Decoding of low-rate Reed-Muller codes with polylogarithmic complexity

Ilya Dumer*

Abstract

Reed-Muller (RM) codes (m,r) of growing length 2^m and fixed order r are considered when a channel has high crossover error probability $1/2-\varepsilon$. For an arbitrarily small $\varepsilon>0$, new recursive decoding algorithms are designed that allow one to retrieve all k information bits with a vanishing error probability and polylogarithmic complexity of order $O(m^{r+1})$.

1 Introduction

In our presentation, we wish to design new decoding algorithms for RM codes that can enhance techniques known to date. We use notation $\left\{ {m \atop r} \right\}$ for RM codes of length $n=2^m$, dimension $k=\sum_{i=0}^{r}\binom{m}{i}$, and distance $d=2^{m-r}$. These codes are designed using the set $\{f_r^m\}$ of all m-variate Boolean polynomials $f_r^m : E_2^m \rightarrow E_2$ of degree r or less. Here a codeword $\mathbf{c}_f$ is obtained as the sequence of values that a polynomial f takes on a complete m-dimensional space E_2^m of its inputs.

RM codes have found numerous applications thanks to simple code structure and fast decoding procedures. First, majority algorithm was developed in [1] followed later by numerous developments. The algorithm requires complexity order of nk or less to execute bounded distance decoding. In addition, majority decoding substantially extends bounded-distance threshold of $d/2$. Here, given an infinite sequence of codes $A_i(n_i,d_i)$, we say that a decoding algorithm Ψ has a threshold sequence δ_i and a residual sequence $\epsilon_i \rightarrow 0$ if for $n_i \rightarrow \infty$:

- a vanishing fraction of error patterns of weight $\delta_i(1-\epsilon_i)$ or less is left uncorrected;
- a nonvanishing fraction of error patterns of weight δ_i or less is left uncorrected[1].

For majority decoding, the threshold has been found in [6]. Namely, for RM codes of *fixed order* r, majority decoding achieves the maximum possible threshold $\delta=n/2$ (here and below we omit index i) with a residual

$$\varepsilon_r^{\mathrm{maj}}=(cm/d)^{1/2^{r+1}}, \quad m\rightarrow\infty, \tag{1}$$

where positive constant c does not depend on m or r. One more efficient algorithm [7] makes use of the symmetry group of RM codes. For long RM codes $\left\{ {m \atop 2} \right\}$ the algorithm of [7] allows one to reduce the residual term $\varepsilon_2^{\mathrm{maj}}$ from (1) to the lower order of $(cm/d)^{1/4}$ for any $c>\ln 4$, while slightly increasing complexity to the order of n^2m. The corresponding thresholds for higher orders $r\geq 3$ are yet unknown. Another result of [7] concerns maximum-likelihood (ML)

*The author is with the College of Engineering, University of California, Riverside, CA 92521. This research was supported by the NSF grant CCR-0097125.

[1]Note that multiple sequences $\epsilon_i \rightarrow 0$ can satisfy the same definition.

decoding. It is shown that ML decoding of RM codes of fixed order r has a substantially lower residual term

$$\varepsilon_r^{\mathrm{ml}} \sim c m^{r/2} n^{-1/2}, \quad c > 2((2^r-1)(\ln 2)/r!)^{1/2}, \quad m \to \infty.$$

However, even the best known algorithm of ML decoding designed by the multilevel trellis structure in [8] has yet complexity that is exponent in n.

Finally, new recursive techniques were introduced in [2] and [4] (see also [3] and [12]). These algorithms use different metrics but rely on the *Plotkin construction* $(\mathbf{u}, \mathbf{u}+\mathbf{v})$. The construction allows one to decompose RM codes $\left\{ {m \atop r} \right\}$ onto shorter codes [5], by taking subblocks $\mathbf{u}$ and $\mathbf{v}$ from codes $\left\{ {m-1 \atop r} \right\}$ and $\left\{ {m-1 \atop r-1} \right\}$. It is shown that this recursive structure allows one to execute both encoding [2] and bounded distance decoding [4], [12] with the lowest complexity order of $n \min(r, m-r)$ known for RM codes of an arbitrary order r.

In our presentation, we also employ Plotkin construction. The basic recursive procedure will split RM code $\left\{ {m \atop r} \right\}$ of length n into two RM codes of length $n/2$. Decoding is then relegated further to the shorter codes until we reach basic codes of order $r \le 1$ or $r = m$. In all intermediate steps, we shall only define and calculate the reliabilities of the newly defined symbols. In doing so, we wish to define efficient recalculation metrics that can give good asymptotic performance. The summary of our results presented below shows that recursive techniques outperform other polynomial algorithms known for RM codes.

2 Summary of results

The results are summarized in the following three statements, which represent different types of trade-offs between decoding complexity and its threshold.

Theorem 1 *Long RM codes $\left\{ {m \atop r} \right\}$ of fixed order r can be decoded with linear complexity $O(n)$ and decoding threshold*

$$\delta = n/2, \quad \varepsilon_r = (2r(\ln m)/d)^{1/2^{r+1}}, \quad m \to \infty.$$

Theorem 2 *Long RM codes $\left\{ {m \atop r} \right\}$ of fixed order r can be decoded with quasi-linear complexity $O(n \log n)$ and decoding threshold*

$$\delta = n/2, \quad \varepsilon_r' = (cm/d)^{1/2^r}, \quad c > \ln 2, \quad m \to \infty.$$

One straightforward corollary from these theorems is as follows.

Corollary 3 *Long RM codes $\left\{ {m \atop r} \right\}$ of fixed order r can be decoded with vanishing error probability and linear complexity $O(n)$ (or quasi-linear complexity $O(n \log n)$) on a binary channel with crossover error probability $(1-\varepsilon_r)/2$ (correspondingly, $(1-\varepsilon_r')/2$) as $n \to \infty$.*

Theorem 4 *For any constant $\varepsilon > 0$, long RM codes $\left\{ {m \atop r} \right\}$ of fixed order r can correct errors of weight*

$$\delta = n(1-\varepsilon)/2, \quad m \to \infty, \tag{2}$$

with vanishing error probability and polylogarithmic complexity of order $m^{r+1}\varepsilon^{-2^r}$.

Note that Theorem 1 increases the decoding threshold of the recursive techniques introduced in [2] and [4] while keeping linear decoding complexity. Theorem 2 improves both the complexity and decoding residual of majority decoding. It also reduces complexity of the algorithm [7] and extends this algorithm to an arbitrary order $r \geq 2$.

Theorem 4 also yields some important implications. First, polylogarithmic decoding complexity $O(m^{r+1})$ will be obtained here by retrieving all k information bits from a small fraction $kl_m = o(n)$ of received symbols, where l_m is a slowly growing function (say, $\ln m$). Second, the converse to the Shannon coding theorem shows that Theorem 4 gives near-minimum complexity for nonvanishing ε. Formally, the converse of Shannon theorem gives the following corollary.

Corollary 5 *For any $\varepsilon > 0$, a long (n,k) code requires complexity order of at least* $\min(n, k/\varepsilon^2)$ *to achieve decoding threshold $\delta = n(1-\varepsilon)/2$, as $n \to \infty$.*

Finally, we compare Theorem 4 with other polylogarithmic algorithms known for RM codes. Decoding of RM codes (or, equivalently, reconstruction of Boolean polynomials with corrupted outputs) has been extensively researched in the areas of computational self-correctors, cryptography, and learning theory (see [10]). Polylogarithmic complexity was first obtained in [9] for biorthogonal codes $\left\{ {m \atop 1} \right\}$. For any constants $\varepsilon > 0$ and $s > 0$, the paper [9] presents a randomized list decoding of codes $\left\{ {m \atop 1} \right\}$ that runs in polynomial time $\mathsf{poly}(ms/\varepsilon^2)$ and outputs with probability $1 - \exp\{-s\}$ a complete list of codewords located within radius (2) from the received vector. An important point is that the algorithm can equally well withstand both random noise and adversarial noise of the same weight δ.

The latter results were substantially advanced in papers [10] and [11] for long q-ary RM codes. Namely, given a q-ary RM code $\left\{ {m \atop r} \right\}_q$ and a parameter s, consider any radius $\rho(q,r,s)n$ such that all codewords located in *any sphere* of this radius can be found with probability $1 - \exp\{-s\}$ in $\mathsf{poly}(m,s)$ time as $m \to \infty$. For codes of low order $2 \leq r < q$, the latest results [10], [11] show that

$$(1 - 2\sqrt{r/q}) \leq \sup \rho(q,r,s) \leq (1 - r/q - (r-1)/q^2). \tag{3}$$

(the case $r = 1$ is a notable exception that has maximum possible threshold $\rho_{\max} = 1 - 1/q$). Namely, a randomized algorithm from [11] performs list decoding with complexity $\mathsf{poly}(m)$ if ρ falls below the lower bound in (3). By contrast, [10] exhibits a subset of q^{m-1} codewords all of which have the weight no more than the upper bound in (3).

For binary codes, the above results give complexity $\mathsf{poly}(m)$ only for $r = 1$. Now we see that Theorem 4 gives different results in three aspects. First, polylogarithmic complexity is obtained in Theorem 4 for any fixed order $r \geq 2$ in contrast to $r < q$ in (3). Second, for any order r, poly(m) complexity is now achieved even if radius ρ is arbitrarily close to the maximum 1/2.

On the other hand, Theorem 4 relies on a much weaker setting. Namely, successful decoding is provided here with high fidelity for a (typical) random error instead of any (advesarial) noise used in list decoding algorithms. Therefore this difference rests on the fact that a typical sphere of radius (2) includes at most one codeword of the $\left\{ {m \atop r} \right\}$ code.

¿From the practical prospective, it turns out that RM codes are especially efficient on *moderate* blocklengths up to 512, where these (asymptotically bad) codes still have good distance properties. Also, these properties can be realized by recursive decoding with low complexity. In turn, this allows us to partially fill the gap left by optimum maximum likelihood (ML) decoding and suboptimal iterative decoding. An important open problem is whether recursive techniques can enable fast near-ML decoding for the longer codes. A positive solution to this problem would allow one to completely fill the gap in the blocklengths left by the best algorithms known to date.

References

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

[2] S.N. Litsyn, "On decoding complexity of low-rate Reed-Muller codes," *Proc. 9th All-Union Conf. on Coding Theory and Info. Transmission,* Part 1, Odessa, USSR, pp. 202-204, 1988 (in Russian).

[3] F. Hemmati, "Closest coset decoding of $u|u+v|$ codes," *IEEE Selected Areas Commun.,* vol. 7, pp. 982-988, 1989.

[4] G.A. Kabatyanskii, "On decoding of Reed-Muller codes in semicontinuous channels," *Proc. 2nd Int. Workshop "Algebr. and Comb. Coding Theory"*, Leningrad, USSR, 1990, pp. 87-91.

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

[6] R.E. Krichevskiy, "On the Number of Reed-Muller Code Correctable Errors," *Dokl. Soviet Acad. Sciences,* vol. 191, pp. 541-547, 1970.

[7] V. Sidel'nikov and A. Pershakov, "Decoding of Reed-Muller codes with a large number of errors," *Probl. Info. Transmission,* vol. 28, no. 3, pp. 80-94, 1992 (in Russian).

[8] G.D. Forney, "Coset codes-part II: Binary lattices and related codes," *IEEE Trans. Info. Theory,* vol. 34, pp. 1152-1187, 1987.

[9] O. Goldreich and L. A. Levin, "A hard-core predicate for all one way functions," *Proc. 21th Annual ACM Symp. on Theory Comp.,* Seattle, WA, May 15-17, 1989, pp. 25-32.

[10] O. Goldreich, R. Rubinfeld, and M. Sudan, "Learning polynomials with queries: The highly noisy case," *SIAM Journal on Discrete Mathematics,* 13(4):535-570, November 2000.

[11] M. Sudan, L. Trevisan, and S. Vadhan, "Pseudorandom generators without the XOR Lemma," *Computer and System Sciences,* 62(2): 236–266, March 2001.

[12] G. Schnabl and M. Bossert, "Soft-decision decoding of Reed-Muller Codes as generalized multiple concatenated codes," *IEEE Trans. Info. Theory,* vol. 41, pp. 304-308, 1995.