf{u}+\mathbf{v}$ correspondingly.

*Algorithm.* Given $\epsilon$ and any received vector $\mathbf{y}$, we consider below an algorithm $\Phi(s,m,\epsilon)$ that decodes $\mathbf{y}$ into the list $L_T(\mathbf{y})$ within the radius $T(s,m,\epsilon)=n(\delta_s-\epsilon)$.

Step 1. Decode the vector $\mathbf{y}^v=\mathbf{y}'+\mathbf{y}''$ within the radius $T(s,m,\epsilon)=T(s-1,m-1,2\epsilon)$, using the algorithm $\Phi(s-1,m-1,2\epsilon)$. The resulting list of codewords $L^v$ belongs to $\mathrm{RM}(s-1,m-1)$.

Step 2. Decode both vectors $\mathbf{y}'$ and $\mathbf{y}''$ within the radius $T(s,m,\epsilon)/2=T(s,m-1,\epsilon)$ using the algorithm $\Phi(s,m-1,\epsilon)$. The resulting lists of codewords $L'$and $L''$ belong to $\mathrm{RM}(s,m-1)$.

3. Consider the two lists of vectors

$$A=\{(\mathbf{u}',\mathbf{u}'+\mathbf{v}):\ \mathbf{u}'\in L',\mathbf{v}\in L^v\}$$

$$B=\{(\mathbf{u}''+\mathbf{v},\mathbf{u}''):\ \mathbf{u}''\in L'',\mathbf{v}\in L^v\}$$

Calculate the distance from $\mathbf{y}$ to each vector of the two lists. Leave the vectors located within distance $T(s,m,\epsilon)$.

The above algorithm gives complete list $L_{T(s,m,\epsilon)}(\mathbf{y})$ and thus performs the required decoding. This is due to the following:

1. Vector $\mathbf{y}^v$ has no more errors than $\mathbf{y}$;
2. Either $\mathbf{y}'$ or $\mathbf{y}''$ has at most $T(s,m,\epsilon)/2$ errors.

*Complexity.* Algorithm $\Phi(s,m,\epsilon)$ includes one decoding $\Phi(s-1,m-1,2\epsilon)$, two decodings $\Phi(s,m-1,\epsilon)$ plus requires the order of $2nl(s,m-1,\epsilon)l(s-1,m-1,2\epsilon)$ operations to verify the distance from vector of lists $A$ and $B$ to the vector $\mathbf{y}$. Thus, algorithm $\Phi(s,m,\epsilon)$ has complexity

$$\begin{aligned}\chi(s,m,\epsilon)\le{}&\chi(s-1,m-1,2\epsilon)+2\chi(s,m-1,\epsilon)\\&+2nl(s,m-1,\epsilon)l(s-1,m-1,2\epsilon).\end{aligned}\tag{5}$$

Now we proceed, for $s = 2, 3, ..$ using complexity $\chi(1, m, \epsilon) = 2^m \ln^2 \epsilon^{-1}$ in step $s = 1$, the Johnson bound $l(1, m, \epsilon) \le (2\epsilon)^{-2}$ for $RM - 1$ codes and the upper bound (2) for $s > 1$. Then

$$\chi(2, m, \epsilon) = O(m2^m \left[\ln^2 \epsilon^{-1} + \epsilon^{-18}\right]) = O(m2^m \epsilon^{-18})$$

and for any $s > 2$ we obtain the estimate

$$\begin{aligned}\chi(s, m, \epsilon) &= O(m^{s-1} 2^m \epsilon^{-18}) + \sum_{i=3}^{s} O\left(m^{s-i+1} 2^m \epsilon^{8-16i}\right) \\ &= O(\epsilon^{-18} n \ln^{s-1} n) + O(\epsilon^{8-16s} n \ln n)\end{aligned}$$

which proves Theorem 1.

## References


[1] I. S. Reed, A class of multiple error correcting codes and the decoding scheme, *IEEE Trans. Inform. Theory* 4, 1954, 38-49.

[2] S. Litsyn, On complexity of decoding low rate Reed-Muller codes, *Proc. 9th All Union Conf. Coding Theory Inform. Transm.* 1, 1988, 202-204 (in Russian).

[3] G. A. Kabatianskii, On decoding of Reed-Muller codes in semicontinuous channels, *Proc. Second Intern. Workshop ACCT*, Leningrad, USSR, 1990, 87-91.

[4] I. Dumer, Recursive decoding and its performance for low-rate Reed-Muller codes, *IEEE Trans. Inform. Theory* 50, 2004, 811-823.

[5] P. Elias, List decoding for noisy channels, *1957-IRE WESCON Conven. Record* 2, 1957, 94-104.

[6] P. Gopalan, A. R. Klivans, D. Zuckerman, List-decoding Reed-Muller codes over small fields, STOC 2008.

[7] I. Dumer, G. Kabatiansky, C. Tavernier, List decoding of Reed-Muller codes up to the Johnson bound with almost linear complexity, *IEEE Symp. Inform. Theory*, 2006, Seattle, WA, USA, 138-142.

[8] I. Dumer, G. Kabatiansky, C. Tavernier, List decoding for binary Reed-Muller codes of the first order, *Probl. Inform. Transm.* 43, 3, 66-74, 2007.

[9] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1981.