#### Review of vector terms

- ▶ A *D*-vector over  $\mathbb{F}$  is a function with domain *D* and co-domain  $\mathbb{F}$ .  $\mathbb{F}$  must be a field.
- ▶ The set of such vectors is written  $\mathbb{F}^D$  (recall from *The Function*)
- ▶ An *n*-vector over  $\mathbb{F}$  is a function with domain  $\{0, 1, 2, ..., n-1\}$  and co-domain  $\mathbb{F}$ . Can also represent as an *n*-element list.

## Vector algebraic properties

#### **Addition**

- ► Addition is associative: (u + v) + w = u + (v + w)
- ▶ Addition is commutative:  $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$

#### Scalar-vector multiplication

► Scalar-vector multiplication is associative:  $(\alpha \beta) \mathbf{v} = \alpha (\beta \mathbf{v})$ 

#### Both addition and scalar-vector multiplication

► Scalar-vector multiplication distributes over addition:  $\alpha(\mathbf{u} + \mathbf{v}) = \alpha \mathbf{u} + \alpha \mathbf{v}$ 

#### **Dot-product**

- ▶ Dot-product is commutative:  $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$
- **▶ Dot-product is homogeneous:**  $(\alpha \mathbf{u}) \cdot \mathbf{v} = \alpha (\mathbf{u} \cdot \mathbf{v})$
- ▶ Dot-product distributes over addition:  $\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w}$

# Solving a triangular system of linear equations

#### How to find solution to this linear system?

Write 
$$\mathbf{x} = [x_1, x_2, x_3, x_4]$$
. System becomes

# Solving a triangular system of linear equations: Backward substitution

#### **Solution strategy:**

- ▶ Solve for  $x_4$  using fourth equation.
- ▶ Plug value for  $x_4$  into third equations and solve for  $x_3$ .
- ▶ Plug values for  $x_4$  and  $x_3$  into second equation and solve for  $x_2$ .
- ▶ Plug values for  $x_4, x_3, x_2$  into first equation and solve for  $x_1$ .

The Vector Space

# [3] The Vector Space

## Linear Combinations

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

An expression

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

The scalars  $\alpha_1, \ldots, \alpha_n$  are the *coefficients* of the linear combination.

The scalars  $\alpha_1, \ldots, \alpha_n$  are the *coefficients* of the linear combination.

**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

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

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

**Definition:** A linear combination is *trivial* if the coefficients are all zero.

# Linear Combinations: JunkCo

The JunkCo factory makes five products:











using various resources.

	metal	concrete	plastic	water	electricity
garden gnome	0	1.3	0.2	8.0	0.4
hula hoop	0	0	1.5	0.4	0.3
slinky	0.25	0	0	0.2	0.7
silly putty	0	0	0.3	0.7	0.5
salad shooter	0.15	0	0.5	0.4	8.0

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

For making one gnome:

 $\mathbf{v}_1 = \{ \text{metal:0, concrete:1.3, plastic:0.2, water:.8, electricity:0.4} \}$ 

### Linear Combinations: JunkCo

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 **b** and a list  $[\mathbf{v}_1, \dots, \mathbf{v}_n]$  of vectors
- output: a list  $[\alpha_1, \dots, \alpha_n]$  of coefficients such that  $\mathbf{b} = \alpha_1 \mathbf{v}_1 + \dots + \alpha_n \mathbf{v}_n$  or a report that none exists.

#### Question: Is the solution unique?

### Lights Out

Button vectors for 2 × 2 *Lights Out*:

For a given initial state vector  $\mathbf{s} = \begin{bmatrix} \bullet \\ \bullet \end{bmatrix}$ , Which subset of button vectors sum to  $\mathbf{s}$ ?

Reformulate in terms of linear combinations.

Write

$$= \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_4$$

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* 

Find subset of 
$$GF(2)$$
 vectors  $\mathbf{v}_1, \dots, \mathbf{v}_n$  whose sum equals  $\mathbf{s}$ 

ctors 
$$\Rightarrow$$
 Express  $\mathbf{s}$  as a linear combination of  $\mathbf{v}_1, \dots, \mathbf{v}_n$ 

Which set of button vectors sum to **s**?

## Lights Out

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

## Span

**Definition:** The set of all linear combinations of some vectors  $\mathbf{v}_1, \dots, \mathbf{v}_n$  is called the *span* of these vectors

Written Span  $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ .

# Span: Attacking the authentication scheme

If Eve knows the password satisfies

$$\mathbf{a}_1 \cdot \mathbf{x} = \beta_1$$
  
 $\vdots$   
 $\mathbf{a}_m \cdot \mathbf{x} = \beta_m$ 

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

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

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

Suppose 
$$\mathbf{u} = u_1 \mathbf{u}_1 + \dots + u_m \mathbf{u}_m$$
. Then

$$\mathbf{a} \cdot \mathbf{x} = (\alpha_1 \, \mathbf{a}_1 + \dots + \alpha_m \, \mathbf{a}_m) \cdot \mathbf{x}$$
  
=  $\alpha_1 \, \mathbf{a}_1 \cdot \mathbf{x} + \dots + \alpha_m \, \mathbf{a}_m \cdot \mathbf{x}$  by distributivity

$$= \alpha_1 (\mathbf{a}_1 \cdot \mathbf{x}) + \dots + \alpha_m (\mathbf{a}_m \cdot \mathbf{x})$$
$$= \alpha_1 \beta_1 + \dots + \alpha_m \beta_m$$

by homogeneity

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)?

**Answer:** The linear combinations are

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

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 $\mathbf{v}_1, \dots, \mathbf{v}_n$ are vectors such that

 $\mathcal{V} = \mathsf{Span} \; \{ \mathbf{v}_1, \dots, \mathbf{v}_n \} \; \mathsf{then}$ 

- we say  $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$  is a *generating set* for  $\mathcal{V}$ ;
- we refer to the vectors  $\mathbf{v}_1, \dots, \mathbf{v}_n$  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  $\{[1,0,0],[1,1,0],[1,1,1]\}$

#### Why is that sufficient?

- ightharpoonup 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:

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

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:

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

# Solving a triangular system of linear equations: Backward substitution

$$1x_3 = -4 - 5x_4 = -4 - 5(3) = -19$$
  
so  $x_3 = -19/1 = -19$ 

$$3x_2 = 3 - 3x_3 - 2x_4$$

so  $x_4 = 6/2 = 3$ 

$$1x_3 = -4 - 5x_4 = -4 - 5(3) = -19$$
  
so  $x_3 = -19/1 = -19$   
 $3x_2 = 3 - 3x_3 - 2x_4 = 3 - 2(3) - 3(-19) = 54$   
so  $x_2 = 54/3 = 18$ 

$$1x_1 = -8 - 0.5x_2 + 2x_3 - 4x_4 = -8 - 4(3) + 2(-19) - 0.5(18) = -67$$
  
so  $x_1 = -67/1 = -67$ 

## Backsub Quiz

Use Back Substitution to solve the following triangular system of linear equations.

$$\begin{array}{rclrcrcr}
2x_1 & + & 2x_2 & - & 6x_3 & = & 0 \\
& & -5x_2 & + & 4x_3 & = & 7 \\
& & & 2x_3 & = & 1
\end{array}$$

# Solving a triangular system of linear equations: Backward substitution Hack to implement backward substitution using vectors:

- Initialize vector x to zero vector.
- Procedure will populate x entry by entry.
- ▶ When it is time to populate  $x_i$ , entries  $x_{i+1}, x_{i+2}, \dots, x_n$  will be populated, and other entries will be zero.
- ► Therefore can use dot-product:

return x

```
• Suppose you are computing x_2 using [0, 3, 3, 2] \cdot [x_1, x_2, x_3, x_4] = 3
```

• So far, vector 
$$\mathbf{x} = [x_1, x_2, x_3, x_4] = [0, 0, -19, 3].$$

▶ 
$$x_2 := (3 - ([0,3,3,2] \cdot x))/3$$
 def triangular\_solve(rowlist, b):

x = zero\_vec(rowlist[0].D)
for i in reversed(range(len(rowlist))):
 x[i] = (b[i] - rowlist[i] \* x)/rowlist[i][i]

Solving a triangular system of linear equations: Backward substitution

```
def triangular_solve(rowlist, b):
    x = zero_vec(rowlist[0].D)
    for i in reversed(range(len(rowlist))):
        x[i] = (b[i] - rowlist[i] * x)/rowlist[i][i]
    return x
```

#### **Observations:**

- ▶ If rowlist[i][i] is zero, procedure will raise ZeroDivisionError.
- ▶ If this never happens, solution found is the *only* solution to the system.

# Solving a triangular system of linear equations: Backward substitution

```
def triangular_solve(rowlist, b):
    x = zero vec(rowlist[0].D)
    for i in reversed(range(len(rowlist))):
        x[i] = (b[i] - rowlist[i] * x)/rowlist[i][i]
    return x
Our code only works when vectors in rowlist have domain D = \{0, 1, 2, \dots, n-1\}.
For arbitrary domains, need to specify an ordering for which system is "triangular":
def triangular_solve(rowlist, label_list, b):
    x = zero vec(set(label list))
    for r in reversed(range(len(rowlist))):
        c = label list[r]
        x[c] = (b[r] - x*rowlist[r])/rowlist[r][c]
    return x
```