Vector Spaces over Finite Fields

First recall the basic notions about vector spaces: linear combination of vectors, linear independence/dependence, generating system, basis, dimension, subspace, subspace generated by a set of vectors,...

If the ground field is finite, nothing changes, so for example there is a unique n-dimensional vector space, namely $\mathrm{GF}(q)^n$, that is the sequences of length n, whose elements belong to $\mathrm{GF}(q)$. In coding theory a vector will always be a **row** vector.

The unique n-dimensional vector space over $\mathrm{GF}(q)$ will be denoted as $V = V(n,q)$. Hence $|V| = q^n$.

We need to describe subspaces of $V = V(n,q)$. Let $U \leq V$ be the k-dimensional subspace generated by the (independent) vectors $\mathbf{g}_1, \ldots, \mathbf{g}_k$. Denote the coordinates by $\mathbf{g}_i = (g_{i1}, \ldots, g_{in})$. Then the subspace U can be described by the $k \times n$-matrix

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{pmatrix}.$$

Note that G has rank k, so the rows are independent, this is essentially the only condition. Two $k \times n$ matrices G and G' are generator matrices of the same subspace if and only if the rows of G' are linear combinations of G, and vice versa. This means that $G' = BG$ for some non-singular (invertible) $k \times k$ matrix B.

There is another way of describing a k-dimensional subspace, namely as an intersection of hyperplanes ($(n-1)$-dimensional subspaces). To get a k-dim. subspace we need to take the intersection of $n-k$ independent hyperplanes. A hyperplane can be described by a linear equation, so $H = \{(x_1, \ldots, x_n) : h_1 x_1 + \ldots + h_n x_n = 0\}$. Hence the intersectionf $n-k$ independent hyperplanes can be described as the set of solutions of a system of $n-k$ independent (homogeneous) linear equations, so by $xH^T = 0$ for some $(n-k) \times n$ matrix H of rank $n-k$.

This can be made more explicit by introducing the scalar product and the orthogonal complement.

Definition. Let $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ be two vectors. Then $x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n$. Instead of $x \cdot y$ we typically just write xy. We say that $x \perp y$ if $xy = 0$.

Of course, all the operations are to be computed in the ground field. (For example, if $x = (1, 2, 1, 0)$ and $y = (2, 0, 2, 0)$ and we are over the field GF(3), then $x \cdot y = 2 + 0 + 2 + 0 = 1$. If these elements are in GF(5), then the result is 4.)

In general, we always have to be very careful how to interpret symbols. They can be scalars (elements of the ground field), vectors, and in this case we have to clarify the length. We also note that these things are very similar to the same notions over the reals, the main difference is that over a finite field $xx = 0$ is possible also for $x \neq 0$. An easy example for this is the vector $(1, 1) \in \mathrm{GF}(2)^2$.

Definition. For a subspace $U \leq V$ we define $U^\perp = \{x \in V : x \cdot u = 0, \forall u \in U\}$.

This is similar to the orthogonal complement but it is in general not true that $U \cap U^\perp = \{0\}$. On the other hand, it is true that $\dim(U^\perp) = n - k$, if $\dim(U) = k$. Indeed, it is enough to check $x \cdot u = 0$ for a basis $u_1, \ldots, u_k$. This is a set of k independent homogeneous linear equations that defines $U^\perp$. From linear algebra it follows that k such equations define an $(n - k)$-dimensional subspace. It is clear that $U \leq (U^\perp)^\perp$, and from the dimensions above we have equality here. So $U = (U^\perp)^\perp$.

Consider a generator matrix of $U^\perp$. Such a matrix is called a *parity check matrix* of the original subspace U. Using $U = (U^\perp)^\perp$, we have that H and H' are parity check matrices of the same subspace if and only if $H = BH'$, for an invertible (non-singular) $(n - k) \times (n - k)$ matrix.

Finally note that for the generator matrix G and parity check matrix of a subspace U we have $GH^T = O$, where O is the $k \times (n - k)$ all-zero matrix.

The next theorem gives an important connection between the generator and the parity check matrix.

Theorem. *Assume that G, the generator matrix of a subspace U, is of the the form $(I_k|A)$. Then the matrix $H = (-A^T|I_{n-k})$ is a parity check matrix of U.*

We will sometimes work in *the affine space* $\mathrm{AG}(n, q)$. Here the points are the same as in $V(n, q)$, the only difference is that we also consider affine subspaces, which are translates (or cosets) of a vector subspace. So, if U is a k-dim. vector subspace, then $x + U$ is a k-dim. affine subspace and these are all affine subspaces.

We will also use the *projective space* $\mathrm{PG}(n, q)$. Here the points are 1-dim. subspaces of $V(n + 1, q)$ and a k-dim projective subspace is nothing else than a $(k + 1)$-dim. vector subspace.

Finally, for some counting, let us see what the number of k-dimensional subspaces of $V(n, q)$ is. This number is called the q-binomial coefficient (or Gaussian binomial coefficient) and it is

$$\frac{\prod_{i=0}^{k-1}(q^n - q^i)}{\prod_{i=0}^{k-1}(q^k - q^i)}.$$

The usual notation for this is $\begin{bmatrix} n \\ k \end{bmatrix}_q$.