1 MDS codes, GRS codes

The minimum distance of the code can be found using the parity check matrix.

Theorem 1.1 *Let C be a linear code and H be a parity check matrix of it. The minimum distance of C is $d+1$ if and only if every d columns of H are linearly independent but there are $d+1$ columns that are dependent.*

Proof. We can show the assertion for minimum weight instead of minimum distance, since they are equal. For a codeword $\mathbf{c} \in \mathbf{C}$, we have $\mathbf{cH^T} = \mathbf{0}$. This gives a linear combination of the columns of H yielding the zero vector. The number of non-zero coefficients in this linear combination is the weight of our codeword $\mathbf{c}$. This observation proves our theorem. ■

Let us remark that finding the minimum distance of a code is seemingly simple but it is actually computationally difficult.

"Good codes" can correct many errors. In case of linear codes the error correcting capability and the dimension of the code work against each other if the length is given. This is the content of the next theorem.

Theorem 1.2 (Singleton's bound for linear codes) *If d denotes the minimum distance of a linear C $[n, n-k]$ code then*

$$d \leq k+1.$$

Proof. It is enough to show that C contains a non-zero codeword with weight at most $k+1$. If G is a generator matrix of C then we can transform G, using elementary transformations, into the form

$$G = (I_{(n-k)\times(n-k)} | G^*_{(n-k)\times k}),$$

which is also a generator matrix of C. Here I_{n-k} is the $(n-k)\times(n-k)$ identity matrix. Since there are at most k non-zero elements in each row of G^*, the weight of the codeword corresponding to any row of G^* is at most $k+1$.■

Definition 1.3 *If the minimum distance of a linear $[n, n-k]$ code is d and the inequality in Singleton's bound is satisfied with equality, that is $d = k+1$, then the code is called an* MDS code.

According to Theorem 1.2, MDS codes have the largest minimum distance for a given dimension. In case of a given length and minimun distance MDS codes have the largest dimension. This essentially means that MDS codes are optimal in many respects. However, for a given q and a pair (n, k) there does not exist an MDS code with these parameters in general.

The next result gives a connection of MDS codes and arcs in higher dimensions, it is very much related to György Kiss's course on Finite Geometry. Let us recall first the definition of an arc: it is a set of points in $\mathrm{PG}(r, q)$ with the property that no $r + 1$ points lie in a hyperplane (are dependent). This geometric connection allows us to use geometric techniques.

Theorem 1.4 *Let us fix q, the size of the underlying field. For given natural numbers n and k there is a linear MDS code with parameters $[n, n-k]$ if and only if there is an n-arc in the projective space* $\mathrm{PG}(k-1, q)$.

Proof. Assume that there is a linear $[n, n-k, k+1]_q$ code C. Let H denote a parity check matrix of C. Then any k columns of H are linearly independent by Theorem 1.1.

Cosider the columns as points in $\mathrm{PG}(k-1, q)$. The linear independence of any k columns of H implies that no k of these points are in a hyperplane. Hence these points form an arc (consisting of n points).

Conversely, assume that there is an n-arc in $\mathrm{PG}(k-1, q)$. Let H be the matrix of size $n \times k$ whose columns are representative vectors of the points of our n-arc. Then H is a parity check matrix of a linear $[n, n-k]$ code C. Any set of k columns of H are indeppendent, since the points form an arc. So the minimum distance of the code is at least $k+1$. By Singleton's bound we have equality here, hence C is an MDS code. ∎

Theorem 1.5 *The dual of an MDS code is an MDS code.*

Proof. Let C be an MDS code of length n and dimension $n-k$. Let us denote by H a parity check matrix of C. It is the generator matrix of the dual code $C^{\perp}$. To prove that $C^{\perp}$ is MDS we have to show that any linear combination of the rows of H has weight at least $n-k+1$. Replacing an appropriate row of H by this linear combination of the rows one can see that it is enough to check this for an arbitrary row of H. As any k columns of H are independent, no row of H can contain k 0-s. Thus the weight of any row is at least $n-k+1$ and it cannot be larger by Singleton's bound. ∎

Let us now see the usual description of *Reed-Solomon codes*. The codes are called generalized Reed-Solomon (GRS) codes. The reason we need the slight generalization will be clear after the result on duals of such codes.

Definition 1.6 *Let* $\mathbf{a} = (\alpha_\mathbf{1}, \ldots, \alpha_\mathbf{n})$ *be a vector consisting of* n *pairwise distinct elements of* $\mathrm{GF(q)}$. *Moreover, let* $\mathbf{v} = (\mathbf{v_1}, \ldots, \mathbf{v_n})$ *be a fixed vector having no zero coordinates, that is* $v_i \neq 0$ *for every* $i = 1, \ldots, n$. *Define the code* $\mathrm{GRS_k}(\mathbf{a}, \mathbf{v})$ *by*

$$\mathrm{GRS_k}(\mathbf{a}, \mathbf{v}) = \{(\mathbf{v_1 f}(\alpha_\mathbf{1}), \ldots, \mathbf{v_n f}(\alpha_\mathbf{n})) : \mathbf{f} \in \mathrm{GF(q)[x]},\, \deg \mathrm{f} < \mathrm{k}\}.$$

This code is called a generalized Reed-Solomon code. *In other words, we evaluate polynomials of degree less than* k *at* $\alpha_1, \ldots, \alpha_n$, *and multiply the result coordinatewise by the vector* $\mathbf{v}$.

As polynomials of degree less than k form a vector space of dimension k, we immediately get that $\mathrm{GRS_k}(\mathbf{a}, \mathbf{v})$ is a linear $[n, k]$ code. Assume that $\mathrm{GRS_k}(\mathbf{a}, \mathbf{v})$ contains a codeword of weight less than $n - k + 1$. This must come from a polynomial f, which is zero for at least k of the α_i's. By the fact that a polynomial has at most as many roots as its degree, such a polynomial f must be the zero polynomial. This contradiction shows that the minimum weight, and hence the minimum distance, of $\mathrm{GRS_k}(\mathbf{a}, \mathbf{v})$ is at least $n - k + 1$.

So the GRS code is MDS by Singleton's bound. To describe the code explicitly, we can choose the basis $1, x, \ldots, x^{k-1}$ in the vector space of polynomials of degree less than k and consider the corresponding vectors in $\mathrm{GRS_k}(\mathbf{a}, \mathbf{v})$. They are consecutive powers of the elements α_i multiplied by v_i. Clearly, these vectors form a basis of the GRS code. Putting them in a generator matrix we get a Vandermonde type matrix, where the columns are multiplied by non-zero field elements.

Proposition 1.7 $\mathrm{GRS_k}(\mathbf{a}, \mathbf{v})^\perp = \mathrm{GRS_{n-k}}(\mathbf{a}, \mathbf{v}')$, *for a suitable vector* $\mathbf{v}'$.

Proof. The vector $\mathbf{v}'$ turns out to be independent of k. Hence we find it for $k = n - 1$ and then show that it is suitable for any k.

The code $\mathrm{GRS_{n-1}}(\mathbf{a}, \mathbf{v})$ is MDS, hence its dual $\mathrm{GRS_{n-1}}(\mathbf{a}, \mathbf{v})^\perp$ is also MDS. This dual code has dimension $1 = n - (n - 1)$ and its minimum distance is $n - 1 + 1 = n$. If $\mathbf{v}' = (\mathbf{v}'_\mathbf{1}, \ldots, \mathbf{v}'_\mathbf{n})$ generates this 1-dimensional

subspace, then $v_i' \neq 0$, for every i. As $\mathbf{v}'$ is orthogonal to the standard basis of $\mathrm{GRS}_{n-1}(\mathbf{a}, \mathbf{v})$ we get

$$0 = \sum_{i=1}^{n} v_i v_i' \alpha_i^j, \quad 0 \leq j < n-1.$$

In the j-th equation the polynomial x^j was evaluated at the coordinates of $\mathbf{a}$. The same system of equations immediately implies that $(v_1\alpha_1^s, \ldots, v_n\alpha_n^s)$ is orthogonal to the vector $(v_1'\alpha_1^t, \ldots, v_n'\alpha_n^t)$ if $s + t < n - 1$. In our case $t \leq n - k - 1$, $s \leq k - 1$, proving the assertion. ■

This theorem shows why one generalizes Reed Solomon codes: it is not true that the dual code of an RS code is an RS code but it is true for GRS codes.