# Linear function invertibility, revisited

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

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

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

**Proof:** We saw before that $f$

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

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

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

Therefore

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

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 $f(\mathbf{x}) = A\mathbf{x}$:

- Ker $f$ = 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** $\Rightarrow$

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

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.

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

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

# 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 its columns are 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 an invertible matrix. 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 the Rank Theorem, its rows are linearly independent.

The columns of the transpose $A^T$ are the rows of $A$, so the columns of $A^T$ are linearly independent.

Since $A^T$ is square and its columns are linearly independent, we conclude that $A^T$ 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.

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