The Weight Distribution and Randomness of Linear Codes

K.-M. Cheung

Communications Systems Research Section

Finding the weight distributions of block codes is a problem of theoretical and practical interest. Yet the weight distributions of most block codes are still unknown except for a few classes of block codes. In this article, by using the inclusion and exclusion principle, an explicit formula is derived which enumerates the complete weight distribution of an (n,k,d) *linear code using a partially known weight distribution. This expression is analogous to the Pless power-moment identities—a system of equations relating the weight distribution of a linear code to the weight distribution of its dual code.*

Also, an approximate formula for the weight distribution of most linear (n,k,d) *codes is derived. It is shown that for a given linear* (n,k,d) *code over* GF(q), *the ratio of the number of codewords of weight* u *to the number of words of weight* u *approaches the constant* $Q = q^{-(n-k)}$ *as* u *becomes large. A relationship between the randomness of a linear block code and the minimum distance of its dual code is given, and it is shown that most linear block codes with rigid algebraic and combinatorial structure also display certain random properties which make them similar to random codes with no structure at all.*

I. Introduction

Finding the weight distribution of block codes is a problem of theoretical and practical interest. When an incomplete decoding algorithm is used (e.g., bounded distance decoding), the probabilities of correct decoding, decoding error, and decoding failure can all be expressed in terms of the code's weight enumerator [2].

Let C be a linear (n,k,d) code over $GF(q)$, and $C^{\perp}$ be its $(n,n-k,d^{\perp})$ dual code. Let G be the generator matrix of C. Let the number of codewords of weight u be denoted by A_u. MacWilliams [3] showed that the weight enumerator of the dual $C^{\perp}$ of a linear code C is given by a linear transformation of the weight enumerator of C. Pless [1] introduced the power-moment identities—a system of equations relating the weight distribution of a linear code to the weight distribution of its dual code. In this article, by using the inclusion and exclusion principle, it is shown in Section III that the complete set of A_u's, $0 \leqslant u \leqslant n$, can be generated if only the partial set of A_u's, $d \leqslant u \leqslant n-d^{\perp}$, is known.

By modifying the techniques used in the above derivation, an approximate formula for A_u of most (n,k,d) nonbinary linear codes is derived. This formula, together with the approximate formula for A_u of binary linear code derived by Kasami et al. [4], shows that the distribution $q^{-(n-k)} \binom{n}{u} (q-1)^u$ is a close approximation to A_u for most (n,k,d) codes over $GF(q)$.

The intrinsic randomness of a linear (n,k,d) block code over $GF(q)$ is implicit in the Pless identities which show that the νth binomial moment, for $\nu = 0, 1, \ldots, d^{\perp} - 1$, is independent of the code and is equal to that of the whole vector space, i.e., the $(n,n,1)$ code $(GF(q))^n$. In this article, an explicit relationship between the randomness of a linear block code and the minimum distance of its dual code is given, and it is shown that for large u,

$$\frac{\text{no. of codewords of weight } u}{\text{no. of vectors of weight } u} \rightarrow \frac{\text{total no. of codewords}}{\text{total no. of vectors}} = q^{-(n-k)} \overset{\text{def}}{=} Q \qquad (1)$$

Equation (1) states that if the vector space $(GF(q))^n$ is partitioned into weight classes according to the Hamming weights of the vectors, then the ratio of the number of codewords in a weight class to the number of vectors in that weight class approaches a constant Q, where Q is the ratio of the size of the code to the size of the whole vector space $(GF(q))^n$. This remarkable relationship shows that most linear block codes with rigid algebraic and combinatorial structure also display certain intrinsic random properties which make them similar to random codes with no structure at all.

II. Mathematical Preliminaries

In this section combinatorial and coding techniques required to derive the results in later sections are introduced.

A. Principle of Inclusion and Exclusion [5]

Let χ be a set of N objects, and $P(1), P(2), \ldots, P(u)$ be a set of u properties. Let $N(i_1, i_2, \ldots, i_r)$ be the number of objects with properties $P(i_1), P(i_2), \ldots, P(i_r)$. The number of objects $N(\emptyset)$ with none of the properties is given by

$$N(\emptyset) = N - \sum_{i} N(i) + \sum_{i_1 < i_2} N(i_1,i_2) + \ldots$$
$$+ (-1)^r \sum_{i_1 < i_2 \ldots < i_r} N(i_1, i_2, \ldots, i_r) + \ldots$$
$$+ (-1)^u N(1, 2, 3, \ldots, u) \qquad (2)$$

There are $u + 1$ terms in the RHS of Eq. (2), with the 0th term representing the total number of objects in χ. If the RHS of Eq. (2) is truncated at the rth term, where r is even, the truncated sum represents a lower bound on $N(\emptyset)$. Similarly, if the RHS of Eq. (2) is truncated at an odd term, an upper bound on $N(\emptyset)$ is obtained. Thus the maximum error magnitude introduced by the inclusion and exclusion formula by truncating the sum at the rth term does not exceed the magnitude of the rth term. This fact will be used later to upper bound the magnitude of the errors of the approximate weight distribution formula.

B. Facts on Coding Theory

A linear (n,k,d) code over $GF(q)$ can be generated by a $k \times n$ generator matrix G, not necessarily unique and such that $\text{rank}(G) = k$. Let l be the maximum number such that no l or fewer columns of G add to zero. Then

$$l \leqslant k \qquad (3)$$

Equality in Eq. (3) is achieved in the case of *maximum distance separable* (MDS) codes. Since G is the parity-check matrix of $C^{\perp}$, $I = d^{\perp} - 1$. Let $\text{col}_{i_1}, \text{col}_{i_2}, \ldots, \text{col}_{i_j}$, be any j particular columns of G, $j \leqslant l \leqslant k$. It is obvious that there exists a $k \times n$ generator matrix G' of C and a $k \times k$ nonsingular matrix K such that

$$G' = KG \qquad (4)$$

and $\text{col}_{i_1}, \text{col}_{i_2}, \ldots, \text{col}_{i_j}$ of G' form a $k \times j$ submatrix of the form $\left(\begin{smallmatrix} I \\ \cdots \\ 0 \end{smallmatrix}\right)$. This fact guarantees that the number of codewords with zeros on the i_1th, i_2th, $\ldots$, i_jth coordinates equals q^{k-j} for $j \leqslant l$.

III. Derivation of Formula

Let $\underline{c}$ be a codeword of C with Hamming weight u, $u \geqslant n - l$. Let the coordinates of $\underline{c}$ be indexed by $\{0,1, \ldots, n-1\}$. Then $\underline{c}$ has ν zeros ($\nu \leqslant l$), where $\nu = n - u$. Let V be a set of ν coordinates, $|V| = \nu$. Let $\{i_1,i_2, \ldots, i_j\} \subseteq \{0,1, \ldots, n-1\} - V$ be a set of j coordinates. Define $S(i_1,i_2, \ldots, i_j) = \{\underline{c} : \underline{c} \in C$ and $\underline{c}$ has zeros in $V \cup \{i_1,i_2, \ldots, i_j\}\}$. A codeword $\underline{c} \in S(i_1, i_2, \ldots, i_j)$ always has at least $\nu + j$ zeros. Let

$$T_j = \sum_{|V| = \nu} \sum_{i_1 < i_2 < \ldots < i_j} |S(i_1,i_2, \ldots, i_j)|$$

That is, T_j is the jth term in the inclusion and exclusion formula. From the discussion in Section II.B, the number of codewords in $S(i_1,i_2, \ldots, i_j)$ is

$$|S(i_1,i_2, \ldots, i_j)| = q^{k-\nu-j} \qquad \text{for} \qquad 0 \leqslant j \leqslant l - \nu \qquad (5)$$

There are $\binom{n}{v}$ ways to choose V from $0, 1, \ldots, n-1$ and for each choice of V there are $\binom{u}{j}$ $(u = n - v)$ ways to choose $i_1, i_2, \ldots, i_j$ from the remaining set of $u = n - v$ coordinates. Thus

$$T_j = \binom{n}{v}\binom{u}{j} q^{k-v-j} \qquad \text{for} \qquad 0 \leqslant j \leqslant l - v \tag{6}$$

For $l - v + 1 \leqslant j \leqslant n - d - v$, the number of zeros in the codewords of $S(i_1, i_2, \ldots, i_j)$ exceeds l and therefore T_j cannot be expressed using Eq. (5). In this case T_j is evaluated by counting the number of $S(i_1, i_2, \ldots, i_j)$ each codeword can contribute to. For a given v and j, the codewords that can contribute to T_j are the zero codeword and the codewords of weight $n - m, v + j \leqslant m \leqslant n - d$. For the zero codeword, there are $\binom{n}{v}$ ways of choosing V and $\binom{u}{j}$ ways of choosing the remaining j zero coordinates. For a codeword of weight $n - m$ (m zeros), $v + j \leqslant m \leqslant n - d$, there are $\binom{m}{v}$ ways to choose V and $\binom{m-v}{j}$ ways to choose the j remaining zero coordinates. There are A_{n-m} codewords of weight $n - m$. Thus

$$T_j = \binom{n}{v}\binom{u}{j} + \sum_{m=v+j}^{n-d} \binom{m}{v}\binom{m-v}{j} A_{n-m}$$

$$\text{for} \qquad l - v + 1 \leqslant j \leqslant n - d - v \tag{7}$$

For $n - d - v + 1 \leqslant j \leqslant n - v$, the number of zeros in the codewords of $S(i_1, i_2, \ldots, i_j)$ exceeds $n - d + 1$. Since the code has minimum distance d, $S(i_1, i_2, \ldots, i_j) = \{\underline{0}\}$. Thus,

$$|S(i_1, i_2, \ldots, i_j)| = 1$$

$$\text{for} \qquad n - d - v + 1 \leqslant j \leqslant n - v \tag{8}$$

As in the case for $0 \leqslant j \leqslant l - v$, there are $\binom{n}{v}$ ways to choose V and for each V there are $\binom{u}{j}$ ways to choose $i_1, i_2, \ldots, i_j$. Thus

$$T_j = \binom{n}{v}\binom{u}{j} \qquad \text{for} \qquad n - d - v + 1 \leqslant j \leqslant n - v \tag{9}$$

By the principle of inclusion and exclusion, the number of codewords of weight u (v zeros), which is denoted by A_u, is given as follows:

$$A_u = \sum_{j=0}^{u} (-1)^j T_j \tag{10}$$

Although the above derivation is based upon the assumption that $u \geqslant n - l$, it is not hard to show that Eq. (10) is indeed true for all u, $0 \leqslant u \leqslant n$. For $d \leqslant u \leqslant n - l + 1$, Eq. (10) is reduced to the identity $A_u = A_u$ (proof omitted).

It is observed from the above that only the derivation of T_j's in the range $l - v + 1 \leqslant j \leqslant n - d - v$ $(l + 1 \leqslant v + j \leqslant n - d$, where $v + j$ is the number of zeros in a codeword) requires prior knowledge of A_{n-m}'s (weight enumerator of codewords with m zeros), where $v + j \leqslant m \leqslant n - d$. Thus the complete set of A_u's, $0 \leqslant u \leqslant n$, can be generated if only the partial set of A_u's, $d \leqslant u \leqslant n - d^{\perp}$, is known. An example which generates the weight distribution of the (7,4) Hamming code is given in Appendix A.

The above results are summarized in the following theorem and corollary.

Theorem 1. If C is an (n,k,d) code over $GF(q)$, then

$$A_u = \sum_{j=0}^{u} (-1)^j T_j \qquad \text{for} \qquad n - d^{\perp} + 1 \leqslant u \leqslant n$$

where

$$T_j = \binom{n}{v}\binom{u}{j} q^{k-v-j} \qquad \text{for} \qquad 0 \leqslant j \leqslant l - v$$

$$T_j = \binom{n}{v}\binom{u}{j} + \sum_{m=v+j}^{n-d} \binom{m}{v}\binom{m-v}{j} A_{n-m}$$

$$\text{for} \qquad l - v + 1 \leqslant j \leqslant n - d - v$$

$$T_j = \binom{n}{v}\binom{u}{j} \qquad \text{for} \qquad n - d - v + 1 \leqslant j \leqslant n - v$$

Corollary 1. If A_u, $d \leqslant u \leqslant n - d^{\perp}$, of an (n,k,d) linear code C over $GF(q)$ are given, the remaining A_u's, $n - d^{\perp} + 1 \leqslant u \leqslant n$, can be evaluated explicitly using the equations given in Theorem 1.

IV. Approximate Formula

Theorem 1 and Corollary 1 in Section III enable one to enumerate the complete weight distribution A_u, $0 \leqslant u \leqslant n$, given that the partial set of A_u, $d \leqslant u \leqslant n - d^{\perp}$, is known. This partial set of A_u is required in the calculation of T_j, $l - v + 1 \leqslant j \leqslant n - d - v$. In cases in which knowledge of this partial set is not available, one can still derive an approximate formula for A_u as follows. For a given coordinate set V, $|V| = v$, let A'_V denote the number of codewords with exactly v zeros in V.

Using a similar derivation as in Section III, A'_V can be represented by the inclusion and exclusion principle as follows:

$$\begin{aligned} A'_V &= |S(\emptyset)| + (-1) \sum_{i_1} |S(i_1)| + \dots \\ &\quad + (-1)^r \sum_{i_1<i_2<\dots<i_r} |S(i_1, i_2, \dots, i_r)| + \dots \\ &\quad + (-1)^{n-v} S(i_1, i_2, \dots, i_{n-v}) \\ &= \sum_{j=0}^{l-v} (-1)^j \binom{u}{j} q^{k-v-j} \\ &\quad + \sum_{j=l-v+1}^{n-d-v} (-1)^j \sum_{i_1<i_2<\dots<i_j} |S(i_1, i_2, \dots, i_j)| \\ &\quad + \sum_{j=n-d-v+1}^{n-v} (-1)^j \binom{u}{j} \end{aligned} \qquad (11)$$

If the above inclusion and exclusion formula is truncated at the $(l - v)$th term, Eq. (7) is reduced to

$$A'_V = \sum_{j=0}^{l-v-1} (-1)^j \binom{u}{j} q^{k-v-j} + E_1 \qquad (12)$$

where

$$\begin{aligned} E_1 &= (-1)^{l-v} \binom{u}{l-v} q^{k-l} \\ &\quad + \sum_{j=l-v+1}^{n-d-v} \sum_{i_1<i_2<\dots<i_j} (-1)^j |S(i_1, i_2, \dots, i_j)| \\ &\quad + \sum_{j=n-d-v+1}^{n-v} (-1)^j \binom{u}{j} \end{aligned}$$

From the discussion in Section II.A, $|E_1| \leq \binom{u}{l-v} q^{k-l}$. If

$$E_2 = \sum_{j=l-v}^{u} (-1)^j \binom{u}{j} q^{k-v-j}$$

is added to and subtracted from Eq. (12), one has

$$A'_V = \frac{(q-1)^u}{q^{n-k}} + E_1 + E_2 \qquad (13)$$

If $\binom{u}{l-v} q \geqslant \binom{u}{l-v+1}$, that is, if $u \geqslant [(q+1)/q](n-l) - 1$, E_2 is a sum of terms with alternate signs and decreasing magnitude. Then $|E_2| \leqslant \binom{u}{l-v} q^{k-l}$. Thus

$$A'_V = \frac{(q-1)^u}{q^{n-k}} + E \qquad (14)$$

where $E = E_1 + E_2$ and $|E| \leqslant 2 \binom{u}{l-v} q^{k-l}$. A'_V can thus be approximated by $[(q-1)^u]/q^{n-k}$, and the goodness of approximation depends on how small the ratio $R = E/[(q-1)^u \times q^{-(n-k)}]$ is. By using the upper bound on $|E|$, an upper bound on this ratio is given by

$$R \leqslant \frac{2\binom{u}{n-l} q^{k-l}}{(q-1)^u}$$

Since $v \leqslant l$, there are $\binom{n}{v} = \binom{n}{u}$ ways to choose v zeros from $\{0, 1, \dots, n-1\}$. Then A_u can be approximated by the following expression:

$$A_u = \sum_{|V|=n-u} A'_V \approx q^{-(n-k)} \binom{n}{u} (q-1)^u \qquad (15)$$

for $u \geqslant \max \{n - l, [(q+1)/q](n-l) - 1\}$.

Strictly speaking, the derivation of Eq. (15) is only valid for $u \geqslant \max \{n - l, [(q+1)/q](n-l) - 1\}$. However, it is observed that in most cases, $q^{-(n-k)} \binom{n}{u} (q-1)^u$ is also a close approximation to A_u for u considerably smaller than $n - l$ (as in the case of Reed-Solomon codes). The upper bound of R derived above has a denominator term $(q-1)^u$ and this indicates that this approximation formula is good for nonbinary linear codes, and is not useful for binary linear codes. The looseness of this approximation for binary linear codes is best illustrated by extended binary codes which only have even weights. However, it is observed that for most extended binary codes, the number of codewords of weight u, where u is even and is not close to 0 or n, can be approximated by the sum of two adjacent binomial coefficients $2^{-(n-k-1)} \binom{n-1}{u-1} + 2^{-(n-k-1)} \binom{n-1}{u}$. This is obvious since an (n,k,d) extended binary code can always be constructed from an $(n-1,k,d-1)$

binary code by appending each codeword with a parity bit. The weight distribution and its approximation for the (128, 113,6) binary extended BCH code are given in Fig. 1. In the case of binary primitive codes, Kasami et al. [4] generalized Sidel'nikov's approach [6] and showed that the weights of most binary primitive codes have approximate binomial distribution. For nonbinary linear codes, the upper bound on R shows that the approximation in Eq. (11) is particularly good for codes with large alphabet sets. The upper bound on R for the (31,15,17) Reed-Solomon code over $GF(32)$ is given in Fig. 2. The weight distribution and its approximation (using Eq. 11) of the (31,15,17) Reed-Solomon code are given in Fig. 3.

V. Randomness of a Linear Block Code

In this section, the approximation for the weight distribution of linear codes will be used to investigate the randomness of linear block codes. It was shown in [7] that in the case of MDS codes, where both the weight distribution of the codes and the weight enumerators of decodable words are known, the following relationships are obtained:

$$\frac{\text{no. of MDS codewords of weight } u}{\text{no. of vectors of weight } u} \rightarrow \frac{\text{total no. of MDS codewords}}{\text{total no. of vectors}} = q^{-(n-k)} \tag{16}$$

and

$$\frac{\text{no. of decodable words of weight } u}{\text{no. of vectors of weight } u} \rightarrow \frac{\text{total no. of decodable words}}{\text{total no. of vectors}} = q^{-(n-k)}\, V_n(t) \tag{17}$$

where $V_n(t)$ is the volume of the Hamming sphere of the codes. In this article, by using the approximation in Eq. (11), Eq. (12) is generalized to all linear block codes. That is, for an (n,k,d) linear code C,

$$\frac{\text{no. of codewords of weight } u}{\text{no. of vectors of weight } u} \approx \frac{q^{-(n-k)} \binom{n}{u} (q-1)^u}{\binom{n}{u} (q-1)^u} = q^{-(n-k)} = \frac{\text{total no. of codewords}}{\text{total no. of vectors}} \tag{18}$$

for $u \geqslant \max \{n - l, [(q+1)/q](n-l) - 1\}$. As was discussed in Section III, in the case of nonbinary block codes, the goodness of the approximation in Eq. (14) depends upon the ratio $R = E/[(q-1)^u\, q^{-(n-k)}]$, which is upper bounded by $[2\binom{u}{n-l} q^{k-l}]/(q-1)^u$. A larger weight u and/or a larger $d^\perp$ of C correspond to a better approximation of the weight distribution of C by the formula $\binom{n}{u}(q-1)^u$. This in turn implies that if $d^\perp$ of C is large, the ratio of the number of codewords of weight u to the number of words of weight u approaches $q^{-(n-k)}$ more quickly as u gets large. This result is, in some way, analogous to Pless power-moment identities [1] which state that for a linear (n,k,d) block code, there are $d^\perp$ $(0, 1, \ldots, d^\perp - 1)$ binomial moments that are independent of the code and are equal to the binomial moments of the whole vector space.

VI. Conclusion

In this article, by using the inclusion and exclusion principle, an explicit formula which enumerates the complete weight distribution of an (n,k,d) linear code using a partially known weight distribution is derived. Using similar combinatoric and coding techniques an approximate formula for the weight distribution of most linear (n,k,d) codes is derived. A relationship between the randomness of a linear block code and the minimum distance of its dual code is given, and it is shown that most linear block codes with rigid algebraic and combinatorial structure also display certain random properties which make them similar to random codes with no structure at all. The results presented can help to simplify the calculations of the probabilities of correct decoding, decoding error, and decoding failure which are all expressed in terms of the code's weight enumerator.

References

[1] V. Pless, "Power Moment Identities on Weight Distributions in Error Correcting Codes," *Info. and Control*, no. 6, pp. 147–152, 1963.

[2] E. Berlekamp, *Algebraic Coding Theory*, Laguna Hills, California: Aegean Park Press, 1984.

[3] F. MacWilliams, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977.

[4] T. Kasami, T. Fujiwara, and S. Lin, "An Approximation to the Weight Distribution of Binary Linear Codes," *IEEE Trans. Inform. Theory*, IT-31, no. 6, pp. 769–780, November 1985.

[5] R. Stanley, *Enumerative Combinatorics, Vol. I*, Monterey, California: Wadsworth and Brooks-Cole, 1986.

[6] V.M. Sidel'nikov, "Weight Spectrum of Binary Bose-Chaudhuri-Hocquenghem Codes," *Probl. Peredachi Inform.*, vol. 7, no. 1, pp. 14–22, January–March, 1971.

[7] K. Cheung, "More on the Decoder Error Probability of Reed-Solomon Codes," to appear in *IEEE Trans. Inform. Theory*.

u	Au (Exact)	A'u (Approx.)
0	1.000e+000	1.000e+000
2	0.000e+000	4.961e-001
4	0.000e+000	6.511e+002
6	3.414e+005	3.310e+005
8	8.729e+007	8.726e+007
10	1.384e+010	1.385e+010
12	1.448e+012	1.448e+012
14	1.061e+014	1.061e+014
16	5.697e+015	5.697e+015
18	2.315e+017	2.315e+017
20	7.303e+018	7.303e+018
22	1.827e+020	1.827e+020
24	3.683e+021	3.683e+021
26	6.070e+022	6.070e+022
28	8.272e+023	8.272e+023
30	9.413e+024	9.413e+024
32	9.020e+025	9.020e+025
34	7.332e+026	7.332e+026
36	5.087e+027	5.087e+027
38	3.029e+028	3.029e+028
40	1.555e+029	1.555e+029
42	6.914e+029	6.915e+029
44	2.672e+030	2.672e+030
46	8.998e+030	8.998e+030
48	2.649e+031	2.649e+031
50	6.834e+031	6.834e+031
52	1.548e+032	1.548e+032
54	3.082e+032	3.082e+032
56	5.406e+032	5.406e+032
58	8.359e+032	8.359e+032
60	1.141e+033	1.141e+033
62	1.374e+033	1.374e+033
64	1.462e+033	1.462e+033

* Au = 0 for odd u.
**Au = A_{128-u} and A'u = A'_{128-u}.

Fig. 1. Weight distribution and its approximation of the (128, 113, 6) BCH code.

u	R
16	2.74943144e-024
17	1.50775270e-024
18	4.37734673e-025
19	8.94296586e-026
20	1.44241389e-026
21	1.95423782e-027
22	2.31146419e-028
23	2.44993596e-029
24	2.37090920e-030
25	2.12446863e-031
26	1.78181347e-032
27	1.41082139e-033
28	1.06190837e-034
29	7.64152968e-036
30	5.28215447e-037
31	3.52143591e-038

Fig. 2. Upper bound on *R* for the (31, 15, 17) RS code.

u	Au (Exact)	A'u (Approx.)
0	1.000e+000	8.272e-025
1	0.000e+000	7.949e-022
2	0.000e+000	3.696e-019
3	0.000e+000	1.108e-016
4	0.000e+000	2.404e-014
5	0.000e+000	4.024e-012
6	0.000e+000	5.405e-010
7	0.000e+000	5.984e-008
8	0.000e+000	5.565e-006
9	0.000e+000	4.409e-004
10	0.000e+000	3.007e-002
11	0.000e+000	1.780e+000
12	0.000e+000	9.195e+001
13	0.000e+000	4.166e+003
14	0.000e+000	1.660e+005
15	0.000e+000	5.833e+006
16	0.000e+000	1.808e+008
17	8.221e+009	4.946e+009
18	9.591e+010	1.193e+011
19	2.629e+012	2.530e+012
20	4.676e+013	4.705e+013
21	7.646e+014	7.640e+014
22	1.076e+016	1.077e+016
23	1.306e+017	1.306e+017
24	1.349e+018	1.349e+018
25	1.171e+019	1.171e+019
26	8.380e+019	8.380e+019
27	4.811e+020	4.811e+020
28	2.130e+021	2.130e+021
29	6.832e+021	6.832e+021
30	1.412e+022	1.412e+022
31	1.412e+022	1.412e+022

Fig. 3. Weight distribution and its approximation for the (31, 15, 17) RS code over *GF*(32).

Appendix A

An Example Which Generates the Complete Weight Distribution of the (7,4,3) Hamming Code from an Incomplete Weight Distribution

This example illustrates the use of Theorem 1 to evaluate the complete weight distribution of the (7,4,3) Hamming code C. It is given that C has minimum distance $d = 3$ and $C^{\perp}$ has minimum distance $d^{\perp} = 4$. According to Theorem 1 it is also required to know the partial weight distribution A_u, $3 = d \leqslant u \leqslant n - d^{\perp} = 3$. It is given that $A_3 = 7$. A_4, A_5, A_6, and A_7 are now evaluated as follows:

1. **$u = 4$ ($\nu = 3$).** In this case T_0, T_1, T_2, T_3, and T_4 are $\binom{7}{3}\binom{4}{0}2$, $\binom{7}{3}\binom{4}{1} + \binom{4}{3}7$, $\binom{7}{3}\binom{4}{2}$, $\binom{7}{3}\binom{4}{3}$, and $\binom{7}{3}\binom{4}{4}$, respectively. Thus,

$$A_4 = 70 - 168 + 210 - 140 + 35 = 7$$

2. **$u = 5$ ($\nu = 2$).** In this case T_0, T_1, T_2, T_3, T_4, and T_5 are $\binom{7}{2}\binom{5}{0}2^2$, $\binom{7}{2}\binom{5}{1}2$, $\binom{7}{2}\binom{5}{2} + \binom{4}{2}7$, $\binom{7}{2}\binom{5}{3}$, $\binom{7}{2}\binom{5}{4}$, and $\binom{7}{2}\binom{5}{5}$, respectively. Thus,

$$A_5 = 84 - 210 + 252 - 210 + 105 - 21 = 0$$

3. **$u = 6$ ($\nu = 1$).** In this case $T_0, T_1, T_2, T_3, T_4, T_5$, and T_6 are $\binom{7}{1}\binom{6}{0}2^3$, $\binom{7}{1}\binom{6}{1}2^2$, $\binom{7}{1}\binom{6}{2}2$, $\binom{7}{1}\binom{6}{3} + \binom{4}{1}7$, $\binom{7}{1}\binom{6}{4}$, $\binom{7}{1}\binom{6}{5}$, and $\binom{7}{1}\binom{6}{6}$, respectively. Thus,

$$A_6 = 56 - 168 + 210 - 168 + 105 - 42 + 7 = 0$$

4. **$u = 7$ ($\nu = 0$).** In this case $T_0, T_1, T_2, T_3, T_4, T_5, T_6$, and T_7 are $\binom{7}{0}2^4$, $\binom{7}{1}2^3$, $\binom{7}{2}2^2$, $\binom{7}{3}2$, $\binom{7}{4} + \binom{4}{0}7$, $\binom{7}{5}$, $\binom{7}{6}$, and $\binom{7}{7}$, respectively. Thus,

$$A_7 = 16 - 56 + 84 - 70 + 42 - 21 + 7 - 1 = 1$$