Journal of Universal Computer Science, vol. 22, no. 4 (2016), 552-566
submitted: 1/10/15, accepted: 30/3/16, appeared: 1/4/16

Secure Channel Coding Schemes based on Algebraic-Geometric Codes over Hermitian Curves

Omar A. Alzubi
(Al-Balqa Applied University, Salt, Jordan
o.zubi@bau.edu.jo)

Thomas M. Chen
(City University London, London, United Kingdom
tom.chen.1@city.ac.uk)

Jafar A. Alzubi
(Al-Balqa Applied University, Salt, Jordan
j.zubi@bau.edu.jo)

Hasan Rashaideh
(Al-Balqa Applied University, Salt, Jordan
rashaideh@bau.edu.jo)

Nijad Al-Najdawi
(Al-Balqa Applied University, Salt, Jordan
n.al-najdawi@bau.edu.jo)

Abstract: Algebraic-Geometric (AG) codes are new paradigm in coding theory with promising performance improvements and diverse applications in point to point communications services and system security. AG codes offer several advantages over state-of-the art Reed-Solomon (RS) codes. Algebraic-Geometric Codes are proposed and implemented in this paper. The design, construction and implementation are investigated and a software platform has been developed. Simulation results are presented for the first time showing significant performance improvements of AG codes over RS codes using different modulation schemes. The superiority in error correcting and security of AG codes over RS codes has been demonstrated clearly when Rayleigh fading channel is used. Also the results show an obvious improvement when using higher modulation schemes, namely 16QAM and 64QAM.

Key Words: Reliability, Security and Protection, Systems Programs and Utilities
Category: D.4.5, D.4.6, D.4.9

1 Introduction

The main challenges of communication systems are: security, error performance, energy efficiency and implementation costs. Error correcting codes has recently attracted lots of research attention with respect to approaching Shannon bound at lowest computational complexity possible. However, Algebraic-Geometric (AG) codes did not receive enough attention due to the fact that an advanced mathematical background is required in order to implement them. AG codes offer attractive properties such as large code length.

1.1 Problem Definition

Despite its great mathematical properties and powerful error detection/correction performance, AG codes are still in their infancy in secure wireless communication systems. They are yet to be applied in main stream secure wireless networks - such as Wide band Code Division Multiple Access (WCDMA) and Orthogonal Frequency Division Multiple Access (OFDMA) - based air interfaces e.g Long Term Evolution (LTE) and Long Term Evolution Advanced (LTE-A). The only previous attempt to evaluate the Bit Error Rate (BER) performance of AG codes in comparison to traditional RS codes in a simulation environment was presented in [Justesen at el. 1989]. However, [Justesen at el. 1989] did not provide a comprehensive procedure and methodology for evaluating such performance in other secure wireless systems. The results presented in [Justesen at el. 1989] were limited to BPSK modulation over AWGN and Rayleigh fading channel models. It remains an open research problem to find how AG codes behave in different secure wireless systems characterized by variable channel conditions and data rates.

Another issue in AG codes implementations is the parameterization of these codes. Namely how to select the code length, finite field size and coding rate to ensure fair comparison [Goppa 1981]. How these parameters affect the BER performance results is often ignored, however, in fact they greatly alter the conclusions drawn which is proven by the results of this paper.

1.2 Proposed Evaluation Framework

This paper sets itself apart from the few existing works by providing a framework for AG codes performance evaluation. The proposed framework includes parameterization, encoder construction, decoder construction and a detailed Hard decision decoding algorithm. It also provides detailed procedure for end-to-end performance evaluation that can easily be applied to various wireless systems and channel models.

The first issue is addressed by providing a general hard-decision AG decoding algorithm that is capable of allowing change in the modulation index, code rate and channel model. The proposed algorithm presented in this paper, for the first time, as a flow chart to facilitates its implementation in various wireless systems.

The Second issue is addressed in this framework by providing an accurate parameterization procedure to enable better BER performance comparison fairness. This is achieved by keeping the same data block size, relatively the same code rate assuming different finite field for both AG and RS codes. This is in contrast to the [Justesen at el. 1989] work where the finite field is kept the same at the expense of different data block length. In this paper, we argue that this would lead to different results and consequently alters the conclusions made.

2 System Model

This paper considers a comprehensive decoder implementation of AG codes. The investigation considers the BER performance using various modulation schemes and under varying channel conditions. The system model employs different code designs and compares BER performance of AG codes with RS codes. In contrast to existing work a fairer comparison criteria was adopted. The simulations use almost same data block size, relatively same code rate assuming different finite field for both AG and RS codes due to the fact that it is impossible to get RS codes of same size as AG codes at same finite fields. This is different from existing work where the same finite field and almost same code rate are employed while the data block size is different. We believe such assumption is of greater impact on the accuracy of the results and same data block size is the corner stone for making any like-for-like comparisons.

2.1 Parametrization of AG Codes

In [Justesen at el. 1989] a simple method for constructing AG codes was introduced by choosing an irreducible affine smooth curve over a finite field. This method attracts huge research interest and employed by many researchers [Alzubi 2015, Carrasco and Johnston 2008]. Several types of curves can be used - such as Hermitian curves, elliptic curves, hyperelliptic curves, ... etc - for AG codes construction [Ozbudak and Stichtenoth 1999]. In this paper, in order to produce long AG codes Hermitian curves have been used in the following form:

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

Where $r = \sqrt{q}$ and q is the finite field length. To find the message length (k) and the designed minimum Hamming distance (d^*), $n = r^3$ points that satisfy $C(x, y) = 0$ has to be found. Hasse - Weil bound defines the upper bound of the number of point [Justesen at el. 1989] as a function of γ the genus of the curve as,

$$n \leq 2\gamma\sqrt{q} + 1 + q \tag{2}$$

When this bound becomes tighter, Hermitian curves starts to saturate Hasse - Weil bound and called maximal curves. Those codes are then suitable for generating long AG codes. Justesen's construction method suggests a non negative integer j which is bounded by [Alzubi-Omar 2015, Johnston and Carrasco 2005]:

$$m - 2 \leq j \leq \left| \frac{n-1}{m} \right| \tag{3}$$

Calculating the code parameters (n, k, d) for AG codes is different from normal RS codes. The designed minimum Hamming distance of AG codes is characterized by inverse relationship to the genus of the curve. This is in contrast of RS codes where the minimum Hamming distance is independent of the genus [Alzubi 2015, Carrasco and Johnston 2008]. For AG codes, the lower bound of the Hamming distance must be calculated and named the designed minimum Hamming distance d^* as the Hamming distance (d) cannot be calculated always accurately. To find the optimal designed minimum Hamming distance calculations should meet singleton bound as suggested by [Wicker 1995] and is given as a function of the genus by [Pretzel 1998, Johnston and Carrasco 2005, Feng and Rao 1993]:

$$d^* = n - k - \gamma + 1 \tag{4}$$

The AG code parameters can then be written as [Johnston and Carrasco 2005]:

$$k = n - mj + \gamma - 1 \tag{5}$$

$$d^* = mj - 2\gamma + 2 \tag{6}$$

where the codeword length n is equal to the number of affine points on the curve.

2.2 Encoding of AG Codes

In order to design the AG encoder, a generator matrix must be constructed first. This can be done by finding all the points on the curve ($C(x, y) = 0$ excluding the point at infinity). An interesting property of Harmitian curves is that the number of these points equals to $n = r^3$ where r is $\sqrt{q}$ and q is the finite field size [Johnston and Carrasco 2005].

The next step in the encoder design is to define a k two variables monomial basis as following: $F = x^a y^b$ where $0 \leq a < m$ and $b \geq 0$ and ordered using total graduated degree ($<_T$). The total graduated degree used here follows a certain criterion which is:

First-degree pair $(a, b) = (0, 0)$. Next-degree pair (a', b') is [Sakata 1988, Kirwan 1992]:

$$(a', b') = \begin{cases} (a-1, b+1), & \text{if } a > 0 \\ (b+1, 0), & \text{if } a = 0 \end{cases} \tag{7}$$

Therefore, degree pairs ordering is:
$(0,0) <_T (1,0) <_T (0,1) <_T (2,0) <_T (1,1) <_T (0,2) <_T (3,0) <_T (2,1) <_T (1,2) <_T (0,3) <_T (4,0) <_T (3,1) <_T (2,2) ...etc$

This gives monomial basis (ϕ_i):

$$\{1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3, x^4, x^3y, x^2y^2, xy^3, y^4, x^5, ...\} \tag{8}$$

Next step, the monomial basis ϕ_i, $i = 1, 2, ..., k$ in $L(aQ)$ must be computed at affine point on the curve in order to get the final non-systematic generator matrix of the code as below:

$$G = \begin{bmatrix} \phi_1(p_1) & \phi_1(p_2) & \cdots & \phi_1(p_{n-1}) & \phi_1(p_n) \\ \phi_2(p_1) & \phi_2(p_2) & \cdots & \phi_2(p_{n-1}) & \phi_2(p_n) \\ \phi_3(p_1) & \phi_3(p_2) & \cdots & \phi_3(p_{n-1}) & \phi_3(p_n) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \phi_{k-1}(p_1) & \phi_{k-1}(p_2) & \cdots & \phi_{k-1}(p_{n-1}) & \phi_{k-1}(p_n) \\ \phi_k(p_1) & \phi_k(p_2) & \cdots & \phi_k(p_{n-1}) & \phi_k(p_n) \end{bmatrix} \tag{9}$$

The last step in encoder design is to convert the constructed non-systematic generator matrix to a systematic one because the extraction process of the original message out of the decoded codeword is difficult and complex. The designed code produced is - in fact- a non cyclic code, a technique known as Gauss-Jordan elimination must be used. However, the traditional multi-stage shift register technique is only appropriate in case of cyclic codes like RS codes [Alzubi 2014, Carrasco and Johnston 2008, Massey 1969].

Its worth to notice here that in the process of applying Gauss-Jordan elimination, any interchange in columns must followed by same pattern on points [Johnston and Carrasco 2005, Atkinson 1989].

2.3 Decoding of AG Codes

In this section, a complete description of the decoding algorithm is presented in depth. This algorithm is used to decode the AG codes that are made up of Hermitian Curves [Johnston and Carrasco 2005].

STEP 1: Calculation of known syndromes:

(a) The known syndromes $S_{0,0}$ till $S_{0,j}$ can be found using the following equation [Justesen at el. 1992]:

$$S_{a,b} = \sum_{i=1}^{n} r_i x_i^a y_i^b = \sum_{i=1}^{n} (c_i + e_i) x_i^a y_i^b = \sum_{i=1}^{n} e_i x_i^a y_i^b \tag{10}$$

where r_i is a received element within the received codeword r, c_i is a coded symbol, e_i is the corresponding error magnitude in the i-th position, and (x_i, y_i) is the i-th affine point. Where $i \in I$, $I \subseteq \{1, 2, 3, ..., n\}$.

(b) The known syndromes $S_{j+1,0}$ till $S_{m,j-m+1}$ will be calculated by applying the following equation [Carrasco and Johnston 2008]:

$$S_{a,b} = S_{a-m,b+1} + S_{a-m,b+m-1} \tag{11}$$

STEP 2: Allocating error location:
In order to find errors locations the known syndromes $S_{0,0}$ till $S_{m,j-m+1}$ and some of the unknown ones up to $S_{0,j+m}$ must be computed in the following pattern:

(a) Feed the known syndromes found in step 1 to Sakata's algorithm [Sakata 1988].

(b) All the unknown syndromes of the form $S_{a,b}$ for $b \geq m - 1$ can be found using equation (11).

(c) The unknown syndromes obtained from steps 2-a and 2-b are fed again to Sakata's algorithm in order to find any unknown syndromes of the form $S_{a,b}$,for $a \geq m$.

(d) Any unknown syndromes of the form $S_{a,b}, a < m$ can be found using majority voting scheme (MV).

(e) All other unknown syndromes can be obtained using equation (11).

(f) The unknown syndromes obtained from steps 2-d and 2-e are fed again to Sakata's algorithm in order to find more unknown syndromes of the form $S_{a,b}$, for $b \geq m - 1$.

(g) At the end of this step, a set of minimal (error-locating) polynomials is produced which is denoted by F [Sakata 1988]. The roots obtained from substituting the points on the curve in any element of F constitute the errors locations.

STEP 3: Errors magnitudes calculation:
It is necessary to have all elements in the two dimensional syndrome array calculated (from $S_{j+1+m,0}$ to the last unknown syndrome $S_{q-1,q-1}$)in order to compute the error magnitudes in the following manner:

(a) The value of any unknown syndromes of the form $S_{a,b}$,for $a \geq m$ can be obtained using equation (11).

(b) The value of any unknown syndromes of the form $S_{a,b}$, for $a < m$ will be computed using a recursive relationship between the syndromes. This relationship is formed by substituting last minimal polynomial in the set F in the following equation [Carrasco and Johnston 2008, Sakata at el. 1995]:

$$\sum f_{k,l}^{(i)} S_{a-t_1^{(i)}+k,b-t_2^{(i)}+l} = 0 \tag{12}$$

(c) By applying Inverse Discrete Fourier Transform (IDFT) the value of the errors can be calculated [Sakata at el. 1995, Liu 1999]:

– If the error location is at the origin point $P_{x,y} = (0,0)$ then its magnitude calculated by equation (11).

– If the error location is at a point with zero x- coordinate and nonzero y-coordinate $P_{x,y} = (0,y)$ then its magnitude calculated using following equation:

$$E_n = \sum_{i=0}^{q-2} S_{0,q-1-i} \alpha^{ni} \tag{13}$$

where α is the primitive element of the finite field and E_n is the summation of all error values occurred at the points of nonzero y-coordinate α^n. Luckily Hermitian curves - the subject of this paper - have a property that whenever there is a point on the curve of zero x-coordinate and nonzero y-coordinate then there will be no points on the curve of same y-coordinate value with nonzero x-coordinate (α^m, α^n), which means that E_n is in fact the error magnitude of the error took place at the point $P_{(0,y)} = (0, \alpha^n)$.

– If the error location is at a point with nonzero x- coordinate and zero y-coordinate $P_{x,y} = (x,0)$ then its magnitude calculated by following equation:

$$E_m = \sum_{i=0}^{q-2} S_{q-1-i,0} \alpha^{mi} \tag{14}$$

where α is the primitive element of the finite field and E_m is the summation of all error values happening at the points of nonzero x-coordinate α^m. The above mentioned property of Hermitian curves still applying which indicates that there are no points on the curve with same x-coordinate value α^m and nonzero y-coordinate. So, E_m is in fact the error magnitude of the error took place at the point $P_{(x,0)} = (\alpha^m, 0)$.

– if the error location is at a point with nonzero x- coordinate and nonzero y-coordinate $P_{x,y} = (x, y)$ then its magnitude calculated by following equation:

$$e_i = \sum_{a=0}^{q-2} \sum_{b=0}^{q-2} S_{a,b} x_i^{-a} y_i^{-b} \tag{15}$$

where e_i is the error magnitude of the error that happened at the point P_i, and q is the size of the finite field.

STEP 4: Correcting errors:
After locating the errors in *step* 2 and the errors magnitudes in *step* 3, now simply these magnitudes are added into the same locations within the received codeword to form the decoded codeword. Since the code is systematic it is obvious that the original message is the first k symbols.

2.4 Channel Model

In addition to ensuring fairer comparison, we aim to investigate the BER performance of AG codes under various channel conditions. Both AWGN and Rayeliegh fast fading models are employed.

The channel model can be described by the canonical discrete time model as:

$$Y = xh + n \tag{16}$$

where Y is the received signal, x is the transmitted signal(*i.e.* the modulated codeword), n is the complex additive white Gaussian noise again taken from $CN(0, N_0/2)$, and h is the Rayleigh fading channel coefficient. The generation of h follows a complex circularly symmetric Gaussian distribution and written as $CN(0, \sigma^2)$, where σ^2 is the fading variance [Sklar 1998].

The fading coefficient represents fast fading phenomena where the coherence time (τ) is far less than the system maximum codeword length. In particular we set the coherence time to one bit duration.

This fast fading channel model represents the instances of extremely bad channel conditions which we used in order to better characterize the AG code BER performance. In reality, though, a block(slow) fading channel model is usually assumed, in which, the coherence time (τ) is higher than the maximum codeword length. The AWGN channel can be considered as a special case of the fading channel model by setting $h = 1$ in equation (16) [Peter-Sweeney 2004].

3 Numerical results

In order to validate the correctness of the proposed AG code implementation (software platform), simulation results using BPSK modulation scheme were carried out over AWGN and Rayleigh fast fading Channels and compared to those published in literature [Johnston and Carrasco 2005].

In this research, the results confirm the superiority of the AG codes over RS codes and were completely matching with [Johnston and Carrasco 2005]. Those results are shown in (Fig.1) for AWGN channel. Moreover, due to the proposed parameterization procedure, the coding gain of AG codes at finite field $GF(2^4)$ for BER of 10^{-6} of 0.4, 1.05 and 1.4 dBs with code rates of 0.77, 0.69 and 0.61 respectively in comparison to RS code of code rate 0.74 at finite field $GF(2^8)$. These gains were 1.6, 0.9 and 1.6 dBs respectively for the same code rates above using the old parameterization approach in [Johnston and Carrasco 2005].

In addition, in [Johnston and Carrasco 2005] gains were obtained with respect to different reference RS code rates unlike our procedure where we keep the reference constant. Note due to our more accurate parameterization, the coding gains of AG code are lower than those reported in the literature. Those gains are still of significant magnitudes and offer great transmission reliability. QPSK curves - not shown in this paper - shows similar gains to the BPSK with slight improvements.

From the channel capacity perspective, the AG codes result in 0.226, 0.298, 0.364 Bits per Channel Use shift from the Shannon capacity at BER 10^-6 for code rates 0.77, 0.69 and 0.61 respectively, whereas the RS codes is 0.258 Bits per Channel Use Shift from the Shannon capacity at same BER using BPSK.

The simulation results for AG codes using 16QAM modulation scheme over the AWGN channel are presented for the first time in this paper. As shown in (Fig.2), the coding gains of AG codes at finite field $GF(2^4)$ for BER of 10^{-6} are 0.6, 1.25 and 2.05 dBs with code rates of 0.77, 0.69 and 0.61 respectively in comparison to RS code of code rate 0.74 at finite field $GF(2^8)$. Those results clearly emphasize the superiority of AG codes over RS codes even for lower code rates. A code gain of 2.05 dB is a remarkable result that is being acquired for the first time.

From the channel capacity perspective, the AG codes result in 0.9, 1.17, 1.42 Bits per Channel Use shift from the Shannon capacity at BER 10^{-6} for code rates 0.77, 0.69 and 0.61 respectively , whereas the RS codes is 1.03 Bits per Channel Use Shift from the Shannon capacity at same BER.

In addition to this, the 64QAM modulation scheme results are obtained by comparing the BER performance of AG codes having same code rates and finite fields - which used with the 16QAM modulation - with the RS code at rate 0.74. Those results are illustrated in (Fig.3). The obtained code gains are 1.1, 1.9 and 2.8 dBs at BER of 10^{-6} for code rates of 0.77, 0.69 and 0.61 respectively.

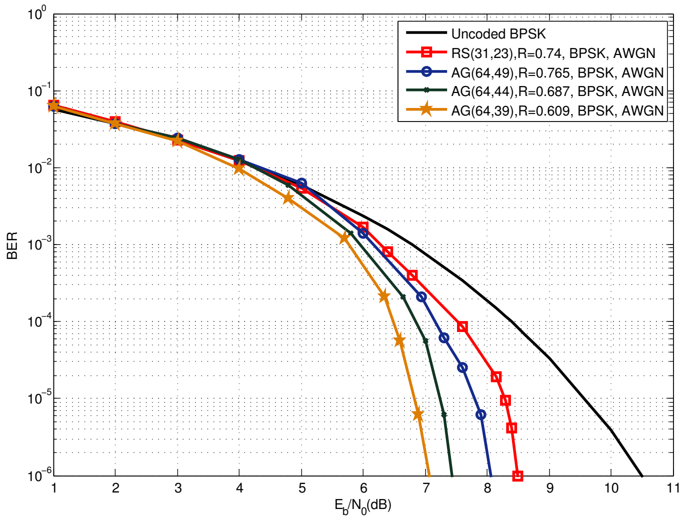

Figure 1: BER of AG codes vs. RS codes using BPSK over AWGN

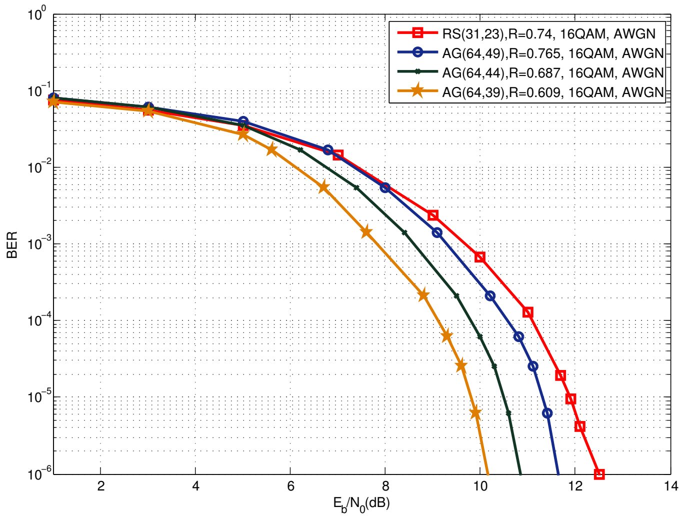

Figure 2: BER of AG codes vs. RS codes using 16QAM over AWGN

To further validate the effectiveness of the developed software platform, simulations over Rayleigh fast fading channel model were performed. This includes results using 16QAM and 64QAM modulation schemes which have not been presented before in literature.

Observing the trend of the BER performance results over different modu-

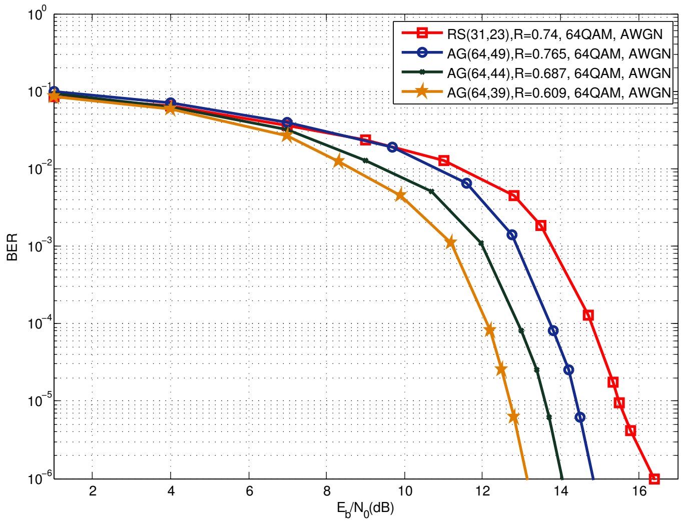

Figure 3: BER of AG codes vs. RS codes using 64QAM over AWGN

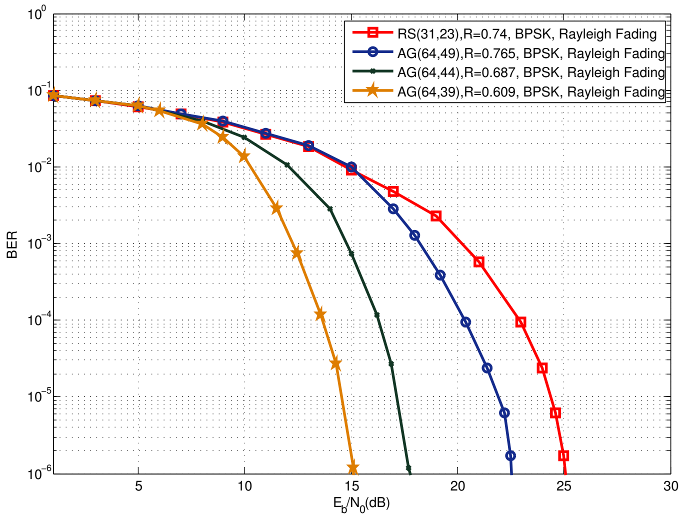

Figure 4: BER of AG codes vs. RS codes using BPSK over Rayleigh fading cahnnel

lation schemes and adverse channel conditions is useful in giving insights into the parameterization of the new AG codes developed in this paper. The results over different modulation schemes using Rayleigh fading channel are presented in (Fig.4), (Fig.5), and (Fig.6).

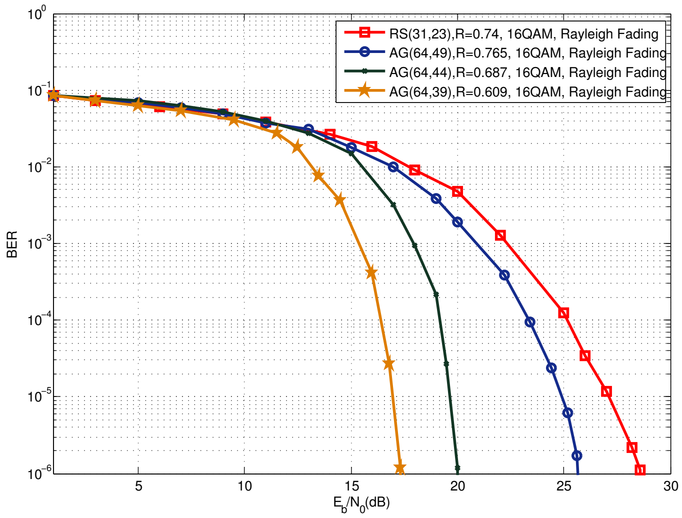

Figure 5: BER of AG codes vs. RS codes using 16QAM over Rayleigh fading cahnnel

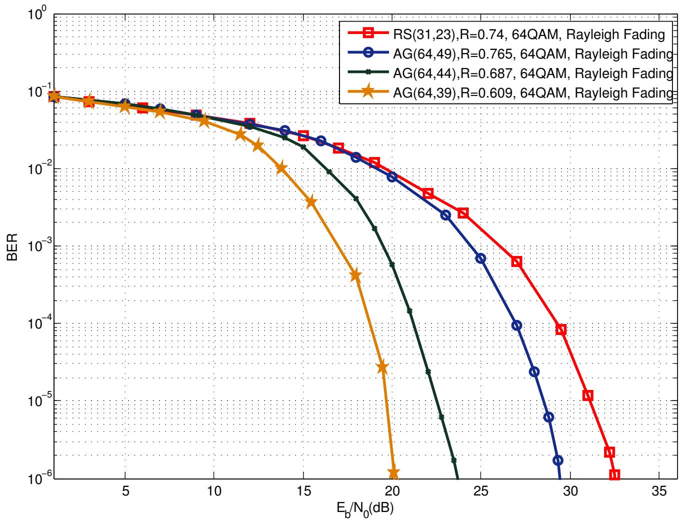

Figure 6: BER of AG codes vs. RS codes using 64QAM over Rayleigh fading cahnnel

Using BPSK modulation scheme as shown in (Fig.4), the coding gains of AG codes at finite field $GF(2^4)$ for BER of 10^{-6} of 2.5, 7.3 and 9.9 dBs with code rates of 0.77, 0.69 and 0.61 respectively, in comparison to RS code of code rate 0.74 at finite field $GF(2^8)$. These gains are significantly higher than those achieved over the AWGN channel. Those results matches the ones in [Johnston and Carrasco 2005] and emphasize the effectiveness of our developed software platform while confirming the benefits of AG codes over adverse channel conditions.

The obtained BPSK fading results motivated us to explore the BER performance using higher modulation schemes such as 16QAM and 64QAM.

Regarding 16QAM modulation scheme results which are shown in (Fig.5). The coding gains of AG codes at finite field $GF(2^4)$ for BER of 10^{-6} are 3.1, 8.7 and 11.4 dBs for the code rates of 0.77, 0.69 and 0.61 respectively in comparison to RS code of code rate 0.74 at finite field $GF(2^8)$. Once again the effectiveness of AG codes is manifested under fading channel conditions.

However, for 64QAM, the coding gains for code rates of 0.77, 0.69 and 0.61 are 3.55, 9.35 and 12.75 respectively, in comparison to RS code of code rate 0.74 at BER of 10^{-6}. Those results are shown in (Fig.6).

We notice that the higher the modulation index, the more coding gain is obtained for the same code rate. This phenomena is shown in both AWGN and Rayleigh fast fading channel models, making the AG codes very attractive at high throughput applications and services currently needed in next generation wireless systems such as 4G, High Speed Packet Access (HSPA) and Long Term Evolution (LTE).

4 Conclusions

In this paper, the software platform to evaluate the BER performance of AG codes is established and compared with the performance of RS codes. Simulation results confirmed the correctness and security of developed software platform by providing the exact published results in the literature for the case of BPSK modulation over both AWGN and Rayleigh fast fading channel conditions.

The results of BER performance of AG codes over Hermitian curves using 16QAM and 64QAM modulation schemes - to the best of this paper authors' knowledge - are obtained over both AWGN and Rayleigh fast fading channels for the first time.

The obtained simulation results provide a sufficient evidence of the superiority (in terms of both error correcting and security) of the AG codes over RS codes even for higher order modulations such as 16QAM and 64QAM over AWGN channel. Interestingly, the behaviour of coding gains achieved is directly proportional to the modulation index.

In the case of Rayleigh fast fading channel using 16QAM and 64QAM modulation schemes, the obtained results once again confirm that a great gain is achieved using AG codes. These results highlight the robustness and security of AG codes to sever fading conditions as the coding gains obtained are higher than those achieved for the AWGN channel. Also the trend of increased coding gains with the modulation index increase applies.

References

[Alzubi 2014] Alzubi, J., Alzubi, O., Thomas, C.: "Forward Error Correction Based On Algebraic-Geometric Theory"; *SpringerBriefs in Electrical and Computer Engineering*,(2014).http:http://springer.com/gp/book/9783319082929

[Alzubi 2015] Alzubi, O.: "An Empirical Study of Irregular AG Block Turbo Codes over Fading Channels"; *Research Journal of Applied Sciences, Engineering and Technology*, 11, 12, (Dec. 2015).

[Alzubi-Omar 2015] Alzubi, O.: "Performance Evaluation of AG Block Turbo Codes over Fading Channels Using BPSK"; *Proceedings of the The International Conference on Engineering & MIS 2015*, Istanbul, Turkey,(Dec. 2015), 36:1-6. http://doi.acm.org/10.1145/2832987.2833044

[Atkinson 1989] Atkinson, K.,: "An Introduction to Numerical Analysis"; 2nd ed., John Wiley & Sons, Inc., (1989).

[Carrasco and Johnston 2008] Carrasco, R. and Johnston, M.: "Non-Binary Error Control Coding for Wireless Communication and Data Storage"; John Wiley & Sons, Ltd, 2008.

[Feng and Rao 1993] Feng, G. and Rao, T.: "Decoding algebraic-geometric codes up to the designed minimum distance"; *Information Theory, IEEE Transactions on*, 39, 1, (Jan 1993), 37-45.

[Goppa 1981] Goppa, V.: "Codes on algebraic curves"; *Soviet Math. Dokl.*, 24, (1981) , 75-91.

[Johnston and Carrasco 2005] Johnston, M. and Carrasco, R.: "Construction and performance of algebraic-geometric codes over awgn and fading channels"; *Communications, IEE Proceedings-*, 152, 5, (Oct. 2005),713-722.

[Justesen at el. 1989] Justesen, J., Larsen, K., Jensen, H., Havemose, A., and Hoholdt, T.: "Construction and decoding of a class of algebraic geometry codes"; Information Theory, IEEE Transactions on, 35, 4,(Jul 1989), 811-821.

[Justesen at el. 1992] Justesen, J., Larsen, K., Jensen, H., and Hoholdt, T.: "Fast decoding of codes from algebraic plane curves"; *Information Theory, IEEE Transactions on*, 38, 1, (Jan. 1989), 111-119.

[Kirwan 1992] Kirwan, F.: "Complex Algebraic Curves"; number 23 in london mathematical society student texts ed., Cambridge University Press, (1992).

[Liu 1999] Liu, C.: "Determination of error values for decoding hermitian codes with the inverse affine fourier transform"; *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 82, 10, (1999), 2302-2305. http://ci.nii.ac.jp/naid/110003208168/en/

[Massey 1969] Massey, J.,: "Shift-register synthesis and bch decoding"; *Information Theory, IEEE Transactions on*, 15, 1, (Jan 1969), 122-127.

[Ozbudak and Stichtenoth 1999] Ozbudak, F. and Stichtenoth, H.: "Constructing codes from algebraic curves"; *Information Theory, IEEE Transactions on*, 45, 7, (Nov 1999), 2502-2505.

[Peter-Sweeney 2004] Peter-Sweeney, P.: "Error control coding: from theory to practice"; John Wiley & Sons, Ltd., (Mar. 2004).

[Pretzel 1998] Pretzel, O.: "Codes and algebraic curves"; New York, NY, USA: Oxford University Press, Inc., (1998).

[Sakata 1988] Sakata, S.: "Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array"; *Journal of Symbolic Computation*, 5, 3, (1988), 321-337. http://www.sciencedirect.com/science/article/pii/S0747717188800336

[Sakata at el. 1995] Sakata, S., Justesen, J., Madelung, Y., Jensen, H., and Hoholdt, T.: "Fast decoding of algebraic-geometric codes up to the designed minimum distance"; *Information Theory, IEEE Transactions on*, 41, 6, (Nov. 1995), 1672-1677.

[Sklar 1998] Sklar, B.: "Digital communications: fundamentals and applications"; River, NJ, USA: Prentice-Hall, Inc., (1988).

[Wicker 1995] Wicker, S.: "Error control systems for digital communication and storage"; NJ, USA, Prentice-Hall, Inc., (1995).