

2010

Good codes from generalised algebraic geometry codes

Jibril, M

<http://hdl.handle.net/10026.1/1476>

10.1109/ISIT.2010.5513687

Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on IEEE

All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.

Good Codes From Generalised Algebraic Geometry Codes

Mubarak Jibril*, Martin Tomlinson*, Mohammed Zaki Ahmed* and Cen Tjhai*

*School of Computing and Mathematics

Faculty of Technology

University of Plymouth

United Kingdom

Email: mubarak.jibril@plymouth.ac.uk

Abstract—Algebraic geometry codes or Goppa codes are defined with places of degree one. In constructing generalised algebraic geometry codes places of higher degree are used. In this paper we present 41 new codes over \mathbb{F}_{16} which improve on the best known codes of the same length and rate. The construction method uses places of small degree with a technique originally published over 10 years ago for the construction of generalised algebraic geometry codes.

I. INTRODUCTION

In coding theory, it is desirable to obtain an error correcting code with the maximum possible minimum distance d , given a code length n and code dimension k . Algebraic geometry (AG) codes have good properties and some families of these codes have been shown to be asymptotically superior as they exceed the well-known Gilbert Vashamov bound [1] when the defining finite field \mathbb{F}_q has size $q \geq 49$ with q always a square. A closer look at tables of best known codes in [2] and [3] shows that algebraic geometry codes feature as the best known linear codes for an appreciable range of code lengths for different field sizes q . Algebraic geometry codes are codes derived from curves and were first discovered by Goppa [4] in 1981. Goppa's description uses rational places of the curve to define these codes. Rational places are called places of degree one. A generalised construction of algebraic geometry codes was presented by Xing *et al* in [5] [6] and Ozbudak *et al* in [7]. An extension of the method which utilises places of higher degrees as well as a concatenation concept was introduced in [8]. This method was shown in [9] [10] [11] to be effective in constructing codes that are better than the best known codes and many codes were presented for finite fields up to \mathbb{F}_9 . In this paper we present several new codes over finite field \mathbb{F}_{16} . These codes represent improvements on minimum distance compared to some previously best known codes. We first give a description of the codes and an exposition of the construction in the Section II. Finally we present our results in Section III.

II. CONSTRUCTION

A two dimensional affine space $\mathbb{A}^2(\mathbb{F}_q)$ is given by the set of points $\{(\alpha, \beta) : \alpha, \beta \in \mathbb{F}_q\}$ while its projective closure $\mathbb{P}^2(\mathbb{F}_q)$ is given by the set of equivalence points $\{(\alpha : \beta :$

$1)\} \cup \{(\alpha : 1 : 0)\} \cup \{(1 : 0 : 0)\} : \alpha, \beta \in \mathbb{F}_q\}$. Given a homogeneous polynomial $F(x, y, z)$, a curve \mathcal{X} defined in $\mathbb{P}^2(\mathbb{F}_q)$ is a set of distinct points $\{P \in \mathbb{P}^2(\mathbb{F}_q) : F(P) = 0\}$. We are only interested in the case where \mathcal{X} is irreducible and is non-singular in order to obtain AG codes. Let \mathbb{F}_{q^ℓ} be an extension of the field \mathbb{F}_q , the Frobenius automorphism is given as

$$\begin{aligned} \phi_{q,\ell} : \mathbb{F}_{q^\ell} &\rightarrow \mathbb{F}_{q^\ell} \\ \phi_{q,\ell}(\beta) &= \beta^q \quad \beta \in \mathbb{F}_{q^\ell} \end{aligned}$$

and its action on a projective point $(x : y : z)$ in \mathbb{F}_{q^ℓ} is

$$\phi_{q,\ell}((x : y : z)) = (x^q : y^q : z^q).$$

A place of degree ℓ [12] is a set of ℓ points of a curve defined in the extension field \mathbb{F}_{q^ℓ} denoted by $\{P_0, P_1, \dots, P_{\ell-1}\}$ where each $P_i = \phi_{q,\ell}^i(P_0)$. Places of degree one are called rational places. An example of a place of degree two is a pair of points $\{P_0, P_1\}$ such that $P_0 = (x, y)$ has coordinates in \mathbb{F}_{q^2} and $P_1 = \phi_{q,2}(P_0) = (x^q, y^q)$.

We will now describe two maps that are useful in the Xing *et al* construction of generalised AG codes. We observe that \mathbb{F}_q is a subfield of \mathbb{F}_{q^ℓ} for all $\ell \geq 2$. It is then possible to map \mathbb{F}_{q^ℓ} to an ℓ -dimensional vector space with elements from \mathbb{F}_q using a suitable basis. We define the mapping,

$$\begin{aligned} \pi_\ell : \mathbb{F}_{q^\ell} &\rightarrow \mathbb{F}_q^\ell \\ \pi_\ell(\beta_j) &= [c_1^j \ c_2^j \ \dots \ c_\ell^j] \quad \beta_j \in \mathbb{F}_{q^\ell}, \ c_i^j \in \mathbb{F}_q. \end{aligned}$$

Suppose $[\gamma_1 \gamma_2 \dots \gamma_\ell]$ forms a suitable basis of the vector space \mathbb{F}_q^ℓ , then $\beta_j = c_1^j \gamma_1 + c_2^j \gamma_2 + \dots + c_\ell^j \gamma_\ell$. Finally we use $\sigma_{\ell,n}$ to represent an encoding map from an ℓ -dimensional message space in \mathbb{F}_q to an n -dimensional code space,

$$\sigma_{\ell,n} : \mathbb{F}_q^\ell \rightarrow \mathbb{F}_q^n$$

with $\ell \leq n$.

We now give a description of generalised AG codes as presented in [8] [10] [11]. Let $F = F(x, y, z)$ be a homogeneous polynomial defined in \mathbb{F}_q . Let g be the genus of the curve \mathcal{X}/\mathbb{F}_q corresponding to the polynomial F . Also let P_1, P_2, \dots, P_r be r distinct places of \mathcal{X}/\mathbb{F}_q and $k_i = \deg(P_i)$

(deg is degree of). W is a divisor of the curve \mathcal{X}/\mathbb{F}_q such that $W = P_1 + P_2 + \dots + P_r$ and G a divisor so that $\text{supp}(W) \cap \text{supp}(G) = \emptyset$. More specifically $G = m(Q - R)$ where $\text{deg}(Q) = \text{deg}(R) + 1$. Associated with the divisor G is a Riemann-Roch space $\mathcal{L}(G)$ with $m = \text{deg}(G)$ an integer, $m \geq 0$. From the Riemann-Roch theorem we know that the dimension of $\mathcal{L}(G)$ is given by $l(G)$ and

$$l(G) \geq m - g + 1$$

with equality when $m \geq 2g - 1$. Also associated with each P_i is a q -ary code C_i with parameters $[n_i, k_i = \text{deg}(P_i), d_i]_q$ with the restriction that $d_i \leq k_i$. We denote $\{f_1, f_2, \dots, f_k : f_i \in \mathcal{L}(G)\}$ as a set of k linearly independent elements of $\mathcal{L}(G)$ that form a basis. We can create a generator matrix for a generalised AG code as such,

$$M = \begin{bmatrix} \sigma_{k_1, n_1}(\pi_{k_1}(f_1(P_1))) & \dots & \sigma_{k_r, n_r}(\pi_{k_r}(f_1(P_r))) \\ \sigma_{k_1, n_1}(\pi_{k_1}(f_2(P_1))) & \dots & \sigma_{k_r, n_r}(\pi_{k_r}(f_2(P_r))) \\ \vdots & & \vdots \\ \sigma_{k_1, n_1}(\pi_{k_1}(f_k(P_1))) & \dots & \sigma_{k_r, n_r}(\pi_{k_r}(f_k(P_r))) \end{bmatrix}$$

where $f_i(P_i)$ is an evaluation of a polynomial and basis element f_i at a point P_i , π_{k_i} is a mapping from $\mathbb{F}_q^{k_i}$ to \mathbb{F}_q and σ_{k_i, n_i} is the encoding of a message vector in $\mathbb{F}_q^{k_i}$ to a code vector in $\mathbb{F}_q^{n_i}$. It is desirable to choose the maximum possible minimum distance for all codes C_i so that $d_i = k_i$. The same code is used in the map σ_{k_i, n_i} for all points of the same degree k_i i.e. the code C_j has parameters $[n_j, j, d_j]_q$ for a place of degree j . Let A_j be an integer denoting the number of places of degree j and B_j be an integer such that $0 \leq B_j \leq A_j$. If t is the maximum degree of any place P_i we choose to use in the construction, then the generalised AG code is represented as a $C(k; t; B_1, B_2, \dots, B_t; d_1, d_2, \dots, d_t)$. Let $[n, k, d]_q$ represent a linear code in \mathbb{F}_q with length n , dimension k and minimum distance d , then a generalised AG code is given by the parameters [8],

$$k = l(G) \geq m - g + 1$$

$$n = \sum_{i=1}^r n_i = \sum_{j=1}^t B_j n_j$$

$$d \geq \sum_{i=1}^r d_i - g - k + 1 = \sum_{j=1}^t B_j d_j - g - k + 1.$$

III. RESULTS

We use two polynomials and their associated curves to obtain codes in \mathbb{F}_{16} better than the best known codes in [3]. The two polynomials are given in Table I while Table II gives a summary of the properties of their associated curves (with $t = 4$). The number of places of degree j , A_j , is determined by computer algebra system MAGMA [13]. The best known linear codes from [3] over \mathbb{F}_{16} with $j = d_j$ for $1 \leq j \leq 4$ are

$$[1, 1, 1]_{16} \quad [3, 2, 2]_{16} \quad [5, 3, 3]_{16} \quad [7, 4, 4]_{16}$$

which correspond to C_1 , C_2 , C_3 and C_4 respectively. Since $t = 4$ for all the codes in this paper and

$$[d_1, d_2, d_3, d_4] = [1, 2, 3, 4]$$

TABLE I
POLYNOMIALS IN \mathbb{F}_{16}

$F_1 = x^5 z^{10} + x^3 z^{12} + x z^{14} + y^{15}$
$F_2 = x^5 + y^4 z + y z^4$

TABLE II
PROPERTIES OF $\mathcal{X}_i/\mathbb{F}_{16}$

$F(x, y, z)$	Genus	A_1	A_2	A_3	A_4	Reference
\mathcal{X}_1	12	83	60	1320	16140	[15]
\mathcal{X}_2	6	65	0	1600	15600	

TABLE III
BEST CONSTRUCTIBLE CODES FROM \mathcal{X}_1

Codes	k Range	Description	#
$[83, k, d \geq 72 - k]_{16}$	$8 \leq k \leq 52$	$C(k; [83, 0, 0, 0])$	45
$[89, k, d \geq 76 - k]_{16}$	$9 \leq k \leq 54$	$C(k; [83, 2, 0, 0])$	46
$[94, k, d \geq 79 - k]_{16}$	$10 \leq k \leq 57$	$C(k; [83, 2, 1, 0])$	48
$[92, k, d \geq 78 - k]_{16}$	$9 \leq k \leq 57$	$C(k; [83, 3, 0, 0])$	49
$[98, k, d \geq 82 - k]_{16}$	$11 \leq k \leq 59$	$C(k; [83, 5, 0, 0])$	49

TABLE IV
BEST CONSTRUCTIBLE CODES FROM \mathcal{X}_2

Codes	k Range	Description	#
$[72, k, d \geq 64 - k]_{16}$	$11 \leq k \leq 50$	$C(k; [65, 0, 0, 1])$	40
$[79, k, d \geq 68 - k]_{16}$	$11 \leq k \leq 48$	$C(k; [65, 0, 0, 2])$	38
$[77, k, d \geq 67 - k]_{16}$	$10 \leq k \leq 51$	$C(k; [65, 0, 1, 1])$	42
$[75, k, d \geq 66 - k]_{16}$	$9 \leq k \leq 51$	$C(k; [65, 0, 2, 0])$	43

TABLE V
NEW CODES FROM \mathcal{X}_1

Codes	k Range	Description	#
$[70, k, d \geq 63 - k]_{16}$	$10 \leq k \leq 50$	$C(k; [65, 0, 1, 0])$	41

we shorten the representation

$$C(k; t; B_1, B_2, \dots, B_t; d_1, d_2, \dots, d_t) \equiv C(k; B_1, B_2, \dots, B_t).$$

Tables III-IV give codes obtained from the two curves associated with the two polynomials F_i for $1 \leq i \leq 2$ that improve on the best constructible codes in the tables in [3]. Table V gives new codes that improve on both constructible and non-constructible codes in [3]. It is also worth noting that codes of the form $C(k; N, 0, 0, 0)$ are simply Goppa codes (defined with only rational points). The symbol # in the Tables III-IV denotes the number of new codes from each generalised AG code $C(k; B_1, B_2, \dots, B_t)$. The tables in [14] contain curves known to have the most number of rational points for a given genus. Over \mathbb{F}_{16} the curve with the highest number of points with genus $g = 12$ from [14] has 88 rational points, was constructed using class field theory and is not defined by an explicit polynomial. On the other hand the curve $\mathcal{X}_1/\mathbb{F}_{16}$ obtained by Kummer covering of the projective line in [15] has $A_1 = 83$ rational points and genus $g = 12$ and is explicitly presented. Codes from this curve represent the best constructive codes in \mathbb{F}_{16} with code length 83. The curve $\mathcal{X}_2/\mathbb{F}_{16}$ is defined by the well-known Hermitian polynomial.

Table VI gives the new codes obtained from \mathcal{X}_2 . The codes have length N , dimension K and minimum distance D . D_m

TABLE VI
NEW CODES IN \mathbb{F}_{16}

N	K	D	D_m
70	10	53	52
70	11	52	51
70	12	51	50
70	13	50	49
70	14	49	48
70	15	48	47
70	16	47	46
70	17	46	45
70	18	45	44
70	19	44	43
70	20	43	42
70	21	42	41
70	22	41	40
70	23	40	39
70	24	39	38
70	25	38	37
70	26	37	36
70	27	36	35
70	28	35	34
70	29	34	33
70	30	33	32
70	31	32	31
70	32	31	30
70	33	30	29
70	34	29	28
70	35	28	27
70	36	27	26
70	37	26	25
70	38	25	24
70	39	24	23
70	40	23	22
70	41	22	21
70	42	21	20
70	43	20	19
70	44	19	18
70	45	18	17
70	46	17	16
70	47	16	15
70	48	15	14
70	49	14	13
70	50	13	12

is the lower bound on the minimum distance of codes from [3] with the same length and dimension as the constructed generalised AG codes.

IV. CONCLUSION

We have presented 41 new codes and 400 improvements on constructible codes in \mathbb{F}_{16} over the codes in [3]. The construction method yields many good codes as shown here, as long as curves with many places of small degree are used, however traditional search for good codes has focused primarily on finding rational curves with many points. In order to obtain more codes from generalised AG codes, curves with small genera and many places of small degree need to be found.

REFERENCES

- [1] M. Tsfasman, S. Vladut, and T. Zink, "On goppa codes which are better than the varshamov-gilbert bound," *Math. Nacr.*, vol. 109, pp. 21–28, 1982.
- [2] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at <http://www.codetables.de>, 2007, accessed on 2009-12-21.
- [3] W. Schimd and R. Shurer, "Mint: A database for optimal net parameters," Online available at <http://mint.sbg.ac.at>, 2004, accessed on 2009-12-21.
- [4] V. Goppa, *Geometry and Codes*. Dordrecht: Kluwer Academic Publishers, 1988.
- [5] C. Xing, H. Niederreiter, and K. Y. Lam, "Constructions of algebraic-geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 4, pp. 1186 – 1193, 1999.
- [6] H. Niederreiter, C. Xing, and K. Y. Lam, "A new construction of algebraic-geometry codes," *Appl. Algebra Engrg. Comm. Comput.*, vol. 9, no. 5, 1999.
- [7] F. Ozbudak and H. Stichtenoth, "Constructing codes from algebraic curves," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, 2502-2505.
- [8] C. Xing, H. Niederreiter, and K. Lam, "A generalization of algebraic-geometry codes," *Information Theory, IEEE Transactions on*, vol. 45, no. 7, pp. 2498–2501, 1999.
- [9] K. H. Leung, S. Ling, and C. Xing, "New binary linear codes from algebraic curves," *Information Theory, IEEE Transactions on*, vol. 48, no. 1, pp. 285 –287, jan 2002.
- [10] C. Ding, H. Niederreiter, and C. Xing, "Some new codes from algebraic curves," *Information Theory, IEEE Transactions on*, vol. 46, no. 7, pp. 2638–2642, Nov 2000.
- [11] C. Xing and S. L. Yeo, "New linear codes and algebraic function fields over finite fields," *Information Theory, IEEE Transactions on*, vol. 53, no. 12, pp. 4822–4825, 2007.
- [12] J. L. Walker, *Codes and Curves*. Rhode Island: American Mathematical Society, 2000.
- [13] W. Bosma, C. J., and P. C., "The magma algebra system i: The user language," *J. Symbolic Comput.*, vol. 24, pp. 235–265, 1997.
- [14] G. van der Geer *et al.*, "Manypoints: A table of curves with many points," Online available at <http://www.manypoints.org>.
- [15] V. Shabat, "Curves with many points," Ph.D. dissertation, Univ. of Amsterdam, Amsterdam, 2001. [Online]. Available: <http://www.science.uva.nl/math/Research/Dissertations/Shabat2001.text.pdf>