Aidan W. Murphy

Dr.Aidan.Murphy@gmail.com ■ Home Page ■ LinkedIn

RESEARCH STATEMENT

Introduction

One of the largest areas of research in applied algebra is the field of error-correcting codes, which started in the late 1940s [5, 16]. Coding theory focuses on storing information so that it gains resilience to the loss or corruption, and has found applications in many areas of information storage or transmission.

This widespread application is especially true of Reed-Solomon codes, which use polynomials over finite fields to encode information [15]. More specifically, Reed-Solomon codes form the basis for CD and DVD technology, enable communications with the Voyager probes, and more [21]. A modern application of error-correcting codes is within the field of distributed storage, inspired by the server storage systems of large tech companies such as Google, Amazon, and Microsoft. This has been an active area of research for the past decade [2, 3, 19].

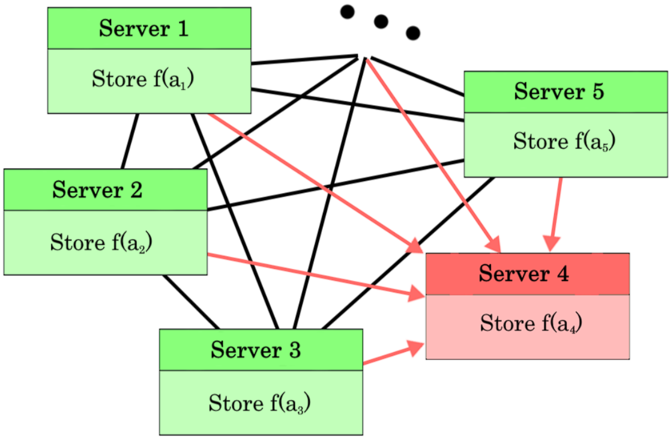

Figure 1: Information distributed over a set of servers, sending information along red connections to repair the information corrupted in Server 4. Graphic from [20].

The success of Reed-Solomon codes has inspired much work in the theory of error correction. An important instance of this is the class of algebraic geometry (AG) codes, which are formed by considering more general algebraic curves over finite fields [4]. Comparing to Reed-Solomon codes, classical AG codes use the rational points on algebraic curves instead of points on an affine line, and use the Riemann-Roch spaces of certain divisors as evaluation functions instead of just univariate polynomials. The study of these and similar codes forms a rich combination of algebraic geometry and classical coding theory.

Past Work

Locally recoverable codes (LRCs) are designed for applications involving distributed storage of information, and perform error correction by accessing less information than previous decoding methods. This can conserve the bandwidth on the communication between servers where partial information is stored, leading to faster information recovery times. Another measure of LRCs is their availability, which is the number of unique ways that the same piece of information can be recovered. These unique sets are called repair groups. Algebraic curves over finite fields can lend themselves naturally to forming LRCs. This is done by considering the intersections of lines with the curve, and using the points from each intersection to perform local error correction; these codes are called Hermitian-lifted codes [6].

The Hermitian-lifted code construction is of special interest because of the number of repair groups formed, and is a place where other LRCs struggle. Hermitian-lifted codes also offer a vastly improved asymptotic storage than classical Hermitian codes. My dissertation work extends this to other algebraic curves beyond the Hermitian curve, yielding codes with much higher relative availability [10]. This natural availability offered could be beneficial for implementation on servers, because the availability scales well with size when other LRCs do not. Moreover, in my dissertation I form criterion to classify the behavior which governs whether or not a code will yield interesting results in the same way as the Hermitian-lifted codes [14]. With some specific facts about a given algebraic curve, one can determine whether or not the asymptotic storage gain could match that of Hermitian-lifted codes. This work on curve-lifted codes continues to be of research interest to myself and to others [7, 8]. Finding appropriate curves will offer developers of distributed storage systems better options for large-scale systems, which could drastically improve maintenance of the data centers we rely on.

In addition to LRCs, I also have work in alternative decoding techniques that use less information than prior decoding methods. Fractional decoding utilizes less information in a different way than LRCs. Where LRCs access less information symbols, fractional decoding compacts information by utilizing properties of the field trace. In collaboration with Gretchen Matthews and Welington Santos, I look at fractional decoding applied to AG codes, which opens exploration of other benefits offered by AG codes [11, 12]. This is done by partitioning the points on the Hermitian code using a set of parallel lines which all intersect the Hermitian curve in the same number of affine points, as can be seen in Figure 2.

Additionally, in my dissertation I construct algorithms for the fractional decoding of Hermitian-lifted codes and norm-trace-lifted codes [14]. Observing that intersections of lines and curves is core to both the curve-lifted code construction and to fractional decoding, I compound the ways in which these codes may be recovered with less information, further building the case for their use in applications.

Future Directions

The first research direction is extending my past research. My general results on curve-lifted codes described in my dissertation is dependent on specific knowledge of intersections between lines and algebraic curves, which is not in general known. Finding sufficiently tight

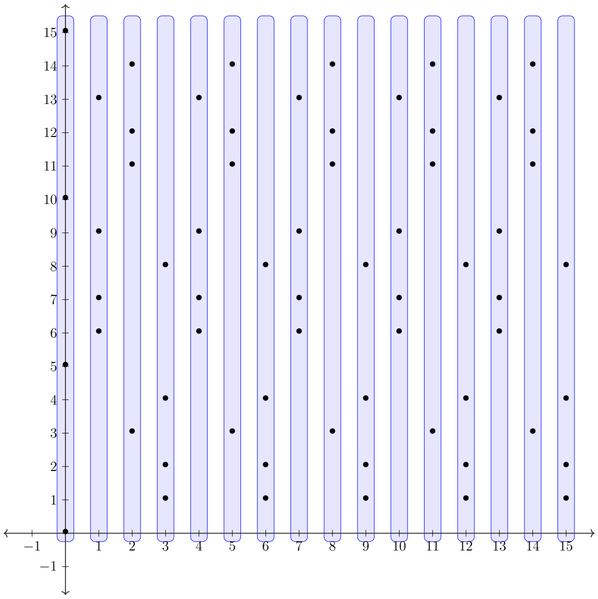

Figure 2: Partition of affine Hermitian points over $\mathbb{F}_{16}$ with vertical lines.

bounds on these intersection numbers will give an idea of what algebraic curves fit within this code construction. As another project, the performance improvements of fractional decoding applied more generally to LRCs has yet to be studied in general. I propose looking further into fractional decoding applied to Hermitian-lifted codes and norm-trace-lifted codes, to begin understanding the benefits of fractional decoding of LRCs. Even more project directions involve altering the geometry of the code construction, either by considering AG codes constructed from higher-dimensional varieties, or by considering repair groups formed by low-degree polynomials other than lines.

Another related area of research is quantum error-correcting codes [17]. Good quantum codes are necessary for scaling physical implementations of quantum computers, due to the instability of quantum information. Connections made in the mid-1990s between classical codes and quantum codes remain a viable option for generating better quantum codes from classical codes [1, 18]. Since norm-trace-lifted codes might have good dual codes as a result of the predictability of their monomial bases, they are a prime candidate for considering with quantum code constructions. This work will benefit from the time I have spent at the Johns Hopkins Applied Physics Laboratory learning about quantum error correction.

Also inspired by the rise of quantum computing is the need for post-quantum cryptography. Current classical cryptosystems are susceptible to Shor's factoring algorithm, which factors integers in polynomial time, and so for the past couple years NIST has orchestrated the search for a new post-quantum standard. By far the oldest of these candidates is the McEliece cryptosystem, which is based on error-correcting codes [13]. This work will be a natural extension of experiences I had during my graduate studies, since I spent much of that time studying the literature on code-based cryptography, and have co-written a chapter of an undergraduate textbook on these cryptosystems [9]. Specifically, the work of continuing the search for classes of codes that offer security in current cryptosystem candidates is important to continue offering options for NIST standardization.

Many of my research directions involve exploring new fields of study, partially in order to see what other unknown connections exist between algebraic geometry and information storage. The connections that AG codes share to all these important applications places their properties in a unique position. Because the goals of coding theory are so broad, the problem of storing information has many distinct approaches, including via algebraic geometry. Through this, the richness of algebraic geometry has unexpected impact on the way that information may be stored on the technologies of the future, and I appreciate my place in the research community as being able to bridge the gap between what might otherwise appear to be very disconnected fields of study.

Last Updated: 2024/02/03

References

[1] A Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098, 1996.

[2] Parikshit Gopalan, Cheng Huang, Bob Jenkins, and Sergey Yekhanin. Explicit maximally recoverable codes with locality. *IEEE Transactions on Information Theory*, 60(9):5245–5256, 2014.

[3] Parikshit Gopalan, Cheng Huang, Huseyin Simitci, and Sergey Yekhanin. On the locality of codeword symbols. *IEEE Transactions on Information theory*, 58(11):6925–6934, 2012.

[4] Valerii Denisovich Goppa. Algebraico-geometric codes. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 46(4):762–781, 1982.

[5] Richard W Hamming. Error detecting and error correcting codes. *The Bell system technical journal*, 29(2):147–160, 1950.

[6] Hiram López, Beth Malmskog, Gretchen Matthews, Fernando Piñero-González, and Mary Wootters. Hermitian-lifted codes. *Designs, Codes, and Cryptography*, 89:497 – 515, 2021.

[7] Beth Malmskog and Na'ama Nevo. Lower rate bounds for Hermitian-lifted codes for odd prime characteristic. *arXiv preprint arXiv:2308.14961*, 2023.

[8] Gretchen L Matthews, Travis Morrison, and Aidan W Murphy. Curve-lifted codes for local recovery using lines. *arXiv preprint arXiv:2307.13183*, 2023.

[9] Gretchen L Matthews and Aidan W Murphy. Cryptography. In *Mathematics in Cyber Research*, pages 53–96. Chapman and Hall/CRC, 2022.

[10] Gretchen L Matthews and Aidan W Murphy. Norm-trace-lifted codes over binary fields. In *2022 IEEE International Symposium on Information Theory (ISIT)*, pages 3079–3084. IEEE, 2022.

[11] Gretchen L Matthews, Aidan W Murphy, and Welington Santos. Fractional decoding of codes from Hermitian curves. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 515–520. IEEE, 2021.

[12] Gretchen L Matthews, Aidan W Murphy, and Welington Santos. Fractional decoding of r-Hermitian codes. *Finite Fields and Their Applications*, 92:102278, 2023.

[13] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.

[14] Aidan W Murphy. *Codes from norm-trace curves: local recovery and fractional decoding.* PhD thesis, Virginia Tech, 2022.

[15] Irving S Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*, 8(2):300–304, 1960.

[16] Claude Elwood Shannon. A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423, 1948.

[17] Peter W Shor. Scheme for reducing decoherence in quantum computer memory. *Physical review A*, 52(4):R2493, 1995.

[18] Andrew M Steane. Simple quantum error-correcting codes. *Physical Review A*, 54(6):4741, 1996.

[19] Itzhak Tamo and Alexander Barg. A family of optimal locally recoverable codes. *IEEE Transactions on Information Theory*, 60(8):4661–4676, 2014.

[20] Daniel Valvo. Daniel Valvo homepage. https://sites.google.com/vt.edu/danielvalvo/home?authuser=0 2023. Accessed: 12/2/23.

[21] Stephen B Wicker and Vijay K Bhargava. *Reed-Solomon codes and their applications.* John Wiley & Sons, 1999.