BCH codes

Let us first define subcodes over subfields. In this setting we have a large field $\mathrm{GF}(q^m)$, and a (linear) code C over $\mathrm{GF}(q^m)$. We want to get a code over $\mathrm{GF}(q)$, using C. There are two natural ways to get such a code. First of all, the elements of $\mathrm{GF}(q^m)$ can be represented as vectors of length m over $\mathrm{GF}(q)$ (just write each element as a linear combination in a fixed basis). If C has parameters $[n,k,d]_{q^m}$, then with this idea we get a $[nm, km, \geq d]_q$ code. The disadvantage is that the minimum distance stays the same. This idea is used in practice to design codes which can correct long *burst errors*. Namely, if we have a burst error of length $h \leq (d-1)m+1$ (that is h consecutive errors), then it only affects at most d (consecutive) coordinates in the original code C, so it can be corrected.

The other idea is the one we will consider in more details. Let us just consider those codewords of C, whose coordinates belong to $\mathrm{GF}(q)$. This code is usually denoted as $C|_q$. Then the length does not increase, the minimum distance does not decrease, the only problematic parameter is the dimension. This can be estimated in the following way: let H be a parity check matrix of C. (So, the elements of H are from $\mathrm{GF}(q^m)$.) Write the elements h_{ij} as a *column* vectors of length m (as before, we write the elements of $\mathrm{GF}(q^m)$ in a fixed basis). This way, we get a matrix H^*, which has $m(n-k)$ rows and n columns. Note that the original H is a sort of parity check matrix for $C|_q$ in the sense that $cH^T = 0$, and this applies for the larger matrix H^*. The problem with H is that its elements do not belong to $\mathrm{GF}(q)$, the problem with H^* is that its rows are not necessarily independent. The „real" parity heck matrix is obtained from H^* by selecting a basis of the rows. This matrix will be denoted as H_q.

Definition. Let C be a $[n,k,d]_{q^m}$ code (over the field $\mathrm{GF}(q^m)$). The *subfield subcode* $C|_q$ consists of all codewords of C, whose coordinates belong to $\mathrm{GF}(q)$.

Proposition. *Let C be a $[n,k,d]_{q^m}$ code (over the field $\mathrm{GF}(q^m)$). The code $C|_q$ is an $[n,k_0,\geq d]_q$ code with $n - m(n-k) \leq k_0 \leq k$.*

As we saw above, the parity check matrix H_q has at most $m(n-k)$ rows. This gives the lower bound. The upper bound comes from the fact that the above operations do not change the column rank (so, whenewer a set of $n-k$ columns are independent in H, then the corresponding columns are independent in H_q).

To define the BCH codes we have to recall the definition of Reed-Solomon codes in the polynomial setting.

Definition. Let $\alpha \in \mathrm{GF}(q)$ be a primitive n-th root of unity, $n|q-1$. Consider the polynomial $g^*(x) = (x-\alpha^t)(x-\alpha^{t+1})\dots(x-\alpha^{t+n-k-1})$ for a fixed t. Then $C = \{g^*(x)f(x) : \deg(f) \leq k-1\}$ is called the narrow sense Reed-Solomon code in the polynomial setting. We remark that they have parameters $[n, k, n-k+1]_q$, since they are GRS codes.

To define the BCH (Bose, Ray-Chaudhuri, Hocquenheim) code we will consider the Reed-Solomon codes over a larger field $\mathrm{GF}(q^m)$ and consider the subfield subcode over $\mathrm{GF}(q)$.

Definition. Let q^m be such that $n|q^m - 1$ and let $\alpha \in \mathrm{GF}(q^m)$ be a primitive n-th root of unity. The BCH code $\mathrm{BCH}_{\alpha,t,\delta}$ is the subfield subcode of the RS code over $\mathrm{GF}(q^m)$ in the polynomial setting. More explicitely, let $g^*(x) = (x-\alpha^t)(x-\alpha^{t+1})\dots(x-\alpha^{t+\delta-2})$ for a fixed t. Then

$$\mathrm{BCH}_{\alpha,t,\delta} = \{f(x) \in \mathrm{GF}(q)[x] : \deg(f) \leq n-1,\ g(x)|f(x)\}.$$

The parameter δ is called the *designed distance* of the BCH code.

Note that the parameters of the RS code over $\mathrm{GF}(q^m)$ are $[n, n-\delta+1, \delta]_{q^m}$. We just have to compare the value $\delta - 2$ with $n-k-1$ in the above definition. This clearly implies that the BCH code has $d \geq \delta$. On the other hand, it is known (we will not show it) that $d \leq 2\delta$, so we essentially know the minimum distance.

Recall that one way to describe a cyclic code is to specify the roots (or some of the roots) of $g(x)$ in a field extension of $\mathrm{GF}(q)$. If the roots $\alpha_1, \dots, \alpha_s$ are given, then $g(x)$ will be the least common multiple of the minimal polynomials of $\alpha_1, \dots, \alpha_s$.

Proposition (BCH bound). *If α is a primitive n-th root of unity in $\mathrm{GF}(q^m)$, and for the generator polynomial $g(x)$ of a cyclic code over $\mathrm{GF}(q)$ we have that $\alpha^t, \alpha^{t+1}, \dots, \alpha^{t+\delta-2}$ are roots of $g(x)$, then the minimum distance of $C = (g(x))$ is at least δ.*

Roughly speaking, the narrow sense RS code defined over $\mathrm{GF}(q^m)$ by α, t, δ contains the code C, so C is a subcode of the BCH code $\mathrm{BCH}_{\alpha,t,\delta}$. The minimum distance of the BCH code is at least the designed distance δ.

In the definition of the BCH codes the polynomial $f(x)$ is over $\mathrm{GF}(q)$, the polynomial $g^*(x)$ is defined over $\mathrm{GF}(q^m)$, hence it would be natural to describe this divisibility over $\mathrm{GF}(q)$. To do this, we have to recall the notion of minimal polynomial of an element α^i in $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$. This is the polynomial $m_{\alpha^i}(x) \in \mathrm{GF}(q)[x]$ of smallest degree, of which α^i is a root (that is, $m_{\alpha^i}(\alpha^i) = 0$). We have learnt that besider α^i, also $\alpha^{qi}, \alpha^{q^2 i}, \dots$ are rooth of $m_{\alpha^i}(x) \in \mathrm{GF}(q)[x]$ an actually it is the product of $(x-\beta)$, where β runs through the algebraic conjugates of α^i. So, the generator polynomial of the BCH codes can be written in the following way: determine $m_{\alpha^i}(x) \in \mathrm{GF}(q)[x]$ for $i = t, \dots t+\delta-2$. Then $g(x)$ will be the least common multiple of these polynomials. Actually, we just have to ignore those $m_{\alpha^i}(x)$, which occur more than once in this list and take the product of the remaining ones.

This also shows how the dimension of BCH codes can be computed.

Proposition. *The dimension k of the code* $\mathrm{BCH}_{\alpha,t,\delta}$ *is* $n - \deg(g)$*, where* $g(x)$ *is the least common multiple of the minimal polynomials* $m_{\alpha^i}(x)$*. In terms of* δ*, we have* $n - m(\delta - 1) \leq k \leq n - (\delta - 1)$*.*

Finally, our favourite code, the binary Hamming code can be obtained as a BCH code.

Proposition. *Let* $n = 2^m - 1$ *and let* α *be a primitive* n*-th root of unity in* $\mathrm{GF}(2^m)$*. Then the BCH code defined by* α*,* $t = 1$*, and* $\delta = 2$ *is the (binary) Hamming code* $\mathrm{Ham}(m)$*.*

Note that $\mathrm{BCH}_{\alpha,1,2} = \mathrm{BCH}_{\alpha,1,3}$, because not only α but also the element α^2 is automatically a root of $m_\alpha(x)$. Hence the minimum distance is at least 3. The dimension of the code is at least $n - m$. The Hamming bound gives that in both cases we must have equality, hence the parameters are the same as in case of $\mathrm{Ham}(m)$. Since the code is linear, it is $\mathrm{Ham}(m)$.

The altermative proof is that the parity check matrix (H above) is $(1, \alpha, \ldots \alpha^{n-1})$ if we consider the original RS code over $\mathrm{GF}(2^m)$. The coordinates are just the non-zero elements (in a certain order). Therefore, expressing them over $\mathrm{GF}(2)$ gives all the non-zero vectors of length m (the matrix H^* above). This is the parity check matrix of $\mathrm{Ham}(m)$, in paricular, the rows are independent and $H^* = H|q$.