Arch. Math., Vol. 54, 307–312 (1990)

0003-889X/90/5403-0307 $ 2.70/0

Visible codes

By

HAROLD N. WARD

Introduction. Generalized Reed-Muller codes are extended cyclic codes, and their minimum weights can be obtained from the BCH bound [5]. However, their ambient spaces have bases with the property that the minimum weight of any of the codes is the smallest weight among the words of the subset spanning it. That is, the minimum weight is visible in the members of the spanning set; moreover, this property holds for any code spanned by a subset of such a "visible" basis.

The ambient space involved is a tensor product, and this paper shows that visible bases may be formed in these spaces from visible bases for the factors. Another example of such a space is the group algebra of a p-group over a field of characteristic p; the visible basis leads to a formula for the minimum weights of powers of the radical. The numerical ingredients are certain invariants described by Jennings [4], and the result extends an old one of Berman [2]. Other connections between code properties and the work of Jennings have recently been discussed by Landrock and Manz [6] in their unification of various realizations of classical codes as ideals in group algebras. Indeed, the present paper was inspired by a visit at Aarhus University to Peter Landrock, whom I wish to thank for his hospitality.

1. Visible sets and codes. The framework used here for linear codes over a finite field F consists of an ambient F-vector space A along with a finite set L of linear functionals on A, the coding functionals. For example, when $A = F^n$, the space of n-tuples or words of length n, the coding functionals are the coordinate functions. A code is a subspace of A, and a code member c is encoded as the word of length $|L|$ (the length of the code) whose components are the values $\lambda(c)$ in some order, as λ runs through L. The weight $w(c)$ is the number of functionals that are not 0 on c. One tacitly assumes that L satisfies the coding axiom [1]: the encoding map is one-to-one. That is, L must span the dual space of A. As with F^n, coding functionals are frequently the coordinate functions for some standard basis. Thus when A is the group algebra FG of a finite group, the group G itself serves as the standard basis.

A set V in the ambient space A is called *visible* if the minimum weight of the code spanned by each nonempty subset of V is the smallest weight among the members of the subset. Alternatively, the weight of a nonzero linear combination of members of V must be at least the weight of one of its terms. The standard basis of F^n and its set of differences are visible; so is the set of generators of Reed-Solomon codes based on a chosen primitive element. The set is called visible because the minimum weight of codes spanned by subsets is indeed "visible" among the spanning members; no weight analysis of combinations is needed. The codes themselves are also called visible (with respect to V).

The Singleton bound implies that the dimension of the span of the words of weight d or more from a visible set is at most $n - d + 1$, $n = |L|$. If words of weight n and $n - 1$ are present, then $|F| \geqq n$.

2. Tensor products. When A_1, and A_2 are ambient spaces with coding functional sets L_1 and L_2, respectively, the tensor product $A_1 \otimes A_2$ over F becomes an ambient space with the functional set whose members are the products $\lambda_1 \otimes \lambda_2$ with $\lambda_i \in L_i$. If V_i is a subset of A_i, $V_1 \otimes V_2$ will denote the set of products $v_1 \otimes v_2$, where $v_i \in V_i$. (This notation seems safe since it will not be necessary to refer to tensor products of subspaces, which would be written the same way.)

Theorem. *Let A_1 and A_2 be two ambient spaces, and let V_i be a visible subset of A_j $(i = 1, 2)$. Then $V_1 \otimes V_2$ is a visible subset of $A_1 \otimes A_2$.*

Proof. Let V be a nonempty subset of $V_1 \otimes V_2$. Discarding unused members of V_1, assume that V_1 itself is the set of first factors of members of V. For each v in V_1, let $V_2(v)$ be the set of second factors with which v appears in V. Then a linear combination of members of V has the form $\sum v \otimes s(v)$, where v runs over V_1 and $s(v)$ is in the span of $V_2(v)$. Suppose a is such a combination and $a \neq 0$.

Let $\lambda \in L_1$, the set of coding functionals of A_1, and put $a(\lambda) = \sum \lambda(v) s(v)$. Then $a(\lambda) \in A_2$, and the weight of a is the sum of the weights of the $a(\lambda)$. Let N be the set of members λ in L_1 for which $a(\lambda) \neq 0$, and let $M = L_1 - N$. Then let W be the subset of members of V_1 whose weight exceeds $|N|$.

Now if $a(\lambda) \neq 0$, then $a(\lambda)$ is in the span of $\bigcup \{V_2(v) \mid v \in V_1 - W\}$. This is trivially so if $N = L_1$. To see it when $N \neq L_1$, first observe that there is a set of members $\gamma_{\lambda\mu}$ of F for which

$$\lambda(v) = \sum_{\mu \in M} \gamma_{\lambda\mu} \mu(v)$$

for all λ in N and all v in W. For if not, there would be members α_v of F, indexed by W, such that $\sum \alpha_v \mu(v) = 0$ for all μ in M, but $\sum \alpha_v \lambda(v) \neq 0$ for some λ in N (both sums over W). But then the element $\sum \alpha_v v$ in the span of W would be nonzero and have weight at most $|N|$, violating the visibility of V_1.

Then write $a(\lambda) = a(\lambda) - \sum\limits_{\mu \in M} \gamma_{\lambda\mu} a(\mu)$ for $\lambda \in N$, using the fact that the $a(\mu)$ are 0. That is,

$$\begin{aligned} a(\lambda) &= \sum_{v} \lambda(v) s(v) - \sum_{\mu \in M} \gamma_{\lambda\mu} \sum_{v} \mu(v) s(v) \\ &= \sum_{v \in V_1 - W} \Big\{\lambda(v) - \sum_{\mu \in M} \gamma_{\lambda\mu} \mu(v)\Big\} s(v), \end{aligned}$$

in the span of $\bigcup \{V_2(v) \mid v \in V_1 - W\}$ as wished. By the visibility of V_2, $w(a(\lambda)) \geqq w(v_2)$ for any member v_2 of this union having least weight. If $v_1 \in V_1 - W$ is such that $v_2 \in V_2(v_1)$, then $w(v_1) \leqq |N|$ and $w(v_1 \otimes v_2) = w(v_1) w(v_2) \leqq |N| w(v_2)$. But

$w(a) = \sum_{\lambda \in N} w(a(\lambda)) \geqq |N| \, w(v_2)$. That is, $w(a) \geqq w(v_1 \otimes v_2)$, the inequality needed to show $V_1 \otimes V_2$ visible.

3. Codes specified by heights. The tensor product theorem in Section 2 extends to products of more than two factors. Suppose $A_1, \ldots, A_m$ is a collection of ambient spaces, each A_i having a visible basis V_i, and suppose each V_i has one word of each possible nonzero weight. Let $|V_i| = q_i$ and assume $q_1 \leqq \cdots \leqq q_m$. For the tensor product $A = A_1 \otimes \cdots \otimes A_m$, with visible basis $V = V_1 \otimes \cdots \otimes V_m$, let $(w_1, \ldots, w_m)$ stand for the basis element whose i^{th} factor has weight w_i. Suppose a sequence $0 < h_1 \leqq \cdots \leqq h_m$ of heights is given, and let C_h be the code in A spanned by the members $(w_1, \ldots, w_m)$ of V for which

$$\sum h_i (w_i - 1) \geqq h .$$

The largest allowed h is $\sum h_i (q_i - 1)$; on occasion one may wish to use the "co-weights" $q_i - w_i$ and describe C_h by the inequality

$$\sum h_i (q_i - w_i) \leqq r = \sum h_i (q_i - 1) - h .$$

To obtain the minimum weight of C_h, reason as follows: suppose $(w_1, \ldots, w_m)$ displays the minimum weight, $w_1 \cdots w_m$. If $i < j$ but $w_i > w_j$, the m-tuple with w_i and w_j switched still represents a basis element, since $q_i \leqq q_j$. It is also in C_h because

$$(h_i w_j + h_j w_i) - (h_i w_i + h_j w_j) = (h_j - h_i)(w_i - w_j) \geqq 0 .$$

We can thus take $w_1 \leqq \cdots \leqq w_m$. If now $1 < w_i$ and $w_j < q_j$ for some index pair with $i < j$, then because $w_i w_j > (w_i - 1)(w_j + 1)$, w_i could be lowered by 1 and w_j raised by 1 (increasing the defining sum by $h_j - h_i$) to reduce the weight. Consequently, at the minimum weight there is an index l for which $w_i = 1$ when $i < l$ and $w_i = q_i$ when $i > l$. Such an index satisfies

$$\sum_{l+1}^{m} (q_i - 1) h_i \leqq h \leqq \sum_{l}^{m} (q_i - 1) h_i$$

(and may be taken as a or $a - 1$ if $h = \sum_{a}^{m} (q_i - 1) h_i$). Then

$$\begin{aligned} w_l &= 1 + \Big\lceil \Big(h - \sum_{l+1}^{m} (q_i - 1) h_i\Big) / h_l \Big\rceil \\ &= q_l - \Big[\Big(\sum_{l}^{m} (q_i - 1) h_i - h\Big) / h_l \Big], \end{aligned}$$

$\lceil x \rceil$ the least integer not less than x and $[x]$ the integer part. Thus

Theorem. *The minimum weight of C_h is $w_l \prod_{l+1}^{m} q_i$, with l and w_l as above.*

4. Reed-Muller codes. Forgoing some of the algebraic structure, one may assemble the generalized Reed-Muller codes over the field $GF(q)$ of q elements this way: begin with the set of polynomials of degree at most $q - 1$ in $GF(q)[X]$ as an ambient space. The coding functionals are the q evaluation maps $f(X) \to f(\alpha)$, $\alpha \in GF(q)$. Let $\alpha_1, \ldots, \alpha_q$ be a listing of the members of $GF(q)$, and let

$$f_d(X) = \prod_{i=1}^{d} (X - \alpha_i),$$

$0 \leqq d \leqq q - 1$, with $f_0 = 1$. Then $w(f_d) = q - d$. The f_d form a visible basis, because the degree of any linear combination will be the highest index appearing.

The ambient space for Reed-Muller codes in m variables is now the tensor product of m copies of the above space. If X_i is the variable for the i^{th} factor, the r^{th} order Reed-Muller code is spanned by the products

$$f_{d_1}(X_1) \cdots f_{d_m}(X_m)$$

for which $\sum d_i \leqq r$. In the notation of Section 3, $q_i = q$, $w_i = q - d_i$, $h_i = 1$, and $h = m(q-1) - r$; the d_i are the co-weights. Then $l = 1 + [r/(q-1)]$ and $w_l = q - (r - (l-1)(q-1))$. If $r = Q(q-1) + R$, with $0 \leqq R \leqq q - 2$, then $l = Q + 1$ and $w_l = q - R$. Thus by the theorem of Section 3, the minimum weight of the r^{th} order Reed-Muller code is

$$(q - R)\, q^{m-Q-1},$$

a standard result [5].

5. Modular group-algebra codes. Let $\langle g \rangle$ be a cyclic group of order p, p the characteristic of the field F, and let $F\langle g \rangle$ be the group algebra of $\langle g \rangle$ as an ambient space. Then the powers of $g - 1$ form a visible basis. To establish that, think of $F\langle g \rangle$ as the quotient ring $F[X]/(X^p - 1)$ by the map $f(X) \to f(g)$. Differentiation carries the kernel into itself, so that the formal derivative a' can be defined for $a \in F\langle g \rangle$, with the usual properties. Evidently, $w(a') = w(a) - 1$ unless the 1-coefficient of a is 0, when $w(a') = w(a)$. If $a \neq 0$, some cycling $g^i a$ of a has a nonzero 1-coefficient. These observations facilitate an induction showing that if $a = b(g-1)^t \neq 0$, then $w(a) \geqq t + 1$, and that in turn establishes the visibility.

Now suppose G is a finite p-group. The radical R of FG has codimension 1; it is the augmentation ideal, spanned by the elements $g - 1$, $g \in G$. By the theorem of Jennings [3, 4], G has a generating set $g_1, \ldots, g_m$ with these two properties:

(1) each member of G can be written uniquely in the form $g_1^{t_1} \cdots g_m^{t_m}$, with $0 \leqq t_i < p$;

(2) to each g_i there is associated a height h_i in such a way that R^h has a basis the products

$$(g_1 - 1)^{t_1} \cdots (g_m - 1)^{t_m}$$

for which $0 \leqq t_i < p$ and $\sum h_i t_i \geqq h$. Moreover, $h_1 \leqq \cdots \leqq h_m$.

The group algebra as an ambient space (but not necessarily as a group algebra) can be construed as the tensor product of copies of the group algebra $F\langle g \rangle$ above. The identifying map is given by

$$g^{t_1} \otimes \cdots \otimes g^{t_m} \to g_1^{t_1} \cdots g_m^{t_m}.$$

Moreover, the theorem of Section 2 establishes that the Jennings basis involved in the radical powers is visible. Since $w((g-1)^t) = t + 1$, the code C_h of Section 3 is R^h. Consequently, we have

Theorem. *The minimum weight of* R^h *is*

$$w_l p^{m-l}$$

where

$$(p-1)\sum_{l+1}^{m} h_i \leqq h \leqq (p-1)\sum_{l}^{m} h_i$$

and

$$w_l = 1 + \left\lceil \left(h - (p-1)\sum_{l+1}^{m} h_i\right)/h_l \right\rceil.$$

As an application, let G be an Abelian group of exponent p^e and type $(p^{e_1}, \ldots, p^{e_n})$, where $e = e_1 \geqq \cdots \geqq e_n$. Following Berman [2], let l_a be the number of exponents e_i with $e_i > a$, so that $l_0 = n$ and $l_e = 0$. The heights h_i are all equal to p^a when i is in the range

$$\sum_{j=0}^{a-1} l_j < i \leqq \sum_{j=0}^{a} l_j$$

[4, Section 6]. Then let $m_a = l_a(p-1)p^a$, and choose b so that

$$\sum_{a=b+1}^{e} m_a \leqq h < \sum_{a=b}^{e} m_a.$$

Write $h = \sum_{a=b+1}^{e} m_a + t(p-1)p^b + s$, with $t(p-1)p^b \leqq h - \sum_{a=b+1}^{e} m_a < (t+1)(p-1)p^b$. The index l is now $\sum_{a=0}^{b} l_a - t$, and $w_l = 1 + \lceil sp^{-b} \rceil$. Since $m = \sum_{a=0}^{e} l_a$, we obtain Berman's formula [2, Theorem 1.2]: the minimum weight of R^h is $p^c w_l$, where $c = \sum_{a=b+1}^{e} l_a + t$ (the largest allowed h is $\sum_{a=0}^{e} m_a$, one less than the index of nilpotency of R; for that h, $c = \sum_{a=0}^{e} l_a = m$ and $w_l = 1$. R^h is just the span of the all – 1 word [3, Chapter VIII, Corollary 2.8].)

For example, if G is cyclic, $l_a = 1$ for $a < e$, and $h_i = p^{i-1}$. Write h base p as $d_{e-1} \cdots d_0$. Then the digits d_i with $i > b$ are $p - 1$'s, while $d_b < p - 1$. Here $t = 0$ and $s = d_b \cdots d_0$. Thus $w_l = 1 + d_b$ if $d_{b-1} \cdots d_0 = 0$ and $2 + d_b$ if not. The minimum weight is $p^{e-b-1}(d_b + 1)$ or $p^{e-b-1}(d_b + 2)$, respectively.

References

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., Error-correcting codes: an axiomatic approach. Inform. and Control **6**, 315–330 (1963).

[2] S. D. Berman, On the theory of group codes. Cybernetics (1) **3**, 25–31 (1967).

[3] B. Huppert and N. Blackburn, Finite Groups II. Berlin-Heidelberg-New York 1982.

[4] S. A. Jennings, The structure of the group ring of a p-group over a modular field. Trans. Amer. Math. Soc. **50,** 175–185 (1941).

[5] T. Kasami, S. Lin and W. W. Peterson, New generalizations of the Reed-Muller codes, Part I: Primitive codes. IEEE Trans. Inform. Theory **14,** 189–199 (1968).

[6] P. Landrock and O. Manz, Classical codes as ideals in group algebras. Preprint.

Eingegangen am 1. 8. 1988

Anschrift des Autors:

Harold N. Ward
Department of Mathematics
University of Virginia
Charlottesville, Virginia 22903-3199
USA