# VIEWING MULTIPOINT CODES AS SUBCODES OF ONE-POINT CODES

GRETCHEN L. MATTHEWS
DEPARTMENT OF MATHEMATICAL SCIENCES
CLEMSON UNIVERSITY
CLEMSON, SC 29634-0975
U.S.A.
E-MAIL: GMATTHE@CLEMSON.EDU

ABSTRACT. We consider ways in which multipoint algebraic geometry codes may be viewed as subcodes of the more traditionally studied one-point codes. Examples are provided to illustrate the impact of choices made on this embedding.

## 1. INTRODUCTION

An $m$-point algebraic geometry (AG) code is constructed by evaluating functions which are allowed to have poles at $m$ specified points on a curve $X$ over a finite field. While Goppa's construction [6] certainly encompasses multipoint codes, most subsequent work has focused on the one-point case. While multipoint codes can have better parameters than comparable one-point codes on the same curve [13], one-point codes are certainly better understood. Recently, there has been more work on multipoint codes [1, 2, 8, 9, 10, 11]. Here, we see that multipoint codes may be viewed as subcodes of the more traditionally studied one-point codes and illustrate the impact of choices made on this embedding.

**Notation.** Let $X$ be a smooth, projective, absolutely irreducible curve of genus $g$ over a finite field $\mathbb{F}$. The divisor of a rational function $f$ on $X$ will be denoted by $(f)$. Given a divisor $A$ on $X$ defined over $\mathbb{F}$, let $\mathcal{L}(A)$ be the set of rational functions $f$ on $X$ defined over $\mathbb{F}$ with divisor $(f) \geq -A$ together with the zero function. The dimension of $\mathcal{L}(A)$ as an $\mathbb{F}$-vector space is denoted by $\ell(A)$. Clearly, if $A \leq B$ for divisors $A$ and $B$ on $X$, then $\mathcal{L}(A) \subseteq \mathcal{L}(B)$.

Given distinct $\mathbb{F}$-rational points $P_1, \ldots, P_n, Q_1, \ldots, Q_m$ on $X$, set $D := P_1 + \cdots + P_n$ and $G := a_1Q_1 + \cdots + a_mQ_m$ where $a_i \geq 0$. Then

$$C_{\mathcal{L}}(D, G) = \{(f(Q_1), f(Q_2), \ldots, f(Q_n)) : f \in \mathcal{L}(G)\}$$

This project was supported by NSF DMS-0201286 and NSA H-98230-06-1-0008.

is sometimes called an $m$-point code. We do not require the divisor $D$ to be supported by all $\mathbb{F}$-rational points that are not in the support of $G$. Excellent references for algebraic geometry codes include [7, 14, 15].

## 2. Embedding a multipoint code in a one-point code

Consider the multipoint code $C_{\mathcal{L}}(D,G)$ from above. Since the field $\mathbb{F}$ is finite, the group of divisor classes of degree zero has finite order. Hence, there exists a rational function $f$ with divisor

$$(f) = b_2 Q_2 + \cdots + b_m Q_m - b_1 Q_1$$

where $b_i \geq a_i$ for all $2 \leq i \leq m$ and $b_1 = \sum_{i=2}^m b_i$. Multiplication by $f$ induces an isomorphism of Riemann-Roch spaces

$$\begin{array}{ccc} \mathcal{L}\left(\sum_{i=1}^m a_i Q_i\right) & \to & \mathcal{L}\left(\left(a_1+b_1\right)Q_1 - \left(\sum_{i=2}^m \left(b_i - a_i\right)Q_i\right)\right) \\ h & \mapsto & fh \end{array}$$

which gives rise to an isometry of codes

$$C_{\mathcal{L}}\left(D, \sum_{i=1}^m a_i Q_i\right) \cong C_{\mathcal{L}}\left(D, \left(a_1+b_1\right)Q_1 - \left(\sum_{i=2}^m \left(b_i - a_i\right)Q_i\right)\right).$$

As a consequence, the $m$-point code $C_{\mathcal{L}}\left(D,G\right)$ is isometric to a subcode of the one-point code $C_{\mathcal{L}}\left(D,\left(a_1+b_1\right)P_1\right)$.

## 3. Examples

While the existence of the function $f$ above is guaranteed by the fact that the class number of $X$ is finite, this may not be that helpful in finding the most appropriate function. To illustrate the effects of the choice of $f$, we consider the following two examples.

**Example 3.1.** Consider the Hermitian curve $X$ defined by $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$. Set $G := 2(q+1)P_\infty + \sum_{\beta^q+\beta=0} P_{0\beta}$, and let $D$ be the sum of all other $\mathbb{F}_{q^2}$-rational points on $X$. Since the class number of $X$ is $(q+1)(q^2-q)$, there exists a function $f$ such that

$$(f) = (q+1)(q^2-q) \sum_{\beta^q+\beta=0} P_{0\beta} - q(q+1)(q^2-q)P_\infty.$$

Multiplication by $f$ gives

$$\begin{array}{rcl} f\mathcal{L}(G) & = & \mathcal{L}\left(\left(q^4-q^2-2q-2\right)P_\infty - \left(q^3-q-1\right)\sum_{\beta^q+\beta=0} P_{0\beta}\right) \\ & \subseteq & \mathcal{L}\left(\left(q^4-q^2-2q-2\right)P_\infty\right). \end{array}$$

Therefore, the $(q+1)$-point code $C_{\mathcal{L}}(D,G)$ is isometric to a subcode of the one-point code $C_{\mathcal{L}}\left(D,\left(q^4-q^2-2q-2\right)P_\infty\right)$. The dimension of superspace is $\ell\left(\left(q^4-q^2-2q-2\right)P_\infty\right) = q^4 - \frac{3q^2}{2} - \frac{3q}{2} - 1$ while the dimension of the original vector space is $\ell(G) = 9$. Therefore, while $C_{\mathcal{L}}(D,G) \subseteq C_{\mathcal{L}}(D, (q^4 - q^2 - 2q - 2)\, P_\infty)$, it is difficult to glean information about $C_{\mathcal{L}}(D,G)$ by studying the larger code.

It may be possible to find a more appropriate function $f$. Given any $\mathbb{F}_{q^2}$-rational point $P_{ab}$ on $X$, the rational function $\tau_{ab} := y - b - a^q(x-a)$ has divisor $(\tau_{ab}) = (q+1)\, P_{ab} - (q+1)\, P_\infty$ [12]. Hence, a natural choice for the function $f$ would be $f = \prod_{\beta^q+\beta=0} \tau_{0\beta}$. This gives

$$f\mathcal{L}(G) = \mathcal{L}\left( \left(q^2+3q+2\right) P_\infty - q \sum_{\beta^q+\beta=0} P_{0\beta} \right) \subseteq \mathcal{L}\left( \left(q^2+3q+2\right) P_\infty \right).$$

Here, the difference in dimensions of the Riemann-Roch spaces is much smaller as $\ell\left(\left(q^2+3q+2\right) P_\infty\right) = \frac{q^2}{2} + \frac{7q}{2} + 3$.

Taking $f = x$ gives $x\mathcal{L}(G) = \mathcal{L}\left((3q+2)\, P_\infty\right)$. Now, we can see that $C_{\mathcal{L}}(D,G) \cong C_{\mathcal{L}}\left(D, (3q+2)\, P_\infty\right)$; that is, the $(q+1)$-point code $C_{\mathcal{L}}(D,G)$ is isometric to the one-point code $C_{\mathcal{L}}\left(D, (3q+2)\, P_\infty\right)$. Therefore, the exact parameters of $C_{\mathcal{L}}(D,G)$ can be determined [16]. From this, one may conclude that there is no need to consider the possibly more complicated $(q+1)$-point code since it is isometric to a one-point code. Note that not all multipoint codes are isometric to one-point codes [13].

**Example 3.2.** Again, let $X$ be defined by $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$. Let $c$ be a positive integer, and fix an $\mathbb{F}_{q^2}$-rational point $P_{ab}$ on $X$ with $a \neq 0$. Set $G = cP_\infty + (q+2)P_{ab} + \sum_{\beta^q+\beta=0,\ \beta\neq 0} P_{0\beta} + \sum_{\beta^q+\beta=a^{q+1},\ \beta\neq b} P_{a\beta}$, and take $D$ to be the sum of all other $\mathbb{F}_{q^2}$-rational points.

Taking $f = \tau_{ab}^2 \prod_{\beta^q+\beta=0,\beta\neq 0} (y-\beta) \prod_{\beta^q+\beta=a^{q+1},\beta\neq b} (y-\beta)$ yields

$$f\mathcal{L}(G) = \mathcal{L}\left(\left(2q^2+2q+c\right) P_\infty - qP_{ab} - A\right) \subseteq \mathcal{L}\left(\left(2q^2+c-2\right) P_\infty\right)$$

where $A := q \sum_{\beta^q+\beta=0,\ \beta\neq 0} P_{0\beta} + \sum_{\beta^q+\beta=a^{q+1},\ \beta\neq b} \sum_{\beta^q+\beta=\alpha^{q+1},\ \alpha\neq a} P_{\alpha\beta}$. This is a bit troubling as the subcode we are interested in is defined by the Riemann-Roch space of a divisor supported by many points. In particular, bases for this Riemann-Roch space are not known for arbitrary $q$. Moreover, the supports of $A$ and $D$ have points in common. While this could corrected by redefining $D$, it changes the code length. In effect, this would require that one consider in advance the supports of the principal divisors in question to even know the code length. In light of this, we instead multiply by $x\,(x-a)\,\tau_{ab}$ to obtain

$$x\,(x-a)\,\tau_{ab}\mathcal{L}(G) = \mathcal{L}\left((3q+c+1)\, P_\infty - P_{00}\right).$$

Bases for the associated Riemann-Roch space and for the code may now be determined as in [12].

## 4. Conclusion

The idea of studying subcodes of one-point codes is not a new one (see, for instance, [3, 4, 5, 7]). The thrust of our approach is that improved bounds on the parameters are known for certain multipoint codes, enabling one to identify subcodes with good parameters. Then, viewing a multipoint code $C$ as a subcode of a one-point code $C'$ may provide additional insight into $C$. Moreover, it may yield a simplified decoding algorithm for $C$, a topic to be addressed in another paper.

## References


[1] P. Beelen, The order bound for general AG codes, preprint.

[2] C. Carvalho and F. Torres, On Goppa codes and Weierstrass gaps at several points, Designs, Codes Cryptogr. **35** (2005), 211–225.

[3] G. L. Feng and T. R. N. Rao, Decoding algebraic-geometry codes up to the designed minimum distance, IEEE Trans. Inform. Theory **39** (1993), no. 1, 37–45.

[4] G. L. Feng and T. R. N. Rao, Improved geometric Goppa codes, Part I: Basic theory, IEEE Trans. Inform. Theory **41** (1995), 1678–1693.

[5] G. L. Feng and T. R. N. Rao, A simple approach for construction of algebraic geometry codes from affine plane curves, IEEE Trans. Inform. Theory **40** (1994), 1003–1012.

[6] V. D. Goppa, Algebraico-geometric codes, Math. USSR-Izv. **21** (1983), 75–91.

[7] T. Høholdt, J. H. van Lint, and R. Pellikaan, Algebraic geometry codes, in Handbook of Coding Theory, V. Pless, W. C. Huffman, and R. A. Brualdi, Eds., **1**, Elsevier, Amsterdam (1998), 871–961.

[8] M. Homma and S. J. Kim, Goppa codes with Weierstrass pairs, J. Pure Appl. Algebra **162** (2001), 273–290.

[9] M. Homma and S. J. Kim, Toward the determination of the minimum distance of two-point codes on a Hermitian curve. Des. Codes Cryptogr. 37 (2005), no. 1, 111–132.

[10] M. Homma and S. J. Kim, The two-point codes on a Hermitian curve with the designed minimum distance. Des. Codes Cryptogr. 38 (2006), no. 1, 55–81.

[11] M. Homma and S. J. Kim, The two-point codes with the designed distance on a Hermitian curve in even characteristic. Des. Codes Cryptogr. 39 (2006), no. 3, 375–386.

[12] H. Maharaj, G. L. Matthews, and G. Pirsic, Riemann-Roch spaces for the Hermitian curve with applications to algebraic geometry codes and low-discrepancy sequences, J. Pure and Appl. Algebra, **195** (2005), no. 3, 261–280.

[13] G. L. Matthews, Weierstrass pairs and minimum distance of Goppa codes, Des. Codes Cryptogr. **22** (2001), 107–121.

[14] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, 1993.

[15] M. A. Tsfasman and S. G. Vladut, Algebraic-Geometric Codes, Kluwer Academic Publishers, Boston, 1991.

[16] K. Yang and P. V. Kumar, On the true minimum distance of Hermitian codes, Coding Theory and Algebraic Geometry, Proceedings, Luminy, 1991, Lecture Notes in Mathematics **1518**, Springer-Verlag, 1992, 99–107.