NATIONAL UNIVERSITY OF SINGAPORE
Department of Mathematics

AY2021, Semester 1 MA1508E Linear Algebra for Engineering Tutorial 6

Solutions

1. For each of the following sets of vectors S,

   (i) Determine if S is linearly independent.

   (ii) If S is linearly dependent, express one of the vectors in S as a linear combination of the others.

   (a) $S = \left\{ \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \\ 6 \end{pmatrix} \right\}$.

   S is linearly dependent since it contains 4 vectors from $\mathbb{R}^3$.

$$\begin{pmatrix} 2 & 0 & 2 & 3 \\ -1 & 3 & 4 & 6 \\ 0 & 2 & 3 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & \frac{9}{2} \\ 0 & 1 & 0 & \frac{15}{2} \\ 0 & 0 & 1 & -3 \end{pmatrix}.$$

   So

$$\begin{pmatrix} 3 \\ 6 \\ 6 \end{pmatrix} = \frac{9}{2} \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix} + \frac{15}{2} \begin{pmatrix} 0 \\ 3 \\ 2 \end{pmatrix} - 3 \begin{pmatrix} 2 \\ 4 \\ 3 \end{pmatrix}.$$

   (b) $S = \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 2 \end{pmatrix} \right\}$.

   S is linearly independent since S has only two vectors which are not multiples of each other.

   (c) $S = \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}$.

   Any set containing the zero vector is linearly dependent.

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = 0 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 0 \begin{pmatrix} 3 \\ 4 \\ 2 \end{pmatrix}.$$

   (d) $S = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix} \right\}$.

   Solving $a \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + c \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$,

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 1 & -1 & 0 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right).$$

So $a\begin{pmatrix}1\\0\\0\end{pmatrix}+b\begin{pmatrix}0\\1\\1\end{pmatrix}+c\begin{pmatrix}1\\2\\-1\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}$ has only the trivial solution and S is a linearly independent set.

2. For each of the following subspaces V, write down a basis for V.

(a) $V=\left\{\begin{pmatrix}a+b\\a+c\\c+d\\b+d\end{pmatrix}\middle|\, a,b,c,d\in\mathbb{R}\right\}$.

$$\begin{aligned}
V &= \left\{\begin{pmatrix}a+b\\a+c\\c+d\\b+d\end{pmatrix}\middle|\, a,b,c,d\in\mathbb{R}\right\}\\
&= \left\{a\begin{pmatrix}1\\1\\0\\0\end{pmatrix}+b\begin{pmatrix}1\\0\\0\\1\end{pmatrix}+c\begin{pmatrix}0\\1\\1\\0\end{pmatrix}+d\begin{pmatrix}0\\0\\1\\1\end{pmatrix}\middle|\, a,b,c,d\in\mathbb{R}\right\}\\
&= \operatorname{span}\left\{\begin{pmatrix}1\\1\\0\\0\end{pmatrix},\begin{pmatrix}1\\0\\0\\1\end{pmatrix},\begin{pmatrix}0\\1\\1\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\\1\end{pmatrix}\right\}
\end{aligned}$$

$$\left(\begin{array}{cccc|c}1&1&0&0&0\\1&0&1&0&0\\0&0&1&1&0\\0&1&0&1&0\end{array}\right)\longrightarrow\left(\begin{array}{cccc|c}1&0&0&-1&0\\0&1&0&1&0\\0&0&1&1&0\\0&0&0&0&0\end{array}\right).$$

This means that the fourth vector is redundant. It is easy to see that the first three vectors are linearly independent. So

$$\left\{\begin{pmatrix}1\\1\\0\\0\end{pmatrix},\begin{pmatrix}1\\0\\0\\1\end{pmatrix},\begin{pmatrix}0\\1\\1\\0\end{pmatrix}\right\}$$

is a basis for V.

(b) $V=\operatorname{span}\left\{\begin{pmatrix}1\\0\\-1\end{pmatrix},\begin{pmatrix}-1\\2\\3\end{pmatrix},\begin{pmatrix}0\\3\\0\end{pmatrix},\begin{pmatrix}1\\-1\\1\end{pmatrix}\right\}$.

Since the set contains 4 vectors in $\mathbb{R}^3$, it cannot be linearly independent. One can check that $\left\{\begin{pmatrix}1\\0\\-1\end{pmatrix},\begin{pmatrix}-1\\2\\3\end{pmatrix},\begin{pmatrix}0\\3\\0\end{pmatrix}\right\}$ is linearly independent. Hence it is a basis for $V=\mathbb{R}^3$.

(c) V is the solution space of the following homogeneous linear system

$$\left\{\begin{array}{ccccccccccc}a_1 & & & + & a_3 & + & a_4 & - & a_5 & = & 0\\ & & a_2 & + & a_3 & + & 2a_4 & + & a_5 & = & 0\\ a_1 & + & a_2 & + & 2a_3 & + & a_4 & - & 2a_5 & = & 0\end{array}\right.$$

Solving the homogeneous system:

$$\left(\begin{array}{ccccc|c} 1 & 0 & 1 & 1 & -1 & 0 \\ 0 & 1 & 1 & 2 & 1 & 0 \\ 1 & 1 & 2 & 1 & -2 & 0 \end{array}\right) \longrightarrow \left(\begin{array}{ccccc|c} 1 & 0 & 1 & 0 & -2 & 0 \\ 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{array}\right)$$

So the solution set is

$$\left\{ s\begin{pmatrix}-1\\-1\\1\\0\\0\end{pmatrix} + t\begin{pmatrix}2\\1\\0\\-1\\1\end{pmatrix} \;\middle|\; s,t\in\mathbb{R} \right\}.$$

It is easy to see that $\left\{\begin{pmatrix}-1\\-1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}2\\1\\0\\-1\\1\end{pmatrix}\right\}$ is linearly independent, and is thus a basis for V.

3. Let $\mathbf{v}_1 = \begin{pmatrix}3\\1\\1\\1\end{pmatrix}$, $\mathbf{v}_2 = \begin{pmatrix}1\\2\\1\\1\end{pmatrix}$, $\mathbf{v}_3 = \begin{pmatrix}1\\1\\0\\1\end{pmatrix}$, $\mathbf{v}_4 = \begin{pmatrix}4\\3\\2\\2\end{pmatrix}$ and $\mathbf{u} = \begin{pmatrix}4\\4\\3\\2\end{pmatrix}$.

   (a) Express $\mathbf{u}$ as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4$ in two distinct ways.

   Solving $a\begin{pmatrix}3\\1\\1\\1\end{pmatrix} + b\begin{pmatrix}1\\2\\1\\1\end{pmatrix} + c\begin{pmatrix}1\\1\\0\\1\end{pmatrix} + d\begin{pmatrix}4\\3\\2\\2\end{pmatrix} = \begin{pmatrix}4\\4\\3\\2\end{pmatrix}$,

$$\left(\begin{array}{cccc|c} 3 & 1 & 1 & 4 & 4 \\ 1 & 2 & 1 & 3 & 4 \\ 1 & 1 & 0 & 2 & 3 \\ 1 & 1 & 1 & 2 & 2 \end{array}\right) \longrightarrow \left(\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

   This means that $\begin{pmatrix}a\\b\\c\\d\end{pmatrix} = \begin{pmatrix}1\\2\\-1\\0\end{pmatrix} + s\begin{pmatrix}-1\\-1\\0\\1\end{pmatrix}$ for any $s\in\mathbb{R}$. In other words,

$$\begin{pmatrix}4\\4\\3\\2\end{pmatrix} = (1-s)\begin{pmatrix}3\\1\\1\\1\end{pmatrix} + (2-s)\begin{pmatrix}1\\2\\1\\1\end{pmatrix} - \begin{pmatrix}1\\1\\0\\1\end{pmatrix} + s\begin{pmatrix}4\\3\\2\\2\end{pmatrix}, \text{ for any } s\in\mathbb{R}.$$

   So we may choose $s=0$ and $s=1$.

   (b) Is it possible to express $\mathbf{u}$ as a linear combination of $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ in two distinct ways?

It is not possible. Solving $a\begin{pmatrix}3\\1\\1\\1\end{pmatrix}+b\begin{pmatrix}1\\2\\1\\1\end{pmatrix}+c\begin{pmatrix}1\\1\\0\\1\end{pmatrix}=\begin{pmatrix}4\\4\\3\\2\end{pmatrix}$

$$\left(\begin{array}{ccc|c}3&1&1&4\\1&2&1&4\\1&1&0&3\\1&1&1&2\end{array}\right)\longrightarrow\left(\begin{array}{ccc|c}1&0&0&1\\0&1&0&2\\0&0&1&-1\\0&0&0&0\end{array}\right)$$

The solution is unique. It corresponds to the choice of $s=0$ in (a).

This question demonstrates that a vector $\mathbf{u}\in\text{span}\{\mathbf{v}_1,\mathbf{v}_2,...,\mathbf{v}_k\}$ has a unique linear combination expression if and only if the set $\{\mathbf{v}_1,\mathbf{v}_2,...,\mathbf{v}_k\}$ is linearly independent.

4. (a) For what values of a will $\mathbf{u}_1=\begin{pmatrix}a\\1\\-1\end{pmatrix}$, $\mathbf{u}_2=\begin{pmatrix}-1\\a\\1\end{pmatrix}$, $\mathbf{u}_3=\begin{pmatrix}1\\-1\\a\end{pmatrix}$ form a basis for $\mathbb{R}^3$?

(b)

$$\left(\begin{array}{ccc|c}a&-1&1&0\\1&a&-1&0\\-1&1&a&0\end{array}\right)\xrightarrow{R_1\leftrightarrow R_2}\left(\begin{array}{ccc|c}1&a&-1&0\\a&-1&1&0\\-1&1&a&0\end{array}\right)\xrightarrow[R_3+R_1]{R_2-aR_1}$$

$$\left(\begin{array}{ccc|c}1&a&-1&0\\0&-1-a^2&1+a&0\\0&1+a&a-1&0\end{array}\right)\xrightarrow{-R_2}\left(\begin{array}{ccc|c}1&a&-1&0\\0&1+a^2&-1-a&0\\0&1+a&a-1&0\end{array}\right)\xrightarrow{R_3-\frac{1+a}{1+a^2}R_2}$$

$$\left(\begin{array}{ccc|c}1&a&-1&0\\0&1+a^2&-1-a&0\\0&0&\frac{a(a^2+3)}{1+a^2}&0\end{array}\right)$$

So $\mathbf{u}_1,\mathbf{u}_2,\mathbf{u}_3$ will form a basis for $\mathbb{R}^3$ if and only if $a\neq 0$.

(c) For what values of a will the determinant of $\begin{pmatrix}a&-1&1\\1&a&-1\\-1&1&a\end{pmatrix}$ be nonzero?

The determinant is $a(a^2+3)$, which is 0 if and only if $a=0$.

(d) Base on your results in (a) and (b), make a conjecture.

A set of n vectors $\{\mathbf{u}_1,...,\mathbf{u}_n\}$ is a basis for $\mathbb{R}^n$ if any only if the determinant of the matrix $A=(\mathbf{u}_1\cdots\mathbf{u}_n)$ is nonzero.

5. For each of the following cases, find the coordinate vector of $\mathbf{v}$ relative to the basis $S=\{\mathbf{u}_1,\mathbf{u}_2,\mathbf{u}_3\}$.

(a) $\mathbf{v}=\begin{pmatrix}1\\-2\\6\end{pmatrix}$, $\mathbf{u}_1=\begin{pmatrix}1\\1\\1\end{pmatrix}$, $\mathbf{u}_2=\begin{pmatrix}0\\2\\2\end{pmatrix}$, $\mathbf{u}_3=\begin{pmatrix}0\\0\\3\end{pmatrix}$.

$$\left(\begin{array}{ccc|c}1&0&0&1\\1&2&0&-2\\1&2&3&6\end{array}\right)\longrightarrow\left(\begin{array}{ccc|c}1&0&0&1\\0&1&0&-\frac{3}{2}\\0&0&1&\frac{8}{3}\end{array}\right)$$

So $(\mathbf{v})_S = \frac{1}{6}\begin{pmatrix} 6 \\ -9 \\ 16 \end{pmatrix}$.

(b) $\mathbf{v} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, $\mathbf{u}_1 = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$, $\mathbf{u}_2 = \begin{pmatrix} -1 \\ 1 \\ -2 \end{pmatrix}$, $\mathbf{u}_3 = \begin{pmatrix} 1 \\ 3 \\ 3 \end{pmatrix}$.

$$\left(\begin{array}{ccc|c} 1 & -1 & 1 & 0 \\ 1 & 1 & 3 & 0 \\ 2 & -2 & 3 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{array}\right)$$

So $(\mathbf{v})_S = \begin{pmatrix} -2 \\ -1 \\ 1 \end{pmatrix}$.

Supplementary Problems

6. In computers, information is stored and processed in the form of strings of binary digits, 0 and 1. For this exercise, we will work in the “world” of binary digits

$$\mathbb{B} = \{0, 1\}\,.$$

Addition in $\mathbb{B}$ works just as it does in $\mathbb{R}$, save for one special rule:

$$1 + 1 = 0.$$

We can similarly perform scalar multiplication in $\mathbb{B}$—however, note that in our “binary world”, we only have two possible scalars: 0 and 1 (as opposed to any real number).

Remark. The special rule for binary addition is equivalent to performing our standard operations **modulo 2**. That is, in our “binary world,” we evaluate a sum according to its remainder when divided by 2: if the remainder is 0 (i.e., when a number is even), then it corresponds to the binary digit 0, and if the remainder is 1 (i.e., when a number is odd), then it corresponds to the binary digit 1.

(a) Using the rules on the basic operations in $\mathbb{B}$, complete the addition and multiplication tables below.

$+$	0	1
0		
1		

$\times$	0	1
0		
1		

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

(b) Recall that we created the Euclidean space $\mathbb{R}^n$ by taking the set of all n-vectors with real components (i.e., with components in $\mathbb{R}$). We can create the set $\mathbb{B}^n$ in a similar fashion, by taking the set of all n-vectors whose components are binary digits, 0 or 1. Observe, then, that the basic properties of addition and scalar multiplication in $\mathbb{R}^n$ directly apply to $\mathbb{B}^n$, as long as we remember that $1 + 1 = 0$ and the only scalars we are allowed to multiply by are 0 and 1.

i. Consider the Euclidean 3-space $\mathbb{R}^3$, which has infinitely many vectors. How many vectors does $\mathbb{B}^3$ have?
We can list out the vectors in $\mathbb{B}^3$, noting that the elements of each vector can only either be a 0 or a 1.

$$\begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}$$

We find that $\mathbb{B}^3$ only contains eight vectors.

ii. A *byte*—the fundamental unit of data used by many computers—is a string of 8 binary digits. Observe that we can treat each byte as a vector in $\mathbb{B}^8$. How many distinct bytes exist; that is, how many vectors are there in $\mathbb{B}^8$? How does this compare to Euclidean 8-space $\mathbb{R}^8$?
For an arbitrary string of 8 binary digits, we have two choices for each of the vector's entries: either 0 or 1. There are thus a total of $2^8 = 256$ different ways we can create a byte, and the set $\mathbb{B}^8$ contains 256 vectors, as opposed to the infinitely many vectors in $\mathbb{R}^8$.

iii. The Euclidean n-space $\mathbb{R}^n$ has infinitely many vectors. More generally, how many vectors are there in $\mathbb{B}^n$?
The set $\mathbb{B}^n$ has 2^n vectors.

For the purposes of this exercise, you may assume that $\mathbb{B}^n$ has all the properties of a subspace—that is, $\mathbb{B}^n$ is closed under addition and scalar multiplication. (Try to prove this yourself!)

(c) To get a sense of how vectors work in $\mathbb{B}^n$, we take a simple example. Let's begin by working in $\mathbb{B}^3$—the set of all 3-vectors whose components are binary digits.

i. Let $S = \left\{ \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \right\}$ be the set of standard unit vectors in $\mathbb{R}^3$. Show that S forms a basis for $\mathbb{B}^3$.
To show that S is a basis for $\mathbb{B}^3$, we need to show that $\operatorname{span}(S) = \mathbb{B}^3$ and that S is linearly independent. To show that S spans $\mathbb{B}^3$, consider the vector equation

$$c_1 \begin{pmatrix}1\\0\\0\end{pmatrix} + c_2 \begin{pmatrix}0\\1\\0\end{pmatrix} + c_3 \begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}x\\y\\z\end{pmatrix} \quad \text{where } x, y, z \in \mathbb{B}.$$

Simplifying the left-hand side of the equation, we have

$$(c_1, c_2, c_3) = (x, y, z).$$

Note that we are taking the scalars c_1, c_2, c_3 from $\mathbb{B} = \{0, 1\}$ as well; thus, S spans $\mathbb{B}$. In the case when $x = y = z = 0$, we require that $c_1 = c_2 = c_3 = 0$. Thus, S must be linearly independent as well.

ii. Show that the set $T = \left\{ \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\end{pmatrix} \right\}$ forms a basis for $\mathbb{R}^3$. Does T form a basis for $\mathbb{B}^3$?

Observe that T is a set of 3 vectors in $\mathbb{R}^3$. Thus, to show that T is basis for $\mathbb{R}^3$, it suffices to show that either $\operatorname{span}(T) = \mathbb{R}^3$ or T is linearly independent. We show that T is linearly independent: consider the vector equation

$$c_1 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + c_2 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + c_3 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \mathbf{0}.$$

We can row-reduce the corresponding augmented matrix uxing MATLAB:

```
>> rref([1 1 0 0; 0 1 1 0; 1 0 1 0])
```

In particular, we find that

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right).$$

Thus, the vector equation has only the trivial solution, and T is a linearly independent set of 3 vectors in $\mathbb{R}^3$.

Now, we consider T as a subset of $\mathbb{B}^3$: observe that

$$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

In particular, the third vector in T is a linear combination of the first two. Thus, T is linearly dependent in $\mathbb{B}^3$ and is hence not a basis for $\mathbb{B}^3$.

(d) The *Hamming matrix* with n rows, $\boldsymbol{H}_n$, is formed by collecting all the nonzero vectors in $\mathbb{B}^n$ as columns of a matrix.

i. How many columns does $\boldsymbol{H}_n$ have?
$\mathbb{B}^n$ has 2^n vectors, including the zero vector. Thus, $\boldsymbol{H}_n$ has $2^n - 1$ columns.

ii. Suppose we write $\boldsymbol{H}_3$ as

$$\boldsymbol{H}_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Show that the solution set S of $\boldsymbol{H}_3\boldsymbol{x} = \mathbf{0}$ is a subspace of $\mathbb{B}^7$ by expressing it as a linear span $S = \operatorname{span}\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k\}$, where $\boldsymbol{v}_i \in \mathbb{B}^7$ for $i = 1, \ldots, k$. Hence, find a basis for S.
Observe that $\boldsymbol{H}_3$ is already in reduced row-echelon form. We assign arbitrary parameters to $x_4 = q, x_5 = r, x_6 = s, x_7 = t$ for $q, r, s, t \in \mathbb{B}$. Then,

the solution set $\boldsymbol{H}_3\boldsymbol{x} = \mathbf{0}$ is

$$\left\{ q\begin{pmatrix}-1\\-1\\-1\\1\\0\\0\\0\end{pmatrix} + r\begin{pmatrix}0\\-1\\-1\\0\\1\\0\\0\end{pmatrix} + s\begin{pmatrix}-1\\0\\-1\\0\\0\\1\\0\end{pmatrix} + t\begin{pmatrix}-1\\-1\\0\\0\\0\\0\\1\end{pmatrix} \,\middle|\, q, r, s, t \in \mathbb{R} \right\}.$$

By the addition rule $1 + 1 = 0$, we have $1 = -1$. Hence,

$$S = \text{span}\{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4\} = \text{span}\left\{\begin{pmatrix}1\\1\\1\\1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\\0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\\0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\\0\\0\\0\\1\end{pmatrix}\right\}.$$

We can observe that the set $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4\}$ is linearly independent: for each $\boldsymbol{v}_i$, there is a 1 in the $(i+3)$-th entry, whereas the other vectors contain a 0 in that same entry. Thus, $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4\}$ forms a basis for S.

(e) Create the matrix $\boldsymbol{M}$ by taking the vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ as its columns.

i. What is the size of $\boldsymbol{M}$?
$\boldsymbol{M}$ is the 7×4 matrix given by

$$\boldsymbol{M} = \begin{pmatrix}1&0&1&1\\1&1&0&1\\1&1&1&0\\1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

ii. For an arbitrary vector $\boldsymbol{x} \in \mathbb{B}^4$, what can you say about $\boldsymbol{H}_3(\boldsymbol{M}\boldsymbol{x})$?
Hint: MATLAB can take a number x and calculate its value modulo 2. To do this, we may simply key in

```
>> mod(x,2)
```

What might happen if we replace the number x with an entire matrix?
Since matrix multiplication is associative, $\boldsymbol{H}_3(\boldsymbol{M}\boldsymbol{x}) = (\boldsymbol{H}_3\boldsymbol{M})\boldsymbol{x}$.
We may use MATLAB to calculate the matrix product $\boldsymbol{H}_3\boldsymbol{M}$, modulo 2:

```
>> H =[1 0 0 1 0 1 1; 0 1 0 1 1 0 1; 0 0 1 1 1 1 0];

>> v1= [1 1 1 1 0 0 0]';
```

```
>> v2= [0 1 1 0 1 0 0]';

>> v3= [1 0 1 0 0 1 0]';

>> v4= [1 1 0 0 0 0 1]';

>> M=[v1 v2 v3 v4];

>> mod(H*M,2)
```

We find that the matrix product $\boldsymbol{H}_3\boldsymbol{M}$ is simply the 3×4 zero matrix, which implies that for all $\boldsymbol{x} \in \mathbb{B}^4$,

$$\boldsymbol{H}_3(\boldsymbol{M}\boldsymbol{x}) = (\boldsymbol{H}_3\boldsymbol{M})\boldsymbol{x} = \mathbf{0}\boldsymbol{x} = \mathbf{0}.$$

In next week's tutorial, we will see how working with binary vectors can help us detect—and potentially, correct—errors in information transmitted between computers.

7. Let $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ be a basis for a vector space V. Let $\mathbf{u}$ be a vector in V and let c be a scalar. Prove the following:

   (a) $(\mathbf{u}+\mathbf{v})_S = (\mathbf{u})_S + (\mathbf{v})_S$.
   We first write $\mathbf{u}$ and $\mathbf{v}$ in terms of the basis vectors, say

   $$\mathbf{u} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \ldots + c_n\mathbf{v}_n \text{ and } \mathbf{v} = d_1\mathbf{v}_1 + d_2\mathbf{v}_2 + \ldots + d_n\mathbf{v}_n.$$

   Then
   $$\mathbf{u}+\mathbf{v} = (c_1+d_1)\mathbf{v}_1 + (c_2+d_2)\mathbf{v}_2 + \ldots + (c_n+d_n)\mathbf{v}_n$$
   which implies

   $$(\mathbf{u}+\mathbf{v})_S = \begin{pmatrix} c_1+d_1 \\ c_2+d_2 \\ \vdots \\ c_n+d_n \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} + \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} = (\mathbf{u})_S + (\mathbf{v})_S.$$

   (b) $(c\mathbf{u})_S = c(\mathbf{u})_S$.
   Similarly,

   $$c\mathbf{u} = (cc_1)\mathbf{v}_1 + (cc_2)\mathbf{v}_2 + \ldots + (cc_n)\mathbf{v}_n \Rightarrow (c\mathbf{u})_S = \begin{pmatrix} cc_1 \\ cc_2 \\ \vdots \\ cc_n \end{pmatrix} = c\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = c(\mathbf{u})_S.$$

Suppose $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ are vectors in V. Note that for each $i = 1, 2, \ldots, k$, $(\mathbf{u}_i)_S$ is a vector in $\mathbb{R}^n$. By induction and using (a) and (b), it follows that if $c_1, c_2, \ldots, c_k \in \mathbb{R}$, then

$$(c_1\mathbf{u}_1 + c_2\mathbf{u}_2 + \ldots + c_k\mathbf{u}_k)_S = c_1 (\mathbf{u}_1)_S + c_2 (\mathbf{u}_2)_S + \ldots + c_k (\mathbf{u}_k)_S .$$

Prove the following:

(c) $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$ is linearly independent in V if and only if $\{(\mathbf{u}_1)_S, (\mathbf{u}_2)_S, \ldots, (\mathbf{u}_k)_S\}$ is linearly independent in $\mathbb{R}^n$.

Assume that $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k\}$ is linearly independent in V. Consider the equation $c_1 (\mathbf{u}_1)_S + \ldots + c_k (\mathbf{u}_k)_S = \mathbf{0}$ which is a vector equation in $\mathbb{R}^n$. By part (c), the equation above can be rewritten as $(c_1\mathbf{u}_1 + c_2\mathbf{u}_2 + \ldots + c_k\mathbf{u}_k)_S = \mathbf{0}$. So the coordinates of $c_1\mathbf{u}_1 + \ldots + c_k\mathbf{u}_k$ with respect to the basis S are all zero, that is, $c_1\mathbf{u}_1 + \ldots + c_k\mathbf{u}_k = 0\mathbf{v}_1 + 0\mathbf{v}_2 + \ldots + 0\mathbf{v}_n = \mathbf{0}$. As $\{\mathbf{u}_1, \ldots \mathbf{u}_k\}$ is linearly independent, the equation above implies $c_1 = c_2 = \ldots = c_k = 0$, so $\{(\mathbf{u}_1)_S, \ldots, (\mathbf{u}_k)_S\}$ is linearly independent.

Conversely, assume $\{(\mathbf{u}_1)_S, \ldots, (\mathbf{u}_k)_S\}$ is a linearly independent set in $\mathbb{R}^n$. Consider the equation

$$c_1\mathbf{u}_1 + c_2\mathbf{u}_2 + \ldots + c_k\mathbf{u}_k = \mathbf{0}$$

which implies

$$(c_1\mathbf{u}_1 + c_2\mathbf{u}_2 + \ldots + c_k\mathbf{u}_k)_S = (\mathbf{0})_S = \mathbf{0},$$

Using the result in part (c), we have

$$c_1 (\mathbf{u}_1)_S + \ldots + c_k (\mathbf{u}_k)_S = \mathbf{0}$$

and this implies that $c_1 = c_2 = \ldots = c_k = 0$ since $\{(\mathbf{u}_1)_S, \ldots, (\mathbf{u}_k)_S\}$ is linearly independent. Thus we have shown that $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ is a linearly independent set in V.