Locally Decodable Codes

Locally Decodable Codes

Sergey Yekhanin

Microsoft Research Silicon Valley
Mountain View, CA 94043
USA
yekhanin@microsoft.com

the essence of knowledge

Boston – Delft

Foundations and Trends® in Theoretical Computer Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
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 S. Yekhanin, Locally Decodable Codes, Foundation and Trends® in Theoretical Computer Science, vol 6, no 3, pp 139–255, 2010

ISBN: 978-1-60198-544-6

Foundations and Trends® in
Theoretical Computer Science
Volume 6 Issue 3, 2010

Editorial Scope

Foundations and Trends® in Theoretical Computer Science will publish survey and tutorial articles in the following topics:

- Algorithmic game theory
- Computational algebra
- Computational aspects of combinatorics and graph theory
- Computational aspects of communication
- Computational biology
- Computational complexity
- Computational geometry
- Computational learning
- Computational Models and Complexity
- Computational Number Theory
- Cryptography and information security
- Data structures
- Database theory
- Design and analysis of algorithms
- Distributed computing
- Information retrieval
- Operations Research
- Parallel algorithms
- Quantum Computation
- Randomness in Computation

Information for Librarians

Foundations and Trends® in Theoretical Computer Science, 2010, Volume 6, 4 issues. ISSN paper version 1551-305X. ISSN online version 1551-3068. Also available as a combined paper and online subscription.

Foundations and Trends® in
Theoretical Computer Science
Vol. 6, No. 3 (2010) 139–255

DOI: 10.1561/0400000030

Locally Decodable Codes

Sergey Yekhanin

Microsoft Research Silicon Valley, 1065 La Avenida, Mountain View, CA 94043, USA, yekhanin@microsoft.com

Abstract

Locally decodable codes are a class of "error-correcting codes." Error-correcting codes help to ensure reliability when transmitting information over noisy channels. They allow a sender of a message to add redundancy to messages, encoding bit strings representing messages into longer bit strings called codewords, in a way that the message can still be recovered even if a certain fraction of the codeword bits are corrupted. Classical error-correcting codes however do not work well when one is working with massive messages, because their decoding time increases (at least) linearly with the length of the message. As a result in typical applications the message is first partitioned into small blocks, each of which is then encoded separately. Such encoding allows efficient random-access retrieval of the message, but yields poor noise resilience.

Locally decodable codes are codes intended to address this seeming conflict between efficient retrievability and reliability. They are codes that simultaneously provide efficient random-access retrieval and high noise resilience by allowing reliable reconstruction of an arbitrary bit of the message from looking at only a small number of randomly chosen codeword bits. This review introduces and motivates locally decodable codes, and discusses the central results of the subject. In particular, local decodability comes at the price of certain loss in terms of code efficiency, and this review describes the currently known limits on the efficiency that is achievable.

Contents

1

Introduction

Locally Decodable Codes (LDCs) are a special kind of error-correcting codes. Error-correcting codes are used to ensure reliable transmission of information over noisy channels as well as to ensure reliable storage of information on a medium that may be partially corrupted over time (or whose reading device is subject to errors).

In both of these applications the message is typically partitioned into small blocks and then each block is encoded separately. Such encoding strategy allows efficient random-access retrieval of the information, since one needs to decode only the portion of data one is interested in. Unfortunately, this strategy yields very poor noise resilience, since in case even a single block (out of possibly tens of thousands) is completely corrupted some information is lost. In view of this limitation, it would seem preferable to encode the whole message into a single codeword of an error-correcting code. Such solution clearly improves the robustness to noise, but is also hardly satisfactory, since one now needs to look at the whole codeword in order to recover any particular bit of the message (at least when classical error-correcting codes are used). Such decoding complexity is prohibitive for modern massive data-sets.

Locally decodable codes are error-correcting codes that avoid the problem mentioned above by having extremely efficient *sublinear-time* decoding algorithms. More formally, an r-query locally decodable code C encodes k-bit messages $\mathbf{x}$ in such a way that one can probabilistically recover any bit $\mathbf{x}(i)$ of the message by querying only r bits of the (possibly corrupted) codeword $C(\mathbf{x})$, where r can be as small as 2.

Example 1.1. The classical Hadamard code encoding k-bit messages to 2^k-bit codewords provides the simplest nontrivial example of locally decodable codes. In what follows, let $[k]$ denote the set $\{1,\ldots,k\}$. Every coordinate in the Hadamard code corresponds to one (of 2^k) subsets of $[k]$ and stores the XOR of the corresponding bits of the message $\mathbf{x}$. Let $\mathbf{y}$ be an (adversarially corrupted) encoding of $\mathbf{x}$. Given an index $i \in [k]$ and $\mathbf{y}$, the Hadamard decoder picks a set S in $[k]$ uniformly at random and outputs the XOR of the two coordinates of $\mathbf{y}$ corresponding to sets S and $S \vartriangle \{i\}$. (Here, $\vartriangle$ denotes the symmetric difference of sets such as $\{1,4,5\} \vartriangle \{4\} = \{1,5\}$, and $\{1,4,5\} \vartriangle \{2\} = \{1,2,4,5\}$). It is not difficult to verify that if $\mathbf{y}$ differs from the correct encoding of $\mathbf{x}$ in at most δ fraction of coordinates than with probability $1 - 2\delta$ both decoder's queries go to uncorrupted locations. In such case, the decoder correctly recovers the ith bit of $\mathbf{x}$. The Hadamard code allows for a super-fast recovery of the message bits (such as, given a codeword corrupted in 0.1 fraction of coordinates, one is able to recover any bit of the message with probability 0.8 by reading only two codeword bits).

The main parameters of interest in locally decodable codes are the codeword length and the query complexity. The length of the code measures the amount of redundancy that is introduced into the message by the encoder. The query complexity counts the number of bits that need to be read from the (corrupted) codeword in order to recover a single bit of the message. Ideally, one would like to have both of these parameters as small as possible. One however cannot minimize the length and the query complexity simultaneously. There is a trade-off. On one end of the spectrum we have classical error correcting codes that have both query complexity and codeword length proportional to the message length. On the other end we have the Hadamard code that has query complexity 2 and codeword length exponential in the message length. Establishing the optimal trade-off between the length and the query complexity is the major goal of research in the area of locally decodable codes.

Interestingly, the natural application of locally decodable codes to data transmission and storage described above is neither the historically earliest nor the most important. LDCs have a host of applications in other areas of theoretical computer science.

1.1 Families of Locally Decodable Codes

One can informally classify the known families of locally decodable codes into three broad categories based on the relation between the message length k and the query complexity r.

1. Low query complexity. Here we look at codes where r is a constant independent of k or some very slowly growing function of k. Such codes have important applications in cryptography to constructions of private information retrieval schemes. Early examples of such codes are the Hadamard code and the Reed Muller (RM) code that is sketched below.

Reed Muller code. The code is specified by three integer parameters, an alphabet size q, a number of variables n, and a degree $d < q-1$. The code encodes $k = \binom{n+d}{d}$-long q-ary messages to q^n-long codewords. We fix a certain collection of vectors $W = \{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ in $\mathbb{F}_q^n$. A message $\mathbf{x}$ is encoded by a complete $\mathbb{F}_q^n$-evaluation of a polynomial $F \in \mathbb{F}_q[z_1, \ldots, z_n]$ of degree up to d, such that for all $i \in [k]$, $\mathbf{x}(i) = F(\mathbf{w}_i)$. Our choice of W ensures that such a polynomial exists for any $\mathbf{x}$. Given $i \in [k]$ and a δ-corrupted evaluation of F the Reed Muller decoder needs to recover the value of F at $\mathbf{w}_i$. To do this the decoder picks a random affine line L through $\mathbf{w}_i$ and reads the (corrupted) values of F at $d+1$ points of $L \setminus \{\mathbf{w}_i\}$. Next, the decoder uses univariate polynomial interpolation to recover the restriction of F to L. Each query of the decoder samples a random location, thus with probability at least $1-(d+1)\delta$, it never queries a corrupted coordinate and decodes correctly. Setting d and q to be constant and letting n grow one gets r-query codes of length $N = \exp(k^{1/(r-1)})$.

Other families of codes in this category are the recursive codes of Beimel et al. and the Matching Vector (MV) codes. MV codes offer the best-known trade-off between the query complexity and the codeword length of locally decodable codes for small values of query complexity. In particular they give three-query codes of length $N(k)$ where N grows slower than any function of the form $\exp(k^{\epsilon})$.[1] In this review we cover the construction of matching vector codes in full detail.

2. Medium query complexity. Here we look at codes with $r = \log^c k$, for some $c > 1$. Such codes have been used in constructions of probabilistically checkable proofs. They also have applications to worst-case to average-case reductions in computational complexity theory. Setting $d = n^c$, $q = \Theta(d)$ in the definition of Reed Muller codes, and letting the number of variables n grow to infinity yields codes of query complexity $\log^c k$ and codeword length $N = k^{1+1/(c-1)+o(1)}$. These are the best-known locally decodable codes in this regime.

3. High query complexity. Here we look at codes with $r = k^{\epsilon}$, for some $\epsilon > 0$. This is the only regime where we (so far) have locally decodable codes of positive rate, that is, codeword length proportional to message length. Such codes are potentially useful for data transmission and storage applications. The early examples of such codes are the Reed Muller codes with the number of variables $n = 1/\epsilon$, growing d, and $q = \Theta(d)$. Such setting of parameters yields codes of query complexity $r = k^{\epsilon}$ and rate $\epsilon^{\Theta(1/\epsilon)}$. The rate is always below $1/2$. Another family of codes in the high query complexity category is the family of multiplicity codes. Multiplicity codes are based on evaluating high degree multivariate polynomials together with their partial derivatives. Multiplicity codes extend Reed Muller codes; inherit the local-decodability of these codes, and at the same time achieve better tradeoffs and flexibility in their rate and query complexity. In particular for all $\alpha, \epsilon > 0$ they yield locally decodable codes of query complexity $r = k^{\epsilon}$ and rate $1 - \alpha$. In this survey we cover multiplicity codes in full detail.

---

[1] Throughout the survey we use the standard notation $\exp(x) = 2^{O(x)}$.

1.2 Organization

The goal of this survey is to summarize the state-of-the-art in locally decodable codes. Our main focus is on multiplicity codes and on matching vector codes. The survey is organized into eight sections.

In Section 2 we formally define locally decodable codes and give a detailed treatment of Reed Muller codes. In Section 3 we study multiplicity codes. We show how multiplicity codes generalize Reed Muller codes and obtain bounds on their rate and query complexity.

In Section 4 we introduce the concept of matching vectors and present a transformation that turns an arbitrary family of such vectors into a family of locally decodable (matching vector) codes. We provide a detailed comparison between the parameters of matching vector codes based on the currently largest known matching families and Reed Muller codes. Section 5 contains a systematic study of families of matching vectors. We cover several constructions as well as impossibility results.

In Section 6 we deal with lower bounds for the codeword length of locally decodable codes. In Section 7 we discuss some prominent applications of locally decodable codes, namely, applications to private information retrieval schemes, secure multi party computation, and average case complexity. Finally, in the last section we list (and comment on) the most exciting open questions relating to locally decodable codes and private information retrieval schemes.

1.3 Notes

We now review the history of locally decodable codes. Ideas behind the early constructions of LDCs go back to classical codes [77, Section 10], named after their discoverers, Reed and Muller. Muller discovered the codes [70] in the 1950s, and Reed proposed the majority logic decoding [81]. Since then, local decodability of these codes has been exploited extensively. In particular, in the early 1990s a number of theoretical computer science papers developed and used local decoding algorithms for some variants of these codes [5, 11, 24, 43, 44, 67, 78]. The first formal definition of locally decodable codes was given however only in

2000 by Katz and Trevisan [60], who cited Leonid Levin for inspiration. See also [90].

Today there are three families of locally decodable codes that surpass Reed Muller codes in terms of query complexity vs. codeword length trade-off. These are the recursive codes of Beimel et al. [15] (see also [97]), the matching vector codes [18, 19, 35, 38, 59, 61, 69, 79, 85, 99], and the multiplicity codes [63]. Matching vector codes offer the best-known trade-off between the query complexity and the codeword length of locally decodable codes for small values of query complexity. Multiplicity codes are the best-known locally decodable codes for large values of query complexity.

The first lower bounds for the codeword length of locally decodable codes were obtained in [60]. Further work on lower bounds includes [31, 41, 48, 62, 74, 94, 95, 96]. It is known that 1-query LDCs do not exist [60]. The length of optimal 2-query LDCs was settled in [62] and is exponential in the message length. However for values of query complexity $r \geq 3$ we are still very far from closing the gap between lower and upper bounds. Specifically, the best lower bounds to date are of the form $\tilde{\Omega}(k^{1+1/(\lceil r/2 \rceil - 1)})$ due to [95], while the best upper bounds are super-polynomial in k when r is a constant [38, 69].

References

[1] N. Alon, "Eigenvalues, geometric expanders, sorting in rounds, amd Ramsey theory," *Combinatorica*, vol. 6, pp. 207–219, 1986.

[2] N. Alon and J. Spencer, *The Probabilistic Method.* 2000.

[3] A. Ambainis, "Upper bound on the communication complexity of private information retrieval," in *International Colloquium on Automata, Languages and Programming (ICALP)*, vol. 1256 of Lecture Notes in Computer Science, pp. 401–407, 1997.

[4] S. Arora and M. Sudan, "Improved low-degree testing and its applications," *Combinatorica*, vol. 23, pp. 365–426, 2003.

[5] L. Babai, L. Fortnow, L. Levin, and M. Szegedy, "Checking computations in polylogarithmic time," in *ACM Symposium on Theory of Computing (STOC)*, pp. 21–31, 1991.

[6] L. Babai and P. Frankl, *Linear Algebra Methods in Combinatorics.* 1998.

[7] B. Barak, Z. Dvir, A. Wigderson, and A. Yehudayoff, "Rank bounds for design matrices with applications to combinatorial geometry and locally correctable codes," in *ACM Symposium on Theory of Computing (STOC)*, 2011.

[8] B. Barak, A. Rao, R. Shaltiel, and A. Wigderson, "2-source dispersers for sub-polynomial entropy and Ramsey graphs beating the Frankl-Wilson construction," in *ACM Symposium on Theory of Computing (STOC)*, pp. 671–680, 2006.

[9] O. Barkol, Y. Ishai, and E. Weinreb, "On locally decodable codes, self-correctable codes, and t-private PIR," in *International Workshop on Randomization and Computation (RANDOM)*, pp. 311–325, 2007.

[10] D. A. Barrington, R. Beigel, and S. Rudich, “Representing Boolean functions as polynomials modulo composite numbers,” *Computational Complexity*, vol. 4, pp. 67–382, 1994.

[11] D. Beaver and J. Feigenbaum, “Hiding instances in multioracle queries,” in *International Symposium on Theoretical Aspects of Computer Science (STACS)*, vol. 415 of Lecture Notes in Computer Science, pp. 37–48, 1990.

[12] D. Beaver, J. Feigenbaum, J. Kilian, and P. Rogaway, “Security with low communication overhead,” in *International Cryptology Conference (CRYPTO)*, pp. 62–76, 1990.

[13] D. Beaver, S. Micali, and P. Rogaway, “The round complexity of secure protocols,” in *ACM Symposium on Theory of Computing (STOC)*, pp. 503–513, 1990.

[14] A. Beimel, Y. Ishai, and E. Kushilevitz, “General constructions for information-theoretic private information retrieval,” *Journal of Computer and System Sciences*, vol. 71, pp. 213–247, 2005.

[15] A. Beimel, Y. Ishai, E. Kushilevitz, and J.-F. Raymond, “Breaking the $O(n^{1/(2k-1)})$ barrier for information-theoretic private information retrieval,” in *IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 261–270, 2002.

[16] A. Beimel, Y. Ishai, and T. Malkin, “Reducing the servers’ computation in private information retrieval: PIR with preprocessing,” in *International Cryptology Conference (CRYPTO)*, vol. 1880 of Lecture Notes in Computer Science, pp. 56–74, 2000.

[17] A. Beimel and Y. Stahl, “Robust information theoretic private information retrieval,” in *Conference on Security in Communication Networks*, 2002.

[18] A. Ben-Aroya, K. Efremenko, and A. Ta-Shma, “Local list decoding with a constant number of queries,” in *IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 715–722, 2010.

[19] A. Ben-Aroya, K. Efremenko, and A. Ta-Shma, “A note on amplifying the error-tolerance of locally decodable codes,” in *Electronic Colloquium on Computational Complexity (ECCC) TR10-134*, 2010.

[20] A. Ben-Aroya, O. Regev, and R. de Wolf, “A hypercontractive inequality for matrix-valued functions with applications to quantum computing and LDCs,” in *IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 477–486, 2008.

[21] M. Ben-Or, S. Goldwasser, and A. Wigderson, “Completeness theorems for non-cryptographic fault-tolerant distributed computation,” in *ACM Symposium on Theory of Computing (STOC)*, pp. 1–10, 1988.

[22] A. Bhattacharyya, Z. Dvir, S. Saraf, and A. Shpilka, “Tight lower bounds for 2-query LCCs over finite fields,” in *IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 638–647, 2011.

[23] M. Blum and S. Kannan, “Designing programs that check their work,” in *ACM Symposium on Theory of Computing (STOC)*, pp. 86–97, 1989.

[24] M. Blum, M. Luby, and R. Rubinfeld, “Self-testing/correcting with applications to numerical problems,” *Journal of Computer and System Sciences*, vol. 47, pp. 549–595, 1993.

[25] C. Cachin, S. Micali, and M. Stadler, “Computationally private information retrieval with polylogarithmic communication,” in *International Cryptology Conference (EUROCRYPT)*, vol. 1592 of Lecture Notes in Computer Science, pp. 402–414, 1999.
[26] P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*. 1994.
[27] D. Chaum, C. Crepeau, and I. Damgard, “Multiparty unconditionally secure protocols,” in *ACM Symposium on Theory of Computing (STOC)*, pp. 11–19, 1988.
[28] V. Chen, E. Grigorescu, and R. de Wolf, “Efficient and error-correcting data structures for membership and polynomial evaluation,” in *Symposium on Theoretical Aspects of Computer Science (STACS)*, 2010.
[29] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, “Private information retrieval,” *Journal of the ACM*, vol. 45, pp. 965–981, 1998.
[30] R. de Wolf, “Error-correcting data structures,” in *Annual Symposium on Theoretical Aspects of Computer Science (STACS 09)*, pp. 313–324, 2009.
[31] A. Deshpande, R. Jain, T. Kavitha, S. Lokam, and J. Radhakrishnan, “Better lower bounds for locally decodable codes,” in *IEEE Computational Complexity Conference (CCC)*, pp. 184–193, 2002.
[32] G. Di-Crescenzo, Y. Ishai, and R. Ostrovsky, “Universal service-providers for private information retrieval,” *Journal of Cryptology*, vol. 14, pp. 37–74, 2001.
[33] A. Drucker and R. de Wolf, *Quantum Proofs for Classical Theorems*. Arxiv 0910.3376, 2009.
[34] Z. Dvir, “On matrix rigidity and locally self-correctable codes,” in *IEEE Computational Complexity Conference (CCC)*, pp. 102–113, 2010.
[35] Z. Dvir, P. Gopalan, and S. Yekhanin, “Matching vector codes,” *SIAM Journal on Computing*, 2011. (to appear).
[36] Z. Dvir, S. Kopparty, S. Saraf, and M. Sudan, “Extensions to the method of multiplicities, with applications to Kakeya sets and mergers,” in *IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 181–190, 2009.
[37] Z. Dvir and A. Shpilka, “Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits,” *SIAM Journal on Computing*, vol. 36, no. 5, pp. 1404–1434, 2006.
[38] K. Efremenko, “3-query locally decodable codes of subexponential length,” in *ACM Symposium on Theory of Computing (STOC)*, pp. 39–44, 2009.
[39] P. Elias, *List Decoding for Noisy Channels*. Research laboratory for electronics, MIT, 1957.
[40] G. D. Forney, *Concatenated Codes*. Cambridge: MIT Press, 1966.
[41] A. Gal and A. Mills, “Three query locally decodable codes with higher correctness require exponential length,” in *International Symposium on Theoretical Aspects of Computer Science (STACS)*, pp. 673–684, 2011.
[42] W. Gasarch, “A survey on private information retrieval,” *The Bulletin of the EATCS*, vol. 82, pp. 72–107, 2004.
[43] P. Gemmell, R. Lipton, R. Rubinfeld, M. Sudan, and A. Wigderson, “Self testing/correcting for polynomials and for approximate functions,” in *ACM Symposium on Theory of Computing (STOC)*, pp. 32–42, 1991.
[44] P. Gemmell and M. Sudan, “Highly resilient correctors for polynomials,” *Information Processing Letters*, vol. 43, pp. 169–174, 1992.

[45] C. Gentry and Z. Ramzan, "Single-database private information retrieval with constant communication rate," in *International Colloquium on Automata, Languages and Programming (ICALP)*, pp. 803–815, 2005.

[46] Y. Gertner, S. Goldwasser, and T. Malkin, "A random server model for private information retrieval," in *International Workshop on Randomization and Computation (RANDOM)*, vol. 1518 of Lecture Notes in Computer Science, pp. 200–217, 1998.

[47] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, "Protecting data privacy in private information retrieval schemes," *Journal of Computer and System Sciences*, vol. 60, pp. 592–629, 2000.

[48] O. Goldreich, H. Karloff, L. Schulman, and L. Trevisan, "Lower bounds for locally decodable codes and private information retrieval," in *IEEE Computational Complexity Conference (CCC)*, pp. 175–183, 2002.

[49] P. Gopalan, "Computing with polynomials over composites," PhD Thesis, Georgia Institute of Technology, 2006.

[50] V. Grolmusz, "Constructing set-systems with prescribed intersection sizes," *Journal of Algorithms*, vol. 44, pp. 321–337, 2002.

[51] V. Grolmusz, "Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs," *Combinatorica*, vol. 20, pp. 71–86, 2000.

[52] V. Guruswami, "List decoding of error-correcting codes," PhD Thesis, Massachusetts Institite of Technology, 2001.

[53] V. Guruswami and A. Rudra, "Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy," *IEEE Transactions on Information Theory*, vol. 54, pp. 135–150, 2008.

[54] V. Guruswami, A. Sahai, and M. Sudan, "Soft-decision decoding of Chinese Remainder Codes," in *Proceedings of the IEEE Symposium on Foundations of Computer Science*, pp. 159–168, Redondo Beach, California, November 12–14 2000.

[55] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometric codes," *IEEE Transactions on Information Theory*, vol. 45, pp. 1757–1767, 1999.

[56] G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*. Oxford: Clarendon Press, 1985.

[57] A. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Problems of Information Transmission*, vol. 9, pp. 177–183, 1973.

[58] Y. Ishai and E. Kushilevitz, "On the hardness of information-theoretic multiparty computation," in *Eurocrypt 2004*, vol. 3027 of Lecture Notes in Computer Science, pp. 439–455, 2004.

[59] T. Itoh and Y. Suzuki, "New constructions for query-efficient locally decodable codes of subexponential length," *IEICE Transactions on Information and Systems*, pp. 263–270, 2010.

[60] J. Katz and L. Trevisan, "On the efficiency of local decoding procedures for error-correcting codes," in *ACM Symposium on Theory of Computing (STOC)*, pp. 80–86, 2000.

[61] K. S. Kedlaya and S. Yekhanin, "Locally decodable codes from nice subsets of finite fields and prime factors of Mersenne numbers," *SIAM Journal on Computing*, vol. 38, pp. 1952–1969, 2009.

[62] I. Kerenidis and R. de Wolf, "Exponential lower bound for 2-query locally decodable codes via a quantum argument," *Journal of Computer and System Sciences*, vol. 69, pp. 395–420, 2004.

[63] S. Kopparty, S. Saraf, and S. Yekhanin, "High-rate codes with sublinear-time decoding," in *ACM Symposium on Theory of Computing (STOC)*, pp. 167–176, 2011.

[64] E. Kushilevitz and R. Ostrovsky, "Replication is not needed: Single-database computationally-private information retrieval," in *IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 364–373, 1997.

[65] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge: Cambridge University Press, 1983.

[66] H. Lipmaa, "An oblivious transfer protocol with log-squared communication," Technical Report 2004/063, International Association for Cryptologic Research, 2004.

[67] R. Lipton, "Efficient checking of computations," in *International Symposium on Theoretical Aspects of Computer Science (STACS)*, vol. 415 of Lecture Notes in Computer Science, pp. 207–215, 1990.

[68] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, New York: North Holland, 1977.

[69] Y. Meng Chee, T. Feng, S. Ling, H. Wang, and L. Zhang, "Query-efficient locally decodable codes of subexponential length," in *Electronic Colloquium on Computational Complexity (ECCC)*, TR10-173, 2010.

[70] D. E. Muller, "Application of boolean algebra to switching circuit design and to error detection," *IEEE Transactions on Computers*, vol. 3, pp. 6–12, 1954.

[71] M. Naor and B. Pinkas, "Oblivious transfer and polynomial evaluation," in *ACM Symposium on Theory of Computing (STOC)*, pp. 245–254, 1999.

[72] A. Nayak, "Optimal lower bounds for quantum automata and random access codes," in *IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 369–377, 1999.

[73] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2000.

[74] K. Obata, "Optimal lower bounds for 2-query locally decodable linear codes," in *International Workshop on Randomization and Computation (RANDOM)*, vol. 2483 of Lecture Notes in Computer Science, pp. 39–50, 2002.

[75] R. Ostrovsky and V. Shoup, "Private information storage," in *ACM Symposium on Theory of Computing (STOC)*, pp. 294–303, 1997.

[76] F. Parvaresh and A. Vardy, "Correcting errors beyond the Guruswami-Sudan radius in polynomial time," in *46th IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 285–294, 2005.

[77] W. W. Peterson and E. J. Weldon Jr., *Error Correcting Codes*. 1972.

[78] A. Polishchuk and D. Spielman, "Nearly-linear size holographic proofs," in *ACM Symposium on Theory of Computing (STOC)*, pp. 194–203, 1994.

[79] P. Raghavendra, "A note on Yekhanin's locally decodable codes," in *Electronic Colloquium on Computational Complexity (ECCC)*, TR07-016, 2007.

[80] A. Razborov and S. Yekhanin, "An $\Omega(n^{1/3})$ lower bound for bilinear group based private information retrieval," *Theory of Computing*, vol. 3, pp. 221–238, 2007.

[81] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *IEEE Transactions on Information Theory*, vol. 4, pp. 38–49, 1954.

[82] A. Romashchenko, "Reliable computations based on locally decodable codes," in *International Symposium on Theoretical Aspects of Computer Science (STACS)*, vol. 3884 of Lecture Notes in Computer Science, pp. 537–548, 2006.

[83] M. Rozenbloom and M. Tsfasman, "Codes for the m-metric," *Problems Information Transmission*, vol. 33, pp. 45–52, 1997.

[84] S. Saraf and M. Sudan, "Improved lower bound on the size of Kakeya sets over finite fields," *Analysis and PDE*, vol. 1, pp. 375–379, 2008.

[85] S. Saraf and S. Yekhanin, "Noisy interpolation of sparse polynomials, and applications," in *IEEE Computational Complexity Conference (CCC)*, 2011.

[86] J. Sgall, "Bounds on pairs of families with restricted intersections," *Combinatorica*, vol. 19, pp. 555–566, 1999.

[87] V. Shoup, *A Computational Introduction to Number Theory and Algebra*. Cambridge: Cambridge University Press, 2005.

[88] M. Sudan, "Ideal error-correcting codes: Unifying algebraic and number-theoretic algorithms," in *AAECC*, pp. 36–45, 2001.

[89] M. Sudan, *Personal Communication*. 2009.

[90] M. Sudan, L. Trevisan, and S. Vadhan, "Pseudorandom generators without the XOR lemma," in *ACM Symposium on Theory of Computing (STOC)*, pp. 537–546, 1999.

[91] G. Tardos and D. Barrington, "A lower bound of the mod 6 degree of the OR function," *Computational Complexity*, vol. 7, pp. 99–108, 1998.

[92] L. Trevisan, *Coding Theory and Complexity*. Lecture Notes, 2003.

[93] L. Trevisan, "Some applications of coding theory in computational complexity," *Quaderni di Matematica*, vol. 13, pp. 347–424, 2004.

[94] S. Wehner and R. de Wolf, "Improved lower bounds for locally decodable codes and private information retrieval," in *International Colloquium on Automata, Languages and Programming (ICALP)*, vol. 3580 of Lecture Notes in Computer Science, pp. 1424–1436, 2005.

[95] D. Woodruff, "New lower bounds for general locally decodable codes," in *Electronic Colloquium on Computational Complexity (ECCC)*, TR07-006, 2007.

[96] D. Woodruff, "A quadratic lower bound for three query linear locally decodable codes over any field," in *International Workshop on Randomization and Computation (RANDOM)*, 2010.

[97] D. Woodruff and S. Yekhanin, "A geometric approach to information theoretic private information retrieval," in *IEEE Computational Complexity Conference (CCC)*, pp. 275–284, 2005.

[98] C. Xing, "Nonlinear codes from algebraic curves improving the Tsfasman-Vladut-Zink bound," *IEEE Transactions on Information Theory*, vol. 49, pp. 1653–1657, 2003.

[99] S. Yekhanin, "Towards 3-query locally decodable codes of subexponential length," *Journal of the ACM*, vol. 55, pp. 1–16, 2008.

[100] S. Yekhanin, "Private information retrieval," *Communications of the ACM*, vol. 53, no. 4, pp. 68–73, 2010.