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.

Superset-Basis Lemma

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

Proof: Use version of Grow algorithm:

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

At first, S will consist of vectors in C until S contains all of C.

Then more vectors will be added to S until Span $S = \mathcal{V}$

Consequence: At the end, S will definitely contain C.

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 $|D|$.

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

Theorem: For finite D, every subspace of $\mathbb{F}^D$ contains a basis.
Proof: Let $\mathcal{V}$ be a subspace of $\mathbb{F}^D$.
Therefore $\dim \mathcal{V} \leq |D|$.

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

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

- In each iteration, a new vector is added to S.
- Therefore after k iterations, $|S| = k$.
- At each point in the execution of the algorithm, the set S is linearly independent.
- Therefore, so after k iterations, rank $S = k$.
- Every vector added belongs to $\mathcal{V}$ so Span S is a subspace of $\mathcal{V}$.
- After $\dim \mathcal{V}$ iterations, Span S has dimension $\dim \mathcal{V}$
- Therefore, by D2, Span $S = \mathcal{V}$ QED

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

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

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

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 $A = BU$.

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 matrix-matrix equation $A = BU$.

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

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

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.

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

$$\begin{bmatrix} & & \\ & A & \\ & & \end{bmatrix} = \begin{bmatrix} & & \\ & B & \\ & & \end{bmatrix} \begin{bmatrix} & & \\ & U & \\ & & \end{bmatrix}$$

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 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.

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.

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

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:

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

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

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

Use matrix-vector definition of matrix-matrix multiplication to rewrite as 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 knowns 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 m.

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`.