Math 2^8: The Theory of Error-Correcting Codes

Quadratic residue (QR) codes

Here's another approach to QR codes of prime length $n = 4j - 1$. Fix some $\alpha \in F$. Let $c(0)$ be the word with entry α in the zeroth coordinate, 1 at each quadratic residue of n, and 0 at the quadratic nonresidues. [We might prefer -1 at the qadratic nonresidues but that would not work in the important case $|F| = 2$.] For $a \bmod n$, let $c(a)$ be the translate of c by a, which has entry α and 1 at coordinate a and $a + r^2$ and 0 else. Then $(c(a), c(a)) = \alpha^2 + 2j - 1$. We claim $(c(a), c(b)) = \alpha + j - 1$ for $a \neq b$. We prove this using $(-1/n) = 0$ (that's why we needed $n \equiv -1 \bmod 4$) and the fact that the equation $b - a = r^2 - s^2 = (r + s)(r - s)$ has $n - 1$ solutions in $\mathbf{Z}/n\mathbf{Z}$, of which 2 have $r = 0$ or $s = 0$. In particular, if α can be chosen so that $\alpha^2 + 2j - 1$ and $\alpha + a - 1$ both vanish in F then the $c(a)$ generate a self-orthogonal cyclic code of length n. For example, if j is a multiple of the characteristic then we can choose $\alpha = 1$. This gives rise to QR codes C over $\mathbf{Z}/2\mathbf{Z}$ and $\mathbf{Z}/3\mathbf{Z}$ when $n \equiv -1 \bmod 8$ and $\bmod 12$ respectively. Since C has automorphisms by $c_x \mapsto c_{\rho x}$ for any quadratic residue ρ, the corresponding $S \subset \mathbf{Z}/n\mathbf{Z}$ is a union of some of $\{0\}$, the quadratic residues, and the quadratic nonresidues. Since $\dim C > 1$ (because $c(0)$ and $c(1)$ are not proportional) but $2 \dim C < n$ (by self-orthogonality) we must have $\dim C = 2j - 1 = (n - 1)/2$, and S consists either of the quadratic residues or the quadratic nonresidues (depending on the choice of generator of $\boldsymbol{\mu}_n$).

For $F = \mathbf{Z}/2\mathbf{Z}$, all the generators have weight $2j \equiv 0 \bmod 4$, so the code is doubly even; extending to a code of length $n + 1$ by adjoining an idle coordinate "at ∞" and then including the all-ones word $\mathbf{1}$ yields a Type II code. Likewise for $F = \mathbf{Z}/3\mathbf{Z}$ we get a Type III code of length $n + 1$ in the same way. The name ∞ for the extra coordinate is appropriate, because the extended code has automorphisms by $c_x \mapsto c_{-1/x}$ (with $0 \leftrightarrow \infty$), and thus by $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$.

To construct such a code when j need not vanish in F, we extend each $c(a)$ by an $(n + 1)$st coordinate equal to some fixed $\beta \in F$ that need not be zero either. These extended vectors have inner product $\alpha^2 + 2j - 1 + \beta^2$ with themselves and $\alpha + j - 1 + \beta^2$ with each other. Setting both of these equal zero and subtracting yields $\alpha^2 - \alpha + j = 0$. This quadratic has discriminant $1 - 4j = -n$, so has a solution whenever $-n$ is a square in F, which by Quadratic Reciprocity happens *iff* $|F|$ is a square mod n, exactly the condition we need for the quadratic residues mod n to be permuted by multiplication by F. (In characteristic 2, the condition becomes $2 \bmod j$ when $|F|$ is an odd power of 2, and no condition when $|F|$ is a square.) We can then take $\beta = 1 - \alpha$ (which agrees with our earlier choice of $\beta = 1$ when $\alpha = 0$). The resulting vectors are also orthogonal to the vector with coordinate $1 - 2\alpha$ at infinity and a at each element of $\mathbf{Z}/n\mathbf{Z}$; this vector, together with our n extended-$c(a)$ vectors, span a QR code of length $n + 1$ with automorphisms by $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$.

For QR codes over a fixed small field F we can improve on the BCH bound, which is expected to grow only as $\log n$ for large n. Consider the case $F = \mathbf{Z}/2\mathbf{Z}$. Because C is self-orthogonal and contains $c(a)$, for any word $c \in C$ we find that $\prod_{c_x=1}(a - x)$ is either zero or a square for all $a \in \mathbf{Z}/2\mathbf{Z}$. Using the Weil estimates(!) we deduce that if $c \neq 0$ then c has weight $\gg \sqrt{n}$. Alas this is still $o(n)$, so even for QR codes the minimum weight is known only for finitely many n.