

1 Background for coding theory

The concepts revised in this section are important background for coding theory. We believe that most of you are familiar with these concepts so we will not spend time in class discussing them. Please read through this section carefully in your own time and ensure that you are familiar with the concepts and examples presented here. Solutions to the exercises are included at the end of the section. Throughout these notes, the abbreviation iff will be used for “if and only if”.

1.1 Vector spaces

In previous courses you most likely dealt with vectors whose components were real numbers, for example the vector $(3, 4)$ in \mathbb{R}^2 or the vector $(2, -1, 3)$ in \mathbb{R}^3 . The vectors we will use in coding theory are binary vectors, that is, each component is 0 or 1. We will usually write our vectors without brackets and without commas between components.

Definition 1.1 Let $K = \{0, 1\}$. For $a, b \in K$, define $a + b = 0$ iff $a = b$, and $a + b = 1$ otherwise. Define $a \times b = 1$ iff $a, b = 1$, and $a \times b = 0$ otherwise. An element $a \in K$ is called a *scalar*.

Definition 1.2 Let $K^n = \{a_1a_2 \dots a_n \mid a_i \in K, 1 \leq i \leq n\}$, and call an element $v \in K^n$ a *vector*. For $u, v \in K^n$, define $u + v$ componentwise, using addition as defined above on K . Define scalar multiplication of $v \in K^n$ by $a \in K$ by multiplying each component of v by a , using multiplication as defined above on K . If v contains all 0s, then v is called the *zero vector* and is denoted $\mathbf{0}$.

As an example, consider the vectors $u = 01011$ and $v = 11001$ in K^5 . The sum $u + v = 10010$ and the scalar multiples of u with scalars 0 and 1 are $0u = 00000$ and $1u = 01011$. It is easy to see that if you sum two elements of K^n , the result is an element of K^n and if you take a scalar multiple of K^n (with scalar 0 or 1) then the result is an element of K^n . Thus K^n is closed under addition and scalar multiplication. We will use the terms “word” and “vector” interchangeably.

Definition 1.3 Let $u, v, w \in K^n$ be words (vectors) of length n and let $\alpha, \beta \in K$ be scalars. Then, using addition and scalar multiplication as defined, K^n is a *vector space*. That is, it satisfies the properties:

1. $v + w \in K^n$
2. $(u + v) + w = u + (v + w)$
3. $v + \mathbf{0} = \mathbf{0} + v = v$, where $\mathbf{0}$ is the zero word
4. there exists $v' \in K^n$ such that $v + v' = v' + v = \mathbf{0}$
5. $v + w = w + v$
6. $\alpha v \in K^n$
7. $\alpha(v + w) = \alpha v + \alpha w$
8. $(\alpha + \beta)v = \alpha v + \beta v$
9. $(\alpha\beta)v = \alpha(\beta v)$
10. $1v = v$

Notice that the vector v' in property 4 above is actually the vector v itself.

Definition 1.4 A nonempty subset U of a vector space V is a *subspace* of V if U is closed under vector addition and scalar multiplication. That is, U is a subspace of V if for any $v, w \in U$ and any scalar α , we have $v + w \in U$ and $\alpha v \in U$.

As the only scalars in K are 0 and 1, a subset U of K^n is a subspace of K^n iff U is closed under addition.

In the remainder of this section we will be solving many equations over K . Note that since we are using binary arithmetic, if $x, y \in K$ then the following statements hold.

- If you sum a variable an even number of times, you will get zero, regardless of the value of the variable. In particular, if $x + x = 0$ then you cannot conclude anything about the value of x .
- If you sum a variable an odd number of times, you can get either zero or one. In particular, if $x + x + x = 0$, then $x = 0$ and if $x + x + x = 1$ then $x = 1$.
- If $x + y = 0$ then $x = y$.
- If $x + y = 1$ then precisely one of x or y is 1 (and the other is 0).

Definition 1.5 A vector w is a *linear combination* of vectors v_1, v_2, \dots, v_k if there are scalars $\alpha_1, \alpha_2, \dots, \alpha_k$ such that

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_k v_k.$$

Definition 1.6 The set of all linear combinations of the vectors in a given set $S = \{v_1, v_2, \dots, v_k\}$ is called the *linear span* or *span* of S , and is written $\langle S \rangle$.

If S is empty, we define $\langle S \rangle = \{\mathbf{0}\}$.

For any subset S of a vector space V , the span $\langle S \rangle$ is a subspace of V , called the subspace *spanned* or *generated* by S . In particular, if we have a subset S of the vector space K^n , we have the following characterisation of $\langle S \rangle$.

Theorem 1.7 For any subset S of K^n , the set $\langle S \rangle$ consists precisely of the following words: the zero word, all words in S , and all sums of two or more words in S .

We say that S is *minimal* if removing any element of S gives a different span.

Definition 1.8 If the set $C = \langle S \rangle$ and S is minimal, then we say that S is a *generator set* for C . Usually there is more than one generator set for a set C .

Exercise 1.9 Let $S = \{0100, 0011, 1100\}$. Find the set C generated by S . (Solution on page 7.)

Definition 1.10 A set of vectors $S = \{v_1, v_2, \dots, v_k\}$ is *linearly dependent* if there are scalars $\alpha_1, \alpha_2, \dots, \alpha_k$ not all zero such that

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_k v_k = \mathbf{0}.$$

Otherwise, S is said to be *linearly independent*.

The above definition of linear dependence is equivalent to saying that one of the vectors in S can be written as a linear combination of other vectors in S .

Algorithm 1.11 Test for linear independence

To test a set $S = \{v_1, v_2, \dots, v_k\}$ for linear independence, form the vector equation

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_k v_k = \mathbf{0}$$

for arbitrary scalars $\alpha_1, \alpha_2, \dots, \alpha_k$. If this equation forces **all** of the scalars to be 0, then S is linearly independent. If *at least one* scalar α_i can be chosen to be nonzero then S is linearly dependent.

Exercise 1.12 Is the set $S = \{110, 011, 101, 111\}$ linearly independent? (Solution on page 7.)

Any set of vectors $S \neq \{\mathbf{0}\}$ contains a largest linearly independent subset. We can find such a subset by continually removing from S those vectors which can be written as a linear combination of other vectors in S .

Exercise 1.13 Using S as defined in Exercise 1.12, show that the vector 101 can be written as the linear combination of other vectors in S . Then show that $S' = S \setminus \{101\}$ is a linearly independent set. (Solution on page 7.)

Any set of vectors containing the zero vector is linearly dependent (if vector v_i is the zero vector, take $\alpha_i = 1$ and $\alpha_j = 0$ for all $j \in \{1, 2, \dots, n\}$, $i \neq j$).

We have the following important definition:

Definition 1.14 A nonempty subset of vectors B from a vector space V forms a *basis* for V if

1. B spans V , so $V = \langle B \rangle$; and
2. B is a linearly independent set.

The plural of basis is bases.

Any linearly independent set of vectors B is automatically a basis for $\langle B \rangle$.

Exercise 1.15 Let $S = \{0101, 1010, 1100, 1111\}$. Find a basis B for the set $C = \langle S \rangle$ and list the vectors in C . (Solution on page 7.)

Exercise 1.16 Find a basis for K^4 . (Solution on page 8.)

Definition 1.17 In general a vector space usually has many bases. However, *all bases for a vector space contain the same number of elements*, and this number is called the *dimension* of the vector space.

Exercise 1.18 What is the dimension of K^n ? What is the dimension of the set C in Exercise 1.15? (Solution on page 8.)

Given a vector space V with basis $\{v_1, v_2, \dots, v_k\}$, any vector $w \in V$ can be expressed as a unique combination of the basis vectors. That is, given any $w \in V$, there exist unique scalars $\alpha_1, \alpha_2, \dots, \alpha_k$ such that $w = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_k v_k$.

Exercise 1.19 Let C be the set defined in Exercise 1.15. Write each of the following vectors of C as a unique linear combination of the vectors in the basis $B = \{0101, 1010, 1100\}$:

$$1111 \quad 0011 \quad 0101 \quad 0000$$

(Solution on page 8.)

If a subspace C of K^n has dimension k and if $B = \{v_1, v_2, \dots, v_k\}$ is a basis for C , then each vector w in C can be written as

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_k v_k$$

for a unique choice of scalars $\alpha_1, \alpha_2, \dots, \alpha_k$. Noting that each α_i is either 0 or 1, for $1 \leq i \leq k$, there are 2^k distinct choices for $\alpha_1, \alpha_2, \dots, \alpha_k$. We thus have the following very important theorem.

Theorem 1.20 *A subspace of K^n having dimension k contains precisely 2^k vectors.*

1.2 Orthogonal vectors

Definition 1.21 If $v = v_1 v_2 \dots v_n$ and $w = w_1 w_2 \dots w_n$ are vectors in K^n , we define the *scalar product* or *dot product* of v and w by

$$v \cdot w = v_1 w_1 + v_2 w_2 + \dots + v_n w_n.$$

Note that this matches the usual definition of dot product in \mathbb{R}^n . In particular, the dot product is a scalar, not a vector.

Definition 1.22 Vectors v and w are said to be *orthogonal* if $v \cdot w = 0$. If S is a set of vectors in K^n , we say that a vector v is *orthogonal to the set S* iff $v \cdot w = 0$ for all vectors $w \in S$. The set of all vectors orthogonal to S is denoted by S^\perp , and is called the *orthogonal complement* of S .

For any subset S of a vector space V , the orthogonal complement S^\perp is a subspace of V .

Exercise 1.23 If $S = \{0100, 0101\}$, find the orthogonal complement S^\perp . (Hint: write down a general vector of S^\perp as $\alpha_1 \alpha_2 \alpha_3 \alpha_4$ and solve the resulting simultaneous equations.) (Solution on page 8.)

We have the following important result relating the dimensions of the span of a set and its orthogonal complement.

Theorem 1.24 *Let $\langle S \rangle$ be the vector space generated by a subset S of K^n . If the dimension of $\langle S \rangle$ is k_1 and the dimension of S^\perp is k_2 then we must have $k_1 + k_2 = n$.*

Exercise 1.25 Let S be a subset of K^7 and assume S^\perp has dimension 3.

1. Find the dimension of $\langle S \rangle$.
2. Find the number of words in $\langle S \rangle$ and the number of words in S^\perp .

(Solution on page 8.)

1.3 Matrices

Most of the standard methods of dealing with matrices over \mathbb{R} are applied in the same way when working over $K = \{0, 1\}$.

Definition 1.26 The product of an $m \times n$ matrix \mathbf{A} and an $n \times p$ matrix \mathbf{B} , written \mathbf{AB} , is the $m \times p$ matrix which has for its (i, j) entry the dot product of row i of \mathbf{A} with column j of \mathbf{B} .

Definition 1.27 An $m \times n$ matrix in which every entry is 0 is called the *zero* matrix, denoted $\mathbf{0}_{m \times n}$. An $n \times n$ matrix in which the (i, j) entry is 0 if $i \neq j$ and 1 otherwise is called the *identity* matrix, denoted \mathbf{I}_n .

Exercise 1.28 Let A and B be the following matrices over K . Determine AB .

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(Solution on page 8.)

Definition 1.29 There are two *elementary row operations* (EROS) which may be performed on matrices over K . These are:

1. interchange two rows; and
2. replace a row by itself plus another row.

Two matrices are called *row equivalent* if one can be obtained from the other by a sequence of EROS.

Definition 1.30 If a row of a matrix over K is not a zero row (that is, does not contain all zeros), the leftmost 1 in that row is called a *leading* 1. Any column which contains a leading 1 is called a *leading column*.

Definition 1.31 A matrix \mathbf{M} is in *row echelon form* (or REF) if

1. all zero rows of \mathbf{M} occur below all nonzero rows of \mathbf{M} ; and
2. the leading 1 in a nonzero row i is in a column to the right of the leading 1 in any row above row i .

Definition 1.32 If \mathbf{M} has the further property that

3. the only 1 in a leading column is the leading 1

then \mathbf{M} is said to be in *reduced row echelon form*, or RREF.

Any matrix over K is row equivalent to a matrix over K in REF, and to a matrix over K in RREF. For a given matrix, there may be many row equivalent matrices in REF, but its RREF equivalent is unique.

Exercise 1.33 Let $\mathbf{M} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$. Find the RREF of \mathbf{M} . (Solution on page 8.)

Definition 1.34 The *rank* of a matrix \mathbf{M} over K is the number of nonzero rows in any REF of \mathbf{M} .

Definition 1.35 The *transpose* of an $m \times n$ matrix \mathbf{A} is the $n \times m$ matrix \mathbf{A}^T which has column i of \mathbf{A} as its i th row. If \mathbf{A} and \mathbf{B} are matrices over K then $(\mathbf{A}^T)^T = \mathbf{A}$ and $(\mathbf{AB})^T = \mathbf{B}^T \mathbf{A}^T$.

1.4 Permutations, combinations and probability

An ordered selection of m distinct objects from a set of n distinct objects can be made in

$$n \times (n - 1) \times \cdots \times (n - m + 1) = \frac{n!}{(n - m)!}$$

ways, since the first object can be chosen in any of n ways, then the second in any of $(n - 1)$ ways, and so on.

For example, the number of three letter “words” having distinct letters that can be created from the set of letters A, B, C, D is $4 \times 3 \times 2 = 24$ since there are 4 choices for the first letter, 3 choices remaining for the second letter, and 2 choices remaining for the third letter. The “words” are:

$ABC \quad ACB \quad ABD \quad ADB \quad ACD \quad ADC \quad BAC \quad BCA \quad BAD \quad BDA \quad BCD \quad BDC$
 $CAB \quad CBA \quad CAD \quad CDA \quad CBD \quad CDB \quad DAB \quad DBA \quad DAC \quad DCA \quad DBC \quad DCB$

The number of unordered selections of m distinct objects from a set of n distinct objects is

$$\binom{n}{m} = \frac{n!}{m!(n - m)!}$$

For example, the number of three letter combinations having distinct letters that can be created from the set of letters A, B, C, D is

$$\binom{4}{3} = \frac{4!}{3!1!} = \frac{4 \times 3 \times 2 \times 1}{3 \times 2 \times 1 \times 1} = 4.$$

This corresponds to the 24 ordered selections from the previous example, divided by 6 since there are 6 arrangements of three letters. The (unordered) combinations are:

$ABC \quad ABD \quad ACD \quad BCD$

The probability of any event lies between 0 and 1 inclusive. Impossible events have probability 0 and events which are certain to occur have probability 1. For example, if a fair die is thrown then the probability of obtaining a five is $1/6$. The probability of an event A is often denoted by $p(A)$.

There are simple rules for combining probabilities. Suppose that A and B are events and that A' denotes the event that A does not occur.

1. $p(A') = 1 - p(A)$.
2. If A and B are *independent events*, then $p(A \text{ and } B) = p(A) \times p(B)$. By saying that A and B are independent we mean that the occurrence of either event is not influenced by the occurrence of the other.
3. If A and B are *mutually exclusive events*, then $p(A \text{ or } B) = p(A) + p(B)$. By saying that A and B are mutually exclusive we mean that the occurrence of either event precludes the occurrence of the other.

Suppose that an experiment with two possible outcomes (A and A') is repeated n times. If the probability of event A is $p(A) = p$, so $p(A') = 1 - p$, then the probability of A occurring k times out of n is

$$\binom{n}{k} p^k (1 - p)^{n-k}.$$

1.5 Solutions to Exercises

Solution to Exercise 1.9 The set generated by S is the zero vector, all vectors in S , and the sum of any two or more vectors from S . Since $0100 + 0011 = 0111$, $0100 + 1100 = 1000$, $0011 + 1100 = 1111$ and $0100 + 0011 + 1100 = 1011$, we have

$$C = \langle S \rangle = \{0000, 0100, 0011, 1100, 0111, 1000, 1111, 1011\}.$$

Solution to Exercise 1.12 Consider $\alpha(110) + \beta(011) + \gamma(101) + \delta(111) = 000$. Comparing components we obtain the equations

$$\alpha + \gamma + \delta = 0 \quad (1)$$

$$\alpha + \beta + \delta = 0 \quad (2)$$

$$\beta + \gamma + \delta = 0 \quad (3)$$

Summing equations (1), (2) and (3) we obtain $\alpha + \alpha + \beta + \beta + \gamma + \gamma + \delta + \delta + \delta = 0$, but in K twice anything is zero, so this is equivalent to $\delta = 0$. The equations are satisfied if we have

$$\alpha = 1 \quad \beta = 1 \quad \gamma = 1 \quad \delta = 0.$$

Thus the set of vectors is not linearly independent.

Solution to Exercise 1.13 The vector 101 is a linear combination of the other vectors in S since $101 = 1(110) + 1(011) + 0(111)$. We must now consider $\alpha(110) + \beta(011) + \gamma(111) = 000$. This gives the set of equations

$$\alpha + \gamma = 0 \quad (1)$$

$$\alpha + \beta + \gamma = 0 \quad (2)$$

$$\beta + \gamma = 0 \quad (3)$$

Equation (1) says that $\alpha = \gamma$ and equation (3) says that $\beta = \gamma$. Substituting these into equation (2) we see that $\gamma + \gamma + \gamma = 0$ so $\gamma = 0$. Thus the only solution is

$$\alpha = \beta = \gamma = 0$$

so the set S' is a linearly independent set.

Solution to Exercise 1.15 We must find a largest set of linearly independent vectors within the set S . Since $1111 = 1(0101) + 1(1010) + 0(1100)$, the vector 1111 is a linear combination of the other vectors, so we will throw it out. Now consider the equation $\alpha(0101) + \beta(1010) + \gamma(1100) = 0000$. This gives the equations

$$\beta + \gamma = 0 \quad (1)$$

$$\alpha + \gamma = 0 \quad (2)$$

$$\beta = 0 \quad (3)$$

$$\alpha = 0 \quad (4)$$

From equations (3) and (4) we have $\alpha = \beta = 0$ and from equation (1) $\gamma = \beta$ so the only solution is

$$\alpha = \beta = \gamma = 0$$

and the set $B = \{0101, 1010, 1100\}$ is a basis for C . (Note that you could have found other bases for C , but your basis must have three vectors in it.)

The vectors in C are: the zero vector, the vectors in the basis B , and the sum of any two or more vectors from the basis B .

$$0000 \quad 0101 \quad 1010 \quad 1100 \quad 1111 \quad 1001 \quad 0110 \quad 0011$$

Solution to Exercise 1.16 A basis for K^4 must be a set of linearly independent vectors that can generate every binary vector of length 4. Thus a basis for K^4 is $\{1000, 0100, 0010, 0001\}$.

Solution to Exercise 1.18 The dimension of K^n is n since a basis for K^n is the set of all vectors of length n having precisely one component equal to 1.

The dimension of C is Exercise 1.15 is 3.

Solution to Exercise 1.19

$$\begin{aligned} 1111 &= 1(0101) + 1(1010) + 0(1100) & 0011 &= 1(0101) + 1(1010) + 1(1100) \\ 0101 &= 1(0101) + 0(1010) + 0(1100) & 0000 &= 0(0101) + 0(1010) + 0(1100) \end{aligned}$$

Solution to Exercise 1.23 A vector $\alpha_1\alpha_2\alpha_3\alpha_4$ of S^\perp must be orthogonal to each vector in S . Hence

$$\begin{aligned} (\alpha_1\alpha_2\alpha_3\alpha_4) \cdot (0100) &= 0 \quad (1) \\ \text{and } (\alpha_1\alpha_2\alpha_3\alpha_4) \cdot (0101) &= 0 \quad (2) \end{aligned}$$

Equation (1) says that $\alpha_2 = 0$ and equation (2) says that $\alpha_2 + \alpha_4 = 0$ so we must have $\alpha_2 = \alpha_4 = 0$ but there are no constraints on α_1 or α_3 . Thus the set

$$S^\perp = \{0000, 1000, 0010, 1010\}.$$

Solution to Exercise 1.25 Since K^7 has dimension 7 and S^\perp has dimension 3, we find that the dimension of $\langle S \rangle$ is 4.

The number of words in $\langle S \rangle$ is $2^4 = 16$ and the number of words in S^\perp is $2^3 = 8$.

Solution to Exercise 1.28

$$AB = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Solution to Exercise 1.33 In the row operations below, we use the short-hand $R1 + R2 \rightarrow R2$ to mean replace row 2 with row 1 plus row 2, and $R2 \leftrightarrow R3$ to mean interchange rows 2 and 3.

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \begin{array}{l} R1 + R2 \rightarrow R2 \\ R1 + R3 \rightarrow R3 \end{array} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} R2 \leftrightarrow R3 \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} R1 + R3 \rightarrow R1 \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

The RREF of M is $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.