Looking at things differently

Let n be prime and 2 be primitive modulo n. Consider the action of the cyclic shift operator

$$L = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ & & \ddots & \\ 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{bmatrix}$$

on the vectors of $\mathbb{F}_2^n$. L is diagonalizable in the Galois field $\mathbb{F}_2(\omega) = \mathbb{F}_{2^{n-1}}$, where ω is an nth root of unity (the fact that 2 is primitive modulo n garantees that $\mathbb{F}_2(\omega)$ contains all the nth roots of unity, namely, they are all the powers of ω).

Its eigenvectors are

$$x_0 = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}, x_1 = \begin{pmatrix} 1 \\ \omega \\ \omega^2 \\ \vdots \\ \omega^{n-1} \end{pmatrix}, x_2 = \begin{pmatrix} 1 \\ \omega^2 \\ \omega^4 \\ \vdots \\ \omega^{2(n-1)} \end{pmatrix}, \ldots, x_{n-1} = \begin{pmatrix} 1 \\ \omega^{n-1} \\ \vdots \\ \omega^{(n-1)(n-1)} \end{pmatrix}.$$

Notice that these are the columns of the $n \times n$ DFT matrix.
Now consider the action of the double cyclic shift operator

$$\begin{bmatrix} L & 0 \\ 0 & L \end{bmatrix}$$

on the vectors of $\mathbb{F}_2^{2n}$. Its eigenvectors over $\mathbb{F}_{2^{n-1}}$ are of the form $\begin{pmatrix} x_i \\ 0 \end{pmatrix}$ or $\begin{pmatrix} 0 \\ x_i \end{pmatrix}$ for the x_i defined above.
Thus a basis for $\mathbb{F}_{2^{n-1}}^{2n}$ is

$$\left\{ \begin{pmatrix} x_0 \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} x_{n-1} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x_0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ x_{n-1} \end{pmatrix} \right\}.$$

Our goal is to describe double circulant codes of length $2n$ over $\mathbb{F}_2$, that is, subspaces of $\mathbb{F}_{2^{n-1}}^{2n}$ that have a generator matrix of the form $[I_n|A]$, where A is a circulant matrix (this ensures the double circulant property) and such that they are invariant under the Frobenius map

$$\sigma : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_1^2 \\ \vdots \\ x_n^2 \end{pmatrix}$$

(this ensures that the subspaces live over $\mathbb{F}_2$, so that we have indeed codes over $\mathbb{F}_2$).

A basis for such invariant subspaces is given by $B \begin{bmatrix} F & 0 \\ 0 & F \end{bmatrix}$, where B is an $n \times 2n$ matrix to be determined, and F is the DFT matrix, and should have the

form $[I_n|A]$, where $A = \begin{bmatrix} a_0 & a_1 & \cdots & a_n \\ \vdots & & & \\ a_1 & a_2 & \cdots & a_0 \end{bmatrix}$ is circulant, and $a_0, \ldots, a_n$ can take any values in $\mathbb{F}_2$. Solving for B, we get that B must be of the form

$$B = \left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & \cdots & 0 & \alpha & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & \beta & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & \beta^2 & \cdots & 0 \\ & & & \ddots & & & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 & \cdots & \beta^{n-1} \end{array}\right],$$

where α can take any value in $\mathbb{F}_2$ and β can take any value in $\mathbb{F}_{2^{n-1}}$. This gives us 2^n subspaces of $\mathbb{F}_{2^{n-1}}^{2n}$ invariant under the double circular shift. Moreover, the fact that the basis vectors are weighted by β and all its conjugates ensure the invariance of these subspaces under the Frobenius map! Thus we have enumerated all binary double circulant codes of length $2n$ and rate $1/2$.

Modules. Back to counting

Consider the action of a group G on a vector space V. That is, define a multiplication between a group element g and a vector v such that

- $vg \in V$
- $v(gh) = (vg)h$
- $v1 = v$
- $(\lambda v)g = \lambda(vg)$
- $(u + v)g = ug + vg$.

V is called a module under the action of G. If V' is a subspace of V closed under the action of G, then V' is a (sub)module.

If V is a module under the action of G such that its only submodules are $\{0\}$ and itself, we call V irreducible.

In our case: consider the action of the cyclic group $G =< \sigma, \sigma^n = 1 >$ generated by the double circular shift σ acting on $\mathbb{F}_2^{2n}$. That is,

$$\sigma : (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n}) \mapsto (x_n, x_1, \ldots, x_{n-1}, x_{2n}, x_{n+1}, \ldots, x_{2n-1}).$$

The modules of this group action are the subspaces of $\mathbb{F}_2^{2n}$ invariant under the action of the elements of G, that is, the subspaces invariant under the action of the generating element σ. These are the subspaces described above; each module is of the form

$$M_{\alpha,\beta} = \left\langle \begin{pmatrix} x_0 \\ \alpha x_0 \end{pmatrix}, \begin{pmatrix} x_1 \\ \beta x_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ \beta^2 x_2 \end{pmatrix}, \ldots, \begin{pmatrix} x_{n-1} \\ \beta^{n-1} x_{n-1} \end{pmatrix} \right\rangle.$$

Let us consider the following modules:

$$M_\beta = \left\langle \begin{pmatrix} x_1 \\ \beta x_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ \beta^2 x_2 \end{pmatrix}, \ldots, \begin{pmatrix} x_{n-1} \\ \beta^{n-1} x_{n-1} \end{pmatrix} \right\rangle$$

(we lose 1 in the dimension but it does not really make a difference asymptotically). They are indeed modules of $\mathbb{F}_2^{2n}$ since the presence of β and all its conjugates garantee that they live over the base field. Each of these modules is of dimension $n-1$, and is irreducible: any space spanned by less than $n-1$ vectors $\begin{pmatrix} x_i \\ \beta^i x_i \end{pmatrix}$ is not invariant under Frobenius.

We can thus consider the counting argument as follows. Let n be prime, and let 2 be primitive modulo n. Let $M_1, \ldots, M_L$ be irreducible G-modules of $\mathbb{F}_2^{2n}$, where G is the code generated by the double cyclic shift σ. Let w be such that

$$|B_{2n}(w)| < nL.$$

Then there exists an M_i such that M_i does not contain nonzero words of weight w or less.

Proof First note that M_i irreducible $\forall i$ implies that $M_i \cap M_j = \{0\}$. Also note that by the double circulant property, if $x \in M_i$, then all of $\mathrm{orb}(x) \subseteq M_i$. The size of $\mathrm{orb}(x)$ is n for x nonzero and not equal to the all-ones codeword (by primality of n). The double circular shift is weight-preserving so that if a given M_i contains a codeword x of weight w, then it contains (at least) n codewords of weight w.

Suppose now that every M_i contains a nonzero element of $B_{2n}(w)$. Then every M_i contains at least n elements of $B_{2n}(w)$. Since the M_is intersect only in $\{0\}$, we would then have

$$|B_{2n}(w)| \geq L.n,$$

a contradiction. □

In our case, L was shown above to be 2^{n-1}. This gives the following result:

Theorem 1 *If n is prime and 2 is primitive modulo n, then there exist double circulant codes of parameters $[2n, n, d > w]$ for each w such that*

$$|B_{2n}(w)| < n2^{n-1}.$$

Generalizing diagonal action of group

We would like to generalize the example above.

Let G be a finite group. In the example above, a crucial property of G, was that it was a subgroup of S_n, and that the action of its elements was a permutation of the codeword coordinates, thus preserving the weight of codewords, which was an essential part of the proof when counting over low-weight codewords.

So it makes sense to consider G as a finite group acting transitively on $\{1, \ldots, n\}$. We view the elements $\{1, \ldots, n\}$ as elementary basis vectors in a space of dimension n. The elements of G can thus be viewed as permutation matrices over a space of dimension n.

Definition 1 *Let G be a finite group acting on a set V. We say that the action of G is transitive if $\forall a, b \in V$, there exists a group element g such that $a.g = b$.*

It is clear that in the setting above, the action of G is transitive (if a and b are two permutations of $\{1,\ldots,n\}$ living in a space closed under the action of G, there must be a permutation matrix $g \in G$ such that g takes a to b ????)
G acts on $\mathbb{F}_q^n$, and acts diagonally on $\mathbb{F}_q^n \oplus \mathbb{F}_q^n$. Suppose we have $M_1,\ldots,M_L$ distinct irreducible G-modules, all of dimension k. For every element x in $\mathbb{F}_q^n \oplus \mathbb{F}_q^n$, let $\mathrm{orb}(x)$ be the orbit of x under G. Then

Theorem 2 *If*

$$\sum_{x \in B_{2n}(w)} \frac{1}{|orb(x)|} < L,$$

then there exists a $[2m,k,d>w]_q$*- code.*

Proof We show that there is i such that M_i contains no words of weight w or less. Suppose otherwise. Then each M_i contains a full orbit of elements of $B_{2n}(w)$. Since the M_i's are complementary, this means that the number of distinct orbits of elements of $B_{2n}(w)$ is more than L (an orbit belongs to no more than one M_i). But

$$\#\text{ orbits of } B_{2n}(w) = \sum_{x \in B_{2n}(w)} \frac{1}{|\mathrm{orb}(x)|},$$

which is given to be strictly less than L. □
So we are now interested in the diagonal action of a group G on two copies of a module. Let M be a module of $\mathbb{F}_q^n$ under the action of G. How can we combine two copies of M to construct a module of $\mathbb{F}_q^{2n}$ under the action of G? Consider ϕ, an element of $GL_n(\mathbb{F}_q)$, and suppose that ϕ commutes with the action of G. $\phi(M) = \{\phi(\mu), \mu \in M\}$ need not be a module under the action of G. But consider the subspace of $\mathbb{F}_q^{2n}$ given by

$$M_\phi = \{(\mu, \phi(\mu)), \mu \in M\}.$$

This subspace is a G-invariant module. To see this, let σ be an element of G, and ψ_σ be the automorphism of F_q^n corresponding to the action of σ. Then

$$\psi_\sigma(\mu,\phi(\mu)) = (\psi_\sigma(\mu), \psi_\sigma\phi(\mu)) = (\psi_\sigma(\mu), \phi\psi_\sigma(\mu)) \in M_\phi.$$

We are thus interested in the (invertible. why?) linear maps that commute with the elements of G: this is the **centralizer** of G.
We thus want to find $G \leq GL_n(\mathbb{F}_q)$ such that $C_{GL_n(\mathbb{F}_q)}(G)$ is large.

Why doubly-transitive group action will not do.

Let G be a group acting on a set V. The action of G is said to be 2-transitive if for all $a_1 \neq a_2, b_1 \neq b_2 \in V$, there exists a group element g such that $g(a_1) = a_2$ and $g(b_1) = b_2$.

Back to our G, group of permutation matrices, acting transitively (why?) on F_q^n. Suppose the action of G was 2-transitive. We will prove that the centralizer of G cannot be too large.
Let $A = (a_{ij})$ belong to $C(G)$. Then for any element Π of G, we must have

$$\Pi A = A\Pi,$$

i.e.,

$$\Pi^{-1} A \Pi = A.$$

This is equivalent to requiring that

$$a_{\pi(i)\pi(j)} = a_{ij} \ \forall i, j.$$

Since the action of G is 2-transitive, this means that for all $i \neq j, l \neq k$, there exists a π such that $\pi(i) = l, \pi(j) = k$, and thus we must have $a_{ij} = a_{lk}$. On the diagonal, since the action of G is transitive, we must have $a_{ii} = a_{jj}$ for all i and j. This means that if A belongs to $C(G)$, it must look as follows:

$$A = \begin{bmatrix} a & b & \cdots & b \\ b & a & \cdots & b \\ & & \ddots & \\ b & b & \cdots & a \end{bmatrix}.$$

Then the size of the centralizer is smaller than $q(q-1)$.

Goppa Codes

Can we find codes that we know lie on the GV bound, and have large automorphism groups? We know that Goppa codes are good. What can we say about their automorphism group?

Let $g(x)$ be an irreducible polynomial of degree t over $\mathbb{F}_{2^m}$. The corresponding Goppa code C_g is given by

$$C_g = \{(c_\alpha | \alpha \in \mathbb{F}_{2^m}) \in \mathbb{F}_2^{2^m} : \sum_{\alpha \in \mathbb{F}_{2^m}} \frac{c_\alpha}{x - \alpha} = 0 \pmod{g(x)}\}.$$

Consider a low weight codeword $c \in C_g$ of weight w, and assume wlog that the nonzero coordinates of c are $c_1, \ldots, c_w$. Then the polynomial

$$\sum_{i=1}^{w} c_i \prod_{j \neq i} (x - \alpha_j)$$

is a polynomial of degree less than or equal to $w - 1$ and is a multiple of $g(x)$. But such a polynomial can have at most w/t irreducible factors of degree t and hence the corresponding word can belong to at most w/t codes.