[3] The Vector Space
Linear Combinations

An expression

$$\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n$$

is a \textit{linear combination} of the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$.

The scalars $\alpha_1, \ldots, \alpha_n$ are the \textit{coefficients} of the linear combination.

\textbf{Example:} One linear combination of $[2, 3.5]$ and $[4, 10]$ is

$$-5 [2, 3.5] + 2 [4, 10]$$

which is equal to $[-5 \cdot 2, -5 \cdot 3.5] + [2 \cdot 4, 2 \cdot 10]$

Another linear combination of the same vectors is

$$0 [2, 3.5] + 0 [4, 10]$$

which is equal to the zero vector $[0, 0]$.

\textbf{Definition:} A linear combination is \textit{trivial} if the coefficients are all zero.
Linear Combinations: JunkCo

The JunkCo factory makes five products:

![Garden Gnome](image1.png) ![Hula Hoop](image2.png) ![Slinky](image3.png) ![Silly Putty](image4.png) ![Salad Shooter](image5.png)

using various resources.

<table>
<thead>
<tr>
<th></th>
<th>metal</th>
<th>concrete</th>
<th>plastic</th>
<th>water</th>
<th>electricity</th>
</tr>
</thead>
<tbody>
<tr>
<td>garden gnome</td>
<td>0</td>
<td>1.3</td>
<td>0.2</td>
<td>0.8</td>
<td>0.4</td>
</tr>
<tr>
<td>hula hoop</td>
<td>0</td>
<td>0</td>
<td>1.5</td>
<td>0.4</td>
<td>0.3</td>
</tr>
<tr>
<td>slinky</td>
<td>0.25</td>
<td>0</td>
<td>0</td>
<td>0.2</td>
<td>0.7</td>
</tr>
<tr>
<td>silly putty</td>
<td>0</td>
<td>0</td>
<td>0.3</td>
<td>0.7</td>
<td>0.5</td>
</tr>
<tr>
<td>salad shooter</td>
<td>0.15</td>
<td>0</td>
<td>0.5</td>
<td>0.4</td>
<td>0.8</td>
</tr>
</tbody>
</table>

For each product, there is a vector specifying how much of each resource is used per unit of product.

For making one gnome:
\[ \mathbf{v}_1 = \{\text{metal}:0, \text{concrete}:1.3, \text{plastic}:0.2, \text{water}:0.8, \text{electricity}:0.4\} \]
For making one gnome:
\[ \mathbf{v}_1 = \{ \text{metal:0, concrete:1.3, plastic:0.2, water:0.8, electricity:0.4} \} \]
For making one hula hoop:
\[ \mathbf{v}_2 = \{ \text{metal:0, concrete:0, plastic:1.5, water:0.4, electricity:0.3} \} \]
For making one slinky:
\[ \mathbf{v}_3 = \{ \text{metal:0.25, concrete:0, plastic:0, water:0.2, electricity:0.7} \} \]
For making one silly putty:
\[ \mathbf{v}_4 = \{ \text{metal:0, concrete:0, plastic:0.3, water:0.7, electricity:0.5} \} \]
For making one salad shooter:
\[ \mathbf{v}_5 = \{ \text{metal:1.5, concrete:0, plastic:0.5, water:0.4, electricity:0.8} \} \]

Suppose the factory chooses to make \( \alpha_1 \) gnomes, \( \alpha_2 \) hula hoops, \( \alpha_3 \) slinkies, \( \alpha_4 \) silly putties, and \( \alpha_5 \) salad shooters.

Total resource utilization is
\[ \mathbf{b} = \alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \alpha_3 \mathbf{v}_3 + \alpha_4 \mathbf{v}_4 + \alpha_5 \mathbf{v}_5 \]
Linear Combinations: JunkCo: Industrial espionage

Total resource utilization is $\mathbf{b} = \alpha_1 \mathbf{v}_1 + \alpha_2 \mathbf{v}_2 + \alpha_3 \mathbf{v}_3 + \alpha_4 \mathbf{v}_4 + \alpha_5 \mathbf{v}_5$

Suppose I am spying on JunkCo.

I find out how much metal, concrete, plastic, water, and electricity are consumed by the factory.

That is, I know the vector $\mathbf{b}$. Can I use this knowledge to figure out how many gnomes they are making?

**Computational Problem:** *Expressing a given vector as a linear combination of other given vectors*

- **input:** a vector $\mathbf{b}$ and a list $[\mathbf{v}_1, \ldots, \mathbf{v}_n]$ of vectors
- **output:** a list $[\alpha_1, \ldots, \alpha_n]$ of coefficients such that

  $\mathbf{b} = \alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n$

  or a report that none exists.

**Question:** Is the solution unique?
**Lights Out**

Button vectors for $2 \times 2$ *Lights Out*:

\[
\begin{array}{c}
\bullet \bullet \\
\bullet \\
\end{array}
\quad
\begin{array}{c}
\bullet \\
\bullet \bullet \\
\bullet \\
\end{array}
\quad
\begin{array}{c}
\bullet \\
\bullet \\
\bullet \bullet \\
\bullet \\
\end{array}
\quad
\begin{array}{c}
\bullet \bullet \\
\bullet \\
\bullet \\
\bullet \\
\end{array}
\]

For a given initial state vector $s =
\begin{array}{c}
\bullet \\
\bullet \\
\end{array}$, which subset of button vectors sum to $s$?

Reformulate in terms of linear combinations.

Write

\[
\begin{array}{c}
\bullet \\
\bullet \\
\end{array}
= \alpha_1
\begin{array}{c}
\bullet \\
\bullet \bullet \\
\bullet \\
\end{array}
+ \alpha_2
\begin{array}{c}
\bullet \\
\bullet \\
\bullet \bullet \\
\bullet \\
\end{array}
+ \alpha_3
\begin{array}{c}
\bullet \bullet \\
\bullet \\
\bullet \\
\bullet \\
\end{array}
+ \alpha_4
\begin{array}{c}
\bullet \bullet \\
\bullet \\
\bullet \\
\bullet \\
\end{array}
\]

What values for $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ make this equation true?

**Solution:** $\alpha_1 = 0, \alpha_2 = 1, \alpha_3 = 0, \alpha_4 = 0$

Solve an instance of *Lights Out* $\Rightarrow$ Which set of button vectors sum to $s$?

$\Rightarrow$ Find subset of $GF(2)$ vectors $v_1, \ldots, v_n$ whose sum equals $s$ $\Rightarrow$ Express $s$ as a linear combination of $v_1, \ldots, v_n$
We can solve the puzzle if we have an algorithm for

**Computational Problem:** Expressing a given vector as a linear combination of other given vectors
**Definition:** The set of all linear combinations of some vectors \( \mathbf{v}_1, \ldots, \mathbf{v}_n \) is called the *span* of these vectors. Written \( \text{Span} \{ \mathbf{v}_1, \ldots, \mathbf{v}_n \} \).
Span: Attacking the authentication scheme

If Eve knows the password satisfies

\[
\begin{align*}
    a_1 \cdot x &= \beta_1 \\
    \vdots \\
    a_m \cdot x &= \beta_m
\end{align*}
\]

Then she can calculate right response to any challenge in Span \( \{a_1, \ldots, a_m\} \):

**Proof:** Suppose \( a = \alpha_1 a_1 + \cdots + \alpha_m a_m \). Then

\[
\begin{align*}
    a \cdot x &= (\alpha_1 a_1 + \cdots + \alpha_m a_m) \cdot x \\
    &= \alpha_1 a_1 \cdot x + \cdots + \alpha_m a_m \cdot x \quad \text{by distributivity} \\
    &= \alpha_1 (a_1 \cdot x) + \cdots + \alpha_m (a_m \cdot x) \quad \text{by homogeneity} \\
    &= \alpha_1 \beta_1 + \cdots + \alpha_m \beta_m
\end{align*}
\]

**Question:** Any others? Answer will come later.
Quiz: How many vectors are in \( \text{Span} \ \{[1, 1], [0, 1]\} \) over the field \( GF(2) \)?

Answer: The linear combinations are

\[
\begin{align*}
0 [1, 1] + 0 [0, 1] &= [0, 0] \\
0 [1, 1] + 1 [0, 1] &= [0, 1] \\
1 [1, 1] + 0 [0, 1] &= [1, 1] \\
1 [1, 1] + 1 [0, 1] &= [1, 0]
\end{align*}
\]

Thus there are four vectors in the span.
Span: $GF(2)$ vectors

**Question:** How many vectors in Span $\{[1, 1]\}$ over $GF(2)$?

**Answer:** The linear combinations are

\[
\begin{align*}
0 [1, 1] &= [0, 0] \\
1 [1, 1] &= [1, 1]
\end{align*}
\]

Thus there are two vectors in the span.

**Question:** How many vectors in Span $\{\}$?

**Answer:** Only one: the zero vector

**Question:** How many vectors in Span $\{[2, 3]\}$ over $\mathbb{R}$?

**Answer:** An infinite number: $\{\alpha [2, 3] : \alpha \in \mathbb{R}\}$
Forms the line through the origin and $(2, 3)$. 
Generators

**Definition:** Let $\mathcal{V}$ be a set of vectors. If $\mathbf{v}_1, \ldots, \mathbf{v}_n$ are vectors such that $\mathcal{V} = \text{Span} \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ then

- we say $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a *generating set* for $\mathcal{V}$;
- we refer to the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ as *generators* for $\mathcal{V}$.

**Example:** $\{[3, 0, 0], [0, 2, 0], [0, 0, 1]\}$ is a generating set for $\mathbb{R}^3$.

**Proof:** Must show two things:

1. Every linear combination is a vector in $\mathbb{R}^3$.
2. Every vector in $\mathbb{R}^3$ is a linear combination.

First statement is easy: every linear combination of 3-vectors over $\mathbb{R}$ is a 3-vector over $\mathbb{R}$, and $\mathbb{R}^3$ contains all 3-vectors over $\mathbb{R}$.

Proof of second statement: Let $[x, y, z]$ be any vector in $\mathbb{R}^3$. I must show it is a linear combination of my three vectors....

$$[x, y, z] = (x/3) [3, 0, 0] + (y/2) [0, 2, 0] + z [0, 0, 1]$$
Generators

**Claim:** Another generating set for $\mathbb{R}^3$ is $\{[1, 0, 0], [1, 1, 0], [1, 1, 1]\}$

Another way to prove that every vector in $\mathbb{R}^3$ is in the span:

- We already know $\mathbb{R}^3 = \text{Span} \{[3, 0, 0], [0, 2, 0], [0, 0, 1]\}$,
- so just show $[3, 0, 0], [0, 2, 0], \text{and} [0, 0, 1]$ are in $\text{Span} \{[1, 0, 0], [1, 1, 0], [1, 1, 1]\}$

\[
\begin{align*}
[3, 0, 0] &= 3 [1, 0, 0] \\
[0, 2, 0] &= -2 [1, 0, 0] + 2 [1, 1, 0] \\
[0, 0, 1] &= -1 [1, 0, 0] - 1 [1, 1, 0] + 1 [1, 1, 1]
\end{align*}
\]

Why is that sufficient?

- We already know any vector in $\mathbb{R}^3$ can be written as a linear combination of the old vectors.
- We know each old vector can be written as a linear combination of the new vectors.
- We can convert a linear combination of linear combination of new vectors into a linear combination of new vectors.
Generators

We can convert a linear combination of linear combination of new vectors into a linear combination of new vectors.

▶ Write \([x, y, z]\) as a linear combination of the old vectors:

\[
[x, y, z] = \left(\frac{x}{3}\right)[3, 0, 0] + \left(\frac{y}{2}\right)[0, 2, 0] + z[0, 0, 1]
\]

▶ Replace each old vector with an equivalent linear combination of the new vectors:

\[
[x, y, z] = \left(\frac{x}{3}\right)\left(3 [1, 0, 0]\right) + \left(\frac{y}{2}\right)\left( -2 [1, 0, 0] + 2 [1, 1, 0]\right)
+ z \left( -1 [1, 0, 0] - 1 [1, 1, 0] + 1 [1, 1, 1]\right)
\]

▶ Multiply through, using distributivity and associativity:

\[
[x, y, z] = x [1, 0, 0] - y [1, 0, 0] + y [1, 1, 0] - z [1, 0, 0] - z [1, 1, 0] + z [1, 1, 1]
\]

▶ Collect like terms, using distributivity:

\[
[x, y, z] = (x - y - z) [1, 0, 0] + (y - z) [1, 1, 0] + z [1, 1, 1]
\]
Question: How to write each of the old vectors \([3, 0, 0], [0, 2, 0], \) and \([0, 0, 1]\) as a linear combination of new vectors \([2, 0, 1], [1, 0, 2], [2, 2, 2], \) and \([0, 1, 0]\)?

Answer:

\[
[3, 0, 0] = 2 [2, 0, 1] - 1 [1, 0, 2] + 0 [2, 2, 2]
\]
\[
[0, 2, 0] = -\frac{2}{3} [2, 0, 1] - \frac{2}{3} [1, 0, 2] + 1 [2, 2, 2]
\]
\[
[0, 0, 1] = -\frac{1}{3} [2, 0, 1] + \frac{2}{3} [1, 0, 2] + 0 [2, 2, 2]
\]
Standard generators

Writing \([x, y, z]\) as a linear combination of the vectors \([3, 0, 0]\), \([0, 2, 0]\), and \([0, 0, 1]\) is simple.

\[
[x, y, z] = \left(\frac{x}{3}\right) [3, 0, 0] + \left(\frac{y}{2}\right) [0, 2, 0] + z [0, 0, 1]
\]

Even simpler if instead we use \([1, 0, 0]\), \([0, 1, 0]\), and \([0, 0, 1]\):

\[
[x, y, z] = x [1, 0, 0] + y [0, 1, 0] + z [0, 0, 1]
\]

These are called *standard generators* for \(\mathbb{R}^3\).
Written \(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\)
Standard generators

**Question:** Can $2 \times 2$ *Lights Out* be solved from every starting configuration?

Equivalent to asking whether the $2 \times 2$ button vectors

![Button Vectors](image)

are generators for $GF(2)^D$, where $D = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$.

Yes! For proof, we show that each standard generator can be written as a linear combination of the button vectors:

- $\bullet \bullet = 1 \bullet \bullet + 1 \bullet \bullet + 0 \bullet \bullet$
- $\bullet \bullet = 1 \bullet \bullet + 1 \bullet \bullet + 1 \bullet \bullet$
- $\bullet \bullet = 1 \bullet \bullet + 0 \bullet \bullet + 1 \bullet \bullet$
- $\bullet \bullet = 0 \bullet \bullet + 1 \bullet \bullet + 1 \bullet \bullet$
Geometry of sets of vectors: span of vectors over $\mathbb{R}$

Span of a single nonzero vector $\mathbf{v}$:

$$\text{Span} \{ \mathbf{v} \} = \{ \alpha \mathbf{v} : \alpha \in \mathbb{R} \}$$

This is the line through the origin and $\mathbf{v}$. One-dimensional

Span of the empty set: just the origin. Zero-dimensional

Span $\{ [1, 2], [3, 4] \}$: all points in the plane. Two-dimensional

Span of two 3-vectors? Span $\{ [1, 0, 1.65], [0, 1, 1] \}$ is a plane in three dimensions:

Two-dimensional
Is the span of \( k \) vectors always \( k \)-dimensional?

No.

- Span \( \{[0, 0]\} \) is 0-dimensional.
- Span \( \{[1, 3], [2, 6]\} \) is 1-dimensional.
- Span \( \{[1, 0, 0], [0, 1, 0], [1, 1, 0]\} \) is 2-dimensional.

**Fundamental Question:** How can we predict the dimensionality of the span of some vectors?
Geometry of sets of vectors: span of vectors over $\mathbb{R}$

Span of two 3-vectors? Span $\{[1, 0, 1.65], [0, 1, 1]\}$ is a plane in three dimensions:

*Two-dimensional*

Useful for plotting the plane

\[\{\alpha [1, 0.1.65] + \beta [0, 1, 1] : \\
\alpha \in \{-5, -4, \ldots, 3, 4\}, \\
\beta \in \{-5, -4, \ldots, 3, 4\}\}\]
Geometry of sets of vectors: span of vectors over $\mathbb{R}$

Span of two 3-vectors? Span $\{(1, 0, 1.65), (0, 1, 1)\}$ is a plane in three dimensions:

Two-dimensional

Perhaps a more familiar way to specify a plane:

$$\{(x, y, z) : ax + by + cz = 0\}$$

Using dot-product, we could rewrite as

$$\{[x, y, z] : [a, b, c] \cdot [x, y, z] = 0\}$$

Set of vectors satisfying a linear equation with right-hand side zero.

We can similarly specify a line in three dimensions:

$$\{[x, y, z] : a_1 \cdot [x, y, z] = 0, a_2 \cdot [x, y, z] = 0\}$$

Two ways to represent a geometric object (line, plane, etc.) containing the origin:

- Span of some vectors
- Solution set of some system of linear equations with zero right-hand sides
Geometry of sets of vectors: Two representations

Two ways to represent a geometric object (line, plane, etc.) containing the origin:

- Span of some vectors
- Solution set of some system of linear equations with zero right-hand sides

![Graphical representation of geometric objects]

**Span** \{\[4, -1, 1\], \[0, 1, 1\]\} \quad \{\[x, y, z\] : \[1, 2, -2\] \cdot \[x, y, z\] = 0\}

**Span** \{\[1, 2, -2\]\} \quad \{\[x, y, z\] : 
\[4, -1, 1\] \cdot \[x, y, z\] = 0, 
\[0, 1, 1\] \cdot \[x, y, z\] = 0\}
Geometry of sets of vectors: Two representations

Two ways to represent a geometric object (line, plane, etc.) containing the origin:
- Span of some vectors
- Solution set of some system of linear equations with zero right-hand sides

*Each representation has its uses.*

Suppose you want to find the plane containing two given lines

- First line is Span \{[4, −1, 1]\}.
- Second line is Span \{[0, 1, 1]\}.

- The plane containing these two lines is Span \{[4, −1, 1], [0, 1, 1]\}
Geometry of sets of vectors: Two representations

Two ways to represent a geometric object (line, plane, etc.) containing the origin:
  - Span of some vectors
  - Solution set of some system of linear equations with zero right-hand sides

*Each representation has its uses.*

Suppose you want to find the intersection of two given planes:

- First plane is
  \[
  \{[x, y, z] : [4, -1, 1] \cdot [x, y, z] = 0\}.
  \]

- Second plane is
  \[
  \{[x, y, z] : [0, 1, 1] \cdot [x, y, z] = 0\}.
  \]

- The intersection is
  \[
  \{[x, y, z] :
  [4, -1, 1] \cdot [x, y, z] = 0, [0, 1, 1] \cdot [x, y, z] = 0\}.
  \]
Two representations: What's common?

Subset of $\mathbb{F}^D$ that satisfies three properties:

Property V1 Subset contains the zero vector $\mathbf{0}$

Property V2 If subset contains $\mathbf{v}$ then it contains $\alpha \mathbf{v}$ for every scalar $\alpha$

Property V3 If subset contains $\mathbf{u}$ and $\mathbf{v}$ then it contains $\mathbf{u} + \mathbf{v}$

$\text{Span} \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ satisfies

- Property V1 because
  \[ 0 \mathbf{v}_1 + \cdots + 0 \mathbf{v}_n \]

- Property V2 because
  \[ \text{if } \mathbf{v} = \beta_1 \mathbf{v}_1 + \cdots + \beta_n \mathbf{v}_n \text{ then } \alpha \mathbf{v} = \alpha \beta_1 \mathbf{v}_1 + \cdots + \alpha \beta_n \mathbf{v}_n \]

- Property V3 because
  \[ \text{if } \mathbf{u} = \alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n \]
  \[ \text{and } \mathbf{v} = \beta_1 \mathbf{v}_1 + \cdots + \beta_n \mathbf{v}_n \]
  \[ \text{then } \mathbf{u} + \mathbf{v} = (\alpha_1 + \beta_1) \mathbf{v}_1 + \cdots + (\alpha_n + \beta_n) \mathbf{v}_n \]

Solution set $\{ \mathbf{x} : a_1 \mathbf{x} = 0, \ldots, a_m \mathbf{x} = 0 \}$ satisfies

- Property V1 because
  \[ a_1 \cdot 0 = 0, \ldots, a_m \cdot 0 = 0 \]

- Property V2 because
  \[ \text{if } a_1 \cdot \mathbf{v} = 0, \ldots, a_m \cdot \mathbf{v} = 0 \text{ then } a_1 \cdot (\alpha \mathbf{v}) = \alpha (a_1 \cdot \mathbf{v}) = 0, \ldots, a_m \cdot (\alpha \mathbf{v}) = \alpha (a_m \cdot \mathbf{v}) = 0 \]

- Property V3 because
  \[ \text{if } a_1 \cdot \mathbf{u} = 0, \ldots, a_m \cdot \mathbf{u} = 0 \]
  \[ \text{and } \mathbf{v} = \beta_1 \mathbf{v}_1 + \cdots + \beta_n \mathbf{v}_n \]
  \[ \text{then } a_1 \cdot (\mathbf{u} + \mathbf{v}) = (a_1 + \beta_1) \mathbf{v}_1 + \cdots + (a_m + \beta_n) \mathbf{v}_n \]

Any subset $V$ of $\mathbb{F}^D$ satisfying the three properties is called a vector space.

Example: $\text{Span} \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ and $\{ \mathbf{x} : a_1 \mathbf{x} = 0, \ldots, a_m \mathbf{x} = 0 \}$ are vector spaces.

If $U$ is also a vector space and $U$ is a subset of $V$ then $U$ is called a subspace of $V$.

Example: $\text{Span} \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ and $\{ \mathbf{x} : a_1 \mathbf{x} = 0, \ldots, a_m \mathbf{x} = 0 \}$ are subspaces of $\mathbb{R}^D$.

Possibly profound fact we will learn later: Every subspace of $\mathbb{R}^D$ can be written in the form $\text{Span} \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ or can be written in the form $\{ \mathbf{x} : a_1 \mathbf{x} = 0, \ldots, a_m \mathbf{x} = 0 \}$. 
Abstract vector spaces

In traditional, abstract approach to linear algebra:

- We don’t define vectors as sequences \([1,2,3]\) or even functions \(\{a:1, \ b:2, \ c:3\}\).
- We define a vector space over a field \(\mathbb{F}\) to be any set \(V\) that is equipped with
  - an *addition* operation, and
  - a *scalar-multiplication* operation

satisfying certain axioms (e.g. commutate and distributive laws) and Properties V1, V2, V3.

Abstract approach has the advantage that it avoids committing to specific structure for vectors.

I avoid abstract approach in this class because more concrete notion of vectors is helpful in developing intuition.
Geometric objects that exclude the origin

How to represent a line that does *not* contain the origin?

Start with a line that *does* contain the origin.
We know that points of such a line form a vector space $\mathcal{V}$.

Translate the line by adding a vector $c$ to every vector in $\mathcal{V}$:

$$\{c + v : v \in \mathcal{V}\}$$

(abbreviated $c + \mathcal{V}$)

Result is line through $c$ instead of through origin.
Geometric objects that exclude the origin

How to represent a plane that does not contain the origin?

▶

Start with a plane that does contain the origin.

We know that points of such a plane form a vector space \( \mathcal{V} \).

▶

Translate it by adding a vector \( \mathbf{c} \) to every vector in \( \mathcal{V} \)

\[ \{ \mathbf{c} + \mathbf{v} : \mathbf{v} \in \mathcal{V} \} \]

(abbreviated \( \mathbf{c} + \mathcal{V} \))

▶ Result is plane containing \( \mathbf{c} \).
**Definition:** If $c$ is a vector and $V$ is a vector space then $c + V$ is called an *affine space*.

**Examples:** A plane or a line not necessarily containing the origin.
**Example:** The plane containing $u_1 = [3, 0, 0]$, $u_2 = [-3, 1, -1]$, and $u_3 = [1, -1, 1]$.

Want to express this plane as $u_1 + V$ where $V$ is the span of two vectors (a plane containing the origin)

Let $V = \text{Span} \{a, b\}$ where

$$a = u_2 - u_1 \text{ and } b = u_3 - u_1$$

Since $u_1 + V$ is a translation of a plane, it is also a plane.

- $\text{Span} \{a, b\}$ contains 0, so $u_1 + \text{Span} \{a, b\}$ contains $u_1$.
- $\text{Span} \{a, b\}$ contains $u_2 - u_1$ so $u_1 + \text{Span} \{a, b\}$ contains $u_2$.
- $\text{Span} \{a, b\}$ contains $u_3 - u_1$ so $u_1 + \text{Span} \{a, b\}$ contains $u_3$.

Thus the plane $u_1 + \text{Span} \{a, b\}$ contains $u_1, u_2, u_3$.

Only one plane contains those three points, so this is that one.
Affine space and affine combination

**Example:** The plane containing $\mathbf{u}_1 = [3, 0, 0]$, $\mathbf{u}_2 = [-3, 1, -1]$, and $\mathbf{u}_3 = [1, -1, 1]$:

$$\mathbf{u}_1 + \text{Span} \{ \mathbf{u}_2 - \mathbf{u}_1, \mathbf{u}_3 - \mathbf{u}_1 \}$$

Cleaner way to write it?

$$\mathbf{u}_1 + \text{Span} \{ \mathbf{u}_2 - \mathbf{u}_1, \mathbf{u}_3 - \mathbf{u}_1 \} = \{ \mathbf{u}_1 + \alpha (\mathbf{u}_2 - \mathbf{u}_1) + \beta (\mathbf{u}_3 - \mathbf{u}_1) : \alpha, \beta \in \mathbb{R} \}$$

$$= \{ \mathbf{u}_1 + \alpha \mathbf{u}_2 - \alpha \mathbf{u}_1 + \beta \mathbf{u}_3 - \beta \mathbf{u}_1 : \alpha, \beta \in \mathbb{R} \}$$

$$= \{ (1 - \alpha - \beta) \mathbf{u}_1 + \alpha \mathbf{u}_2 + \beta \mathbf{u}_3 : \alpha, \beta \in \mathbb{R} \}$$

$$= \{ \gamma \mathbf{u}_1 + \alpha \mathbf{u}_2 + \beta \mathbf{u}_3 : \gamma + \alpha + \beta = 1 \}$$

**Definition:** A linear combination $\gamma \mathbf{u}_1 + \alpha \mathbf{u}_2 + \beta \mathbf{u}_3$ where $\gamma + \alpha + \beta = 1$ is an **affine combination**.
**Affine combination**

**Definition:** A linear combination

$$\alpha_1 \mathbf{u}_1 + \alpha_2 \mathbf{u}_2 + \cdots + \alpha_n \mathbf{u}_n$$

where

$$\alpha_1 + \alpha_2 + \cdots + \alpha_n = 1$$

is an *affine combination*.

**Definition:** The set of all affine combinations of vectors $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ is called the *affine hull* of those vectors.

$$\text{Affine hull of } \mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n = \mathbf{u}_1 + \text{Span } \{ \mathbf{u}_2 - \mathbf{u}_1, \ldots, \mathbf{u}_n - \mathbf{u}_1 \}$$

This shows that the affine hull of some vectors is an affine space.
Geometric objects not containing the origin: equations

Can express a plane as $u_1 + \mathcal{V}$ or affine hull of $u_1, u_2, \ldots, u_n$.

More familiar way to express a plane:

The solution set of an equation $ax + by + cz = d$

In vector terms,

$$\left\{ [x, y, z] : [a, b, c] \cdot [x, y, z] = d \right\}$$

In general, a geometric object (point, line, plane, ...) can be expressed as the solution set of a system of linear equations.

$$\left\{ x : a_1 \cdot x = \beta_1, \ldots, a_m \cdot x = \beta_m \right\}$$

Conversely, is the solution set an affine space?

Consider solution set of a contradictory system of equations, e.g. $1x = 1, 2x = 1$:

- Solution set is empty....
- ...but a vector space $\mathcal{V}$ always contains the zero vector,
- ...so an affine space $u_1 + \mathcal{V}$ always contains at least one vector.

Turns out this the only exception:

**Theorem**: The solution set of a linear system is either empty or an affine space.
Affine spaces and linear systems

**Theorem:** The solution set of a linear system is either empty or an affine space.

Each linear system corresponds to a linear system with zero right-hand sides:

\[
\begin{align*}
\mathbf{a}_1 \cdot \mathbf{x} &= \beta_1 \\
&\vdots \\
\mathbf{a}_m \cdot \mathbf{x} &= \beta_m \\
\end{align*}
\]

\[\Rightarrow\]

\[
\begin{align*}
\mathbf{a}_1 \cdot \mathbf{x} &= 0 \\
&\vdots \\
\mathbf{a}_m \cdot \mathbf{x} &= 0 \\
\end{align*}
\]

**Definition:**
A linear equation \( \mathbf{a} \cdot \mathbf{x} = 0 \) with zero right-hand side is a *homogeneous* linear equation. A system of homogeneous linear equations is called a *homogeneous* linear system.

**We already know:** The solution set of a homogeneous linear system is a vector space.

**Lemma:** Let \( \mathbf{u}_1 \) be a solution to a linear system. Then, for any other vector \( \mathbf{u}_2 \), \( \mathbf{u}_2 \) is also a solution if and only if \( \mathbf{u}_2 - \mathbf{u}_1 \) is a solution to the corresponding homogeneous linear system.
Affine spaces and linear systems

\[
\begin{align*}
\mathbf{a}_1 \cdot \mathbf{x} &= \beta_1 \\
\vdots \\
\mathbf{a}_m \cdot \mathbf{x} &= \beta_m
\end{align*}
\quad \Rightarrow \quad \\
\begin{align*}
\mathbf{a}_1 \cdot \mathbf{x} &= 0 \\
\vdots \\
\mathbf{a}_m \cdot \mathbf{x} &= 0
\end{align*}
\]

**Lemma:** Let \( \mathbf{u}_1 \) be a solution to a linear system. Then, for any other vector \( \mathbf{u}_2 \), \( \mathbf{u}_2 \) is also a solution if and only if \( \mathbf{u}_2 - \mathbf{u}_1 \) is a solution to the corresponding homogeneous linear system.

**Proof:** We assume \( \mathbf{a}_1 \cdot \mathbf{u}_1 = \beta_1, \ldots, \mathbf{a}_m \cdot \mathbf{u}_1 = \beta_m \), so

\[
\begin{align*}
\mathbf{a}_1 \cdot \mathbf{u}_2 &= \beta_1 \\
\vdots \\
\mathbf{a}_m \cdot \mathbf{u}_2 &= \beta_m
\end{align*}
\quad \text{iff} \quad \\
\begin{align*}
\mathbf{a}_1 \cdot \mathbf{u}_2 - \mathbf{a}_1 \cdot \mathbf{u}_1 &= 0 \\
\vdots \\
\mathbf{a}_m \cdot \mathbf{u}_2 - \mathbf{a}_m \cdot \mathbf{u}_1 &= 0
\end{align*}
\quad \text{iff} \quad \\
\begin{align*}
\mathbf{a}_1 \cdot (\mathbf{u}_2 - \mathbf{u}_1) &= 0 \\
\vdots \\
\mathbf{a}_m \cdot (\mathbf{u}_2 - \mathbf{u}_1) &= 0
\end{align*}
\]

\[QED\]
Lemma: Let $u_1$ be a solution to a linear system. Then, for any other vector $u_2$, $u_2$ is also a solution if and only if $u_2 - u_1$ is a solution to the corresponding homogeneous linear system.

We use this lemma to prove the theorem:

**Theorem:** The solution set of a linear system is either empty or an affine space.

- Let $\mathcal{V} =$ set of solutions to corresponding homogeneous linear system.
- If the linear system has no solution, its solution set is empty.
- If it does has a solution $u_1$ then

\[
\{\text{solutions to linear system}\} = \{u_2 : u_2 - u_1 \in \mathcal{V}\}
\]

(substitute $v = u_2 - u_1$)

\[
= \{u_1 + v : v \in \mathcal{V}\}
\]

QED
Number of solutions to a linear system

We just proved:

If \( \mathbf{u}_1 \) is a solution to a linear system then

\[
\{ \text{solutions to linear system} \} = \{ \mathbf{u}_1 + \mathbf{v} : \mathbf{v} \in \mathcal{V} \}
\]

where \( \mathcal{V} = \{ \text{solutions to corresponding homogeneous linear system} \} \)

Implications:

**Long ago we asked:** How can we tell if a linear system has only one solution?

**Now we know:** If a linear system has a solution \( \mathbf{u}_1 \) then that solution is unique if the only solution to the corresponding homogeneous linear system is \( \mathbf{0} \).

**Long ago we asked:** How can we find the number of solutions to a linear system over \( GF(2) \)?

**Now we know:** Number of solutions either is zero or is equal to the number of solutions to the corresponding *homogeneous* linear system.
A **checksum function** maps long files to short sequences.

**Idea:**
- Web page shows the checksum of each file to be downloaded.
- Download the file and run the checksum function on it.
- If result does not match checksum on web page, you know the file has been corrupted.
- If random corruption occurs, how likely are you to detect it?

**Impractical but instructive checksum function:**
- **input:** an \( n \)-vector \( \mathbf{x} \) over \( GF(2) \)
- **output:** \([a_1 \cdot \mathbf{x}, a_2 \cdot \mathbf{x}, \ldots, a_{64} \cdot \mathbf{x}]\)

where \( a_1, a_2, \ldots, a_{64} \) are sixty-four \( n \)-vectors.
Number of solutions: checksum function

Our checksum function:

- **input**: an \( n \)-vector \( \mathbf{x} \) over \( GF(2) \)
- **output**: \([a_1 \cdot \mathbf{x}, a_2 \cdot \mathbf{x}, \ldots, a_{64} \cdot \mathbf{x}]\)

where \( a_1, a_2, \ldots, a_{64} \) are sixty-four \( n \)-vectors.

Suppose \( p \) is the original file, and it is randomly corrupted during download.

**What is the probability that the corruption is undetected?**

The checksum of the original file is \([\beta_1, \ldots, \beta_{64}] = [a_1 \cdot \mathbf{p}, \ldots, a_{64} \cdot \mathbf{p}]\).

Suppose corrupted version is \( p + e \).

Then checksum of corrupted file matches checkum of original if and only if

\[
\begin{align*}
    a_1 \cdot (p + e) &= \beta_1 & \quad & a_1 \cdot p - a_1 \cdot (p + e) &= 0 & \quad & a_1 \cdot e &= 0 \\
    \vdots & & \text{iff} & \vdots & & \text{iff} & \vdots \\
    a_{64} \cdot (p + e) &= \beta_{64} & \quad & a_{64} \cdot p - a_{64} \cdot (p + e) &= 0 & \quad & a_{64} \cdot e &= 0
\end{align*}
\]

iff \( e \) is a solution to the homogeneous linear system \( a_1 \cdot \mathbf{x} = 0, \ldots, a_{64} \cdot \mathbf{x} = 0 \).
Number of solutions: checksum function

Suppose corrupted version is $p + e$.
Then checksum of corrupted file matches checksum of original if and only if $e$ is a solution to homogeneous linear system

\[
\begin{align*}
a_1 \cdot x &= 0 \\
&\vdots \\
a_{64} \cdot x &= 0
\end{align*}
\]

If $e$ is chosen according to the uniform distribution,

\[
\text{Probability} \left( p + e \text{ has same checksum as } p \right) = \frac{\text{Probability} \left( e \text{ is a solution to homogeneous linear system} \right)}{\text{number of } n\text{-vectors}} = \frac{\text{number of solutions to homogeneous linear system}}{2^n}
\]

**Question:**
How to find out number of solutions to a homogeneous linear system over $GF(2)$?
Geometry of sets of vectors: convex hull

**Earlier, we saw:** The \( \mathbf{u} \)-to-\( \mathbf{v} \) line segment is

\[
\{ \alpha \mathbf{u} + \beta \mathbf{v} : \alpha \in \mathbb{R}, \beta \in \mathbb{R}, \alpha \geq 0, \beta \geq 0, \alpha + \beta = 1 \}\]

**Definition:** For vectors \( \mathbf{v}_1, \ldots, \mathbf{v}_n \) over \( \mathbb{R} \), a linear combination

\[
\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n
\]

is a *convex combination* if the coefficients are all nonnegative and they sum to 1.

- Convex hull of a single vector is a point.
- Convex hull of two vectors is a line segment.
- Convex hull of three vectors is a triangle

Convex hull of more vectors? Could be higher-dimensional... but not necessarily.

For example, a convex polygon is the convex hull of its vertices