Quiz

- Prove that the dimension of $\mathbb{R}^5$ is 5, using the definition of *dimension*.
- Find the rank of the following set of vectors over $GF(2)$:

$$\{[1,1,0,0,0],[0,1,1,0,0],[0,0,1,1,0],[0,0,0,1,1],[1,0,0,0,1]\}$$

  Prove that your answer is correct, using the definition of *rank*.

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 $S = \mathcal{V}$.

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 B.

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

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 $\dim \text{Span } S \leq 4$.

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

$$\begin{bmatrix} \quad & \mathrm{A} & \quad \end{bmatrix}$$

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: $\left[\begin{array}{c} \mathbf{a}_j \end{array}\right] = \left[\begin{array}{c|c|c} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{array}\right] \left[\begin{array}{c} \mathbf{u}_j \end{array}\right]$

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

B has r columns and U has r rows.

Take transpose of both sides

Write A^T and B^T in terms of cols: col j of A^T equals U^T times col i of B^T.

Write U^T in terms of cols: col i of A^T is a linear combination of cols of U^T.

Each col of A is in span of the r cols of U^T. **Thus col rank of A^T (which is row rank of A)**

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 $A = BU$.
B has r columns and U has r rows.
Take transpose of both sides
Write A^T and B^T in terms of cols: col j of A^T equals U^T times col i of B^T.
Write U^T in terms of cols: col i of A^T is a linear combination of cols of U^T.
Each col of A is in span of the r cols of U^T. **Thus col rank of A^T (which is row rank of A)**

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

$$\left[\begin{array}{c|c|c|c|c|c|c|c|c} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 \end{array}\right] = \left[\begin{array}{c|c|c|c|c} b_1 & b_2 & b_3 & b_4 & b_5 \end{array}\right] \left[\begin{array}{c|c|c|c|c|c|c|c|c} u_1 & u_2 & u_3 & u & u_5 & u_6 & u_7 & u_8 & u_9 \end{array}\right]$$

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 $A = BU$.
B has r columns and U has r rows.
Take transpose of both sides
Write A^T and B^T in terms of cols: col j of A^T equals U^T times col i of B^T.
Write U^T in terms of cols: col i of A^T is a linear combination of cols of U^T.
Each col of A is in span of the r cols of U^T. **Thus col rank of A^T (which is row rank of A)**

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

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

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 $A = BU$.

B has r columns and U has r rows.

Take transpose of both sides

Write A^T and B^T in terms of cols: col j of A^T equals U^T times col i of B^T.

Write U^T in terms of cols: col i of A^T is a linear combination of cols of U^T.

Each col of A is in span of the r cols of U^T. **Thus col rank of A^T (which is row rank of A)**

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

$$\begin{bmatrix} & A & \end{bmatrix} = \begin{bmatrix} B \end{bmatrix}\begin{bmatrix} & U & \end{bmatrix} \quad \begin{bmatrix} & A^T & \end{bmatrix} = \Big[$$

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: $\begin{bmatrix} \mathbf{a}_j \end{bmatrix} = \left[\begin{array}{c|c|c} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{array}\right]\begin{bmatrix} \mathbf{u}_j \end{bmatrix}$

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

B has r columns and U has r rows.

Take transpose of both sides

Write A^T and B^T in terms of cols: col j of A^T equals U^T times col i of B^T.

Write U^T in terms of cols: col i of A^T is a linear combination of cols of U^T.

Each col of A is in span of the r cols of U^T. **Thus col rank of A^T (which is row rank of A)**

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

$$\left[\begin{array}{c|c|c|c|c|c|c|c|c} \bar{a}_1 & \bar{a}_2 & \bar{a}_3 & \bar{a}_4 & \bar{a}_5 & \bar{a}_6 & \bar{a}_7 & \bar{a}_8 & \bar{a}_9 \end{array}\right] = \left[\quad \mathrm{U}^{\mathrm{T}} \quad\right] \left[\begin{array}{c|c|c|c|c|c|c|c|c} \bar{b}_1 & \bar{b}_2 & \bar{b}_3 & \bar{b}_4 & \bar{b}_5 & \bar{b}_6 & \bar{b}_7 & \bar{b}_8 & \bar{b}_9 \end{array}\right]$$

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: $\left[\begin{array}{c} \mathbf{a}_j \end{array}\right] = \left[\begin{array}{c|c|c} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{array}\right] \left[\begin{array}{c} \mathbf{u}_j \end{array}\right]$

$\bar{a}_1$

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

B has r columns and U has r rows.

Take transpose of both sides

Write A^T and B^T in terms of cols: col j of A^T equals U^T times col i of B^T.

Write U^T in terms of cols: col i of A^T is a linear combination of cols of U^T.

Each col of A is in span of the r cols of U^T. **Thus col rank of A^T (which is row rank of A)**

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

$$\left[\begin{array}{c|c|c|c|c|c|c|c|c} \overline{a}_1 & \overline{a}_2 & \overline{a}_3 & \overline{a}_4 & \overline{a}_5 & \overline{a}_6 & \overline{a}_7 & \overline{a}_8 & \overline{a}_9 \end{array}\right] = \left[\begin{array}{c|c|c|c|c|c} \overline{u}_1 & \overline{u}_2 & \overline{u}_3 & \overline{u}_4 & \overline{u}_5 & \overline{u}_6 \end{array}\right] \left[\begin{array}{c|c|c|c|c|c|c|c|c} \overline{b}_1 & \overline{b}_2 & \overline{b}_3 & \overline{b}_4 & \overline{b}_5 & \overline{b}_6 & \overline{b}_7 & \overline{b}_8 & \overline{b}_9 \end{array}\right]$$

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: $\left[\begin{array}{c} \mathbf{a}_j \end{array}\right] = \left[\begin{array}{c|c|c} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{array}\right] \left[\begin{array}{c} \mathbf{u}_j \end{array}\right]$

$\overline{a}_1$

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

B has r columns and U has r rows.

Take transpose of both sides

Write A^T and B^T in terms of cols: col j of A^T equals U^T times col i of B^T.

Write U^T in terms of cols: col i of A^T is a linear combination of cols of U^T.

Each col of A is in span of the r cols of U^T. **Thus col rank of A^T (which is row rank of A)**

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

$$\mathbf{a}_1, b_1 \\ \vdots \\ \mathbf{a}_m, b_m$$

where 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 $\hat{\mathbf{x}} +$ Null A
Once rank A reaches n, cols 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

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

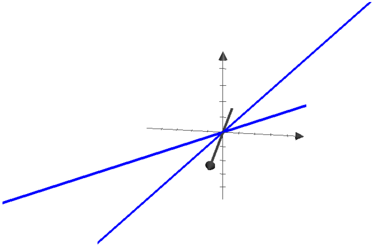
Therefore we cannot form $\mathcal{U} \oplus \mathcal{V}$.

Direct Sum: Example

Vectors over $\mathbb{R}$:

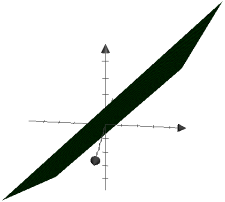
Example:

- 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 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

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

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