STOPPING SETS OF HERMITIAN CODES

SARAH E. ANDERSON AND GRETCHEN L. MATTHEWS

Abstract. Combinatorial structures called stopping sets are useful in analyzing the performance of a linear code when coupled with an iterative decoding algorithm over an erasure channel. In this paper, we consider stopping sets of Hermitian codes.

1. Introduction

Combinatorial structures called stopping sets are useful in analyzing the performance of a linear code when coupled with an iterative decoding algorithm over an erasure channel [5, 20]. Given a code C with an $r \times n$ parity-check matrix H and a set S of column indices of H, S is a stopping set of C if and only if the $r \times |S|$ matrix formed from H by deleting those columns with indices not in S does not have a row of weight 1. Iterative decoding is typically applied to codes defined by sparse matrices, meaning low-density parity-check (LDPC) codes. Even so, the algorithms themselves apply to any linear code. Perhaps it is for this reason that stopping sets have been studied for a number of codes, including Hamming codes [1]; Reed-Muller codes [9]; the Simplex codes, the Hamming codes, the first order Reed-Muller codes and the extended Hamming codes [12]; and array codes [7, 8].

The study of stopping sets of algebraic geometric codes was initiated by Zhang, Fu, and Wan [24]. They demonstrate that Riemann-Roch spaces may be used to determine if a set of column indices of the parity-check matrix whose rows are precisely the nonzero codewords of the dual is a stopping set. Using these ideas, they consider algebraic geometric codes from function fields of low genus, meaning those from the rational function field and elliptic function fields. They observe that stopping sets of Reed-Solomon codes are completely determined by their cardinalities and give a characterization of stopping sets of algebraic geometric codes from elliptic function fields.

There are several motivations for our examination of stopping sets of algebraic geometric codes. First, iterative decoding algorithms, though best suited to low-density parity-check codes, apply to any linear code, and adaptations have been suggested to handle codes defined by dense matrices. Moreover, every linear code can be viewed as an algebraic geometric code [18]. Second, since the columns of a parity-check matrix for an algebraic geometric code correspond to rational points on a curve, one might expect certain configurations of points to produce stopping sets; that is, the structure of the stopping set may be linked to that of the underlying curve. Third, there are recent applications of algebraic geometric codes to polar coding. In particular, polar codes depend on a kernel matrix used, which may arise from

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975; email: gmatthe@clemson.edu

G. L. Matthews' work is supported in part by NSA MSP-111006 and NSF DMS-1403062.

algebraic -geometric codes. Recent work on graph representations of polar codes suggests new ties between these kernels, iterative decoding, and stopping sets [3]. Furthermore, the performance of finite-length polar codes over the binary erasure channel when coupled with belief propagation decoding has recently been analyzed along with stopping sets of these codes. Specifically, Eslami and Pishro-Nik proposed a polar-LDPC concatenation using belief propagation decoding for the polar and LDPC codes to use in optical transport networks and showed these codes outperform current coding schemes [6]. Finally, while stopping sets of algebraic geometric codes have been considered for low genus curves (i.e., 0 and 1), a hallmark of the algebraic geometric construction is the ability to produce long codes with a variety of parameters, which relies on the use of curves of larger genus.

Other than the Reed-Solomon codes, Hermitian codes are the best understood class of algebraic geometric codes. Moreover, Hermitian codes are known to have excellent parameters and can outperform Reed-Solomon codes over the same field. Hermitain codes have much longer codewords and larger Hamming minimum distance than Reed-Solomon codes. As a result, Hermitain codes have good bit-error correction [23] as well as significantly better burst error correction [4] compared to Reed-Solomon codes over the same field size. However, Hermitian codes have higher decoding complexity [10, 14].

In this paper, we consider stopping sets of Hermitian codes. We construct stopping sets corresponding to collections of points, which in some cases are collinear in a certain sense. This suggests a relationship between stopping sets, which are combinatorial structures, and the underlying geometry of the curve. In [24], Zhang et al. use the group structure of the set of points on an elliptic curve to provide conditions for whether a collection of points corresponds to a stopping set. In the absence of this structure for curves of larger genus, we rely on explicit bases for Riemann-Roch spaces associated with the Hermitian curve. A benefit of this approach is that particular collections of points are identified as giving rise to stopping sets whereas others are ruled out as stopping sets.

This paper is organized as follows. Section 2 contains background information on stopping sets, especially those of algebraic geometric codes and their dependence on related Riemann-Roch spaces. Our main results are featured in Section 3 where we study stopping sets of Hermitian codes. Examples are found in Section 4, followed by closing comments found in Section 5.

2. Riemann-Roch spaces and stopping sets of algebraic geometric codes

The structure of an algebraic geometric code reveals information about its stopping sets, as demonstrated in [24]. In particular, dimensions of Riemann-Roch spaces can be used to determine if a set is a stopping set. In this section, we review the relevant results of [24], extending and supplementing them as necessary.

In this paper, we consider linear codes. Let H be a parity-check matrix of an $[n, k, d]$-code C over $\mathbb{F}_q$, the finite field with q elements, and let $[n] = \{1, \ldots, n\}$ denote the set of column indices of H.

Definition. A stopping set S of the code C with parity-check matrix H is a subset of $[n]$ such that the restriction of H to S does not contain a row of weight 1.

Notice that stopping sets depend not just on the code but also on the choice of parity-check matrix of the code. Hence, we write $C = \Gamma(H)$ to mean a code C with parity-check matrix H. If H is an $r \times n$ matrix and $S \subseteq [n]$, we write $H|_S$ to denote the restriction of H to S, meaning the $r \times |S|$ matrix formed from H by deleting those columns of H indexed by elements of $[n] \setminus S$.

Given a code C, let H^* denote a parity-check matrix whose rows are precisely the nonzero codewords of the dual code $C^\perp$. As shown in the next result, determining stopping sets of $C = \Gamma(H^*)$ allows one to find stopping sets of $\Gamma(H)$ where H is an arbitrary parity-check matrix of C. Considering codes represented by H^* is not a new notion. For instance, it was noted by Kelley and Sridhara [13] that adding all possible check nodes to a Tanner graph gives a graph with the smallest number of lift-realizable pseudocodewords among all possible representations of the code and that if this graph does not have any bad noncodeword-pseudocodewords then the performance obtained with iterative decoding is the same as the optimal ML performance. Schwartz and Vardy used the matrix H^* to show that the stopping redundancy of a code, which is smallest number of rows in a parity-check matrix for a code whose stopping distance is equal to the minimum distance, is well defined [20].

Proposition 2.1. *If S is a stopping set of $C^\perp = \Gamma(H^*)$ and C' is a subcode of C, then S is a stopping set of $C'^\perp = \Gamma(H')$ for any parity-check matrix H' of $C'^\perp$. In particular, if S is a stopping set of $\Gamma(H^*)$, then S is a stopping set of $\Gamma(H)$ for any parity-check matrix H of C.*

Proof. Suppose $C' \subseteq C$. Let H' be a parity-check matrix of $C'^\perp$, meaning $C'^\perp = \Gamma(H')$. Then H' is a generator matrix for C'. Let H^* denote a matrix whose rows are precisely the nonzero codewords of C. It follows that H' is a submatrix of H^*, because $C' \subseteq C$. Suppose that S is a stopping set of $C^\perp = \Gamma(H^*)$. By definition, $H^*|_S$ has no rows of weight 1. Since $H'|_S$ is a submatrix of $H^*|_S$ with the same column indices, $H'|_S$ has no rows of weight 1. Thus, S is a stopping set of $\Gamma(H') = C'^\perp$. □

Stopping sets of algebraic geometric codes were first studied by Zhang, Fu, and Wan [24], and their work focuses on codes $\Gamma(H^*)$. In this section, we review their results and extend some to $\Gamma(H)$ where H is an arbitrary parity-check matrix of C. This lays the groundwork for studying stopping sets of Hermitian codes in the next section. We begin by setting up notation to be used for algebraic geometric codes.

Let F be a function field over $\mathbb{F}_q$ of genus g. Let $\mathbb{P}_F$ denote the set of places of the function field F. Given a divisor $G = \sum_{P \in \mathbb{P}_F} a_P P$ of F, $v_P(G) := a_P$. If $f \in F \setminus \{0\}$, we write $v_P(f)$ to mean $v_P((f))$ where (f) denotes the principal divisor of the function f. Given two divisors G and G' of F, we write $G \leqslant G'$ if and only if $v_P(G) \leqslant v_P(G')$ for all $P \in \mathbb{P}_F$. The support of a divisor G is $\operatorname{supp} G = \{P \in \mathbb{P}_F : v_P(G) \neq 0\}$.

An algebraic geometric (or AG) code $C_{\mathcal{L}}(D, G)$ is constructed using two divisors G and $D = P_1 + \cdots + P_n$ on F with disjoint supports, where the P_i are distinct places of F of degree 1. The algebraic geometric code $C_{\mathcal{L}}(D, G)$ is

$$C_{\mathcal{L}}(D, G) = \{\operatorname{ev}(f) : f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n,$$

where

$$\operatorname{ev}(f) = (f(P_1), \ldots, f(P_n))$$

and

$$\mathcal{L}(G) = \{f \in F \mid (f) \geqslant -G\} \cup \{0\}$$

is the Riemann-Roch space of G. Let $\ell(G) := dim(\mathcal{L}(G))$. Its dual is

$$C_\Omega(D, G) = C_\mathcal{L}(D, G)^\perp.$$

A parity-check matrix of $C_\Omega(D, G)$ is a generator matrix for $C_\mathcal{L}(D, G)$; hence, it has the form

$$\begin{bmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\ \vdots & \vdots & & \vdots \\ f_k(P_1) & f_k(P_2) & \cdots & f_k(P_n) \end{bmatrix}$$

where $\{f_1, \ldots, f_k\}$ spans $\mathcal{L}(G)$ as an $\mathbb{F}_q$-vector space. Notice that the columns of a parity-check matrix of $C_\Omega(D, G)$ correspond to the places in the support of the divisor D. Hence, at times, we sometimes speak of stopping sets of such codes as being sets of places in the support of D, rather than the indices of the places.

In this paper, we consider strongly algebraic geometric codes, meaning those satisfying $2g - 2 < \deg G < n$, as coined by Pellikaan, Shen, and van Wee [18].

The following result is similar to [24, Theorem 6]; in fact, Lemma 2.2(2) is a restatement.

Lemma 2.2. *Let $C = C_\Omega(D, G)$ be a code of length n and $S \subseteq [n]$.*

(1) *If*

$$\mathcal{L}\left(G - \sum_{j \in S} P_j\right) = \mathcal{L}\left(G - \sum_{j \in S \setminus \{i\}} P_j\right)$$

for all $i \in S$, then S is a stopping set of $\Gamma(H)$ for any parity-check matrix H of C.

(2) *The set S is a stopping set of $\Gamma(H^*)$ if and only if*

$$\mathcal{L}\left(G - \sum_{j \in S} P_j\right) = \mathcal{L}\left(G - \sum_{j \in S \setminus \{i\}} P_j\right)$$

for all $i \in S$.

(3) *Let H be a parity-check matrix of C. If S is a stopping set of $\Gamma(H)$, then $ev(f)$ is not a row of H for any*

$$f \in \mathcal{L}\left(G - \sum_{j \in S \setminus \{i\}} P_j\right) \setminus \mathcal{L}\left(G - \sum_{j \in S} P_j\right)$$

and $i \in S$.

Proof. Let $C = C_\Omega(D, G)$ be a code of length n and $S \subseteq [n]$.

(1) Fix a parity-check matrix H of C. Suppose $S = \{i_1, \ldots, i_j\}$ is not a stopping set of $\Gamma(H)$. Then $H|_S$ contains a row of weight 1. Hence, there exists $f \in \mathcal{L}(G)$ such that

$$\text{wt}\left((f(P_{i_1}), \ldots, f(P_{i_j}))\right) = 1.$$

Therefore, there exists $i \in S$ such that $f(P_i) \neq 0$ and $f(P_j) = 0$ for all $j \in S \setminus \{i\}$. Then

$$(f) \geqslant \sum_{j \in S \setminus \{i\}} P_j - G$$

and $v_{P_i}(f) = 0$, which implies

$$f \in \mathcal{L}\left(G - \sum_{j \in S \setminus \{i\}} P_j\right) \setminus \mathcal{L}\left(G - \sum_{j \in S} P_j\right).$$

(2) According to (1), if $\mathcal{L}\left(G - \sum_{j \in S} P_j\right) = \mathcal{L}\left(G - \sum_{j \in S \setminus \{i\}} P_j\right)$ for all $i \in S$, then S is a stopping set of $\Gamma(H^*)$.

Now assume $S = \{i_1, \ldots, i_j\}$ is a stopping set of $\Gamma(H^*)$. Suppose

$$\mathcal{L}\left(G - \sum_{j \in S} P_j\right) \neq \mathcal{L}\left(G - \sum_{j \in S \setminus \{i\}} P_j\right)$$

for some $i \in S$. Then there exists

$$f \in \mathcal{L}\left(G - \sum_{j \in S \setminus \{i\}} P_j\right) \setminus \mathcal{L}\left(G - \sum_{j \in S} P_j\right).$$

As a result, there exists an effective divisor M with $P_i \notin \mathrm{supp} M$ such that

$$(f) = \sum_{j \in S \setminus \{i\}} P_j - G + M.$$

Notice that $\mathrm{wt}\left((f(P_{i_1}), \ldots, f(P_{i_j}))\right) = 1$ since $f(P_j) = 0$ for all $j \in S \setminus \{i\}$ and $f(P_i) \neq 0$. This is a contradiction as $H^*|_S$ does not contain a row of weight one. Therefore,

$$\mathcal{L}\left(G - \sum_{j \in S} P_j\right) = \mathcal{L}\left(G - \sum_{j \in S \setminus \{i\}} P_j\right)$$

for all $i \in S$.

(3) Let H be a parity-check matrix of C and S be a stopping set of $\Gamma(H)$. Suppose $\mathrm{ev}(f)$ is a row of H where $f \in \mathcal{L}\left(G - \sum_{j \in S \setminus \{i\}} P_j\right) \setminus \mathcal{L}\left(G - \sum_{j \in S} P_j\right)$ for some $i \in S$. As in the proof of (2), this implies $\mathrm{wt}\left((f(P_{i_1}), \ldots, f(P_{i_j}))\right) = 1$ which yields a contradiction. Hence, H has no rows of the form $\mathrm{ev}(f)$ where $f \in \mathcal{L}\left(G - \sum_{j \in S \setminus \{i\}} P_j\right) \setminus \mathcal{L}\left(G - \sum_{j \in S} P_j\right)$.

□

Lemma 2.2 indicates that the cardinality of a set plays a role in whether or not it is a stopping set, as shown in Figure 1 for the parity-check martix H^*. This is stated in the next result (cf. [24, Corollary 7] which applies to the parity-check matrix H^*.)

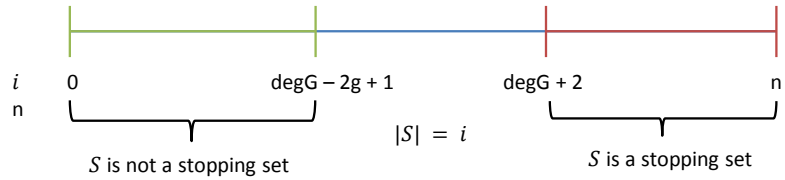

FIGURE 1. For very small and very large sets S, $|\ S\ |$ determines whether or not S is a stopping set of $C_\Omega(D,G)$ with parity-check matrix H^*.

Proposition 2.3. *Let $C = C_\Omega(D,G)$ be a code of length n and $S \subseteq [n]$.*

(1) *If $|S| \geqslant \deg G + 2$, then S is a stopping set of $\Gamma(H)$ for any parity-check matrix H of C.*
(2) *If $|S| \leqslant \deg G - 2g + 1$, then S is not a stopping set of $\Gamma(H^*)$.*
(3) *If $|S| \leqslant \deg G - 2g + 1$, then S is not a stopping set of $\Gamma(H)$ for any parity-check matrix H of C that has a row given by $ev(f)$ where $f \in \mathcal{L}\left(G - \sum_{j\in S\setminus\{i\}} P_j\right) \setminus \mathcal{L}\left(G - \sum_{j\in S} P_j\right)$ for some $i \in S$.*

Proof. Let $C = C_\Omega(D,G)$ be a code of length n and $S \subseteq [n]$.

(1) Let H be a parity-check matrix of C. Suppose $|S| \geqslant \deg G + 2$. Then

$$\deg\left(G - \sum_{j\in S} P_j\right) < \deg\left(G - \sum_{j\in S\setminus\{i\}} P_j\right) = \deg G - (|S| - 1) \leqslant -1 < 0.$$

Consequently,

$$\mathcal{L}\left(G - \sum_{j\in S} P_j\right) = \mathcal{L}\left(G - \sum_{j\in S\setminus\{i\}} P_j\right) = \{0\}.$$

By Lemma 2.2(1), S is a stopping set of $\Gamma(H)$.

(2) Suppose $|S| \leqslant \deg G - 2g + 1$. For any $i \in S$,

$$\deg\left(G - \sum_{j\in S\setminus\{i\}} P_j\right) > \deg\left(G - \sum_{j\in S} P_j\right) \geqslant 2g - 1.$$

By the Riemann-Roch Theorem,

$$\ell\left(G - \sum_{j\in S} P_j\right) = \deg G - |S| + 1 - g \neq \deg G - |S| + 2 - g = \ell\left(G - \sum_{j\in S\setminus\{i\}} P_j\right).$$

Thus, S is not a stopping set of $\Gamma(H^*)$ by Lemma 2.2(2).

(3) Notice that if $\mathrm{ev}(f)$ is a row of H, where $C = \Gamma(H)$ and $f \in \mathcal{L}\left(G - \sum_{j\in S\setminus\{i\}} P_j\right) \setminus \mathcal{L}\left(G - \sum_{j\in S} P_j\right)$, then Lemma 2.2(3) combined with the argument in (2) above indicates that S is not a stopping set of $\Gamma(H)$.

□

Next, we provide a result which is useful in finding stopping sets of algebraic geometric codes. This is determined for $\Gamma(H^*)$ by Zhang et. al. [24, Theorem 8].

Lemma 2.4. *Let H be a parity-check matrix of a code $C = C_\Omega(D, G)$ of length n and $S \subseteq [n]$. If for all $i \in S$, there exists a function h with*

$$(h) = K + \sum_{j\in S} P_j - G - M$$

where K is a canonical divisor and M is an effective divisor such that $P_i \notin \mathrm{supp}M$, then S is a stopping set of $\Gamma(H)$. The converse holds for $\Gamma(H^*)$ as well as for $\Gamma(H)$ where H has no rows of the form $ev(f)$ with $(f) \geqslant \sum_{j\in S\setminus\{i\}} P_j - G$ and $v_{P_i}(f) = 0$ for all $i \in S$.

Proof. Let H be a parity-check matrix of $C = C_\Omega(D, G)$ and $i \in S$. Suppose there exists a function h with

$$(h) = K + \sum_{j\in S} P_j - G - M$$

where K is a canonical divisor and M is an effective divisor with $P_i \notin \mathrm{supp}M$. Then

$$(h^{-1}) = G + M - K - \sum_{j\in S} P_j,$$

which implies

$$h^{-1} \in \mathcal{L}\left(K + \sum_{j\in S} P_j - G\right) \setminus \mathcal{L}\left(K + \sum_{j\in S\setminus\{i\}} P_j - G\right).$$

Thus,

$$\ell\left(K + \sum_{j\in S} P_j - G\right) = \ell\left(K + \sum_{j\in S\setminus\{i\}} P_j - G\right) + 1.$$

By the Riemann-Roch Theorem,

$$\begin{aligned}
\ell\left(G - \textstyle\sum_{j\in S} P_j\right) &= \deg G - |S| + 1 - g + \ell\left(K - G + \textstyle\sum_{j\in S} P_j\right) \\
&= \deg G - |S| + 1 - g + \ell\left(K - G + \textstyle\sum_{j\in S\setminus\{i\}} P_j\right) + 1 \\
&= \deg G - (|S| - 1) + 1 - g + \ell\left(K - G + \textstyle\sum_{j\in S\setminus\{i\}} P_j\right) \\
&= \ell\left(G - \textstyle\sum_{j\in S\setminus\{i\}} P_j\right).
\end{aligned}$$

Thus, S is a stopping set by Lemma 2.2(1).

Assume S is a stopping set of $\Gamma(H^*)$. According to Lemma 2.2(2),

$$\ell\left(G-\sum_{j\in S}P_j\right)=\ell\left(G-\sum_{j\in S\setminus\{i\}}P_j\right)$$

for all $i\in S$. It follows from the Riemann-Roch Theorem that

$$\begin{aligned}\ell\left(K-G+\textstyle\sum_{j\in S}P_j\right) &= \ell\left(G-\textstyle\sum_{j\in S}P_j\right)-\deg G+|S|-1+g\\ &= \ell\left(G-\textstyle\sum_{j\in S\setminus\{i\}}P_j\right)-\deg G+|S|-1+g\\ &= \ell\left(K-G+\textstyle\sum_{j\in S\setminus\{i\}}P_j\right)+1,\end{aligned}$$

where K is a canonical divisor of F. Hence, there exists

$$h\in\mathcal{L}\left(K-G+\sum_{j\in S}P_j\right)\setminus\mathcal{L}\left(K-G+\sum_{j\in S\setminus\{i\}}P_j\right).$$

Consequently,

$$(h)\geqslant G-K-\sum_{j\in S}P_j$$

and $v_{P_i}(h)=-1$. Thus, there exists an effective divisor M with $P_i\notin\operatorname{supp}M$ such that $(h)=M+G-K-\sum_{j\in S}P_j$; that is, $(h^{-1})=K+\sum_{j\in S}P_j-G-M$.

Note that if H has no rows of the form $\operatorname{ev}(f)$ with $(f)=\sum_{j\in S\setminus\{i\}}P_j-G$ for all $i\in S$, then Lemma 2.2(3) combined with the argument above gives the desired result. □

Proposition 2.5. *Suppose $C_{\mathcal{L}}(D,G')$ and $C_{\mathcal{L}}(D,G)$ are algebraic geometric codes with $G'\leqslant G$. If S is a stopping set of $\Gamma(H^*)$ where $C=C_\Omega(D,G)$, then S is a stopping set of $C_\Omega(D,G')$ with any choice of parity-check matrix H'.*

Proof. This follows immediately from Proposition 2.1. □

3. Stopping sets of Hermitian codes

In this section, we consider stopping sets of Hermitian codes, meaning algebraic geometric codes on the Hermitian function field. Throughout, we take q to be a power of a prime. Let $F=\mathbb{F}_{q^2}(x,y)$ be the function field with defining equation $y^q+y=x^{q+1}$ where q is a power of a prime. We consider the Hermitian code $C_\Omega(D,mP_\infty)$ over $\mathbb{F}_{q^2}$ where m is a positive integer, $D=\sum_{\alpha,\beta\in\mathbb{F}_{q^2},\beta^q+\beta=\alpha^{q+1}}P_{\alpha,\beta}$ and $P_{\alpha,\beta}$ is a common zero of $x-\alpha$ and $y-\beta$, and P_∞ is the infinite place of F. Recall that the Hermitian function field F has genus

$$g=\frac{q(q-1)}{2}.$$

The code $C_\Omega(D,mP_\infty)$ has length $n=q^3$.

Keeping in mind Proposition 2.3 and the fact that we are interested in strongly algebraic geometric codes, in all that follows, we consider codes $C_\Omega(D,mP_\infty)$ and $S\subseteq[n]$ where $2g-2<m<n$ and $m-2g+1<|S|<m+1$.

Corollary 3.1. *Consider the Hermitian code $C = C_\Omega(D, mP_\infty)$ over $\mathbb{F}_{q^2}$. Given any parity-check matrix H of C, any subset of $[n]$ with cardinality at least $m+2$ is a stopping set of $\Gamma(H)$. Any non-empty subset of $[n]$ with cardinality at most $m-q^2+q+1$ is not a stopping set of $\Gamma(H^*)$.*

Proof. This follows immediately from Proposition 2.3. □

To say more about stopping sets of Hermitian codes, we will need some additional tools that are useful in studying Hermitian codes. One such object is the Weierstrass semigroup of places of the function field F. Let $\mathbb{N}$ denote the set of nonnegative integers. Given distinct rational places $P_1, \ldots, P_m$, the Weierstrass semigroup of the m-tuple of places $(P_1, \ldots, P_m)$ is

$$H(P_1, \ldots, P_m) = \{(\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m : \exists f \in F \text{ with } (f)_\infty = \alpha_1 P_1 + \cdots + \alpha_m P_m\}.$$

We will write $\langle a_1, \ldots, a_k\rangle := \{\sum_{i=1}^k c_i a_i : c_i \in \mathbb{N}\}$ to denote the subsemigroup of nonnegative integers generated by $a_1, \ldots, a_k \in \mathbb{N}$. It is well known that $H(P) = \langle q, q+1\rangle$ for any place P of degree one of the Hermitian function field over $\mathbb{F}_{q^2}$. In addition, $H(P_1, P_2)$ has been completely determined [17]. Given $\alpha \in \mathbb{N}$,

$$\beta_\alpha := \min\{\beta \in \mathbb{N} : (\alpha, \beta) \in H(P_1, P_2)\}.$$

For any two distinct rational points P_1 and P_2 on the Hermitian function field over $\mathbb{F}_{q^2}$,

$$\beta_{(t-j)(q+1)+j} = (q-t-1)(q+1) + j \tag{1}$$

for $1 \leqslant j \leqslant t \leqslant q-1$ [17, Theorem 3.4]. Let F/K be a function field with distinct places $P_1, \ldots, P_m$ of degree one and γ denote its gonality, meaning γ is the minimum degree of a field extension $F/K(z)$ where $z \in F$. Then as stated in [2]

$$\gamma \leqslant \min\left\{\alpha_1 + \cdots + \alpha_m : (\alpha_1, \ldots, \alpha_m) \in H(P_1, \ldots, P_m) \setminus \{(0, \ldots, 0)\}\right\}.$$

Hence, for the Hermitian function field over $\mathbb{F}_{q^2}$,

$$q \leqslant \min\left\{\alpha_1 + \cdots + \alpha_m : (\alpha_1, \ldots, \alpha_m) \in H(P_1, \ldots, P_m) \setminus \{(0, \ldots, 0)\}\right\}. \tag{2}$$

Next, we describe important families of places of the Hermitian function field, because they will often make up large parts of stopping sets of Hermitian codes. Given $\alpha \in \mathbb{F}_{q^2}$, let

$$K_\alpha := \left\{\beta \in \mathbb{F}_{q^2} \mid \beta^q + \beta = \alpha^{q+1}\right\}.$$

Then $P_{\alpha\beta}$ is a place of degree one of F, for all $\beta \in K_\alpha$. Similarly, for $\beta \in \mathbb{F}_{q^2}$, set

$$L_\beta := \left\{\alpha \in \mathbb{F}_{q^2} : \beta^q + \beta = \alpha^{q+1}\right\}.$$

Notice that $|K_\alpha| = q$ and $|L_\beta| = q+1$.

We say that a set $S \subseteq [q^3]$ is a collinear set if the columns of the parity-check matrix of $C_\Omega(D, mP_\infty)$ indexed by S correspond to places in the set

$$\{P_1, \ldots, P_t\} \cup \{P_{\alpha_s\beta} : 1 \leqslant s \leqslant b, \beta \in K_{\alpha_s}\} \tag{3}$$

where b is a nonnegative integer, $P_j \in \{P_{\alpha,\beta} \in \mathbb{P}_F \mid \beta \in K_\alpha\}$ for some $\alpha \in \mathbb{F}_{q^2}$, and $|S| = bq + t$ with $0 \leqslant t \leqslant q-1$. If S is not of the form given in (3), we say that S is a

noncollinear set. In [15, Theorem 3.6], the authors determine that

$$\ell\left(rP_\infty + \sum_{\beta\in K_\alpha} k_\beta P_{\alpha,\beta}\right) = \sum_{i=0}^{q} \max\left\{\left\lfloor \frac{r-iq}{q+1}\right\rfloor + \sum_{\beta\in K_\alpha}\left\lfloor\frac{k_\beta+i}{q+1}\right\rfloor + 1, 0\right\} \tag{4}$$

for any $r, k_\beta \in \mathbb{Z}$. This allows us to verify the existence of collinear stopping sets of $C_\Omega(D, mP_\infty)$ of sizes a for $m - q^2 + q + 2 \leqslant a \leqslant m + 1$. These stopping sets consist of either:

- all columns corresponding to points with $x = \alpha$ for b values $\alpha \in \{\alpha_1, \ldots, \alpha_b\} \subseteq \mathbb{F}_{q^2}$, or
- all columns corresponding to points with $x = \alpha$ for b values $\alpha \in \{\alpha_1, \ldots, \alpha_b\} \subseteq \mathbb{F}_{q^2}$ along with "enough" columns corresponding to points with $x = \alpha'$ for some $\alpha' \in \mathbb{F}_{q^2} \setminus \{\alpha_1, \ldots, \alpha_b\}$

where $b = \left\lfloor \frac{a}{q}\right\rfloor$. We will see that any collection consisting of all columns corresponding to points with $x = \alpha_i$ for b values $\alpha_1, \ldots, \alpha_b \in \mathbb{F}_{q^2}$ forms a stopping set and that if one adds "enough" additional columns corresponding to another value $x = \alpha'$ this also constitutes a stopping set. This is made precise in the next argument.

Theorem 3.2. *Consider the Hermitian code $C = C_\Omega(D, mP_\infty)$ over $\mathbb{F}_{q^2}$. Let b and t be nonnegative integers with $0 \leqslant t \leqslant q-1$. There exists a collinear stopping set of $\Gamma(H^*)$ of size $bq+t$ where $m-2g+2 \leqslant bq+t \leqslant m+1$ if and only if $\left\lfloor \frac{m-bq}{q+1}\right\rfloor + 2 \leqslant t$ or $t = 0$. Given any parity-check matrix H of C, if $\left\lfloor \frac{m-bq}{q+1}\right\rfloor + 2 \leqslant t$ or $t = 0$ where $m - 2g + 2 \leqslant bq + t \leqslant m + 1$, then $\Gamma(H)$ has a stopping set of size $bq + t$.*

Proof. Fix a parity-check matrix H of C. Let $n = q^3$. Suppose $S \subseteq [n]$ is a collinear set as in (3). Let $S' \subseteq S$ denote the set of column indices corresponding to $\cup_{i\in\{1,\ldots,b\}}\{P_{\alpha_i,\beta} \mid \beta \in K_{\alpha_i}\}$, and let $S'' \subseteq S$ denote those corresponding to $\{P_1, \ldots, P_t\}$; that is, abusing notation,

$$S' = \cup_{i\in\{1,\ldots,b\}}\{P_{\alpha_i,\beta} \mid \beta \in K_{\alpha_i}\}$$

and

$$S'' = \{P_1, \ldots, P_t\}.$$

First, observe that

$$\mathcal{L}\left(mP_\infty - \sum_{j\in S} P_j\right) \cong \mathcal{L}\left((m-bq)P_\infty - \sum_{j\in S''} P_j\right).$$

To see this, consider $f \in \mathcal{L}\left(mP_\infty - \sum_{j\in S} P_j\right)$. Notice that

$$f\prod_{s=1}^{b}(x-\alpha_s)^{-1} \in \mathcal{L}\left((m-bq)P_\infty - \sum_{j\in S''} P_k\right).$$

Furthermore, multiplication by $\prod_{s=1}^{b}(x-\alpha_s)^{-1}$ defines the desired isomorphism. Similarly, one may check that for all $i \in S''$,

$$\mathcal{L}\left(mP_\infty - \sum_{j\in S\setminus\{i\}} P_j\right) \cong \mathcal{L}\left((m-bq)P_\infty - \sum_{j\in S''\setminus\{i\}} P_j\right).$$

Moreover, if $i \in S'$, then

$$\mathcal{L}\left(mP_\infty - \sum_{j\in S\setminus\{i\}} P_j\right) \cong \mathcal{L}\left((m-bq)P_\infty + P_i - \sum_{j\in S''} P_j\right).$$

Next, assume $t = 0$. Let $h = \prod_{s=1}^{b}(x-\alpha_s)$. Then

$$(h) = (2g-2)P_\infty + \sum_{j\in S} P_j - mP_\infty - (bq+2g-2-m)P_\infty$$

satisfies the conditions of Lemma 2.4, because $|S| \geqslant m-(2g-2)$ which implies $(bq+2g-2-m)P_\infty$ is an effective divisor. Thus, S is a stopping set of $\Gamma(H)$. Hence, in the rest of the proof, we assume $1 \leqslant t \leqslant q-1$.

Now, assume that $\left\lfloor \frac{m-bq}{q+1} \right\rfloor + 2 \leqslant t$. According to Equation (4),

$$\begin{aligned}\ell\left((m-bq)P_\infty - \textstyle\sum_{j\in S''} P_j\right) &= \max\left\{\left\lfloor \tfrac{m-bq}{q+1}\right\rfloor - t + 1, 0\right\} \\ &\quad + \textstyle\sum_{r=1}^{q} \max\left\{\left\lfloor \tfrac{m-bq-rq}{q+1}\right\rfloor + 1, 0\right\}.\end{aligned}$$

If $i \in S''$, then

$$\begin{aligned}\ell\left((m-bq)P_\infty - \textstyle\sum_{j\in S''\setminus\{i\}} P_j\right) &= \max\left\{\left\lfloor \tfrac{m-bq}{q+1}\right\rfloor - t + 2, 0\right\} \\ &\quad + \textstyle\sum_{r=1}^{q} \max\left\{\left\lfloor \tfrac{m-bq-rq}{q+1}\right\rfloor + 1, 0\right\} \\ &= 0 + \textstyle\sum_{r=1}^{q} \max\left\{\left\lfloor \tfrac{m-bq-rq}{q+1}\right\rfloor + 1, 0\right\} \\ &= \max\left\{\left\lfloor \tfrac{m-bq}{q+1}\right\rfloor - t + 1, 0\right\} \\ &\quad + \textstyle\sum_{r=1}^{q} \max\left\{\left\lfloor \tfrac{m-bq-rq}{q+1}\right\rfloor + 1, 0\right\} \\ &= \ell\left((m-bq)P_\infty - \textstyle\sum_{j\in S''} P_j\right),\end{aligned}$$

since $\left\lfloor \frac{m-bq}{q+1} \right\rfloor + 1 \leqslant \left\lfloor \frac{m-bq}{q+1} \right\rfloor + 2 \leqslant t$. Now consider $i \in S'$. Recall that

$$\mathcal{L}\left((m-bq)P_\infty - \sum_{j\in S''} P_j\right) \subseteq \mathcal{L}\left((m-bq)P_\infty + P_i - \sum_{j\in S''} P_j\right).$$

If

$$\ell\left((m-bq)P_\infty - \sum_{j\in S''} P_j\right) \neq \ell\left((m-bq)P_\infty + P_i - \sum_{j\in S''} P_j\right),$$

then there exists $f \in F$ with $(f)_\infty = P_i + aP_\infty$ for some $a \in \mathbb{N}$ with $a \leqslant m - bq$. Consequently, Equation (1) implies $a \geqslant \beta_1 = (q-2)(q+1)+1$. It follows that $(q-2)(q+1)+1 \leqslant a \leqslant m-bq$ and

$$q \leqslant \left\lfloor \frac{(q-2)(q+1)+1}{q+1} \right\rfloor + 2 \leqslant \left\lfloor \frac{m-bq}{q+1} \right\rfloor + 2 \leqslant t,$$

which is a contradiction as $1 \leqslant t \leqslant q-1$. Thus, S is a stopping set of $\Gamma(H)$ by Lemma 2.2.

Finally, we claim that if S is a collinear stopping set of $\Gamma(H^*)$, then $\left\lfloor \frac{m-bq}{q+1} \right\rfloor + 2 \leqslant t$ or $t = 0$. Suppose

$$\ell\left(G - \sum_{j \in S} P_j\right) = \ell\left(G - \sum_{j \in S \setminus \{i\}} P_j\right)$$

for all $i \in S$. Then either $t = 0$ or

$$\begin{aligned} \ell\left((m-bq)P_\infty - \textstyle\sum_{j \in S''} P_j\right) &= \ell\left((m-bq)P_\infty - \textstyle\sum_{j \in S'' \setminus \{i\}} P_j\right) \\ &= \ell\left((m-bq)P_\infty + P_i - \textstyle\sum_{j \in S''} P_j\right). \end{aligned}$$

According to Equation (4), this implies $t = 0$ or

$$\max\left\{\left\lfloor \frac{m-bq}{q+1} \right\rfloor - t + 1, 0\right\} = \max\left\{\left\lfloor \frac{m-bq}{q+1} \right\rfloor - t + 2, 0\right\}.$$

Thus, $t = 0$ or $\left\lfloor \frac{m-bq}{q+1} \right\rfloor + 2 \leqslant t$. □

Next, we find some noncollinear stopping sets of certain Hermitian codes. Here, the stopping sets are consist of all columns corresponding to points with $x = \alpha_i$ for b values $\alpha_1, \ldots, \alpha_b \in \mathbb{F}_{q^2}$ along with all columns corresponding to points with $y = \beta_i$ for t values $\beta_1, \ldots, \beta_t \in \mathbb{F}_{q^2}$, provided $b \leqslant q^2 - q$. One may think of the stopping set as consisting of b sets of columns that are collinear in x and t sets of columns that are collinear in y. This is made precise in the following argument.

Theorem 3.3. *Let b and t be nonnegative integers with $1 \leqslant t \leqslant q-1$. If $0 \leqslant b - t \leqslant q^2 - q$, then there exists a stopping set of the Hermitian code $C_\Omega(D, mP_\infty)$ over $\mathbb{F}_{q^2}$ of size $bq + t$ where $m - 2g + 2 \leqslant bq + t \leqslant m + 1$ for any choice of parity-check matrix.*

Proof. Write $bq + t = (b-t)q + t(q+1)$. Label the elements of $\mathbb{F}_{q^2}$ so that $\alpha_0 = 0$,

$$\alpha_i^{q+1} = \cdots = \alpha_{(i-1)(q+1)+j}^{q+1}$$

for $1 \leqslant i \leqslant q-2$ and $1 \leqslant j \leqslant q+1$, $L_{\beta_i} = \left\{\alpha_{(i-1)(q+1)+j} : 1 \leqslant j \leqslant q+1\right\}$, and

$$\mathbb{F}_{q^2} = \dot{\cup}_{i=0}^{q-1} L_{\beta_i};$$

that is, the sets $L_0, L_{\beta_1}, \ldots, L_{\beta_{q-2}}$ form a partition of $\mathbb{F}_{q^2}$. Let

$$S = \left(\cup_{s=0}^{b-t-1} \left(\cup_{\beta \in K_{\alpha_s}} P_{\alpha_s \beta}\right)\right) \cup \left(\cup_{s=1}^{t} \left(\cup_{\alpha \in L_{\beta_s}} P_{\alpha \beta_s}\right)\right).$$

Then $|S| = bq + t$. We claim that S is a stopping set of $\Gamma(H)$.

Define

$$h := \left(\prod_{s=0}^{b-t-1}(x-\alpha_s)\right)\cdot\left(\prod_{s=1}^{t}(y-\beta_s)\right).$$

Observe that if $b=t$, $h=\left(\prod_{s=1}^{t}(y-\beta_s)\right)$; if $t=0$, then $h=\left(\prod_{s=0}^{b-t-1}(x-\alpha_s)\right)$. Then

$$\operatorname{supp}\left(\prod_{s=0}^{b-t-1}(x-\alpha_s)\right)\cap\operatorname{supp}\left(\prod_{s=1}^{t}(y-\beta_s)\right)=\emptyset$$

by construction. In fact,

$$(h)=\sum_{s=0}^{b-t-1}\left(\sum_{\beta\in K_{\alpha_s}}P_{\alpha_s\beta}\right)+\sum_{s=1}^{t}\left(\sum_{\alpha\in L_{\beta_s}}P_{\alpha\beta_s}\right)-\left((b-t)q+t(q+1)\right)P_\infty.$$

To demonstrate that h satisfies the conditions of Lemma 2.4, we write

$$(h)=\sum_{j\in S}P_j+(2g-2)P_\infty-mP_\infty-M$$

where $K=(2g-2)P_\infty$ and $M=\left((b-t)q+t(q+1)+(2g-2)-m\right)P_\infty$. Then M is an effective divisor as $m-(2g-2)\leqslant bq+t$. By Lemma 2.4, S is a stopping set of $\Gamma(H)$. □

Theorem 3.2 proves that if a is a multiple of q, then $C_\Omega(D,mP_\infty)$ has a stopping set of size a. In the next result, consider stopping sets of size $a\equiv 1 \mod q$. Here, we assume that m is a multiple of q. The stopping sets described here consist of

- all columns corresponding to points with $x=\alpha$ for $b-1$ values $\alpha\in\{\alpha_1,\ldots,\alpha_{b-1}\}\subseteq\mathbb{F}_{q^2}$ together with
- all but one column corresponding to points with $x=\alpha_b\in\mathbb{F}_{q^2}\setminus\{\alpha_1,\ldots,\alpha_{b-1}\}$ and
- two columns corresponding to points with $x=\alpha_{b+1}\in\mathbb{F}_{q^2}\setminus\{\alpha_1,\ldots,\alpha_b\}$.

This is made precise in the next argument.

Theorem 3.4. *Consider $C_\Omega(D,mP_\infty)$ over $\mathbb{F}_{q^2}$. Then there exists a stopping set of size $m+1$ if m is multiple of q and any choice of parity-check matrix.*

Proof. Let $C=C_\Omega(D,mP_\infty)$ and $m=bq$ for $0\leqslant b<q^2$. Let $S'=\cup_{s=1}^{b-1}\{P_{\alpha_s,\beta}\mid\beta\in K_{\alpha_s}\}$, and let $S''=\{P_1,\ldots,P_{q-1}\}$ such that $P_j\in\{P_{\alpha',\beta}\in\mathbb{P}_F\mid\beta\in K_{\alpha'}\}$ for some $\alpha'\in\mathbb{F}_{q^2}$ such that $\alpha'\notin\{\alpha_1,\alpha_2,\ldots,\alpha_{b-1}\}$. Let $S=S'\cup S''\cup\{P,Q\}$, where $P,Q\in\{P_{\alpha'',\beta}\in\mathbb{P}_F\mid\beta\in K_{\alpha''}\}$ for some $\alpha''\in\mathbb{F}_{q^2}$ such that $\alpha''\notin\{\alpha_1,\alpha_2,\ldots,\alpha_{b-1},\alpha'\}$. Notice the size of S is $m+1$.

Observe that $\ell\left(mP_\infty-\sum_{j\in S}P_j\right)=\ell\left(R-P-Q\right)$ where $K_{\alpha'}=S''\cup\{R\}$. To see this, consider $f\in\mathcal{L}\left(mP_\infty-\sum_{j\in S}P_j\right)$. Then $(f)\geqslant\sum_{j\in S}P_j-mP_\infty$. Hence, since $m=bq$,

$$\left(f\left(\frac{1}{x-\alpha'}\right)\prod_{s=1}^{b-1}\frac{1}{x-\alpha_s}\right)\geqslant -R+P+Q-mP_\infty+bqP_\infty=-R+P+Q.$$

To find $\ell\left(mP_\infty-\sum_{j\in S\setminus i}P_j\right)$, there are three cases to consider: $P_i\in S'$, $P_i\in S''$, or $P_i=P$ or Q.

Case 1: Suppose $P_i \in S'$. Then $\ell\left(mP_\infty - \sum_{j\in S\setminus\{i\}} P_j\right) = \ell(R + P_i - P - Q)$ since if $f \in \mathcal{L}\left(mP_\infty - \sum_{j\in S} P_j\right)$, then

$$\left(f\left(\frac{1}{x-\alpha'}\right)\prod_{s=1}^{b-1}\frac{1}{x-\alpha_s}\right) \geqslant -R - P_i + P + Q.$$

Case 2: Suppose $P_i \in S''$. Using the same techniques as above, $\ell\left(mP_\infty - \sum_{j\in S\setminus\{i\}} P_j\right) = \ell(R + P_i - P - Q)$.

Case 3: Suppose $P_i \in \{P, Q\}$. Then, as above, $\ell\left(mP_\infty - \sum_{j\in S\setminus\{i\}} P_j\right) = \ell(R - Q)$ or $\ell\left(mP_\infty - \sum_{j\in S\setminus\{i\}} P_j\right) = \ell(R - P)$.

Putting this all together, we see that $\ell\left(mP_\infty - \sum_{j\in S} P_j\right) = \ell\left(mP_\infty - \sum_{j\in S\setminus\{i\}} P_j\right)$ if and only if

$$\ell\left(R - P - Q\right) = \ell(R + P_i - P - Q) = \ell(R - P).$$

Clearly, $\mathcal{L}\left(R - P - Q\right) = \{0\}$ as $\deg(R - P - Q) = -1$. Because $1 \notin H(P) = \langle q, q+1\rangle$, $\mathcal{L}(R - P) = \{0\}$. Similarly, $\mathcal{L}\left(R + P_i - P - Q\right) = \{0\}$ as $\beta_1 > 1$. Thus, S is a stopping set of $\Gamma(H)$ of size $m + 1$ by Lemma 2.2. □

Theorem 3.5. *Consider the Hermitian code $C = C_\Omega(D, mP_\infty)$ over $\mathbb{F}_{q^2}$. If $2(q^2 - q - 1) \leqslant m \leqslant q^3 - q^2 + 2q - 1$, then there exists a stopping set of $\Gamma(H)$ of size a for all $a \in [m - 2g + 2, m + 1]$ for any choice of parity-check matrix H.*

Proof. Let $2(q^2 - q - 1) \leqslant m \leqslant q^3 - q^2 + 2q - 1$ and $a \in [m - 2g + 2, m + 1]$. Write $a = bq + t$ with $0 \leqslant t \leqslant q - 1$. If $t = 0$, then there exists a stopping set of cardinality a by Theorem 3.2. Hence, we assume $1 \leqslant t \leqslant q - 1$ in the rest of the argument. If $0 \leqslant b - t \leqslant q^2 - q$, then then there exists a collinear stopping set of cardinality a by Theorem 3.3. Suppose $b - t < 0$ or $q^2 - q < b - t$. If $b - t < 0$, then

$$\begin{aligned} a &= bq + t \\ &= (b - t)q + t(q + 1) \\ &\leqslant -q + t(q + 1) \text{ since } b - q \leqslant -1 \\ &\leqslant -q + (q - 1)(q + 1) \text{ since } t \leqslant q - 1 \\ &= q^2 - q - 1. \end{aligned}$$

However, this is a contradiction, since

$$a \geqslant m - 2g + 2 \geqslant (2q^2 - 2q - 2) - 2g + 2 = q^2 - q.$$

Similarly, if $q^2 - q < b - t$, then

$$a = bq + t = (b - t)q + t(q + 1) \geqslant (q^2 - q + 1)q + t(q + 1) \geqslant q^3 - q^2 + q + (q + 1) = q^3 - q^2 + 2q + 1.$$

However,

$$a \leqslant m + 1 \leqslant q^3 - q^2 + 2q - 1 + 1 = q^3 - q^2 + 2q.$$

Therefore, $0 \leqslant b - t \leqslant q^2 - q$ and there exists a stopping set of size a according to Theorem 3.3. □

Next, we consider small values of m, meaning $2g-1 \leqslant m \leqslant 2(2g-1)$.

Theorem 3.6. *Consider the Hermitian code $C = C_\Omega(D, mP_\infty)$ over $\mathbb{F}_{q^2}$ where $q^2-q-1 \leqslant m \leqslant 2q^2-2q-3$. Then there exists a stopping set of $\Gamma(H)$ of size a for all $a \in [2g, m+1]$ for any choice of parity-check matrix H of C. In addition, there exists a stopping set of $\Gamma(H)$ of size a for all $a \in [m-2g+2, 2g-1] \cap \langle q, q+1\rangle$ for any choice of parity-check matrix H of C.*

Proof. Let $m = 2q^2-2q-3$, and consider $a \in [2g, m+1]$. Write $a = bq+t$ where $b, t \in \mathbb{Z}$ with $0 \leqslant t \leqslant q-1$. If $t = 0$, then there exists a stopping set of size a by Theorem 3.2. Note that $b \geqslant t$; otherwise, $a = bq+t \leqslant (q-2)q+q-1 < 2g-1$ which contradicts $a \geqslant m-2g+3 = q^2-q$. One may also observe that $b-t \leqslant q^2-q$. Indeed, if $b-t > q^2-q$, then

$$q^3-q^2+q+t(q+1) \leqslant (b-t)q+t(q+1) = a \leqslant m+1 \leqslant 2q^2-2q-2$$

which is a contradiction. According to Theorem 3.3, there exists a stopping set S of $\Gamma(H)$ of size a. Now by Proposition 2.5, if $q^2-q-1 \leqslant m' \leqslant m$, then S is a stopping set of $\Gamma(H')$ where H' is any parity-check matrix of $C = C_\Omega(D, m'P_\infty)$.

Again let $m = 2q^2-2q-3$, and now consider $a \in [m-2g+2, 2g-1] \cap \langle q, q+1\rangle$ As above, write $a = bq+t$ where $b, t \in \mathbb{Z}$ with $0 \leqslant t \leqslant q-1$. If $t = 0$, then there exists a stopping set of C of size a by Theorem 3.2. Thus, we may assume $1 \leqslant t \leqslant q-1$. If $b-t \geqslant q^2-q+1$, then

$$q^3-q^2+2q+1 \leqslant (b-t)q+t(q+1) = a \leqslant 2g-1 = q^2-q-1$$

which is a contradiction as above. Now suppose that $b-t < 0$. It follows that $t = q-1$ as

$$q^2-q-1 = m-2g+2 \leqslant a = (b-t)q+t(q+1) \leqslant -q+t(q+1).$$

Then $b \leqslant q-2$. However, according to [19, Lemma 1] (see also [16, Proposition 2.5]), this implies $b \notin \langle q, q+1\rangle$. Thus, we conclude that the hypotheses of Theorem 3.3 apply and there exists a stopping set S of $C_\Omega(D, mP_\infty)$ of size a. Now by Proposition 2.5, if $q^2-q-1 \leqslant m' \leqslant m$, then S is a stopping set of $\Gamma(H')$ where H' is any parity-check matrix of $C = C_\Omega(D, m'P_\infty)$. □

Notice that in the previous result, we found stopping sets of size a for semigroup elements $a \in \langle q, q+1\rangle$, meaning elements of the gap set of $H(P)$ where P is a rational place of F. Next, we consider $a \in \mathbb{N} \setminus \langle q, q+1\rangle$. As the next two results show, whether or not $C_\Omega(D, mP_\infty)$ has a stopping set of size a depends on both a and m.

Theorem 3.7. *Consider the Hermitian code $C = C_\Omega(D, mP_\infty)$ over $\mathbb{F}_{q^2}$ where $q^2-q-1 \leqslant m \leqslant 2q^2-2q-3$ and $m = 2q^2-2q-(2k+i-3)q-k-1$ for some $0 \leqslant i \leqslant q-k-1$ and $2 \leqslant k \leqslant q$. Then there exists a stopping set of $\Gamma(H)$ of size a for all $a = (q-k-i)q+q-k+1$, for any choice of parity-check matrix H of C.*

Proof. Let $a = (q-k-i)q+q-k+1$ and $m = 2q^2-2q-(2k+i-3)q-k+1$ where $0 \leqslant i \leqslant q-k-1$ and $2 \leqslant k \leqslant q$. Because $m-(q-k-i)q = (q+1)(q-k-1)+q$,

$$\left\lfloor \frac{m-(q-k-i)q}{q+1} \right\rfloor + 2 = (q-k-1)+2 = q-k+1.$$

Hence, Theorem 3.2 applies and C has a stopping set of size a for all $2g-1 \leqslant m' \leqslant m$ by Proposition 2.5. □

Theorem 3.8. *Consider the Hermitian code $C = C_\Omega(D, mP_\infty)$ over $\mathbb{F}_{q^2}$ with parity-check matrix H. If $1 \leqslant a \leqslant q-1$, then there are no stopping sets of $\Gamma(H^*)$ size a for any m. If $a \in \mathbb{N} \setminus \langle q, q+1\rangle$ and $m \in [a+2g-3, a+2g-2]$, then there is no stopping set of $\Gamma(H)$ of size a.*

Proof. Let $C = C_\Omega(D, mP_\infty)$ and $1 \leqslant a \leqslant q-1$. Suppose there exists a stopping set of $\Gamma(H^*)$ of size a. By Lemma 2.4, there exists a function $h \in F$ with $(h) = K + \sum_{j\in S} P_j - mP_\infty - M$ for some canonical divisor K and effective divisor M of F. Since any two canonical divisors of F are linearly equivalent, we may assume that $K = (2g-2)P_\infty$. Then

$$\left(h^{-1}\right) = M + (m-(2g-2))P_\infty - \sum_{j\in S} P_j.$$

It follows that there exist $\{i_1, \ldots, i_s\} \subseteq S$ such that

$$(1, \ldots, 1) \in H(P_{i_1}, \ldots, P_{i_s}).$$

This is a contradiction to Equation (2), as $s \leqslant a \leqslant q-1$. Hence, $\Gamma(H^*)$ has no stopping set of size a.

Let $m = a+2g-3$, and assume $a \in \mathbb{N}\setminus\langle q, q+1\rangle$. Express a as $a = bq+t$ with $0 \leqslant t \leqslant q-1$. Then $0 \leqslant b \leqslant t-1 \leqslant q-2$, since otherwise $a = (b-t)q + t(q+1) \in \langle q, q+q\rangle$. Suppose there exists a stopping set of $\Gamma(H)$ of size a. According to Lemma 2.4, there exists a function h such that

$$(h) = K + \sum_{j\in S} P_j - mP_\infty - M$$

for some canonical divisor K and effective divisor M with $P_j \notin \mathrm{supp} F$ for all $j \in S$. Using the fact that any two canonical divisors are linearly equivalent, we may assume $K = (2g-2)P_\infty$. Observe that $\deg M = (2g-2)+|S|-m = (2g-2)+a-(a+2g-3) = 1$. Hence, M is a place of degree one. Observe that $(h) = \sum_{j\in S} P_j - M - (a-1)P_\infty$ implies $(1, a-1) \in H(M, P_\infty)$. Consequently, $a-1 \geqslant \beta_1 = q^2-q-1$, so $a \geqslant q^2-q$. Recall that the Frobenius number of $\langle q, q+1\rangle$ is $q(q+1)-q-(q+1) = q^2-q-1$, meaning every integer greater than q^2-q-1 is an element of $\langle q, q+1\rangle$. This yields a contradiction as $a \notin \langle q, q+1\rangle$. Therefore, no such stopping set exists.

The result holds for $m = a+2g-2$ by Proposition 2.5.

□

We will now consider the existence of stopping sets for large values of m; that is, $q^3-q^2+2q \leqslant m \leqslant q^3-1$.

Theorem 3.9. *Let $q^3-q^2+2q \leqslant m \leqslant q^3-1$, and set $a = m-2g+2$. Then $C_\Omega(D, m'P_\infty)$ has a stopping set of size a for all $q^3-q^2+2q \leqslant m' \leqslant m$ for any choice of parity-check matrix.*

Proof. Let $m = q^3-q^2+2q+s$, where $0 \leqslant s \leqslant q^2-2q-1$, and

$$a = m-2g+2 = q^3-2q^2+3q+s+2.$$

Write $a = bq + t$ where $0 \leqslant t \leqslant q-1$. If $t = 0$, then there exists a stopping set of size a by Theorem 3.2. Thus, we may assume $1 \leqslant t \leqslant q-1$. Notice that $b = q^2 - 2q + 3 + i$ and $t = s + 2 - iq$, where $0 \leqslant s + 2 - iq \leqslant q - 1$. Then

$$b - t = q^2 - 2q + 3 + i - (s + 2 - iq) \geqslant q^2 - 2q + 3 - (q-1) \geqslant 0.$$

Furthermore,

$$b - t = q^2 - 2q + 3 + i - t \leqslant q^2 - 2q + 3 + i - 1 \leqslant q^2 - q$$

since $i \leqslant q-2$. By Theorem 3.3, $C_\Omega(D, mP_\infty)$ has stopping set of size $a = m - 2g + 2$ for $q^3 - q^2 + 2q \leqslant m \leqslant q^3 - 1$. Applying Proposition 2.5, we conclude that $C_\Omega(D, m'P_\infty)$ has stopping set of size $a = m - 2g + 2$ for $q^3 - q^2 + 2q \leqslant m' \leqslant m$. □

Theorem 3.10. *Let $a = q^3 - q^2 + q + cq + d$ where $1 \leqslant cq + d \leqslant q^2 - q$ and $0 \leqslant d \leqslant q-1$. If $d = 0$, $q \leqslant c + d$, or $c + 1 \leqslant d$, then $C_\Omega(D, mP_\infty)$ has a stopping set of size a for all $q^3 - q^2 + 2q \leqslant m \leqslant q^3 - 1$ with $m - 2g + 2 \leqslant a \leqslant m + 1$ for any choice of parity-check matrix.*

Proof. Let $a = q^3 - q^2 + q + cq + d$ where $1 \leqslant cq + d \leqslant q^2 - 1$ and $0 \leqslant d \leqslant q-1$, and let $C = C_\Omega(D, mP_\infty)$ where $m = q^3 - 1$. Fix a parity-check matrix H for C. If $d = 0$, then $\Gamma(H)$ has a stopping set of size a. Thus, in the following, we assume $1 \leqslant d \leqslant q-1$. Notice that this implies $c \leqslant q-2$; otherwise $cq + d \geqslant (q-1)q + d \geqslant q^2 - q + 1$.

Suppose $q \leqslant c + d$. Since

$$\left\lfloor \frac{m - (q^3 - q^2 + q + cq)}{q+1} \right\rfloor + 2 \leqslant \left\lfloor \frac{(q+1)(q - (c+2)) + q - 1}{q+1} \right\rfloor + 2 = q - c \leqslant d,$$

Theorem 3.2 applies. Thus, $\Gamma(H)$ has a stopping set of size a.

Now assume that $c + 1 \leqslant d$. Expressing a as $a = bq + t$ with $0 \leqslant t \leqslant q-1$, we see that $b = q^2 - q + 1 + c$ and $d = t$. Clearly, $b \geqslant t$. Furthermore, $b - t = q^2 - q + 1 + c - d \leqslant q^2 - q + d - d = q^2 - q$. Consequently, Theorem 3.3 applies and $\Gamma(H)$ has a stopping set of size a.

The result for $m \leqslant q^3 - 1$ follows immediately from Proposition 2.5. □

Corollary 3.11. *Let $q^3 - q^2 + 2q \leqslant m \leqslant q^3 - 1$. Then $C_\Omega(D, mP_\infty)$ has a stopping set of size a for all $m - 2g + 2 \leqslant a \leqslant q^3 - q^2 + 2q$ for any choice of parity-check matrix.*

Proof. This result follows immediately from Theorem 3.9 and Theorem 3.10. □

4. Examples

In this section, we consider codes $C_m := C_\Omega(D, mP_\infty)$ on the Hermitian function field $\mathbb{F}_{q^2}(x, y)$ with $y^q + y = x^{q+1}$ for small values of q.

Example 1. Consider the function field $F = \mathbb{F}_{16}(x, y)$ where $y^4 + y = x^5$; that is, let F be the Hermitian function field with $q = 4$. The genus of F is $g = 6$, and we consider codes C_m with $11 \leqslant m \leqslant 63$. As we detail now, the results presented in Section 3 determine the existence (or nonexistence) of stopping sets of strongly algebraic geometric codes C_m of size a for almost all pairs (m, a).

For $11 \leqslant m \leqslant 21$, Theorem 3.6 guarantees the existence of a stopping set of size a for all $a \in [12, m+1]$ and for all $a \in [m-10, 11] \cap \{4, 5, 8, 9, 10\}$. According to Theorem 3.8, there

are no stopping sets of sizes 1, 2, or 3. Theorem 3.8 also shows that the codes C_{15} and C_{16} have no stopping sets of size 6, C_{16} and C_{17} have no stopping sets of size 7, and C_{20} and C_{21} have no stopping sets of size 11. Stopping sets of sizes 6, 7, and 11 exist for the C_m with $m \leqslant 12$, $m \leqslant 13$, and $m \leqslant 17$, respectively, according to Theorem 3.7. Using SAGE [21], one may find stopping sets of size 6 for C_{13}. By Theorem 3.5, for $22 \leqslant m \leqslant 55$, there exists a stopping set of C_m of size a for all $a \in [m - 2g + 2, m + 1]$. For $56 \leqslant m \leqslant 63$, C_m has a stopping set of size a for all $a \in [m - 2g + 2, 56]$ by Corollary 3.11. By Theorem 3.10, there exists a stopping set of C_m of size 59 for $58 \leqslant m \leqslant 63$, of size 60 for $59 \leqslant m \leqslant 63$, of size 62 for $61 \leqslant m \leqslant 63$, of size 63 for $62 \leqslant m \leqslant 63$, and of size 64 for $m = 63$. For $57 \leqslant m \leqslant 60$, there exists a stopping set of C_m of size 58 by Theorem 3.2. In addition, by Theorem 3.4, stopping sets of sizes 57 and 61 exist for the C_m with $m = 56$ and $m = 60$, respectively. One may find stopping sets using SAGE [21] of C_m of size 57 for $57 \leqslant m \leqslant 61$, of size 58 for $61 \leqslant m \leqslant 62$, and of size 61 for $61 \leqslant m \leqslant 63$.

It remains to determine whether stopping sets of C_m of size a exist for the following pairs (m, a): $(14, 6), (14, 7), (15, 7), (18, 11), (19, 11), (62, 57), (63, 57), (63, 58)$.

Example 2. Consider the function field $F = \mathbb{F}_{25}(x, y)$ where $y^5 + y = x^6$; that is, let F be the Hermitian function field with $q = 5$. The genus of F is $g = 10$, and we consider the strongly algebraic geometric codes C_m on F, meaning those with $19 \leqslant m \leqslant 124$.

For $38 \leqslant m \leqslant 111$, there exist stopping sets of every size $a \in [m - 18, m + 1]$, according to Theorem 3.5. By Theorem 3.6, for $19 \leqslant m \leqslant 37$, there exist stopping sets of sizes $a \in [20, m + 1]$ as well as of sizes $a \in [m - 18, 19] \cap \{5, 6, 10, 11, 12, 15, 16, 17, 18\}$. From Theorem 3.8 we see that there are no stopping sets of sizes 1, 2, 3, or 4. Theorem 3.8 also shows that the codes C_{24} and C_{25} have no stopping sets of size 7; C_{25} and C_{26} have no stopping sets of size 8; and C_{26} and C_{27} have no stopping sets of size 9; C_{30} and C_{31} have no stopping sets of size 13; C_{31} and C_{32} have no stopping sets of size 14; and C_{36} and C_{37} have no stopping sets of size 19. By Theorem 3.7, C_m has a stopping set of size 9, for $19 \leqslant m \leqslant 22$, of size 13 for $19 \leqslant m \leqslant 23$, of size 14 for $19 \leqslant m \leqslant 27$, and of size 19 for $19 \leqslant m \leqslant 32$. Using SAGE [21], one may find stopping sets of C_m of size 8 for $19 \leqslant m \leqslant 22$ and of size 13 for $22 \leqslant m \leqslant 27$. By Corollary3.11, C_m has a stopping set of size a for $110 \leqslant m \leqslant 124$ of size $m - 2q + 1 \leqslant a \leqslant 110$. By Theorem 3.10, there exists a stopping set of C_m of size 112 for $111 \leqslant m \leqslant 124$, of size 113 for $112 \leqslant m \leqslant 124$, of size 114 for $113 \leqslant m \leqslant 124$, of size 115 for $114 \leqslant m \leqslant 124$, of size 118 for $117 \leqslant m \leqslant 124$, of size 119 for $118 \leqslant m \leqslant 124$, of size 120 for $119 \leqslant m \leqslant 124$, of size 122 for $121 \leqslant m \leqslant 124$, of size 123 for $122 \leqslant m \leqslant 124$, of size 124 for $124 \leqslant m \leqslant 124$, and of size 125 for $m = 124$. By Theorem 3.2, there exists a stopping set of C_m of size 117 for $116 \leqslant 120$. By Theorem 3.4, stopping sets of sizes 111, 116 and 121 exist for the C_m with $m = 110$, $m = 115$ and $m = 120$, respectively. In addition, using SAGE [21], one may find stopping sets of C_m of size 111 for $111 \leqslant m \leqslant 121$, of size 116 for $116 \leqslant m \leqslant 124$, of size 117 for $121 \leqslant m \leqslant 124$, and of size 121 for $121 \leqslant m \leqslant 124$.

It remains to determine if C_m has a stopping set of size 7 for $19 \leqslant m \leqslant 23$, of size 8 for $23 \leqslant m \leqslant 24$, of size 9 for $23 \leqslant m \leqslant 25$, of size 13 for $28 \leqslant m \leqslant 29$, of size 14 for $28 \leqslant m \leqslant 30$, of size 19 for $33 \leqslant m \leqslant 35$, and of size 111 for $122 \leqslant m \leqslant 124$.

5. Conclusion

In this paper, we study stopping sets of Hermitian codes, $C = C_\Omega(D, mP_\infty)$. If $(q^2 - q - 1) \leqslant m \leqslant q^3 - q^2 + 2q - 1$, we prove that a stopping set of size a exists for $m - 2g + 2 \leqslant a \leqslant q^3$ for any choice of parity-check matrix. For $2(q^2 - q - 1) \leqslant m \leqslant q^3 - q^2 + 2q - 1$, we have completely determined if $\Gamma(H^*)$ has stopping set of any size. For small and large values of m, meaning m satisfying $2g - 1 \leqslant m \leqslant 2(2g - 1)$ or $q^3 - q^2 + 2q \leqslant m \leqslant q^3 - 1$, we find stoppings sets for certain m and a values for any choice of parity-check matrix. In addition, for specific small m and a values, we have shown stopping sets do not exist.

References

[1] K. Abdel-Ghaffar and J. Weber, Complete enumeration of stopping sets of full-rank parity-check matrices of Hamming codes, IEEE Trans. Inform. Theory 53 (2007), no. 9, 3196-3201.

[2] E. Ballico, On the Weierstrass semigroups of n points of a smooth curve, Arch. Math. 104 (2015), 207-215.

[3] J. Bolkema, K. Morrison, and J. L. Walker, Graph Realizations of Polar Codes, preprint.

[4] R. Carrasco and M. Johnston, *Non-Binary Error Control Coding for Wireless Communication and Data Storage*, Wiley, 2009.

[5] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson, and R. L. Urbanke, Finite-length analysis of low-density parity-check codes on the binary erasure channel, IEEE Trans. Inform. Theory 48 (2002), no. 6, 1570-1579.

[6] A. Eslami and H. Pishro-Nik, On Finite-Length Performance of Polar Codes: Stopping Sets, Error Floor, and Concatenated Design, IEEE Trans. Comm. 61 (2013), no. 3, 919–929.

[7] M. Esmaeili and M. Amoshahy, On the stopping distance of array code parity-check matrices, IEEE Trans. Inform. Theory 55 (2009), no. 8, 3488-3493

[8] M. Esmaeili, M. Tadayon, and T. Gulliver, More on the stopping and minimum distances of array codes, IEEE Trans. Commun. 59 (2011), no. 3, 750-757.

[9] T. Etzion, On the stopping redundancy of Reed-Muller codes, IEEE Trans. Inform. Theory 52 (2006), no. 11, 4867–4879.

[10] V. Guruswami and M. Sudan, Improved decoding of Reed-Solomon and algebraic-geometry codes, IEEE Trans. Inform. Theory 45 (1999), no. 6, 17571767.

[11] M. Homma and S. J. Kim, Goppa Codes with Weierstrass Pairs, J. Pure Appl. Algebra 162 (2001), no. 2, 273–290.

[12] Y. Jiang, S.-T. Xia, F.-W. Fu, Stopping Set Distributions of Some Reed-Muller Codes, IEEE Trans. Inform. Theory 57 (2011), no. 9, 6078–6088..

[13] C. Kelley and D. Sridhara, Pseudocodewords of Tanner graphs, IEEE Trans. Inform. Theory **53** (2007), no. 11, 4013–4038.

[14] K. Lee and M. E. OSullivan, Algebraic Soft-Decision Decoding of Hermitian Codes, IEEE Trans. on Inform. Theory 56 (2010), no 6, 2587 2600.

[15] H. Maharaj, G. Matthews, and G. Pirsic, Riemann-Roch spaces of the Hermitian function field with applications to algebraic-geometric codes and low-discrepancy sequences, J. Pure Appl. Algebra 195 (2005), no. 3, 261–280.

[16] G. L. Matthews, On numerical semigroups generated by generalized arithmetic sequences, Comm. Algebra 32 (2004), no. 9, 3459–3469.

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

[18] R. Pellikaan, B.-Z. Shen, and G. J. M. van Wee, Which linear codes are algebraic-geometric? IEEE Trans. Inform. Theory 37 (1991), no. 3, part 1, 583–602.

[19] J. B. Roberts, Note on linear forms. Proc. Amer. Math. Soc. 7 (1956), 465–469.

[20] M. Schwartz and A. Vardy, On the stopping distance and the stop- ping redundancy of codes, IEEE Trans. Inform. Theory 52 (2006), no. 3, 922–932.

[21] W.A. Stein et al. Sage Mathematics Software (Version 5.11), The Sage Development Team, 2014, http://www.sagemath.org.
[22] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.
[23] B. E. Whalen and J. Jimenez, Performance comparison of Hermitian and ReedSolomon codes, Proc. 1997 IEEE Military Communications Conf. 1 (1997), 15 - 19.
[24] J. Zhang, F.-W. Fu, and D. Wan, Stopping sets of algebraic geometry codes, IEEE Trans. Inform. Theory 60 (2014), no. 3, 1488-1495.