Contributions to Discrete Mathematics

Volume 2, Number 1, Pages 35–42
ISSN 1715-0868

CLASSES OF CODES FROM QUADRATIC SURFACES OF *PG(3,q)*

KEITH E. MELLINGER

Abstract. We examine classes of binary linear error correcting codes constructed from certain sets of lines defined relative to one of the two classical quadratic surfaces in $PG(3, q)$. We give an overview of some of the properties of the codes, providing proofs where the results are new. In particular, we use geometric techniques to find small weight codewords, and hence, bound the minimum distance.

1. Introduction

Low-density parity-check (LDPC) codes were introduced by Gallager in the 1960's [3], and it was shown in [8] that these codes perform well with certain iterative probabilistic decoding algorithms. Quite simply, LDPC codes are defined by a sparse parity-check matrix rather than a generator matrix which is perhaps more common. In 2001, Fossorier *et al.* [7] examined classes of LDPC codes generated by incidence structures in finite geometries. Other mathematicians have since produced other LDPC codes based on various incidence structures in discrete mathematics (see [6], [9], [12], [14], for instance). A common technique in describing these codes relies on their graph theoretic representation due to Tanner [16].

In this paper, we examine five classes of binary linear error-correcting codes which may be considered as LDPC codes. Each of these codes is generated by an incidence structure in a finite projective space that involves one of the two classical quadratic surfaces in $PG(3, q)$. The incidence structure of the points and lines is used to create a matrix which we then use as the parity-check matrix for a code. We study the mathematical properties of these codes, in particular, providing geometric arguments to bound minimum distances.

Received by the editors February 10, 2006, and in revised form October 2, 2006.
2000 *Mathematics Subject Classification.* 51E20, 94A10, 05B25.
Key words and phrases. linear code, elliptic quadric, hyperbolic quadric.
Research supported in part by a Faculty Development Grant from the University of Mary Washington.

2. Preliminaries

There are two non-degenerate quadratic surfaces in $\Sigma = PG(3,q)$, the so-called hyperbolic quadric, and the elliptic quadric. It can be shown that every hyperbolic quadratic is equivalent to $\mathcal{H}$ whose projective points (w,x,y,z) satisfy the equation $wy = xz$. There are $(q+1)^2$ points of $\mathcal{H}$ that are ruled by two families of $q+1$ lines each. Every point lies on exactly two lines, one from each ruling class. The set of lines forming a ruling class is also known as a *regulus*.

Every elliptic quadric is projectively equivalent to $\mathcal{E}$ whose points satisfy $dw^2 + wx + x^2 + yz = 0$, where $1 - 4d$ is a non-square when q is odd. When q is even, we require d to have trace 1 (see Chapter 5 of [5] for more detail). One can show that $\mathcal{E}$ has q^2+1 points and exactly one tangent plane at any point on $\mathcal{E}$. Moreover, the points of $\mathcal{E}$ form a cap (*i.e.*, no three points of $\mathcal{E}$ are collinear). Any non-tangential planar cross section of $\mathcal{E}$ is an oval, a set of $q+1$ planar points, no three collinear.

One might naturally ask why finite geometry would be considered an appropriate tool for constructing linear block codes. This is quite natural and deserves some discussion. First, the use of finite geometry in constructing codes is well documented. The Reed-Muller codes, for instance, were one of the first codes used in practice. They have a natural geometric representation. In addition, as mentioned earlier, Fossorier *et al.* [7], showed that finite geometry can be used to construct LDPC codes with strong performance under iterative decoding. But why use quadratic surfaces? One reason is that the classical quadratic surfaces of $PG(3,q)$ have a considerably large automorphism group, either $PGO_+(4,q)$ or $PGO_-(4,q)$. As a result, a code constructed from the points or lines related in some natural way to the quadratic surface will naturally inherit the symmetry (*i.e.*, automorphism group) of the geometric object. Hence, constructing codes from these surfaces provides a systematic way for constructing codes with a naturally large automorphism group. One might hope that a large automorphism group may lead to efficient storage, encoding, or decoding.

3. Codes generated by a hyperbolic quadric

We construct an incidence matrix for the points and lines of $\mathcal{H}$ by labeling the columns of a matrix with the $(q+1)^2$ points of $\mathcal{H}$ and the rows with the $2q+2$ lines of $\mathcal{H}$. We place a one in position (i,j) if the line corresponding to row i is incident with the point corresponding to column j, and a zero in that position otherwise. We then obtain a matrix with row weight $q+1$, since there are $q+1$ points on every line, and column weight two, since two lines (one from each ruling class) run through every point. This yields a sparse matrix that we use to generate a low-density parity-check code. We use $\mathcal{C}^1$ to denote this class of codes generated by the hyperbolic quadric $\mathcal{H}$ of Σ. Similarly, we use C_q^1 and H_q^1 to denote a code of $\mathcal{C}^1$ and its corresponding

parity-check matrix, where q is the order of the projective space used in the construction.

For every low-density parity-check code, there is a corresponding bipartite incidence graph, commonly called the "Tanner graph" [16]. Our code $\mathcal{C}_q^1$ creates a bipartite graph with one partition class representing the points of $\mathcal{H}$, the other representing the lines of $\mathcal{H}$, and edges determined by incidence. The girth of this graph is the length of the shortest cycle and there is evidence that high girth is desirable for efficient decoding. The hyperbolic quadric is of special interest because of the girth of its Tanner graph.

Proposition 3.1. *For all q, the girth of the Tanner graph for C_q^1 is 8.*

The geometry of the hyperbolic quadric is quite structured. As a result, the geometry lends a hand in proving properties of the associated code. Showing the dimension is q^2 is a straightforward linear algebra argument. The minimum distance is determined by considering quadrangles in $\mathcal{H}$. A detailed proof for all of these results can be found in [10].

Proposition 3.2. *The code C_q^1 in $\mathcal{C}^1$ is a $[(q+1)^2, q^2, 4]$ code.*

Another class of codes $\mathcal{C}^2$ can be constructed using the points and lines of $PG(3,q)$ off the hyperbolic quadric. In this case, counting can be used to show that there are $q^3 - q$ such points and $\frac{1}{2}q^2(q-1)^2$ such lines. We can use the incidence matrix H to create two classes of codes. If we label the columns of H with the points, we obtain a code of length $q^3 - q$. The software package *Magma* was used to show that, for $q = 2, 3, 4, 5$ and 7, an optimal $[6, 4, 2]$ code, as well as $[24, 10, 4]$, $[60, 24, 12]$, $[120, 26, 24]$, and $[336, 50, 48]$ codes can all be generated in this fashion. We conjecture that these codes have dimension $q^2 + 1$ when q is odd, and *Magma* computations up to $q = 13$ confirm this statement.

We obtain the code $\overline{C}_q^2$ of length $\frac{1}{2}q^2(q-1)^2$ in the class $\overline{\mathcal{C}}^2$ if we instead use the matrix H^T. Again, *Magma* was used to show that, when $q = 3, 4$, and 5, the optimal $[18, 4, 8]$ code, as well as $[72, 36, 6]$ and $[200, 106]$ codes, are generated in this fashion. If the above conjecture on dimension is true, then we would have a corresponding result on the dimension of these codes when q is odd. Although we cannot prove much about the dimension of these codes, we can use the geometry to bound the minimum distance.

Proposition 3.3. *For q odd, the code C_q^2 in $\mathcal{C}^2$ has minimum distance d satisfying $\frac{(q-1)^2}{2} \leq d \leq q^2 - 1$.*

Proof. We exhibit a codeword whose weight is $q^2 - 1$. As the code C_q^2 has minimum distance $q^2 - 1$ for $q = 5, 7$, this bound is likely quite good. Constructing a codeword with weight w amounts to finding a set of w points off the hyperbolic quadric with the property that every line meets our point set in an even number of points. Let Q be any planar cross section of $\mathcal{H}$, a conic, and let P be a point off the hyperbolic quadric such that the lines

$\mathcal{L}$ through P meeting $\mathcal{H}$ meet $\mathcal{H}$ in exactly the points of Q. Essentially, we have a hyperbolic quadric and a quadratic cone meeting in the conic Q. Then, let S be the set of points on any line of $\mathcal{L}$ but with the points of $\mathcal{H}$ and the special point P deleted. We claim that the characteristic vector for this point set is a codeword. That is, if we create a vector with a 1 in the coordinates corresponding to the points in S (using the same labeling as in the columns of H), and 0 everywhere else, then this vector is a codeword.

Here is one way to construct such a configuration. Let $\mathcal{H}$ be the hyperbolic quadric defined by the set of points (w, x, y, z) satisfying $wy = xz$, and consider the plane π determined by the three points $(1, 0, 0, 0), (0, 0, 1, 0)$, and $(0, 1, 0, 1)$. A simple argument shows that π meets $\mathcal{H}$ in the points $Q = \{(1, x, x^2, x) : x \in GF(q)\} \cup \{(0, 0, 1, 0)\}$. Clearly, Q represents a planar conic. Now, choose $P = (0, 1, 0, -1)$. The points of S are of the form $(1, x + k, x^2, x - k)$ or $(0, 1, k, -1)$ for some $k \in GF(q)$, $k \neq 0$, and one can easily check that none of these points lies on $\mathcal{H}$. Note that the -1 is necessary here which implies that our result will only hold for odd values of q.

There are $q^2 + q + 1$ points covered by the lines of $\mathcal{L}$. With the points of $\mathcal{H}$ and the point P deleted, we have $q^2 - 1$ points remaining. Now, it is well known (see Section 15.3 of [4]) that every line meets a quadratic cone in 0, 1, 2 or $q+1$ points. Hence, we only need to show that lines meeting the cone in 1 point also meet the hyperbolic quadric. Any line m meeting the cone in a single point, say R, is necessarily in the unique tangent plane through R. In this setting, the tangent plane is defined as the plane meeting the cone in one of the lines of $\mathcal{L}$. Let g be the line of $\mathcal{L}$ that passes through R and let l be one of the ruling lines of $\mathcal{H}$ that passes through the point where g meets $\mathcal{H}$.

Now, there are $q + 1$ planes through g. One of these planes necessarily contains l. If the plane π_l that contains l and g is not the tangent plane through g, then π_l must meet the cone in a second ruling line, say g'. But then the lines l and g' necessarily meet in a point as they are both in the plane π_l. This means that the cone and the hyperbolic quadric meet in some point that is not part of the conic Q. This is a contradiction, since we assumed that the cone and $\mathcal{H}$ meet precisely in the conic Q. So, the ruling line l of $\mathcal{H}$ must lie in the tangent plane through g. Since two lines in a projective plane always meet, m must intersect one of the ruling lines of $\mathcal{H}$. Hence, it is impossible for a line skew to $\mathcal{H}$ to meet our point set S in 1 point.

We obtain the lower bound on minimum distance as follows. Through any point P off of $\mathcal{H}$, there are at least $\frac{(q-1)^2}{2} - 1$ lines skew to $\mathcal{H}$. This number is obtained by elementary counting. Now, if P were in a set of points S as defined above, then each of the lines through P would necessarily contain a second point of S. This immediately gives us at least the desired

number of points in any such set S and hence a lower bound on the minimum distance. □

Note that the above upper bound argument does not hold for q even. Our computational results for $q = 2, 4$ seem to reflect a minimum distance of $q + 2$. This seems more difficult to prove. The lower bound, however, holds for all q.

Proposition 3.4. *The code $\overline{C}_q^2$ in $\overline{\mathcal{C}}^2$ has minimum distance d satisfying $q + 2 \leq d \leq 2(q + 1)$. When q is odd, $d = 2(q + 1)$.*

Proof. Since we have interchanged the roles of points and lines in our parity check matrix, codewords now correspond to sets of *lines* with the property that every point lies on an even number of them. With this in mind, it is not difficult to construct a codeword of weight $2(q + 1)$. To do this, simply choose a hyperbolic quadric $\mathcal{H}_1$ skew to our fixed hyperbolic quadric. Such a hyperbolic quadric exists trivially because of the existence of so-called *regular spreads* in $PG(3, q)$. The ruling lines of $\mathcal{H}_1$ are all skew to $\mathcal{H}$. Now consider the characteristic vector for the set of lines of $\mathcal{H}_1$ where the coordinates are labeled just as they are on the columns of H^T. This vector is orthogonal to every row of H^T since every point lies on either 0 or 2 of these lines. Hence, this characteristic vector is a codeword.

In general, finding codewords amounts to finding sets of lines with the property that any point lies on an even number of lines from your set. If you choose one line l for your set, that immediately implies that you need to include $q+1$ more lines to meet the points of l. Hence, the minimal such set of line has size $q + 2$. It is impossible to find such a set of lines in the plane when q is odd. Hence, any such set of lines must be non-planar when q is odd. But then the smallest set of lines necessarily forms a grid in $PG(3, q)$, the smallest example of which is a hyperbolic quadric. Hence, when q is odd, the minimum distance is $2(q + 1)$. □

4. Codes generated by an elliptic quadric

We form codes $\mathcal{C}^3$ using the points off $\mathcal{E}$ along with the lines skew to $\mathcal{E}$ to create a parity-check matrix H_q^3. We label the columns of H_q^3 with the $\frac{1}{2}q^2(q^2 + 1)$ lines and the rows with the $q(q^2 + 1)$ points (reversing the roles of points and lines gives us trivial codes). Hence, the column weight of H_q^3 is $q + 1$ since there are $q + 1$ points on a line in Σ. Counting easily shows that the row weight is $\frac{1}{2}q(q + 1)$. Note that the row weight will be odd if $q \equiv 1 \pmod 4$ and even if $q \equiv 3 \pmod 4$. This seems to affect the dimension of the code, since, as a function of q, the dimension changes by 1 when q is congruent to either 1 or 3 modulo 4. When q is odd, the sum of the rows of H_q^3 is the zero vector. Hence, we can bound the dimension.

Proposition 4.1. *For q odd, the dimension of C_q^3 is at least $\frac{1}{2}q(q^2+1)(q-2)+1$.*

When q is really small, *Magma* shows that the minimum distance for these codes is 4, 8, and 6 when $q = 2, 3$, and 4, respectively. One can easily find a hyperbolic quadric skew to any elliptic quadric. As before, the characteristic vector corresponding to the $2(q+1)$ ruling lines of such a hyperbolic quadric is a codeword. Hence, we have found a codeword of weight $2(q+1)$ which gives an upper bound on the minimum distance. In this setting, however, we can say something stronger.

Proposition 4.2. *The minimum distance d for the codes C_q^3 in $\mathcal{C}^3$ is $2(q+1)$ when q is odd and $q+2$ when q is even.*

Proof. When q is odd, the argument of Proposition 3.4 can be used to show that the minimum distance is $2(q+1)$. When q is even, choose any tangent plane to the elliptic quadric $\mathcal{E}$ and let D be a dual hyperoval lying in that plane none of whose lines contains a point of $\mathcal{E}$. Here, a dual hyperoval is a set of lines, no 3 concurrent. Such sets are known to exist, but only when q is even. One can easily show that D is a set of lines in which every point lies on either 0 or 2 of these lines. So D corresponds to a codeword. As the argument of Proposition 3.4 guarantees that the minimum distance is at least $q+2$, we have shown that the minimum distance is exactly $q+2$ when q is even. □

Note that the argument does not work as nicely for the codes $\overline{C}_q^2$. This is because every plane meets a hyperbolic quadric in a conic. Hence, we would need to guarantee the existence of a dual hyperoval in a plane π, none of whose lines contain any points of a fixed conic of π. This seems more difficult to prove. Hence, we cannot strengthen Proposition 3.4 in the same way we could in the case of the elliptic quadric.

The construction of our last class of codes, denoted $\mathcal{C}^4$, arising from the elliptic quadric is a bit more involved. For this construction, we will be looking at sets of lines of $AG(4,q)$ meeting in a common point of the hyperplane $\Sigma \cong PG(3,q)$ of $PG(4,q)$. Note that any two such lines are coplanar, but do not meet. Hence, they are "parallel" in the traditional sense. Let $\mathcal{E}$ be an elliptic quadric in Σ. For the construction of this new class of codes we consider points in $AG(4,q)$ along with the set of lines of $PG(4,q)$, denoted $\mathcal{L}$, that meet Σ in a point of $\mathcal{E}$. The number of lines in our newly defined incidence structure is the number of affine lines through a point of $\mathcal{E}$, q^3, multiplied by the number of points of $\mathcal{E}$, q^2+1. Hence, there are $q^3(q^2+1) = q^5+q^3$ lines and q^4 points under consideration. We note that this incidence structure forms the "affine portion" of a generalized quadrangle (see [11] for an overview of generalized quadrangles). This connection leads to the following proposition.

Proposition 4.3. *The set of lines $\mathcal{L}$ forms a triangle-free line set of $AG(4,q)$. As a result, the corresponding Tanner graph for $\mathcal{C}_q^4$ has girth 8.*

We create the incidence matrix H_q^4 by labeling the columns of H_q^4 with the q^5+q^3 lines of $\mathcal{L}$ and the rows with the q^4 points of $AG(4,q)$. The

	Girth	Length	Dimension	Min dist d
C_q^1	8	$(q+1)^2$	q^2	4
C_q^2	6	q^3-q	$q^2+1^\dagger$, q odd	$\frac{(q-1)^2}{2} \le d$ $d \le q^2-1$, q odd
$\overline{C}_q^2$	6	$\frac{1}{2}q^2(q-1)^2$	$n-(q^3-q^2-q-1)^\dagger$, q odd	$q+2 \le d \le 2(q+1)$, q even, $2(q+1)$, q odd
C_q^3	6	$\frac{1}{2}q^2(q^2+1)$	$\ge \frac{1}{2}q(q^2+1)(q-2)+1$	$q+2$, q even $2(q+1)$, q odd
C_q^4	8	q^5+q^3	$q^5-q^4+q^3$, q odd	$2q$

TABLE 1. Summary of Parameters († – conjecture)

Code	Length	Dimension	Min dist
C_9^1	100	81	4
C_{13}^1	196	169	4
C_{17}^1	324	289	4
C_2^2	6	4	2
C_3^2	24	10	4
C_4^2	60	24	12
C_5^2	120	26	24
C_7^2	336	50	48
$\overline{C}_3^2$	18	4	8
$\overline{C}_4^2$	72	36	6
$\overline{C}_5^2$	200	106	12

Code	Length	Dimension	Min dist
C_2^3	10	4	4
C_3^3	45	17	8
C_4^3	136	92	6
C_5^3	325	196	12
C_2^4	40	25	4
C_3^4	270	189	6
C_4^4	1088	861	8

TABLE 2. Examples of codes

matrix H_q^4 has column weight q since there are $q+1$ points on every line in Σ, but we omit the one point on $\mathcal{E}$ that is deleted along with the rest of Σ.

For q odd, the dimension of these codes is $q^5-q^4+q^3$ and follows from some known results on 2-ranks (see Proposition 1.1 of [1]). In addition, we are able to determine the minimum distance exactly. An upper bound of $2q+2$ on this minimum distance follows from Theorem 3.4 of [9]. Theorem 2 of [15] improves this bound to the following.

Proposition 4.4. *The code C_q^4 in $\mathcal{C}^4$ has minimum distance $d = 2q$.*

Table 1 summarizes our theoretical results. Many of the expressions for minimum distance are proven, but some of the dimensions are conjectured. It would be nice to find geometric arguments that provide at least a bound on dimension, similar to the arguments for minimum distance. Table 2 gives a list of the parameters for some of the codes. We note that in many cases, the proven bounds are met by examples from this table.

5. Conclusion

In this paper we have provided a systematic method for constructing several classes of codes based on quadratic surfaces of $PG(3, q)$. In each case, we were able to prove some properties of the parameters of the codes using purely geometric techniques. We hope that further investigation into the geometry of these quadratic surfaces might provide a complete explanation of the coding parameters that we were unable to determine here. One property that has not been exploited is the large size of the automorphism groups for these codes. Another possible next step is to use these groups to examine some practical concerns like storage, encoding, or decoding.

References

1. A. E. Brouwer and H. A. Wilbrink, *Some 2-ranks*, Discrete Math. (1992), no. 106/107, 83–92.
2. J. Cannon and C. Playoust, *An introduction to Magma*, University of Sydney, Sydney, Australia, 1994.
3. R. G. Gallager, *Low density parity check codes*, IRE Trans. Infom. Theory **IT-8** (1962), 21–28.
4. J.W.P. Hirschfeld, *Finite projective spaces of three dimensions*, Oxford University Press, 1985.
5. ———, *Projective geometries over finite fields*, 2 ed., Oxford University Press, 1998.
6. J.-L. Kim, U. N. Peled, I. Perepelitsa, and V. Pless, *Explicit construction of families of LDPC codes of girth at least six*, 2002, pp. 1024–1031.
7. Y. Kuo, S. Lin, and M. P. C. Fossorier, *Low-density parity-check codes based on finite geometries: a rediscovery and new results*, IEEE Trans. Inform. Theory **47** (2001), no. 7, 2711–2736.
8. D. J. C. MacKay and R. M. Neal, *Near Shannon limit performance of low density parity check codes*, Electron. Lett. **32** (1996), no. 18, 1645–1646.
9. K. E. Mellinger, *LDPC codes and triangle-free line sets*, Designs, Codes, and Cryptog. **32** (2004), 341–350.
10. A. Passmore and J. Stovall, *On codes generated by quadratic surfaces of $PG(3, q)$*, Rose-Hulman Institute of Technology Undergraduate Research Journal **5** (2004).
11. S. Payne and J. Thas, *Finite generalized quadrangles*, (1984).
12. J. Rosenthal and P. O. Vontobel, *Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis*, 2000, pp. 248–257.
13. C. E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J. **27** (1948), 379–423, 623–656.
14. M. Sipser and D. A. Spielman, *Expander codes*, IEEE Trans. Inform. Theory **42** (1996), no. 6, 1710–1722.
15. J. Stovall and K. E. Mellinger, *A new class of LDPC codes in $PG(4, q)$*, ΠME Journal, to appear.
16. R. M. Tanner, *A recursive approach to low complexity codes*, IEEE Trans. Inform. Theory **IT-27** (1981), 533–547.

Department of Mathematics, University of Mary Washington,
1301 College Avenue, Trinkle Hall,
Fredericksburg, VA, USA 22401
E-mail address: kmelling@umw.edu