Consecutive Weierstrass Gaps and Minimum Distance of Goppa Codes

Arnaldo Garcia[1], Seon Jeong Kim[2], and R.F. Lax[3]

Abstract: We prove that if there are consecutive gaps at a rational point on a smooth curve defined over a finite field, then one can improve the usual lower bound on the minimum distance of certain algebraic-geometric codes defined using a multiple of the point.

A q-ary linear code of length n and dimension k is a vector subspace of dimension k of $\mathbf{F}_q^n$, where $\mathbf{F}_q$ denotes the finite field with q elements. The minimum distance of a code is the minimum number of places in which two distinct codewords differ. The greater the minimum distance, the greater the number of errors that the code can detect or correct. For a linear code, the minimum distance is also the minimum weight of a nonzero codeword, where the weight of a codeword is the number of nonzero places in that codeword. A linear code of length n, dimension k and minimum distance d is called an $[n, k, d]$-code.

V.D. Goppa [3,4] realized that one could use the Riemann-Roch Theorem to show that certain codes produced from two divisors G and D on a curve have good properties. In particular, he gave lower bounds for the minimum distances of these codes. In a previous article [1], the first and third authors showed that if G is taken to be a multiple of a point P, then knowledge of the gaps at P may allow one to say that the minimum distance of the resulting code is greater than Goppa's lower bound. We also showed that the presence of t consecutive gaps, together with certain conditions on osculating spaces at the point P, could allow one to conclude that the resulting code has minimum distance at least t greater than Goppa's bound.

Here, we drop any assumptions about osculating spaces at P and show that, by assuming more about the gaps at P, one may obtain a similar result relating consecutive gaps with an improvement of Goppa's bound on the minimum distance. In the first section, we give the necessary definitions. The second section contains our main results (Theorems 3 and 4), and in the final section, we present two examples illustrating the theorems.

1. Let X denote a nonsingular, geometrically irreducible, projective curve of genus $g > 1$ defined over $\mathbf{F}_q$. Assume that X has $\mathbf{F}_q$-rational points. Let D be a divisor on X defined over $\mathbf{F}_q$ (i.e., D is invariant under $\mathrm{Gal}(\overline{\mathbf{F}_q}/\mathbf{F}_q)$). Then $L(D)$ will denote the $\mathbf{F}_q$-vector space of all rational functions f on X, defined over $\mathbf{F}_q$, with divisor $(f) \geq -D$, together with the zero function, and $\Omega(D)$ will denote the $\mathbf{F}_q$-vector space of all rational differentials η on X, defined over $\mathbf{F}_q$, with divisor $(\eta) \geq D$, together with the zero differential. Put $l(D) = \dim_{\mathbf{F}_q} L(D)$ and $i(D) = \dim_{\mathbf{F}_q} \Omega(D)$. The Riemann-Roch Theorem states that

$$\begin{aligned} l(D) &= \deg D + 1 - g + i(D) \\ &= \deg D + 1 - g + l(K - D), \end{aligned}$$

[1] Partially supported by a CNPq grant

[2] Partially supported by a KOSEF grant

[3] Partially supported by NSF grant INT-9101337

where K is any canonical divisor on X. Also, we will write D_0 (resp. D_∞) for the divisor of zeros (resp. divisor of poles) of D. Hence we have

$$D_0 \geq 0, D_\infty \geq 0, (\text{Supp } D_0) \cap (\text{Supp } D_\infty) = \emptyset, \text{ and } D = D_0 - D_\infty.$$

Let G be a divisor on X defined over $\mathbf{F}_q$ and let $D = P_1 + P_2 + \cdots + P_n$ be another divisor on X where $P_1, \ldots, P_n$ are distinct $\mathbf{F}_q$-rational points and none of the P_i is in the support of G. The algebraic-geometric Goppa codes $C_L(G, D)$ and $C_\Omega(G, D)$ are defined as follows (cf. [3,4,6,9]). The code $C_L(G, D)$ is the image of the linear map $\phi : L(G) \to \mathbf{F}_q^n$ defined by

$$f \longmapsto (f(P_1), f(P_2), \ldots, f(P_n)).$$

If deg $G < n$, then this code has dimension $l(G) \geq \deg G + 1 - g$ and minimum distance at least $n - \deg G$.

The code $C_\Omega(G, D)$ is the image of the linear map $\phi^* : \Omega(G - D) \to \mathbf{F}_q^n$ defined by

$$\eta \longmapsto (\text{res}_{P_1}(\eta), \text{res}_{P_2}(\eta), \ldots, \text{res}_{P_n}(\eta)).$$

If deg $G > 2g - 2$, then this code has dimension $l((K + D - G) \geq n - \deg G + g - 1$ and minimum distance at least deg $G - (2g - 2)$. The codes $C_L(G, D)$ and $C_\Omega(G, D)$ are dual codes (i.e., dual vector subspaces of $\mathbf{F}_q^n$ under the usual inner product). Alternatively, if one fixes a nonzero rational differential ω with (canonical) divisor K, then, the image of ϕ^* is the same as the image of the map $\psi^* : L(K + D - G) \to \mathbf{F}_q^n$ defined by

$$f \longmapsto (\text{res}_{P_1}(f\omega), \text{res}_{P_2}(f\omega), \ldots, \text{res}_{P_n}(f\omega)).$$

Now let P denote a (closed) $\mathbf{F}_q$-rational point on X and let B be a divisor defined over $\mathbf{F}_q$. We call a natural number γ a B-gap at P if there is no rational function f on X such that

$$((f) + B)_\infty = \gamma P.$$

By the Riemann-Roch Theorem, γ is a B-gap at P if and only if $\gamma - 1$ is an order at P for the divisor $K - B$ (where K denotes a canonical divisor on X); i.e., we have

$$K - B \sim (\gamma - 1)P + E,$$

where $E \geq 0$, $P \notin$ Supp(E), and $\sim$ denotes linear equivalence. With this terminology, the usual Weierstrass gaps at P are the 0-gaps at P.

2. In [1], the first and third authors proved the following result, which shows how knowledge of the gaps at P can lead to a code with minimum distance greater than the lower bound above.

Theorem 1. *Suppose γ_j and γ_k are B-gaps at P. Put $G = (\gamma_j + \gamma_k - 1)P + 2B$. Suppose $D = P_1 + P_2 + \cdots + P_n$, where the P_i are n distinct $\mathbf{F}_q$-rational points, each not belonging to the support of G. If the dimension of $C_\Omega(G, D)$ is positive, then the minimum distance of this code is at least* $\deg G - 2g + 3$.

The following similar result for the codes $C_L(G,D)$ was proved by Janwa [5] in the case of Weierstrass gaps.

Theorem 2. *Suppose γ is a B-gap at P. Put $G = \gamma P + B$. Suppose $D = P_1 + P_2 + \cdots + P_n$, where the P_i are n distinct $\mathbf{F}_q$-rational points, each not belonging to the support of G. If the code $C_L(G,D)$ has positive dimension, then its minimum distance is at least $n - \deg G + 1$.*

Proof. Suppose the minimum distance is exactly $n - \deg G$. Then there exists a rational function f such that, after renumbering the P_i if necessary, we have

$$(f) = P_1 + P_2 + \cdots + P_{\deg G} - G.$$

But then

$$(f) + B = P_1 + P_2 + \cdots + P_{\deg G} - \gamma P,$$

contradicting the fact that γ is a B-gap at P. ▮

In [1], the first and third authors went on to show that if there were $t+1$ consecutive B-gaps $\gamma_j, \gamma_j + 1, \ldots, \gamma_j + t$ and if certain osculating spaces at P missed certain linear spaces, then the minimum distance of the code in Theorem 1 is at least $\deg G - (2g-2) + (t+1)$. In this paper, we show that by assuming more about the sequence of B-gaps at P, one may drop the conditions on the osculating spaces. This results in an easy-to-check (once the gaps are known) criterion for showing that the minimum distance of certain codes is significantly better than the usual lower bound.

First, we present a generalization of Theorem 2 to the case of $t+1$ consecutive gaps.

Theorem 3. *Suppose that each of the integers $\gamma - t, \gamma - (t-1), \ldots, \gamma - 1, \gamma$ is a B-gap at P. Put $G = \gamma P + B$. Suppose $D = P_1 + P_2 + \cdots + P_n$, where the P_i are n distinct $\mathbf{F}_q$-rational points, each not belonging to the support of G. If the code $C_L(G,D)$ has positive dimension, then its minimum distance is at least $n - \deg G + t + 1$.*

Proof. Assume that there exists a rational function $f \in L(G)$ such that f gives rise to a codeword of weight $w \le n - \deg G + t$. Then, after renumbering the P_i if necessary,

$$(f) = P_1 + P_2 + \cdots + P_{n-w} - G + E,$$

where E is an effective divisor of degree at most t defined over $\mathbf{F}_q$. Write $E = \lambda P + E'$, where E' is effective, P is not in the support of E', and $0 \le \lambda \le t$. Using the fact that $G = \gamma P + B$, we then get

$$(f) + B = P_1 + P_2 + \cdots + P_{n-w} + E' - (\gamma - \lambda)P.$$

But this contradicts the hypothesis that $\gamma - \lambda$ is a B-gap at P. ▮

Now we present a generalization of Theorem 1.

Theorem 4. *Suppose that each of the integers $\alpha, \alpha+1, \ldots, \alpha+t, \beta-(t-1), \ldots, \beta-1, \beta$ is a B-gap at P, with $\alpha + t \le \beta$ and $t \ge 1$. Put $G = (\alpha + \beta - 1)P + 2B$. Suppose $D = P_1 + P_2 + \cdots + P_n$, where the P_i are distinct $\mathbf{F}_q$-rational points, each not belonging to* *the support of G. If the code $C_\Omega(G,D)$ has positive dimension, then its minimum distance is at least* $\deg G-(2g-2)+(t+1)$.

Our proof of Theorem 4 requires the following Lemma.

Lemma . *With assumptions as in Theorem 4, further assume that there exists a canonical divisor K of the form*

$$K=G+E-(P_1+P_2+\cdots P_w),$$

where E is an effective divisor (defined over $\mathbf{F}_q$) of degree t, and where $w=\deg G-(2g-2)+t\leq n$. Then

1) $L((\alpha+i)P+E+B)\neq L((\alpha+i-1)P+E+B)$ for $i=0,1,\ldots,t-1$. Also, $L((\beta-j)P+E+B)\neq L((\beta-j-1)P+E+B)$ for $j=0,1,\ldots,t$.

2) If $P\notin$ Supp(E), then the function $h(s)=l(sP+E+B)-l(sP+B)$ is a nondecreasing function of s.

3) Suppose $h(s)=m$. If either $\alpha-1\leq s\leq\alpha+t-2$ or $\beta-t\leq s<\beta$, then $h(s+1)=m+1$.

Proof of the Lemma.
(1) Suppose that $L((\alpha+i)P+E+B)=L((\alpha+i-1)P+E+B)$ for some $i=0,1,\ldots,t-1$. Then $L((\alpha+i)P+E+B-P_1-P_2-\cdots-P_w)=L((\alpha+i-1)P+E+B-P_1-P_2-\cdots-P_w)$, since no P_i equals P. Then using the canonical divisor K and the Riemann-Roch Theorem, we obtain $L((\beta-i-1)P+B)\neq L((\beta-i)P+B)$, contradicting the assumption that $\beta-i$ is a B-gap at P. The second assertion is proved similarly using the fact that $\alpha+j$ is a B-gap at P.

(2) It suffices to show that if $l(sP+B)=l((s-1)P+B)+1$, then $l(sP+E+B)=l((s-1)P+E+B)+1$. But if $f\in L(sP+B)\setminus L((s-1)P+B)$, then $f\in L(sP+E+B)\setminus L((s-1)P+E+B)$ since $P\notin\mathrm{Supp}(E)$.

(3) From part (1) of the Lemma, it follows that $l((s+1)P+E+B)=l(sP+E+B)+1$. Since $s+1$ is a B-gap at P, it follows that $l((s+1)P+B)=l(sP+B)$. Hence $h(s+1)=l((s+1)P+E+B)-l((s+1)P+B)=l(sP+E+B)+1-l(sP+B)=h(s)+1$. ∎

Proof of Theorem 4. Our proof will proceed by induction on t. Suppose $t=1$. From Theorem 1, we know that the minimum distance of $C_\Omega(G,D)$ is at least $\deg G-2g+3$. Assume that equality holds and let $\eta\in\Omega(G-D)$ be a differential that gives rise to a codeword of weight $w=\deg G-2g+3$. Then, after possibly renumbering the P_i,

$$(\eta)=G-(P_1+P_2+\cdots+P_w)+Q,$$

where Q is some $\mathbf{F}_q$-rational point of X. It follows from the first part of the Lemma that $L(\alpha P+Q+B)\neq L((\alpha-1)P+Q+B)$. From this, we may conclude that $Q\neq P$, since $\alpha+1$ is a B-gap at P. Now consider the function $h(s)$ defined in the second part of the Lemma with $E=Q$. It follows from (3) of the Lemma that $h(\alpha)\geq 1$. Hence, by (2) of the Lemma, $h(\beta-1)\geq 1$ and, by (3) of the Lemma, $h(\beta)\geq 2$. This is a contradiction since $h(\beta)=l(\beta P+Q+B)-l(\beta P+B)\leq\deg Q=1$.

Now assume that the Theorem is true when t is replaced by $t-1$. Then the minimum distance of $C_\Omega(G,D)$ is at least $\deg G-(2g-2)+t$. Assume that equality holds and let

$\eta \in \Omega(G-D)$ be a differential that gives rise to a codeword of weight $w = \deg G - (2g-2) + t$. Then

$$(\eta) = G - (P_1 + P_2 + \cdots + P_w) + E,$$

where E is an effective divisor of degree t defined over $\mathbf{F}_q$. We claim that $P \notin \mathrm{Supp}(E)$. For if P were in the support of E, then by putting $G' = G + P$ and applying the induction hypothesis (viewing $\alpha+1, \ldots, \alpha+t$ as t consecutive gaps), we would have that the minimum distance of $C_\Omega(G', D)$ is at least $\deg G' - (2g-2) + t = w+1$; but η gives rise to a codeword of this code of weight w.

Now, as in the proof of the $t = 1$ case, we have $h(\alpha) \geq 1$ and $h(\beta) = l(\beta P + E + B) - l(\beta P + B) \leq \deg E = t$. But from (3) of the Lemma, $h(\alpha + t - 1) = h(\alpha) + t - 1 \geq t$. Since $\alpha + t - 1 \leq \beta - 1$, it follows from (2) and (3) of the Lemma, that $h(\beta)$ is at least $t + 1$, which is a contradiction. ∎

Corollary. *Suppose $\alpha, \alpha + 1, \ldots, \alpha + t$ are $t + 1$ consecutive B-gaps at P. Put $G = (2\alpha + t - 1)P + 2B$. If the code $C_\Omega(G, D)$, with D as in Theorem 4, has positive dimension, then its minimum distance is at least* $\deg G - (2g - 2) + (t + 1)$.

In the special case that $t = 1$, we can also prove the following result by similar reasoning.

Theorem 5. *Suppose α, β, and $\beta + 1$ are all B-gaps at P, with $\alpha < \beta$. Then with G and D as in Theorem 4, the code $C_\Omega(G, D)$, if nontrivial, has minimum distance at least* $\deg G - 2g + 4$.

3. We close with two examples to illustrate our results.

Example 1. Let X denote the Hermitian curve $y^q + y = x^{q+1}$ defined over the field $\mathbf{F}_{q^2}$. Codes on X have been studied by Stichtenoth [8], Yang and Kumar [11], and Xing [10], among others. We show how Theorems 3 and 4 may be used to give another method for determining the minimum distance of some of these codes. The Weierstrass points of X are precisely the $\mathbf{F}_{q^2}$-rational points and the gap sequence at each Weierstrass point is

$$\begin{aligned}
&1, 2, 3, \ldots, q-1, \\
&q+2, q+3, \ldots, 2q-1, \\
&2q+3, 2q+4, \ldots, 3q-1, \\
&\qquad\qquad \vdots \\
&(q-4)(q+1)+1, (q-4)(q+1)+2, (q-3)q-1, \\
&(q-3)(q+1)+1, (q-2)q-1, \\
&(q-2)(q+1)+1 (= (q-1)q-1 = 2g-1)
\end{aligned}$$

(cf. [7,2,8]). Let P denote the point at infinity. Fix an integer r with $1 \leq r \leq q-2$. Put $\gamma = (r+1)q - 1, G = \gamma P$, and let D denote the divisor of the q^3 $\mathbf{F}_{q^2}$-rational points other than P. Then $r(q+1)+1, r(q+1)+2, \ldots, \gamma$ are $q - r - 1$ consecutive gaps at P. Hence, by Theorem 3, the minimum distance of $C_L(G, D)$ is at least $q^3 - r(q+1)$. We can see that equality holds as follows. Choose r distinct elements $b_1, b_2, \ldots, b_r \in \mathbf{F}_{q^2}$ that do not satisfy the equation $y^q + y = 0$. Then the function

$$f = \prod_{i=1}^{r} (y - b_i)$$

is in $L(G)$ and has precisely $r(q+1)$ zeros among the finite points on X. Therefore, f gives rise to a codeword of weight $q^3 - r(q+1)$ of the code $C_L(G, D)$.

To illustrate Theorem 4, fix an integer s with $0 \le s \le q-3$. Put $\alpha = s(q+1)+1, \beta = (s+2)q - 1$, and $G = (\alpha + \beta - 1)P = (2(s+1)q + s - 1)P$. Then by Theorem 4, the minimum distance of $C_\Omega(G, D)$ is at least $\deg G - (2g-2) + (q - s - 1) = q(2s + 4 - q)$. Take $s > (q-4)/2$. We claim that the minimum distance is exactly $q(2s+4-q)$. Choose $2s + 4 - q$ distinct elements $a_1, a_2, \ldots, a_{2s+4-q} \in \mathbf{F}_{q^2}$. Then the rational differential

$$\frac{dx}{\prod_{j=1}^{2s+4-q} (x - a_j)}$$

is in $\Omega(G - D)$ and has weight exactly $q(2s + 4 - q)$.

Example 2. Let X denote the nonsingular model of the function field defined by the equation $y^q + y = x^m$, where $m > 2$ divides $q + 1$, over the field $\mathbf{F}_{q^2}$. Such curves have been studied by F.K. Schmidt [7], and by the first author and P. Viana [2]. The curve X has genus $g = (m-1)(q-1)/2$ and has $1 + q(1 + m(q-1))$ rational points over $\mathbf{F}_{q^2}$, the maximum possible by the Hasse-Weil bound. These $\mathbf{F}_{q^2}$-rational points are precisely all the Weierstrass points of X. Again, take P to be the point at infinity. Put $u = (q+1)/m$. The Weierstrass gaps at P are all positive integers of the form $rm + s + 1$, where r and s are all the nonnegative integers such that $r + su \le q - 1 - u$ (cf. [2]).

Let r be an integer with $0 \le r \le q - 1 - 2u$ and such that u divides $r + 2$. Put

$$\begin{aligned}
&\alpha = rm + 1, \\
&\beta = (r+u)m + (q - 1 - 2u - r)/u + 1 = (r+u)m + m - (r+2)/u - 1, \\
&G = (\alpha + \beta - 1)P.
\end{aligned}$$

Let D denote the sum of the remaining $\mathbf{F}_{q^2}$-rational points. Then Theorem 4 applies with $t = (q - 1 - u - r)/u = m - (r+2)/u - 1$. Hence, the minimum distance d of $C_\Omega(G, D)$ satisfies

$$\begin{aligned}
d &\ge \deg G - (2g-2) + m - (r+2)/u \\
&= q(2v - m + 1) + m(u - 1),
\end{aligned}$$

where $v = (r+2)/u$. Now, further suppose that $2v - m + 1 \ge 0$ (equivalently, that $r \ge (q - u - 3)/2$). Then we claim that equality holds in the above bound on d.

Choose $u - 1$ distinct elements $b_1, b_2, \ldots, b_{u-1} \in \mathbf{F}_{q^2}$ such that $b_j^q + b_j$ is not equal to either 0 or 1 for $j = 1, 2, \ldots, u-1$. Choose $2v - m + 1$ distinct elements $a_1, a_2, \ldots, a_{2v-m+1}$ in the cyclic subgroup of $\mathbf{F}_{q^2}^*$ of order m. (Note that since $r \le q - 3 = mu - 4$, we have

$v = (r+2)/u < m$. Hence, $2v - m + 1 < m$.) Thus $a_i^m = 1$ for $i = 1, 2, \ldots, 2v - m + 1$. Then it is not hard to see that the rational differential

$$\frac{dx}{\prod_{j=1}^{u-1}(y - b_j) \cdot \prod_{i=1}^{2v-m+1}(x - a_i)}$$

is in $\Omega(G - D)$ and has precisely $q(2v - m + 1) + m(u - 1)$ simple (since $a_i^m = 1 \neq b_j^q + b_j$ for all i and j) poles. To our knowledge, the determination of the minimum distance of these codes is new.

References

1. A. Garcia and R.F. Lax, Goppa codes and Weierstrass gaps, in: Proceedings of AGCT-3, Luminy, 1991, to appear.
2. A. Garcia and P. Viana, Weierstrass points on certain non-classical curves, Arch. Math. **46** (1986), 315–322.
3. V.D. Goppa, Algebraico-geometric codes, Math. USSR Izvestiya **21** (1983), 75–91.
4. V.D. Goppa, Geometry and codes (Kluwer, Dordrecht, 1988).
5. H. Janwa, On the parameters of algebraic geometric codes, in: Proceedings of applied algebra, algebraic algorithms, and error-correcting codes : 9th International Symposium (AAECC-9), New Orleans, LA, 1991, Lecture Notes in Computer Science **539**, 19–28.
6. J.H. van Lint and G. van der Geer, Introduction to coding theory and algebraic geometry (Birkhäuser, Basel, 1988).
7. F.K. Schmidt, Zur arithmetischen Theorie der algebraischen Funktionen II. Allgemeine Theorie der Weierstrasspunkte, Math. Z. **45** (1939), 75–96.
8. H. Stichtenoth, A note on Hermitian codes over $GF(q^2)$, IEEE Trans. Inform. Theory **34**, no. 5 (1988), 1345–1348.
9. M.A. Tsfasman and S.G. Vladut, Algebraic-geometric codes (Kluwer, Dordrecht, 1991).∎
10. C.-P. Xing, A note on the minimum distance of Hermitian codes, preprint, Univ. Science and Tech. of China, Hefei, Anhui, 1991.
11. K. Yang and P.V. Kumar, On the true minimum distance of Hermitian codes, in: Proceedings of AGCT-3, Luminy, 1991, to appear.

Instituto de Matemática Pura e Aplicada, Estrada Dona Castorina 110, 22.460 Rio de Janeiro, Brasil (E-mail: garp@lncc.bitnet)

Department of Mathematics, Gyeongsang National University, Chinju, 660-701, Korea

Department of Mathematics, LSU, Baton Rouge, LA 70803, USA
(E-mail: lax@marais.math.lsu.edu)