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 ${\bf v}$ in ${\cal V}$ that is not in Span ${\cal S}$, and put it in ${\cal S}$.

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.

all linear combinations of vectors in T, so at this point Span $S = \mathcal{V}$.

▶ The original Grow algorithm stops only once Span S contains every vector in V. However, that's okay: when Span S contains all the vectors in T, Span S also contains

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 \mathcal{C} be a linearly independent set of vectors belonging to \mathcal{V} . Then \mathcal{V} has a basis \mathcal{S} containing all vectors in \mathcal{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 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} < 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 W that contains $\mathbf{u}_1, \dots, \mathbf{u}_k$.

QED

- ▶ $B = \{\mathbf{u}_1, \dots, \mathbf{u}_k, \mathbf{b}_1, \dots, \mathbf{b}_r\}$
- ▶ Thus k < |B|, and
- ▶ If k = |B| then $\{u_1, ..., u_k\} = B$ **Example:** Suppose $V = \text{Span } \{[1, 2], [2, 1]\}.$

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: $S = \{[-0.6, -2.1, -3.5, -2.2], [-1.3, 1.5, -0.9, -0.5], [4.9, -3.7, 0.5, -0.3], [4.9, -3.7, 0.5], [4.9, -3.7, 0.5$

[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 Span S < 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 $V \leq |D|$.

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.
- \blacktriangleright 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 V so Span S is a subspace of V.
- lacktriangle After dim ${\cal V}$ iterations, Span S has dimension dim ${\cal V}$
- ▶ Therefore, by D2, Span S = V

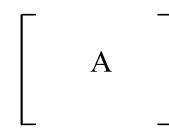
Rank Theorem

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

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

- ▶ Apply lemma to $M \Rightarrow$ row rank of $M \le$ column rank of M
- ▶ Apply lemma to M^T ⇒ row rank of M^T ≤ column rank of M^T ⇒ column rank of M ≤ row rank of M

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



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

$$a_1$$
 a_2
 a_3
 a_4
 a_5
 a_6
 a_7
 a_8
 a_9

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

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

Write each column of
$$A$$
 in terms of basis: $\begin{bmatrix} \mathbf{a}_j \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{bmatrix} \begin{bmatrix} \mathbf{u}_j \end{bmatrix}$

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

$$\begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 \end{bmatrix} = \begin{bmatrix} b_1 & b_2 & b_3 & b_4 & b_5 \end{bmatrix} \begin{bmatrix} u_1 & u_2 & u_3 & u & u_5 & u_6 & u_7 & u_8 & u_9 \end{bmatrix}$$

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

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

Write each column of
$$A$$
 in terms of basis: $\begin{bmatrix} \mathbf{a}_j \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{bmatrix} \begin{bmatrix} \mathbf{u}_j \end{bmatrix}$

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

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

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

Write each column of
$$A$$
 in terms of basis: $\begin{bmatrix} \mathbf{a}_j \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{bmatrix} \begin{bmatrix} \mathbf{u}_j \end{bmatrix}$

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.

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

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

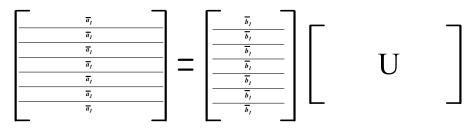
Let $\mathbf{b}_1, \dots, \mathbf{b}_r$ be basis for column space (so column rank = r).

Write each column of
$$A$$
 in terms of basis: $\begin{bmatrix} \mathbf{a}_j \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{bmatrix} \begin{bmatrix} \mathbf{u}_j \end{bmatrix}$

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.



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

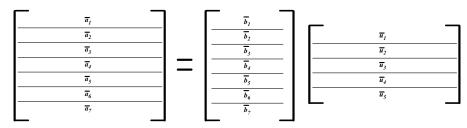
Let $\mathbf{b}_1, \dots, \mathbf{b}_r$ be basis for column space (so column rank = r).

Write each column of
$$A$$
 in terms of basis: $\begin{vmatrix} \mathbf{a}_j \end{vmatrix} = \begin{vmatrix} \mathbf{b}_1 \end{vmatrix} \cdots \begin{vmatrix} \mathbf{b}_r \end{vmatrix} \begin{vmatrix} \mathbf{u}_j \end{vmatrix}$

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.



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

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

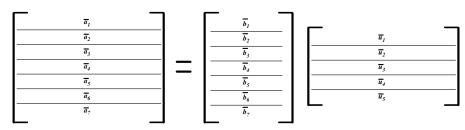
Write each column of
$$A$$
 in terms of basis: $\begin{bmatrix} \mathbf{a}_j \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{bmatrix} \begin{bmatrix} \mathbf{u}_j \end{bmatrix}$

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:



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

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

Write each column of
$$A$$
 in terms of basis: $\begin{bmatrix} \mathbf{a}_j \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_r \end{bmatrix} \begin{bmatrix} \mathbf{u}_j \end{bmatrix}$

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 **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

$$a_1, b_1$$

$$\mathbf{a}_m, b_m$$

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

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

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 $[\mathbf{a}_1, \dots, \mathbf{a}_m]$ is not much less than m.

Once m > n, probably Span $\{a_1, \ldots, a_m\}$ is all of $GF(2)^n$ so Eve can respond to any challenge.

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

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

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.