Discrete Mathematics 98 (1991) 29–34
North-Holland

On even codes

H.-G. Quebbemann

Universität Oldenburg, FB 6 Mathematik, Postfach 2503, W-2900 Oldenburg, Germany

Received 27 August 1987
Revised 8 March 1990

Abstract

Quebbemann, H.-G., On even codes, Discrete Mathematics 98 (1991) 29–34.

The notion of an even selforthogonal code is introduced over $\mathbb{F}_q$, $q = 2^m$, in such a way that codes with this property become ordinary even binary codes (i.e., all weights are multiples of 4) when $\mathbb{F}_q$ is identified with $\mathbb{F}_2^m$ using a selfcomplementary basis. Extended Reed–Solomon codes of rate $\leq\frac{1}{2}$ turn out to be even. Furthermore, it is shown that asymptotically good even selfdual codes arise from the class field tower method used by Serre to obtain curves with many $\mathbb{F}_q$-rational points.

1. Introduction and first results

Let $\tau(x)$ and $\varphi(x)$ denote the linear and the quadratic elementary symmetric polynomial in $x_1, \ldots, x_n$,

$$\tau(x) = \sum_i x_i, \qquad \varphi(x) = \sum_{i<j} x_i x_j.$$

Their values on an $x \in \mathbb{F}_2^n$ of weight w are w and $\binom{w}{2} \bmod 2$, so that w is divisible by 4 if and only if $\tau(x) = \varphi(x) = 0$. Now let q be a power of 2.

Definition. A linear code over $\mathbb{F}_q$ which satisfies $\tau(x) = \varphi(x) = 0$ for all codewords x is called *even* (not to say doubly-even).

An even code must be selforthogonal with respect to the inner product $x \cdot y = \sum x_i y_i$, as follows from the identity

$$\varphi(x + y) - \varphi(x) - \varphi(y) = \tau(x)\tau(y) - x \cdot y. \tag{1.1}$$

A special interest in selforthogonal codes over $\mathbb{F}_q$ comes from the obvious fact that they remain selforthogonal over $\mathbb{F}_2$ after identifying $\mathbb{F}_q$ with $\mathbb{F}_2^m$ by use of a selfcomplementary $\mathbb{F}_2$-basis, i.e., a basis $a_1, \ldots, a_m$ such that $(\lambda(a_i a_j))$ for some $\mathbb{F}_2$-linear map $\lambda : \mathbb{F}_q \rightarrow \mathbb{F}_2$ is the unit matrix (such bases always exist). As even selfdual binary codes are particularly interesting (cf. [3, Chapter 19]), the following may be noteworthy in this connection.

Theorem 1. *Let $\mathbb{F}_q$ be identified with $\mathbb{F}_2^m$ by using a selfcomplementary basis. Then the binary image of an even q-ary code is again an even code.*

Theorem 2. *For $2k \leqslant q$, $q \geqslant 4$, the $[q, k, q+1-k]$ extended Reed–Solomon code over $\mathbb{F}_q$ is even.*

Therefore RS codes of rate $\frac{1}{2}$ give even selfdual binary codes of length $m2^m$ and minimum distance at least $2^{m-1}+4$ for $m \geqslant 3$. This result had been conjectured by Pasquier [4] who verified it for $m \leqslant 5$, observing that 'extremal' codes of length 24 (the Golay code) and 64 arise.

2. Details

The same letter τ (resp. φ) will be used to denote the elementary symmetric polynomials of degree 1 (resp. 2) in different numbers of variables. Theorem 1 is only a special case of the following.

Lemma. *Let $\mathbb{F}_r$ be a subfield of $\mathbb{F}_q$, let $a_1, \ldots, a_m$ be a selfcomplementary $\mathbb{F}_r$-basis of $\mathbb{F}_q$ for the functional $\lambda : \mathbb{F}_q \to \mathbb{F}_r$, and let $x \in \mathbb{F}_q^n$ be mapped to $\bar{x} \in \mathbb{F}_r^{mn}$ with respect to this basis. Then, if $\tau(x) = 0$, we have $\tau(\bar{x}) = 0$, and $\varphi(\bar{x}) = \lambda(\varphi(x))$.*

Proof. Let $x = (x_1, \ldots, x_n)$, $x_j = x_{1j}a_1 + \cdots + x_{mj}a_m$ with $x_{ij} \in \mathbb{F}_r$, and put $x^i = (x_{i1}, \ldots, x_{in})$ for $i = 1, \ldots, m$. Let $\tau(x) = 0$. Then clearly $\tau(x^i) = 0$ for all i, and $\tau(\bar{x}) = 0$. Furthermore,

$$\begin{aligned}\varphi(\bar{x}) &= \sum_i \varphi(x^i) + \sum_{h<i} \tau(x^h)\tau(x^i) \\ &= \sum_i \varphi(x^i) = \sum_i \sum_{j<k} x_{ij}x_{ik} \\ &= \sum_{j<k} \lambda(x_j x_k) = \lambda(\varphi(x)). \qquad \square\end{aligned}$$

Recall that words of the $[q, k]$ extended RS code correspond to polynomials $f \in \mathbb{F}_q[X]$ of degree $<k$. The positions in the codeword are the elements of $\mathbb{F}_q$, and the entries are the values $f(a)$, $a \in \mathbb{F}_q$. For later purposes we prove the following generalization of Theorem 2.

Theorem 2'. *Let U be a subgroup of $\mathbb{F}_q^*$ of order $u \equiv 3 \pmod 4$. For $2k \leqslant u+1$, the code of length $u+1$ obtained by puncturing the $[q, k]$ extended RS code at all positions $a \in \mathbb{F}_q^* \setminus U$ is even.*

Proof. Let A be the union of U and 0. Let x^i, $0 \leq i < k$, denote the generators of the punctured code corresponding to the polynomials X^i. We have $x^0 \cdot x^0 = |A|\,1 = 0$ because $|A|$ is even, and for $0 < j < k$ we have

$$x^i \cdot x^j = \sum_{a \in U} a^{i+j} = 0$$

because $i + j < u$ and U is cyclic. Therefore, our code is selforthogonal. By (1.1), it remains to show that $\varphi(x^i) = 0$ for all i. This holds for $i = 0$ because $|A|$ is a multiple of 4. Now let $i > 0$, and $j = \gcd\,(i, u)$. Then $\varphi(x^i)$ is the coefficient of T^{u-2} in the polynomial

$$\prod_{a \in U} (T - a^i) = (T^{u/j} - 1)^j = T^u - T^{u-u/j} - \cdots - 1.$$

Since $i < u$, u odd, we have $u/j > 2$, and therefore $\varphi(x^i) = 0$. □

Some other examples of even selfdual q-ary codes have been worked out by Maria Dyckhoff (Diplomarbeit, Münster 1986).

3. Goppa codes

We shall now deal with algebraic-geometric Goppa codes $C_L(D, G)$ associated with divisors D and G of an algebraic function field E in one variable over $\mathbb{F}_q$ (q a power of 2). See [1] for the algebraic background, and [2] for the definition of the codes. There is an evident criterion for such a code to be selforthogonal or selfdual; cf. [9]. However, it appears to be difficult to say something about evenness in all generality. Instead we shall make rather restrictive assumptions under which this problem can be easily reduced to rational codes as considered in Section 2.

Let E be a finite Galois extension of the rational function field $K = \mathbb{F}_q(X)$. It will be assumed that $s = [E{:}K]$ is odd. Let A be a subset of $\mathbb{F}_q$ such that for each $a \in A$ there are s distinct prime divisors $P_{a1}, \ldots, P_{as}$ of E lying over p_a = zero of $X - a$. We define the divisor D as the sum of these $n = s\,|A|$ prime divisors P_{ai} (all of degree 1 over $\mathbb{F}_q$). For a prime divisor P of E let $e(P)$ denote its ramification index over K (so $e(P) - 1$ is the differential exponent). We define 'Goppa divisors'

$$G_h = h \cdot \sum_{P \mid p_\infty} e(P)P + \frac{1}{2} \sum_P (e(P) - 1)P$$

for $0 \leq h \leq \frac{1}{2}|A| - 1$ (p_∞ denotes the infinite prime of K with respect to X). If $h = \frac{1}{2}|A| - 1$, then $2G_h - D$ is just the divisor of the differential

$$\prod_{a \in A} (X - a)^{-1}\, dX,$$

and we have an $[n, \frac{n}{2}]$ code

$$C_L(D, G_h) = \{(f(P_{ai}))_{a,i} \mid f \in L(G_h)\},$$

where $L(G_h)$ = space of all $f \in E$ with divisor $\geqslant -G_h$ (or $f = 0$). Let $T: E \to K$ be the trace, and let $\Phi: E \to K$ map $f \in E$ to $\sum_{i<j} f_i f_j$, where $f_1, \ldots, f_s$ are the conjugates of f. If f is in $L(G_h)$, the corresponding codeword $\hat{f}$ satisfies

$$\tau(\hat{f}) = \sum_{a,i} f(P_{ai}) = \sum_{a \in A} (Tf)(a),$$

$$\varphi(\hat{f}) = \sum_{a \in A} (\Phi f)(a) + \sum_{a<b} (Tf)(a)(Tf)(b)$$

(here A is ordered somehow). Furthermore, Tf (resp. Φf) is a polynomial in X of degree at most h (resp. $2h$). Therefore, $C_L(D, G_h)$ will be even as soon as the rational code

$$C_L\Big(\sum_{a \in A} p_a, h \cdot p_\infty\Big)$$

is even. Theorem 2′ implies the following.

Theorem 3. *In the above situation, assume that* $0 \in A$, *and that* $U = A \setminus \{0\}$ *is a subgroup of* $\mathbb{F}_q^*$ *with* $|U| \equiv 3 \pmod 4$. *Then the code* $C_L(D, G_h)$ *is even for* $h \leqslant \frac{1}{2}|A| - 1$.

Recently Scharlau [7] has shown that there exist asymptotically good selfdual algebraic-geometric codes. Here we shall apply the above theorem to prove such a result for even selfdual codes. After Serre [8], infinite class field towers will be used to obtain the required function fields.

Assume that we have a function field $E/\mathbb{F}_q$ of genus g, and that a set S of prime divisors of degree 1 is used to construct the Goppa code C of length $n = |S|$ and rate $\frac{1}{2}$. Then the minimum distance d of C is at least $n/2 - g + 1$. Assume that this number is positive, i.e.,

$$c = \frac{n}{g-1} > 2. \tag{3.1}$$

Now let E'/E be an unramified extension of degree t in which all $P \in S$ are totally decomposed. Then the genus g' of E' and the set S' of prime divisors lying over some $P \in S$ satisfy

$$g' - 1 = t(g-1), \qquad |S'| = t\,|S|.$$

Therefore we obtain a Goppa code C' of length $n' = tn$, rate $\frac{1}{2}$, and $d' \geqslant tn(\frac{1}{2} - 1/c)$. It follows that asymptotically good codes arise if the degree t can be made arbitrarily large. We shall review how this can be achieved.

Let $\mathbb{F}_q$ have a proper subfield $\mathbb{F}_r$, $q = r^e$ (Serre treats the more difficult general case). Let l be a prime which divides $(q-1)/(r-1)$. Let B be a subset of $\mathbb{F}_q$

which is stable under $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_r)$, so that we can write

$$f_B = \prod_{b\in B} (X - b) = \prod_{i\in I} f_i$$

with irreducible polynomials $f_i \in \mathbb{F}_r[X]$. Assume that l does not divide $|B|$. Then the field

$$E_B = K(\sqrt[l]{f_B})$$

is ramified over $K = \mathbb{F}_q(X)$ at all $X - b$, $b \in B$, and at infinity; its genus is

$$g = \frac{1}{2}(l-1)(|B|-1).$$

Furthermore, $E'_B =$ compositum of all $K(\sqrt[l]{f_i})$, $i \in I$, is unramified over E_B. Each $X - a$ with $a \in \mathbb{F}_r$, $a \notin B$, is totally decomposed in E'_B (because $f_i(a) \in \mathbb{F}_r^*$ for all i, and $\mathbb{F}_r^* \subset (\mathbb{F}_q^*)^l$ by the choice of l). Let A be a subset of $\mathbb{F}_r$ which is disjoint from B, and let S be the set of prime divisors of E_B lying over primes $X - a$, $a \in A$. Then the maximal unramified elementary-abelian l-extension of E_B in which all $P \in S$ are totally decomposed (cf. Rosen [6]) has l-rank $\geqslant |I| - 1$ (it contains E'_B). After Golod–Shafarevich, repeated construction of Hilbert l-class fields leads to arbitrarily large unramified extensions of E_B with all $P \in S$ totally decomposed, if the following condition is satisfied:

$$|S| \leqslant \frac{1}{4}(|I|-1)^2 - (|I|-1). \tag{3.2}$$

(See Roquette [5, p. 235]. The proof given there for number fields carries over completely if 'infinite prime' is translated into '$P \in S$'.) Recall that we also had the condition (3.1) saying

$$|S| \geqslant (l-1)(|B|-1) - 1. \tag{3.1$'$}$$

Of course, $|S| = l\,|A|$. Let us now specialize to the case $q = r^2$ and take $l = 3$, which requires $r = 2^m$ with m odd. If we forget about the restriction on A from Theorem 3, the best choice of A and B would be as complementary subsets of $\mathbb{F}_r$. But in conformity with that restriction we shall take $A = \mathbb{F}_r$ and $B \subset \mathbb{F}_q \setminus \mathbb{F}_r$, so that all f_i have degree 2 and $|B| = 2\,|I|$. Then it is checked at once that (3.1′) and (3.2) can be satisfied for $m \geqslant 5$.

Theorem 4. *For $q = r^2$, $r = 2^m$, $m \geqslant 5$ odd, asymptotically good families of even selfdual Goppa codes arise over $\mathbb{F}_q$ by the method above. More precisely, if $|I|$ is chosen as small as (3.2) (with $|S| = 3r$) allows, the codes have length $N = 3rt$, $t \to \infty$, and relative minimal distance*

$$\frac{d}{N} \geqslant \frac{1}{2} - \frac{1}{c}, \qquad c = \frac{3r}{2\,|I| - 2} \sim \frac{1}{4}\sqrt{3r}.$$

Remarks. (1) After Theorem 1 we can also obtain asymptotically good even selfdual codes over $\mathbb{F}_2$. The best lower bound found in this way for the binary relative minimal distance is, however, only about 0.02 (using $r = 2^9$, $|I| = 82$). Even if the better modular curves could be used, one would stay around 0.05 which is still far below the Gilbert–Varshamov bound.

(2) The choice $B = b + \mathbb{F}_r$ with some $b \in \mathbb{F}_q \backslash \mathbb{F}_r$ (possible for $m \geqslant 7$) has the peculiarity that f_B is invariant under the automorphisms $X \mapsto X + a$, $a \in \mathbb{F}_r$, of K. So these automorphisms extend to E_B and, moreover, to the whole class field tower. One then obtains group codes (i.e., codes with a group of automorphisms acting regularly on the positions) which are asymptotically good.

(3) Let us finally see what comes out for $q = r^e$ where e is any fixed prime. Again we require that $r = 2^m$ with m not divisible by e. Let l be a prime factor of $2^e - 1$. Then l divides $(q-1)/(r-1)$, and everything works as before: If m is sufficiently large, we can take $A = \mathbb{F}_r$, $|B| = e\,|I|$, $|I| \sim 2\sqrt{|S|} = 2\sqrt{lr}$ to obtain asymptotically good curves and codes over $\mathbb{F}_q$. The ratio c again becomes a constant (depending only on l) times $\sqrt{r}$. This is, of course, poor compared to the Drinfeld–Vladut bound $c \leqslant \sqrt{q} - 1$.

Acknowledgement

I am very grateful to Eva Bayer who supplied me with her private notes of Serre's lectures [8].

References

[1] C. Chevalley, Introduction to the theory of algebraic functions of one variable, Math. Surveys 6, (1951).

[2] G. Lachaud, Les codes geometriques de Goppa, Seminaire Bourbaki no. 641, Asterisque 133–134 (1986).

[3] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977).

[4] G. Pasquier, Binary selfdual codes construction from selfdual codes over a Galois field $\mathbb{F}_{2^m}$, Ann. Discrete Math. 17 (North-Holland, Amsterdam, 1983) 519–526.

[5] P. Roquette, On class field towers, in: A. Fröhlich and J.W.S. Cassels, eds., Algebraic Number Theory (Academic Press, London, New York, 1967) 231–249.

[6] M. Rosen, The Hilbert class field in function fields, Exposition. Math. 5 (1987) 365–378.

[7] W. Scharlau, Selbstduale Goppa-Codes, Münster, 1987, preprint.

[8] J.-P. Serre, The number of points on curves over finite fields (Lectures Princeton Univ. Press, Princeton, NJ, 1983) see also: C.R. Acad. Sc. Paris 296 (1983) 397–402.

[9] H. Stichtenoth, Selfdual Goppa codes, J. Pure Appl. Algebra 55 (1988) 199–211.