PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 109, Number 1, May 1990

ON THE NUMBER OF SELF-DUAL BASES OF $GF(q^m)$ OVER $GF(q)$

DIETER JUNGNICKEL, ALFRED J. MENEZES, AND SCOTT A. VANSTONE

(Communicated by Andrew Odlyzko)

ABSTRACT. Let $E = GF(q^m)$ be the m-dimensional extension of $F = GF(q)$. We are concerned with the numbers $sd(m, q)$ and $sdn(m, q)$ of self-dual bases and self-dual normal bases of E over F, respectively. We completely determine $sd(m, q)$, en route giving a very simple proof for the Sempel-Seroussi theorem which states that $sd(m, q) = 0$ iff q is odd and m is even. Using results of Lempel and Weinberger and MacWilliams, we can also determine $sdn(m, p)$ for primes p.

1. INTRODUCTION

Let $E = GF(q^m)$ be the m-dimensional extension of $F = GF(q)$, the finite field with q elements. (See Lidl and Niederreiter [15] for background on finite fields.) We recall that the *trace function* $Tr: E \to F$ is defined by

$$Tr(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}; \tag{1}$$

it is well known that Tr is a linear mapping from E onto F. Moreover, setting

$$(\alpha, \beta) = Tr(\alpha\beta) \tag{2}$$

defines a nondegenerate symmetric bilinear form on E (over F), called the *trace bilinear form.* The elements $\alpha_1, \dots, \alpha_m \in E$ form a basis of E over F if and only if

$$\det A = \det \begin{pmatrix} \alpha_1 & \cdots & \alpha_m \\ \alpha_1^q & \cdots & \alpha_m^q \\ \vdots & \ddots & \vdots \\ \alpha_1^{q^{m-1}} & \cdots & \alpha_m^{q^{m-1}} \end{pmatrix} \neq 0. \tag{3}$$

Received by the editors November 3, 1988 and, in revised form, June 8, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 12E20; Secondary 12F10, 11T30.
Key words and phrases. Self-dual basis, normal basis, finite field, orthogonal matrix, circulant matrix.
The first author gratefully acknowledges the hospitality of the University of Waterloo during the time of this research.
This research was partially supported by NSERC grant #A9258.

$\overline{\alpha} = \{\alpha_1, \ldots, \alpha_m\}$ is called a *trace-orthogonal basis*, iff one has

$$Tr(\alpha_i \alpha_j) = 0, \qquad \text{for } i \neq j,\ i, j \in \{1, \ldots, m\}. \tag{4}$$

If additionally

$$\mathrm{Tr}(\alpha_i^2) = 1 \qquad \text{for } i = 1, \ldots, m, \tag{5}$$

then $\overline{\alpha}$ is called a *self-dual basis*. Finally, a basis of the form $\alpha_i = \alpha^{q^i}$ $(i = 0, \ldots, m-1)$ for some $\alpha \in E$ is called a *normal basis*. Both self-dual and normal bases (and, in particular self-dual normal bases) are useful in applications, e.g. the construction of devices for the arithmetic in finite fields (multiplication, exponentiation, discrete logarithms; e.g. see [3, 8, and 18]) and in applications to coding theory, cryptography, and the discrete Fourier transform (see [7, 6, and 4]). Thus it is not surprising that self-dual (normal) bases have found considerable interest in the literature. The first general result is the following theorem of Lempel and Seroussi [13]:

Theorem 1. *E has a trace-orthogonal basis over F. Moreover, E has a self-dual basis over F if and only if either q is even or both q and m are odd.*

In spite of a simplification by Imamura [10], the published proofs of Theorem 1 are lengthy and involved. In §2, we shall give a very simple proof for this result. This will also lead to the following new result (where $\overline{\alpha}$ is called *almost self-dual* if it satisfies (4) and, with possibly one exception, (5)).

Theorem 2. *E has an almost self-dual basis over F.*

In §3, we shall establish a formula for the number of self-dual bases of E over F:

Theorem 3. *The number $sd(m, q)$ of distinct self-dual bases of E over F is*

$$sd(m, q) = \frac{c}{m!} \prod_{i=1}^{m-1} (q^i - a_i), \tag{6}$$

where

$$c = \begin{cases} 0 & \text{if } q \text{ is odd and } m \text{ is even} \\ 1 & \text{if } q \text{ is even} \\ 2 & \text{if } q \text{ and } m \text{ are odd} \end{cases}$$

and where

$$a_i = \begin{cases} 1 & \text{if } i \text{ is even} \\ 0 & \text{if } i \text{ is odd.} \end{cases}$$

Our proof consists of observing that $sd(m, q)$ equals (for $sd(m, q) \neq 0$) the order of the orthogonal group $O(m, q)$ divided by $m!$. The special case of even valued q in Theorem 3 was already observed by Imamura [11] using a direct enumeration.

Recently, a criterion for the existence of a self-dual normal basis of E over F was obtained.

Theorem 4. *E has a self-dual normal basis over F if and only if either m is odd, or q is even and $m \not\equiv 0 \pmod 4$.*

The necessity of the condition in Theorem 4 follows, for q odd, trivially from Theorem 1; for q even, it is due to Imamura and Morii [12]. The sufficiency of the criterion was recently established by Lempel and Weinberger [14]. Using a connection between self-dual normal bases and orthogonal circulant matrices, we can quote results of MacWilliams [17] to prove the following:

Theorem 5. *Assume that q is a prime, and that either m is odd, or that $q = 2$ and $m \not\equiv 0 \pmod 4$. Let $f^*(x)$ denote the reciprocal polynomial of $f(x)$. If $(m, q) = 1$ then let $x^m - 1 = (x-1)\prod_{i=1}^{t} f_i(x) \prod_{j=t+1}^{u} g_j(x)$, where $f_i^*(x) = f_i(x)$ and $g_j(x) = h_j(x)h_j^*(x)$, $h_j(x) \neq h_j^*(x)$, and $f_i(x)$, $h_j(x)$, $h_j^*(x)$ are irreducible over F for all $i \in \{1, \dots, t\}$, $j \in \{t+1, \dots, u\}$.*

Let $\deg f_i = 2c_i$ and $\deg h_j = d_j$. Then the number $sdn(m, q)$ of distinct self-dual normal bases of E over F is given by

$$sdn(m, q) = \begin{cases} \frac{2^a}{m} \prod_{i=1}^{t}(q^{c_i}+1)\prod_{j=t+1}^{u}(q^{d_j}-1) & \text{if } (m, q) = 1 \\ \frac{1}{q} q^{(q-1)(s+b)/2} sdn(s, q) & \text{if } m = sq, \end{cases}$$

where

$$a = \begin{cases} 0 & \text{if } q = 2 \text{ and } m \not\equiv 0 \pmod 4 \\ 1 & \text{if both } q \text{ and } m \text{ are odd}, \end{cases}$$

and

$$b = \begin{cases} 0 & \text{if both } q \text{ and } m \text{ are odd} \\ 1 & \text{if } q = 2 \text{ and } s \text{ is odd.} \end{cases}$$

2. The existence of self-dual bases

In this section, we prove Theorems 1 and 2. We shall use the following well-known lemma; cf. Artin [1]:

Lemma 1. *Let $F = GF(q)$. If q is odd, then there are exactly two equivalence classes of nondegenerate symmetric bilinear forms on F^m, represented by the matrices I and $N = \mathrm{diag}(1, \dots, 1, n)$, where n is an arbitrary nonsquare in F.*

Proof of Theorem 1. We distinguish the cases q even and q odd. First, let q be even; note that then $Tr(\alpha)^2 = Tr(\alpha^2)$ for all $\alpha \in E$. Since $Tr(x) = 1$ describes a hyperplane in the affine geometry $AG(m, q)$, we may select $1 \neq \alpha_1 \in E$ with $Tr(\alpha_1^2) = 1$. Assume that we have already found $\alpha_1, \dots, \alpha_k \in E$ with $\mathrm{Tr}(\alpha_i\alpha_j) = \delta_{ij}$ for $i, j = 1, \dots, k$, $k < m$, where we also assume that $\alpha_1 + \cdots + \alpha_k \neq 1$. It is easily verified that $\alpha_1, \dots, \alpha_k$ are linearly independent over F. We want to select α_{k+1} with $Tr(\alpha_i\alpha_{k+1}) = \delta_{i,k+1}$ for $i = 1, \dots, k+1$ and $\alpha_1 + \cdots + \alpha_{k+1} \neq 1$ (except for the case $k = m-1$ when $\alpha_1 + \cdots + \alpha_{k+1} = 1$). First assume that the orthogonal complement $\langle \alpha_1, \dots, \alpha_k \rangle^{\perp}$ is contained in the hyperplane $H = \{x : Tr(x) = 0\}$; taking orthogonal complements, it is easily seen that this implies that $1 \in \langle \alpha_1, \dots, \alpha_k \rangle$. Write $1 = c_1\alpha_1 + \cdots + c_k\alpha_k$; multiplying by α_i and taking the trace shows that $c_i = 1$ for $i = 1, \dots, k$. Thus $\alpha_1 + \cdots + \alpha_k = 1$, contradicting the inductive hypothesis. Hence $\langle \alpha_1, \dots, \alpha_k \rangle^\perp$ intersects H in a subspace of dimension $m - k - 1$; thus each coset of H contains q^{m-k-1} elements. In particular, the coset $H_1 = \{x : Tr(x) = 1\}$ contains an element α_{k+1} with $Tr(\alpha_{k+1}) = 1$ and $\alpha_1 + \cdots + \alpha_k + \alpha_{k+1} \neq 1$, where $k \neq m - 1$. If $k = m - 1$ then $\langle \alpha_1, \dots, \alpha_{m-1} \rangle^\perp \cap H_1 = \{\alpha_m\}$ with $\alpha_1 + \cdots + \alpha_m = 1$.

Now assume that q is odd. As noted in the introduction, the trace bilinear form on E over F defined by (2) is a nondegenerate symmetric bilinear form. Note that, in terms of the matrix A defined in (3), the trace bilinear form is represented by the matrix

$$B = A^T A = (Tr(\alpha_i \alpha_j)), \tag{7}$$

where $\overline{\alpha} = \{\alpha_1, \dots, \alpha_m\}$ is any basis of E over F. We will have a self-dual basis of E over F if and only if the trace bilinear form may be represented by the identity matrix; Lemma 1 shows that this is equivalent to requiring that $\det B$ is a square in F (for any given basis $\overline{\alpha}$). But clearly $\det B = (\det A)^2$ is a square in E, and thus $\det B$ is a square in F if and only if $\det A$ is an element of F, i.e. iff $(\det A)^q = \det A$. Note that $(\det A)^q = \det A^{(q)}$, where $A^{(q)}$ denotes the matrix obtained from A by replacing each entry by its qth power. Thus

$$(\det A)^q = \det A^{(q)} = \det \begin{pmatrix} \alpha_1^q & \dots & \alpha_m^q \\ \alpha_1^{q^2} & \dots & \alpha_m^{q^2} \\ \vdots & \ddots & \vdots \\ \alpha_1^{q^{m-1}} & \dots & \alpha_m^{q^{m-1}} \\ \alpha_1 & \dots & \alpha_m \end{pmatrix},$$

and so $A^{(q)}$ arises from A by a cyclic permutation of the m rows. This shows that

$$(\det A)^q = (-1)^{m-1} \det A,$$

and therefore $\det A \in F$ iff m is odd, proving the theorem. $\square$

We note that for odd q, Lemma 1 always guarantees the existence of a basis $\overline{\alpha}$ for which the trace bilinear form is either represented by I or by N. Such a basis is an almost self-dual basis of E over F, which gives the proof of Theorem 2.

3. Enumeration of self-dual (normal) bases

Let $\overline{\alpha} = (\alpha_1, \dots, \alpha_m)$ be any fixed basis of E over F. Then every basis of E over F may be written in the form $\overline{\beta} = (\beta_1, \dots, \beta_m)$ with

$$\beta_i = \sum_{j=1}^{m} c_{ij}\alpha_j, \qquad (i = 1, \dots, m), \tag{8}$$

where $C = (c_{ij})$ is an invertible $(m \times m)$-matrix over F. We shall establish two lemmas which are the key to proving Theorems 3 and 5. The first of these is as follows:

Lemma 2. *Assume that $\overline{\alpha}$ is a self-dual basis. Then $\overline{\beta}$ is likewise self-dual if and only if C is an orthogonal matrix (i.e. $CC^T = C^T C = I$).*

Proof. $\overline{\beta}$ is self-dual if and only if for all $i, j = 1, \ldots, m$

$$\delta_{ij} = Tr(\beta_i \beta_j) = Tr\left(\left(\sum_{h=1}^{m} c_{ih}\alpha_h\right)\left(\sum_{k=1}^{m} c_{jk}\alpha_k\right)\right)$$
$$= \sum_{h,k=1}^{m} c_{ih}c_{jk}Tr(\alpha_h\alpha_k) = \sum_{k=1}^{m} c_{ik}c_{jk},$$

(since $\overline{\alpha}$ is self-dual), which holds if and only if $CC^T = I$. □

Corollary 1. *Denote by $O(m, q)$ the group of orthogonal $m \times m$-matrices over $GF(q)$. Then $sd(m, q) = (1/m!)|O(m, q)|$, provided that $sd(m, q) \neq 0$.*

Using the well-known formulae for the order of $O(m, q)$ then results in Theorem 3. The required result may be found in the tables of Hirschfeld [9]; an elementary derivation was given by MacWilliams [16]. (We remark that one may similarly count the number of almost self-dual bases for q odd, m even; the result will be $((q-1)/2m!)|O(m, q)|$.) We now prove our second key lemma:

Lemma 3. *Assume that $\overline{\alpha}$ is a normal basis. Then $\overline{\beta}$ is likewise normal if and only if C is a circulant matrix (i.e. $c_{i+1,j+1} = c_{ij}$ for all i and j, where indices are computed modulo m).*

Proof. By hypothesis we may write $\alpha_j = \alpha^{q^j} (j = 1, \ldots, m)$. Then

$$\beta_i = \sum_{j=1}^{m} c_{ij}\alpha^{q^j}$$

and therefore

$$\beta_i^q = \sum_{j=1}^{m} c_{ij}\alpha^{q^{j+1}}.$$

Thus we have $\beta_{i+1} = \beta_i^q$ for $i = 1, \ldots, m$ (making $\overline{\beta}$ a normal basis) if and only if

$$\beta_i^q = \sum_{j=1}^{m} c_{ij}\alpha^{q^{j+1}} = \beta_{i+1} = \sum_{j=1}^{m} c_{i+1,j}\alpha^{q^j} = \sum_{j=1}^{m} c_{i+1,j+1}\alpha^{q^{j+1}},$$

for $i = 1, \ldots, m$. Clearly this holds if and only if $c_{ij} = c_{i+1,j+1}$ for all $i, j = 1, \ldots, m$, i.e. iff C is circulant. □

Corollary 2. *The number of normal bases of E over F is $(1/m)|C(m, q)|$, where $C(m, q)$ denotes the group of invertible circulant $(m \times m)$-matrices over $GF(q)$.*

Of course, the number of normal bases is well known (see e.g. Lidl and Niederreiter [15] or Berlekamp [2]), and we refrain from restating it. Combining Lemmas 2 and 3, we get our principal result:

Corollary 3. *Assume $sdn(m, q) \neq 0$ (cf. Theorem 4). Then $sdn(m, q) = (1/m)|OC(m, q)|$, where $OC(m, q)$ denotes the group of orthogonal circulant $(m \times m)$-matrices over $GF(q)$.*

MacWilliams [17] has determined the order of $OC(m, q)$ and described a way of generating the matrices in question, provided that q is prime. Using her results in Corollary 3 then gives Theorem 5.

4. Conclusions

Self-dual and self-dual normal bases of $GF(q^m)$ over $GF(q)$ are important in a variety of applications. Using only simple techniques from linear algebra and basic facts about finite fields, we have obtained a new short proof for the existence criterion for self-dual bases. We have also enumerated such bases completely, and we enumerated self-dual normal bases if the ground field $GF(q)$ has prime order. Beth and Geiselmann [5] have recently extended MacWilliams' formulae to determine the order of $OC(m, q)$, where q is any prime power, thus completing the enumeration of self-dual normal bases.

References

1. E. Artin, *Geometric algebra*, Interscience Publishers, New York, 1957.
2. E. R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968.
3. ———, *Bit serial Reed-Solomon encoders*, IEEE Trans. Inform. Theory **IT-28** (1982), 869–874.
4. T. Beth, *Generalizing the discrete fourier transform*, Discrete Math. **56** (1985), 95–100.
5. T. Beth and W. Geiselmann, *Selbstduale Normalbasen über $GF(q)$*, Archiv. Math. (to appear).
6. W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory **IT-22** (1976), 644–654.
7. W. Fumy, *Orthogonal transform encoding of cyclic codes*, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Comput. Sci., vol. 229, Springer-Verlag, 1986, 131–134.
8. W. Geiselmann and D. Gollmann, *Symmetry and duality in normal basis multiplication*, AAECC-6 Proceedings (to appear).
9. J. W. P. Hirschfeld, *Projective geometries over finite fields*, Clarendon Press, Oxford, 1979.
10. K. Imamura, *On self-complementary bases of $GF(q^n)$ over $GF(q)$*, Trans. IECE Japan (Section E) **E66** (1983), 717–721.
11. K. Imamura, *The number of self-complementary bases of a finite field of characteristic two*, IEEE Internat. Sympos. Inform. Theory, Kobe, Japan, 1988.
12. K. Imamura and M. Morii, *Two classes of finite fields which have no self-complementary normal bases*, IEEE Internat Sympos. Inform. Theory Brighton, England, June 1985.

13. A. Lempel and G. Seroussi, *Factorization of symmetric matrices and trace-orthogonal bases in finite fields*, SIAM J. Comput. **9** (1980), 758–767.

14. A. Lempel and M. J. Weinberger, *Self-complementary normal bases in finite fields*, SIAM J. Disc. Math. **1** (1988), 193–198.

15. R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, 1987.

16. F. J. MacWilliams, *Orthogonal matrices over finite fields*, Amer. Math. Monthly **76** (1969), 152–164.

17. ——, *Orthogonal circulant matrices over finite fields and how to find them*, J. Combin. Theory **10** (1971), 1–17.

18. R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson, *Optimal normal bases in $GF(p^m)$*, Discrete Appl. Math. **22** (1988–89), 149–161.

MATHEMATISCHES INSTITUT, JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN, ARNDTSTR. 2, D-6300 GIESSEN, GERMANY

DEPARTMENT OF COMBINATORICS AND OPTIMIZATION, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO N2L 3G1 CANADA