COMBINATORICA
Akadémiai Kiadó — Springer-Verlag

NOTE

WEIGHT DISTRIBUTION OF TRANSLATES OF MDS CODES

P. G. BONNEAU

Received February 28, 1987
Revised May 25, 1989

The following is a particular case of a theorem of Delsarte: the weight distribution of a translate of an MDS code is uniquely determined by its first $n-k$ terms. Here an explicit formula is derived from a completely different approach.

1. Preliminaries

Let F be a finite alphabet of cardinality $q \geqq 2$. Let n be a positive integer. An MDS code C in F^n is a subset of F^n that meets the Singleton bound $d \leqq n - \log_q |C| + 1$, where d stands for the minimum Hamming distance of C, and $|X|$ denotes the cardinality of any finite set X. The code is not assumed to be linear. Everything done below applies equally to cosets of linear MDS codes, and the results obtained in that case appear to be new.

Write $k = \log_q |C|$, $P = \{1, 2, ..., n\}$. Then any k-subset I of P is a "set of information positions", i.e. given any family $(x_i)_{i \in I}$ of elements of F, there exists exactly one codeword c with $c_i = x_i$ whenever $i \in I$. In [6] Chap. 8 and 10, [7] Chap. 8 or [9] Chap. 11, one can find more on linear or nonlinear MDS codes.

Choose for convenience a distinguished element 0 in F, and write 0 for any family, with arbitrary indexing set, when its components are always 0. Of course, one does not assume that 0 is a codeword. The weight $wt(x)$ of a word $x \in F^n$ is the number of its nonzero components. Let B_w stand for the number of codewords with a given weight w. Then it is clear from Delsarte's famous paper "Four fundamental Parameters ..." [5] that the weight distribution $(B_0, B_1, ..., B_n)$ of an MDS code is uniquely determined by its first $n-k$ terms $B_0, B_1, ..., B_{n-k-1}$. The purpose of this paper is to give an explicit formula. Delsarte's approach is much more general and has proved useful in actual computations. But our formula can hardly be deduced from it. And Krawtchouk polynomials, so important in Delsarte's proof, are useless here.

AMS subject classification (1980): 94B60

2. The computation

When J is a subset of P, let C_J stand for the set of codewords vanishing on every position in J. If $J=\{i\}$ is a singleton, the shorthand notation C_i is used. A variation of the sieve formula will be applied to the C_i. Remark that a codeword has weight w if and only if there exist exactly $n-w$ positions i such that c belongs to C_i. Hence, using theorem A of [4] p. 27, one gets

$$B_w = \sum_{l=n-w}^{n} (-1)^{l+w-n} \binom{l}{n-w} S_l$$

where S_l stands for the sum of the cardinalities of the intersection of l C_i, that is

$$S_l = \sum_{|J|=l} |C_J|.$$

The problem is now to compute the S_l. To that end remark that S_l is the number of pairs (J, C), where J is a l-subset of P and c is a codeword vanishing everywhere on J. From the information position property, it is easily seen that $|C_J|=q^{k-l}$ when $l=|J|\leqq k$. In that case $S_l=\binom{n}{l}q^{k-l}$. When $l>k$, S_l is computed by mean of the beginning of the weight distribution of C. Fix a codeword c, of weight w (say). Then the number of l-subsets J of P such that c belongs to C_J is clearly $\binom{n-w}{l}$. Hence

$$S_l = \sum_{w=0}^{n-l} B_w \binom{n-w}{l}$$

and

$$B_w = \sum_{l=n-w}^{k} (-1)^{l+w-n} \binom{l}{n-w}\binom{n}{l} q^{k-l} +$$

$$+ \sum_{l=k+1}^{n} (-1)^{l+w-n} \sum_{v=0}^{n-l} \binom{l}{n-w}\binom{n-v}{l} B_v.$$

Because $\binom{l}{n-w}\binom{n}{l}=\binom{n}{w}\binom{w}{n-l}$,

$$B_w = \binom{n}{w} \sum_{l=n-w}^{k} (-1)^{l+w-n} \binom{w}{n-l} q^{k-l} +$$

$$+ \sum_{l=k+1}^{n} (-1)^{l+w-n} \sum_{v=0}^{n-l} \binom{l}{n-w}\binom{n-v}{l} B_v =$$

$$= \binom{n}{w} \sum_{j=0}^{w-d+1} (-1)^j \binom{w}{j} q^{w-d-j+1} + \sum_{j=w-d+2}^{w} (-1)^j \sum_{v=0}^{w-j} \binom{j+n-w}{j}\binom{n-v}{w-j-v} B_v.$$

3. Concluding remarks

An additional property of the above formulas may be of interest. Let us say that a sum of the form

$$s=\sum_{j=0}^{r}(-1)^j a_j$$

is alternating when the a_j are nonnegative and s lies between two consecutive partial sums, that is

$$(-1)^t\sum_{j=t}^{r}(-1)^j a_j \geqq 0$$

whenever t is an integer $0\leqq t\leqq r$. Then from the above result of combinatorial theory, the last sum is alternating (and analoguous properties hold for the other ones).

Prior work was mainly devoted to the case when 0 is a codeword. Suppose this is the case. The above results seemed to have been proved first by Marguinaud [8]. In [2] and [3] Chap. 2, the writer has studied the number of codewords that are zero on a given set S of positions and are nonzero outside S. This number was shown to depend only on $|S|$. This fact is implicitly proved in Berlekamp's book ([1] p. 431) for linear codes.

References

[1] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York (1968).

[2] P. G. Bonneau, Un Renforcement de la Formule d'Enumération des Poids des codes optimaux, *C. R. Acad. Sc. Paris*, t. 296 Série I (1983), 863, 4.

[3] P. G. Bonneau, *Codes et Combinatoire (thesis)*, Université Pierre et Marie Curie, Paris (1984).

[4] L. Comtet, *Analyse Combinatoire* (tome second) Presses Universitaires de France, Paris (1970).

[5] Ph. Delsarte, Four Fondamental Parameters of a Code and Their Combinatorial Significance, *Info. and Control*, 23 (1973), 407—438.

[6] J. Denes and A. D. Keedwell, *Latin Squares and their Applications*, Academic Press, New York (1974).

[7] W. Heise and P. Quattrocchi, *Informations- und Codierungstheorie*, Springer-Verlag, Berlin, Heidelberg New York (1983).

[8] A. Marguinaud, Codes a Distance Maximale, *Revue du Cethedec*, 22 (1970), 33—46.

[9] F. J. Mac Williams and N. J. A. Sloane, *The Theory of Error-Correcting codes* (third printing), North Holland—Amsterdam, New York, Oxford (1981).

Pierre G. Bonneau

20 rue Camot
62930 Wimereuse
France