Linear spaces of quadrics and new good codes

Andries E. Brouwer

Abstract

A conjecture of Mario de Boer about the weights occurring in a space of quadrics is proved. Some record-breaking codes are constructed.

Let V be a vector space of dimension m over $\mathbb{F}_q$ and consider the space F of all quadratic forms on V. Then $\dim F = \binom{m+1}{2}$. If Q is a quadratic form on V with radical R, then we can define a nondegenerate form $\overline{Q}$ on V/R by $\overline{Q}(x+R) = Q(x)$ for $x \in V$. We shall call Q elliptic, parabolic or hyperbolic when $\overline{Q}$ is. The *rank* of Q is the dimension of V/R.

Theorem

For $0 \le t \le \frac{1}{2}m$ there do exist linear subspaces F_t of F such that

(i) these subspaces form a chain: $F_{t+1} \subseteq F_t$ for all t,

(ii) $\dim F_t = \binom{m+1}{2} - mt$,

(iii) all nonzero quadrics in F_t have rank at least $2t$ (indeed, the associated symmetric bilinear forms all have rank at least $2t$),

(iv) the nonzero hyperbolic quadrics in F_t have rank at least $2t+2$,

(v) if m is odd, then the elliptic quadrics in F_t have rank at least $2t+2$,

(vi) if $m = 2t$, then the nonzero quadrics in F_t are all elliptic.

Parts (i)-(iv),(vi) are due to Mario de Boer [1]. Part (v) was conjectured by him.

One may construct a linear code C from F (and C_t from F_t), by fixing one representative x in each projective point (1-space) $\langle x \rangle$ in the projective space PV, and use evaluation to get for each quadratic form $Q \in F_t$ a code word $c_Q = (Q(x))_x$. Its weight is the number of projective points outside the quadric defined by Q. Clearly, this code has word length $|PV|$ and dimension $\dim F_t$.

Received by the editors September 1997.

Communicated by Albrecht Beutelspacher.

1991 *Mathematics Subject Classification.* 51A, 51E22.

Key words and phrases. linear spaces, quadrics, codes.

Lemma

The quadric defined by Q in PV has

$$\frac{q^{m-1}-1}{q-1}+\varepsilon q^{\frac{1}{2}(m+r)-1}$$

points, where $r = \dim \operatorname{Rad} Q$ and $\varepsilon = -1, 0, 1$ when Q is elliptic, parabolic or hyperbolic, respectively.

It follows that

Corollary

For $0 \le t \le \frac{1}{2}m$ there do exist linear subcodes C_t of C with parameters

$$[\frac{q^m-1}{q-1},\ \binom{m+1}{2}-mt,\ q^{m-1}-q^{m-t-2}]$$

and these codes form a chain: $C_{t+1} \subseteq C_t$ for all t.

If m is even, then C_t has at most $m-2t+2$ nonzero weights (precisely $m+1$ if $t=0$); if m is odd, then C_t has at most $m-2t$ nonzero weights.

The smallest of these codes in fact have a larger minimum distance: if $t = \frac{1}{2}(m-1)$ then C_t has parameters

$$[\frac{q^m-1}{q-1},\ m,\ q^{m-1}]$$

and if $t=\frac{1}{2}m$ then C_t has parameters

$$[\frac{q^m-1}{q-1},\ \frac{1}{2}m,\ q^{m-1}+q^{\frac{1}{2}m-1}].$$

In these last two cases, C_t is equidistant.

(In [2] it is claimed incorrectly that for $m = 2t+1$ the code C_t is a 2-weight code.)

The code C (a 2nd order projective Reed-Muller code) is not very good, but for $t > 0$ the codes C_t are often the best codes known, given their word length and dimension. Mario de Boer conjectures that C_t has the largest possible dimension among the linear subcodes of C not containing hyperbolic quadrics of rank at most $2t$ except in case $q=2$, $m=2$, $t=1$. This would mean that in all cases C_t is the largest possible linear subcode of C with its minimum distance.

Proof (of the theorem). Take $V=\mathbb{F}_{q^m}$. Then we have

$$F=\{\sum_{i,j} a_{ij}x^{q^i}x^{q^j} \mid a_{ij}\in\mathbb{F}_{q^m},\ a_{i+1,j+1}=a_{ij}^q\}$$

where the sum is over the unordered pairs i,j in $\{0,...,m-1\}$, regarded as the additive group of integers modulo m. Let F_t be the subspace of F defined by $a_{ij}=0$ for $|i-j|<t$. Then (i) and (ii) hold.

Note that for odd m the elements of F can be written as

$$Q(x) = \mathrm{Tr}\,\Big(\sum_{0\le j<m/2} a_{0j}x^{1+q^j}\Big)$$

where Tr is the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, while if $m = 2n$ is even, we have

$$Q(x) = \mathrm{Tr}\,\Big(\sum_{0\le j<m/2} a_{0j}x^{1+q^j}\Big) + \mathrm{tr}\,(a_{0n}x^{1+q^n})$$

where tr is the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ (and $a_{0n}x^{1+q^n}$ actually lies in $\mathbb{F}_{q^n}$).

The symmetric bilinear form B corresponding to Q is given by $B(x,y) = \sum a_{ij}(x^{q^i} y^{q^j} + x^{q^j}y^{q^i}) = \mathrm{Tr}\,(xL(y))$ where $L(y) = 2a_{00}y + \sum_{j>0} a_{0j}y^{q^j}$ for all m.

We have $\mathrm{Rad}\,Q \subseteq \mathrm{Rad}\,B$, and $y \in \mathrm{Rad}\,B$ if and only if $L(y) = 0$. But if $Q \in F_t$, then $L(x) = M(x)^{q^t}$, where M has degree at most q^{m-2t}, so $|\mathrm{Rad}\,B| \le q^{m-2t}$ and $\dim \mathrm{Rad}\,B \le m - 2t$, unless $M = 0$, i.e., $B = 0$, so that q is even, $t = 0$, and Q is the square of a linear form. This proves (iii).

Each nonzero polynomial Q in F_t has degree at most $q^{m-1} + q^{m-1-t}$ and has smallest degree term of degree at least $1 + q^t$ (unless $q = 2$, $t = 0$). Put $\hat{Q}(x) = Q(x)/x^{q^t}$. Then every root of Q is a root of $\hat{Q}$ so that Q defines a quadric with at most $(q^{m-1}+q^{m-1-t}-q^t-1)/(q-1)$ projective points, and we see that F_t does not contain hyperbolic quadrics Q with $r = \dim \mathrm{Rad}\,Q \ge m-2t$. If $t = \frac{1}{2}m$, then we see that the nonzero quadrics Q in F_t have fewer than $\frac{q^{m-1}-1}{q-1}$ points, hence are all elliptic. This proves (iv) and (vi).

Assume that m is odd, and consider the field $W = \mathbb{F}_{q^{2m}}$ as a vector space of dimension m over $\mathbb{F}_{q^2}$. Each quadric $Q(x) = \sum_{k,l} b_{k,l}x^{q^{2k}}x^{q^{2l}}$ on W has restriction $\sum_{i,j} a_{i,j}x^{q^i}x^{q^j}$ to $\mathbb{F}_{q^m}$, where $a_{2k,2l} = b_{k,l}$ (subscripts modulo m). If this restriction is an elliptic (or hyperbolic) quadric with radical of dimension $m-2t$ (over $\mathbb{F}_q$), and $a_{ij} = 0$ for $|i-j| < t$, then Q is a hyperbolic quadric with radical of the same dimension, and $b_{k,l} = a_{2k,2l}$ (subscripts mod m). But for the coefficients we still need that they vanish when the indices differ by less than t, and this was lost. Choose h such that $2^h \equiv 1 \pmod{m}$. Go to the field $\mathbb{F}_{q^N}$ with $N = 2^h m$. Then the equation is the same again ($Q(x) = \sum_{i,j} a_{i,j}x^{z^i}x^{z^j}$ where $z = q^{2^h}$), and the quadric is hyperbolic. Contradiction. This proves (v). ∎

The above codes are good, as we mentioned — usually they are as good as the best codes known, given length and dimension. A little bit of fiddling yields improvements in the tables.

We can enlarge our codes by adding the all-1 vector. Let $D_t = C_t + \langle 1\rangle$. Then $\dim D_t = \dim C_t + 1$. What about the minimum distance?

The largest weight occurring in C_t is $q^{m-1}+q^{m-t-2}$ if m is odd, and $q^{m-1}+q^{m-t-1}$ if m is even. Thus, if $q = 2$ and m is odd, we find a $[2^m, \binom{m+1}{2}-mt+1, 2^{m-1}-2^{m-t-2}]$-code (extending D_t by one extra position 0 where the quadratic forms vanish and the nonzero constants do not). This is an extended BCH code.

If q is odd, then the nonzero positions of Q are partitioned into the x for which $Q(x)$ is a square and those for which it is a nonsquare. If Q is a hyperbolic or elliptic quadric, then both parts have the same size $(q^{m-1} - \varepsilon q^{\frac{1}{2}(m+r)-1})/2$. If Q is parabolic, then $Q(x)$ is a square or a non-square for $(q^{m-1} + \eta q^{(m+r-1)/2})/2$ points

x, where $\eta = \pm 1$. In particular, for $q = 3$ we find that D_t has minimum distance (at least) $3^{m-1} - (3^{m-t-1} + 1)/2$, that is $\delta = (3^{m-t-2} + 1)/2$ smaller than the minimum distance of C_t. This means that we can lengthen D_t, adding δ ones to the all-1 vector, and obtain ternary $[(3^m + 3^{m-t-2})/2, \binom{m+1}{2} - mt + 1, 3^{m-1} - 3^{m-t-2}]$- codes. For example, with $m = 5$, $t = 1$ we find ternary $[126, 11, 72]$-codes, while the current record holder was a $[126, 11, 68]$-code. It seems likely that we can do even better by adjoining a random vector to C_t, instead of the all-1 vector.

References

[1] M. A. de Boer. *Codes: Their parameters and geometry*. Ph. D. thesis, Eindhoven Univ. Techn., 1997.

[2] M. A. de Boer. Codes spanned by quadratic and Hermitian forms. *IEEE Trans. Inf. Th.* **42** (1996) 1600-1604.

A. E. Brouwer
Tech. University Eindhoven
P.O. Box 513
5600 MB Eindhoven
The Netherlands
e-mail: aeb@win.tue.nl