Span

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 Span $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$.

Span: Attacking the authentication scheme

If Eve knows the password satisfies

$$\begin{aligned} \mathbf{a}_1 \cdot \mathbf{x} &= \beta_1 \\ &\vdots \\ \mathbf{a}_m \cdot \mathbf{x} &= \beta_m \end{aligned}$$

Then she can calculate right response to any challenge in Span $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$:

Proof: Suppose $\mathbf{a} = \alpha_1\, \mathbf{a}_1 + \cdots + \alpha_m\, \mathbf{a}_m$. Then

$$\begin{aligned} \mathbf{a} \cdot \mathbf{x} &= (\alpha_1\, \mathbf{a}_1 + \cdots + \alpha_m\, \mathbf{a}_m) \cdot \mathbf{x} \\ &= \alpha_1\, \mathbf{a}_1 \cdot \mathbf{x} + \cdots + \alpha_m\, \mathbf{a}_m \cdot \mathbf{x} && \text{by distributivity} \\ &= \alpha_1\, (\mathbf{a}_1 \cdot \mathbf{x}) + \cdots + \alpha_m\, (\mathbf{a}_m \cdot \mathbf{x}) && \text{by homogeneity} \\ &= \alpha_1\, \beta_1 + \cdots + \alpha_m\, \beta_m \end{aligned}$$

Question: Any others? Answer will come later.

Span: $GF(2)$ vectors

Quiz: How many vectors are in Span $\{[1,1],[0,1]\}$ over the field $GF(2)$?

Span: $GF(2)$ vectors

Quiz: How many vectors are in Span $\{[1,1],[0,1]\}$ over the field $GF(2)$?

Answer: The linear combinations are

$$\begin{aligned} 0\,[1,1] + 0\,[0,1] &= [0,0] \\ 0\,[1,1] + 1\,[0,1] &= [0,1] \\ 1\,[1,1] + 0\,[0,1] &= [1,1] \\ 1\,[1,1] + 1\,[0,1] &= [1,0] \end{aligned}$$

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

$$0\,[1,1] = [0,0]$$
$$1\,[1,1] = [1,1]$$

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 $[3,0,0]$, $[0,2,0]$, and $[0,0,1]$ are in Span $\{[1,0,0],[1,1,0],[1,1,1]\}$

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

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:

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

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

$$\begin{aligned}[x, y, z] = (x/3)\Big(3\,[1, 0, 0]\Big) \quad &+ \quad (y/2)\Big(-2\,[1, 0, 0] + 2\,[1, 1, 0]\Big) \\ &+ \quad z\Big(-1\,[1, 1, 0] + 1\,[1, 1, 1]\Big)\end{aligned}$$

- Multiply through, using distributivity and associativity:

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

- Collect like terms, using distributivity:

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

Generators

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:

$$
\begin{aligned}
[3,0,0] &= 2\,[2,0,1] - 1\,[1,0,2] + 0\,[2,2,2] \\
[0,2,0] &= -\frac{2}{3}\,[2,0,1] - \frac{2}{3}\,[1,0,2] + 1\,[2,2,2] \\
[0,0,1] &= -\frac{1}{3}\,[2,0,1] + \frac{2}{3}\,[1,0,2] + 0\,[2,2,2]
\end{aligned}
$$

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.

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

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 2×2 *Lights Out* be solved from every starting configuration?

Equivalent to asking whether the 2×2 button vectors

$$\begin{bmatrix} \bullet & \bullet \\ \bullet & \end{bmatrix} \quad \begin{bmatrix} \bullet & \bullet \\ & \bullet \end{bmatrix} \quad \begin{bmatrix} \bullet & \\ \bullet & \bullet \end{bmatrix} \quad \begin{bmatrix} & \bullet \\ \bullet & \bullet \end{bmatrix}$$

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:

$$\begin{bmatrix} \bullet & \\ & \end{bmatrix} = 1\begin{bmatrix} \bullet & \bullet \\ \bullet & \end{bmatrix} + 1\begin{bmatrix} \bullet & \bullet \\ & \bullet \end{bmatrix} + 1\begin{bmatrix} \bullet & \\ \bullet & \bullet \end{bmatrix} + 0\begin{bmatrix} & \bullet \\ \bullet & \bullet \end{bmatrix}$$

$$\begin{bmatrix} & \bullet \\ & \end{bmatrix} = 1\begin{bmatrix} \bullet & \bullet \\ \bullet & \end{bmatrix} + 1\begin{bmatrix} \bullet & \bullet \\ & \bullet \end{bmatrix} + 0\begin{bmatrix} \bullet & \\ \bullet & \bullet \end{bmatrix} + 1\begin{bmatrix} & \bullet \\ \bullet & \bullet \end{bmatrix}$$

$$\begin{bmatrix} & \\ \bullet & \end{bmatrix} = 1\begin{bmatrix} \bullet & \bullet \\ \bullet & \end{bmatrix} + 0\begin{bmatrix} \bullet & \bullet \\ & \bullet \end{bmatrix} + 1\begin{bmatrix} \bullet & \\ \bullet & \bullet \end{bmatrix} + 1\begin{bmatrix} & \bullet \\ \bullet & \bullet \end{bmatrix}$$

$$\begin{bmatrix} & \\ & \bullet \end{bmatrix} = 0\begin{bmatrix} \bullet & \bullet \\ \bullet & \end{bmatrix} + 1\begin{bmatrix} \bullet & \bullet \\ & \bullet \end{bmatrix} + 1\begin{bmatrix} \bullet & \\ \bullet & \bullet \end{bmatrix} + 1\begin{bmatrix} & \bullet \\ \bullet & \bullet \end{bmatrix}$$