INFORMATION AND COMPUTATION 77, 123–130 (1988)

One-Step Completely Orthogonalizable Codes from Generalized Quadrangles

BHASKAR BAGCHI AND N. S. NARASIMHA SASTRY

Mathematics and Theoretical Statistics Division, Indian Statistical Institute, 203 Barrackpore Trunk Road, Calcutta 700 035, India

For q any power of two, the dual D_q of the binary linear code spanned by the lines of the regular (q, q)-generalized quadrangle $W(q)$ is shown to be a q-error correcting one-step completely orthogonalizable code of length q^3+q^2+q+1. By a previous result (Bagchi and Sastry, 1987, *Geom. Dedicata* **22**, 137–147), the rate of D_q is at least half in the limit as $q \to \infty$. We also determine the full automorphism group and maximum weight of D_q and the minimum weight of its dual. © 1988 Academic Press, Inc.

1. INTRODUCTION

1.1. The only codes considered here are binary linear codes. Accordingly, it is convenient to identify a code word with its suport. Under this identification, vector addition is the same as set-theoretic symmetric difference, the Hamming weight of a word w is its cardinality $|w|$, and the inner product of two words is the cardinality modulo 2 of their intersection. See, e.g., Blahut (1983) or MacWilliams and Sloane (1977) for background material in coding theory.

1.2. A binary linear code A with minimum weight d is said to be *one-step completely orthogonalizable* (Blake and Mullin, 1976, p. 108) if, for each coordinate position x, there are $d-1$ words w_i, $1 \leqslant i \leqslant d-1$, in the dual code $A^{\perp}$ such that $w_i \cap w_j = \{x\}$ for $i \neq j$. It is evident that one cannot have more than $d-1$ such words through a position in the support of a weight d word of A. This notion was introduced in Massey (1963) and for more on it see (Blahut, 1983, Chapter 13; Goethals, 1973). These codes are important in practice because the full error-correcting ability of such a code can be utilized by implementing the one-step majority logic decoding procedure which is among the simplest known decding algorithms. The following seem to be the only known constructive families of binary one-step completely orthogonalizable codes: (i) duals of binary Hamming codes (MacWilliam and Sloane, 1977, p. 23); (ii) the codes constructed in

0890-5401/88 $3.00

Smith (1968) from Steiner 2-designs, discussed in the survey article by Goethals (1973); (iii) the codes constructed in Delsarte (1971) from odd-order miquelian inversive planes; and (iv) the dual of the binary linear code spanned by the lines of a projective plane of order q, q a power of two (see Weldon, 1966).

1.3. *The Construction.* For each power q of two, let C_q denote the binary linear code spanned by the lines of the unique regular (q, q)-generalized quadrangle $W(q)$ (i.e., the generalized quadrangle of order (q, q) in which every point is regular (see 5.2.1, p. 77 in Payne and Thas, 1984). Let $D_q = C_q^\perp$ be its orthogonal dual. In this paper we prove:

1.4. THEOREM. *Let $q = 2^e$, $e \geqslant 1$. Then,*

(a) *D_q is a one-step completely orthogonalizable binary linear code of length $q^3 + q^2 + q + 1$, dimension $\geqslant \frac{1}{2}q^3 + q - 1$, minimum weight $2q + 2$, and maximum weight $q^3 + q$.*

(b) *The words of minimum weight in D_q are the dual grids of $W(q)$ and the words of maximum weight in D_q are the complements of the ovoids of $W(q)$ (see 2.2 below for definitions).*

(c) *The minimum weight of $D_q^\perp$ is $q + 1$ and the words of minimum weight in $D_q^\perp$ are the lines of $W(q)$.*

(d) *Unlike $D_q^\perp$, D_q is not spanned by its minimum weight words if $q > 2$. Further, for $q > 2$, $D_q \cap D_q^\perp$ is doubly even.*

(e) *The full automorphism group of D_q is $\Gamma\,\mathrm{Sp}(4, q)$, that is, the symplectic group $\mathrm{Sp}(4, q)$ extended by a cyclic group of order e. It is transitive on the coordinate positions of D_q.*

1.5. Though the codes D_q are inferior in relative error-correcting ability to the codes mentioned in (iii) and (iv) of 1.2 above, they may still be of interest in view of their rich geometric structure on the one hand, and the paucity of one-step completely orthogonalizable codes on the other hand. Notice that in view of the inequality in 1.4(a), the rate of D_q is at least half in the limit as q goes to infinity.

1.6. Since the generalized quadrangles $W(q)$ do not have ovoids for odd prime-powers q (Theorems 3.2.1 and 3.4.1 in Payne and Thas, 1984), our Theorem 1.4 does not hold for such q. Indeed, the proof that D_q is one-step completely orthogonalizable depends on the existence of many ovoids in $W(q)$, so that q must be a power of two.

2. Preliminaries

2.1. *Generalized quadrangles.* Recall (Payne and Thas, 1984, p. 1) that an (s, t)-generalized quadrangle is a linear space (i.e., an incidence system with at most one line through any two distinct points) with $s+1$ points per line and $t+1$ lines per point, such that given a point x and a line λ off x, there is a unique line through x which meets λ. Given an (s, t)-generalized quadrangle $X=(P, L)$ and a set $A \subseteq P$, the set $A^{\perp} \subseteq P$ is defined to be the set of points which are collinear with every point in A. If x and y are two non-collinear points of X then it is easy to see that $|\{x, y\}^{\perp}| = t+1$ and $|\{x, y\}^{\perp\perp}| \leqslant t+1$. The point x is called *regular* if equality holds in the last inequality for every point y which is not collinear with x (Payne and Thea, 1984, p. 4). We say that X is regular if every point of X is regular. If that is the case, then for each pair x, y of non-collinear points, the point set $\{x, y\}^{\perp} \cup \{x, y\}^{\perp\perp}$ is called a *dual grid* of X. Note that when X is regular, a dual grid of X is nothing but the point-set of a $(1, t)$ subquadrangle of X. Thus this definition of regularity coincides with the definition in Bagchi and Sastry (1988). It is easy to see that every line meets each dual grid in 0 or 2 points.

An *ovoid* of an (s, t)-generalized quadrangle X is a set of $st+1$ points no two of which are collinear. Since X has $(s+1)\cdot(st+1)$ points and $(t+1)\cdot(st+1)$ lines, an ovoid of X may also be defined as a point-set which meets every line in a unique point (Payne and Thas, 1984, p. 12). For a point x, the *star* at x is defined to be the union of the lines through x. Thus each star meets each ovoid in 1 or $t+1$ points.

2.2. *On $W(q)$.* By a Theorem of Benson (Payne and Thas, 1984, p. 77), for each prime-power q there is a unique regular (q, q)-generalized quadrangle; it is denoted by $W(q)$. From the standard construction (Payne and Thas, 1984, p. 37) of $W(q)$, it is clear that $W(q)$ admits the classical simple group $P\,\mathrm{Sp}(4, q)$ as an automorphism group. Indeed, the full automorphism group $P\Gamma\,\mathrm{Sp}(4, q)$ of $W(q)$ is the extension of $P\,\mathrm{Sp}(4, q)$ by the automorphism group of the field of order q. From the proof of Benson's theorem one sees that $W(q)$ is canonically embedded in a copy of the projective 3-space $\mathrm{PG}(3, q)$ over the field of order q, such that the planes (projective 2-flats) of $\mathrm{PG}(3, q)$ are the stars of $W(q)$. Indeed, the lines of $W(q)$ are precisely the absolute lines of $\mathrm{PG}(3, q)$ relative to the sympletic polarity of $\mathrm{PG}(3, q)$ mapping a point x to the star at x. We shall call an ovoid of $W(q)$ an *elliptic ovoid* in case it is an elliptic quadric (Dembowski, 1968) in the ambient $\mathrm{PG}(3, q)$ (see Bagchi and Sastry, 1987, for a more detailed discussion).

2.3. *Strongly regular graphs.* We recall that a strongly regular graph with parameters (v, k, λ, μ) is a (simple, undirected, loopless) graph on v vertices which is regular of degree k in which any two distinct vertices are together adjacent with either λ or μ other vertices according as the two vertices are adjacent or not.

2.4. *Standing notations.* Throughout the rest of this paper q will stand for a power of 2 (see 1.6 above). In this case $P\,\mathrm{Sp}(4, q) = \mathrm{Sp}(4, q)$, $P\Gamma\,\mathrm{Sp}(4, q) = \Gamma\,\mathrm{Sp}(4, q)$ and $W(q)$ is self-dual (Payne and Thas, 1984, p. 43). C_q and D_q will denote the binary linear codes associated with $W(q)$ as in 1.3 above. For any set w, $|w|$ will stand for the number of elements of w. P and L will denote the set of points and lines (respectively) of $W(q)$.

3. Proof of the Main Theorem

Since q is a power of two, the following is a model of $W(q)$ in view of Theorem 3.2.1 in (Payne and Thas, 1984, p. 43). Fix a nondegenerate quadric Q in $\mathrm{PG}(4, q)$. The points and lines of $W(q)$ are the points and lines of $\mathrm{PG}(4, q)$ contained in Q. In terms of this model, the elliptic ovoids of $W(q)$ are precisely the sections of Q by hyperplanes of $\mathrm{PG}(4, q)$ which are elliptic quadrics in the hyperplane. Hence it is clear that for any two distinct elliptic ovoids θ_1, θ_2 of $W(q)$, $|\theta_1 \cap \theta_2| = 1$ or $q + 1$. Indeed, the intersection is either a singleton or a conic in dimension two. Further, it is easy to see in terms of this model that the following result is a reformulation of the case $q = 2^e$, $n = 2$ of the theorem in Hubaut and Metz (1982).

3.1. Theorem (Hubaut and Metz). *Let G_q be the graph whose vertices are the elliptic ovoids of $W(q)$, two vertices θ_1 and θ_2 being adjacent if and only if $|\theta_1 \cap \theta_2| = 1$. Then G_q is strongly regular with the parameters*

$$v = q^2(q^2 - 1)/2, \quad k = (q - 1)(q^2 + 1), \quad \lambda = (q - 1)(q + 2), \quad \mu = 2q(q - 1).$$

The following result is implicitly contained in Example 1.4(d) in Debroey and Thas (1978) attributed to Metz. We sketch a proof of this theorem since no published proof appears to be available.

3.2. Theorem (Metz). *For each point x of $W(q)$ there is a set of q elliptic ovoids of $W(q)$, any two of which are tangent at x. Indeed, any elliptic ovoid of $W(q)$ containing x belongs to exactly one such set.*

Proof. We first prove the following.

Claim. If θ_1, θ_2, θ_3 are three distinct elliptic ovoids of $W(q)$ and x is a point of $W(q)$ such that $\theta_1 \cap \theta_2 = \{x\} = \theta_1 \cap \theta_3$ then $\theta_2 \cap \theta_3 = \{x\}$.

Suppose not. Then $\theta_2 \cap \theta_3 = C$ is a conic with $x \in C$. Sp(4, q) has a subgroup (namely a copy of PGL(2, q)) which fixes both θ_2 and θ_3 and acts transitively on C as well as on $\theta_2 \backslash C$. Hence there are two constants a_1 and a_2 such that each point $y \in C$ lies on exactly a_1 elliptic ovoids of $W(q)$ tangent to both θ_2 and θ_3, whereas each point $z \in \theta_2 \backslash C$ lies on exactly a_2 such ovoids. Since by assumption there is an elliptic ovoid θ_1 tangent to both θ_2 and θ_3 at a point $x \in C$, we have $a_1 \geqslant 1$. The total number of elliptic ovoids of $W(q)$ which are tangent to both θ_2 and θ_3 is $(q+1)\,a_1 + (q^2-q)\,a_2 = \mu = 2q(q-1)$ by Theorem 3.1. Hence we have

$$(q+1)\,a_1 = (2-a_2)\,q(q-1). \tag{3.1}$$

Since the left-hand side of (3.1) is strictly positive, so is the right-hand side. Hence $a_2 = 0$ or 1. In either case $2-a_2$ is relatively prime to $q+1$. Hence $q+1$ divides $q(q-1)$, which is absurd since $q \geqslant 2$. This establishes the claim.

Now let θ_1 be any elliptic ovoid of $W(q)$ with $x \in \theta_1$. Since the stabilizer of θ_1 in Sp(4, q) is transitive on θ_1, it follows from Theorem 3.1 that exactly $k/(q^2+1) = q-1$ elliptic ovoids θ_i, $2 \leqslant i \leqslant q$, are tangent to θ_1 at x. By the claim proved above, the q ovoids θ_i, $1 \leqslant i \leqslant q$, are mutually tangent at x.

We shall also need the following result (Proposition 2 in Bagchi and Sastry (1987)):

3.3. THEOREM (Bagchi and Sastry). *The elliptic ovoids of* $W(q)$ *belong to the binary code* C_q *of* $W(q)$. (*Indeed, by Theorem* 2 *in Bagchi and Sastry,* 1987, *all the known ovoids of* $W(q)$ *belong to* C_q.)

3.4. *Proof of Theorem* 1.4. The statements regarding minimum weight words of D_q and $D_q^{\perp}$ are special cases of Theorem 2.8 in Bagchi and Sastry (1988) wherein analogous statements are proved for all regular generalized polygons. We include their proofs for completeness.

(a) By definition, D_q is a binary linear code of length q^3+q^2+q+1. The inequality $\dim(D_q) \geqslant \frac{1}{2}q^3+q-1$ is Theorem 4 in Bagchi and Sastry (1987). For any coordinate position x of D_q (i.e., any point x of $W(q)$), Theorem 3.2 guarantees the existence of q mutually tangent elliptic ovoids through x. By Theorem 3.3, the definition of ovoids and the definition of $C_q = D_q^{\perp}$, these q ovoids together with the $q+1$ lines of $W(q)$ through x constitute a set of $2q+1$ mutually tangent words of $D_q^{\perp}$ through x. Since by the following argument the minimum weight of D_q is $2q+2$, this shows that D_q is one-step completely orthogonalizable.

Let w be a nonempty word of D_q. Let $x \in w$. Let λ_i, $0 \leqslant i \leqslant q$, be the lines of $W(q)$ through x. Since each line of $W(q)$ meets w in an even number of points, there is $x_i \in \lambda_i \cap w$, $x_i \neq x$ $(0 \leqslant i \leqslant q)$. Let m_i, $1 \leqslant i \leqslant q$, be the lines other than λ_0 through x_0. There is $y_i \in m_i \cap w$, $y_i \neq x_0$ $(1 \leqslant i \leqslant q)$. Since a generalized quadrangle has no triangles, the $2q+2$ points x, x_i $(0 \leqslant i \leqslant q)$ and y_i $(1 \leqslant i \leqslant q)$ of w are distinct. Thus $|w| \geqslant 2q+2$. On the other hand, the dual grids of $W(q)$ are sets of size $2q+2$ meeting each line in 0 or 2 points, so that they are words of weight $2q+2$ in D_q. Thus the minimum weight of D_q is $2q+2$.

Let w be any word of D_q. Since each line λ of $W(q)$ has size $q+1$ and meets w in an even number of points, we have $|\lambda \cap w| \leqslant q$. Also, through each point pass $q+1$ lines and there is a total of $(q+1)(q^2+1)$ lines. Hence, counting in two ways the number n of ordered pairs (x, λ), where λ is a line and $x \in \lambda \cap w$, we get $(q+1)|w| = n \leqslant q(q+1) \cdot (q^2+1)$. Hence $|w| \leqslant q(q^2+1)$. Clearly the complements of ovoids of $W(q)$ are words of D_q attaining this bound. So the maximum weight of D_q is q^3+q.

(b) Let $w \in D_q$ with $|w| = 2q+2$. Let x and y be two non-collinear points in w (it is easy to see that one cannot have more than $q+1$ mutually collinear points of $W(q)$). Because of equality in the argument in (a) above, w must contain exactly $q+1$ points x_i, $0 \leqslant i \leqslant q$, collinear with x; further, each of the q points of w other than x, x_i $(0 \leqslant i \leqslant q)$, is collinear with all the x_i. In particular, y is collinear with each x_i. Thus $\{x, y\}^{\perp} = \{x_i : 0 \leqslant i \leqslant q\} \subseteq w$. If $u, v \in \{x, y\}^{\perp}$ then, of course, u and v are noncollinear points in w and hence $\{u, v\}^{\perp} \subseteq w$. But $W(q)$ is regular, so that $\{u, v\}^{\perp} = \{x, y\}^{\perp\perp}$. Thus $w \supseteq \{x, y\}^{\perp} \cup \{x, y\}^{\perp\perp} = w_0$ (say). But w_0 is a dual grid and its size is $2q+2 = |w|$. Hence $w = w_0$ is a dual grid. Thus the minimum weight words of D_q are the dual grids of $W(q)$.

Next let $w \in D_q$ with $|w| = q^3+q$. Then by equality in the argument in (a) above, each line meets w in q points, so that the complement of w is an ovoid of $W(q)$. Thus the maximum weight words of D_q are the complements of ovoids.

(c) Let w be a nonzero word of $D_q^{\perp}$. Fix $x \in w$. Note that (i) since the dual grids are in D_q they meet w in an even number of points, (ii) the number of dual grids of $W(q)$ containing two given (distinct) points is q or 1 according as these two points are collinear or not, and (iii) through each point pass q^2 dual grids. Hence we can estimate in two ways the number m of ordered pairs (y, δ), where δ is a dual grid through x and $y \neq x$ is a point such that $\{x, y\} \subseteq w \cap \delta$, to obtain $q^2 \leqslant m \leqslant (|w|-1)\,q$, so that $|w| \geqslant q+1$. If, further $|w| = q+1$, then this argument shows that w must be a set of $q+1$ pairwise collinear points, and hence w is a line. Thus the minimum weight of $D_q^{\perp}$ is $q+1$ and the lines of $W(q)$ are the only minimum weight words.

(d) In view of (c) and the definition of D_q, $D_q^{\perp}$ is generated by its minimum-weight words. On the other hand, an easy counting argument shows that any two of the minimum-weight words of D_q (viz. the dual grids of $W(q)$) meet in 0 or 2 points. So if D_q were spanned by its minimum weight words then it would follow that D_q is self-orthogonal: $D_q \subseteq D_q^\perp$. For $q > 2$ this implies, in view of the next paragraph, that D_q is doubly even. But this is not true: the weight $2q + 2 \equiv 2 \pmod 4$ occurs in D_q.

Let θ_0 be an elliptic ovoid of $W(q)$. Let G be a cyclic subgroup of order $q^2 + 1$ of $\mathrm{Sp}(4, q)$ such that G fixes θ_0. Define the linear transformation $\sigma: F_2^P \to F_2^P$ by $\sigma(w) = \Sigma\{g(w) \colon g \in G\}$. By Lemma 4 in Bagchi and Sastry (1987), σ maps $D_q^\perp$ into $\{\varphi, P, \theta_0, \bar{\theta}_0\}$. Here $\bar{\theta}_0$ is the complement of θ_0 in the point-set P of $W(q)$.

Since clearly $\sigma(D_q) \subseteq D_q$, it follows that

$$\sigma(D_q \cap D_q^\perp) \subseteq D_q \cap \sigma(D_q^\perp) = \{\varphi, \bar{\theta}_0\}.$$

Hence we have

$$\text{for } q > 2 \text{ and } w \in D_q \cap D_q^\perp, \qquad |\sigma(w)| \equiv 0 \pmod 4. \tag{3.2}$$

Now let w be a word of $D_q \cap D_q^\perp$. Since $D_q \cap D_q^\perp$ is self-orthogonal, $|w|$ is even. Suppose, if possible, that $|w| \equiv 2 \pmod 4$. Then $g(w)$, $g \in G$, are $q^2 + 1$ words of $D_q \cap D_q^\perp$ each of weight $2 \pmod 4$. Since $D_q \cap D_q^\perp$ is self-orthogonal, these words are pairwise orthogonal. By definition of σ, $\sigma(w)$ is the sum of these words. Thus $\sigma(w)$ is the sum of an odd number of pairwise orthogonal words each of weight $2 \pmod 4$. Hence $|\sigma(w) \equiv 2 \pmod 4$. But for $q > 2$ this contradicts (3.2). So $|w| \equiv 0 \pmod 4$ in this case. Thus for $q > 2$, $D_q \cap D_q^\perp$ is doubly even.

(e) It is obvious that the full automorphism group $\Gamma\mathrm{Sp}(4, q)$ of $W(q)$ acts as an automorphism group of D_q. On the other hand, each automorphism of D_q maps the minimum-weight words of $D_q^\perp$ into themselves and hance by (c) is an automorphism of $W(q)$. Thus $\Gamma\mathrm{Sp}(4, q)$ is the full automorphism group of D_q. It is well known that $\Gamma\mathrm{Sp}(4, q)$ acts transitively on the points of $W(q)$, i.e., on the coordinate positions of D_q.

3.5. *Remarks.* It is easy to see that D_2 is a self-orthogonal code of length 15 and dimension 5. It has 1 word of weight 0 (the empty set), 10 words of weight 6 (dual grids), 15 words of weight 8 (complements of stars), and 6 words of weight 10 (complements of ovoids). Thus equality holds in the inequality of Theorem 1.4(a) for $q = 2$; we have adhoc arguments to show that equality holds for $q = 4$ as well. Perhaps equality holds for all powers of two. Some interesting consequences of this conjecture have been discussed in Bagchi and Sastry (1987).

RECEIVED August 6, 1986; ACCEPTED July 23, 1987

References

Bagchi, B., and Sastry, N. S. N. (1988), Codes associated with generalized polygons, *Geom. Dedicata*, in press.

Bagchi, B., and Sastry, N. S. N. (1987), Even order inversive planes, generalized quadrangles and codes, *Geom. Dedicata* **22**, 137–147.

Blahut, R. E. (1983), "Theory and Practice of Error Control Codes," Addison–Wesley, Reading, MA.

Blake, I. F., and Mullin, R. C. (1976), "An Introduction to Algebraic and Combinatorial Coding Theory," Academic Press, New York/San Francisco/London.

Debroey, I., and Thas, J. A. (1978), On semi-partial geometries, *J. Combin. Theory Ser. A* **25**, 242–250.

Delsarte, P. (1971), Majority decodable codes from finite inversive planes, *Inform. and Control* **18**, 319–325.

Dembowski, P. (1968), "Finite Geometries," Springer-Verlag, Berlin/Heidelberg/New York.

Goethals, J. M. (1973), Some combinatorial aspects of coding theory, *in* "A Survey of Combinatorial Theory" (J. N. Srivastava *et al.*, Eds.), pp. 189–208, North-Holland, Amsterdam/London.

Hubaut, X., and Metz, R. (1982), A class of strongly regular graphs related to orthogonal groups, *in* "Combinatorics '81" (A. Barlotti *et al.*, Eds.), North-Holland, Amsterdam/New York/Oxford.

MacWilliams, F. J., and Sloane, N. J. A. (1977), "The Theory of Error-Correcting Codes, Part I," North-Holland, Amsterdam/New York/Oxford.

Massey, J. L. (1963), "Threshold Decoding," M. I. T. Press, Cambridge, MA.

Payne, S. E., and Thas, J. A. (1983), "Finite Generalized Quadrangles," Pitman, Boston/London/Melbourne.

Smith, K. J. C. (1968), An application of incomplete block designs to the construction of error-correcting codes, *in* Inst. Statist. Mimeo. Series Vol. **587**, Chapel Hill, NC.

Weldon, E. J., Jr. (1966), Difference set cyclic codes, *Bell System Techn. J.* **45**, 1045–1055.