

Asymptotics of the minimal distance of quadratic residue codes

José Felipe Voloch

The binary quadratic residue codes are defined as follows. Given a prime $p \equiv \pm 1 \pmod{8}$, let ξ be a primitive p -th root of unity in the algebraic closure of \mathbf{F}_2 , the field of two elements. The hypothesis on p entails that the monic polynomial $a(x)$, say, whose roots are ξ^r , with r running over the non-zero quadratic residues modulo p , is defined over \mathbf{F}_2 and the cyclic code of length p whose generator polynomial is $a(x)$ is, by definition, the binary quadratic residue code of length p . Different choices of ξ lead to different choices of $a(x)$ that give different but equivalent codes. Their minimal distance d_p is, in general, not known although the lower bound $d_p \geq \sqrt{p}$ and minor improvements are known, see [MS]. It is possible, using the results of Stark [S] and Helleseth's formula for the weight (see [H] and lemma 1 below), to improve slightly this lower bound (See [HV]). However, the general behaviour of d_p is not known, in particular, whether there is an asymptotically good subfamily of quadratic residue codes, i.e., whether $\limsup d_p/p > 0$. We will show that there are asymptotically bad subfamilies of quadratic residue codes, i.e., $\liminf d_p/p = 0$. More precisely,

Theorem. *For infinitely many primes p , the minimal distance d_p of the binary quadratic residue code of length p is $O(p/\log \log p)$. If furthermore, the generalised Riemann hypothesis is true, then the bound can be improved to $O(p/\log p)$.*

In the proof of the Theorem we will use the following lemma of Helleseth. For a proof see [H] or [HV].

Lemma 1. *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 $q(x)a(x)$ 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 of the Theorem: Let ℓ be an odd prime, ζ a primitive complex ℓ -th root of unity and K the extension of the rational number field obtained by adjoining $\zeta, \sqrt{2}$ and $\sqrt{\zeta^k - 1}$ for all $k = 1, \dots, \ell - 1$. Let p be a prime that splits completely in K , I claim that $d_p \leq (p - 1)/2\ell$. Note that $\ell | (p - 1)$ since p splits in the ℓ -th cyclotomic field. Let $f(t) = t^{(p-1)/\ell} - 1 \in \mathbf{F}_p[t]$, then $f(t)$ has all its roots in \mathbf{F}_p and yields a codeword \mathbf{c} of C_p as in the lemma. Again, by the assumption on p , $f(t)$ is a square for all $t \in \mathbf{F}_p$, since $t^{(p-1)/\ell}$ is an ℓ -th root of unity for $t \in \mathbf{F}_p^*$ and -1 is a square in \mathbf{F}_p . The roots of $f(t)$ form a subgroup G of index ℓ in \mathbf{F}_p^* , $f'(t) = (p - 1)/\ell t$ in G and it follows easily that $\sum_{t \in G} \chi(f'(t)) = 0$. So $w(\mathbf{c}) = (p - 1)/2\ell$ and the claim follows.

To complete the proof of the theorem we vary ℓ as above and, for each ℓ , we take p to be the smallest prime that splits completely in K . We will show that $\ell \gg \log \log p$ and $\ell \gg \log p$ under the generalised Riemann hypothesis and this will prove the theorem. To bound p in terms of ℓ we use the following estimates (see [LO] and [LMO] respectively). Let d be the discriminant of K . Then $\log p \ll \log d$ and, under the generalised Riemann hypothesis, $p \ll (\log d)^2$. To estimate d note that only p and 2 ramify in K . Now we use Hensel's bound on the different (see [Se] remark 1 after Proposition III.13), which yields that the contribution of a ramified prime to the discriminant has exponent at most $n(n + 1)$, where n is the absolute degree of K . We conclude that $d \leq (2p)^{n(n+1)}$. Finally, it is immediate that $n \leq (p - 1)2^p$, which gives the results claimed.

Remark: The quadratic residue codes have been generalized to (no longer cyclic) binary codes of length q for a prime power q when 2 is a square modulo q ([vLM]). The above lemma has a generalization to these codes sketched in [HV]. For q a square it was shown in [vLM] that the square root bound is best possible. From our perspective, their example consists of noticing that $t^{\sqrt{q}} + t$ is a square for all $t \in \mathbf{F}_q$. It can be proved (unconditionally) that there are infinitely many non-square prime powers q for which the binary quadratic residue code length q has minimal distance $O(q/\log q)$, using an idea of S. Ball.

References.

[MS] J. MacWilliams and N. Sloane, *The theory of error-correcting codes*, North-Holland, 1977.

[H] T. Helleseth, “Legendre sums and codes related to QR codes,” *Discrete Applied Math.*, vol. 35, pp. 107-113, 1992.

[HV] T. Helleseth; J. F. Voloch, “Double Circulant Quadratic Residue Codes” *IEEE Transactions on Information Theory*, to appear.

[LMO] J. C. Lagarias, H. L. Montgomery and A. M. Odlyzko “A bound for the least prime ideal in the Chebotarev density theorem” *Invent. Math.*, vol 54 (1979), 271–296.

[LO] J. C. Lagarias, A. M. Odlyzko, “Effective versions of the Chebotarev density theorem” in *Algebraic Number Fields*, A. Frohlich ed., Academic Press 1997, pp 409–464.

[vLM] van Lint, J.; MacWilliams, F., “Generalized quadratic residue codes” *IEEE Transactions on Information Theory* Vol. 24, 1978 pp. 730- 737

[Se] J.-P. Serre, *Local Fields*, Springer, New York, 1979.

[S] H.M. Stark, “On the Riemann hypothesis in hyperelliptic function fields,” *Analytic number theory*, Proc. Sympos. Pure Math., Vol. XXIV, pp. 285-302, 1972.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu