

Double Circulant Quadratic Residue Codes ^{*}

Tor Helleseeth [†] José Felipe Voloch [‡]

January 26, 2004

Abstract

We give a lower bound for the minimum distance of double circulant binary quadratic residue codes for primes $p \equiv \pm 3 \pmod{8}$. This bound improves on the square root bound obtained by Calderbank, using a completely different technique. The key to our estimates is to apply a result by Helleseeth, to which we give a new and shorter proof. Combining this result with the Weil bound leads to the improvement of Calderbank's bound. For large primes p , the bound due to Calderbank is of order $\sqrt{2p}$ while our new improved bound is of order $2\sqrt{p}$.

1 Introduction

In this note we give a lower bound for the minimum distance of the double circulant binary quadratic residue codes defined by Karlin [3] for primes $p \equiv \pm 3 \pmod{8}$. This bound is comparable to the square root bound for the usual quadratic residue codes and improves on the square root bound obtained by Calderbank [1] using a completely different technique. The key to our estimates

^{*}The first author was supported by the Norwegian Research Council and the second author by NSA grant MDA904-03-1-0117.

[†]The Selmer Center, Department of Informatics, University of Bergen, PB 7800, N-5020 Bergen, Norway (email: tor.helleseeth@ii.uib.no)

[‡]Department of Mathematics, University of Texas, Austin, TX 78712, USA (email: voloch@math.utexas.edu)

is a result in Helleseth [2] to which we give a new and shorter proof. This result relates the weight of codewords of a quadratic residue code to the number of points of hyperelliptic curves over \mathbf{F}_p to which the Weil bound can be applied to obtain the improvement of Calderbank's bound.

A double circulant code is a code with generator matrix $[I|W]$ where I is the $n \times n$ identity matrix and W is an $n \times n$ circulant matrix. We work throughout with codes over the binary field \mathbf{F}_2 . We take $n = p$, a prime, and let W be the $p \times p$ matrix whose (j, t) entry ($j, t = 0, 1, \dots, p-1$) is 1 if and only if $t - j$ is a nonzero quadratic residue modulo p . We denote the corresponding binary $[2p, p]$ code by C_p . Our convention differs slightly from those of Karlin [3], but the results can be readily translated. When $p \equiv \pm 1 \pmod{8}$, the codes with W as a generator matrix or parity check matrix are quadratic residue codes in the usual sense and the minimum distance of C_p can be readily related to the minimum distance of the usual quadratic residue codes. If we view \mathbf{F}_2^{2p} as $\mathbf{F}_2[x]/(x^p - 1) \oplus \mathbf{F}_2[x]/(x^p - 1)$, then $C_p = \{(a(x), \omega(x)a(x)) \mid a(x) \in \mathbf{F}_2[x]/(x^p - 1)\}$, where $\omega(x) = \sum_{q \in Q} x^q$ and $Q \subset \{1, \dots, p-1\}$ is the set of nonzero quadratic residues modulo p .

A standard calculation gives the following well known result, that is needed later.

Lemma 1 *Let $\omega(x) = \sum_{q \in Q} x^q$. If $p \equiv 3 \pmod{8}$ then $\omega(x)^3 \equiv 1 \pmod{x^p - 1}$. If $p \equiv -3 \pmod{8}$ then $\omega(x)^3 \equiv 1 + \frac{x^p - 1}{x - 1} \pmod{x^p - 1}$.*

2 Main results

In this section we will first give a shorter and simpler proof of the result originally proved in Helleseth [[2], Theorem 1.1]. Thereafter we will combine this result with the Weil bound to improve the previous best bound due to Calderbank [1] on the minimum distance of some double circulant codes.

Lemma 2 *If $a(x) = \sum_{i=1}^r x^{j_i} \in \mathbf{F}_2[x]/(x^p - 1)$, define $f(t) = \prod_{i=1}^r (t - j_i) \in \mathbf{F}_p[t]$, then the weight $w(\mathbf{c})$ of $\omega(x)a(x)$ is*

$$w(\mathbf{c}) = \frac{1}{2} \left(p + (-1)^{r-1} \left(\sum_{t \in \mathbf{F}_p} \chi(f(t)) - \sum_{i=1}^r \chi(f'(j_i)) \right) \right)$$

where χ denotes the quadratic character (Legendre symbol) mod p .

Proof. Let $c(x) = \omega(x)a(x) = \sum_{i=0}^{p-1} c_i x^i$. From the definition of $c(x)$ it is immediate to describe the positions where $c_t = 1$. Let $J = \{j_1, j_2, \dots, j_r\}$. In the case $t \notin J$, then $c_t = 1$ if and only if an odd number of elements among the r elements $t - j$, $j \in J$ belong to Q . In the case $t \in J$, then $c_t = 1$ if and only if an odd number of elements among the $r - 1$ nonzero elements $t - j$, $j \in J$ belong to Q .

This description immediately gives that in the case $t \notin J$ then $c_t = 1$ if and only if $(-\chi(t - j_1))(-\chi(t - j_2)) \cdots (-\chi(t - j_r)) = -1$. Similarly in the case $t \in J$, say $t = j_1$ then $c_t = 1$ if and only if $(-\chi(j_1 - j_2))(-\chi(j_1 - j_3)) \cdots (-\chi(j_1 - j_r)) = -1$. Note that $f'(j_i) = \prod_{a=1, a \neq i}^r (j_i - j_a)$. Therefore, the codeword $c(x)$ can be described most simply as follows: $(-1)^{c_t} = (-1)^r \chi(f(t))$ when $t \notin J$ and $(-1)^{c_t} = (-1)^{r-1} \chi(f'(t))$ when $t \in J$.

Let $w(\mathbf{c})$ denote the Hamming weight of $\mathbf{c} = (c_1, c_2, \dots, c_{p-1})$, then we obtain,

$$p - 2w(\mathbf{c}) = \sum_{i=0}^{p-1} (-1)^{c_i} = (-1)^r \left(\sum_{t \in \mathbf{F}_p} \chi(f(t)) - \sum_{t \in J} \chi(f'(t)) \right).$$

This completes the proof of the lemma.

Remark Let $\omega^*(x) = \sum_{n \in N} x^n$ where N is the set of quadratic nonresidues modulo p . The proof of Lemma 2 is easily modified and leads to the following weight $w(\mathbf{c})$ of $w^*(x)a(x)$:

$$p - 2w(\mathbf{c}) = \sum_{i=0}^{p-1} (-1)^{c_i} = \sum_{t \in \mathbf{F}_p} \chi(f(t)) + \sum_{t \in J} \chi(f'(t)).$$

The Weil bound, in the notation of the above lemma, implies that

$$\left| \sum_{t \in \mathbf{F}_p} \chi(f(t)) \right| \leq (r - 1)\sqrt{p}.$$

Combining the Weil bound with Lemma 2 and the remark above we obtain:

Corollary 1 *Let $\omega(x) = \sum_{q \in Q} x^q$ or $\omega^*(x) = \sum_{n \in N} x^n$, where Q (resp. N) is the set of quadratic residues (resp. nonresidues) modulo p . The weight $w(\mathbf{c})$ of any codeword $\omega(x)a(x)$ or $\omega^*(x)a(x)$ is bounded by*

$$\frac{1}{2}(p - (r - 1)\sqrt{p} - r) \leq w(\mathbf{c}) \leq \frac{1}{2}(p + (r - 1)\sqrt{p} + r).$$

Theorem 1 *The minimum distance d of C_p when $p \equiv \pm 3 \pmod{8}$ is bounded by,*

$$d \geq \frac{2(p + \sqrt{p})}{\sqrt{p} + 3}.$$

Proof. Let d be the minimum distance of C_p . The codewords are represented by $(a(x), w(x)a(x))$ where the polynomials are computed modulo $x^p - 1$. Given a codeword of weight d , let r be the weight of the vector formed by the first p coordinates of this codeword (corresponding to $a(x)$) and $d - r$ the weight of the last p coordinates (corresponding to $b(x) = w(x)a(x)$).

Assume first that $r \leq d/2$. By Corollary 1 we obtain,

$$\begin{aligned} d &\geq r + \frac{1}{2}(p - (r - 1)\sqrt{p} - r) \\ &= \frac{1}{2}(p + \sqrt{p} - r(\sqrt{p} - 1)) \\ &\geq \frac{1}{2}(p + \sqrt{p} - d(\sqrt{p} - 1)/2) \end{aligned}$$

which implies

$$d \geq 2(p + \sqrt{p})/(\sqrt{p} + 3).$$

Assume next that $r > d/2$. From Lemma 1 we obtain $\omega(x)^3 = 1 + \delta(x^p - 1)/(x - 1)$ where $\delta \in \{0, 1\}$. Let $b(x) = w(x)a(x)$, then $w(x)^2b(x) = w(x)^3a(x) = a(x) + r\delta(x^p - 1)/(x - 1)$. Interchanging the coordinates of the first and last p coordinates in the codeword $(a(x), w(x)a(x))$ gives $(b(x), \omega(x)^2b(x) + r\delta(x^p - 1)/(x - 1))$. Note that since 2 is a quadratic nonresidue mod p , then $\omega(x)^2 = \sum_{q \in Q} x^{2q} = \sum_{n \in N} x^n = w^*(x)$, where N is the set of quadratic non-residues mod p .

In the case $\delta r = 0 \pmod{2}$ the codeword is $(b(x), w^*(x)b(x))$. Since the weight of $b(x)$ is $d - r \leq d/2$, interchanging the role of $a(x)$ and $b(x)$ and applying Corollary 1, reduces the proof of this case to the previous case where $r \leq d/2$.

Finally, when $\delta r = 1 \pmod{2}$, the codeword becomes $(b(x), \omega(x)^*b(x) + (x^p - 1)/(x - 1))$, and Corollary 1 implies,

$$\begin{aligned} d &\geq d - r + (p - (p + (d - r - 1)\sqrt{p} + d - r - 1)/2) \\ &= d - r + (p + \sqrt{p} + 1)/2 + r(\sqrt{p} + 1)/2 - d(\sqrt{p} + 1)/2. \end{aligned}$$

Hence,

$$d(\sqrt{p} + 1)/2 \geq (p + \sqrt{p} + 1)/2 + r(\sqrt{p} - 1)/2$$

and since $r > d/2$, we conclude

$$d > 2(p + \sqrt{p} + 1)/(\sqrt{p} + 3) \geq 2(p + \sqrt{p})/(\sqrt{p} + 3)$$

which completes the proof.

Using the results of Stark [4] one can push the lower bound on d to $2.13\sqrt{p}$ for large p .

3 Conclusions

A new direct and simple proof of the connection between Legendre sum and quadratic residue code has been given. In combination with the Weil bound this result has been applied to improve Calderbank's bound on the minimum distance of double circulant codes. For large primes p , the lower bound due to Calderbank is of order $\sqrt{2p}$ while this correspondence provides an improved lower bound of order $2\sqrt{p}$.

References

- [1] R. Calderbank, "A square root bound on the minimum weight in quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. 29, pp. 332-337, May 1983.
- [2] T. Helleseth, "Legendre sums and codes related to QR codes," *Discrete Applied Math.*, vol. 35, pp. 107-113, 1992.
- [3] M. Karlin, "New binary coding results by circulants," *IEEE Trans. Inform. Theory*, vol. 15, pp. 81-92, Jan. 1969.
- [4] H.M. Stark, "On the Riemann hypothesis in hyperelliptic function fields," *Analytic number theory*, Proc. Sympos. Pure Math., Vol. XXIV, pp. 285-302, 1972.