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

Cyclic codes

Where Reed-Muller codes have one of the largest automorphism groups that can acts on codes more interesting than the repetition and single-checksum codes, cyclic codes are required only to have an action by one of the smallest groups that's still of use: a group of cyclic permutations of the coordinates. These include many of the linear codes that we have seen already, but there are notable exceptions such as the extended Golay codes, whose automophism groups $2M_{12}$ and M_{24} cannot contain an n-cycle because the groups are contained in A_n (else they could not be simple) but a cycle of even length has sign -1.

In general, suppose G is any subgroup of the automorphism group $(F^*)^n \rtimes S_n$ of Hamming space F^n. Then F^n is a linear representation of G, or equivalently a module for the group ring $F[G]$, and a linear code with an action of G is a sub-representation (equivalently: a submodule) of F^n.

For a cyclic code, G is $\mathbf{Z}/n\mathbf{Z}$, and $F[G] = F[X]/(X^n - 1)$ where the generator of $\mathbf{Z}/n\mathbf{Z}$ acts by multiplication by X; so we can identify F^n with $F[G]$ (once we've identified the set of n coordinates with $\mathbf{Z}/n\mathbf{Z}$ by choosing a zeroth coordinate), so a submodule is just an ideal of $F[G]$. Now in general if A is any commutative ring and I any ideal then ideals of A/I correspond bijectively with ideals of A that contain I (associate the ideal $\bar{J}$ of A/I with its preimage J in A under the quotient map, and associate any ideal $J \supseteq I$ with the ideal J/I of A/I). In our case $A = F[G]$ and $I = (X^n - 1)$, so cyclic codes correspond to ideals of $F[X]$ that contain $X^n - 1$. But $F[G]$ is a principal ideal domain whose unit group is F^*, so any nonzero ideal can be written uniquely as the principal ideal (P) for some monic polynomial $P = P(X)$. This ideal contains $(X^n - 1)$ iff P is a factor of $X^n - 1$. In summary, cyclic codes correspond bijectively with monic factors P of $X^n - 1$ in $F(X)$. The polynomial P is thus called the *generator* of the code $C_P = (P) \bmod X^n - 1$. This code has dimension $n - \deg(P)$; as usual the minimum weight is hard to determine in general, but must be at least $\deg(P) + 1$ by the Singleton bound. For example, the zero code, repetition code, single-checksum code, and F^n itself correspond to the factors $X^n - 1,\ (X^n - 1)/(X - 1),\ X - 1,$ and 1 respectively (note that $P \mid Q \iff C_P \supseteq C_Q$). The $[7, 4, 3]$ Hamming code can be taken to have generator $1 + X + X^3$.

We usually assume that n is not a multiple of the characteristic of F, or equivalently that $\gcd(n, q) = 1$ where $q = |F|$. Then $X^n - 1$ has distinct roots in $\overline{F}$, which constitute the group $\boldsymbol{\mu}_n$ of n-th roots of unity in $\overline{F}$. (One way to see this is to calculate that at a root x of $X^n - 1$ the derivative of $X^n - 1$ is nX^{n-1}, which is always zero if n is a multiple of the characteristic, but never zero otherwise.) Now monic factors of $X^n - 1$ correspond bijectively with subsets of $\boldsymbol{\mu}_n$, and monic factors in $F[X]$ correspond with subsets that are stable (i.e. the union of orbits) under $\mathrm{Gal}(\overline{F}/F)$, or equivalently under $x \mapsto x^q$. Now $\boldsymbol{\mu}_n$ is a cyclic group of order n, and if we (non-canonically) identify $\boldsymbol{\mu}_n$ with $\mathbf{Z}/n\mathbf{Z}$ then cyclic codes correspond to subsets stable under multiplication by q. For example, if n is prime and q is a primitive residue of n (i.e. a generator of $(\mathbf{Z}/n\mathbf{Z})^*$) then $(X^n - 1)/(X - 1)$ is irreducible in $F[X]$ and the only cyclic codes are the four corresponding to $X^n - 1,\ (X^n - 1)/(X - 1),\ X - 1,$ and 1. Note that while 7 is prime, 2 is *not* a primitive residue (since $2^3 \equiv 1 \bmod 7$), so other Hamming codes are allowed; e.g. there are two such codes of dimension 4, associated with the factors $1 + X + X^3$ and $1 + X^2 + X^3$ of $(X^7 - 1)/(X - 1)$, and both isomorphic with the $[7, 4, 3]$ Hamming code (they are isomorphic with each other under $X \leftrightarrow 1/X$).

Since the dual of a cyclic code is again cyclic, duality must give rise to a bijection on monic factors of $X^n - 1$. There's an obvious bijection that takes P to Q when $PQ = X^n - 1$, but that's not quite right: it turns out that the dual of C_P is not C_Q but $C_{r(Q)}$ where r is the reversal

$$(r(Q))(X) = X^{\deg(Q)} r(X^{-1})/r(0)$$

obtained by reading the coefficients of Q backwards and scaling to make $r(Q)$ monic, so the roots of $r(Q)$ are the multiplicative inverses of the roots of Q. We see this from the following analysis. Over $\overline{F}$, the polynomial $X^n - 1$ factors completely as $\prod_{x \in \boldsymbol{\mu}_n} (X - x)$, and any subset of $\boldsymbol{\mu}_n$ yields a cyclic code in $\overline{F}^n$. These include n codes of dimension 1, with the factor $(X^n - 1)/(X - x)$ corresponding to the code with generator $(1, x^{-1}, x^{-2}, \ldots, x^{-(n-1)})$ (the last coordinate also equals x). Letting c_x be that generator, we see that the inner product (c_x, c_y) vanishes unless $xy = 1$ when $(c_x, c_y) = n \neq 0$.

It follows that the c_x form a basis for $\overline{F}^n$; we could also have seen this directly from discrete Fourier analysis — which is equivalent to the computation of (c_x, c_y) — or by computing the determinant of the c_x using the Vandermonde factorization. Now if $PQ = X^n - 1$ then $C_P \otimes \overline{F}$ has a basis consisting of the c_x with x a root of Q. It follows that $C_P^\perp$ has a basis consisting of the c_x with x^{-1} a root of P, i.e. with x a root of $r(P)$. Since $r(P)r(Q) = r(PQ) = r(X^n - 1) = X^n - 1$ we conclude that $C_P^\perp = C_{r(Q)}$ as claimed. In terms of subsets of $\boldsymbol{\mu}_n$, the reversal corresponds to inversion $S \leftrightarrow S^{-1} = \{x^{-1} \mid x \in S\}$, so duality is the inverse complement.

For cyclic codes C over F, we have also $S = S^q$, which means that if c_x is in our basis of $C \otimes \overline{F}$ then so is c_{x^q}. Now the m-th coordinate of c_{x^q} is the (qm)-th coordinate of c_x (with qm taken mod n), so we deduce that a cyclic code is automatically stable under the group of coordinate permutations of the form $m \mapsto q^e m + b \bmod n$. For example, the cyclic construction of the Hamming $[7, 4, 3]$ code already shows it has at least 21 automorphisms. If $S \subseteq \boldsymbol{\mu}_n$ is stable under some subgroup of $(\mathbf{Z}/N\mathbf{Z})^*$ larger than $q^{\mathbf{Z}}$ then that group also acts on the code. For example, if n is an odd prime and q is a quadratic residue of n (i.e. a nonzero square mod n) then we obtain a cyclic code of dimension $(n+1)/2$ from the set of quadratic residues in $\mathbf{Z}/n\mathbf{Z}$, and that code has automorphisms by the group of permutations $m \mapsto am + b$ with $(a/n) = +1$. This is one of a few closely related codes called "quadratic residue (QR) codes". For example, binary QR codes exist when the prime n is $\equiv \pm 1 \bmod 8$; the first example is the Hamming code for $n = 7$, and we shall see that $n = 23$ yields the binary Golay code $\mathcal{G}_{23}$. Likewise for $q = 3$ we must have $n \equiv \pm 1 \bmod 12$, and the first example $n = 11$ is the ternary Golay code $\mathcal{G}_{11}$. These cases ($n = 7$ and $n = 23$ for $q = 2$, and $n = 11$ for $q = 3$) are the only cases where these codes have more automorphism than the guaranteed $am + b$ maps.

While we cannot give a general recipe for $\mathrm{wt}_{\min}(C_P)$, there is an important lower bound: if C_P has a nonzero word of weight w then P cannot have w zeros in geometric progression (equivalently, the corresponding subset S of $\mathbf{Z}/N\mathbf{Z}$ cannot have w elements in arithmetic progression). This is the BCH (Bose-Chaudhuri-Hocquenghem) bound. To prove it, assume that P does have w zeros in geometric progression, and consider the associated vectors c_x in the dual of $C_P \otimes \overline{F}$. This gives w homogeneous linear equations in w variables, represented by a Vandermonde matrix with distinct rows and columns; since such a matrix is invertible we have our contradiction.

As an example application, consider the binary QR code of length 23, with $P = X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1$. The quadratic residues mod 23 include $1, 2, 3, 4$, so $\mathrm{wt}_{\min}(C_P) > 4$. We claim that in fact the minimum is 7. Indeed consider the even subcode C_P^0, with generator

$$(X+1)P = X^{12} + X^{10} + X^7 + X^4 + X^3 + X^2 + X + 1.$$

This code is self-orthogonal (because $(-1/23) = -1$), and it is generated by word of weight 8, so it is doubly even. The odd vectors in C_P constitute the ones' complements of C_P^0, so their weights are $3 \bmod 4$. By BCH this proves that $\mathrm{wt}_{\min}(C_P) = 7$. Hence C_P is a perfect 3-error-correcting code, and its parity-check extension to length 24 is doubly even. We conclude that $C_P \cong \mathcal{G}_{23}$ and the extension is isomorphic with $\mathcal{G}_{24}$. Likewise for the ternary Golay codes, starting from the factorization

$$X^{11} - 1 = (X-1)(X^5 - X^3 + X^2 - X - 1)(X^5 + X^4 - X^3 + X^2 - 1)$$

over $\mathbf{Z}/3\mathbf{Z}$, and the observation that $3, 4, 5$ are consecutive quadratic residues mod 11.

BCH codes of designed minimum weight w are binary codes of length $n = 2^m - 1$ for which S contains $0, 1, 2, \ldots, w-2$ and all their $2^{\mathbf{Z}}$ multiples mod $2^m - 1$. Note that once S contains 0 and all the odd numbers up to $w-2$, the rest is automatic (and thus we may assume that w is odd, else we get $w+1$ for free). Equivalently, the code consists of all functions $f : \mathbf{F}_{2^m}^* \to F$ such that $\sum_{a \in \mathbf{F}_{2^m}^*} a^s f(s) = 0$ in $\mathbf{F}_{2^m}$ for each $a = 0, 1, 2, \ldots, w-2$. We can extend by a parity-check bit at $s = 0$, and then the code has automorphisms by the $ax+b$ group of $\mathbf{F}_{2^m}$ together with $\mathrm{Gal}(\mathbf{F}_{2^m}/F)$. For example, the $w = 3$ code is the generalized Hamming code; the extended $w = 7$ code contains the dual of $RM(2, n)$, and once $n > 5$ the containment is strict without reducing the minimum weight. (Likewise for any $w = 2^r - 1$.) Given w, the designed minimum weight is attained for sufficiently large m by a pigeonhole argument, and for $w = 5$ the minimal words can still be enumerated using the structure of quadratic forms (because a polynomial of degree < 7 on $\mathbf{F}_{2^m}$ is a quadratic form).