Stopping Sets of Algebraic Geometry Codes

Jun Zhang, Fang-Wei Fu, and Daqing Wan

***Abstract*— Stopping sets and stopping set distribution of a linear code play an important role in the performance analysis of iterative decoding for this linear code. Let C be an $[n, k]$ linear code over $\mathbb{F}_q$ with parity-check matrix H, where the rows of H may be dependent. Let $[n] = \{1, 2, \ldots, n\}$ denote the set of column indices of H. A *stopping set* S of 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. The *stopping set distribution* $\{T_i(H)\}_{i=0}^{n}$ enumerates the number of stopping sets with size i of C with parity-check matrix H. Denote H^*, the parity-check matrix, consisting of all the nonzero codewords in the dual code $C^{\perp}$. In this paper, we study stopping sets and stopping set distributions of some residue algebraic geometry (AG) codes with parity-check matrix H^*. First, we give two descriptions of stopping sets of residue AG codes. For the simplest AG codes, i.e., the generalized Reed–Solomon codes, it is easy to determine all the stopping sets. Then, we consider the AG codes from elliptic curves. We use the group structure of rational points of elliptic curves to present a complete characterization of stopping sets. Then, the stopping sets, the stopping set distribution, and the stopping distance of the AG code from an elliptic curve are reduced to the search, counting, and decision versions of the subset sum problem in the group of rational points of the elliptic curve, respectively. Finally, for some special cases, we determine the stopping set distributions of the AG codes from elliptic curves.**

***Index Terms*— Algebraic geometry codes, elliptic curves, stopping distance, stopping sets, stopping set distribution, subset sum problem.**

I. Introduction

Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$ with length n, dimension k and minimum distance d. Let H be a parity-check matrix of C, where the rows of H may be dependent. Let $[n] = \{1, 2, \ldots, n\}$ denote the set of column indices of H. A *stopping set* S of C with parity-check matrix H is a subset of $[n]$ such that the restriction of H to S, say $H(S)$, does not contain a row of weight 1. The *stopping set distribution* $\{T_i(H)\}_{i=0}^{n}$ enumerates the number of stopping sets with size i of C with parity-check matrix H. Note that the empty set $\emptyset$ is defined as a stopping set and $T_0(H) = 1$.

Manuscript received April 25, 2013; revised November 7, 2013; accepted December 16, 2013. Date of publication January 10, 2014; date of current version February 12, 2014. J. Zhang and F.-W. Fu were supported in part by the National Key Basic Research Program of China (973) under Grant 2013CB834204 and in part by the National Natural Science Foundation of China under Grants 61171082, 10990011, and 60872025. This paper was presented at the 2012 Annual Conference on Theory and Applications of Models of Computation.

J. Zhang is with the Chern Institute of Mathematics, Nankai University, Tianjin 300071, China (e-mail: zhangjun04@mail.nankai.edu.cn).

F.-W. Fu is with the Chern Institute of Mathematics, LPMC, Nankai University, Tianjin 300071, China (e-mail: fwfu@nankai.edu.cn).

D. Wan is with the Department of Mathematics, University of California, Irvine, CA 92697 USA (e-mail: dwan@math.uci.edu).

Communicated by N. Kashyap, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2014.2299545

A number of researchers have recently studied the stopping sets and stopping set distributions of linear codes, e.g., see [1]–[27]. Stopping sets and stopping set distribution of a linear code are used to determine the performance of this linear code under iterative decoding [24].

The *stopping distance* $s(H)$ of C with the parity-check matrix H is the minimum size of nonempty stopping sets. It plays an important role in the performance analysis of the iterative decoding, just as the role of the minimum Hamming distance d of a code for maximum-likelihood or algebraic decoding. Analogously to the redundancy of a linear code, Schwartz and Vardy [3] introduced the *stopping redundancy* $\rho(C)$, the minimal number of rows in the parity-check matrix H for the linear code C such that the stopping distance $s(H) = d$, to characterize the minimal "complexity" of the iterative decoding for the code C. The stopping redundancy of some linear codes such as Reed-Muller codes, cyclic codes and maximal distance separable (MDS) codes have been studied recently [3]–[21].

Note that the stopping distance, the stopping sets and stopping set distribution depend on the choice of the parity-check matrix H of C. Recall that H^* is the parity-check matrix consisting of all non-zero codewords in the dual code $C^{\perp}$. For any parity-check matrix H, it is obvious that $T_i(H) \geqslant T_i(H^*)$ for all i, since H is a sub-matrix formed by some rows of H^*. Although the iterative decoding with the parity-check matrix H^* has the highest decoding complexity, it achieves the best possible performance as it has the smallest stopping set distribution. It is known from [11] and [19] that the iterative decoding with the parity-check matrix H^* is an optimal decoding for the binary erasure channel. The stopping set distribution is used to characterize the performance under iterative decoding. So it is important to determine the stopping set distribution of C with the parity-check matrix H^*. However, in general, it is difficult to determine the stopping set distribution of C with the parity-check matrix H^*. Using finite geometry, Jiang *et al.* [8] gave characterizations of stopping sets of some Reed-Muller codes (the Simplex codes, the Hamming codes, the first order Reed-Muller codes and the extended Hamming codes). Furthermore, they determined the stopping set distributions of these codes. Since the iterative decoding with parity-check matrix H^* has the highest decoding complexity, they [8] considered a parity-check matrix H, a submatrix of H^*, such that the stopping set distribution of C with parity-check matrix H is the same as that with H^*, but has the smallest number of rows. Such a parity-check matrix H is called *optimal*. In general, it is difficult to obtain an optimal parity-check matrix for a general linear code. In [8], they obtained optimal parity-check matrices for the Simplex codes, the Hamming codes,

the first order Reed-Muller codes and the extended Hamming codes. They also proposed an interesting problem to determine the stopping set distributions of well known linear codes with the parity-check matrix H^*. In this paper, we consider AG codes and a specific class of AG codes, i.e., AG codes associated with elliptic curves. We study the stopping sets and stopping set distributions of AG codes with the parity-check matrix H^*.

This paper is organized as follows. We first summarize our main results in Section II. In Section III, we study stopping sets of an arbitrary AG code and give algebraic and geometric descriptions of stopping sets. In Section IV, we study the stopping sets and stopping set distributions of AG codes from elliptic curves. We use the group structure of rational points of elliptic curves to present a complete characterization of stopping sets. It is shown that the stopping sets, the stopping set distribution and the stopping distance of the AG code from an elliptic curve can be reduced to the search, counting and decision versions of the subset sum problem in the group of rational points of the elliptic curve, respectively. We present the counting formula for the stopping set distributions of AG codes from elliptic curves. In particular, for some special cases, we determine explicitly the stopping set distributions of AG codes from elliptic curves. Finally, some conclusions and open problems are given in Section V.

II. Main Result

In this section, we summarize our main results in this paper. From now on, we always choose the parity-check matrix H^* for linear codes in this paper. It is well-known that

Proposition 1 ([3]). *Let C be a linear code with minimum distance $d(C)$, and let H^* denote the parity-check matrix for C consisting of all the nonzero codewords of the dual code $C^\perp$. Then the stopping distance $s(H^*) = d(C)$.*

Note that the generalized Reed-Solomon codes are MDS codes. For the $[n, k, d]$ MDS code C, i.e., $d = n - k + 1$, its dual code $C^\perp$ is still an $[n, n-k, k+1]$ MDS code. Since any non-zero codeword in $C^\perp$ has at most $n-k-1$ zeros and any $(n-k)$ positions form an information set, we have

Proposition 2. *Let C be an $[n, k, n-k+1]$ MDS code. Then*

(i) *any subset of $[n]$ with cardinality $\geqslant n-k+1$ is a stopping set;*
(ii) *any non-empty subset of $[n]$ with cardinality $\leqslant n-k$ is not a stopping set.*

By Proposition 2, we obtain the stopping set distribution of MDS codes.

Corollary 3. *Let C be an $[n, k, n-k+1]$ MDS code. Then the stopping set distribution of C is given by*

$$T_i(H^*) = \begin{cases} 1, & \text{if } i = 0, \\ 0, & \text{if } 1 \leqslant i \leqslant n-k, \\ \binom{n}{i}, & \text{if } i \geqslant n-k+1. \end{cases}$$

As a generalization of the generalized Reed-Solomon codes, next we study the stopping sets and stopping set distributions of AG codes. We briefly recall the construction of AG codes.

Constructions of AG Codes.

We fix some notation valid for the entire paper.

- *$X/\mathbb{F}_q$ is a geometrically irreducible smooth projective curve of genus g over the finite field $\mathbb{F}_q$ with function field $\mathbb{F}_q(X)$.*
- *$X(\mathbb{F}_q)$ is the set of all $\mathbb{F}_q$-rational points on X.*
- *$D = \{P_1, P_2, \ldots, P_n\}$ is a proper subset of $X(\mathbb{F}_q)$.*
- *With slight abuse of notation, also write $D = P_1 + P_2 + \cdots + P_n$.*
- *G is a divisor of degree m ($2g - 2 < m < n$) with $\mathrm{Supp}(G) \cap D = \emptyset$.*

Let V be a divisor on X. Denote by $\mathscr{L}(V)$ the $\mathbb{F}_q$-vector space of all rational functions $f \in \mathbb{F}_q(X)$ with the principal divisor $\mathrm{div}(f) \geqslant -V$, together with the zero function. Denote by $\Omega(V)$ the $\mathbb{F}_q$-vector space of all the Weil differentials ω with divisor $\mathrm{div}(\omega) \geqslant V$, together with the zero differential (cf. [28]). For any $\mathbb{F}_q$-rational point P on X, choose one uniformizer t for P. Then for any differential ω, we can write $\omega = udt$ with some $u \in \mathbb{F}_q(X)$. Write the P-adic expansion $u = \sum_{i=i_0}^{\infty} a_i t^i$ for some $i_0 \in \mathbb{Z}$ and $a_i \in \mathbb{F}_q$, the residue map of ω at the point P is defined to be

$$res_P(\omega) = res_{P,t}(u) = a_{-1}.$$

One can show that the above definition is well-defined [28, Proposition 4.2.9].

The residue AG code $C_\Omega(D, G)$ is defined to be the image of the following residue map:

$$\begin{aligned} res : \Omega(G - D) &\to \mathbb{F}_q^n \\ \omega &\mapsto (res_{P_1}(\omega), res_{P_2}(\omega), \ldots, res_{P_n}(\omega)). \end{aligned}$$

Its dual code, the functional AG code $C_{\mathscr{L}}(D, G)$, is defined to be the image of the following evaluation map:

$$ev : \mathscr{L}(G) \to \mathbb{F}_q^n;\ f \mapsto (f(P_1), f(P_2), \ldots, f(P_n)).$$

They are linear codes over $\mathbb{F}_q$, and have the code parameters $[n, n-m+g-1, d \geqslant m-2g+2]$ and $[n, m-g+1, d \geqslant n-m]$, respectively. Moreover they can be represented from each other [28, Proposition 8.1.2]. So in this paper we only consider the residue AG codes.

For the simplest AG codes, i.e., the generalized Reed-Solomon codes, we have determined all the stopping sets. Then we consider the AG codes $C_\Omega(D, G)$ from elliptic curves. In this case, using the Riemann-Roch theorem, the stopping sets can be characterized completely as follows.

Main Theorem. Let E be an elliptic curve over $\mathbb{F}_q$, $D = \{P_1, P_2, \ldots, P_n\}$ a subset of $E(\mathbb{F}_q)$ such that the zero element $O \notin D$ and let $G = mO$ ($0 < m < n$). Recall that the empty set is always considered as a stopping set by convention. The non-empty stopping sets of the residue code $C_\Omega(D, G)$ are given as follows:

(i) Any non-empty subset of $[n]$ with cardinality $\leqslant m-1$ is not a stopping set.
(ii) Any subset of $[n]$ with cardinality $\geqslant m+2$ is a stopping set.

(iii) $A \subseteq [n]$, $|A| = m+1$, is a stopping set if and only if for all $i \in A$, the sum

$$\sum_{j \in A \setminus \{i\}} P_j \neq O.$$

(iv) $A \subseteq [n]$, $|A| = m$, is a stopping set if and only if

$$\sum_{j \in A} P_j = O.$$

(v) Denote by $S(m)$ and $S(m+1)$ the two sets of stopping sets with cardinality m and $m+1$ in the cases (iv) and (iii), respectively. Let

$$S^+(m) = \bigcup_{A \in S(m)} \{A \cup \{i\} : i \in [n] \setminus A\}.$$

Then the union in $S^+(m)$ is a disjoint union, and we have

$$S(m+1) \cap S^+(m) = \emptyset,$$

and

$$S(m+1) = \{\text{subsets of } [n] \text{ with size } m+1\} \setminus S^+(m).$$

The proof will be given in Section III. By this theorem, the stopping set distribution of $C_\Omega(D, G)$ follows immediately.

Theorem 4. *Notation as above. The stopping set distribution of $C_\Omega(D, G)$ with the parity-check matrix H^* is*

$$T_i(H^*) = \begin{cases} 1, & \text{if } i = 0, \\ 0, & \text{if } 1 \leqslant i \leqslant m-1, \\ |S(m)|, & \text{if } i = m, \\ \binom{n}{m+1} - (n-m)|S(m)|, & \text{if } i = m+1, \\ \binom{n}{i}, & \text{if } i \geqslant m+2. \end{cases}$$

Then by Theorem 4, we easily see that the stopping distance of $C_\Omega(D, G)$ is m or $m+1$. But to decide it is equivalent to a decision version of m-subset sum problem [29]–[31] in the group $E(\mathbb{F}_q)$, which is an **NP**-hard problem under **RP**-reduction [32]. Hence to compute the stopping distance of $C_\Omega(D, G)$ is **NP**-hard under **RP**-reduction. To compute the stopping set distribution is a counting version of m-subset sum problem in the group $E(\mathbb{F}_q)$, so it is also an **NP**-hard problem. However, for a special $D \subseteq E(\mathbb{F}_q)$ with strong algebraic structure, it is possible to compute the complete stopping set distribution. For instance, if we take $D = U \setminus \{O\}$, where U is a subgroup of $E(\mathbb{F}_q)$. In particular, in application we always choose $D = E(\mathbb{F}_q) \setminus \{O\}$ to get a long linear code which is called *standard* elliptic code. Denote $N = |U|$ the cardinality of U, $\exp(U)$ the exponent of U, $U[d]$ the d-torsion subgroup of U, and

$$N(m) = \frac{1}{N} \sum_{s \mid \exp(U)} (-1)^{m + \lfloor \frac{m}{s} \rfloor} \binom{N/s - 1}{\lfloor m/s \rfloor} \sum_{d \mid s} \mu(s/d) |U[d]|,$$

respectively. It is known from [30], [31] that $|S(m)| = N(m)$. Hence, we have

Theorem 5. *Let $D = U \setminus \{O\}$, where U is a subgroup of $E(\mathbb{F}_q)$. The stopping set distribution of $C_\Omega(D, G)$ with the parity-check matrix H^* is*

$$T_i(H^*) = \begin{cases} 1, & \text{if } i = 0, \\ 0, & \text{if } 1 \leqslant i \leqslant m-1, \\ N(m), & \text{if } i = m, \\ \binom{n}{m+1} - (n-m)N(m), & \text{if } i = m+1, \\ \binom{n}{i}, & \text{if } i \geqslant m+2. \end{cases}$$

III. Stopping Sets of Algebraic Geometry Codes

Let $X/\mathbb{F}_q$ be a geometrically irreducible smooth projective curve of genus g over the finite field $\mathbb{F}_q$ with function field $\mathbb{F}_q(X)$, and $C_\Omega(D, G)$ the residue AG code from X. In this section, we study stopping sets and stopping set distributions of general residue AG codes and give algebraic and geometric descriptions of the stopping sets of $C_\Omega(D, G)$.

Theorem 6. *A subset $A \subseteq [n]$ is a stopping set of $C_\Omega(D, G)$ if and only if*

$$\mathscr{L}(G - \sum_{j \in A} P_j) = \bigcup_{i \in A} \mathscr{L}(G - \sum_{j \in A \setminus \{i\}} P_j),$$

which is equivalent to

$$\mathscr{L}(G - \sum_{j \in A} P_j) = \mathscr{L}(G - \sum_{j \in A \setminus \{i\}} P_j) \quad \text{for any} \quad i \in A.$$

Proof: By the definition, $A \subseteq [n]$ is not a stopping set of $C_\Omega(D, G)$ if and only if there is some $f \in \mathscr{L}(G)$ such that

$$ev(f)|_A = (f(P_i))_{i \in A}$$

has weight 1. That is, there is some $i \in A$ such that

$$f(P_i) \neq 0 \quad \text{and} \quad f(P_j) = 0 \quad \text{for all} \quad j \in A \setminus \{i\}.$$

This is equivalent to saying that

$$f \in \mathscr{L}(G - \sum_{j \in A \setminus \{i\}} P_j) \setminus \mathscr{L}(G - \sum_{j \in A} P_j).$$

So A is a stopping set if and only if for any $i \in A$,

$$\mathscr{L}(G - \sum_{j \in A} P_j) = \mathscr{L}(G - \sum_{j \in A \setminus \{i\}} P_j).$$

Since $\mathscr{L}(G - \sum_{j \in A} P_j) \subseteq \mathscr{L}(G - \sum_{j \in A \setminus \{i\}} P_j)$ for any $i \in A$, we have

$$\begin{aligned} &\mathscr{L}(G - \textstyle\sum_{j \in A} P_j) = \bigcup_{i \in A} \mathscr{L}(G - \sum_{j \in A \setminus \{i\}} P_j) \\ \iff &\mathscr{L}(G - \textstyle\sum_{j \in A} P_j) = \mathscr{L}(G - \sum_{j \in A \setminus \{i\}} P_j) \ \forall i \in A. \end{aligned}$$

So the theorem holds. ∎

As a simple corollary, we obtain

Corollary 7. (i) *Any subset of $[n]$ with cardinality $\geqslant m+2$ is a stopping set of $C_\Omega(D, G)$.*

(ii) *Any non-empty subset of $[n]$ with cardinality $\leqslant m - 2g + 1$ is not a stopping set of $C_\Omega(D, G)$.*

Proof: (i) For any subset $A \subseteq [n]$ with cardinality $\geqslant m+2$, divisors $G - \sum_{j \in A \setminus \{i\}} P_j$ and $G - \sum_{j \in A} P_j$ are negative. So

$$\mathscr{L}(G - \sum_{j \in A} P_j) = \bigcup_{i \in A} \mathscr{L}(G - \sum_{j \in A \setminus \{i\}} P_j) = \{0\}.$$

It follows from Theorem 6 that A is a stopping set.

(ii) For any non-empty subset $A \subseteq [n]$ with cardinality $\leqslant m - 2g + 1$, by the Riemann-Roch theorem we have

$$\dim(\mathscr{L}(G - \sum_{j\in A} P_j)) = m - |A| - g + 1,$$
$$\dim(\mathscr{L}(G - \sum_{j\in A\setminus\{i\}} P_j)) = m - |A| - g + 2.$$

So

$$\mathscr{L}(G - \sum_{j\in A} P_j) \subsetneq \mathscr{L}(G - \sum_{j\in A\setminus\{i\}} P_j)$$

for all $i \in A$. It follows from Theorem 6 that A is not a stopping set. Note that one can also give another proof of (ii) from Proposition 1, since the minimum distance of $C_\Omega(D, G)$ is at least $m - 2g + 2$. ∎

If we represent the generalized Reed-Solomon codes as AG codes from the rational function field, then by Corollary 7, we also obtain Proposition 2 for the generalized Reed-Solomon codes.

Using the Riemann-Roch theorem, we give another description of stopping sets of AG codes $C_\Omega(D, G)$.

Theorem 8. *A subset $A \subseteq [n]$ is a stopping set of $C_\Omega(D, G)$ if and only if for any $i \in A$, there exists an effective divisor F_i with $P_i \notin \mathrm{Supp}(F_i)$ such that*

$$K - G + \sum_{j\in A} P_j \sim F_i,$$

where K is a canonical divisor on X and $\sim$ means that two divisors are linearly equivalent, i.e., the difference between the two divisors is a principal divisor.

Proof: From the proof of Theorem 6, a subset $A \subseteq [n]$ is a stopping set if and only if for any $i \in A$,

$$\dim \mathscr{L}(G - \sum_{j\in A} P_j) = \dim \mathscr{L}(G - \sum_{j\in A\setminus\{i\}} P_j).$$

The Riemann-Roch theorem states that for any divisor V, we have

$$\dim \mathscr{L}(V) = \deg(V) - g + 1 + \dim \mathscr{L}(K - V).$$

So a subset $A \subseteq [n]$ is a stopping set if and only if for any $i \in A$,

$$\dim \mathscr{L}(K - G + \sum_{j\in A} P_j) = \dim \mathscr{L}(K - G + \sum_{j\in A\setminus\{i\}} P_j) + 1.$$

It is equivalent to that for any $i \in A$, there exists

$$f \in \mathscr{L}(K - G + \sum_{j\in A} P_j) \setminus \mathscr{L}(K - G + \sum_{j\in A\setminus\{i\}} P_j).$$

The last statement is equivalent to that for any $i \in A$, there exists an effective divisor F_i with $P_i \notin \mathrm{Supp}(F_i)$ such that

$$K - G + \sum_{j\in A} P_j \sim F_i.$$

Indeed, $F_i = \mathrm{div}(f) + K - G + \sum_{j\in A} P_j$. ∎

By Theorem 8, we immediately have a sufficient condition for a subset to be a stopping set.

Corollary 9. *Keep notation as above. Let A be a subset of $[n]$. If $K - G + \sum_{j\in A} P_j \sim F$ for some effective divisor F whose support has no intersection with $\{P_i \mid i \in A\}$, then A is a stopping set.*

IV. Stopping Sets and Stopping Set Distributions of AG Codes From Elliptic Curves

In the previous section, for the general AG code $C_\Omega(D, G)$, we have seen that there is a gap, $\deg(G) - 2g + 2 \leqslant i \leqslant \deg(G) + 1$, where in general we have not determined whether a subset with cardinality i is a stopping set or not. Note that there is no gap for the case $g = 0$, i.e., the Reed-Solomon codes. Recall that the case $g = 0$ was done in Section II. We are now moving on to the case $g = 1$, i.e., AG codes constructed from elliptic curves.

Let $X = E$ be an elliptic curve over the finite field $\mathbb{F}_q$ with a rational point O. Endow $E(\mathbb{F}_q)$ a group structure with the zero element O. Let $D = \{P_1, P_2, \ldots, P_n\}$ be a subset of the set $E(\mathbb{F}_q)$ such that $O \notin D$. Let $G = mO$ $(0 < m < n)$.

In general, if G is a divisor of degree m on E, then for any rational point $Q \in E(\mathbb{F}_q)$, as $\deg(G - (m-1)Q) = 1$, by the Riemann-Roch theorem, there exists one and only one rational point $P \in E(\mathbb{F}_q)$ such that $G \sim (m-1)Q + P$. Suppose there exist rational points Q, P such that $G \sim (m-1)Q + P$ and $P, Q \notin D$. Let $G' = (m-1)Q + P$. Then the codes $C_\Omega(D, G)$ and $C_\Omega(D, G')$ are equivalent [28, Proposition 2.2.14]. The dual codes $C_{\mathscr{L}}(D, G)$ and $C_{\mathscr{L}}(D, G')$ are also equivalent. Here two linear codes $C_1, C_2 \subseteq \mathbb{F}_q^n$ are said to be *equivalent*[1] if there is a vector $a = (a_1, \ldots, a_n) \in (\mathbb{F}_q^*)^n$ such that

$$C_2 = a \cdot C_1 = \{(a_1c_1, \ldots, a_nc_n) \mid (c_1, \ldots, c_n) \in C_1\}.$$

It is easy to see that two equivalent codes have the same stopping sets and hence the same stopping set distributions. So to study the stopping sets and the stopping set distribution of $C_\Omega(D, G)$, it suffices to determine all the stopping sets and the stopping set distribution of $C_\Omega(D, (m-1)Q + P)$. In this case, we use Q to define the group $E(\mathbb{F}_q)$ with the zero element Q. Then all results in this paper hold similarly for $C_\Omega(D, G)$ with $G \sim (m-1)Q + P$ such that $P, Q \notin D$.

Note that $g = 1$ for elliptic curves. According to Corollary 7, any subset of $[n]$ with cardinality $\geqslant m + 2$ is a stopping set and any non-empty subset of $[n]$ with cardinality $\leqslant m - 1$ is not a stopping set. So it is enough to consider the subsets of $[n]$ with cardinality m and $m + 1$. Below we use the group $E(\mathbb{F}_q)$ [33], [34] to give a description of these two classes of stopping sets with cardinality $m + 1$ and m, respectively.

(i) Suppose $A \subseteq [n]$ with cardinality $m+1$ is not a stopping set. Then there are some $i \in A$ and $f \in \mathscr{L}(G)$ such that

$$f \in \mathscr{L}(G - \sum_{j\in A\setminus\{i\}} P_j) \setminus \mathscr{L}(G - \sum_{j\in A} P_j).$$

Note that

$$\deg(G - \sum_{j\in A\setminus\{i\}} P_j) = m - m = 0,$$

[1] In general, a fixed permutation of coordinates of codewords is also considered as an equivalence relation of linear codes. In this case, stopping set distribution is not changed under permutation equivalences, but not for stopping sets. More precisely, if linear codes C_1 and C_2 are equivalent under the permutation T, i.e., $T(C_1) = C_2$, then the set S is a stopping set of C_1 if and only if $T(S)$ is a stopping set of C_2.

and

$$\mathrm{div}(f) \geqslant -G + \sum_{j\in A\setminus\{i\}} P_j.$$

Since both sides have degree zero, they have to be equal. That is

$$\mathrm{div}(f) = -G + \sum_{j\in A\setminus\{i\}} P_j = \sum_{j\in A\setminus\{i\}} (P_j - O).$$

In this case, $A \subseteq [n]$, $|A| = m+1$, is not a stopping set if and only if there exists some $i \in A$ such that the sum $\sum_{j\in A\setminus\{i\}} P_j$ in the group $E(\mathbb{F}_q)$ is O.

(ii) Suppose $A \subseteq [n]$ with cardinality m is a stopping set. By Theorem 6, for any $i \in A$, we have

$$\mathscr{L}(G - \sum_{j\in A\setminus\{i\}} P_j) = \mathscr{L}(G - \sum_{j\in A} P_j).$$

Note that

$$\deg(G - \sum_{j\in A\setminus\{i\}} P_j) = 1 \geqslant 2g - 1 = 1.$$

By the Riemann-Roch theorem, there exists some $f \in \mathbb{F}_q(E)$ such that

$$0 \neq f \in \mathscr{L}(G - \sum_{j\in A\setminus\{i\}} P_j) = \mathscr{L}(G - \sum_{j\in A} P_j).$$

So

$$\mathrm{div}(f) = G - \sum_{j\in A} P_j = \sum_{j\in A}(O - P_j).$$

This is equivalent to

$$\sum_{j\in A} P_j = O$$

in the group $E(\mathbb{F}_q)$. Conversely, let $A \subseteq [n]$ with cardinality m such that $\sum_{j\in A} P_j = O$. Since the zero divisor $K = 0$ is a canonical divisor for elliptic curves, we have

$$K - G + \sum_{j\in A} P_j \sim 0.$$

By Corollary 9, A is a stopping set.

From the argument above, we obtain the following partial results of the main theorem in Section II.

Theorem 10. *Let E be an elliptic curve over the finite field $\mathbb{F}_q$, $D = \{P_1, P_2, \ldots, P_n\}$ a subset of $E(\mathbb{F}_q)$ such that the zero element $O \notin D$ and let $G = mO$ $(0 < m < n)$. The non-empty stopping sets of the residue code $C_\Omega(D, G)$ are given as follows:*

(i) *Any subset of $[n]$ with cardinality $\leqslant m-1$ is not a stopping set.*

(ii) *Any subset of $[n]$ with cardinality $\geqslant m+2$ is a stopping set.*

(iii) *$A \subseteq [n]$, $|A| = m+1$, is a stopping set if and only if for all $i \in A$, the sum*

$$\sum_{j\in A\setminus\{i\}} P_j \neq O.$$

(iv) *$A \subseteq [n]$, $|A| = m$, is a stopping set if and only if*

$$\sum_{j\in A} P_j = O.$$

Let us give an example to illustrate the theorem.

Example 11. Let E be the elliptic curve defined over $\mathbb{F}_5$ by the equation

$$y^2 = x^3 + x + 1.$$

Then E has 9 rational points: the infinity point O and $P_1 = (0,1)$, $P_2 = (4,2)$, $P_3 = (2,1)$, $P_4 = (3,4)$, $P_5 = (3,1)$, $P_6 = (2,4)$, $P_7 = (4,3)$, $P_8 = (0,4)$. Using Group Law Algorithm 2.3 in [34], one can check that $E(\mathbb{F}_5)$ forms a cyclic group with $P_i = [i]P_1$. Let $D = \{P_1, P_2, \ldots, P_8\}$ and $G = 3O$.

By Corollary 9 and Theorem 10, all nonempty stopping sets of $C_\Omega(D, G)$ are given as follows:

(i) subsets of $[n]$ with cardinality $\geqslant 5$;

(ii) {1,2,3,7}, {1,2,3,8}, {1,2,4,5}, {1,2,4,7}, {1,2,4,8}, {1,2,5,7}, {1,2,5,8}, {1,2,7,8}, {1,3,4,6}, {1,3,4,7}, {1,3,4,8}, {1,3,6,7}, {1,3,6,8}, {1,4,5,6}, {1,4,5,7}, {1,4,5,8}, {1,4,6,7}, {1,4,7,8}, {1,5,6,8}, {1,5,7,8}, {1,6,7,8}, {2,3,5,6}, {2,3,5,7}, {2,3,5,8}, {2,3,6,7}, {2,3,6,8}, {2,4,5,6}, {2,4,5,7}, {2,4,5,8}, {2,4,6,7}, {2,4,7,8}, {2,5,6,8}, {2,5,7,8}, {2,6,7,8}, {3,4,5,6}, {3,4,5,7}, {3,4,5,8}, {3,4,6,7}, {3,5,6,8}, {4,5,7,8};

(iii) {1,2,6}, {1,3,5}, {2,3,4}, {3,7,8}, {4,6,8}, {5,6,7}.

So the stopping set distribution of $C_\Omega(D, G)$ with the parity-check matrix H^* is

$$T_i(H^*) = \begin{cases} 1, & \text{if } i = 0, \\ 0, & \text{if } i = 1 \text{ or } 2, \\ 6, & \text{if } i = 3, \\ 40, & \text{if } i = 4, \\ \binom{8}{i}, & \text{if } i \geqslant 5. \end{cases}$$

Also, the minimum distance of the code $C_\Omega(D, G)$ is 3 by Proposition 1.

Theorem 10 describes all the stopping sets of residue AG codes from elliptic curves. Next, we establish the relationship between the set of stopping sets with cardinality m and the set of stopping sets with cardinality $m+1$.

Denote by $S(m)$ and $S(m+1)$ the two sets of stopping sets with cardinality m and $m+1$ in the cases (iv) and (iii) in Theorem 10, respectively. Let $S^+(m)$ be the extended set of $S(m)$ defined as follows

$$S^+(m) = \bigcup_{A\in S(m)} \{A \cup \{i\} : i \in [n] \setminus A\}.$$

Theorem 12. *Notations as above. We have*

$$S(m+1) \cap S^+(m) = \emptyset,$$

and $S(m+1) = \{subsets\ of\ [n]\ with\ size\ m+1\} \setminus S^+(m)$.

Moreover, the union in the definition of $S^+(m)$ is a disjoint union. Hence

$$\begin{aligned} |S(m+1)| &= \tbinom{n}{m+1} - |S^+(m)| \\ &= \tbinom{n}{m+1} - (n-m)|S(m)|. \end{aligned}$$

Proof: First, $S(m+1) \cap S^+(m) = \emptyset$ is obvious by parts (iii) and (iv) of Theorem 10. So

$S(m+1) \subseteq$ {subsets of [n] with size m+1}$\setminus S^+(m)$.

On the other hand, for any subset A with $|A| = m+1$ and $A \notin S(m+1)$, we have $|A| \geqslant 2$ as $m \geqslant 1$. By Theorem 10 (iii), there is some $i \in A$ such that $\sum_{j \in A \setminus \{i\}} P_j = O$. By Theorem 10 (iv), $A \setminus \{i\} \in S(m)$. So

$$A = (A \setminus \{i\}) \cup \{i\} \in S^+(m).$$

Hence

$S(m+1) = \{\text{subsets of } [n] \text{ with size } m+1\} \setminus S^+(m)$.

If there exist $A \in S(m)$, $A' \in S(m)$, $i \notin A$ and $i' \notin A'$ such that

$$A \cup \{i\} = A' \cup \{i'\} \in S^+(m),$$

then we have $i \in A'$, $i' \in A$ and $A \setminus \{i'\} = A' \setminus \{i\}$.

Since

$$\sum_{j \in A} P_j = \sum_{j \in A'} P_j = O,$$

we get $P_i = P_{i'}$. So

$$A = A', \qquad i = i'.$$

That is, the union in the definition of $S^+(m)$ is a disjoint union. The formula

$$\begin{aligned} |S(m+1)| &= \tbinom{n}{m+1} - |S^+(m)| \\ &= \tbinom{n}{m+1} - (n-m)|S(m)| \end{aligned}$$

follows immediately. ∎

Remark 13. The above theorem shows how we can get $S(m+1)$ from $S(m)$. Conversely, if we know $S(m+1)$, then by the above theorem, we can exclude $S(m+1)$ from the set of all subsets of $[n]$ with $m+1$ elements to get $S^+(m)$. For any $I \in S^+(m)$, we calculate $\sum_{i \in I} P_i$. Then by Theorem 10 (iv), there is some index $j(I) \in I$ such that

$$\sum_{i \in I} P_i = P_{j(I)}.$$

By the definitions of $S(m)$ and $S^+(m)$, we have

$$S(m) = \{I \setminus \{j(I)\} : I \in S^+(m)\}.$$

In the above example, by Theorem 10 (iv), $S(3)$ consists of all the subsets of [8] whose sums have 9 as a divisor. Then by Theorem 12, $S(4)$ follows immediately from $S(3)$.

The following corollary follows immediately from Proposition 1, Theorems 10 and 12.

Corollary 14. *Notations as above. The minimum distance and the stopping distance of the residue AG code $C_\Omega(D, G)$ constructed from an elliptic curve is* $\deg(G)$ *or* $\deg(G)+1$. *More explicitly, if $|S(m)| > 0$, then we have the stopping distance*

$$s(C_\Omega(D,G)) = d(C_\Omega(D,G)) = m = \deg(G).$$

If $|S(m)| = 0$, then we have $|S(m+1)| > 0$ and hence

$$s(C_\Omega(D,G)) = d(C_\Omega(D,G)) = m+1 = \deg(G)+1.$$

Let $\mathcal{G}$ be an abelian group with zero element O and D a finite subset of $\mathcal{G}$. For an integer $0 < k < |D|$ and an element $b \in D$, we denote

$$N_{\mathcal{G}}(k, b, D) = \left| \left\{ S \subseteq D : |S| = k \text{ and } \sum_{x \in S} x = b \right\} \right|.$$

Computing $N_{\mathcal{G}}(k, b, D)$ is called a counting version of the *k-subset sum problem* (k-SSP). In general, a counting k-SSP is **NP**-hard [35]. If there is no confusion, we simply denote

$$N(k, b, D) = N_{\mathcal{G}}(k, b, D).$$

Remark 15. By the above theorem, for a general subset $D \subseteq E(\mathbb{F}_q)$, to decide whether $|S(m)| > 0$ is the decision m-subset sum problem in $E(\mathbb{F}_q)$. It is known that the decision m-subset sum problem in $E(\mathbb{F}_q)$ in general is **NP**-hard under **RP**-reduction [32]. So to compute the stopping distance of $C_\Omega(D, G)$ is **NP**-hard under **RP**-reduction.

For a subset $D \subseteq E(\mathbb{F}_q)$ with special algebraic structure, it is possible to give an explicit formula for $|S(m)| = N(m, O, D)$, and hence explicit formulas for $|S(m+1)|$ and the whole stopping set distribution by Theorem 12. In the following, we consider special subsets $D = U \setminus \{O\}$ for some subgroup U of $E(\mathbb{F}_q)$. In particular, recall that $C_\Omega(D, G)$ is called the standard elliptic code if $D = E(\mathbb{F}_q) \setminus \{O\}$.

Proposition 16 ([30, 31]). *Let $\mathcal{G}$ be a finite abelian group. For $b \in \mathcal{G}$, we have*

$$\begin{aligned} N(i, g, \mathcal{G} \setminus \{0\}) = \tfrac{1}{N} \textstyle\sum_{s | \exp(\mathcal{G})} (-1)^{i + \lfloor \frac{i}{s} \rfloor} \binom{N/s - 1}{\lfloor i/s \rfloor} \\ \cdot \textstyle\sum_{d | \gcd(e(g), s)} \mu(s/d) \# \mathcal{G}[d]. \end{aligned}$$

where $N = |\mathcal{G}|$, $\exp(\mathcal{G})$ is the exponent of $\mathcal{G}$, $e(b) = \max\{d : d | \exp(\mathcal{G}),\ b \in d\mathcal{G}\}$, μ is the Möbius function and $\mathcal{G}[d]$ is the d-torsion subgroup of $\mathcal{G}$.

Set $\mathcal{G} = U$ a subgroup of $E(\mathbb{F}_q)$ in Proposition 16. Let $N = |U| = n+1$ and $D = U \setminus \{O\}$. Then we have

Theorem 17. *The number of stopping sets of $C_\Omega(D, mO)$ with cardinality m is*

$$|S(m)| = \frac{1}{N} \sum_{s | \exp(U)} (-1)^{m + \lfloor \frac{m}{s} \rfloor} \binom{N/s - 1}{\lfloor m/s \rfloor} \cdot \sum_{d | s} \mu(s/d) |U[d]|.$$

So together with Theorems 10 and 1, we obtain Theorem 5.

It is well-known [36] that the group $E(\mathbb{F}_q)$ of rational points is isomorphic to

$$E(\mathbb{F}_q) \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z},$$

for some integers $m_1 | m_2$. Then by Theorems 10, 12 and 17, we can determine the stopping set distribution of the standard residue AG code $C_\Omega(D, mO)$ from any elliptic curve $E/\mathbb{F}_q$ provided that we know the group structure of $E(\mathbb{F}_q)$. Explicitly, we can compute $|S(3)|$ in Example 11:

$$\begin{aligned} |S(3)| &= \tfrac{1}{9} \textstyle\sum_{s | 9} (-1)^{3 + \lfloor \frac{3}{s} \rfloor} \binom{9/s - 1}{\lfloor 3/s \rfloor} \sum_{d | s} \mu(s/d) \, |\mathbb{Z}/9\mathbb{Z}[d]| \\ &= \tfrac{1}{9} \left(\tbinom{8}{3} + \tbinom{2}{1}(3-1) - (9-3) \right) = 6. \end{aligned}$$

So $|S(4)| = \binom{8}{4} - (8-3)|S(3)| = 40$. This agrees with the exhausting calculation in Example 11.

For a general subgroup of $E(\mathbb{F}_q)$, the refined structure of the subgroup is required to compute $|S(m)|$. By the formula

in Theorem 17, we even need to know the factorization of the exponent of the subgroup which is hard to be known if the exponent is big. If we take some special subgroups of $E(\mathbb{F}_q)$, then we have the following corollary.

Corollary 18. *Notations as above.*

(i) *If we take*

$$U \cong \mathbb{Z}/p^t\mathbb{Z}$$

for some prime integer p and integer $t \geqslant 1$, then

$$|S(m)| = \frac{1}{p^t}\left(\binom{p^t-1}{m} + (-1)^m(p^t - p^{\lfloor \log_p(m)\rfloor}) + \sum_{i=1}^{\lfloor \log_p(m)\rfloor}(-1)^{m+\lfloor \frac{m}{p^i}\rfloor}(p^i - p^{i-1})\binom{p^{t-i}-1}{\lfloor \frac{m}{p^i}\rfloor}\right).$$

In particular, if $t = 1$, then

$$|S(m)| = \frac{1}{p}\left(\binom{p-1}{m} + (-1)^m(p-1)\right).$$

If $t = 2$, then

$$|S(m)| = \frac{1}{p^2}\left(\binom{p^2-1}{m} + (-1)^m(p^2-p) + (-1)^{m+\lfloor \frac{m}{p}\rfloor}\cdot(p-1)\binom{p-1}{\lfloor \frac{m}{p}\rfloor}\right).$$

(ii) *If we take*

$$U \cong \mathbb{Z}/p^{t_1}\mathbb{Z} \oplus \mathbb{Z}/p^{t_2}\mathbb{Z}$$

for some prime integer p and integers $1 \leqslant t_1 \leqslant t_2$, then

$$|S(m)| = \frac{1}{p^{t_1+t_2}}\left(\binom{p^{t_1+t_2}-1}{m} + \sum_{i=1}^{t_2}(-1)^{m+\lfloor \frac{m}{p^i}\rfloor}\cdot\binom{p^{t_1+t_2-i}-1}{\lfloor \frac{m}{p^i}\rfloor}(p^{i+\min\{i,t_1\}} - p^{i-1+\min\{i-1,t_1\}})\right).$$

(iii) *If we take*

$$U \cong \mathbb{Z}/p_1^{t_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{t_2}\mathbb{Z}$$

for two distinct prime integers p_1, p_2 and integers $t_1, t_2 \geqslant 1$, then

$$\begin{aligned}\#S(m) = \frac{1}{p_1^{t_1}p_2^{t_2}}&\left(\binom{p_1^{t_1}p_2^{t_2}-1}{m} + (p_1-1)(p_2-1)\right.\\ &\cdot\sum_{i=1}^{t_1}\sum_{j=1}^{t_2}(-1)^{m+\lfloor \frac{m}{p_1^ip_2^j}\rfloor}p_1^{i-1}p_2^{j-1}\binom{p_1^{t_1-i}p_2^{t_2-j}-1}{\lfloor \frac{m}{p_1^ip_2^j}\rfloor}\\ &+\sum_{i=1}^{t_1}(-1)^{m+\lfloor \frac{m}{p_1^i}\rfloor}\binom{p_1^{t_1-i}p_2^{t_2}-1}{\lfloor \frac{m}{p_1^i}\rfloor}(p_1^i - p_1^{i-1})\\ &\left.+\sum_{j=1}^{t_2}(-1)^{m+\lfloor \frac{m}{p_2^j}\rfloor}\binom{p_1^{t_1}p_2^{t_2-j}-1}{\lfloor \frac{m}{p_2^j}\rfloor}(p_2^j - p_2^{j-1})\right).\end{aligned}$$

Proof: We first check (i). Note that in this case

$$N = p^t \quad \text{and} \quad \exp(U) = p^t.$$

By Theorem 17, we have

$$\begin{aligned}&|S(m)|\\ &= \frac{1}{p^t}\sum_{s|p^t}(-1)^{m+\lfloor \frac{m}{s}\rfloor}\binom{p^t/s-1}{\lfloor m/s\rfloor}\sum_{d|s}\mu(s/d)|U[d]|\\ &= \frac{1}{p^t}\sum_{i=0}^{t}(-1)^{m+\lfloor \frac{m}{p^i}\rfloor}\binom{p^{t-i}-1}{\lfloor m/p^i\rfloor}\sum_{d|p^i}\mu(p^i/d)|U[d]|\\ &= \frac{1}{p^t}\binom{p^t-1}{m} + \frac{1}{p^t}\sum_{i=1}^{t}(-1)^{m+\lfloor \frac{m}{p^i}\rfloor}\binom{p^{t-i}-1}{\lfloor m/p^i\rfloor}\sum_{j=0}^{i}\mu(p^{i-j})|U[p^j]|\\ &\overset{(1)}{=} \frac{1}{p^t}\binom{p^t-1}{m} + \frac{1}{p^t}\sum_{i=1}^{t}(-1)^{m+\lfloor \frac{m}{p^i}\rfloor}\binom{p^{t-i}-1}{\lfloor m/p^i\rfloor}(|U[p^i]| - |U[p^{i-1}]|)\\ &= \frac{1}{p^t}\binom{p^t-1}{m} + \frac{1}{p^t}\sum_{i=1}^{\lfloor \log_p(m)\rfloor}(-1)^{m+\lfloor \frac{m}{p^i}\rfloor}\binom{p^{t-i}-1}{\lfloor m/p^i\rfloor}(p^i - p^{i-1})\\ &\quad + \frac{1}{p^t}\sum_{i=\lfloor \log_p(m)\rfloor+1}^{t}(-1)^m\binom{p^{t-i}-1}{0}(p^i - p^{i-1})\\ &= \frac{1}{p^t}\left(\binom{p^t-1}{m} + (-1)^m(p^t - p^{\lfloor \log_p(m)\rfloor})\right.\\ &\quad \left.+\sum_{i=1}^{\lfloor \log_p(m)\rfloor}(-1)^{m+\lfloor \frac{m}{p^i}\rfloor}(p^i - p^{i-1})\binom{p^{t-i}-1}{\lfloor \frac{m}{p^i}\rfloor}\right),\end{aligned}$$

where the equality (1) follows from $\mu(1) = 1$, $\mu(p) = -1$ and $\mu(p^i) = 0$ for all $i \geqslant 2$.

The proof of statement (ii) is almost the same as that of (i) with $N = p^{t_1+t_2}$, $\exp(U) = p^{t_2}$ and $|U[p^i]| = p^{i+\min\{i,t_1\}}$. The proof of statement (iii) is similar to that of (i) but with the Möbius function given explicitly by:

$$\mu(p_1^k p_2^l) = \begin{cases} 1, & \text{if } k = 0 \text{ and } l = 0;\\ -1, & \text{if } \{k,l\} = \{0,1\};\\ 0, & \text{if } k \geqslant 2 \text{ or } l \geqslant 2.\end{cases}$$

■

V. Conclusion

In this paper, we study stopping sets and stopping set distributions of residue algebraic geometry codes $C_\Omega(D, G)$. Two descriptions of stopping sets of residue algebraic geometry codes are presented. In particular, there is a gap $\deg(G) - 2g + 2 \leqslant i \leqslant \deg(G) + 1$ where in general we do not know whether a subset with cardinality i is a stopping set or not. In the case $g = 0$, there is no gap and we have a complete understanding. In the case $g = 1$, using the group structure of rational points of elliptic curves, we can characterize all the stopping sets of algebraic geometry codes from elliptic curves. Then determining the stopping sets, the stopping set distribution and the stopping distance of $C_\Omega(D, G)$ are reduced to $\deg(G)$-subset sum problems in finite abelian groups. In the case $g > 1$, only partial results can be obtained. It is still not known how to compute the stopping set distribution. For further work, there are two interesting problems:

(i) There are some papers contributing to compute the stopping redundancy of MDS codes [3], [5], [7]. For AG codes from elliptic curves, we have seen that the code is very closed to be MDS, i.e., MDS or near-MDS [37] (an $[n, k, d]$ linear code is called *near-MDS* if $d = n - k$ and the dual distance $d^\perp = k$). So how about the stopping redundancy of AG codes from elliptic curves?

(ii) In this paper, we have determined the stopping set distributions of AG codes from elliptic curves with the

parity-check matrix H^*. Can we give optimal parity-check matrices for AG codes from elliptic curves?

ACKNOWLEDGMENT

The authors would like to thank the two anonymous reviewers and Associate Editor Navin Kashyap for their valuable suggestions and comments that helped to greatly improve the paper.

REFERENCES

[1] R. Ahlswede and H. Aydinian, "On generic erasure correcting sets and related problems," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 501–508, Feb. 2012.
[2] M. Esmaeili, M. Tadayon, and T. Gulliver, "More on the stopping and minimum distances of array codes," *IEEE Trans. Commun.*, vol. 59, no. 3, pp. 750–757, Mar. 2011.
[3] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 922–932, Mar. 2006.
[4] T. Etzion, "On the stopping redundancy of Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4867–4879, Nov. 2006.
[5] J. Han and P. Siegel, "On the stopping redundancy of MDS codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 2491–2495.
[6] J. Han and P. Siegel, "Improved upper bounds on stopping redundancy," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 90–104, Jan. 2007.
[7] J. Han, P. Siegel, and R. Roth, "Single-exclusion number and the stopping redundancy of MDS codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4155–4166, Sep. 2009.
[8] Y. Jiang, S.-T. Xia, and F.-W. Fu, "Stopping set distributions of some Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 6078–6088, Sep. 2011.
[9] S.-T. Xia and F.-W. Fu, "Stopping set distributions of some linear codes," in *Proc. IEEE Inf. Theory Workshop*, Oct. 2006, pp. 47–51.
[10] S.-T. Xia and F.-W. Fu, "On the stopping distance of finite geometry LDPC codes," *IEEE Commun. Lett.*, vol. 10, no. 5, pp. 381–383, May 2006.
[11] J. Weber and K. Abdel-Ghaffar, "Stopping set analysis for Hamming codes," in *Proc. IEEE Inf. Theory Workshop*, Sep. 2005, pp. 244–247.
[12] T. Wadayama, "Average stopping set weight distributions of redundant random ensembles," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 4991–5004, Nov. 2008.
[13] A. Orlitsky, K. Viswanathan, and J. Zhang, "Stopping set distribution of LDPC code ensembles," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 929–953, Mar. 2005.
[14] S. Laendner and O. Milenkovic, "LDPC codes based on latin squares: Cycle structure, stopping set, and trapping set analysis," *IEEE Trans. Commun.*, vol. 55, no. 2, pp. 303–312, Feb. 2007.
[15] H. Liu, Y. Li, L. Ma, and J. Chen, "On the smallest absorbing sets of LDPC codes from finite planes," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 4014–4020, Jun. 2012.
[16] A. McGregor and O. Milenkovic, "On the hardness of approximating stopping and trapping sets," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1640–1650, Apr. 2010.
[17] K. Krishnan and P. Shankar, "Computing the stopping distance of a Tanner graph is NP-hard," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2278–2280, Jun. 2007.
[18] N. Kashyap and A. Vardy, "Stopping sets in codes from designs," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2003, p. 122.
[19] H. Hollmann and L. Tolhuizen, "On parity-check collections for iterative erasure decoding that correct all correctable erasure patterns of a given size," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 823–828, Feb. 2007.
[20] T. Hehn, O. Milenkovic, S. Laendner, and J. Huber, "Permutation decoding and the stopping redundancy hierarchy of cyclic and extended cyclic codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5308–5331, Dec. 2008.
[21] J. Han, P. Siegel, and A. Vardy, "Improved probabilistic bounds on stopping redundancy," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1749–1753, Apr. 2008.
[22] J. Feldman, M. Wainwright, and D. Karger, "Using linear programming to decode binary linear codes," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 954–972, Mar. 2005.
[23] M. Esmaeili and M. Amoshahy, "On the stopping distance of array code parity-check matrices," *IEEE Trans. Inf. Theory*, vol. 55, no. 8, pp. 3488–3493, Aug. 2009.
[24] C. Di, D. Proietti, I. Telatar, T. Richardson, and R. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1570–1579, Jun. 2002.
[25] K. Abdel-Ghaffar and J. Weber, "Complete enumeration of stopping sets of full-rank parity-check matrices of Hamming codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 9, pp. 3196–3201, Sep. 2007.
[26] R. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.
[27] H. Hollmann and L. Tolhuizen, "Generic erasure correcting sets: Bounds and constructions," *J. Combinat. Theory, Ser. A*, vol. 113, no. 8, pp. 1746–1759, Nov. 2006.
[28] H. Stichtenoth, *Algebraic Function Fields and Codes*, vol. 254, 2nd ed. Berlin, Germany: Springer-Verlag, 2009.
[29] J. Li and D. Wan, "On the subset sum problem over finite fields," *Finite Fields Appl.*, vol. 14, no. 4, pp. 911–929, 2008.
[30] M. Kosters, "The subset sum problem for finite abelian groups," *J. Combinat. Theory, Ser. A*, vol. 120, no. 3, pp. 527–530, 2013.
[31] J. Li and D. Wan, "Counting subset sums of finite abelian groups," *J. Combinat. Theory, Ser. A*, vol. 119, no. 1, pp. 170–182, 2012.
[32] Q. Cheng, "Hard problems of algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 402–406, Jul. 2008.
[33] R. Schoof, "Nonsingular plane cubic curves over finite fields," *J. Combinat. Theory, Ser. A*, vol. 46, no. 2, pp. 183–211, 1987.
[34] J. Silverman, *The Arithmetic of Elliptic Curves*, vol. 106, 2nd ed. Dordrecht, The Netherlands: Springer-Verlag, 2009.
[35] T. Cormen, C. Stein, R. Rivest, and C. Leiserson, *Introduction to Algorithms*, 2nd ed. New York, NY, USA: McGraw-Hill, 2001.
[36] J. Voloch, "A note on elliptic curves over finite fields," *Bull. Soc. Math. France*, vol. 116, no. 4, pp. 455–458, 1988.
[37] M. Shokrollahi, "On the weight distribution of elliptic codes," Inst. für Informatik, Univ. Bonn, Germany, Tech. Rep., Sep. 1990

Jun Zhang was born in Jiangsu, China, on March 30, 1986. He received the B. S. degree in mathematics from Nankai University, Tianjin, China, in 2008. Since September 2008, he has been a Ph.D. student at the Chern Institute of Mathematics, Nankai University. He visited the Department of Mathematics, University of California at Irvine, USA, from September 2012 to September 2013. His research interests include number theory, coding theory and cryptography.

Fang-Wei Fu was born in Hunan, China, on October 28, 1963. He received the B. S. degree in mathematics, the M. S. degree, and the Ph.D. degree in applied mathematics from Nankai University, Tianjin, China, in 1984, 1987 and 1990, respectively.

Since April 2007, he has been with the Chern Institute of Mathematics, Nankai University, Tianjin, China, where he is a Professor. From June 1987 to April 2007, he was with the School of Mathematical Science, Nankai University, Tianjin, China, and became a Professor there in 1995. From February 2002 to March 2007, he was a Research Scientist with the Temasek Laboratories, National University of Singapore, Republic of Singapore. From November 1989 to November 1990, he visited the Department of Mathematics, University of Bielefeld, Germany. From October 1996 to October 1997, he visited the Institute for Experimental Mathematics, University of Essen, Germany. From October 1998 to January 1999, from July 1999 to October 1999, from April 2000 to October 2000, and from July 2001 to February 2002, he visited the Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong. He visited the Department of Mathematics, University of California, Irvine, USA, for one month in April 2013. His current research interests include coding theory, cryptography, and information theory.

Daqing Wan received the B. S. degree from Chengdu Institute of Geology in 1982, the M.S. degree from Sichuan University in 1986, and the Ph.D. degree from the University of Washington in Seattle in 1991. He joined the University of California at Irvine in 1997, where he is now a Professor of Mathematics. His research interests include number theory, coding theory, algorithms and complexity.