Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/140110

On Construction and Performance Evaluation of (4096, 815, 3162) Hermitian Code

Richard Adusei[*] *and Mohammed Muniru Iddrisu*

Department of Mathematics, University for Development Studies, Ghana

Received: 3 May 2019, Revised: 2 Jul. 2019, Accepted: 12 Jul. 2019
Published online: 1 Jan. 2020

Abstract: Algebraic Geometry is a branch of mathematics applied in so many disciplines including Coding Theory. This paper focuses on the construction, performance evaluation and practical implementation of encoding and decoding processes of codes constructed from Hermitian Curves. These codes also known as Hermitian codes are types of Algebraic Geometric codes. In this work, performance of the code is done by simulating the (4096, 815, 3162) hermitian code constructed from a hermitian curve using techniques from algebraic geometry with a (255,153,103) Reed-Solomon code from the same $GF(256)$. The decoding process uses Berlekamp-Massay-Sakata (BMS) algorithm, Majority Voting and Forney algorithm. The stages and algorithm were also implemented using the Python programming language.

Keywords: Algebraic Geometric Code, Hermitian Code, Reed-Solomon Code, Galois Field, Performance, Construction

1 Introduction

Whenever data is transmitted across a channel, errors are likely to occur. It is the goal of coding theory to find efficient ways of encoding the data so that these errors can be detected, or even corrected. Algebraic Geometric Codes have close connections to other mathematical structures such as Lattice, modular forms, topology and sphere packing and algebraic curves. In [1] it was discovered that there is a beautiful connection between codes and algebraic curves over finite fields. Codes constructed using these methods are called Goppa Codes or Algebraic Geometric codes. Algebraic Geometric codes constructed from an affine line and curves are used in common applications, such as compact discs (CD), digital versatile discs (DVD), barcodes and in communication systems like wireless, mobile and satellite communications, digital television and radio and asynchronous digital subscriber lines (ADSL). A lot of research is still ongoing from Goppa's work and in the field of coding theory especially finding an efficient decoding algorithms and also constructing codes of higher dimension and codes of longer distance is a hot area of research.

In [2] a linear code based on curves over finite fields with many rational points was constructed. Today they are called Algebraic Geometric codes or Goppa's Geometry codes. In particular, the Gilbert-Varshamov bound was broken by Algebraic Geometric codes constructed in [3] and [4]. In Goppa's construction, one has to choose a divisor and rational points, then evaluate functions at rational points to form a code. In [5] a simplified construction of Algebraic-Geometric codes that does not require much knowledge of algebraic geometry but still produces the same codes as the conventional (ie. Goppa construction) method was presented. In [5], a decoding algorithm was included based on the well-known Peterson Algorithm for decoding Bose-Chaudhuri-Hocquenghem(BCH) and Reed-Solomon codes but it was not feasible to implement with long codes due to its worst-case decoding complexity of $O(n^3)$, where n is the code length. Sakata [6] published a follow-up paper using the same simplified construction but replacing the Peterson-based decoding algorithm with the Sakata algorithm an extension of the Berlekamp-Massay algorithm to two or more dimensions, which reduced the decoding complexity to $O(n^{7/3})$ for algebraic codes construction from the class of hermitian curves. Feng and Rao [7] made an important contribution for increasing the error-correcting capacity of the decoding algorithms by introducing the majority-voting schemes, which determine the value of unknown

[*] Corresponding author e-mail: radusei@uds.edu.gh

syndromes. Johnston and Carasco [8] presented a simulation results for hermitian code whose performance was close to a Reed-Solomon code of the same code rate and finite field for the A White Gaussian Noise Channel (AWGN) and Rayleigh fading channel. Heegard, Little and Saints [9] again extended the hermitian curves defined over finite field up to $GF(2^6)$. with length 64 and 512 symbols and simulated their results over AWGN and Reyleigh fading channels which had a significant improvement as compared with Reed-Solomon codes.

In this apaper we employ Justesen construction technique to construct (4096, 815, 3162) hermitian code. Results of this construction can be found in section 2 and 3. Comparison with Reed Solomon code over a White Gaussian Noise Channel and Reyleigh Fading Channel can be found in section 4 and 5. In section 6 we discuss our results and section 7 concludes the work.

2 Justesen Simplified Construction

Hermitian Curve are defined over finite field F_q as

$$C(x,y) = x^{r+1} + y^r + 1. \tag{1}$$

Hermitian Curves with degree $m = r+1$ where q = number of elements in the field and $r = \sqrt{q}$ are well known from literature. To define the message length (k) and the minimum hamming distance(d^*), all points that cause the curve to vanish$(C(x,y) = 0)$ must be found(ie. Rational points). The number of Rational Points can be computed with $n = r^3$. The genus of the curve (the number of holes in the curve) is calculated as

$$g = \frac{(m-1)(m-2)}{2}, \tag{2}$$

where m is the degree of the polynomial(the curve). To construct an Algebraic Geometric code using Justesen's construction a non-negative integer j is first chosen and is bounded by

$$m-2 \leq j \leq \lfloor \frac{n-1}{m} \rfloor. \tag{3}$$

The dimension of the code (k) can be found as

$$k = n - mj + g + 1 \tag{4}$$

and the designed distance d^* is also given by

$$d^* = mj - 2g + 2. \tag{5}$$

3 Implemenatation

Given equations (1) to (5) the Hermitian code parameters are obtained as

$$H(x,y) = x^{r+1} + y^r - 1$$

$$r = \sqrt{q} = \sqrt{256} = 16$$

$$H(x,y) = x^{17} + y^{16} - 1$$

$$g = 120$$

$$m = 17$$

$$n = 4096$$

$15 \leq J \leq 240$ when $j = 200$ where $j \in J$

$$k = 4096 - 17(200) + 120 - 1 = 815$$

$$d^* = 17(200) - 2(120) + 2 = 3162.$$

This gives $(4096, 815, 3162)$ Hermitian Code with code rate(k/n) of $815/4096 = 0.1989$.

Table 1: Hermitian and Reed-Solomon code over GF(16) and GF(64)

Name of Code	Code Parameters	Code Rate $(R = k/n)$
Hermitian Code	(64,8,28)	0.125
Reed-Solomon Code	(63,42,23)	0.65

Table 2: Hermitian code and Reed-Solomon code over GF(256)

Name of Code	Code Parameters	Code Rate $(R = k/n)$
Hermitian Code	(4096,815,3162)	0.1989
Reed-Solomon Code	(255,153,103)	0.60

Given a message $f(x,y)$, encoding using hermitian code is done by evaluating the message at the various rational points $C_i = f_i(P_i)$. Table 1 above is an example using a $GF(16)$ and $GF(64)$.

Example using $GF(2^2)$ for the Hermitian curve $H(x,y) = x^{r+1} + y^r + 1$
We have

–q = 4,
–m = r+1 =3,
–r = $\sqrt{q} = \sqrt{4} = 2$,
–n = 8,
–k = 5,
–d^* = 3,

Since $q = 4$ we have 4 elements $(0,1,\alpha,\alpha^2)$. There will be 5 monomials because $k = 5$ $(1,x,y,x^2,xy)$. Number of rational points on the curve will be 8 since $n = 8$ where $P_1(0,0)$, $P_2(0,1)$, $P_3(1,\alpha)$, $P_4(1,\alpha^2)$, $P_5(\alpha,\alpha)$,$P_6(\alpha,\alpha^2)$, $P_7(\alpha^2,\alpha)$, $P_8(\alpha^2,\alpha)$. Given a string of message to be encoded, we then convert it to message polynomial $f(x,y) = 1 + y + x^2$. Then we encode each symbol as $C_i = f(P_i)$.

$$C_1 = f(P_1) = f(0,0) = 1 + 1 + 1 = 1$$

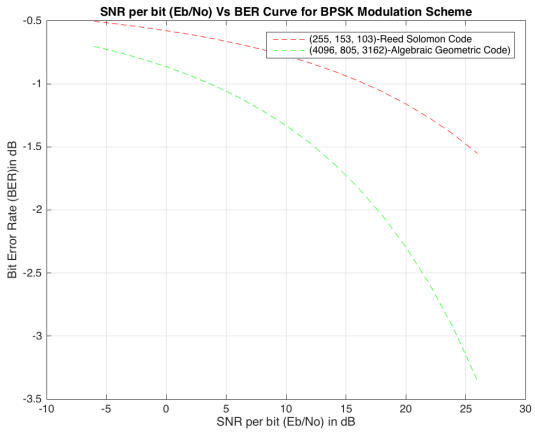

Fig. 1: AWGN simulation over $GF(256)$.

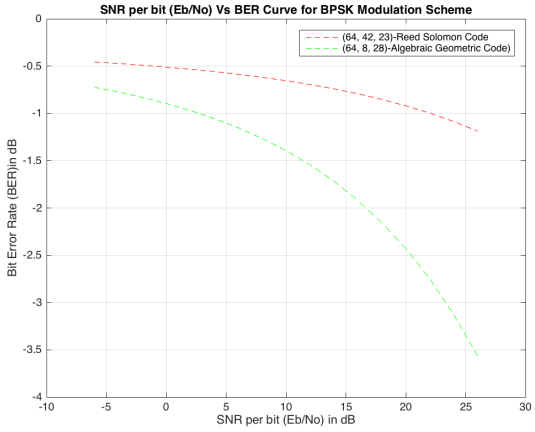

Fig. 2: AWGN simulation over $GF(64)$ and $GF(16)$.

$$C_2 = f(P_2) = f(0,1) = 1+1+0 = 0$$
$$C_3 = f(P_3) = f(1,\alpha) = 1+1+\alpha^2 = \alpha^2$$
$$C_4 = f(P_4) = f(1,\alpha^2) = 1+1+\alpha^4 = \alpha$$
$$C_5 = f(P_5) = f(\alpha,\alpha) = 1+\alpha+1 = 0$$
$$C_6 = f(P_6) = f(\alpha,\alpha^2) = 1+\alpha^2+1 = 1$$
$$C_7 = f(P_7) = f(\alpha^2,\alpha) = 1+\alpha^4+1 = 1$$
$$C_8 = f(P_8) = f(\alpha^2,\alpha^2) = 1+\alpha^2+\alpha^4 = 0$$

So the encoded message is $1,0,\alpha^2,\alpha,0,1,1,0$.

4 Simulation over A White Gaussian Noise (AWGN) channel

A simulation results evaluating the performance of Hermitian code in comparison with Reed-Solomon code over $GF(256)$ are presented. Algebraic Geometric codes have been constructed from Hermitian curves $GF(256)$ in Table 2 with the various parameters and code rates. The performance of these codes are compared with Reed-Solomon codes over the same finite field. Figure 1 shows the simulation of the newly-constructed hermitian code over A White Gaussian Noise Channel (AWGN) using Binary Phase Shift Keying (BPSK) modulation. The results that we got from the AWGN channel shows that the newly-constructed hermitian code has a higher coding gain as compared with Reed-Solomon code. Because the Bit Error Rate (BER) of the constructed code has a closer distance to the Shannon limit that the existing Reed-Solomon code. Other comparisons are also done but over $GF(16)$ and $GF(64)$. It was realised that the coding gain of the Reed-Solomon code has got closer to the hermitian code even with lower finite field ($GF(16)$ and $GF(64)$) but still the newly-constructed code was closer to the Shannon limit done the Reed-Solomon code. Figure 2 shows simulation results of Hermitian code over $GF(64)$ and Reed-Solomon code over $GF(256)$. It can be seen that the coding gain of Reed-Solomon code has got closer to the Hermitian code.

5 Simulation over Reyleigh Fading Channel

The performance of the newly-constructed codes were compared with Reed-Solomon from the same finite field. Figure 3 shows the simulation of the hermitian code over the a Reyleigh Fading Channel using Binary Phase Shift Keying (BPSK) modulation. The results from the Reyleigh fading channel shows that the hermitian code has a higher coding gain as compared with Reed-Solomon codes. Other comparisons are also done but over different finite field ($GF(16)$ and $GF(64)$) especially a lower one for the Reed-Solomon code as was done in the first simulation. We have realised that the coding gain of the Reed-Solomon code has got closer to the hermitian code.(ie. finite field for Reed-Solomon is $GF(64)$ and finite field for Hermitian code is $GF(16)$. Figure 4 and Figure 3 show simulation results of the Hermitian code over $GF(64)$ with Reed-Solomon code over $GF(256)$. It can be seen that the coding gain of Reed-Solomon code has got closer to the Hermitian code.

6 Discussion

Algebraic Geometric Codes constructed from affine points of a projective curve and a set of rational points defined on that curve can be very long which gives them very large hamming distance. Reed-Solomon codes can be described as an Algebraic Geometric Code constructed from affine points of the projective line which makes it similar to Algebraic Geometric Codes and comparable. Consequently Reed-Solomon codes are very short (as indicated that given the same finite field of 256 Algebraic

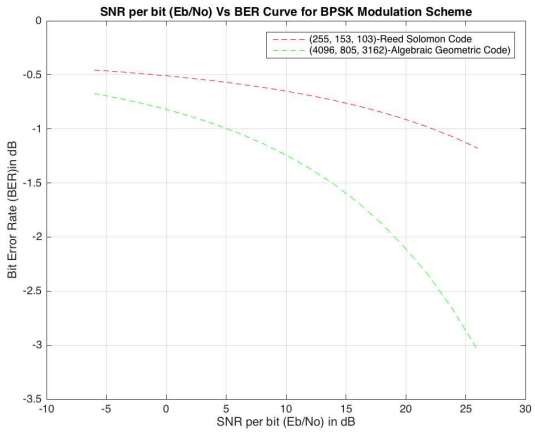

Fig. 3: Reyleigh simulation over $GF(256)$.

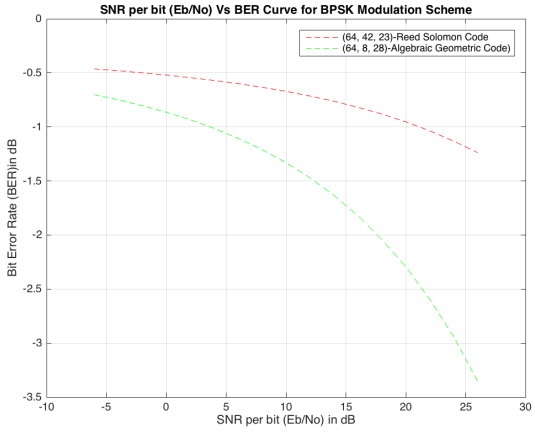

Fig. 4: Reyleigh simulation over $GF(64)$ and $GF(16)$.

Geometric Codes produced 4080 n whiles Reed-Solomon codes produced 255 n) in block length and there are not many Reed- Solomon codes that can be constructed from a particular finite field compared with Algebraic Geometric codes which has more construction given a particular field. However Reed-Solomon codes are Maximum Distance Seperable (MDS) codes unlike Algebraic Geometric Codes, where the genus of the curve reduces the actual minimum hamming distance. Despite the genus penalty, Algebraic Geometric codes still have much larger minimum distance than Reed-Solomon codes defined over the same finite field and consequently Algebraic Geometric codes can correct more errors and also encode a larger block of code at a given time. A disadvantage of Algebraic Geometric codes is their higher decoding complexity. Sakata's algorithm is more complex than Berekamp-Massey algorithm used in decoding Reed-Solomon codes.

The widespread use of Reed-Solomon code in today's systems is rapidly being replaced in communication systems with more powerful coding schemes such as turbo codes, LDPC codes etc. As storage density increases and consequently the effects of ISI become more severe, Reed-Solomon will not be good enough and they will need to be replaced . Algebraic Geometric codes could be a possible alternatives for the error correcting schemes in the future data storage devices and communication systems.

7 Conclusion

(4096,815,3162) Algebraic Geometric code has been constructed from a Hermitian curve of a higher dimension. Finally same simulation results have been presented on the AWGN channel, showing how a hermitian curve defined over $GF(256)$ can outperform a Reed-Solomon code defined over the same finite field. An algebraic structure also has a major role to play in the efficiency of a hermitian code.

Acknowledgement

The authors are grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper.

References

[1] V. Goppa, Algebraic Codes, *Nauk SSSR*, **42**, 75-91, (1862).
[2] V. Goppa, On algebraic Codes,*IEEE Transactions on Information Theory*, **75**, 128-141, (1983).
[3] H. Niederreiter and C. Xing, Towers of Global Function with Asymptotically Many Rational Places and an Improvement on the Gilbert-Varshamov Bound, *Mathematische Nachrichten*, **196**, 171-189,(1998).
[4] M. A. Tsfasman, S.G. Vldutx, and T. Zink, Modular Curves, Shimura Curves, and Goppa Codes, better than Varshamov Gilbert bound , *Mathematische Nachrichten*, **109**, 21-28, (1982).
[5] A. Havemose, *Decoding Algebraic Geometric Codes*. PhD. Thesis, Tekniske Hjsole, Denmarks, (1989).
[6] S. Sakata, Fast decoding of Algebraic Geometric Codes up to the Designed Minimum Distance, *IEEE Trans. Inform. Theory Special Issue on AG Codes*, 1672-1677, (1995).
[7] G.L. Feng and T.R. Rao, Decoding Algebraic-Geometric Codes up to the Designed Minimum Distance, *IEEE Transactions on Information Theory*, **39**, 37 - 45, (1993).
[8] M. Johnston and R. Carasco, Construction and Performance of Algebraic Geometric Codes over AWGN and Fading channels, *IEEE Proc Comm.*, **152**, 713-722, (2005).
[9] C. Heegard, J. Little and K. Saints, Systematic Encoding via Grobner Bases for a class of Algebraic-Geometric Goppa Codes, *IEEE Transactions on Information Theory*, **41**, 1752-1761, (1995).

[10] K.J.L. Justesen and H.E. Jensen, Construction and Decoding of a Class of Algebraic Geometry Codes, *IEEE Transactions on Information Theory*, **35**, 811-821, (1989).

Richard Adusei received his Masters degree in Computational Mathematics at University for Development Studies, Ghana. His research interests are in the areas of applied mathematics, coding theory, computer programming and free software.

Mohammed Muniru Iddrisu is a Senior Lecturer of Mathematics at the University for Development Studies (UDS). He received his BSc, MSc and PhD degrees in Mathematics from the University of Cape Coast, Ghana, Norwegian University of Science and Technology, Trondheim, Norway and University for Development Studies, Ghana respectively. He is an astute academic and has published extensively in reputable journals both locally and internationally. He is also a reviewer and a member of editorial board to many local and international journals. His research interests are in Mathematical Analysis with emphasis on Inequalities, Special functions, Coding Theory, Cryptography, Mathematical Statistics and Applications. He is also a member of the Ghana Mathematics Society, a member of Ghana Science Association, and a member of the Management Board of the National Institute for Mathematical Sciences, Ghana.