[6] Dimension

The size of a basis

Key fact for this week: all bases for a vector space have the same size.

We use this as the "basis" for answering many pending questions.

Morphing Lemma

Morphing Lemma: Suppose S is a set of vectors, and B is a linearly independent set of vectors in Span S. Then $|S| \geq |B|$.

Before we prove it—what good is this lemma?

Theorem: Any basis for $\mathcal{V}$ is a smallest generating set for $\mathcal{V}$.

Proof: Let S be a smallest generating set for $\mathcal{V}$. Let B be a basis for $\mathcal{V}$. Then B is a linearly independent set of vectors in Span S. By the Morphing Lemma, B is no bigger than S, so B is also a smallest generating set.

Theorem: All bases for a vector space $\mathcal{V}$ have the same size.

Proof: They are all smallest generating sets.

Proof of the Morphing Lemma

Morphing Lemma: Suppose S is a set of vectors, and B is a linearly independent set of vectors in Span S. Then $|S| \geq |B|$.

Proof outline: modify S step by step, introducing vectors of B one by one, without increasing the size.

How? Using the Exchange Lemma....

Review of Exchange Lemma

Exchange Lemma: Suppose S is a set of vectors and A is a subset of S. Suppose $\mathbf{z}$ is a vector in Span S such that $A \cup \{\mathbf{z}\}$ is linearly independent.
Then there is a vector $\mathbf{w} \in S - A$ such that

$$\text{Span } S = \text{Span } (S \cup \{\mathbf{z}\} - \{\mathbf{w}\})$$

Proof of the Morphing Lemma

Let $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Define $S_0 = S$.
Prove by induction on $k \leq n$ that there is a generating set S_k of Span S that contains $\mathbf{b}_1, \ldots, \mathbf{b}_k$ and has size $|S|$.

Base case: $k = 0$ is trivial.

To go from S_{k-1} to S_k: use the Exchange Lemma.

- $A_k = \{\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}\}$ and $\mathbf{z} = \mathbf{b}_k$

Exchange Lemma $\Rightarrow$ there is a vector $\mathbf{w}$ in S_{k-1} such that

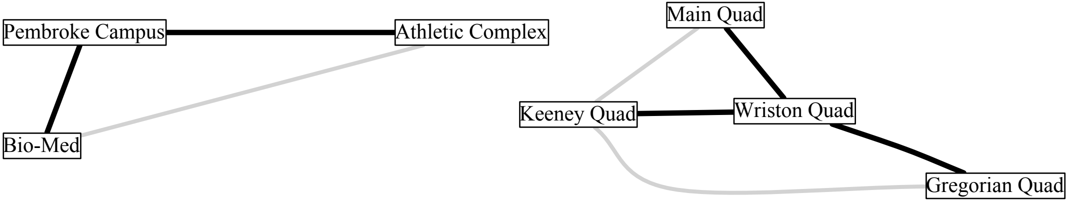
$$\text{Span } (S_{k-1} \cup \{\mathbf{b}_k\} - \{\mathbf{w}\}) = \text{Span } S_{k-1}$$

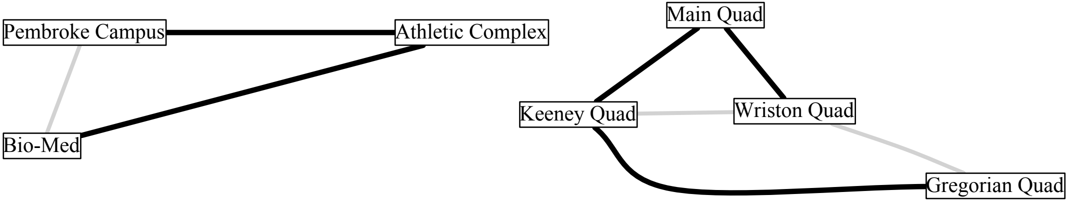
Set $S_k = S_{k-1} \cup \{\mathbf{b}_k\} - \{\mathbf{w}\}$.

QED

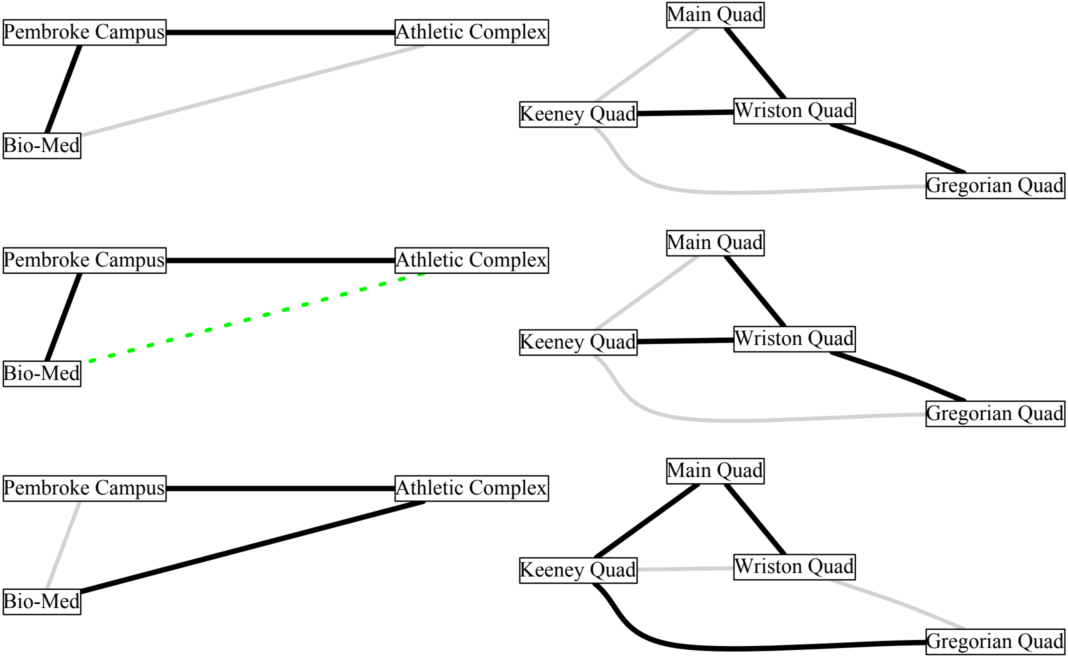
This induction proof is an algorithm.

Morphing from one spanning forest to another

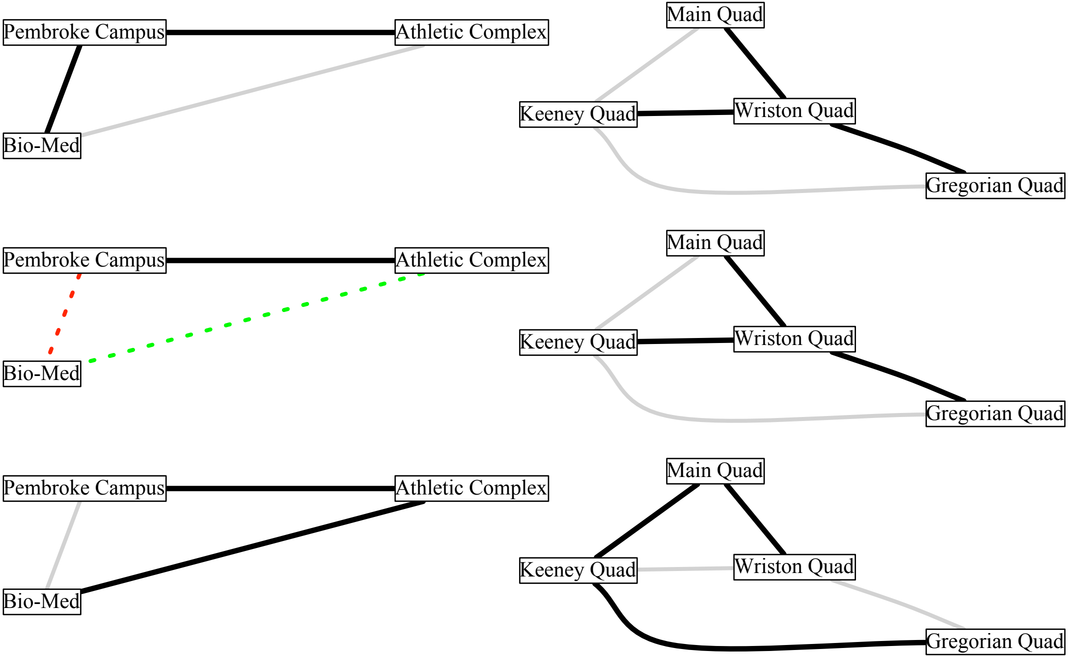




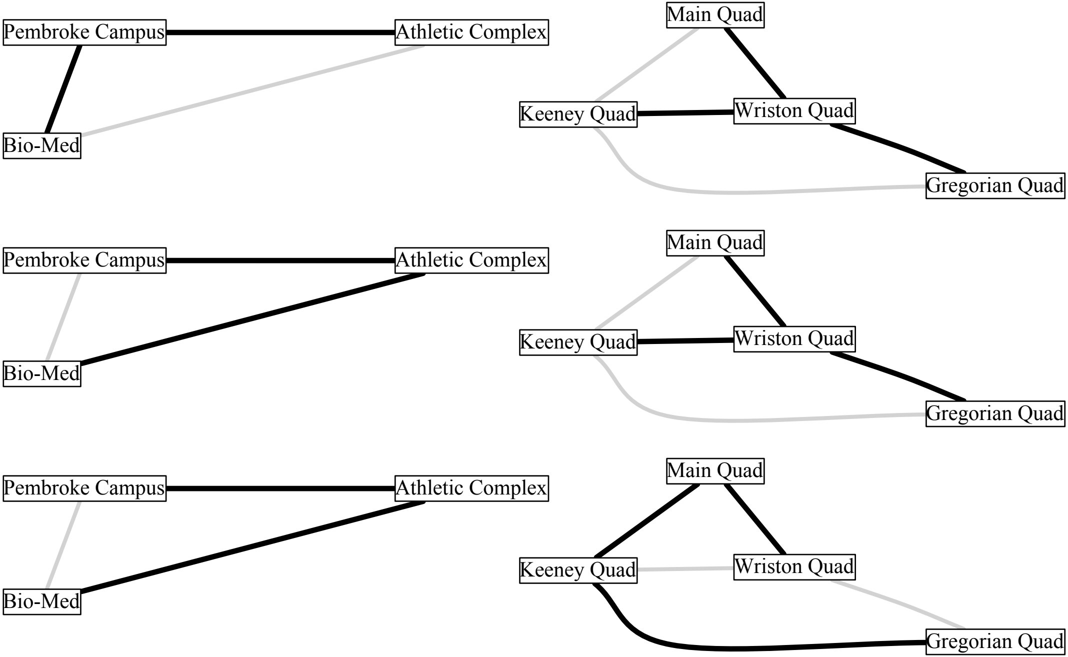
Morphing from one spanning forest to another



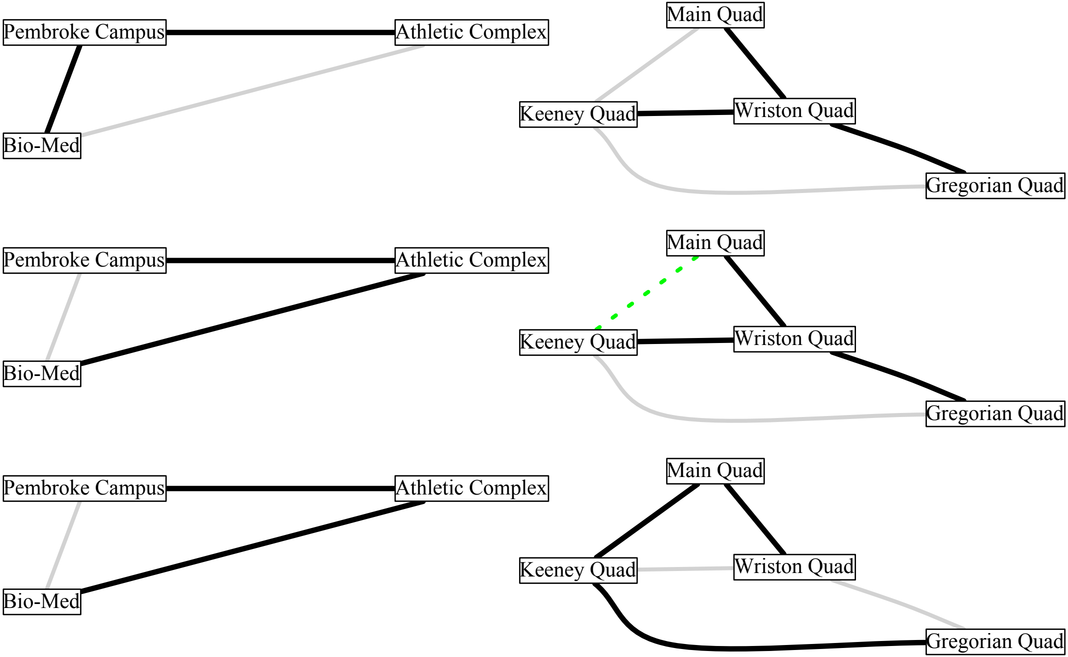
Morphing from one spanning forest to another



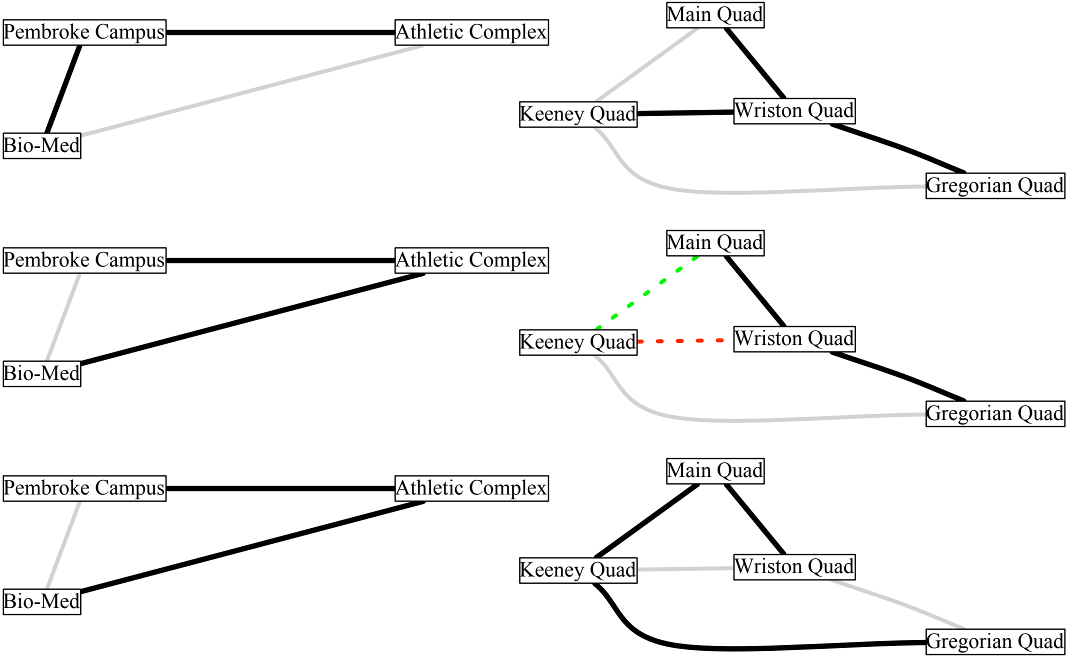
Morphing from one spanning forest to another



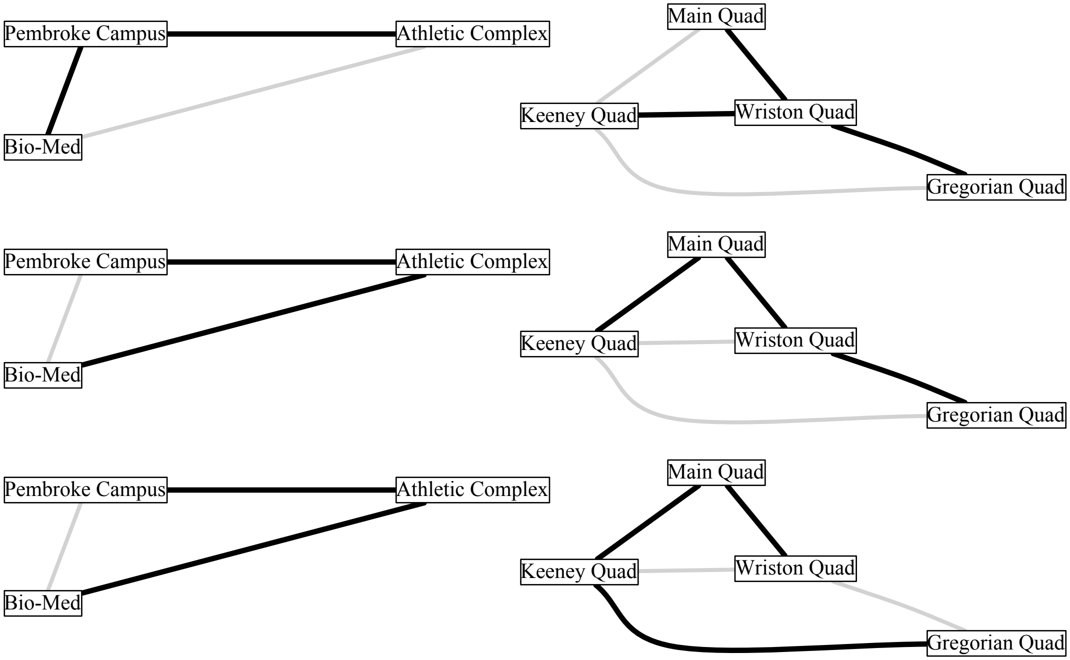
Morphing from one spanning forest to another



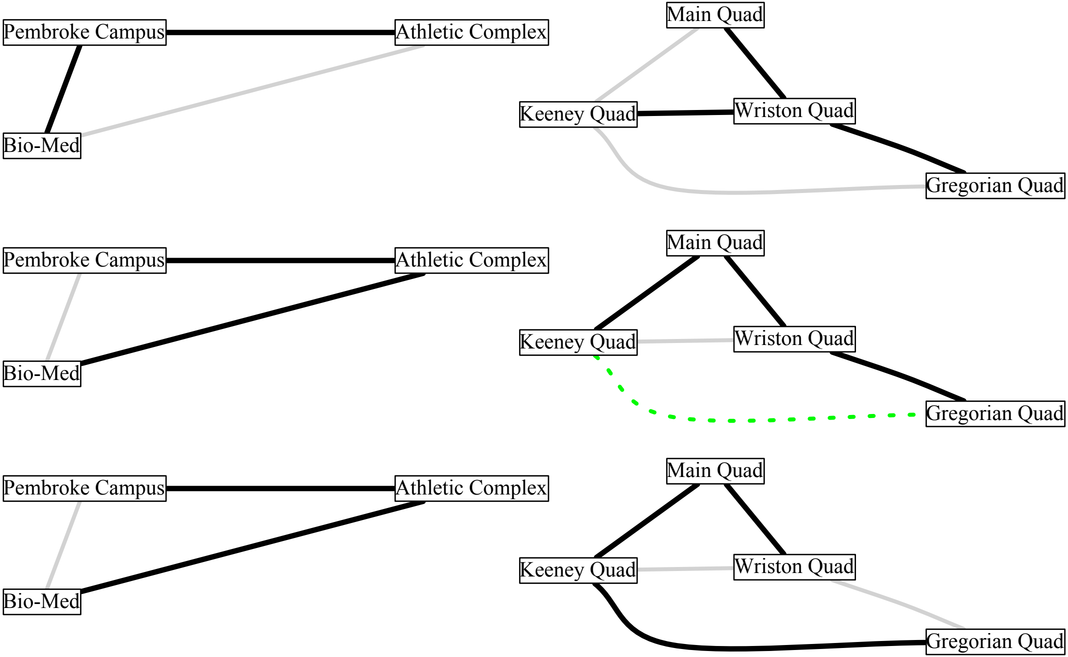
Morphing from one spanning forest to another



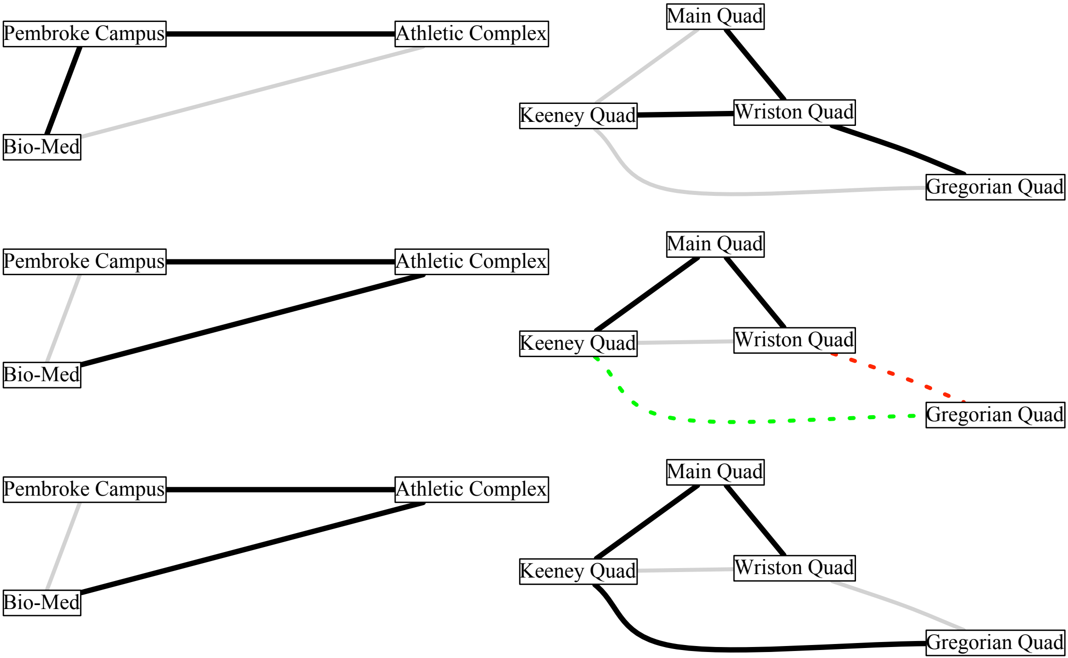
Morphing from one spanning forest to another



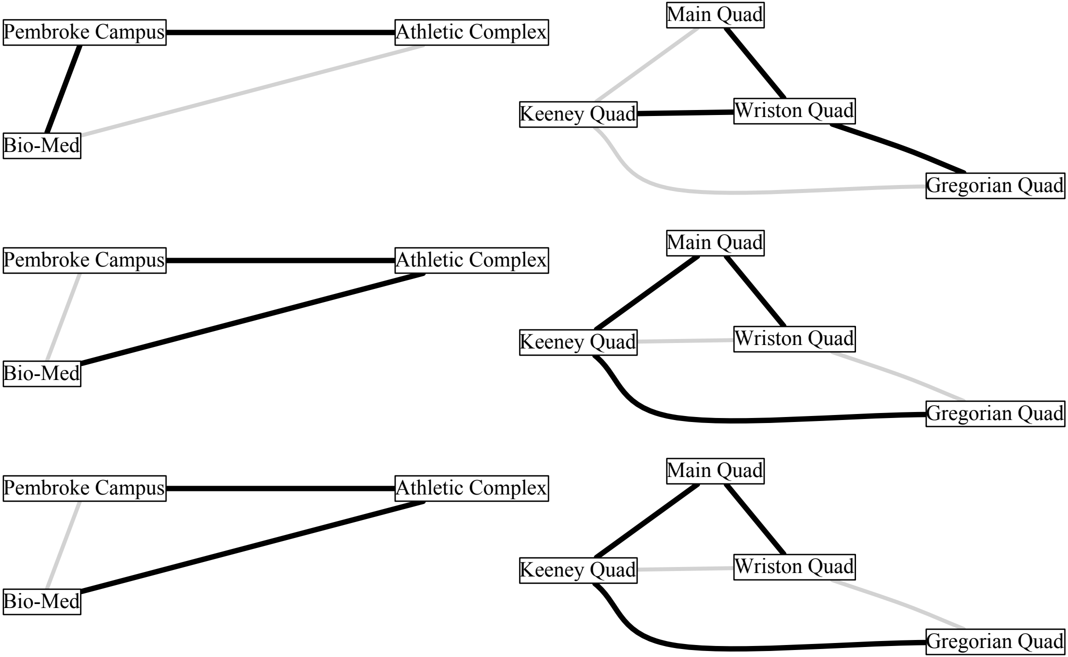
Morphing from one spanning forest to another



Morphing from one spanning forest to another



Morphing from one spanning forest to another



Dimension

Definition: We define the *dimension* of a vector space to be the size of a basis for that vector space. The dimension of a vector space $\mathcal{V}$ is written $\dim \mathcal{V}$.

Definition: We define the *rank* of a set S of vectors as the dimension of Span S. We write rank S.

Example: The vectors $[1, 0, 0], [0, 2, 0], [2, 4, 0]$ are linearly dependent.
Therefore their rank is less than three.
First two of these vectors form a basis for the span of all three, so the rank is two.

Example: The vector space Span $\{[0, 0, 0]\}$ is spanned by an empty set of vectors.
Therefore the rank of $\{[0, 0, 0]\}$ is zero.

Row rank, column rank

Definition: For a matrix M, the *row rank* of M is the rank of its rows, and the *column rank* of M is the rank of its columns.
Equivalently, the row rank of M is the dimension of Row M, and the column rank of M is the dimension of Col M.

Example: Consider the matrix

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 2 & 4 & 0 \end{bmatrix}$$

whose rows are the vectors we saw before: $[1, 0, 0], [0, 2, 0], [2, 4, 0]$
The set of these vectors has rank two, so the row rank of M is two.
The columns of M are $[1, 0, 2]$, $[0, 2, 4]$, and $[0, 0, 0]$.
Since the third vector is the zero vector, it is not needed for spanning the column space.
Since each of the first two vectors has a nonzero where the other has a zero, these two are linearly independent, so the column rank is two.

Row rank, column rank

Definition: For a matrix M, the *row rank* of M is the rank of its rows, and the *column rank* of M is the rank of its columns.
Equivalently, the row rank of M is the dimension of Row M, and the column rank of M is the dimension of Col M.

Example: Consider the matrix

$$M = \begin{bmatrix} 1 & 0 & 0 & 5 \\ 0 & 2 & 0 & 7 \\ 0 & 0 & 3 & 9 \end{bmatrix}$$

Each of the rows has a nonzero where the others have zeroes, so the three rows are linearly independent. Thus the row rank of M is three.
The columns of M are $[1, 0, 0]$, $[0, 2, 0]$, $[0, 0, 3]$, and $[5, 7, 9]$.
The first three columns are linearly independent, and the fourth can be written as a linear combination of the first three, so the column rank is three.

Row rank, column rank

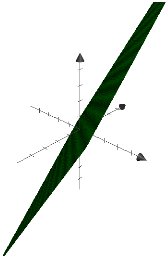
Definition: For a matrix M, the *row rank* of M is the rank of its rows, and the *column rank* of M is the rank of its columns.
Equivalently, the row rank of M is the dimension of Row M, and the column rank of M is the dimension of Col M.

Does column rank always equal row rank? ☺

Geometry

We have asked:

Fundamental Question: How can we predict the dimensionality of the span of some vectors?



Now we can answer:

Compute the rank of the set of vectors.

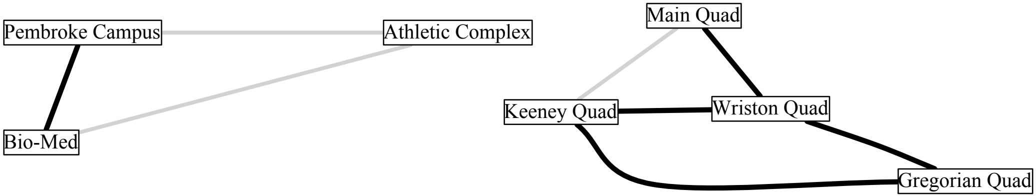
Examples:

• Span $\{[1, 2, -2]\}$ is a line but Span $\{[0, 0, 0]\}$ is a point.
First vector space has dimension one, second has dimension zero.

• Span $\{[1, 2], [3, 4]\}$ consists of all of $\mathbb{R}^2$ but Span $\{[1, 3], [2, 6]\}$ is a line
The first has dimension two and the second has dimension one.

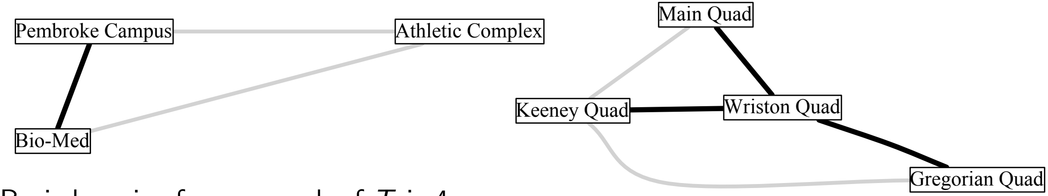
• Span $\{[1, 0, 0], [0, 1, 0], [0, 0, 1]\}$ is $\mathbb{R}^3$ but Span $\{[1, 0, 0], [0, 1, 0], [1, 1, 0]\}$ is a plane.
The first has dimension three and the second has dimension two.

Dimension and rank in graphs



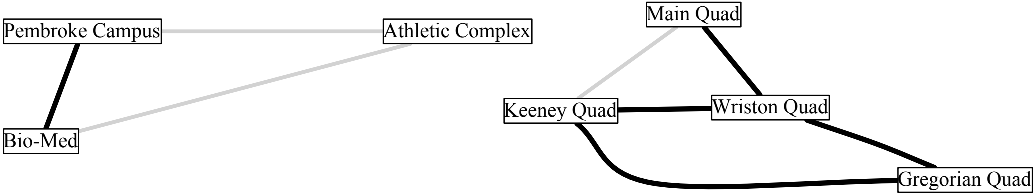
Let T = set of dark edges

Basis for Span T:



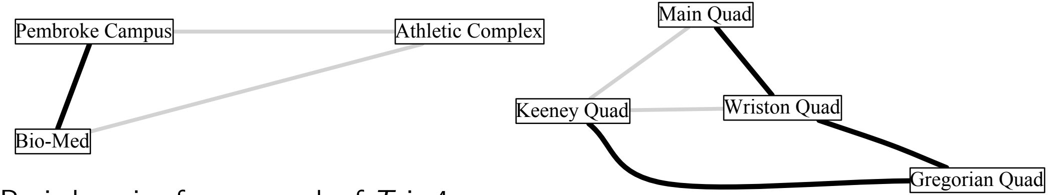
Basis has size four, so rank of T is 4.

Dimension and rank in graphs



Let T = set of dark edges

Basis for Span T:



Basis has size four, so rank of T is 4.

Cardinality of a vector space over $GF(2)$

Recall *checksum problem*
Checksum function $\mathbf{x} \mapsto [\mathbf{a}_1 \cdot \mathbf{x}, \ldots, \mathbf{a}_{64} \cdot \mathbf{x}]$

Original "file" $\mathbf{p}$, transmission error $\mathbf{e}$ so corrupted file is $\mathbf{p} + \mathbf{e}$.

What is probability that corrupted file has the same checksum as original?

If error is chosen according to uniform distribution,

$$\begin{aligned} &\text{Probability}\,(\mathbf{p} + \mathbf{e} \text{ has same checksum as } \mathbf{p}) \\ &= \text{Probability}\,(\mathbf{e} \text{ is a solution to homogeneous linear system}) \\ &= \frac{\text{number of solutions to homogeneous linear system}}{\text{number of } n\text{-vectors}} \\ &= \frac{\text{number of solutions to homogeneous linear system}}{2^n} \end{aligned}$$

raising Question

$\boxed{\text{How to find number of solutions to a homogeneous linear system over } GF(2)\text{?}}$

Cardinality of a vector space over $GF(2)$

How to find number of solutions to a homogeneous linear system over $GF(2)$?

Solution set of a homogeneous linear system is a vector space.
Question becomes

How to find out cardinality of a vector space $\mathcal{V}$ over $GF(2)$?

- Suppose basis for $\mathcal{V}$ is $\mathbf{b}_1, \ldots, \mathbf{b}_n$.
- Then $\mathcal{V}$ is set of linear combinations
$$\beta_1\,\mathbf{b}_1 + \cdots + \beta_n\,\mathbf{b}_n$$
- Number of linear combinations is 2^n.
- By Unique-Representation Lemma, every linear combination gives a different vector of $\mathcal{V}$.
- Thus cardinality is $2^{\dim \mathcal{V}}$.

Cardinality of a vector space over $GF(2)$

Cardinality of a vector space $\mathcal{V}$ over $GF(2)$ is $2^{\dim \mathcal{V}}$.

$\boxed{\text{How to find dimension of solution set of a homogeneous linear system?}}$

Write linear system as $A\mathbf{x} = \mathbf{0}$.

$\boxed{\text{How to find dimension of the null space of } A\text{?}}$

Answers will come later.

Subset-Basis Lemma

Lemma: Every finite set T of vectors contains a subset S that is a basis for Span T.

Proof: The Grow algorithm finds a basis for $\mathcal{V}$ if it terminates.

> Initialize $S = \emptyset$.
> Repeat while possible: select a vector $\mathbf{v}$ in $\mathcal{V}$ that is not in Span S, and put it in S.

Revised version:

> Initialize $S = \emptyset$
> Repeat while possible: select a vector $\mathbf{v}$ in T that is not in Span S, and put it in S.

Differs from original:

- This algorithm stops when Span S contains every vector in T.
- The original Grow algorithm stops only once Span S contains every vector in $\mathcal{V}$.

However, that's okay: when Span S contains all the vectors in T, Span S also contains all linear combinations of vectors in T, so at this point Span $S = \mathcal{V}$.
Shows that original Grow algorithm can be guided to make same choices as this algorithm, so result is a basis. QED

Termination of Grow algorithm

def $\textsc{Grow}(\mathcal{V})$
  $B = \emptyset$
  repeat while possible:
    find a vector $\mathbf{v}$ in $\mathcal{V}$ that is not in Span B, and put it in S.

Grow-Algorithm-Termination Lemma: If $\mathcal{V}$ is a subspace of $\mathbb{F}^D$ where D is finite then $\textsc{Grow}(\mathcal{V})$ terminates.
Proof: By Grow-Algorithm Corollary, B is linearly independent throughout.

Apply the Morphing Lemma with $S = \{\text{standard generators for } \mathbb{F}^D\} \Rightarrow$
$|B| \leq |S| = |D|$.

Since B grows in each iteration, there are at most $|D|$ iterations. QED

Every subspace of $\mathbb{F}^D$ contains a basis

Grow-Algorithm-Termination Lemma: If $\mathcal{V}$ is a subspace of $\mathbb{F}^D$ where D is finite then $\textsc{Grow}(\mathcal{V})$ terminates.
Theorem: For finite D, every subspace of $\mathbb{F}^D$ contains a basis.
Proof: Let $\mathcal{V}$ be a subspace of $\mathbb{F}^D$.

```
def GROW(V)
  B = ∅
  repeat while possible:
        find a vector v in V that is not in Span B, and put it in B.
```

Grow-Algorithm-Termination Lemma ensures algorithm terminates.
Upon termination, every vector in $\mathcal{V}$ is in Span B, so B is a set of generators for $\mathcal{V}$. By Grow-Algorithm Corollary, B is linearly independent. Therefore B is a basis for $\mathcal{V}$.
QED

Superset-Basis Lemma

Grow-Algorithm-Termination Lemma: If $\mathcal{V}$ is a subspace of $\mathbb{F}^D$ where D is finite then $\textsc{Grow}(\mathcal{V})$ terminates.

Superset-Basis Lemma: Let $\mathcal{V}$ be a vector space consisting of D-vectors where D is finite. Let C be a linearly independent set of vectors belonging to $\mathcal{V}$. Then $\mathcal{V}$ has a basis B containing all vectors in C.

Proof: Use version of Grow algorithm:

> Initialize B to the empty set.
> Repeat while possible: select a vector $\mathbf{v}$ in $\mathcal{V}$ (preferably in C) that is not in Span B, and put it in B.

At first, B will consist of vectors in C until B contains all of C. Then more vectors will be added to B until Span $B = \mathcal{V}$ By Grow-Algorithm Corollary, B is linearly independent throughout. Therefore, once algorithm terminates, B contains C and is a basis for $\mathcal{U}$.

Termination is implied by Grow Algorithm Termination Lemma. QED

Estimating dimension

$T = \{[-0.6, -2.1, -3.5, -2.2], [-1.3, 1.5, -0.9, -0.5], [4.9, -3.7, 0.5, -0.3],$
$[2.6, -3.5, -1.2, -2.0], [-1.5, -2.5, -3.5, 0.94]\}.$
What is the rank of T?

By Subset-Basis Lemma, T contains a basis.

Therefore $\dim \text{Span } T \leq |T|$.

Therefore rank $T \leq |T|$.

Proposition: A set T of vectors has rank $\leq |T|$.

Dimension Lemma

Dimension Lemma: If $\mathcal{U}$ is a subspace of $\mathcal{W}$ then

- **D1:** $\dim \mathcal{U} \leq \dim \mathcal{W}$, and
- **D2:** if $\dim \mathcal{U} = \dim \mathcal{W}$ then $\mathcal{U} = \mathcal{W}$

Proof: Let $\mathbf{u}_1, \ldots, \mathbf{u}_k$ be a basis for $\mathcal{U}$.
By Superset-Basis Lemma, there is a basis B for $\mathcal{W}$ that contains $\mathbf{u}_1, \ldots, \mathbf{u}_k$.

- $B = \{\mathbf{u}_1, \ldots, \mathbf{u}_k, \mathbf{b}_1, \ldots, \mathbf{b}_r\}$
- Thus $k \leq |B|$, and
- If $k = |B|$ then $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\} = B$ QED

Example: Suppose $\mathcal{V} = \text{Span } \{[1,2],[2,1]\}$.
Clearly $\mathcal{V}$ is a subspace of $\mathbb{R}^2$.
However, the set $\{[1,2],[2,1]\}$ is linearly independent, so $\dim \mathcal{V} = 2$.
Since $\dim \mathbb{R}^2 = 2$, D2 shows that $\mathcal{V} = \mathbb{R}^2$.
Example: $S = \{[-0.6, -2.1, -3.5, -2.2], [-1.3, 1.5, -0.9, -0.5], [4.9, -3.7, 0.5, -0.3],$
$[2.6, -3.5, -1.2, -2.0], [-1.5, -2.5, -3.5, 0.94]\}$
Since every vector in S is a 4-vector, Span S is a subspace of $\mathbb{R}^4$.
Since $\dim \mathbb{R}^4 = 4$, D1 shows $\dim \text{Span } S \leq 4$.

Proposition: Any set of D-vectors has rank at most $|D|$.

Rank Theorem

Rank Theorem: For every matrix M, row rank equals column rank.

Lemma: For any matrix A, row rank of $A \leq$ column rank of A
To show theorem:

- Apply lemma to $M \Rightarrow$ row rank of $M \leq$ column rank of M
- Apply lemma to $M^T \Rightarrow$ row rank of $M^T \leq$ column rank of $M^T \Rightarrow$ column rank of $M \leq$ row rank of M

Combine $\Rightarrow$ row rank of $M =$ column rank of M

Proof of lemma: For any matrix A, row rank of $A \leq$ column rank of A

$$\left[\begin{array}{c} \\ \\ \text{A} \\ \\ \\ \end{array} \right]$$

Think of A as columns $\mathbf{a}_1, \ldots, \mathbf{a}_n$.
Let $\mathbf{b}_1, \ldots, \mathbf{b}_r$ be basis for column space (so column rank $= r$).

Write each column of A in terms of basis: $\left[\begin{array}{c} \\ \mathbf{a}_j \\ \\ \end{array} \right] = \left[\begin{array}{c|c|c} & & \\ \mathbf{b}_1 & \cdots & \mathbf{b}_r \\ & & \end{array} \right] \left[\begin{array}{c} \\ \mathbf{u}_j \\ \\ \end{array} \right]$

Use matrix-vector definition of matrix-matrix multiplication to rewrite as matrix-matrix equation $A = BU$.
B has r columns and U has r rows.
Write A and B in terms of rows: row i of A equals row i of B times U.
Write U in terms of rows: row i of A is a linear combination of rows of U.
Each row of A is in span of the r rows of U. **Thus row rank of A is at most r.**

Proof of lemma: For any matrix A, row rank of $A \leq$ column rank of A

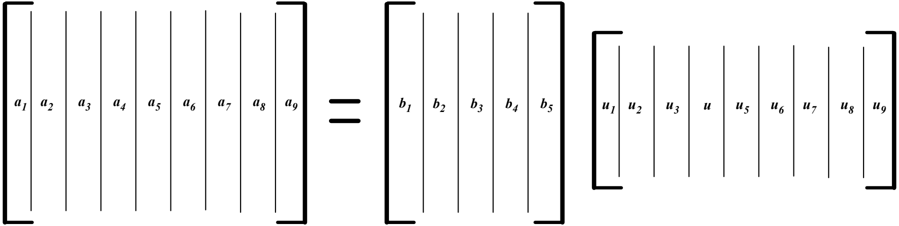
$$\left[\begin{array}{c|c|c|c|c|c|c|c|c} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 \end{array}\right]$$

Think of A as columns $\mathbf{a}_1, \ldots, \mathbf{a}_n$.
Let $\mathbf{b}_1, \ldots, \mathbf{b}_r$ be basis for column space (so column rank $= r$).

Write each column of A in terms of basis: $\left[\begin{array}{c} \mathbf{a}_j \end{array}\right] = \left[\begin{array}{c|c|c} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{array}\right] \left[\begin{array}{c} \mathbf{u}_j \end{array}\right]$

Use matrix-vector definition of matrix-matrix multiplication to rewrite as matrix-matrix equation $A = BU$.
B has r columns and U has r rows.
Write A and B in terms of rows: row i of A equals row i of B times U.
Write U in terms of rows: row i of A is a linear combination of rows of U.
Each row of A is in span of the r rows of U. **Thus row rank of A is at most r.**

Proof of lemma: For any matrix A, row rank of $A \leq$ column rank of A



Think of A as columns $\mathbf{a}_1, \ldots, \mathbf{a}_n$.
Let $\mathbf{b}_1, \ldots, \mathbf{b}_r$ be basis for column space (so column rank $= r$).

Write each column of A in terms of basis: $\left[\begin{array}{c} \mathbf{a}_j \end{array}\right] = \left[\begin{array}{c|c|c} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{array}\right] \left[\begin{array}{c} \mathbf{u}_j \end{array}\right]$

Use matrix-vector definition of matrix-matrix multiplication to rewrite as matrix-matrix equation $A = BU$.
B has r columns and U has r rows.
Write A and B in terms of rows: row i of A equals row i of B times U.
Write U in terms of rows: row i of A is a linear combination of rows of U.
Each row of A is in span of the r rows of U. **Thus row rank of A is at most r.**

Proof of lemma: For any matrix A, row rank of $A \leq$ column rank of A

$$\left[\begin{array}{c|c|c|c|c|c|c|c|c} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 \end{array}\right] = \left[\begin{array}{c|c|c|c|c} b_1 & b_2 & b_3 & b_4 & b_5 \end{array}\right] \left[\begin{array}{ccc} & \mathrm{U} & \end{array}\right]$$

Think of A as columns $\mathbf{a}_1, \ldots, \mathbf{a}_n$.

Let $\mathbf{b}_1, \ldots, \mathbf{b}_r$ be basis for column space (so column rank $= r$).

Write each column of A in terms of basis: $\left[\begin{array}{c} \mathbf{a}_j \end{array}\right] = \left[\begin{array}{c|c|c} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{array}\right] \left[\begin{array}{c} \mathbf{u}_j \end{array}\right]$

Use matrix-vector definition of matrix-matrix multiplication to rewrite as matrix-matrix equation $A = BU$.

B has r columns and U has r rows.

Write A and B in terms of rows: row i of A equals row i of B times U.

Write U in terms of rows: row i of A is a linear combination of rows of U.

Each row of A is in span of the r rows of U. **Thus row rank of A is at most r.**

Proof of lemma: For any matrix A, row rank of $A \leq$ column rank of A

$$\left[\quad A \quad\right] = \left[\quad B \quad\right]\left[\quad U \quad\right]$$

Think of A as columns $\mathbf{a}_1, \ldots, \mathbf{a}_n$.
Let $\mathbf{b}_1, \ldots, \mathbf{b}_r$ be basis for column space (so column rank $= r$).

Write each column of A in terms of basis: $\left[\begin{array}{c} \mathbf{a}_j \end{array}\right] = \left[\begin{array}{c|c|c} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{array}\right]\left[\begin{array}{c} \mathbf{u}_j \end{array}\right]$

Use matrix-vector definition of matrix-matrix multiplication to rewrite as matrix-matrix equation $A = BU$.
B has r columns and U has r rows.
Write A and B in terms of rows: row i of A equals row i of B times U.
Write U in terms of rows: row i of A is a linear combination of rows of U.
Each row of A is in span of the r rows of U. **Thus row rank of A is at most r.**

Proof of lemma: For any matrix A, row rank of $A \leq$ column rank of A

$$\left[\begin{array}{c} \bar{a}_1 \\ \hline \bar{a}_1 \\ \hline \bar{a}_1 \\ \hline \bar{a}_1 \\ \hline \bar{a}_1 \\ \hline \bar{a}_1 \\ \hline \bar{a}_1 \end{array}\right] = \left[\begin{array}{c} \bar{b}_1 \\ \hline \bar{b}_1 \\ \hline \bar{b}_1 \\ \hline \bar{b}_1 \\ \hline \bar{b}_1 \\ \hline \bar{b}_1 \\ \hline \bar{b}_1 \end{array}\right] \left[\begin{array}{c} \quad \mathrm{U} \quad \end{array}\right]$$

Think of A as columns $\mathbf{a}_1, \ldots, \mathbf{a}_n$.

Let $\mathbf{b}_1, \ldots, \mathbf{b}_r$ be basis for column space (so column rank $= r$).

Write each column of A in terms of basis: $\left[\begin{array}{c} \mathbf{a}_j \end{array}\right] = \left[\begin{array}{c|c|c} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{array}\right] \left[\begin{array}{c} \mathbf{u}_j \end{array}\right]$

Use matrix-vector definition of matrix-matrix multiplication to rewrite as matrix-matrix equation $A = BU$.

B has r columns and U has r rows.

Write A and B in terms of rows: row i of A equals row i of B times U.

Write U in terms of rows: row i of A is a linear combination of rows of U.

Each row of A is in span of the r rows of U. **Thus row rank of A is at most r.**

Proof of lemma: For any matrix A, row rank of $A \leq$ column rank of A

$$\begin{bmatrix} \bar{a}_1 \\ \hline \bar{a}_2 \\ \hline \bar{a}_3 \\ \hline \bar{a}_4 \\ \hline \bar{a}_5 \\ \hline \bar{a}_6 \\ \hline \bar{a}_7 \end{bmatrix} = \begin{bmatrix} \bar{b}_1 \\ \hline \bar{b}_2 \\ \hline \bar{b}_3 \\ \hline \bar{b}_4 \\ \hline \bar{b}_5 \\ \hline \bar{b}_6 \\ \hline \bar{b}_7 \end{bmatrix} \begin{bmatrix} \bar{u}_1 \\ \hline \bar{u}_2 \\ \hline \bar{u}_3 \\ \hline \bar{u}_4 \\ \hline \bar{u}_5 \end{bmatrix}$$

Think of A as columns $\mathbf{a}_1, \ldots, \mathbf{a}_n$.
Let $\mathbf{b}_1, \ldots, \mathbf{b}_r$ be basis for column space (so column rank $= r$).

Write each column of A in terms of basis: $\left[\ \mathbf{a}_j\ \right] = \left[\ \mathbf{b}_1 \ \middle|\ \cdots \ \middle|\ \mathbf{b}_r\ \right] \left[\ \mathbf{u}_j\ \right]$

Use matrix-vector definition of matrix-matrix multiplication to rewrite as matrix-matrix equation $A = BU$.
B has r columns and U has r rows.
Write A and B in terms of rows: row i of A equals row i of B times U.
Write U in terms of rows: row i of A is a linear combination of rows of U.
Each row of A is in span of the r rows of U. **Thus row rank of A is at most r.**

Simple authentication revisited

- Password is an n-vector $\hat{\mathbf{x}}$ over $GF(2)$
- **Challenge:** Computer sends random n-vector $\mathbf{a}$
- **Response:** Human sends back $\mathbf{a} \cdot \hat{\mathbf{x}}$.

Repeated until Computer is convinced that Human knows password $\hat{\mathbf{x}}$.

Eve eavesdrops on communication, learns m pairs

$$\begin{array}{c} \mathbf{a}_1, b_1 \\ \vdots \\ \mathbf{a}_m, b_m \end{array}$$

such that b_i is right response to challenge $\mathbf{a}_i$

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

Suppose $\mathbf{a} = \alpha_1 \mathbf{a}_1 + \cdots + \alpha_m \mathbf{a}_m$
Then right response is $\alpha_1 b_1 + \cdots + \alpha_m b_m$

Fact: Probably rank $[\mathbf{a}_1, \ldots, \mathbf{a}_m]$ is not much less than $\min\{m, n\}$.

Once $m > n$, probably Span $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ is all of $GF(2)^n$
so Eve can respond to any challenge.

Also: The password $\hat{\mathbf{x}}$ is a solution to

$$\underbrace{\begin{bmatrix} \mathbf{a}_1 \\ \hline \vdots \\ \hline \mathbf{a}_m \end{bmatrix}}_{A} \begin{bmatrix} \mathbf{x} \end{bmatrix} = \underbrace{\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}}_{\mathbf{b}}$$

Solution set of $A\mathbf{x} = \mathbf{b}$ is $\hat{\mathbf{x}} + \text{Null } A$

Once rank A reaches n, columns of A are linearly independent so Null A is trivial, so only solution is the password $\hat{\mathbf{x}}$, so Eve can compute the password using `solver`.

Direct Sum

Let $\mathcal{U}$ and $\mathcal{V}$ be two vector spaces consisting of D-vectors over a field $\mathbb{F}$.

Definition: If $\mathcal{U}$ and $\mathcal{V}$ share only the zero vector then we define the *direct sum* of $\mathcal{U}$ and $\mathcal{V}$ to be the set

$$\{\mathbf{u} + \mathbf{v} \ : \mathbf{u} \in \mathcal{U}, \mathbf{v} \in \mathcal{V}\}$$

written $\mathcal{U} \oplus \mathcal{V}$

That is, $\mathcal{U} \oplus \mathcal{V}$ is the set of all sums of a vector in $\mathcal{U}$ and a vector in $\mathcal{V}$.

In Python, `[u+v for u in U for v in V]`

(But generally $\mathcal{U}$ and $\mathcal{V}$ are infinite so the Python is just suggestive.)

Direct Sum: Example

Vectors over $GF(2)$:

Example: Let $\mathcal{U} = \text{Span } \{1000, 0100\}$ and let $\mathcal{V} = \text{Span } \{0010\}$.

- Every nonzero vector in $\mathcal{U}$ has a one in the first or second position (or both) and nowhere else.
- Every nonzero vector in $\mathcal{V}$ has a one in the third position and nowhere else.

Therefore the only vector in both $\mathcal{U}$ and $\mathcal{V}$ is the zero vector.

Therefore $\mathcal{U} \oplus \mathcal{V}$ is defined.

$\mathcal{U} \oplus \mathcal{V} = \{0000 + 0000, 1000 + 0000, 0100 + 0000, 1100 + 0000, 0000 + 0010, 1000 + 0010, 0100 + 0010, 1100 + 0010\}$

which is equal to $\{0000, 1000, 0100, 1100, 0010, 1010, 0110, 1110\}$.

Direct Sum: Example

Vectors over $\mathbb{R}$:

Example: Let $\mathcal{U} = \text{Span } \{[1,2,1,2],[3,0,0,4]\}$ and let $\mathcal{V}$ be the null space of $\begin{bmatrix} 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}$.

- The vector $[2,-2,-1,2]$ is in $\mathcal{U}$ because it is $[3,0,0,4]-[1,2,1,2]$
- It is also in $\mathcal{V}$ because

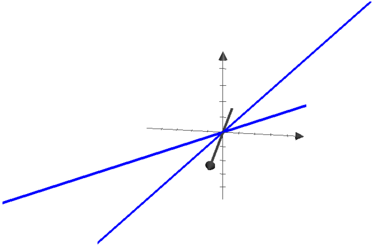
$$\begin{bmatrix} 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 2 \\ -2 \\ -1 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Therefore we cannot form $\mathcal{U} \oplus \mathcal{V}$.

Direct Sum: Example

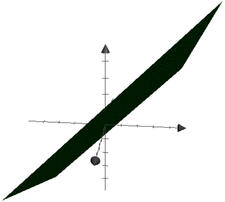
Vectors over $\mathbb{R}$:

Example:



- Let $\mathcal{U} = \text{Span } \{[4, -1, 1]\}$.
- Let $\mathcal{V} = \text{Span } \{[0, 1, 1]\}$.

The only intersection is at the origin, so $\mathcal{U} \oplus \mathcal{V}$ is defined.



- $\mathcal{U} \oplus \mathcal{V}$ is the set of vectors $\mathbf{u} + \mathbf{v}$ where $\mathbf{u} \in \mathcal{U}$ and $\mathbf{v} \in \mathcal{V}$.
- This is just $\text{Span } \{[4, -1, 1], [0, 1, 1]\}$
- Plane containing the two lines

Properties of direct sum

Lemma: $\mathcal{U} \oplus \mathcal{V}$ is a vector space.

(Prove using Properties V1, V2, V3.)

Lemma: The union of

- a set of generators of $\mathcal{U}$, and
- a set of generators of $\mathcal{V}$

is a set of generators for $\mathcal{U} \oplus \mathcal{V}$.

Proof: Suppose $\mathcal{U} = \text{Span } \{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ and $\mathcal{V} = \text{Span } \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$.
Then

- every vector in $\mathcal{U}$ can be written as $\alpha_1 \mathbf{u}_1 + \cdots + \alpha_m \mathbf{u}_m$, and
- every vector in $\mathcal{V}$ can be written as $\beta_1 \mathbf{v}_1 + \cdots + \beta_n \mathbf{v}_n$

so every vector in $\mathcal{U} \oplus \mathcal{V}$ can be written as

$$\alpha_1 \mathbf{u}_1 + \cdots + \alpha_m \mathbf{u}_m \; + \; \beta_1 \mathbf{v}_1 + \cdots + \beta_n \mathbf{v}_n$$

QED

Properties of direct sum

Direct Sum Basis Lemma:

Union of a basis of $\mathcal{U}$ and a basis of $\mathcal{V}$ is a basis of $\mathcal{U} \oplus \mathcal{V}$.

Proof: Clearly

- a basis of $\mathcal{U}$ is a set of generators for $\mathcal{U}$, and
- a basis of $\mathcal{V}$ is a set of generators for $\mathcal{V}$.

Therefore the previous lemma shows that

- the union of a basis for $\mathcal{U}$ and a basis for $\mathcal{V}$ is a generating set for $\mathcal{U} \oplus \mathcal{V}$.

We just need to show that the union is linearly independent.

Properties of direct sum

Direct Sum Basis Lemma:

Union of a basis of $\mathcal{U}$ and a basis of $\mathcal{V}$ is a basis of $\mathcal{U} \oplus \mathcal{V}$.

Proof, cont'd: Let $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ be a basis for $\mathcal{U}$. Let $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis for $\mathcal{V}$.
We need to show that $\{\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is independent.
Suppose

$$\mathbf{0} = \alpha_1 \ \mathbf{u}_1 + \cdots + \alpha_m \mathbf{u}_m + \beta_1 \ \mathbf{v}_1 + \cdots + \beta_n \ \mathbf{v}_n.$$

Then

$$\underbrace{\alpha_1 \ \mathbf{u}_1 + \cdots + \alpha_m \ \mathbf{u}_m}_{\text{in } \mathcal{U}} = \underbrace{(-\beta_1) \ \mathbf{v}_1 + \cdots + (-\beta_n) \ \mathbf{v}_n}_{\text{in } \mathcal{V}}$$

Left-hand side is a vector in $\mathcal{U}$, and right-hand side is a vector in $\mathcal{V}$.

By definition of $\mathcal{U} \oplus \mathcal{V}$, the only vector in both $\mathcal{U}$ and $\mathcal{V}$ is the zero vector.

This shows:

$$\mathbf{0} = \alpha_1 \ \mathbf{u}_1 + \cdots + \alpha_m \ \mathbf{u}_m$$

and

$$\mathbf{0} = (-\beta_1) \ \mathbf{v}_1 + \cdots + (-\beta_n) \ \mathbf{v}_n$$

By linear independence, the linear combinations must be trivial. QED

Direct Sum

Direct Sum Basis Lemma:

Union of a basis of $\mathcal{U}$ and a basis of $\mathcal{V}$ is a basis of $\mathcal{U} \oplus \mathcal{V}$.

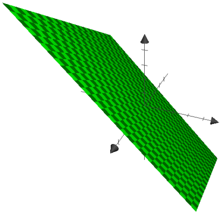
Direct Sum Dimension Corollary: $\dim \mathcal{U} + \dim \mathcal{V} = \dim \mathcal{U} \oplus \mathcal{V}$

Proof: A basis for $\mathcal{U}$ together with a basis for $\mathcal{V}$ forms a basis for $\mathcal{U} \oplus \mathcal{V}$. QED

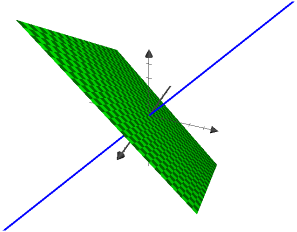
Complementary subspace

If $\mathcal{U} \oplus \mathcal{V} = \mathcal{W}$, we say $\mathcal{U}$ and $\mathcal{V}$ are *complementary* subspaces of $\mathcal{W}$.

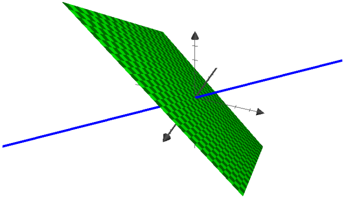
Example: Suppose $\mathcal{U}$ is a plane in $\mathbb{R}^3$.



Then any line through the origin that does not lie in $\mathcal{U}$ is complementary subspace with respect to $\mathbb{R}^3$



Example illustrates that, for a given subspace $\mathcal{U}$ of $\mathcal{W}$, there can be many different subspaces $\mathcal{V}$ such that $\mathcal{U}$ and $\mathcal{V}$ are complementary.



Complementary subspace

Proposition: For any finite-dimensional vector space $\mathcal{W}$ and any subspace $\mathcal{U}$, there is a subspace $\mathcal{V}$ such that $\mathcal{U}$ and $\mathcal{V}$ are complementary.

Proof: Let $\mathbf{u}_1, \ldots, \mathbf{u}_k$ be a basis for $\mathcal{U}$. By Superset-Basis Lemma, there is a basis for $\mathcal{W}$ that includes $\mathbf{u}_1, \ldots, \mathbf{u}_k$:

$$B = \{\mathbf{u}_1, \ldots, \mathbf{u}_k, \mathbf{v}_1, \ldots, \mathbf{v}_r\}$$

Let $\mathcal{V} = \text{Span } \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$.

Any vector in $\mathcal{W}$ can be written in terms of its basis:

$$\mathbf{w} = \underbrace{\alpha_1\,\mathbf{u}_1 + \cdots + \alpha_k\,\mathbf{u}_k}_{\text{in } \mathcal{U}} + \underbrace{\beta_1\,\mathbf{v}_1 + \cdots + \beta_r\,\mathbf{v}_r}_{\text{in } \mathcal{V}}$$

If some vector $\mathbf{v}$ is in Span $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ and in Span $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$
then $\mathbf{v} = \alpha_1\,\mathbf{u}_1 + \cdots + \alpha_k\,\mathbf{u}_k$ and $\mathbf{v} = \beta_1\,\mathbf{v}_1 + \cdots + \beta_r\,\mathbf{v}_r$
so

$$\alpha_1\,\mathbf{u}_1 + \cdots + \alpha_k\,\mathbf{u}_k = \beta_1\,\mathbf{v}_1 + \cdots + \beta_r\,\mathbf{v}_r$$

$$\mathbf{0} = \alpha_1\,\mathbf{u}_1 + \cdots + \alpha_k\,\mathbf{u}_k - \beta_1\,\mathbf{v}_1 - \cdots - \beta_r\,\mathbf{v}_r$$

so $\alpha_1 = \cdots = \alpha_k = \beta_1 = \cdots = \beta_r = 0$ so $\mathbf{v} = \mathbf{0}$. QED

Linear function invertibility

How to tell if a linear function $f : \mathcal{V} \longrightarrow \mathcal{W}$ is invertible?

- *One-to-one?* f is one-to-one if its kernel is trivial. *Equivalent:* if its kernel has dimension zero.
- *Onto?* f is onto if its image equals its co-domain

Recall that the image of a function f with domain $\mathcal{V}$ is $\{f(\mathbf{v}) \ : \mathbf{v} \in \mathcal{V}\}$.

Lemma: The image of f is a subspace of $\mathcal{W}$.

How can we tell if the image of f equals $\mathcal{W}$?

Dimension Lemma: If $\mathcal{U}$ is a subspace of $\mathcal{W}$ then

Property D1: $\dim \mathcal{U} \leq \dim \mathcal{W}$, and

Property D2: if $\dim \mathcal{U} = \dim \mathcal{W}$ then $\mathcal{U} = \mathcal{W}$

Use Property D2 with $\mathcal{U} = \text{Im } f$.
Shows that the function f is onto iff $\dim \text{Im } f = \dim \mathcal{W}$

We conclude:

$$\boxed{f \text{ is invertible } \dim \text{Ker } f = 0 \text{ and } \dim \text{Im } f = \dim \mathcal{W}}$$

Linear function invertibility

$$\boxed{f \text{ is one-to-one if } \dim \operatorname{Ker} f = 0 \text{ and } \dim \operatorname{Im} f = \dim \mathcal{W}}$$

How does this relate to dimension of the domain?

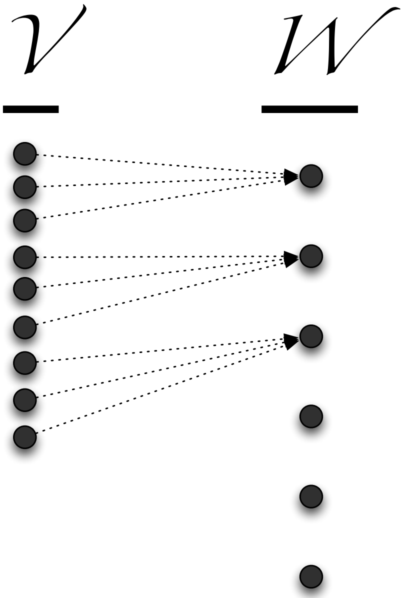
Conjecture: For f to be invertible, need $\dim \mathcal{V} = \dim \mathcal{W}$.

Extracting an invertible function

Starting with a linear function f we will extract a largest possible subfunction that is invertible.

Make it onto by setting co-domain to be image of f.

Make it one-to-one by getting rid of extra domain elements sharing same image.

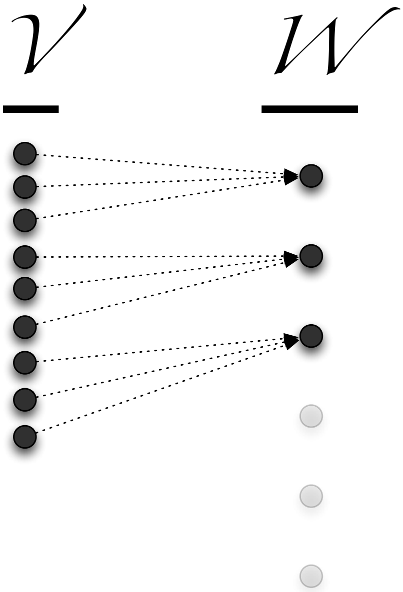


Extracting an invertible function

Starting with a linear function f we will extract a largest possible subfunction that is invertible.

Make it onto by setting co-domain to be image of f.

Make it one-to-one by getting rid of extra domain elements sharing same image.



Extracting an invertible function

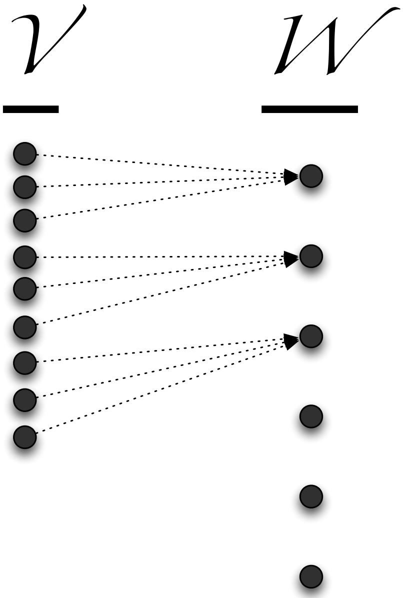
Start with linear function $f : \mathcal{V} \longrightarrow \mathcal{W}$

Step 1: Choose smaller co-domain $\mathcal{W}^*$

Step 2: Choose smaller domain $\mathcal{V}^*$

Step 3: Define function $f^* : \mathcal{V}^* \longrightarrow \mathcal{W}^*$ by $f^*(\mathbf{x}) = f(\mathbf{x})$

In fact, we will end up selecting a *basis* of $\mathcal{W}^*$ and a basis of $\mathcal{V}^*$.



Extracting an invertible function

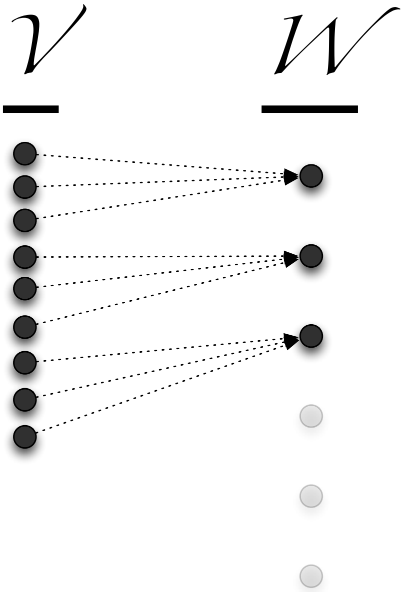
Start with linear function $f : \mathcal{V} \longrightarrow \mathcal{W}$

Step 1: Choose smaller co-domain $\mathcal{W}^*$

Step 2: Choose smaller domain $\mathcal{V}^*$

Step 3: Define function $f^* : \mathcal{V}^* \longrightarrow \mathcal{W}^*$ by $f^*(\mathbf{x}) = f(\mathbf{x})$

In fact, we will end up selecting a *basis* of $\mathcal{W}^*$ and a basis of $\mathcal{V}^*$.



Extracting an invertible function

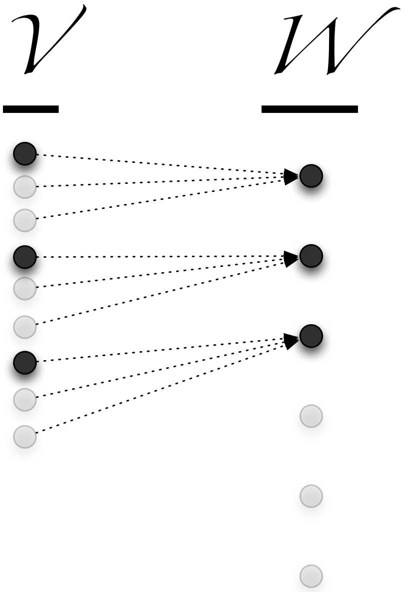
Start with linear function $f : \mathcal{V} \longrightarrow \mathcal{W}$

Step 1: Choose smaller co-domain $\mathcal{W}^*$

Step 2: Choose smaller domain $\mathcal{V}^*$

Step 3: Define function $f^* : \mathcal{V}^* \longrightarrow \mathcal{W}^*$ by $f^*(\mathbf{x}) = f(\mathbf{x})$

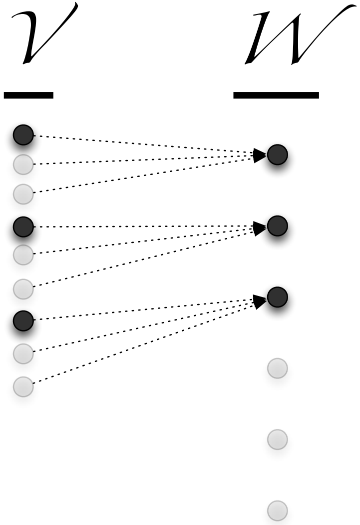
In fact, we will end up selecting a *basis* of $\mathcal{W}^*$ and a basis of $\mathcal{V}^*$.



Extracting an invertible function from linear function $f : \mathcal{V} \longrightarrow \mathcal{W}$

- Choose smaller co-domain $\mathcal{W}^*$
  Let $\mathcal{W}^*$ be image of f

  Let $\mathbf{w}_1, \ldots, \mathbf{w}_r$ be a basis of $\mathcal{W}^*$
- Choose smaller domain $\mathcal{V}^*$
  Let $\mathbf{v}_1, \ldots, \mathbf{v}_r$ be pre-images of $\mathbf{w}_1, \ldots, \mathbf{w}_r$
  That is, $f(\mathbf{v}_1) = \mathbf{w}_1, \ldots, f(\mathbf{v}_r) = \mathbf{w}_r$
  Let $\mathcal{V}^* = \text{Span }\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$
- Define function $f^* : \mathcal{V}^* \longrightarrow \mathcal{W}^*$ by $f^*(\mathbf{x}) = f(\mathbf{x})$



We will show:

- f^* is onto
- f^* is one-to-one (kernel is trivial)
- Bonus: $\mathbf{v}_1, \ldots, \mathbf{v}_r$ form a basis for $\mathcal{V}^*$

Extracting an invertible function from linear function $f : \mathcal{V} \longrightarrow \mathcal{W}$

- Choose smaller co-domain $\mathcal{W}^*$
  Let $\mathcal{W}^*$ be image of f

  Let $\mathbf{w}_1, \ldots, \mathbf{w}_r$ be a basis of $\mathcal{W}^*$
- Choose smaller domain $\mathcal{V}^*$
  Let $\mathbf{v}_1, \ldots, \mathbf{v}_r$ be pre-images of $\mathbf{w}_1, \ldots, \mathbf{w}_r$
  That is, $f(\mathbf{v}_1) = \mathbf{w}_1, \ldots, f(\mathbf{v}_r) = \mathbf{w}_r$
  Let $\mathcal{V}^* = \text{Span } \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$
- Define function $f^* : \mathcal{V}^* \longrightarrow \mathcal{W}^*$
  by $f^*(\mathbf{x}) = f(\mathbf{x})$

We will show:

- f^* is onto
- f^* is one-to-one (kernel is trivial)
- Bonus: $\mathbf{v}_1, \ldots, \mathbf{v}_r$ form a basis for $\mathcal{V}^*$

Onto:

Let $\mathbf{w}$ be any vector in co-domain $\mathcal{W}^*$.
There are scalars $\alpha_1, \ldots, \alpha_r$ such that

$$\mathbf{w} = \alpha_1 \, \mathbf{w}_1 + \cdots + \alpha_r \, \mathbf{w}_r$$

Because f is linear,

$$\begin{aligned} f(\alpha_1 \, \mathbf{v}_1 + \cdots + \alpha_r \, \mathbf{v}_r) & \\ = \; & \alpha_1 \, f(\mathbf{v}_1) + \cdots + \alpha_r \, f(v_r) \\ = \; & \alpha_1 \, \mathbf{w}_1 + \cdots + \alpha_r \, \mathbf{w}_r \end{aligned}$$

so $\mathbf{w}$ is image of $\alpha_1 \, \mathbf{v}_1 + \cdots + \alpha_r \, \mathbf{v}_r \in \mathcal{V}^*$
QED

Extracting an invertible function from linear function $f : \mathcal{V} \longrightarrow \mathcal{W}$

- Choose smaller co-domain $\mathcal{W}^*$
  Let $\mathcal{W}^*$ be image of f

  Let $\mathbf{w}_1, \ldots, \mathbf{w}_r$ be a basis of $\mathcal{W}^*$
- Choose smaller domain $\mathcal{V}^*$
  Let $\mathbf{v}_1, \ldots, \mathbf{v}_r$ be pre-images of $\mathbf{w}_1, \ldots, \mathbf{w}_r$
  That is, $f(\mathbf{v}_1) = \mathbf{w}_1, \ldots, f(\mathbf{v}_r) = \mathbf{w}_r$
  Let $\mathcal{V}^* = \text{Span } \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$
- Define function $f^* : \mathcal{V}^* \longrightarrow \mathcal{W}^*$ by $f^*(\mathbf{x}) = f(\mathbf{x})$

We will show:

- f^* is onto
- f^* is one-to-one (kernel is trivial)
- Bonus: $\mathbf{v}_1, \ldots, \mathbf{v}_r$ form a basis for $\mathcal{V}^*$

One-to-one:
By One-to-One Lemma, need only show kernel is trivial.

Suppose $\mathbf{v}^*$ is in $\mathcal{V}^*$ and $f(\mathbf{v}^*) = \mathbf{0}$

Because $\mathcal{V}^* = \text{Span } \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$, there are scalars $\alpha_1, \ldots, \alpha_r$ such that

$$\mathbf{v}^* = \alpha_1 \mathbf{v}_1 + \cdots + \alpha_r \mathbf{v}_r$$

Applying f to both sides,

$$\begin{aligned} \mathbf{0} &= f(\alpha_1 \mathbf{v}_1 + \cdots + \alpha_r \mathbf{v}_r) \\ &= \alpha_1 \mathbf{w}_1 + \cdots + \alpha_r \mathbf{w}_r \end{aligned}$$

Because $\mathbf{w}_1, \ldots, \mathbf{w}_r$ are linearly independent, $\alpha_1 = \cdots = \alpha_r = 0$

so $\mathbf{v}^* = \mathbf{0}$ QED

Extracting an invertible function from linear function $f : \mathcal{V} \longrightarrow \mathcal{W}$

- Choose smaller co-domain $\mathcal{W}^*$
  Let $\mathcal{W}^*$ be image of f

  Let $\mathbf{w}_1, \ldots, \mathbf{w}_r$ be a basis of $\mathcal{W}^*$
- Choose smaller domain $\mathcal{V}^*$
  Let $\mathbf{v}_1, \ldots, \mathbf{v}_r$ be pre-images of $\mathbf{w}_1, \ldots, \mathbf{w}_r$
  That is, $f(\mathbf{v}_1) = \mathbf{w}_1, \ldots, f(\mathbf{v}_r) = \mathbf{w}_r$
  Let $\mathcal{V}^* = \text{Span } \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$
- Define function $f^* : \mathcal{V}^* \longrightarrow \mathcal{W}^*$ by $f^*(\mathbf{x}) = f(\mathbf{x})$

We will show:

- f^* is onto
- f^* is one-to-one (kernel is trivial)
- Bonus: $\mathbf{v}_1, \ldots, \mathbf{v}_r$ form a basis for $\mathcal{V}^*$

Bonus: $\mathbf{v}_1, \ldots, \mathbf{v}_r$ form a basis for $\mathcal{V}^*$

Need only show linear independence
Suppose $\mathbf{0} = \alpha_1 \mathbf{v}_1 + \cdots + \alpha_r \mathbf{v}_r$

Applying f to both sides,

$$\begin{aligned} \mathbf{0} &= f(\alpha_1 \mathbf{v}_1 + \cdots + \alpha_r \mathbf{v}_r) \\ &= \alpha_1 \mathbf{w}_1 + \cdots + \alpha_r \mathbf{w}_r \end{aligned}$$

Because $\mathbf{w}_1, \ldots, \mathbf{w}_r$ are linearly independent, $\alpha_1 = \cdots = \alpha_r = 0$. QED

Extracting an invertible function from linear function $f : \mathcal{V} \longrightarrow \mathcal{W}$

- Choose smaller co-domain $\mathcal{W}^*$
  Let $\mathcal{W}^*$ be image of f

  Let $\mathbf{w}_1, \ldots, \mathbf{w}_r$ be a basis of $\mathcal{W}^*$
- Choose smaller domain $\mathcal{V}^*$
  Let $\mathbf{v}_1, \ldots, \mathbf{v}_r$ be pre-images of $\mathbf{w}_1, \ldots, \mathbf{w}_r$
  That is, $f(\mathbf{v}_1) = \mathbf{w}_1, \ldots, f(\mathbf{v}_r) = \mathbf{w}_r$
  Let $\mathcal{V}^* = \text{Span } \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$
- Define function $f^* : \mathcal{V}^* \longrightarrow \mathcal{W}^*$ by $f^*(\mathbf{x}) = f(\mathbf{x})$

We will show:

- f^* is onto
- f^* is one-to-one (kernel is trivial)
- Bonus: $\mathbf{v}_1, \ldots, \mathbf{v}_r$ form a basis for $\mathcal{V}^*$

Example:

Let $A = \left[\begin{array}{c|c|c} 1 & 2 & 1 \\ 2 & 1 & 1 \\ 1 & 2 & 1 \end{array}\right]$, and define $\mathbf{f} : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ by $f(\mathbf{x}) = A\mathbf{x}$.

Define $\mathcal{W}^* = \text{Im } f = \text{Col } A = \text{Span } \{[1, 2, 1], [2, 1, 2], [1, 1, 1]\}$.

One basis for $\mathcal{W}^*$ is $\mathbf{w}_1 = [0, 1, 0]$, $\mathbf{w}_2 = [1, 0, 1]$

Pre-images for $\mathbf{w}_1$ and $\mathbf{w}_2$:
$\mathbf{v}_1 = [\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}]$ and $\mathbf{v}_2 = [-\frac{1}{2}, \frac{1}{2}, \frac{1}{2}]$,
for then $A\mathbf{v}_1 = \mathbf{w}_1$ and $A\mathbf{v}_2 = \mathbf{w}_2$.

Let $\mathcal{V}^* = \text{Span } \{\mathbf{v}_1, \mathbf{v}_2\}$

Then $f^* : \mathcal{V}^* \longrightarrow \text{Im } f$ is onto and one-to-one.

Extracting an invertible function from linear function $f : \mathcal{V} \longrightarrow \mathcal{W}$

- Choose smaller co-domain $\mathcal{W}^*$
  Let $\mathcal{W}^*$ be image of f

  Let $\mathbf{w}_1, \ldots, \mathbf{w}_r$ be a basis of $\mathcal{W}^*$
- Choose smaller domain $\mathcal{V}^*$
  Let $\mathbf{v}_1, \ldots, \mathbf{v}_r$ be pre-images of $\mathbf{w}_1, \ldots, \mathbf{w}_r$
  That is, $f(\mathbf{v}_1) = \mathbf{w}_1, \ldots, f(\mathbf{v}_r) = \mathbf{w}_r$
  Let $\mathcal{V}^* = \text{Span } \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$
- Define function $f^* : \mathcal{V}^* \longrightarrow \mathcal{W}^*$
  by $f^*(\mathbf{x}) = f(\mathbf{x})$

We will show:

- f^* is onto
- f^* is one-to-one (kernel is trivial)
- Bonus: $\mathbf{v}_1, \ldots, \mathbf{v}_r$ form a basis for $\mathcal{V}^*$

To show about original function f:
original domain $\mathcal{V} = \text{Ker } f \oplus \mathcal{V}^*$
Must prove two things:

1. Ker f and $\mathcal{V}^*$ share only zero vector
2. every vector in $\mathcal{V}$ is the sum of a vector in Ker f and a vector in $\mathcal{V}^*$

We already showed kernel of f^* is trivial.
This shows only vector of Ker f in $\mathcal{V}^*$ is zero vector. —thing 1 is proved.

Let $\mathbf{v}$ be any vector in $\mathcal{V}$, and let $\mathbf{w} = f(\mathbf{v})$.
Since f^* is onto, its domain $\mathcal{V}^*$ contains a vector $\mathbf{v}^*$ such that $f(\mathbf{v}^*) = \mathbf{w}$
Therefore $f(\mathbf{v}) = f(\mathbf{v}^*)$ so
$f(\mathbf{v}) - f(\mathbf{v}^*) = \mathbf{0}$ so $f(\mathbf{v} - \mathbf{v}^*) = \mathbf{0}$
Thus $\mathbf{u} = \mathbf{v} - \mathbf{v}^*$ is in Ker f
and $\mathbf{v} = \mathbf{u} + \mathbf{v}^*$ —thing 2 is proved.

Extracting an invertible function from linear function $f : \mathcal{V} \longrightarrow \mathcal{W}$

- Choose smaller co-domain $\mathcal{W}^*$
  Let $\mathcal{W}^*$ be image of f

  Let $\mathbf{w}_1, \ldots, \mathbf{w}_r$ be a basis of $\mathcal{W}^*$
- Choose smaller domain $\mathcal{V}^*$
  Let $\mathbf{v}_1, \ldots, \mathbf{v}_r$ be pre-images of $\mathbf{w}_1, \ldots, \mathbf{w}_r$
  That is, $f(\mathbf{v}_1) = \mathbf{w}_1, \ldots, f(\mathbf{v}_r) = \mathbf{w}_r$
  Let $\mathcal{V}^* = \text{Span } \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$
- Define function $f^* : \mathcal{V}^* \longrightarrow \mathcal{W}^*$
  by $f^*(\mathbf{x}) = f(\mathbf{x})$

We will show:

- f^* is onto
- f^* is one-to-one (kernel is trivial)
- Bonus: $\mathbf{v}_1, \ldots, \mathbf{v}_r$ form a basis for $\mathcal{V}^*$

original domain $\mathcal{V}$ = Ker $f \oplus \mathcal{V}^*$

Example: Let $A = \left[\begin{array}{c|c|c} 1 & 2 & 1 \\ 2 & 1 & 1 \\ 1 & 2 & 1 \end{array}\right]$, and

define $\mathbf{f} : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ by $f(\mathbf{x}) = A\mathbf{x}$.

$\mathbf{v}_1 = [\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}]$ and $\mathbf{v}_2 = [-\frac{1}{2}, \frac{1}{2}, \frac{1}{2}]$

$\mathcal{V}^* = \text{Span } \{\mathbf{v}_1, \mathbf{v}_2\}$

Ker $f = \text{Span } \{[1, 1, -3]\}$

Therefore
$\mathcal{V} = (\text{Span } \{[1, 1, -3]\}) \oplus (\text{Span } \{\mathbf{v}_1, \mathbf{v}_2\})$

Extracting an invertible function from linear function $f : \mathcal{V} \longrightarrow \mathcal{W}$

- Choose smaller co-domain $\mathcal{W}^*$
  Let $\mathcal{W}^*$ be image of f

  Let $\mathbf{w}_1, \ldots, \mathbf{w}_r$ be a basis of $\mathcal{W}^*$

- Choose smaller domain $\mathcal{V}^*$
  Let $\mathbf{v}_1, \ldots, \mathbf{v}_r$ be pre-images of $\mathbf{w}_1, \ldots, \mathbf{w}_r$
  That is, $f(\mathbf{v}_1) = \mathbf{w}_1, \ldots, f(\mathbf{v}_r) = \mathbf{w}_r$
  Let $\mathcal{V}^* = \text{Span } \{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$

- Define function $f^* : \mathcal{V}^* \longrightarrow \mathcal{W}^*$
  by $f^*(\mathbf{x}) = f(\mathbf{x})$

We will show:

- f^* is onto
- f^* is one-to-one (kernel is trivial)
- Bonus: $\mathbf{v}_1, \ldots, \mathbf{v}_r$ form a basis for $\mathcal{V}^*$

original domain $\mathcal{V} = \textbf{Ker } f \oplus \mathcal{V}^*$

By Direct-Sum Dimension Corollary,

$$\dim \mathcal{V} = \dim \text{Ker } f + \dim \mathcal{V}^*$$

Since $\mathbf{v}_1, \ldots, \mathbf{v}_r$ form a basis for $\mathcal{V}^*$,

$$\dim \mathcal{V}^* = r = \dim \text{Im } f$$

We have proved...

Kernel-Image Theorem:
For any linear function $f : \mathcal{V} \rightarrow W$,

$$\dim \text{Ker } f + \dim \text{Im } f = \dim \mathcal{V}$$

Linear function invertibility, revisited

Kernel-Image Theorem:
For any linear function $f : \mathcal{V} \to W$,

$$\dim \text{Ker } f + \dim \text{Im } f = \dim \mathcal{V}$$

Linear-Function Invertibility Theorem: Let $f : \mathcal{V} \longrightarrow \mathcal{W}$ be a linear function. Then f is invertible iff $\dim \text{Ker } f = 0$ and $\dim \mathcal{V} = \dim \mathcal{W}$.

Proof: We saw before that f

- is one-to-one iff $\dim \text{Ker } f = 0$
- is onto if $\dim \text{Im } f = \dim \mathcal{W}$

Therefore f is invertible if $\dim \text{Ker } f = 0$ and $\dim \text{Im } f = \dim \mathcal{W}$.

Kernel-Image Theorem states $\dim \text{Ker } f + \dim \text{Im } f = \dim \mathcal{V}$

Therefore

$$\begin{gathered} \dim \text{Ker } f = 0 \text{ and } \dim \text{Im } f = \dim \mathcal{W} \\ \text{iff} \\ \dim \text{Ker } f = 0 \text{ and } \dim \mathcal{V} = \dim \mathcal{W} \end{gathered}$$

QED

Rank-Nullity Theorem

Kernel-Image Theorem:
For any linear function $f : \mathcal{V} \to W$,

$$\dim \text{Ker } f + \dim \text{Im } f = \dim \mathcal{V}$$

Apply Kernel-Image Theorem to the function $f(\mathbf{x}) = A\mathbf{x}$:

- $\text{Ker } f = \text{Null } A$
- $\dim \text{Im } f = \dim \text{Col } A = \text{rank } A$

Definition: The *nullity* of matrix A is $\dim \text{Null } A$

Rank-Nullity Theorem: For any n-column matrix A,

$$\text{nullity } A + \text{rank } A = n$$

Checksum problem revisited

Checksum function maps n-vectors over $GF(2)$ to 64-vectors over $GF(2)$:

$$\mathbf{x} \mapsto [\mathbf{a}_1 \cdot \mathbf{x}, \ldots, \mathbf{a}_{64} \cdot \mathbf{x}]$$

Original "file" $\mathbf{p}$, transmission error $\mathbf{e}$
so corrupted file is $\mathbf{p} + \mathbf{e}$.

If error is chosen according to uniform distribution,
Probability ($\mathbf{p} + \mathbf{e}$ has same checksum as $\mathbf{p}$)

$$= \frac{2^{\dim \mathcal{V}}}{2^n}$$

where $\mathcal{V}$ is the null space of the matrix

$$A = \begin{bmatrix} \mathbf{a}_1 \\ \hline \vdots \\ \hline \mathbf{a}_{64} \end{bmatrix}$$

Fact: Can easily choose $\mathbf{a}_1, \ldots, \mathbf{a}_{64}$ so that
rank $A = 64$

(Randomly chosen vectors will probably work.)

Rank-Nullity Theorem $\Rightarrow$

$$\begin{array}{ccccc} \text{rank } A & + & \text{nullity } A & = & n \\ 64 & + & \dim \mathcal{V} & = & n \\ & & \dim \mathcal{V} & = & n - 64 \end{array}$$

Therefore
Probability $= \frac{2^{n-64}}{2^n} = \frac{1}{2^{64}}$

very tiny chance that the change is undetected

Matrix invertibility

Rank-Nullity Theorem: For any n-column matrix A,

$$\text{nullity } A + \text{rank } A = n$$

Corollary: Let A be an $R \times C$ matrix. Then A is invertible if and only if $|R| = |C|$ and the columns of A are linearly independent.

Proof: Let $\mathbb{F}$ be the field. Define $f : \mathbb{F}^C \longrightarrow \mathbb{F}^R$ by $f(\mathbf{x}) = A\mathbf{x}$.
Then A is an invertible matrix if and only if f is an invertible function.

$$\begin{array}{lll} \text{The function } f \text{ is invertible} & \text{iff} & \dim \operatorname{Ker} f = 0 \text{ and } \dim \mathbb{F}^C = \dim \mathbb{F}^R \\ & \text{iff} & \text{nullity } A = 0 \text{ and } |C| = |R|. \end{array}$$

$$\begin{array}{lll} \text{nullity } A = 0 & \text{iff} & \dim \operatorname{Null} A = 0 \\ & \text{iff} & \operatorname{Null} A = \{\mathbf{0}\} \\ & \text{iff} & \text{the only vector } \mathbf{x} \text{ such that } A\mathbf{x} = \mathbf{0} \text{ is } \mathbf{x} = \mathbf{0} \\ & \text{iff} & \text{the columns of } A \text{ are linearly independent.} \end{array}$$

QED

Matrix invertibility examples

$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ is not square so cannot be invertible.

$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ is square and its columns are linearly independent so it is invertible.

$\left[\begin{array}{c|c|c} 1 & 1 & 2 \\ 2 & 1 & 3 \\ 3 & 1 & 4 \end{array}\right]$ is square but columns not linearly independent so it is not invertible.

Transpose of invertible matrix is invertible

Theorem: The transpose of an invertible matrix is invertible.

$$A = \left[\begin{array}{c|c|c} \mathbf{v}_1 & \cdots & \mathbf{v}_n \end{array}\right] = \left[\begin{array}{c} \mathbf{a}_1 \\ \hline \vdots \\ \hline \mathbf{a}_n \end{array}\right] \qquad A^T = \left[\begin{array}{c|c|c} \mathbf{a}_1 & \cdots & \mathbf{a}_n \end{array}\right]$$

Proof: Suppose A is invertible. Then A is square and its columns are linearly independent. Let n be the number of columns. Then rank $A = n$.

Because A is square, it has n rows. By Rank Theorem, rows are linearly independent.

Columns of transpose A^T are rows of A, so columns of A^T are linearly independent.

Since A^T is square and columns are linearly independent, A^T is invertible. QED

More matrix invertibility

Earlier we proved: *If A has an inverse A^{-1} then AA^{-1} is identity matrix*

Converse: If BA is identity matrix then A and B are inverses? **Not always true.**

Theorem: *Suppose A and B are square matrices such that BA is an identity matrix $\mathbb{1}$. Then A and B are inverses of each other.*

Proof: To show that A is invertible, need to show its columns are linearly independent.

Let $\mathbf{u}$ be any vector such that $A\mathbf{u} = \mathbf{0}$. Then $B(A\mathbf{u}) = B\mathbf{0} = \mathbf{0}$.
On the other hand, $(BA)\mathbf{u} = \mathbb{1}\mathbf{u} = \mathbf{u}$, so $\mathbf{u} = \mathbf{0}$.

This shows A has an inverse A^{-1}. Now must show $B = A^{-1}$.
We know AA^{-1} is an identity matrix.

$$
\begin{aligned}
BA &= \mathbb{1} && \\
(BA)A^{-1} &= \mathbb{1}A^{-1} && \text{by multiplying on the right by } B^{-1} \\
(BA)A^{-1} &= A^{-1} && \\
B(AA^{-1}) &= A^{-1} && \text{by associativity of matrix-matrix mult} \\
B\,\mathbb{1} &= A^{-1} && \\
B &= A^{-1} && \textit{QED}
\end{aligned}
$$

Representations of vector spaces

Two important ways to represent a vector space:

As the solution set of homogeneous linear system

$$\mathbf{a}_1 \cdot \mathbf{x} = 0, \ldots, \mathbf{a}_m \cdot \mathbf{x} = 0$$

Equivalently,

$$\text{Null} \begin{bmatrix} \mathbf{a}_1 \\ \hline \vdots \\ \hline \mathbf{a}_m \end{bmatrix}$$

As Span $\{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$

Equivalently,

$$\text{Row} \begin{bmatrix} \mathbf{b}_1 \\ \hline \vdots \\ \hline \mathbf{b}_k \end{bmatrix}$$

How to transform between these two representations?

From left to right: Given homogeneous linear system $\mathbf{a}_1 \cdot \mathbf{x} = 0, \ldots, \mathbf{a}_m \cdot \mathbf{x} = 0$, find generators $\mathbf{b}_1, \ldots, \mathbf{b}_k$ for solution set

From right to left:
Given generators $\mathbf{b}_1, \ldots, \mathbf{b}_k$,
find homogeneous linear system $\mathbf{a}_1 \cdot \mathbf{x} = 0, \ldots, \mathbf{a}_m \cdot \mathbf{x} = 0$ whose solution set equals Span $\{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$

Annihilator of a vector space

From left to right: Given system $\mathbf{a}_1 \cdot \mathbf{x} = 0, \ldots, \mathbf{a}_m \cdot \mathbf{x} = 0$, find generators $\mathbf{b}_1, \ldots, \mathbf{b}_k$ for solution set

Solution set is the set of vectors $\mathbf{u}$ such that $\mathbf{a}_1 \cdot \mathbf{u} = 0, \ldots, \mathbf{a}_m \cdot \mathbf{u} = 0$

$$\underbrace{\left[\begin{array}{c} \mathbf{a}_1 \\ \hline \vdots \\ \hline \mathbf{a}_m \end{array}\right]}_{A} \left[\begin{array}{c} \mathbf{x} \end{array}\right] = \left[\begin{array}{c} 0 \\ \vdots \\ 0 \end{array}\right]$$

Equivalent: Given rows of a matrix A, find generators for Null A

$$\begin{array}{c} \text{rows of a matrix } A \\ \downarrow \\ \boxed{\text{Algorithm X}} \\ \downarrow \\ \text{generators for Null } A \end{array}$$

If $\mathbf{u}$ is such a vector then

$$\mathbf{u} \cdot (\alpha_1 \, \mathbf{a}_1 + \cdots + \alpha_m \, \mathbf{a}_m) = 0$$

for any coefficients $\alpha_1, \ldots, \alpha_m$.

Definition: The set of vectors $\mathbf{u}$ such that $\mathbf{u} \cdot \mathbf{v} = 0$ for every vector $\mathbf{v}$ in $\mathcal{V}$ is called the *annihilator* of $\mathcal{V}$. Written as $\mathcal{V}^o$.

Example: The annihilator of Span $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ is the solution set for $\mathbf{a}_1 \cdot \mathbf{x} = 0, \ldots, \mathbf{a}_m \cdot \mathbf{x} = 0$

$$\begin{array}{c} \text{generators for a vector space } \mathcal{V} \\ \downarrow \\ \boxed{\text{Algorithm X}} \\ \downarrow \\ \text{generators for annihilator } \mathcal{V}^o \end{array}$$

Annihilator of a vector space

Definition: For a subspace $\mathcal{V}$ of $\mathbb{F}^n$, the *annihilator* of $\mathcal{V}$, written $\mathcal{V}^o$, is

$$\mathcal{V}^o = \{\mathbf{u} \in \mathbb{F}^n \;:\; \mathbf{u} \cdot \mathbf{v} = 0 \text{ for every vector } \mathbf{v} \in \mathcal{V}\}$$

Example over $\mathbb{R}$: Let $\mathcal{V} = \text{Span}\ \{[1,0,1],[0,1,0]\}$. Then $\mathcal{V}^o = \text{Span}\ \{[1,0,-1]\}$:

- Note that $[1,0,-1] \cdot [1,0,1] = 0$ and $[1,0,-1] \cdot [0,1,0] = 0$.
  Therefore $[1,0,-1] \cdot \mathbf{v} = 0$ for every vector $\mathbf{v}$ in Span $\{[1,0,1],[0,1,0]\}$.
- For any scalar β,
  $$\beta\,[1,0,-1] \cdot \mathbf{v} = \beta\,([1,0,-1] \cdot \mathbf{v}) = 0$$
  for every vector $\mathbf{v}$ in Span $\{[1,0,1],[0,1,0]\}$.
- Which vectors $\mathbf{u}$ satisfy $\mathbf{u} \cdot \mathbf{v} = 0$ for every vector $\mathbf{v}$ in Span $\{[1,0,1],[0,1,0]\}$?
  Only scalar multiples of $[1,0,-1]$.

Example over $GF(2)$: Let $\mathcal{V} = \text{Span}\ \{[1,0,1],[0,1,0]\}$. Then $\mathcal{V}^o = \text{Span}\ \{[1,0,1]\}$:

- Note that $[1,0,1] \cdot [1,0,1] = 0$ (remember $GF(2)$ addition) and $[1,0,1] \cdot [0,1,0] = 0$.
- Therefore $[1,0,1] \cdot \mathbf{v} = 0$ for every vector $\mathbf{v}$ in Span $\{[1,0,1],[0,1,0]\}$.
- Of course $[0,0,0] \cdot \mathbf{v} = 0$ for every vector $\mathbf{v}$ in Span $\{[1,0,1],[0,1,0]\}$.
- $[1,0,1]$ and $[0,0,0]$ are the only such vectors.

Annihilator of a vector space

Example over $\mathbb{R}$: Let $\mathcal{V} = \text{Span } \{[1, 0, 1], [0, 1, 0]\}$. Then $\mathcal{V}^o = \text{Span } \{[1, 0, -1]\}$
$\dim \mathcal{V} + \dim \mathcal{V}^o = 3$

Example over $GF(2)$: Let $\mathcal{V} = \text{Span } \{[1, 0, 1], [0, 1, 0]\}$. Then $\mathcal{V}^o = \text{Span } \{[1, 0, 1]\}$.
$\dim \mathcal{V} + \dim \mathcal{V}^o = 3$

Example over $\mathbb{R}$: Let $\mathcal{V} = \text{Span } \{[1, 0, 1, 0], [0, 1, 0, 1]\}$.
Then $\mathcal{V}^o = \text{Span } \{[1, 0, -1, 0], [0, 1, 0, -1]\}$.
$\dim \mathcal{V} + \dim \mathcal{V}^o = 4$

Annihilator Dimension Theorem: $\dim \mathcal{V} + \dim \mathcal{V}^o = n$

Proof: Let $\mathbf{a}_1, \ldots, \mathbf{a}_m$ be generators for $\mathcal{V}$.

Let $A = \begin{bmatrix} \mathbf{a}_1 \\ \hline \vdots \\ \hline \mathbf{a}_m \end{bmatrix}$

Then $\mathcal{V}^o = \text{Null } A$.

Rank-Nullity Theorem states that

$$\begin{array}{ccccc} \text{rank } A & + & \text{nullity } A & = & n \\ \dim \mathcal{V} & + & \dim \mathcal{V}^o & = & n \end{array}$$

QED

Annihilator of a vector space

Definition: For a subspace $\mathcal{V}$ of $\mathbb{F}^n$, the *annihilator* of $\mathcal{V}$, written $\mathcal{V}^o$, is

$$\mathcal{V}^o = \{\mathbf{u} \in \mathbb{F}^n \; : \; \mathbf{u} \cdot \mathbf{v} = 0 \text{ for every vector } \mathbf{v} \in \mathcal{V}\}$$

$$\begin{array}{ccc} \text{rows of a matrix } A & & \text{generators for a vector space } \mathcal{V} \\ \downarrow & & \downarrow \\ \boxed{\text{Algorithm X}} & = & \boxed{\text{Algorithm X}} \\ \downarrow & & \downarrow \\ \text{generators for Null } A & & \text{generators for annihilator } \mathcal{V}^o \end{array}$$

From left to right: Given system $\mathbf{a}_1 \cdot \mathbf{x} = 0, \ldots, \mathbf{a}_m \cdot \mathbf{x} = 0$, find generators $\mathbf{b}_1, \ldots, \mathbf{b}_k$ for solution set

Algorithm X solves left-to-right problem....

what about right-to-left problem?

Annihilator of a vector space

From left to right: Given system
$\mathbf{a}_1 \cdot \mathbf{x} = 0, \ldots, \mathbf{a}_m \cdot \mathbf{x} = 0,$
find generators $\mathbf{b}_1, \ldots, \mathbf{b}_k$ for solution set

$$\text{generators for a vector space } \mathcal{V} \;\downarrow\; \boxed{\text{Algorithm X}} \;\downarrow\; \text{generators for annihilator } \mathcal{V}^o$$

What happens if we apply Algorithm X to generators for annihilator $\mathcal{V}^o$?

$$\text{generators for annihilator } \mathcal{V}^o \;\downarrow\; \boxed{\text{Algorithm X}} \;\downarrow\; \text{generators for annihilator of annihilator } (\mathcal{V}^o)^o$$

From right to left: Given generators $\mathbf{b}_1, \ldots, \mathbf{b}_k$, find system $\mathbf{a}_1 \cdot \mathbf{x} = 0, \ldots, \mathbf{a}_m \cdot \mathbf{x} = 0$ whose solution set equals Span $\{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$

$$\text{generators for annihilator } \mathcal{V}^o \;\downarrow\; \boxed{\text{Algorithm Y}} \;\downarrow\; \text{generators for original space } \mathcal{V}$$

Theorem: $(\mathcal{V}^o)^o = \mathcal{V}$ (The annihilator of the annihilator is the original space.)

Theorem shows:

$$\text{Algorithm X} = \text{Algorithm Y}$$

We still must prove the Theorem...

Annihilator

Theorem: $(\mathcal{V}^o)^o = \mathcal{V}$ (The annihilator of the annihilator is the original space.)

Proof:
Let $\mathbf{a}_1, \ldots, \mathbf{a}_m$ be a basis for $\mathcal{V}$. Let $\mathbf{b}_1, \ldots, \mathbf{b}_k$ be a basis for $\mathcal{V}^o$.
Since $\mathbf{b}_1 \cdot \mathbf{v} = 0$ for every vector $\mathbf{v}$ in $\mathcal{V}$,

$$\mathbf{b}_1 \cdot \mathbf{a}_1 = 0, \mathbf{b}_1 \cdot \mathbf{a}_2 = 0, \ldots, \mathbf{b}_1 \cdot \mathbf{a}_m = 0$$

Similarly $\mathbf{b}_i \cdot \mathbf{a}_1 = 0, \mathbf{b}_i \cdot \mathbf{a}_2 = 0, \ldots, \mathbf{b}_i \cdot \mathbf{a}_m = 0$ for $i = 1, 2, \ldots, k$.

Reorganizing,

$$\mathbf{a}_1 \cdot \mathbf{b}_1 = 0, \mathbf{a}_1 \cdot \mathbf{b}_2 = 0, \ldots, \mathbf{a}_1 \cdot \mathbf{b}_k = 0$$

which implies that $\mathbf{a}_1 \cdot \mathbf{u} = 0$ for every vector $\mathbf{u}$ in $\underbrace{\text{Span }\{\mathbf{b}_1, \ldots, \mathbf{b}_k\}}_{\mathcal{V}^o}$

This shows $\mathbf{a}_1$ is in $(\mathcal{V}^o)^o$. Similarly $\mathbf{a}_2$ is in $(\mathcal{V}^o)^o$, $\mathbf{a}_3$ is in $(\mathcal{V}^o)^o$, ..., $\mathbf{a}_m$ is in $(\mathcal{V}^o)^o$.

Therefore every vector in Span $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m\}$ is in $(V^o)^o$.

Thus $\underbrace{\text{Span }\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m\}}_{\mathcal{V}}$ is a subspace of $(\mathcal{V}^o)^o$.

To show that these are equal, we must show that $\dim \mathcal{V} = \dim(\mathcal{V}^o)^o$.

By Annihilator Dimension Theorem, $\dim \mathcal{V} + \dim \mathcal{V}^o = n$

Annihilator

Theorem: $(\mathcal{V}^o)^o = \mathcal{V}$ (The annihilator of the annihilator is the original space.)

Proof:
Reorganizing,

$$\mathbf{a}_1 \cdot \mathbf{b}_1 = 0, \mathbf{a}_1 \cdot \mathbf{b}_2 = 0, \ldots, \mathbf{a}_1 \cdot \mathbf{b}_k = 0$$

which implies that $\mathbf{a}_1 \cdot \mathbf{u} = 0$ for every vector $\mathbf{u}$ in $\underbrace{\text{Span } \{\mathbf{b}_1, \ldots, \mathbf{b}_k\}}_{\mathcal{V}^o}$

This shows $\mathbf{a}_1$ is in $(\mathcal{V}^o)^o$. Similarly $\mathbf{a}_2$ is in $(\mathcal{V}^o)^o$, $\mathbf{a}_3$ is in $(\mathcal{V}^o)^o$, ..., $\mathbf{a}_m$ is in $(\mathcal{V}^o)^o$.

Therefore every vector in Span $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m\}$ is in $(V^o)^o$.

Thus $\underbrace{\text{Span } \{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m\}}_{\mathcal{V}}$ is a subspace of $(\mathcal{V}^o)^o$.

To show that these are equal, we must show that $\dim \mathcal{V} = \dim(\mathcal{V}^o)^o$.

By Annihilator Dimension Theorem, $\dim \mathcal{V} + \dim \mathcal{V}^o = n$.

By Annihilator Dimension Theorem applied to $\mathcal{V}^o$, $\dim \mathcal{V}^o + \dim(\mathcal{V}^o)^o = n$.

Together these equations show $\dim \mathcal{V} = \dim(\mathcal{V}^o)^o$. QED