Chapter 4

Vector Spaces over Finite Fields

Definition 4.1. $V(n,q) = (GF(q)^n, +, \times) = ((\mathbf{F}_q)^n, +, \times)$, where with $x_i, y_i, \lambda \in \mathbf{F}_q$

$$x = (x_1, x_2, \ldots, x_n), \quad y = (y_1, y_2, \ldots, y_n),$$
$$x + y = (x_1 + y_1, \ldots, x_n + y_n), \quad \lambda x = (\lambda x_1 + \lambda x_2, \ldots, \lambda x_n).$$

Theorem 4.2. *$V(n,q)$ is a vector space over $\mathbf{F}_q$; that is,*

(i) *$(V(n,q), +)$ is an abelian group with identity $0 = (0, \ldots, 0)$; that is,*

- (a) *$x + y \in V(n,q)$ for all $x, y \in V(n,q)$;*
- (b) *$(x + y) + z = x + (y + z)$ for all $x, y, z \in V(n,q)$;*
- (c) *$0 + x = x + 0 = x$ for all $x \in V(n,q)$;*
- (d) *for $x \in V(n,q)$ there exists $-x \in V(n,q)$ with $x + (-x) = x + (-x) = 0$;*
- (e) *$x + y = y + x$ for all $x, y \in V(n,q)$.*

(ii) *With $x, y \in V(n,q)$ and $\lambda, \mu \in \mathbf{F}_q$,*

- (a) *$\lambda(x + y) = \lambda x + \lambda y$;*
- (b) *$(\lambda + \mu)x = \lambda x + \mu x$;*
- (c) *$(\lambda\mu)x = \lambda(\mu x)$;*
- (d) *$1x = x$.*

Definition 4.3. A *subspace* of $V(n,q)$ is a subset of $V(n,q)$ which is a vector space under the same operations.

Theorem 4.4. *A subset C of $V(n,q)$ is a subspace if*

(i) *$x + y \in C$ for all $x, y \in C$;*

(ii) *$\lambda x \in C$ for all $x \in C$, $\lambda \in \mathbf{F}_q$.*

Example 4.5. $\{(x_1, x_2, 0) \mid x_i \in \mathbf{F}_q\}$ is a subspace of $V(3,q)$.

Example 4.6. $\{0\}$, $V(n,q)$ are subspaces of $V(n,q)$.

Example 4.7. If $v_1, \ldots, v_s \in V(n, q)$, then

$$\{\lambda_1 v_1 + \cdots + \lambda_s v_s \mid \lambda_i \in \mathbf{F}_q\}$$

is a subspace; that is, the set of all linear combinations of $v_1, \ldots, v_s$ is a subspace.

Definition 4.8. (i) $v_1, \ldots, v_s$ are *linearly independent* if $\lambda_1 v_1 + \cdots + \lambda_s v_s = 0 \Rightarrow \lambda_i = 0$ for all i.

(ii) $v_1, \ldots, v_s$ are *linearly dependent* if there exist $\lambda_1, \ldots, \lambda_s \in \mathbf{F}_q$ not all zero such that $\lambda_1 v_1 + \cdots + \lambda_s v_s = 0$.

Definition 4.9. (i) Let C be a subspace of $V(n, q)$. Then $\{v_1, \ldots, v_s\}$ is a *spanning* or *generating* set for C if every element of C is a linear combination of $v_1, \ldots, v_s$; that is, given x in C, there exist $\lambda_1, \ldots, \lambda_s \in \mathbf{F}_q$ such that

$$x = \lambda_1 v_1 + \cdots + \lambda_s v_s.$$

(ii) If $v_1, \ldots, v_s$ are linearly independent, then $\{v_1, \ldots, v_s\}$ is a *basis*. In this case $\lambda_1, \ldots, \lambda_s$ are unique.

Example 4.10. $\{(0, 1, 1), (1, 0, 1), (1, 1, 0)\}$ generates a subspace

$$\{(\lambda_2 + \lambda_3, \lambda_1 + \lambda_3, \lambda_1 + \lambda_2) \mid \lambda_i \in \mathbf{F}_2\}$$

of $V(3, 2)$. For example, $\{(0, 1, 1), (1, 0, 1)\}$ is a basis.

Theorem 4.11. *If C a subspace of $V(n, q)$,*

(i) *every generating set contains a basis*;

(ii) *every basis contains the same number of elements, called the* dimension *of C*;

(iii) $|C| = q^k$, *where $k = \dim C$.*

Algorithm 4.12. Given a set of vectors generating C find a basis and hence the dimension of C.

Write the vectors as rows of a matrix A and perform the following operations:

(R1) $r_i \to \lambda r_i$ any $\lambda \in \mathbf{F}_q \setminus \{0\}$;

(R2) $r_i \leftrightarrow r_j$;

(R3) $r_i \to r_i + \lambda r_j$ any $\lambda \in \mathbf{F}_q$.

Hence reduce A to *echelon form*:

$$
\begin{array}{ccc|cccc|ccc}
0 & \cdots & 0 & 1 & * & \cdots & * & * & \cdots & * \\
0 & \cdots & 0 & 0 & 1 & \cdots & * & * & \cdots & * \\
 & \vdots & & & & \vdots & & & \vdots & \\
0 & \cdots & 0 & 0 & 0 & \cdots & 1 & * & \cdots & * \\
\hline
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
 & \vdots & & & & \vdots & & & \vdots & \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0
\end{array}
$$

Example 4.13. $q = 3$ $\quad (2,1,2), (1,2,2), (0,1,2)$

$$
\begin{array}{ccc}2&1&2\\1&2&2\\0&1&2\end{array} \to
\begin{array}{ccc}1&2&1\\1&2&2\\0&1&2\end{array} \to
\begin{array}{ccc}1&2&1\\0&0&1\\0&1&2\end{array} \to
\begin{array}{ccc}1&2&1\\0&1&2\\0&0&1\end{array} \qquad k = 3
$$

Example 4.14. $q = 2$ $\quad (0,1,1), (1,0,1), (1,1,0)$

$$
\begin{array}{ccc}0&1&1\\1&0&1\\1&1&0\end{array} \to
\begin{array}{ccc}1&0&1\\0&1&1\\1&1&0\end{array} \to
\begin{array}{ccc}1&0&1\\0&1&1\\0&1&1\end{array} \to
\begin{array}{ccc}1&0&1\\0&1&1\\0&0&0\end{array} \qquad k = 2
$$

Example 4.15. $q = 2$ $\quad (0,0,1,1), (0,1,0,1), (0,1,1,0)$

$$
\to \begin{array}{cccc}0&1&0&1\\0&0&1&1\\0&0&0&0\end{array} \qquad k = 2
$$

Example 4.16. $q = 7$ $\quad (3,4,2), (6,0,5), (0,1,6)$

$$
\begin{array}{ccc}3&4&2\\6&0&5\\0&1&6\end{array} \to
\begin{array}{ccc}1&6&3\\6&0&5\\0&1&6\end{array} \to
\begin{array}{ccc}1&6&3\\0&1&6\\0&1&6\end{array} \to
\begin{array}{ccc}1&6&3\\0&1&6\\0&0&0\end{array} \qquad k = 2
$$