Reed-Muller Codes

Other titles in Foundations and Trends® in Communications and Information Theory

Topics and Techniques in Distribution Testing: A Biased but Representative Sample
Clément L. Canonne
ISBN: 978-1-63828-100-9

Codes in the Sum-Rank Metric: Fundamentals and Applications
Umberto Martínez-Peñas, Mohannad Shehadeh and Frank R. Kschischang
ISBN: 978-1-63828-030-9

Codes for Distributed Storage
Vinayak Ramkumar, S. B. Balaji, Birenjith Sasidharan, Myna Vajha, M. Nikhil Krishnan and P. Vijay Kumar
ISBN: 978-1-63828-024-8

Rank-Metric Codes and Their Applications
Hannes Bartz, Lukas Holzbaur, Hedongliang Liu, Sven Puchinger, Julian Renner and Antonia Wachter-Zeh
ISBN: 978-1-63828-000-2

Common Information, Noise Stability, and Their Extensions
Lei Yu and Vincent Y. F. Tan
ISBN: 978-1-63828-014-9

Information-Theoretic Foundations of DNA Data Storage
Ilan Shomorony and Reinhard Heckel
ISBN: 978-1-68083-956-2

Reed-Muller Codes

Emmanuel Abbe
EPFL
emmanuel.abbe@epfl.ch

Ori Sberlo
Tel Aviv University
ori.sberlo@gmail.com

Amir Shpilka
Tel Aviv University
shpilka@tauex.tau.ac.il

Min Ye
Tsinghua-Berkeley Shenzhen Institute
yeemmi@gmail.com

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Communications and Information Theory

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

E. Abbe *et al.*. *Reed-Muller Codes*. Foundations and Trends® in Communications and Information Theory, vol. 20, no. 1–2, pp. 1–156, 2023.

ISBN: 978-1-63828-145-0

Foundations and Trends® in Communications and Information Theory
Volume 20, Issue 1–2, 2023

Editorial Board

Editorial Scope

Topics

Foundations and Trends® in Communications and Information Theory publishes survey and tutorial articles in the following topics:

- Coded modulation
- Coding theory and practice
- Communication complexity
- Communication system design
- Cryptology and data security
- Data compression
- Data networks
- Demodulation and Equalization
- Denoising
- Detection and estimation
- Information theory and statistics
- Information theory and computer science
- Joint source/channel coding
- Modulation and signal design
- Multiuser detection
- Multiuser information theory
- Optical communication channels
- Pattern recognition and learning
- Quantization
- Quantum information processing
- Rate-distortion theory
- Shannon theory
- Signal processing for communications
- Source coding
- Storage and recording codes
- Speech and Image Compression
- Wireless Communications

Information for Librarians

Foundations and Trends® in Communications and Information Theory, 2023, Volume 20, 4 issues. ISSN paper version 1567-2190. ISSN online version 1567-2328 . Also available as a combined paper and online subscription.

Contents

Reed-Muller Codes

Emmanuel Abbe[1], Ori Sberlo[2], Amir Shpilka[2] and Min Ye[3*]

[1] *Mathematics Institute and the School of Computer and Communication Sciences, EPFL, Switzerland; emmanuel.abbe@epfl.ch*
[2] *Blavatnik School of Computer Science, Tel Aviv University, Israel; ori.sberlo@gmail.com, shpilka@tauex.tau.ac.il*
[3] *Tsinghua-Berkeley Shenzhen Institute, Tsinghua Shenzhen International Graduate School, China; yeemmi@gmail.com*

ABSTRACT

Reed-Muller (RM) codes are among the oldest, simplest and perhaps most ubiquitous family of codes. They are used in many areas of coding theory in both electrical engineering and computer science. Yet, many of their important properties are still under investigation. This work covers some of the developments regarding the weight enumerator and the capacity-achieving properties of RM codes, as well as some of the algorithmic developments. In particular, it discusses connections established between RM codes, thresholds of Boolean functions, polarization theory, hypercontractivity, and the techniques of approximating low weight codewords using lower degree polynomials (when codewords are viewed as evaluation vectors of degree r polynomials in m variables).

*Corresponding author: Min Ye, yeemmi@gmail.com. O. Sberlo received funding from the ERC (Grant 949499), and from the ISF (Grant Number 952/18). A. Shpilka received funding from the Israel Science Foundation (Grant Number 514/20) and from the Len Blavatnik and the Blavatnik Family foundation. M. Ye received funding from National Key R&D Program of China under Grant No. 2021YFA1001000 and Shenzhen Stable Support program under Grant No. WDZC20220811170401001.

Emmanuel Abbe, Ori Sberlo, Amir Shpilka and Min Ye (2023), “Reed-Muller Codes”, Foundations and Trends® in Communications and Information Theory: Vol. 20, No. 1–2, pp 1–156. DOI: 10.1561/0100000123.

It then overviews some of the algorithms for decoding RM codes, giving both algorithms with provable performance guarantees for every block length, as well as algorithms with state-of-the-art performances in practical regimes, which do not perform as well for large block length. Finally, some applications of RM codes in theoretical computer science and signal processing are given.

1

Introduction

A large variety of codes have been developed over the past 70 years. These were driven by various objectives, in particular, achieving efficiently the Shannon capacity [137], constructing perfect or good codes in the Hamming worst-case model [67], matching the performance of random codes, improving the decoding complexity, the weight enumerator, the scaling law, the universality, the local properties of the code [28], [78], [79], [98], [99], [123], [154], and more objectives in theoretical computer science such as in cryptography (e.g., secrete sharing, private information retrieval), pseudorandomness, extractors, hardness amplification or probabilistic proof systems; see [1] for references. Among this large variety of code developments, one of the first, simplest and perhaps most ubiquitous code is the Reed-Muller (RM) code.

The RM code was introduced by Muller in 1954 [109], and Reed developed shortly after a decoding algorithm decoding up to half its minimum distance [121]. The code construction can be described with a greedy procedure. Consider building a linear code (with block length a power of two); it must contain the all-0 codeword. If one has to pick a second codeword, then the all-1 codeword is the best choice under any meaningful criteria. If now one has to keep these two codewords, the next best choice to maximize the code distance is the half-0 half-1 codeword, and to continue building a basis sequentially, one can add a few more vectors that preserve a relative distance of half, completing the simplex code, which has an optimal rate for the relative distance half. Once saturation is reached at relative distance half, it is less clear how to pick the next codeword, but one can simply re-iterate the simplex construction on any of the support of the previously picked vectors, and iterate this after each saturation, reducing each time the distance by half. This gives the RM code, whose basis is equivalently defined by the evaluation vectors of bounded degree monomials.

As mentioned, the first order RM code is the augmented simplex code or equivalently the Hadamard code, and the simplex code is the dual of the Hamming code that is "perfect". This strong property is clearly lost once the RM code order gets higher, but RM codes preserve nonetheless a decent distance (at root block length for constant rate). Of course this does not give a "good" family of codes (i.e., a family of codes with asymptotically constant rate and constant relative distance), and it is far from achieving the distance that other combinatorial codes can reach, such as Golay codes, BCH codes or expander codes [99]. However, once put under the light of random errors, i.e., the Shannon setting, for which the minimum distance is no longer the right figure or merit, RM codes may perform well again. In [77], Levenshtein and co-authors showed that for the binary symmetric channel, there are codes that improve on the simplex code in terms of the error probability (with matching length and dimension). Nonetheless, in the lens of Shannon capacity, RM codes seem to perform very well. In fact, more than well; it is plausible that they achieve the Shannon capacity on any Binary-input Memoryless Symmetric (BMS) channel [1], [2], [43], [89], [90], [122] and perform comparably to random codes on criteria such as the scaling law [70] or the weight enumerator [82]–[84], [99], [127], [142].

The fact that RM codes have good performance in the Shannon setting, and that they seem to achieve capacity, has long been observed and conjectured. It is hard to track back the first appearance of this belief in the literature, but [89] reports that it was likely already present in the late 60s. The claim was mentioned explicitly in a 1993 talk by Shu Lin, entitled "RM Codes are Not So Bad" [95]. It appears that a 1994 paper by Dumer and Farrell contains the earliest printed discussion on this matter [50]. Since then, the topic has become increasingly prevalent[1] [1], [9], [11], [39], [43], [45], [104].

But the research activity has truly sparked with the emergence of polar codes [11]. Polar codes are close relatives of RM codes. They are derived from the same square matrix (the matrix whose rows correspond to evaluations of multilinear monomials) but with a different rule of row selection. The more sophisticated and channel dependent construction of polar codes gives them the advantage of being provably capacity-achieving on any BMS channel, due to the polarization phenomenon. Even more impressive is the fact that they possess an efficient decoding algorithm down to the capacity.

Shortly after the polar code breakthrough, and given the close relationship between polar and RM codes, the hope that RM codes could also be proved to achieve capacity on any BMS started to propagate, both in the electrical engineering and computer science communities. A first confirmation of this was obtained in extremal regimes of the BEC and BSC [1], exploiting new bounds on the weight enumerator [84], and a first complete proof for the BEC at constant rate was finally obtained in [90]. The paper [122] presented a major breakthrough proving that constant-rate RM codes indeed achieve capacity on all BMS channels under bit-MAP decoding. While [122] comes close to proving the conjecture, the question of whether RM codes achieve capacity under block-MAP decoding still remains open.

The papers mentioned in the previous paragraph however did not exploit the close connection between RM and polar codes. This connection was studied in [2] where it was shown that the RM transform is also polarizing and that a third variant of the RM code achieves capacity on any BMS channel. Furthermore [2] conjectured that this variant is indeed the RM code itself.

Polar codes and RM codes can be compared in different ways. In most performance metrics, and putting aside the decoding complexity, RM codes seem to be superior to polar codes [2], [104]. Namely, they seem

[1]The capacity conjecture for the BEC at constant rate was posed as one of the open problems at the Information Theory Semester at the Simons Institute, Berkeley, in 2015.

to achieve capacity universally and with an optimal scaling-law, while polar codes have a channel-dependent construction with a suboptimal scaling-law [66], [70], [71]. However, RM codes seem more complex both in terms of obtaining performance guarantees (as evidenced by the long standing conjectures) and in terms of their decoding complexity.

Efficient decoding of RM codes is the second main outstanding challenge. Many algorithms have been proposed since Reed's algorithm [121], such as [20], [48], [49], [51], [64], [125], [141], and newer ones have appeared in the post polar code period [129], [130], [153]. Some of these already show that at various block-lengths and rates that are relevant for communication applications, RM codes are indeed competing or even superior to polar codes [104], [153], even compared to the improved versions considered for 5G [57].

This survey is meant to overview these developments regarding both the performance guarantees (in particular on weight enumerator and capacity) and the decoding algorithms for RM codes. At the end of this survey, we discuss a few applications of RM codes in the areas beyond communication, e.g., applications in low degree testing, private information retrieval, and compressed sensing.

1.1 Outline of the Survey and Differences from a Previous Version

Part of this monograph was taken from a previous survey [4] written by the first author, the third author and the fourth author. At the same time, we have added quite a few new elements and optimized the presentation of the contents from [4]. Below we give the outline of this new survey and discuss the difference from [4].

We start in Section 2 with the main definitions and basic properties of RM codes. Most parts of this section already appeared in [4], e.g., the code parameters, recursive structure, duality, automorphism group, and local properties. We have, however, added two new subsections discussing the cyclic property of punctured RM codes and the nonlinear subcodes of RM codes. In Section 3, we introduce some performance measures and important quantities in channel coding. This is a new section that has not appeared in [4]. We then cover the bounds on the weight enumerator of RM codes in Section 4. In Section 5, we cover the capacity-achieving results, using tools from the weight enumerator and sharp thresholds of monotone Boolean functions. In Section 6, we explore the connection between RM codes and polar codes. Although Sections 4–6 have appeared in [4], we have revised the organization of these 3 sections and added some proofs to better explain the results as well as covered results that appeared between the publication time of these two surveys. Section 7 is a new section that describes the finite-length scaling of random codes, RM codes and polar codes. We then cover various decoding algorithms in Section 8, providing pseudo-codes for them. This section is similar to the previous version [4]. Finally, in Section 9, we discuss some applications of RM codes beyond communication and channel coding, which were not covered in the previous version [4].

References

[1] E. Abbe, A. Shpilka, and A. Wigderson, "Reed–Muller codes for random erasures and errors," *IEEE Transactions on Information Theory*, vol. 61, no. 10, pp. 5229–5252, 2015.

[2] E. Abbe and M. Ye, "Reed-Muller codes polarize," in *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE, pp. 273–286, 2019.

[3] E. Abbe, J. Hazla, and I. Nachum, "Almost–Reed–Muller codes achieve constant rates for random errors," *IEEE Transactions on Information Theory*, vol. 67, no. 12, pp. 8034–8050, 2021.

[4] E. Abbe, A. Shpilka, and M. Ye, "Reed–Muller codes: Theory and algorithms," *IEEE Transactions on Information Theory*, vol. 67, no. 6, pp. 3251–3277, 2021.

[5] E. Abbe and Y. Wigderson, "High-girth matrices and polarization," in *2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 2461–2465, 2015.

[6] N. Alon, T. Kaufman, M. Krivelevich, S. Litsyn, and D. Ron, "Testing Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 11, pp. 4032–4039, 2005.

[7] Y. Altuğ and A. B. Wagner, "Moderate deviation analysis of channel coding: Discrete memoryless case," in *2010 IEEE International Symposium on Information Theory*, IEEE, pp. 265–269, 2010.

[8] Y. Altuğ and A. B. Wagner, "Moderate deviations in channel coding," *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4417–4426, 2014.

[9] E. Arikan, "A survey of Reed–Muller codes from polar coding perspective," in *2010 IEEE Information Theory Workshop on Information Theory (ITW 2010, Cairo)*, IEEE, pp. 1–5, 2010.

[10] E. Arikan, "Source polarization," in *2010 IEEE International Symposium on Information Theory*, pp. 899–903, 2010.

[11] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[12] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, "Proof verification and the hardness of approximation problems," *Journal of the ACM (JACM)*, vol. 45, no. 3, pp. 501–555, 1998.

[13] A. Ashikhmin, G. Kramer, and S. ten Brink, "Extrinsic information transfer functions: Model and erasure channel properties," *IEEE Transactions on Information Theory*, vol. 50, no. 11, pp. 2657–2673, 2004.

[14] L. Babai, L. Fortnow, and C. Lund, "Nondeterministic exponential time has two-prover interactive protocols," in *Foundations of Computer Science, 1990. Proceedings., 31st Annual Symposium on*, IEEE, pp. 16–25, 1990.

[15] B. Barak, P. Gopalan, J. Håstad, R. Meka, P. Raghavendra, and D. Steurer, "Making the long code shorter," in *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, pp. 370–379, 2012.

[16] A. Barg and G. D. Forney, "Random codes: Minimum distances and error exponents," *IEEE Transactions on Information Theory*, vol. 48, no. 9, pp. 2568–2573, 2002.

[17] A. Barg, A. Mazumdar, and R. Wang, "Restricted isometry property of random subdictionaries," *IEEE Transactions on Information Theory*, vol. 61, no. 8, pp. 4440–4450, 2015.

[18] P. Beame, S. O. Gharan, and X. Yang, "On the bias of Reed–Muller codes over odd prime fields," *arXiv preprint arXiv:1806.06973*, 2018.

[19] D. Beaver and J. Feigenbaum, "Hiding instances in multioracle queries," in *STACS 90*, Springer, 1990, pp. 37–48.

[20] Y. Be'ery and J. Snyders, "Optimal soft decision block decoders based on fast Hadamard transform," *IEEE Transactions on Information Theory*, vol. 32, no. 3, pp. 355–364, 1986.

[21] A. Beimel, Y. Ishai, and E. Kushilevitz, "General constructions for information-theoretic private information retrieval," *Journal of Computer and System Sciences*, vol. 71, no. 2, pp. 213–247, 2005.

[22] A. Beimel, Y. Ishai, E. Kushilevitz, and J. Raymond, "Breaking the $O(n^{1/(2k-1)})$ barrier for information-theoretic private information retrieval," in *43rd Symposium on Foundations of Computer Science (FOCS 2002), 16-19 November 2002, Vancouver, BC, Canada, Proceedings*, pp. 261–270, IEEE Computer Society, 2002.

[23] I. Ben-Eliezer, R. Hod, and S. Lovett, "Random low-degree polynomials are hard to approximate," *Computational Complexity*, vol. 21, no. 1, pp. 63–81, 2012.

[24] I. Benjamini, G. Kalai, and O. Schramm, "Noise sensitivity of boolean functions and applications to percolation," *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, vol. 90, no. 1, pp. 5–43, 1999.

[25] S. Bhandari, P. Harsha, R. Saptharishi, and S. Srinivasan, "Vanishing spaces of random sets and applications to Reed–Muller codes," in *37th Computational Complexity Conference, CCC 2022, July 20–23, 2022, Philadelphia, PA, USA*, S. Lovett, Ed., ser. LIPIcs, vol. 234, 31:1–31:14, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[26] A. Bhattacharyya, S. Kopparty, G. Schoenebeck, M. Sudan, and D. Zuckerman, "Optimal testing of reed–muller codes," in *Proceedings of the 2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, ser. FOCS '10, pp. 488–497, 2010.

[27] A. Bhattacharyya, S. Kopparty, G. Schoenebeck, M. Sudan, and D. Zuckerman, "Optimal testing of Reed–Muller codes," in *51th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2010, October 23–26, 2010, Las Vegas, Nevada, USA*, pp. 488–497, IEEE Computer Society, 2010.

[28] R. E. Blahut, *Algebraic codes for data transmission.* Cambridge university press, 2003.

[29] R. Blahut, "Hypothesis testing and information theory," *IEEE Transactions on Information Theory*, vol. 20, no. 4, pp. 405–417, 1974.

[30] M. Blum, M. Luby, and R. Rubinfeld, "Self-testing/correcting with applications to numerical problems," *J. Comput. Syst. Sci.*, vol. 47, no. 3, pp. 549–595, 1993.

[31] A. Bogdanov and E. Viola, "Pseudorandom bits for polynomials," *SIAM J. Comput.*, vol. 39, no. 6, pp. 2464–2486, 2010.

[32] J. Bourgain and G. Kalai, "Influences of variables and threshold intervals under group symmetries," *Geometric and Functional Analysis*, vol. 7, no. 3, pp. 438–461, 1997.

[33] S. ten Brink, "Convergence of iterative decoding," *Electronics Letters*, vol. 35, no. 10, pp. 806–808, 1999.

[34] R. Calderbank, S. Howard, and S. Jafarpour, "Construction of a large class of deterministic sensing matrices that satisfy a statistical isometry property," *IEEE Journal of Selected Topics in Signal Processing*, vol. 4, no. 2, pp. 358–374, 2010.

[35] R. Calderbank and S. Jafarpour, "Reed Muller sensing matrices and the LASSO," in *International Conference on Sequences and Their Applications*, Springer, pp. 442–463, 2010.

[36] E. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 489–509, 2006.

[37] E. J. Candes, J. K. Romberg, and T. Tao, "Stable signal recovery from incomplete and inaccurate measurements," *Communications on Pure and Applied Mathematics: A Journal Issued by the Courant Institute of Mathematical Sciences*, vol. 59, no. 8, pp. 1207–1223, 2006.

[38] E. J. Candes and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?" *IEEE Transactions on Information Theory*, vol. 52, no. 12, pp. 5406–5425, 2006.

[39] C. Carlet and P. Gaborit, "On the construction of balanced Boolean functions with a good algebraic immunity," in *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, IEEE, pp. 1101–1105, 2005.

[40] D. Chase, "Class of algorithms for decoding block codes with channel measurement information," *IEEE Transactions on Information Theory*, vol. 18, no. 1, pp. 170–182, 1972.

[41] X. Chen and M. Ye, "Cyclically equivariant neural decoders for cyclic codes," in *International Conference on Machine Learning*, PMLR, pp. 1771–1780, 2021.

[42] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *J. ACM*, vol. 45, no. 6, pp. 965–981, 1998.

[43] D. J. Costello and G. D. Forney, "Channel coding: The road to channel capacity," *Proceedings of the IEEE*, vol. 95, no. 6, pp. 1150–1177, 2007.

[44] P. Delsarte and J.-M. Goethals, "Alternating bilinear forms over GF(q)," *Journal of Combinatorial Theory, Series A*, vol. 19, no. 1, pp. 26–50, 1975.

[45] F. Didier, "A new upper bound on the block error probability after decoding over the erasure channel," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4496–4503, 2006.

[46] R. L. Dobrushin, "Mathematical problems in the Shannon theory of optimal coding of information," in *Proc. 4th Berkeley Symp. Mathematics, Statistics, and Probability*, vol. 1, pp. 211–252, 1961.

[47] D. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[48] I. Dumer, "Recursive decoding and its performance for low-rate Reed-Muller codes," *IEEE Transactions on Information Theory*, vol. 50, no. 5, pp. 811–823, 2004.

[49] I. Dumer, "Soft-decision decoding of Reed-Muller codes: A simplified algorithm," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 954–963, 2006.

[50] I. Dumer and P. Farrell, "Erasure correction performance of linear block codes," in *Workshop on Algebraic Coding*, Springer, pp. 316–326, 1993.

[51] I. Dumer and K. Shabunov, "Soft-decision decoding of Reed-Muller codes: Recursive lists," *IEEE Transactions on information theory*, vol. 52, no. 3, pp. 1260–1266, 2006.

[52] I. M. Duursma and R. Kötter, "Error-locating pairs for cyclic codes," *IEEE Transactions on Information Theory*, vol. 40, no. 4, pp. 1108–1121, 1994.

[53] Z. Dvir and S. Gopi, "2-server PIR with subpolynomial communication," *J. ACM*, vol. 63, no. 4, pp. 39:1–39:15, 2016.

[54] A. G. i Fabregas, I. Land, and A. Martinez, "Extremes of random coding error exponents," in *2011 IEEE International Symposium on Information Theory Proceedings*, IEEE, pp. 2896–2898, 2011.

[55] D. Fathollahi, N. Farsad, S. A. Hashemi, and M. Mondelli, "Sparse multi-decoder recursive projection aggregation for Reed–Muller codes," in *2021 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 1082–1087, 2021.

[56] A. Fazeli, H. Hassani, M. Mondelli, and A. Vardy, "Binary linear codes with optimal scaling: Polar codes with large kernels," *IEEE Transactions on Information Theory*, vol. 67, no. 9, pp. 5693–5710, 2021.

[57] *Final report of 3GPP TSG RAN WG1 #87 v1.0.0*. URL: http://www.3gpp.org/ftp/tsg_ran/WG1_RL1/TSGR1_87/Report/.

[58] D. Forney, "On exponential error bounds for random codes on the BSC," *unpublished manuscript*, 2001.

[59] E. Friedgut and G. Kalai, "Every monotone graph property has a sharp threshold," *Proceedings of the American Mathematical Society*, vol. 124, no. 10, pp. 2993–3002, 1996.

[60] R. Gallager, "A simple derivation of the coding theorem and some applications," *IEEE Transactions on Information Theory*, vol. 11, no. 1, pp. 3–18, 1965.

[61] R. Gallager, "The random coding bound is tight for the average code (corresp.)," *IEEE Transactions on Information Theory*, vol. 19, no. 2, pp. 244–246, 1973.

[62] W. Gasarch, "A survey on private information retrieval," in *Bulletin of the EATCS*, Citeseer, 2004.

[63] M. Geiselhart, A. Elkelesh, M. Ebada, S. Cammerer, and S. ten Brink, "Automorphism ensemble decoding of Reed–Muller codes," *IEEE Transactions on Communications*, vol. 69, no. 10, pp. 6424–6438, 2021.

[64] R. R. Green, "A serial orthogonal decoder," *JPL Space Programs Summary*, vol. 37, pp. 247–253, 1966.

[65] V. Guruswami, A. Riazanov, and M. Ye, "Arikan meets Shannon: Polar codes with near-optimal convergence to channel capacity," in *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pp. 552–564, 2020.

[66] V. Guruswami and P. Xia, "Polar codes: Speed of polarization and polynomial gap to capacity," *IEEE Transactions on Information Theory*, vol. 61, no. 1, pp. 3–16, 2015.

[67] R. W. Hamming, "Error detecting and error correcting codes," *The Bell system technical journal*, vol. 29, no. 2, pp. 147–160, 1950.

[68] A. Hammons, P. Kumar, A. Calderbank, N. Sloane, and P. Sole, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 301–319, 1994.

[69] E. Haramaty, A. Shpilka, and M. Sudan, "Optimal testing of multivariate polynomials over small prime fields," *SIAM J. Comput.*, vol. 42, no. 2, pp. 536–562, 2013.

[70] H. Hassani, S. Kudekar, O. Ordentlich, Y. Polyanskiy, and R. Urbanke, "Almost optimal scaling of Reed-Muller codes on BEC and BSC channels," in *2018 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 311–315, 2018.

[71] S. H. Hassani, K. Alishahi, and R. L. Urbanke, "Finite-length scaling for polar codes," *IEEE Transactions on Information Theory*, vol. 60, no. 10, pp. 5875–5898, 2014.

[72] S. H. Hassani, S. B. Korada, and R. Urbanke, "The compound capacity of polar codes," in *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 16–21, 2009.

[73] S. H. Hassani, R. Mori, T. Tanaka, and R. L. Urbanke, "Rate-dependent analysis of the asymptotic behavior of channel polarization," *IEEE Transactions on Information Theory*, vol. 59, no. 4, pp. 2267–2276, 2013.

[74] S. H. Hassani and R. Urbanke, "Universal polar codes," in *2014 IEEE International Symposium on Information Theory*, pp. 1451–1455, 2014.

[75] M. Hayashi, "Information spectrum approach to second-order coding rate in channel coding," *IEEE Transactions on Information Theory*, vol. 55, no. 11, pp. 4947–4966, 2009.

[76] J. Hazla, A. Samorodnitsky, and O. Sberlo, "On codes decoding a constant fraction of errors on the BSC," in *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21–25, 2021*, S. Khuller and V. V. Williams, Eds., pp. 1479–1488, ACM, 2021.

[77] T. Helleseth, T. Kløve, and V. I. Levenshtein, "The simplex codes and other even-weight binary linear codes for error correction," *IEEE Transactions on Information Theory*, vol. 50, no. 11, pp. 2818–2823, 2004.

[78] T. Helleseth, T. Kløve, and V. I. Levenshtein, "Error-correction capability of binary linear codes," *IEEE Transactions on Information Theory*, vol. 51, no. 4, pp. 1408–1423, 2005.

[79] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. Cambridge university press, 2010.

[80] C. S. Jutla, A. C. Patthak, A. Rudra, and D. Zuckerman, "Testing low-degree polynomials over prime fields," *Random Struct. Algorithms*, vol. 35, no. 2, pp. 163–193, 2009.

[81] T. Kasami, S. Lin, and W. Peterson, "New generalizations of the Reed–Muller codes–I: Primitive codes," *IEEE Transactions on Information Theory*, vol. 14, no. 2, pp. 189–199, 1968.

[82] T. Kasami and N. Tokura, "On the weight structure of reed–muller codes," *IEEE Transactions on Information Theory*, vol. 16, no. 6, pp. 752–759, 1970.

[83] T. Kasami, N. Tokura, and S. Azumi, "On the weight enumeration of weights less than 2.5 d of reed–muller codes," *Information and Control*, vol. 30, no. 4, pp. 380–395, 1976.

[84] T. Kaufman, S. Lovett, and E. Porat, "Weight distribution and list-decoding size of Reed–Muller codes," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2689–2696, 2012.

[85] T. Kaufman and D. Ron, "Testing polynomials over general fields," *SIAM J. Comput.*, vol. 36, no. 3, pp. 779–802, 2006.

[86] A. M. Kerdock, "A class of low-rate nonlinear binary codes," *Information and Control*, vol. 20, no. 2, pp. 182–187, 1972.

[87] S. Kopparty and A. Potukuchi, "Syndrome decoding of Reed–Muller codes and tensor decomposition over finite fields," in *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2018, New Orleans, LA, USA, January 7-10, 2018*, pp. 680–691, 2018.

[88] S. B. Korada, A. Montanari, E. Telatar, and R. Urbanke, "An empirical scaling law for polar codes," in *2010 IEEE International Symposium on Information Theory*, pp. 884–888, 2010.

[89] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, E. Şaşoğlu, and R. Urbanke, "Reed-Muller codes achieve capacity on erasure channels," in *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing (STOC)*, ACM, pp. 658–669, 2016.

[90] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, E. Şaşoğlu, and R. Urbanke, "Reed–Muller codes achieve capacity on erasure channels," *IEEE Transactions on Information Theory*, vol. 63, no. 7, pp. 4298–4316, 2017.

[91] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, and R. Urbanke, "Comparing the bit-map and block-map decoding thresholds of Reed–Muller codes on bms channels," in *2016 IEEE International Symposium on Information Theory (ISIT)*, pp. 1755–1759, 2016.

[92] G. Li, M. Ye, and S. Hu, abs+ polar codes: Exploiting more linear transforms on adjacent bits, arXiv:2209.02461, 2022.

[93] G. Li, M. Ye, and S. Hu, adjacent-bits-swapped polar codes: A new code construction to speed up polarization, arXiv:2202.04454, 2022.

[94] M. Lian, C. Häger, and H. D. Pfister, "Decoding Reed–Muller codes using redundant code constraints," in *2020 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 42–47, 2020.

[95] S. Lin, "RM codes are not so bad," in *IEEE Inform. Theory Workshop*, Invited talk, 1993.

[96] S. Lin and D. J. Costello, *Error control coding*. Prentice hall, 2001.

[97] J. H. van Lint, "Kerdock codes and Preparata codes," *Congressus Numerantium*, vol. 39, pp. 25–41, 1983.

[98] J. H. van Lint, *Introduction to coding theory*. Springer, 1999.

[99] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. Elsevier, 1977.

[100] J. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell System Technical Journal*, vol. 42, no. 1, pp. 79–94, 1963.

[101] A. V. Makkuva, X. Liu, M. V. Jamali, H. Mahdavifar, S. Oh, and P. Viswanath, "KO codes: Inventing nonlinear encoding and decoding for reliable wireless communication via deep-learning," in *International Conference on Machine Learning*, PMLR, pp. 7368–7378, 2021.

[102] C. Méasson, A. Montanari, and R. Urbanke, "Maxwell construction: The hidden bridge between iterative and maximum a posteriori decoding," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5277–5307, 2008.

[103] M. Mitzenmacher and E. Upfal, *Probability and Computing – Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, 2005.

[104] M. Mondelli, S. H. Hassani, and R. L. Urbanke, "From polar to Reed-Muller codes: A technique to improve the finite-length performance," *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3084–3091, 2014.

[105] M. Mondelli, S. H. Hassani, and R. L. Urbanke, "Unified scaling of polar codes: Error exponent, scaling exponent, moderate deviations, and error floors," *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 6698–6712, 2016.

[106] M. Mondelli, S. H. Hassani, and R. L. Urbanke, "Construction of polar codes with sublinear complexity," *IEEE Transactions on Information Theory*, vol. 65, no. 5, pp. 2782–2791, 2019.

[107] R. Mori and T. Tanaka, "Performance and construction of polar codes on symmetric binary-input memoryless channels," in *2009 IEEE International Symposium on Information Theory*, pp. 1496–1500, 2009.

[108] R. Mori and T. Tanaka, "Performance of polar codes with the construction using density evolution," *IEEE Communications Letters*, vol. 13, no. 7, pp. 519–521, 2009.

[109] D. E. Muller, "Application of Boolean algebra to switching circuit design and to error detection," *Transactions of the IRE Professional Group on Electronic Computers*, no. 3, pp. 6–12, 1954.

[110] E. Nachmani, E. Marciano, L. Lugosch, W. J. Gross, D. Burshtein, and Y. Be'ery, "Deep learning methods for improved decoding of linear codes," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 119–131, 2018.

[111] A. W. Nordstrom and J. P. Robinson, "An optimum nonlinear code," *Information and Control*, vol. 11, no. 5-6, pp. 613–616, 1967.

[112] R. O'Donnell, *Analysis of boolean functions.* Cambridge University Press, 2014.

[113] R. Pedarsani, S. H. Hassani, I. Tal, and E. Telatar, "On the construction of polar codes," in *2011 IEEE International Symposium on Information Theory Proceedings*, pp. 11–15, 2011.

[114] R. Pellikaan, "On decoding by error location and dependent sets of error positions," *Discrete Mathematics*, vol. 106-107, pp. 369–381, 1992.

[115] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Transactions on Information Theory*, vol. 40, no. 4, pp. 1284–1292, 1994.

[116] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Transactions on Information Theory*, vol. 56, no. 5, pp. 2307–2359, 2010.

[117] Y. Polyanskiy and S. Verdú, "Channel dispersion and moderate deviations limits for memoryless channels," in *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, IEEE, pp. 1334–1339, 2010.

[118] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," *Journal of the ACM (JACM)*, vol. 36, no. 2, pp. 335–348, 1989.

[119] A. Rao and O. Sprumont, on list decoding transitive codes from random errors, 2022.

[120] A. A. Razborov, "Lower bounds on the size of bounded depth circuits over a complete basis with logical addition," *Math. Notes*, vol. 41, no. 4, pp. 333–338, 1987.

[121] I. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *Transactions of the IRE Professional Group on Information Theory*, vol. 4, no. 4, pp. 38–49, 1954.

[122] G. Reeves and H. D. Pfister, "Reed–Muller codes achieve capacity on BMS channels," arXiv:2110.14631, 2021.

[123] T. Richardson and R. Urbanke, *Modern coding theory.* Cambridge university press, 2008.

[124] R. Rossignol, "Threshold for monotone symmetric properties through a logarithmic sobolev inequality," *The Annals of Probability*, vol. 34, no. 5, pp. 1707–1725, 2006.

[125] B. Sakkour, "Decoding of second order Reed-Muller codes with a large number of errors," in *IEEE Information Theory Workshop*, IEEE, pp. 176–178, 2005.

[126] A. Samorodnitsky, "An improved bound on ℓ_q norms of noisy functions," *arXiv preprint arXiv:2010.02721*, 2020.

[127] A. Samorodnitsky, "An upper bound on ℓ_q norms of noisy functions," *IEEE Transactions on Information Theory*, vol. 66, no. 2, pp. 742–748, 2020.
[128] A. Samorodnitsky and O. Sberlo, "On codes decoding a constant fraction of errors on the BSC," arXiv:2008.07236, 2020.
[129] E. Santi, C. Hager, and H. D. Pfister, "Decoding Reed-Muller codes using minimum-weight parity checks," in *2018 IEEE International Symposium on Information Theory (ISIT)*, IEEE, pp. 1296–1300, 2018.
[130] R. Saptharishi, A. Shpilka, and B. L. Volk, "Efficiently decoding Reed–Muller codes from random errors," *IEEE Transactions on Information Theory*, vol. 63, no. 4, pp. 1954–1960, 2017.
[131] E. Şaşoğlu, "Polar coding theorems for discrete systems," Ph.D. dissertation, EPFL, 2011.
[132] E. Şaşoğlu, "Polarization and polar codes," *Foundations and Trends® in Communications and Information Theory*, vol. 8, no. 4, pp. 259–381, 2012.
[133] E. Şaşoğlu and L. Wang, "Universal polarization," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 2937–2946, 2016.
[134] O. Sberlo and A. Shpilka, "On the performance of Reed–Muller codes with respect to random errors and erasures," in *Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, SIAM, pp. 1357–1376, 2020.
[135] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[136] A. Shamir, "Ip= pspace," *Journal of the ACM (JACM)*, vol. 39, no. 4, pp. 869–877, 1992.
[137] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.
[138] C. E. Shannon, R. G. Gallager, and E. R. Berlekamp, "Lower bounds to error probability for coding on discrete memoryless channels. I," *Information and Control*, vol. 10, no. 1, pp. 65–103, 1967.

[139] A. Ta-Shma, D. Zuckerman, and S. Safra, "Extractors from reed–muller codes," *J. Comput. Syst. Sci.*, vol. 72, no. 5, pp. 786–812, 2006.

[140] N. Shulman and M. Feder, "Random coding techniques for nonrandom codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 2101–2104, 1999.

[141] V. M. Sidel'nikov and A. S. Pershakov, "Decoding of Reed-Muller codes with a large number of errors," *Problemy Peredachi Informatsii*, vol. 28, no. 3, pp. 80–94, 1992.

[142] N. Sloane and E. Berlekamp, "Weight enumerator for second-order Reed–Muller codes," *IEEE Transactions on Information Theory*, vol. 16, no. 6, pp. 745–751, 1970.

[143] N. Sloane and E. Berlekamp, "Weight enumerator for second-order Reed–Muller codes," *IEEE Transactions on Information Theory*, vol. 16, no. 6, pp. 745–751, 1970.

[144] V. Strassen, "Asymptotische abschatzugen in shannon's informationstheorie," in *Transactions of the Third Prague Conference on Information Theory etc, 1962. Czechoslovak Academy of Sciences, Prague*, pp. 689–723, 1962.

[145] I. Tal and A. Vardy, "How to construct polar codes," *IEEE Transactions on Information Theory*, vol. 59, no. 10, pp. 6562–6582, 2013.

[146] I. Tal and A. Vardy, "List decoding of polar codes," *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2213–2226, 2015.

[147] L. G. Tallini and B. Bose, "Reed–Muller codes, elementary symmetric functions and asymmetric error correction," in *2011 IEEE International Symposium on Information Theory Proceedings*, IEEE, pp. 1051–1055, 2011.

[148] J. P. Tillich and G. Zémor, "Discrete isoperimetric inequalities and the probability of a decoding error," *Combinatorics, Probability and Computing*, vol. 9, no. 5, pp. 465–479, 2000.

[149] L. Trevisan, "Some applications of coding theory in computational complexity," *CoRR*, vol. cs.CC/0409044, 2004.

[150] H. P. Wang and I. M. Duursma, "Polar codes' simplicity, random codes' durability," *IEEE Transactions on Information Theory*, vol. 67, no. 3, pp. 1478–1508, 2021.

[151] L. Weiss, "On the strong converse of the coding theorem for symmetric channels without memory," *Quarterly of Applied Mathematics*, vol. 18, no. 3, pp. 209–214, 1960.

[152] J. Wolfowitz, "The coding of messages subject to chance errors," *Illinois Journal of Mathematics*, vol. 1, no. 4, pp. 591–606, 1957.

[153] M. Ye and E. Abbe, "Recursive projection-aggregation decoding of Reed–Muller codes," *IEEE Transactions on Information Theory*, vol. 66, no. 8, pp. 4948–4965, 2020.

[154] S. Yekhanin, "Locally decodable codes," *Foundations and Trends® in Theoretical Computer Science*, vol. 6, no. 3, pp. 139–255, 2012.