A GENERALIZED FLOOR BOUND FOR THE MINIMUM DISTANCE OF GEOMETRIC GOPPA CODES

BENJAMIN LUNDELL AND JASON MCCULLOUGH

Abstract. We prove a new bound for the minimum distance of geometric Goppa codes that generalizes two previous improved bounds. We include examples of the bound applied to one and two point codes over certain Suzuki and Hermitian curves.

1. Introduction

In [5], Goppa gives a construction of a family of error-correcting codes using two divisors on a curve. He also gives a distance bound based on the degrees of the divisors. Yang et. al. in [16] and Chen et. al. in [1] compute the actual minimum distance of the one-point Hermitian and certain one-point Suzuki codes respectively, often showing that the actual distance is significantly higher than Goppa's designed distance. In [2], Feng and Rao present a decoding algorithm for Goppa codes, which always decodes at least up to half the designed distance. The new distance bound obtained from their algorithm is in general very good as few codes have minimum distance exceeding the Feng-Rao (F-R) distance.

Other efforts to improve and generalize the distance bounds have had some success. In [10], Kirfel and Pellikaan generalize a result of Garcia et al. in [3] and improve the designed distance by taking advantage of pairs of large gaps in the Weierstrass gap sequence at a point P. In [12], Maharaj et al. improve the minimum distance by using the notion of the floor of a divisor to capitalize on one large gap in a multi-point code. We prove a new bound, which generalizes the previous two. It can use more than one gap in the gap sequence and also applies nicely to multi-point codes. We state our main result below.

Theorem 3.3 (Generalized Floor Bound)**.** *Let $\mathcal{X}$ be a curve with function field $K/\mathbb{F}_q$ of genus* g*. Let $P_1, \ldots, P_n$ be distinct rational points on $\mathcal{X}$. Define $D := P_1 + \cdots + P_n$. Let A, B, and Z be divisors with support outside of D such that Z is effective, $\ell(A) = \ell(A - Z)$, and $\ell(B) = \ell(B + Z)$. Then, putting $G = A + B$ yields*

$$\mathrm{d}(\mathrm{C}_\Omega(\mathrm{D}, \mathrm{G})) \geq \deg(\mathrm{G}) - (2\mathrm{g} - 2) + \deg(\mathrm{Z}).$$

For some codes, the generalized floor bound (GF bound) achieves parameters that were unattainable by the previous bounds. See Section 4 for specific examples. Section 2 gives definitions and notation that will be used throughout the paper.

Date: July 19, 2005.

Key words and phrases. geometric Goppa codes, algebraic-geometry codes, minimum distance.

Section 3 gives a formal statement of all three mentioned bounds, a proof of the generalized floor bound, and relationships among the three.

2. Preliminaries

Unless otherwise noted, we follow the same definitions and notations as in [12]. If P is a rational point on a curve $\mathcal{X}$ that is defined over $\mathbb{F}_q$ with function field K, then v_P represents the discrete valuation corresponding to P. For a divisor A, we denote the support of A as Supp(A). If B is another divisor, the we define the greatest common divisor of A and B by

$$\gcd(\mathrm{A},\mathrm{B}) := \sum_{\mathrm{P}} \min\{v_{\mathrm{P}}(\mathrm{A}), v_{\mathrm{P}}(\mathrm{B})\}\mathrm{P}.$$

From A, we can create two vector spaces, one of rational functions from the function field K, and one of rational differentials:

$$\mathcal{L}(A) := \{f \in K : (f) + A \succcurlyeq 0\} \cup \{0\}$$

and

$$\Omega(A) := \{\eta \in \Omega : (\eta) \succcurlyeq A\} \cup \{0\}.$$

We denote the dimension of $\mathcal{L}(A)$ over $\mathbb{F}_q$ by $\ell(A)$ and the dimension of $\Omega(A)$ over $\mathbb{F}_q$ by $i(A)$.

Using the distinct rational points $P_1, \ldots, P_n, Q_1, \ldots, Q_m$ on $\mathcal{X}$ to form the two divisors

$$D := P_1 + \cdots + P_n \text{ and } G := \sum_i \alpha_i Q_i \quad \alpha_i \in \mathbb{Z},$$

we can define two linear m-point codes:

$$C_{\mathcal{L}}(D,G) := \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\}$$

and

$$C_{\Omega}(D,G) := \{(\mathrm{res}_{\mathrm{P}_1}(\eta), \ldots, \mathrm{res}_{\mathrm{P}_n}(\eta)) : \eta \in \Omega(\mathrm{G} - \mathrm{D})\}.$$

Both of these codes have length n. The dimension of $C_{\mathcal{L}}$ is $\ell(G) - \ell(G - D)$ and the designed distance is $n - \deg(\mathrm{G})$. The dimension of C_{Ω} is $i(G - D) - i(G)$ and the designed distance is $\mathrm{d}_{\mathrm{Goppa}} := \deg(\mathrm{G}) - (2\mathrm{g} - 2)$, where g is the genus of the curve.

The floor of A is defined in [12] as the unique divisor, A', of minimum degree such that $\mathcal{L}(A') = \mathcal{L}(A)$ and is denoted $\lfloor A \rfloor$.

Finally, we say that an integer α is an A-gap at a point P if and only if $\mathcal{L}(A+\alpha P) = \mathcal{L}(A + (\alpha - 1)P)$.

3. Minimum Distance Bounds

We start by stating two theorems. The first appears as Theorem 2.10 in [12]; the second appears as Proposition 3.10 in [10].

Theorem 3.1 (Floor Bound). *Let $K/\mathbb{F}_q$ be a function field of genus* g. *Let $D := P_1 + \cdots + P_n$ where $P_1, \ldots, P_n$ are distinct rational places of K, and let $G := H + \lfloor H \rfloor$ be a divisor of F such that the support of H does not contain any of the places $P_1, \ldots, P_n$. Set $E_H := H - \lfloor H \rfloor$. Then $C_\Omega(D, G)$ is an $[n, k, \mathrm{d}]$ code whose parameters satisfy*

$$\mathrm{d} \geq \deg(\mathrm{G}) - (2\mathrm{g} - 2) + \deg(\mathrm{E_H}) = 2\deg(\mathrm{H}) - (2\mathrm{g} - 2).$$

Theorem 3.2 (K-P Bound). *Suppose that each of the integers $\alpha, \alpha+1, \ldots, \alpha+t$ is an F-gap at P and $\beta-t, \ldots, \beta-1, \beta$ are G-gaps at P. Put $H = F+G+(\alpha+\beta-1)P$. Suppose $D := P_1 + \cdots + P_n$, where the P_i are n distinct rational points, each not equal to P and not belonging to the support of H. Then the minimum distance of $C_\Omega(D, H)$ is at least* $\deg(\mathrm{H}) - (2\mathrm{g} - 2) + (\mathrm{t} + 1)$.

We adapt the proof of the floor bound in [12] to prove the following theorem, which generalizes both the floor bound and the K-P bound. A similar proof can also be found in Lemma 3.2 in [8].

Theorem 3.3 (Generalized Floor Bound (GF Bound)). *Let $\mathcal{X}$ be a curve with function field $K/\mathbb{F}_q$ of genus* g. *Let $P_1, \ldots, P_n$ be distinct rational points on $\mathcal{X}$. Define $D := P_1 + \cdots + P_n$. Let A, B, G, and Z be divisors with support outside of D such that Z is effective, $\ell(A) = \ell(A - Z)$, $\ell(B) = \ell(B + Z)$, and $G = A + B$. Then*

$$\mathrm{d}(\mathrm{C}_\Omega(\mathrm{D}, \mathrm{G})) \geq \deg(\mathrm{G}) - (2\mathrm{g} - 2) + \deg(\mathrm{Z}).$$

Proof. Let $\eta \in \Omega(G - D)$ such that the code word $\vec{c} := (\mathrm{res}_{\mathrm{P_1}}(\eta), \ldots, \mathrm{res}_{\mathrm{P_n}}(\eta))$ is of minimum nonzero weight. Without loss of generality, we may assume that $c_i \neq 0$ for $1 \leq i \leq \mathrm{d}$ and $c_i = 0$ for $\mathrm{d} < \mathrm{i} \leq \mathrm{n}$. Let $D' := P_1 + \cdots + P_{\mathrm{d}}$. Since $\vec{c}$ is zero outside D', we must have that $(\eta) \succcurlyeq G - D'$. Thus, there exists an effective divisor, E, with support disjoint from that of D' so that $W := (\eta) = G - D' + E$. Taking degrees of both sides we get that

$$2\mathrm{g} - 2 = \deg(\mathrm{G}) - \mathrm{d} + \deg(\mathrm{E}) \Rightarrow \mathrm{d} = \deg(\mathrm{G}) - (2\mathrm{g} - 2) + \deg(\mathrm{E}).$$

Observe that,

$$\deg(\mathrm{E}) \geq \ell(\mathrm{A} + \mathrm{E}) - \ell(\mathrm{A}) = \ell(\mathrm{A} + \mathrm{E}) - \ell(\mathrm{A} - \mathrm{Z}) \geq \ell(\mathrm{A} + \mathrm{E}) - \ell(\mathrm{A} + \mathrm{E} - \mathrm{Z}).$$

By applying the Riemann-Roch Theorem twice, we get that

$$\ell(A + E) = \deg(\mathrm{A} + \mathrm{E}) + 1 - \mathrm{g} + \ell(\mathrm{W} - (\mathrm{A} + \mathrm{E}))$$

and

$$\ell(A + E - Z) = \deg(\mathrm{A} + \mathrm{E} - \mathrm{Z}) + 1 - \mathrm{g} + \ell(\mathrm{W} - (\mathrm{A} + \mathrm{E} - \mathrm{Z}))$$

and thus,

$$\ell(A + E) - \ell(A + E - Z) = \deg(\mathrm{Z}) + \ell(\mathrm{B} - \mathrm{D}') - \ell(\mathrm{B} + \mathrm{Z} - \mathrm{D}').$$

Now

$$\mathcal{L}(B + Z - D') \subseteq \mathcal{L}(B + Z) = \mathcal{L}(B)$$

implies that

$$\mathcal{L}(B + Z - D') = \mathcal{L}(B + Z - D') \cap \mathcal{L}(B) = \mathcal{L}(\gcd(\mathrm{B} + \mathrm{Z} - \mathrm{D}', \mathrm{B})).$$

Since B and Z have support outside of D' and since Z is effective, $\gcd(\mathrm{B}+\mathrm{Z}-\mathrm{D}',\mathrm{B}) = \mathrm{B}-\mathrm{D}'$, and thus $\ell(B+Z-D') = \ell(B-D')$.

Finally we see that this gives that $\deg(\mathrm{E}) \geq \deg(\mathrm{Z})$.

□

We note that the above proof assumes that the code $C_\Omega(D,G)$ is nontrivial and thus has a codeword of nonzero weight. If the code is trivial, the question of minimum distance is not very interesting.

Remark 3.4. Taking the special case $A = H$, $B = \lfloor H \rfloor$ and $Z = H - \lfloor H \rfloor$ in the GF bound gives the floor bound. Unlike the floor bound, the GF bound can always be applied. For an arbitrary divisor G it is not always the case that there exists a divisor H such that G can be written as the sum of H and $\lfloor H \rfloor$; however one can always let $A = G$ and $B = Z = 0$ and use the GF bound trivially. Beyond this, there are many examples (see §4) where the floor bound cannot be applied, but the GF bound gives an improvement over the designed distance. Additionally, there are examples where the floor bound does apply, but another choice of A and B gives a greater improvement.

Remark 3.5. Setting $A = F + (\alpha + t)P$, $B = G + (\beta - t - 1)P$ and $Z = (t+1)P$ in the GF bound yields the K-P bound. So in the case of one point codes, the GF bound reduces to the K-P bound. Note that in its statement, however, Theorem 3.2 makes no assumption about the support of F or G containing only P. Thus, the bound can be applied to m-point codes, but only takes advantage of "one-dimensional" gaps, while the GF bound uses "multi-dimensional" gaps. We also note that in order to prove their bound, Kirfel and Pellikaan compare their estimate to the F-R bound and show that their estimate is always lower. This shows that in the one-point case, the GF bound will not improve on Feng-Rao.

The GF bound also encompasses Theorem 2.1 in [4], Theorem 4 in [3], and Theorems 3.3 and 3.4 in [8].

4. Examples

In this section we give several examples of how the generalized floor bound applies to codes over two specific curves. Examples 4.1 and 4.2 concern codes over the Hermitian curve over $\mathbb{F}_{16}$. Examples 4.3 and 4.4 give codes from the Suzuki curve over $\mathbb{F}_8$. Additionally Tables 1 and 2 compute improved estimates to the minimum distance of two-point codes over these two curves.

Example 4.1. (A one-point Hermitian code) Let $\mathcal{X}$ be the Hermitian curve of genus 6 over $\mathbb{F}_{16}$ with defining equation $\mathrm{y}^4 + \mathrm{y} = \mathrm{x}^5$. Let K be the associated function field. This curve has 65 rational points over $\mathbb{F}_{16}$, denoted by $P_0, P_1, \ldots, P_{63}, P_\infty$ where P_0 is the point $(0,0)$ and P_∞ is the point at infinity. Consider the Weierstrass semigroup of the point P_∞; that is,

$$H(P_\infty) = \{n \in \mathbb{N}_0 : \exists f \in K \text{ with } (f)_\infty = nP_\infty\}.$$

One can show that

$$H(P_\infty) = \langle 4, 5 \rangle = \{0, 4, 5, 8, 9, 10, 12, 13, 14, \ldots\}.$$

It follows that

$$\mathcal{L}(11P_\infty) = \mathcal{L}(10P_\infty) \text{ and } \mathcal{L}(7P_\infty) = \mathcal{L}(6P_\infty).$$

So let $A = 11P_\infty, B = 6P_\infty$, and $Z = P_\infty$. Then for $G = A + B$ and $D = \sum_{i=0}^{63} P_i$, it follows from Theorem 3.3 that

$$\mathrm{d}(\mathrm{C}_\Omega(\mathrm{D}, \mathrm{G})) \geq \deg(\mathrm{G}) - (2\mathrm{g} - 2) + \deg(\mathrm{Z}) = 17 - (10) + 1 = 8.$$

So we get an improvement of one over the designed distance. Note that while the K-P bound would also give this improvement, the Floor Bound would not since there is no way to write $G = H + \lfloor H \rfloor$. Since $C_\Omega(D, 17P_\infty) = C_L(D, 57P_\infty)$ we see from [16] that the minimum distance of this code is exactly 8. So both the GF bound and K-P bound meet the actual distance. Since the estimates for these two bounds are the same for one-point codes, we must consider m-point codes for $m \geq 2$ to find any improvement over the K-P bound.

Example 4.2. (A two-point Hermitian code with improvement over the floor and K-P bounds) Using the notation from Example 4.1 we consider the Hermitian two-point code $C_\Omega(D, G)$ over $\mathbb{F}_{16}$ where $G = 2P_0 + 8P_\infty$ and $D = \sum_{i=1}^{63} P_i$. In [13] Matthews computes the Weierstrass semigroup of the pair (P_0, P_∞). Using this computation we can conclude that

$$\mathcal{L}(2P_0 + 6P_\infty) = \mathcal{L}(5P_\infty) \text{ and } \mathcal{L}(2P_0 + 3P_\infty) = \mathcal{L}(2P_\infty).$$

The GF bound then applies to the above code for $A = 2P_0 + 6P_\infty$, $B = 2P_\infty$, and $Z = 2P_0 + P_\infty$ yielding an improvement of $\deg(\mathrm{Z}) = 3$ over the designed distance of $\deg(\mathrm{G}) - (2\mathrm{g} - 2) = 10 - 10 = 0$. Note that using effective divisors neither the Floor bound nor the K-P bound can achieve this improvement. The best choice of a divisor H for the Floor bound is $H = 2P_0 + 4P_\infty$ with $\lfloor H \rfloor = 4P_\infty$. Then the Floor bound achieves an improvement of $\deg(\mathrm{H}) - \deg(\lfloor \mathrm{H} \rfloor) = 2$. This same gap may be used in the K-P bound to achieve the same improvement; i.e. set $F = G = 2P_0 + 4P_\infty, P = P_0, \alpha = 1, \beta = 1, t = 1$ and apply Theorem 3.2.

To give a more global perspective we consider how the GF bound applies to all two-point Hermitian codes over $\mathbb{F}_{16}$; that is, codes of the form $C_\Omega(D, xP_0 + yP_\infty)$ with $D = \sum_{i=1}^{63} P_i$ as in Example 4.2. (See Table 1.) First we restrict our attention to codes with $G = xP_0 + yP_\infty$ effective and with $\deg(\mathrm{G}) \geq 2\mathrm{g} - 2 = 10$ where the designed distance is nonnegative. It can be shown that $(\mathrm{y}) = 5\mathrm{P}_0 - 5\mathrm{P}_\infty$. Thus we further restrict our attention to codes with $0 \leq y < 5$ since any excluded code is equivalent to one with y value in this range.

Now using the Weierstrass semigroup $H(P_0, P_\infty)$, we compute for each $G = xP_0 + yP_\infty$ in this range the best choice of effective divisors for each of the 3 bounds in Section 3. Given that gaps in the Weierstrass sequence disappear beyond $2g-1$, this is a finite computation. In the upper left (a) we mark with a '+' those codes with minimum distance strictly greater than the designed distance. This was computed using the computer algebra system MAGMA. In the upper right (b) we list the improvement over the designed distance predicted by the floor bound. Thus if $H + \lfloor H \rfloor = xP_0 + yP_\infty$, we write $\deg(\mathrm{H}) - \deg(\lfloor \mathrm{H} \rfloor)$ at position (x, y). Italicized numbers represent codes where the Floor bound did not apply directly but the bound followed from a containment in a larger code to which the Floor bound did apply. For example, the code with $G = 12P_0 + 2P_\infty$ is contained in the code with

$G = 12P_0 + 1P_\infty$, thus its minimum distance is at least that of the larger code. In the lower right (d) we list the best improvement predicted by the GF bound using effective divisors. So the value at position (x, y) is

$$\max_{A,B,Z\geq 0}\{\deg(\mathrm{Z}) : \mathrm{A}+\mathrm{B} = \mathrm{xP}_0 + \mathrm{yP}_\infty, \ell(\mathrm{A}-\mathrm{Z}) = \ell(\mathrm{A}), \text{ and } \ell(\mathrm{B}) = \ell(\mathrm{B}+\mathrm{Z})\}$$

where A, B and Z have supports disjoint with that of D.

y \ x	0	1	2	3	4
6					+
7				+	+
8			+	+	+
9		+	+	+	
10		+	+	+	
11	+	+	+	+	+
12	+	+	+	+	+
13	+	+	+		
14		+	+		
15		+	+		
16	+	+	+	+	+
17	+	+			
18		+			
19		+			
20		+			
21	+				
(a)	$\mathrm{d} > \mathrm{d}_{\mathrm{Goppa}}$				

x \ y	0	1	2	3	4	x / y
6						6
7						7
8				2	*1*	8
9				*1*		9
10		1	2	*1*		10
11	1	2	3	*2*	*1*	11
12	2	3	*2*	*1*		12
13	*1*	*2*	*1*			13
14		*1*				14
15						15
16		1				16
17						17
18		1				18
19						19
20		1				20
21	1					21
(b)	Floor Bound					

y \ x	0	1	2	3	4
6					1
7				2	2
8			2	2	1
9		1	2	1	
10		1	2	1	
11	1	1	2	1	1
12	2	2	2	1	1
13	1	1	1		
14		1	1		
15		1	1		
16	1	1	1	1	1
17	1	1			
18		1			
19		1			
20		1			
21	1				
(c)	K-P Bound				

x / y	0	1	2	3	4	x / y
6					2	6
7				3	2	7
8			3	2	1	8
9		2	2	1		9
10		1	2	1		10
11	1	2	3	2	1	11
12	2	3	2	1	1	12
13	1	2	1			13
14		1	1			14
15		1	1			15
16	1	1	1	1	1	16
17	1	1				17
18		1				18
19		1				19
20		1				20
21	1					21
(d)	GF Bound					

Table 1

Lower Bounds on $\mathrm{d} - \mathrm{d}_{\mathrm{Goppa}}$ for Hermitian two-point codes over $\mathbb{F}_{16}$.
(a) Codes with designed distance strictly greater than the designed distance.
(b) Lower bounds on $\mathrm{d} - \mathrm{d}_{\mathrm{Goppa}}$ given by Theorem 3.1.
(c) Lower bounds on $\mathrm{d} - \mathrm{d}_{\mathrm{Goppa}}$ given by Theorem 3.2.
(d) Lower bounds on $\mathrm{d} - \mathrm{d}_{\mathrm{Goppa}}$ given by Theorem 3.3.

We make the analagous computation for the K-P bound and list its improvement for the same codes in the lower left (c). For example the code in Example 4.2 shows up as a '3' in position $(2, 8)$ of Table 1(d).

Example 4.3. (A two-point Suzuki code that is not a shortened one-point code) We now consider the Suzuki curve $\mathrm{y}^8 - \mathrm{y} = \mathrm{x}^{10} - \mathrm{x}^3$ over $\mathbb{F}_8$. The exact parameters of the one-point codes are given in [1]. A computation of the Weierstrass semigroup of the pair (P_0, P_∞) is given in [14]. We denote the 65 rational points again by $P_0, P_1, \ldots, P_{63}, P_\infty$. Let C be the code $C = C_\Omega(D, G)$ over the Suzuki curve with $G = 5P_0 + 28P_\infty$ and D the sum of the other 63 rational points. From the Weierstrass semigroup we see that

$$\mathcal{L}(1P_0 + 13P_\infty) = \mathcal{L}(2P_0 + 15P_\infty) \text{ and } \mathcal{L}(3P_0 + 13P_\infty) = \mathcal{L}(4P_0 + 15P_\infty).$$

Thus we may take $A = 2P_0 + 15P_\infty$, $B = 3P_0 + 13P_\infty$, and $Z = P_0 + 2P_\infty$ and apply the GF bound to the code C to get $\mathrm{d} \geq \deg(\mathrm{G}) - (2\mathrm{g}-2) + \deg(\mathrm{Z}) = 33 - 26 + 3 = 10$. This code then corresponds to the 3 at position $(x, y) = (5, 28)$ in Table 2, since the GF bound predicts an improvement of 3 over the designed distance. This code has dimension $k = n - \deg G + \mathrm{g} - 1 = 63 - 33 + 14 - 1 = 43$. From [1] we see that the one point codes (that is, codes of the form $C_L(\sum_{i=0}^{63} P_i, \alpha P_\infty)$) with dimension at least 43 have actual minimum distance at most 8. So we see that two-point codes can have parameters better than comparable one-point codes, as is noted in [12], [14] and [13]. We also note that neither the $K - P$ bound nor the Floor bound can predict this improvement.

Example 4.4. (A two-point Suzuki code that achieves a better bound using non-effective divisors) Computing the GF bound for choices of effective divisor A and B as in Tables 1 and 2 often gives good improvement on the minimum designed distance. We show now that this may not always produce the optimal choice of divisors A and B. We again consider the two-point Suzuki codes now with $G = 32P_\infty$ and D as before. One can see from the Weierstrass semigroup $H(P_0, P_\infty)$ that

$$\mathcal{L}(8P_0 + 6P_\infty) = \mathcal{L}(8P_0 + 4P_\infty) \text{ and } \mathcal{L}(5P_0 + 15P_\infty) = \mathcal{L}(5P_0 + 13P_\infty).$$

One can also show that $(\mathrm{y}) = 13\mathrm{P}_0 - 13\mathrm{P}_\infty$, from which it follows that

$$\ell(-5P_0 + 19P_\infty) = \ell(8P_0 + 6P_\infty - (y)) = \ell(8P_0 + 4P_\infty - (y)) = \ell(-5P_0 + 17P_\infty).$$

Thus by setting $A = 5P_0 + 15P_\infty$, $B = -5P_0 + 17P_\infty$ and $Z = 2P_\infty$ the GF bound gives an improvement of $\deg(\mathrm{Z}) = 2$ over the designed distance of $\deg(\mathrm{G}) - (2\mathrm{g} - 2) = 32 - 26 = 6$. Since this is the shortened version of the one-point code $C_\Omega(\sum_{i=0}^{63} P_i, 32P_\infty)$ and since the automorphism group of the Suzuki function field is doubly transitive, we conclude that this code also has minimum distance at least 8. We note that this agrees with the actual minimum distance computed in [1]. By the computation done for Table 2, the best choice of effective A and B yield only an improvement of 1 over the designed distance.

In Table 2 we list the improvement over the designed distance of all two-point Suzuki codes over $\mathbb{F}_8$ given by the GF bound. This is analogous to the computation in Table 1(d). Again we restrict our attention to codes of the form $C_\Omega(D, G)$ where $G = xP_0 + yP_\infty$, $\deg(\mathrm{G}) \geq 2\mathrm{g} - 2 = 26$ and G is effective. As noted in Example 4.4 the linear equivalence $13P_0 \sim 13P_\infty$ allows us to further restrict our attention to codes with $y < 13$.

y \ x	0	1	2	3	4	5	6	7	8	9	10	11	12
14													2
15												3	3
16											3	2	3
17										3	3	2	3
18									3	3	3	2	2
19								4	3	3	3	2	2
20							4	3	3	3	2	2	1
21						3	3	3	2	2	1	1	
22					3	3	3	3	2	2	1	1	1
23				3	3	3	3	2	1	1		1	
24			3	2	2	2	2	2	1	1	1	1	1
25		2	3	3	3	2	2	1		1		1	
26		1	2	2	2	2	2	1		1		1	
27	1	2	3	2	2	2	2	2	1	2	1	2	1
28	2	3	4	3	3	3	2	3	2	2	2	1	1
29	1	2	3	2	2	2	1	2	1	1	1		
30	1	2	3	2	2	2	2	2	1	1	1	1	1
31	1	2	3	2	2	2	1	1	1				
32	1	2	2	1	2	1	2	1	1	1	1	1	1
33	1	2	3	2	2	1	1						
34		1	2	1	1	1	1						
35	1	2	2	1	1		1						
36		1	2	1	1		1						
37	1	2	1		1		1						
38		1	1		1		1						
39		1	1		1		1						
40	1	1	1	1	1	1	1	1	1	1	1	1	1
41	1	1	1	1	1	1							
42		1	1		1								
43	1	1	1	1									
44		1	1										
45	1	1											
46		1											
47		1											
48		1											
49		1											
50		1											
51		1											
52		1											
53	1												

Table 2
The GF bound improvement for the Suzuki curve over $\mathbb{F}_8$.

Note. We note that Tables 1 and 2 were computed using information about the Weierstrass semigroup on two points that appeared in [13] and [14] respectively.

We also note that the GF bound is not sharp as it does not reach the actual distance in all cases. Nor does the GF bound exceed the F-R bound in the case of one-point codes. In the general m-point case, both the floor bound and the GF bound produce improvements for the minimum distance yet they lack decoding algorithms to exploit those improvements.

5. Acknowledgments

The authors would like to thank the referee for helping to improve the presentation, and Professor Iwan Duursma for his advising and tutelage through the course of this project. Benjamin Lundell was supported by an NSF VIGRE REU grant and Jason McCullough by an NSF VIGRE graduate fellowship, both grant number DMS9983.

References

[1] Chien-Yu Chen and Iwan M. Duursma. Geometric Reed-Solomon codes of length 64 and 65 over $\mathbb{F}_8$. *IEEE Transactions on Information Theory*, 49(5), 2003.

[2] Gui-Liang Feng and T.R.N Rao. Decoding algebraic-geometry codes up to the design minimum distance. *IEEE Transactions on Information Theory*, 39(1), 1993.

[3] Arnaldo García, Seon Jeong Kim, and Robert F. Lax. Consecutive Weierstrass gaps and minimum distance of Goppa codes. *Journal of Pure and Applied Algebra*, 84, 1993.

[4] Arnaldo García and R. F. Lax. Goppa codes and Weierstrass gaps. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.* Springer, Berlin, 1992.

[5] V. D. Goppa. *Geometry and Codes*. Kluwer Academic Publishers, Dordrecht, 1988.

[6] Tom Høhold and Ruud Pellikaan. On the decoding of algebraic-geometry codes. *IEEE Transactions on Information Theory*, 41(6), 1995.

[7] Tom Høhold, Jacobus H. van Lint, and Ruud Pellikaan. Algebraic geometry codes. *Handbook of Coding Theory*, 1, 1998.

[8] Masaaki Homma and Seon Jeong Kim. Goppa codes with Weierstrass pairs. *Journal of Pure and Applied Algebra*, 162, 2001.

[9] Seon Jeong Kim. On the index of the Weierstrass semigroup of a pair of points on a curve. *Archiv der Mathematik*, 62(1), 1994.

[10] Christoph Kirfel and Ruud Pellikann. The minimum distance of codes in an array coming from telescopic semigroups. *IEEE Transactions on Information Theory*, 41(6, part 1), 1995.

[11] Hiren Maharaj and Gretchen L. Matthews. On the floor and ceiling of a divisor. *preprint*, 2004.

[12] Hiren Maharaj, Gretchen L. Matthews, and Gottleb Pirsic. Riemann-Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences. *Journal of Pure and Applied Algebra*, 195, 2005.

[13] Gretchen L. Matthews. Weierstrass pairs and minimum distance of Goppa codes. *Designs, Codes and Cryptography*, 22(2), 2001.

[14] Gretchen L. Matthews. Codes from the Suzuki function field. *IEEE Transactions on Information Theory*, 50(12), 2004.

[15] Henning Stichtenoth. A note on Hermitian codes over GF(q^2). *IEEE Transactions on Information Theory*, 34(5), 1988.

[16] K. Yang, P. V. Kumar, and H. Stichtenoth. On the weight hierarchy of geometric goppa codes. *IEEE Trans. Inform. Theory*, IT-40, 1994.

Dept. of Mathematics, University of Illinois, Urbana, Illinois 61801

E-mail address: blundell@math.uiuc.edu, jmccullo@math.uiuc.edu