Stopping Set Enumerators of Full-Rank Parity-Check Matrices of Hamming Codes

Khaled A.S. Abdel-Ghaffar
University of California
Department of ECE
Davis, CA 95616
USA
E-mail: ghaffar@ece.ucdavis.edu

Jos H. Weber
Delft University of Technology
Faculty of EEMCS
Mekelweg 4, 2628 CD Delft
The Netherlands
E-mail: j.h.weber@ewi.tudelft.nl

Abstract—In the 2004 Shannon Lecture, McEliece presented an expression for the number of stopping sets of size three for a full-rank parity-check matrix of the Hamming code. In this paper, we derive an expression for the number of stopping sets of any given size for the same parity-check matrix.

I. INTRODUCTION

Let $C$ be a linear binary $[n,k,d]$ block code, where $n$, $k$, and $d$ denote the code’s length, dimension, and Hamming distance, respectively. The set of codewords of $C$ can be defined as the null space of the row space of an $r \times n$ binary parity-check matrix $H = (h_{i,j})$ of rank $n-k$. Assuming all rows in $H$ are different, $n-k \leq r \leq 2^{n-k}$.

Let $S$ be a subset of $\{1,2,\ldots,n\}$ and $T$ be a subset of $\{1,2,\ldots,r\}$. For any $H = (h_{i,j})$ of size $r \times n$, let $H_{S,T} = (h_{i,j})$ where $i \in T$ and $j \in S$. Then, $H_{S,T}$ is a $|T| \times |S|$ submatrix of $H$. For simplicity, we write $H_S$ and $H^T$ to denote $H_{S,T}$ in case $T = \{1,2,\ldots,r\}$ and $S = \{1,2,\ldots,n\}$, respectively.

A set $S$ is the support of a codeword if and only if all rows in $H_S$ have even weight, i.e., if and only if

$$|\{j \in S : h_{i,j} = 1\}| \equiv 0(2) \quad \forall i = 1,2,\ldots,r. \quad (1)$$

A set $S$ is a stopping set if and only if $H_S$ does not contain a row of weight one, i.e., if and only if

$$|\{j \in S : h_{i,j} = 1\}| \neq 1 \quad \forall i = 1,2,\ldots,r. \quad (2)$$

The polynomial $A(x) = \sum_{i=0}^{n} A_i x^i$, where $A_i$ is the number of codewords of weight $l$, is called the weight enumerator of code $C$. It holds that

$$d = \min\{l \geq 1 : A_l > 0\}. \quad (3)$$

The polynomial $S(x) = \sum_{i=0}^{n} S_i x^i$, where $S_i$ is the number of stopping sets of size $l$, is called the stopping set enumerator of parity-check matrix $H$. Let $s$ denote the smallest size of a non-empty stopping set, i.e.,

$$s = \min\{l \geq 1 : S_l > 0\}. \quad (4)$$

Notice from (1) and (2) that the support of any codeword is a stopping set. Therefore, $S_l \geq A_l$ for $l = 0,1,\ldots,n$ and $s \leq d$.

Considering the vacuous case in which $l = 0$, we notice, from the definitions, that the empty set is both the support of a codeword and a stopping set for any code and any parity-check matrix. Hence, $A_0 = S_0 = 1$. Furthermore, from the observation that (1) and (2) are equivalent for sets $S$ with $|S| \leq 2$, it follows that $A_1 = S_1$ for $l \leq 2$. In particular, $S_0 = 1$ and $S_1 = S_2 = 0$ for any parity-check matrix of a code of minimum distance $d \geq 3$.

The notion of stopping sets is important in the context of iterative decoders (using $H$-based Tanner graphs), in particular for low-density parity-check codes [3]. For example, on the binary erasure channel, an iterative decoder will not lead to successful decoding if and only if the set of erased positions contains a non-empty stopping set. Hence, the minimum (non-empty) stopping set size $s$ and the cardinality $S_s$ are performance indicators for iterative decoding, alike the minimum distance $d$ and the number of minimum weight codewords for maximum-likelihood decoding. However, contrary to the weight enumerator, which is fixed for a code $C$, the stopping set enumerator depends on the choice of the parity-check matrix $H$.

In the 2004 Shannon lecture, McEliece [5] presented the following expression for the number of stopping sets of size three in a $[2^m-1,2^m-m-1,3]$ Hamming code:

$$S_3 = \frac{1}{6} \left(5^m - 3^{m+1} + 2^{m+1}\right) \sim \frac{1}{6} n^{2.322}. \quad (5)$$

He did not mention explicitly which parity-check matrix he had in mind, but from the context, it was clear that it was the full rank $m \times (2^m-1)$ parity-check matrix. This is the parity-check matrix of minimum number of rows for the Hamming code. The value of $S_3$ is of particular interest since $S_0 = 1$ and $S_1 = S_2 = 0$ as the Hamming code has minimum distance three which implies that $s = 3$. Hence, the value of $S_3$ given in (5) corresponding to the full rank parity-check matrix of the Hamming code can be used to obtain a good estimate of the performance of the simplest iterative decoder for the Hamming code. However, as the multiplicities $A_l$ of codewords in a code of weight $l > d$ influence the performance of maximum-likelihood decoding, the multiplicities $S_l$ of stopping sets of size $l > s$ also influence the performance of iterative decoding.
In this paper, we derive the values $S_l$ for all $l$ for the full-rank parity-check matrix of the Hamming code.

Section II gives an expression for $S_l$ in terms of certain parameters that can be derived from the parity-check matrix of any linear code. In Section III, we determine these parameters for the full-rank parity check matrices of Hamming codes and derive expressions for their stopping set enumerators.

II. COMPUTING THE STOPPING SET ENUMERATOR FOR LINEAR CODES

In this section, we derive an expression for the coefficients of $S(x)$ for an $r \times n$ parity-check matrix $H$ of an $[n, k, d]$ binary linear code $C$.

For each subset $T$ of $\{1, 2, \ldots, r\}$, we define $z_T$ to be the number of columns in $H_T$ of weight zero. In particular, if $T$ is empty, then $z_T = n$. If $Y$ is a subset of $\{1, 2, \ldots, n\}$ such that $|Y| = p$, each row in $H_T^Y$ has weight one, and each column in $H_T^Y$ has non-zero weight, then we say that $Y$ is of type $p$ with respect to $T$. Let $Y(T, p)$ be the number of subsets of $\{1, 2, \ldots, n\}$ of type $p$ with respect to $T$. Since every column in $H_T^Y$ should have non-zero weight and every row should have weight one, it follows that

$$Y(T, p) = \begin{cases} 0 & \text{if } T = \emptyset \land p > 1 \lor T \neq \emptyset \land p = 0, \\ 1 & \text{if } T = \emptyset \land p = 0. \end{cases} \tag{6}$$

Theorem I: Let $H$ be an $r \times n$ parity-check matrix of a linear code $C$ of length $n$. Then, for $l = 0, 1, \ldots, n,$

$$S_l = \sum_{T \subseteq \{1, 2, \ldots, r\}} (-1)^{|T|} \sum_{p=0}^{l} Y(T, p) \binom{z_T}{l-p}.$$

Proof. It follows from (6) that the result holds for $l = 0$. Therefore, we assume $l \geq 1$. Let $S$ be a non-empty subset of $\{1, 2, \ldots, n\}$. Following [7], we say that row $h$ in $H$ covers $S$ if and only if $h_S$ has weight one. For $i = 1, 2, \ldots, r$ and $l = 1, 2, \ldots, n$, let $Q_i^l$ and $Q_i^l$ be the family of subsets of $\{1, 2, \ldots, n\}$ and size $l$ that are covered and not covered, respectively, by the $i$th row in $H$. A subset $S \subseteq \{1, 2, \ldots, n\}$ of size $l$ is a stopping set if and only if it is not covered by any row of $H$, i.e., $S \not\in \bigcap_{i=1}^{r} Q_i^l$. In particular, $S_1 = |\bigcap_{i=1}^{r} Q_i^l|$. The Principle of Inclusion and Exclusion (see, e.g., [2], Theorem B, p. 178), yields

$$|\bigcap_{i=1}^{r} Q_i^l| = \sum_{T \subseteq \{1, 2, \ldots, r\}} (-1)^{|T|} |\bigcap_{i \in T} Q_i^l|. \tag{7}$$

In the above sum, $T$ runs over all $2^r$ subsets of $\{1, 2, \ldots, r\}$ where, for the term corresponding to the empty set $\emptyset$,

$$|\bigcap_{i \in T} Q_i^l| = \binom{n}{l},$$

which is the total number of subsets of $\{1, 2, \ldots, n\}$ of size $l$. Notice that a set $S$ of size $l$ belongs to $\bigcap_{i \in T} Q_i^l$ if and only if each row in $H^S$ has weight one. This is the case if and only if, for some $p = 0, 1, \ldots, l$, $S$ contains a subset $Y$ of type $p$ with respect to $T$ and all the columns indexed by $S\setminus Y$ have zero weights. Therefore,

$$|\bigcap_{i \in T} Q_i^l| = \sum_{p=0}^{l} Y(T, p) \binom{z_T}{l-p}.$$

Combining this with (7), the proof is complete. \hfill \blacksquare

III. COMPUTING THE STOPPING SET ENUMERATOR FOR HAMMING CODES

A full-rank parity-check matrix of a $[2^m - 1, 2^m - m - 1, 3]$ Hamming code, where $m \geq 3$, is an $m \times (2^m - 1)$ matrix whose columns are the distinct non-zero vectors of length $m$. From now on, we take $H$ to be such a matrix with $r = m$ and $n = 2^m - 1$, and $S_l$ to be the number of stopping sets of $H$ of size $l$.

In the following derivations, we make use of Stirling numbers. Following the notation of Comtet [2] and Riordan [6], we denote by $s(n, k)$ and $S(n, k)$ the Stirling numbers of the first kind and of the second kind, respectively. Notice that $n$ and $k$ are not necessarily the length and the dimension of a code.

For $n \geq 1$, $(1)^{n-k}s(n, k)$ is the number of permutations of $n$ elements which have exactly $k$ cycles and $S(n, k)$ is the number of ways of partitioning a set of $n$ elements into $k$ non-empty subsets, see, e.g., [1], p. 824, where (8)–(11) can also be found. We also define $s(0, 0) = S(0, 0) = 1$. Notice that for $n \geq 1$, both $s(n, k)$ and $S(n, k)$ are equal to zero if $k \leq 0$ or $k > n$, see e.g., [6].

Stirling numbers of the first kind satisfy the following polynomial identity in $x$

$$\sum_{k=0}^{n} s(n, k)x^k = n!\binom{x}{n} \tag{8}$$

and the recursion

$$s(n+1, k) = s(n, k-1) - ns(n, k), \tag{9}$$

for $n \geq k \geq 1$. We also have

$$s(n, 1) = (-1)^{n-1}(n-1)!.$$

Stirling numbers of the second kind can be computed explicitly using

$$S(n, k) = \frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} (k-i)^n. \tag{11}$$

Lemma I: For $n \geq 0$, the following polynomial identity in $x$ holds

$$n!\binom{x-1}{n} = \sum_{k=1}^{n+1} s(n+1, k)x^{k-1}. \tag{12}$$

Proof. From the definition of binomial coefficients, we have

$$\binom{x-1}{n} = \frac{x-n}{x}\binom{x}{n}. \tag{13}$$

Combining this with (8) we get

$$n!\binom{x-1}{n} = \frac{x-n}{x}\sum_{k=0}^{n} s(n, k)x^k$$

$$= \sum_{k=0}^{n} s(n, k)x^k - n\sum_{k=0}^{n} s(n, k)x^{k-1}$$

$$= \sum_{k=1}^{n+1} (s(n, k-1) - ns(n, k))x^{k-1}$$
since \(ns(n, 0) = 0\) and \(s(n, n + 1) = 0\) for \(n \geq 0\). The result now follows from the recurrence relation (9).

**Lemma 2:** Let \(H\) be an \(m \times (2^m - 1)\) parity-check matrix of a Hamming code of length \(2^m - 1\). Then, for any set \(T \subseteq \{1, 2, \ldots, m\}\) and any \(p = 0, 1, \ldots, n\),

\[
z_T = 2^{m-|T|} - 1
\]

and

\[
Y(T, p) = S([|T|], p) 2^{(m-|T|)p}.
\]

**Proof.** Each non-zero vector of length \(m\) appears exactly once as a column in \(H\). Hence, the zero-weight vector of length \(|T|\) appears exactly \(2^{m-|T|} - 1\) times in \(H_T\). This verifies the expression for \(z_T\). From (6) and (11), it follows that the second part of the lemma holds in case \(T = \emptyset\). Therefore, assume in the following that \(T \neq \emptyset\). Hence, \(1 \leq |T| \leq m\). For each \(j \in \{1, 2, \ldots, 2^m - 1\}\), let

\[
\mathcal{H}_j = \{i \in T : h_{ij} = 1\},
\]

i.e., \(\mathcal{H}_j\) is the set of indices of ones in the \(j\)th column of \(H_T\). Notice that a subset \(J\) of size \(p\) is of type \(p\) with respect to \(T\) if and only if \(\mathcal{H}_j\) is a \(|T| \times p\) matrix, each column of which has non-zero weight, and each row of which has weight one. This is the case if and only if, for \(j \in \mathcal{H}_j\), the sets \(\mathcal{H}_j\) are non-empty, disjoint, and their union is \(T\). There are \(S(|T|, p)\) ways to partition a set of \(|T|\) elements into \(p\) non-empty subsets. Each non-zero vector of length \(|T|\) appears exactly \(2^{m-|T|}\) times as a column in \(H_T\). Therefore, for each partition, there are \(2^{m-|T|}\) choices for \(j\), corresponding to indices of identical non-zero columns in \(H_T\), such that \(\mathcal{H}_j\) is one of the \(p\) subsets in the partition. Since there are \(p\) subsets in each partition, and there are \(S(|T|, p)\) partitions, the total number of \(|T| \times p\) submatrices in \(H_T\), where \(0 \leq p \leq l\), each of its columns has non-zero weight and each of its rows has weight one, is \(S(|T|, p) 2^{(m-|T|)p}\). The number of such matrices equals \(Y(T, p)\).

**Lemma 3:** Let \(H\) be an \(m \times (2^m - 1)\) parity-check matrix of a Hamming code of length \(2^m - 1\). Then, for \(l = 0, 1, \ldots, 2^m - 1\),

\[
S_l = \sum_{t=0}^{m} (-1)^t \binom{m}{t} \sum_{p=0}^{l} S(t, p) 2^{(m-t)l} p^{2^{m-t}-1} - 1\).
\]

**Proof.** From Lemma 2, it follows that for the cardinality of \(T\) and \(Y(T, p)\) in Theorem 1.

**Lemma 3**, when combined with (11), gives an explicit expression for \(S_l\) for \(l = 0, 1, \ldots, 2^m - 1\). Notice that for each value of \(l\), \(S_l\) depends only on \(m\). However, contrary to the expression in (5), the expression in the lemma does not show clearly this dependency. In the next lemma, we make the dependency clear. For this purpose, we define for nonnegative integers \(q\) and \(v\),

\[
b(q, v) = \sum_{p=0}^{v} (-1)^p \binom{v}{p} s(p + 1, p - q + 1).
\]

**Lemma 4:** Let \(H\) be an \(m \times (2^m - 1)\) parity-check matrix of a Hamming code of length \(2^m - 1\). Then, for \(l = 0, 1, \ldots, 2^m - 1\),

\[
S_l = \frac{1}{k^l} \sum_{q=0}^{l} \binom{l}{v} b(q, v) (2^{l-q} - (l-v))^{m}.
\]

**Proof.** From Lemma 1, we have for \(p \leq l\) and \(t \leq m\)

\[
(2^{m-t} - 1) = \frac{1}{(l-p)!} \sum_{u=0}^{l-p} s(l-p+1, u) 2^{(m-t)(u-1)}
\]

\[
= \frac{1}{(l-p)!} \sum_{q=0}^{l-p} s(l-p+1, l-q-p+1) 2^{(m-t)(l-q-p)},
\]

since \(s(n, k) = 0\) for \(k \leq n\). Also, from (11), we obtain

\[
S(t, p) = \frac{1}{p^l} \sum_{i=0}^{p} (-1)^i \binom{p}{i} (p-i)^t
\]

\[
= \frac{(-1)^{p-l} p}{l^t} \sum_{v=0}^{l} (-1)^v \binom{p}{l-v} (l-v)^t.
\]

Substituting (15) and (16) in the expression of \(S_l\) given in Lemma 3, we get

\[
S_l = \sum_{t=0}^{m} (-1)^t \binom{m}{t} \sum_{p=0}^{l} \frac{(-1)^{-p}}{p^t} \sum_{v=0}^{l} (-1)^v \binom{p}{l-v} (l-v)^t
\]

\[
= \frac{1}{l^t} \sum_{q=0}^{l} (-1)^t \binom{m}{t} \sum_{p=0}^{l} (-1)^{-p} \binom{p}{l-q} \sum_{v=0}^{l} (-1)^v \binom{p}{l-v} (l-v)^t
\]

\[
= \frac{1}{l^t} \sum_{q=0}^{l} (-1)^t \binom{m}{t} \sum_{p=0}^{l} s(l-p+1, l-q-p+1) 2^{(m-t)(l-q-p)}.
\]

Noticing that

\[
\binom{l}{v} \binom{p}{l-v} = \binom{l}{v} \binom{v}{l-p},
\]

we obtain by interchanging orders of summations

\[
S_l = \frac{1}{l^t} \sum_{q=0}^{l} (-1)^t \binom{m}{t} \sum_{p=0}^{l} s(l-p+1, l-q-p+1) 2^{(m-t)(l-q-p)}.
\]

It is straightforward to check that the last sum is identical to \(b(q, v)\).

To obtain an expression for \(b(q, v)\) that does not involve Stirling numbers, we derive a recursion for \(b(q, v)\) along with boundary values to apply the recursion.

**Lemma 5:** For nonnegative numbers \(q\) and \(v\), we have

\[
b(q, v) = \begin{cases} 
0 & \text{if } q > v \text{ or } q = 0 < v, \\
\frac{1}{q!} & \text{if } q = v. 
\end{cases}
\]
and for \( q \geq 1 \) and \( v \geq 2 \),

\[
b(q, v) = vb(q - 1, v - 1) - (v - 1)b(q - 1, v - 2).
\]

**Proof.** For \( 0 \leq p \leq v < q \), we have \( p-q+1 \leq 0 \) and, therefore, \( s(p+1, p-q+1) = 0 \). From the definition of \( b(q, v) \) given in (14), it follows that \( b(q, v) = 0 \) in case \( q > v \).

In case \( q = 0 \), it follows from the definition of \( b(q, v) \) and the fact that \( s(p+1, p+1) = 1 \) that \( b(0, v) = 0 \) whenever \( v \geq 1 \).

In case \( q = v \), we have

\[
b(q, q) = \sum_{p=0}^{q} (-1)^{p} \binom{q}{p} s(p+1, p-q+1)
= (-1)^{q} s(q+1, 1) = q!
\]

using (10) and since \( s(p+1, p-q+1) = 0 \) for \( p-q+1 \leq 0 \).

Next, we prove the recursion for \( q \geq 1 \) and \( v \geq 2 \). Using the recurrence formula for the binomial coefficients followed by the recurrence formula (9) for Stirling numbers of the first kind, we obtain

\[
b(q, v) = \sum_{p=0}^{v} (-1)^{p} \binom{v-1}{p} s(p+1, p-q+1)
\]

\[
\cdot (v-1) \binom{v-1}{p-1} s(p, p-q+1)
\]

\[
= \sum_{p=0}^{v} (-1)^{p} \binom{v-1}{p} s(p+1, p-q+1)
\]

\[
+ \sum_{p=0}^{v} (-1)^{p} \binom{v-1}{p} s(p, p-q+1)
\]

\[
= \sum_{p=0}^{v} \left[ (-1)^{p} \binom{v-1}{p} \right] (p+1)
\]

\[
\cdot s(p+1, p-q+1)
\]

\[
= \sum_{p=0}^{v-1} (-1)^{p} \binom{v-1}{p} s(p+1, p-q+2)
\]

\[
+ \sum_{p=0}^{v-1} (-1)^{p} \binom{v-1}{p} ps(p+1, p-q+1)
\]

\[
= \sum_{p=0}^{v-1} \left[ (-1)^{p} \binom{v-1}{p} \right] (p+2)
\]

\[
\cdot s(p+1, p-q+2)
\]

\[
+ \sum_{p=0}^{v-1} \left[ (-1)^{p} \binom{v-1}{p} \right] ps(p+1, p-q+1)
\]

\[
= \sum_{p=0}^{v-1} \left[ (-1)^{p} \binom{v-1}{p} \right] (p+2)
\]

\[
\cdot s(p+1, p-q+2)
\]

Next, we use

\[
\binom{v-1}{p} p = \binom{v-2}{p-1} (v-1)
\]

followed by (9) to conclude that

\[
b(q, v) = b(q - 1, v - 1) + (v - 1) \sum_{p=0}^{v-1} (-1)^{p} \binom{v-2}{p-1} s(p+1, p-q+2)
\]

\[
\cdot s(p+1, p-q+2)
\]

\[
= b(q - 1, v - 1) + (v - 1) \sum_{p=0}^{v-1} (-1)^{p} \binom{v-2}{p-1} s(p, p-q+2)
\]

\[
\cdot (s(p, p-q+1) - ps(p, p-q+2))
\]

\[
= \sum_{p=0}^{v-1} \left[ (-1)^{p} \binom{v-2}{p-1} \right] (v-1)
\]

\[
\cdot s(p, p-q+2)
\]

\[
= b(q - 1, v - 1) - (v - 1)b(q - 1, v - 2)
\]

\[
+ (v - 1)b(q - 1, v - 1),
\]

where we used (14) and (17) after replacing \( v \) by \( v - 1 \) and \( q \) by \( q - 1 \). Hence, we have

\[
b(q, v) = vb(q - 1, v - 1) - (v - 1)b(q - 1, v - 2).
\]

\( \square \)

The values of \( b(q, v) \) for \( 0 \leq q, v \leq 7 \) are listed in Table I.

| \( q \) \( v \) | 0 1 2 3 4 5 6 7 |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 2 | 3 | 5 | 7 | 9 |
| 3 | 0 | 0 | 0 | 6 | 20 | 35 | 63 |
| 4 | 0 | 0 | 0 | 0 | 24 | 104 | 340 |
| 5 | 0 | 0 | 0 | 0 | 0 | 120 | 1044 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 720 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 5040 |

**Lemma 6:** For nonnegative integers \( q \) and \( v \geq q \), we have

\[
b(q, v) = (-1)^{v-q} v!
\]

\[
\sum_{i=1}^{v-q} \frac{1}{k_i}
\]

\( (\ast. \ast. \ast. (\ast)) \)

**Proof.** Let \( \tilde{b}(q, v) \) denote the expression in the right hand side of (18). It suffices to verify that \( \tilde{b}(q, v) \) satisfies the recursion given in Lemma 5 for \( q \geq 1 \) and \( v \geq 2 \) and that \( \tilde{b}(q, v) \) and \( b(q, v) \) agree in the cases \( q = 0 \) and \( v = q \). First, we notice that in case \( q = 0 \), the summation in the expression of \( \tilde{b}(q, v) \) is over all tuples \( 0 = k_0 < k_1 < \cdots < k_{v-q} < k_{v-q+1} = v+2 \) for which \( k_i - k_{i-1} \geq 2 \) for \( i = 1, 2, \ldots, v+1 \). For such tuples

\[
v + 2 = k_{v+1} - k_0 = \sum_{i=1}^{v+1} (k_i - k_{i-1}) \geq 2(v + 1) > v + 2.
\]

This contradiction shows that the sum in the expression of \( \tilde{b}(q, v) \) is empty and, therefore, \( \tilde{b}(0, v) = 0 \) for \( v \geq 1 \), which is identical to \( b(0, v) \) given in Lemma 5. Next, we notice that in case \( v = q \), the summation in the expression of \( \tilde{b}(q, v) \) is over one tuple only, \( (k_0, k_1) \) with \( k_0 = 0 \) and \( k_1 = q + 2 \), while the product is empty, and hence equals one. This verifies that \( \tilde{b}(q, q) = q! \), which is also identical to \( b(q, q) \) given in Lemma 5. Finally, we verify the recursion

\[
\tilde{b}(q, v) = vb(q - 1, v - 1) - (v - 1)b(q - 1, v - 2)
\]

\( (19) \)
for \( q \geq 1 \) and \( v \geq 2 \). We notice that

\[
\begin{align*}
    v\bar{b}(q-1, v-1) &= v(-1)^{v-q}(v-1)!
    \\
    &= \sum_{0-k_0<2k_1<\cdots<2k_{v-2}<2k_{v-1}+1} \prod_{i=1}^{v-1} \frac{1}{k_i}
    \\
    &= (\prod_{i=1}^{v} \frac{1}{k_i})
    \\
    &= (\prod_{i=1}^{v-1} \frac{1}{k_i}) (v-1)
    \\
    &= \sum_{0-k_0<2k_1<\cdots<2k_{v-2}<2k_{v-1}+1} \prod_{i=1}^{v-1} \frac{1}{k_i}
    \\
    &= \sum_{0-k_0<2k_1<\cdots<2k_{v-2}<2k_{v-1}+1} \prod_{i=1}^{v-2} \frac{1}{k_i}.
\end{align*}
\]

and that

\[
\begin{align*}
    (v-1)\bar{b}(q-1, v-2) &= (v-1)(-1)^{v-q-1}(v-2)!
    \\
    &= \sum_{0-k_0<2k_1<\cdots<2k_{v-2}<2k_{v-1}} \prod_{i=1}^{v-2} \frac{1}{k_i}
    \\
    &= (-1)^{v-q} (v-2)!
    \\
    &= \sum_{0-k_0<2k_1<\cdots<2k_{v-2}<2k_{v-1}} \prod_{i=1}^{v-2} \frac{1}{k_i}.
\end{align*}
\]

We notice that the sets of tuples \( k_0, \ldots, k_{v-2} \) over which the summations in (20) and (21) run are disjoint and their union gives the set of tuples over which the summation in the expression of \( \bar{b}(q, v) \) runs. Hence, (19) holds.

The following corollary gives values of \( b(q, v) \) for selected pairs \( (q, v) \).

**Corollary 1:** For nonnegative integers \( q \),

\[
\begin{align*}
    b(q, q) &= q! \\
    b(q, q+1) &= (q+1)\sum_{k=2}^{q+1} \frac{1}{k} \\
    b(q, 2q) &= (-1)^q \prod_{i=0}^{q-1} (2q-2i-1) \\
    b(q, v) &= 0 \text{ for } v > 2q.
\end{align*}
\]

**Proof.** The statement regarding \( b(q, q) \) follows from Lemma 5. The expression for \( b(q, q+1) \) follows readily from (18). For \( v \geq 2q \), we notice that the summation in the right hand side of (18) runs over all tuples \( 0 = k_0, k_1, \ldots, k_{v-2}, k_{v-2}+1 \) with \( v + 2 \) for which \( k_i - k_{i-1} \geq 2 \) for \( i = 1, 2, \ldots, v-1 + 1 \). For such tuples,

\[
v + 2 = k_{v-2}+1 - k_0 = \sum_{i=1}^{v-1} (k_i - k_{i-1}) \geq v - 1.
\]

Hence, for \( v > 2q \), the sum in the expression of \( b(q, v) \) is empty and \( b(q, 2q) = 0 \). For \( v = 2q \), the summation is over one tuple only for which \( k_i = 2i \) for \( i = 0, 1, \ldots, q + 1 \). This proves the expression of \( b(q, 2q) \).

Combining Lemmas 4, 5, and 6, we obtain the major result of this paper.

**Theorem 2:** Let \( H \) be an \( m \times (2^m-1) \) parity-check matrix of a Hamming code of length \( n = 2^m - 1 \). Then, for \( l = 0, 1, \ldots, 2^m - 1 \),

\[
S_l = \frac{1}{\Pi_{q=0}^l} \sum_{v=q}^{\min(2^l, l)} (-1)^v \binom{l}{v} b(q, v) (2^l - q - (l - v))^m
\]

where \( b(q, v) \) is given in Lemma 6. In particular, for a fixed value of \( l \geq 3 \), \( S_l \) behaves asymptotically as a function of the code length \( n \) as

\[
S_l \sim \frac{n^{\log_2(2^l - l)}}{l!}.
\]

It is interesting to compare the asymptotic expression of \( S_l \) with that of \( A_l \), the number of codewords of weight \( l \) in a Hamming code of length \( n = 2^m - 1 \), where \( l \leq 3 \), which can be derived from [4] as

\[
A_l \sim \frac{n^{l-1}}{l!}.
\]

Direct application of Theorem 2 gives the following results including the expression of \( S_3 \) in (5) stated by McEliece [5]

\[
\begin{align*}
    S_0 &= 1, S_1 = S_2 = 0, \\
    S_3 &= \frac{1}{6} (5^m - 3 \times 3^m + 2 \times 2^m), \\
    S_4 &= \frac{1}{24} (12^m - 6 \times 6^m - 4 \times 5^m + 3 \times 4^m \\
    &\quad + 20 \times 3^m - 14 \times 2^m), \\
    S_5 &= \frac{1}{120} (27^m - 10 \times 13^m - 5 \times 12^m \\
    &\quad + 15 \times 7^m + 50 \times 6^m + 20 \times 5^m \\
    &\quad - 35 \times 4^m - 130 \times 3^m + 94 \times 2^m).
\end{align*}
\]

Furthermore, if \( S_m(x) \) denotes the stopping set enumerator for the full-rank parity-check matrix of a Hamming code of length \( 2^m - 1 \), then

\[
\begin{align*}
    S_3(x) &= 1 + 10x^3 + 23x^4 + 21x^5 + 7x^6 + x^7, \\
    S_4(x) &= 1 + 69x^3 + 526x^4 + 1979x^5 + 4332x^6 + 6211x^7 \\
    &\quad + 6403x^8 + 5005x^9 + 3003x^{10} + 1365x^{11} \\
    &\quad + 45x^{12} + 1052x^{13} + 15x^{14} + x^{15}.
\end{align*}
\]

**ACKNOWLEDGMENT**

The authors were supported by the NSF through grants CCR-0117891 and ECS-0121469, and by STW through the McAt research project DTC.6438.

**REFERENCES**


