Linear Algebra

ETH Zürich, HS 2023, 401-0131-00L

The Computer Science Lens

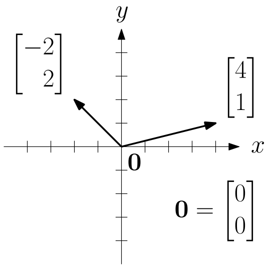
What is a Vector?

Bernd Gärtner

October 20, 2023

So far...

"A vector is (for now) an element of $\mathbb{R}^n$."



vectors in $\mathbb{R}^2$, drawn as arrows

"For now" means that there are also other kinds of vectors.

"An element of $\mathbb{R}^n$" was actually a white lie...

What the Internet thinks a vector is

Oxford Languages:

> *a quantity having direction as well as magnitude, especially as determining the position of one point in space relative to another.*

Chat GPT:

> *In mathematics, a vector is a quantity that has both magnitude and direction. Vectors are typically represented as an arrow in a Euclidean space, with the length of the arrow indicating the magnitude of the vector, and the direction of the arrow indicating the direction of the vector.*

Wikipedia:

> *In mathematics and physics, vector is a term that refers colloquially to some quantities that cannot be expressed by a single number (a scalar), or to elements of some vector spaces.*

What a vector *really* is

Definition
A vector is an element of a vector space.

Definition
A mammal is a vertebrate animal of the class of mammals (Wikipedia).

A vector space is a set together with two operations: vector addition $\mathbf{v} + \mathbf{w}$ and scalar multiplication $c \cdot \mathbf{v}$, each producing another vector.

These operations have to follow some rules (details will follow).

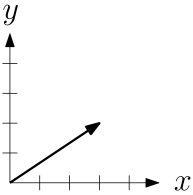
Example
The vector space of polynomials $(x^2 + x + 1, 3x^3, 5x - 2, \ldots)$.

- $(x^2 + x + 1) \ + \ (5x - 2) \ = \ x^2 + 6x - 1$
- $5 \ \cdot \ (x^2 + x + 1) \ = \ 5x^2 + 5x + 5$

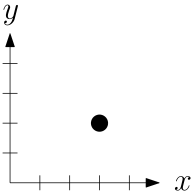
Here, the vectors are polynomials, no "magnitude" or "direction" is apparent.

The white lie: $\mathbb{R}^n$ is *not* a vector space...

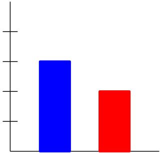
$\mathbb{R}^2$ just contains "raw" pairs of numbers such as $(3, 2)$. The *meaning* can vary.



Vector



Point


Vote

The truth: $(\mathbb{R}^2, +, \cdot)$ is the vector space: this is $\mathbb{R}^2$ together with the vector addition $(+)$ and scalar multiplication $(\cdot)$ that we have seen.

For that vector space, we use arrow drawings and 2×1 matrix notation $\begin{bmatrix} 3 \\ 2 \end{bmatrix}$.

Calling this vector space $\mathbb{R}^2$ is a typical and acceptable "abuse of notation".

Real vector spaces

A real vector space[1] is a triple $(V, +, \cdot)$ where V is a set (the vectors), and

$$\begin{array}{rcll} + & : & V \times V \to V & \text{a function (vector addition),} \\ \cdot & : & \mathbb{R} \times V \to V & \text{a function (scalar multiplication),} \end{array}$$

satisfying the following *axioms* (rules) for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and all $c, d \in \mathbb{R}$.

don't learn them by heart!

1.	$\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$	commutativity
2.	$\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$	associativity
3.	There is a vector $\mathbf{0}$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $\mathbf{v}$	zero vector
4.	There is a vector $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$	negative vector
5.	$1 \cdot \mathbf{v} = \mathbf{v}$	identity element
6.	$(c \cdot d)\mathbf{v} = c \cdot (d \cdot \mathbf{v})$	compatibility
7.	$c(\mathbf{v} + \mathbf{w}) = c\mathbf{v} + c\mathbf{w}$	distributivity over $+$
8.	$(c + d)\mathbf{v} = c\mathbf{v} + d\mathbf{v}$	distributivity over $+$ in $\mathbb{R}$

[1] "real" stands for real numbers $c \in \mathbb{R}$ as scalars

Example: The vector space of polynomials

Polynomial (of degree n): function of the form $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$

V	:	all polynomials	$x^2 + x + 1, 3x^3, 5x - 2, \ldots$
$+$	:	vector addition	$(x^2 + x + 1) + (5x - 2) = x^2 + 6x - 1$
$\cdot$	:	scalar multiplication	$5 \cdot (x^2 + x + 1) = 5x^2 + 5x + 5$

Vector space axioms: easy (and boring) to check...

1. $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$
2. $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$
3. There is a vector $\mathbf{0}$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $\mathbf{v}$ — the zero polynomial $f(x) = 0$ (degree 0, $c_0 = 0$)
4. There is a vector $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$
5. $1 \cdot \mathbf{v} = \mathbf{v}$
6. $(c \cdot d)\mathbf{v} = c \cdot (d \cdot \mathbf{v})$
7. $c(\mathbf{v} + \mathbf{w}) = c\mathbf{v} + c\mathbf{w}$
8. $(c + d)\mathbf{v} = c\mathbf{v} + d\mathbf{v}$

Let's prove some "obvious" facts about real vector spaces (I)

Vector space axioms:

1. $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$
2. $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$
3. There is a vector $\mathbf{0}$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $\mathbf{v}$
4. There is a vector $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$
5. $1 \cdot \mathbf{v} = \mathbf{v}$
6. $(c \cdot d)\mathbf{v} = c \cdot (d \cdot \mathbf{v})$
7. $c(\mathbf{v} + \mathbf{w}) = c\mathbf{v} + c\mathbf{w}$
8. $(c + d)\mathbf{v} = c\mathbf{v} + d\mathbf{v}$

Lemma

There is only one zero vector.

Proof.

Take two zero vectors $\mathbf{0}$ and $\mathbf{0}'$. Then

$$\begin{aligned} \mathbf{0}' &= \mathbf{0}' + \mathbf{0} && (3.\ \mathbf{0} \text{ is a zero vector}) \\ &= \mathbf{0} + \mathbf{0}' && (1.\ \text{commutativity}) \\ &= \mathbf{0} && (3.\ \mathbf{0}' \text{ is a zero vector}) \end{aligned}$$

So $\mathbf{0}$ and $\mathbf{0}'$ are equal. $\square$

Let's prove some "obvious" facts about real vector spaces (II)

Vector space axioms:

1. $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$
2. $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$
3. There is a vector $\mathbf{0}$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $\mathbf{v}$
4. There is a vector $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$
5. $1 \cdot \mathbf{v} = \mathbf{v}$
6. $(c \cdot d)\mathbf{v} = c \cdot (d \cdot \mathbf{v})$
7. $c(\mathbf{v} + \mathbf{w}) = c\mathbf{v} + c\mathbf{w}$
8. $(c + d)\mathbf{v} = c\mathbf{v} + d\mathbf{v}$

Lemma

For every vector $\mathbf{v}$, we have $0 \cdot \mathbf{v} = \mathbf{0}$.

Proof.

$$\begin{array}{rll}
 & 0\mathbf{v} & \\
= & 0\mathbf{v} + \mathbf{0} & \text{(3. zero vector)} \\
= & 0\mathbf{v} + (0\mathbf{v} + (-0\mathbf{v})) & \text{(4. negative)} \\
= & (0\mathbf{v} + 0\mathbf{v}) + (-0\mathbf{v}) & \text{(2. associativity)} \\
= & (0+0)\mathbf{v} + (-0\mathbf{v}) & \text{(8. distributivity } +) \\
= & 0\mathbf{v} + (-0\mathbf{v}) & \text{(rules of } \mathbb{R}) \\
= & \mathbf{0} & \text{(4. negative)}
\end{array}$$

$\square$

Let's prove some "obvious" facts about real vector spaces (III)

Vector space axioms:

1. $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$
2. $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$
3. There is a vector $\mathbf{0}$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $\mathbf{v}$
4. There is a vector $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$
5. $1 \cdot \mathbf{v} = \mathbf{v}$
6. $(c \cdot d)\mathbf{v} = c \cdot (d \cdot \mathbf{v})$
7. $c(\mathbf{v} + \mathbf{w}) = c\mathbf{v} + c\mathbf{w}$
8. $(c + d)\mathbf{v} = c\mathbf{v} + d\mathbf{v}$

Lemma

Each $\mathbf{v}$ *has only one negative vector.*

Proof.

Take two negative vectors $\mathbf{u}$ and $\mathbf{u}'$ of $\mathbf{v}$.
Then

$$
\begin{aligned}
\mathbf{u}' &= \mathbf{u}' + \mathbf{0} && \text{(3. zero vector)}\\
&= \mathbf{u}' + (\mathbf{v} + \mathbf{u}) && \text{(4. } \mathbf{u} \text{ is a negative)}\\
&= (\mathbf{u}' + \mathbf{v}) + \mathbf{u} && \text{(2. associativity)}\\
&= (\mathbf{v} + \mathbf{u}') + \mathbf{u} && \text{(1. commutativity)}\\
&= \mathbf{0} + \mathbf{u} && \text{(4. } \mathbf{u}' \text{ is a negative))}\\
&= \mathbf{u} + \mathbf{0} && \text{(1. commutativity)}\\
&= \mathbf{u} && \text{(3. zero vector)}
\end{aligned}
$$

So $\mathbf{u}$ and $\mathbf{u}'$ are equal. $\square$

$\mathbb{F}$-vector spaces – where $\mathbb{F}$ is a *field* ($\mathbb{R}$ is only one of many fields)

A $\mathbb{F}$-vector space[2] is a triple $(V, +, \cdot)$ where V is a set (the vectors), and

$$\begin{array}{lcll} + & : & V \times V \to V & \text{a function (vector addition),} \\ \cdot & : & \mathbb{F} \times V \to V & \text{a function (scalar multiplication),} \end{array}$$

satisfying the following *axioms* (rules) for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and all $c, d \in \mathbb{F}$.

1.	$\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$	commutativity
2.	$\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$	associativity
3.	There is a vector $\mathbf{0}$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $\mathbf{v}$	zero vector
4.	There is a vector $-\mathbf{v}$ such that $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$	negative vector
5.	$1 \cdot \mathbf{v} = \mathbf{v}$	identity element
6.	$(c \cdot d)\mathbf{v} = c \cdot (d \cdot \mathbf{v})$	compatibility
7.	$c(\mathbf{v} + \mathbf{w}) = c\mathbf{v} + c\mathbf{w}$	distributivity over $+$
8.	$(c + d)\mathbf{v} = c\mathbf{v} + d\mathbf{v}$	distributivity over $+$ in $\mathbb{F}$

[2] "real" stands for real numbers $c \in \mathbb{R}$ as scalars

Fields

A field is a triple $(F, +, \cdot)$ where F is a set (the numbers), and

$$\begin{array}{lcll} + & : & F \times F \to F & \text{a function (addition of two numbers),} \\ \cdot & : & F \times F \to F & \text{a function (multiplication of two numbers),} \end{array}$$

satisfying the following *axioms* (rules) for all $a, b, c \in \mathbb{F}$:

don't learn them by heart!

1.	$a + b = b + a$	commutativity of $+$
2.	$a \cdot b = b \cdot a$	commutativity of $\cdot$
3.	$a + (b + c) = (a + b) + c$	associativity of $+$
4.	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$	associativity of $\cdot$
5.	there is a number 0 such that $a + 0 = a$ for all a	zero
6.	there is a number $1 \neq 0$ such that $a \cdot 1 = a$ for all a	one
7.	There is a number $-a$ such that $a + (-a) = 0$	negative
8.	If $a \neq 0$, there is a number a^{-1} such that $a \cdot a^{-1} = 1$	inverse
9.	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$	distributivity

Examples of fields

- $\mathbb{R}$ (real numbers)
- $\mathbb{C}$ (complex numbers)
- $\mathbb{Q}$ (rational numbers)

Non-examples:

- $\mathbb{Z}$ (integers): no inverses
- $\mathbb{N}$ (natural numbers): no negatives

Finite fields of prime order (very important in cryptography):

- $\mathbb{F}_p = (\{0, 1, \ldots, p-1\}, +, \cdot)$, where p is a prime number.

$$a + b = (\underbrace{a + b}_{+ \text{ in } \mathbb{N}}) \bmod p \qquad a \cdot b = (\underbrace{a \cdot b}_{\cdot \text{ in } \mathbb{N}}) \bmod p$$

- $p = 2 : \mathbb{F}_2 = (\{0, 1\}, +, \cdot)$. The *smallest possible* field (every field has 0 and 1).

$$(a + b) \bmod 2 : \quad \begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad (a \cdot b) \bmod 2 : \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

In all cases, the field axioms have been checked.

The field $\mathbb{F}_2$: Calculating with bits (value 0 or 1)

Adding two bits: the logical exclusive or

+	0	1
0	0	1
1	1	0

$$b_1 + b_2 = \begin{cases} 1 & \text{if either } b_1 = 1 \text{ or } b_2 = 1 \\ 0 & \text{otherwise} \end{cases} = b_1 \text{ XOR } b_2$$

Multiplying two bits: the logical and

$\cdot$	0	1
0	0	0
1	0	1

$$b_2 \cdot b_2 = \begin{cases} 1 & \text{if } b_1 = 1 \text{ and } b_2 = 1 \\ 0 & \text{otherwise} \end{cases} = b_1 \text{ AND } b_2$$

Adding more bits:

$$b_1 + b_2 + \cdots + b_n = \begin{cases} 1 & \text{if an odd number of } b_i\text{'s is 1} \\ 0 & \text{if an even number of } b_i\text{'s is 1} \end{cases}$$

$$\begin{array}{rcc} & & 3 \bmod 2 \\ & & \| \\ 0+1+1+0+1 & = & 1 \\ 1+0+1+1+1 & = & 0 \\ & & \| \\ & & 4 \bmod 2 \end{array}$$

For every field $\mathbb{F}$, we have the $\mathbb{F}$-vector space $\mathbb{F}^n$ (if $\mathbb{F} = \mathbb{R}$, this is $\mathbb{R}^n$)

Vectors: $\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$, where $v_1, v_2, \dots, v_n \in \mathbb{F}$.

Vector addition:

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} + \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} v_1 + w_1 \\ v_2 + w_2 \\ \vdots \\ v_n + w_n \end{bmatrix}, \quad \text{where } + \text{ is the addition in } \mathbb{F}$$

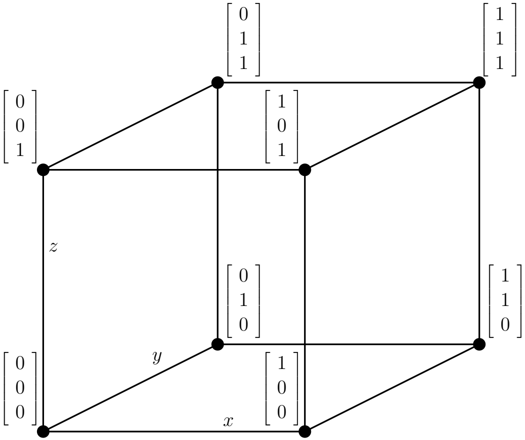
Scalar multiplication:

$$c \cdot \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} c \cdot v_1 \\ c \cdot v_2 \\ \vdots \\ c \cdot tv_n \end{bmatrix}, \quad \text{where } \cdot \text{ is the multiplication in } \mathbb{F}$$

Bit vectors: elements of the vector space $\mathbb{F}_2^n$

$\mathbb{F}_2^n$ contains 2^n vectors.

$n = 3$:



"Hamming cube"

Combinations in $\mathbb{F}_2^n$

$$c_1\mathbf{v}_1 + \cdots + \underset{\substack{\downarrow \\ 1\,:\ \text{take } \mathbf{v}_i \\ 0\,:\ \text{don't take } \mathbf{v}_i}}{c_i\mathbf{v}_i} + \cdots + c_n\mathbf{v}_n$$

Combinations are just sums of vectors (the ones we take).

Vectors are independent if we can only get $\mathbf{0}$ by taking none of them.

$$\underbrace{\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}}_{\text{independent}} \qquad \underbrace{\begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}}_{\text{dependent}} : \quad \begin{bmatrix}1\\1\\0\end{bmatrix} + \begin{bmatrix}0\\1\\1\end{bmatrix} + \begin{bmatrix}1\\0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\end{bmatrix}$$

In $\mathbb{R}^3$, these three vectors would be independent!

Systems of linear equations in $\mathbb{F}^n$

Everything we do in $\mathbb{R}^n$ works the same way in $\mathbb{F}^n$:

- Matrices
- $A\mathbf{x} = \mathbf{b}$ and Gauss elimination
- Inverse matrices
- Gauss-Jordan elimination (Chapter 3)
- Full solution of $A\mathbf{x} = \mathbf{b}$ (Chapter 3)
- ...

Example ($\mathbb{F}_2^5$): solve for the bit vector $\mathbf{x}$!

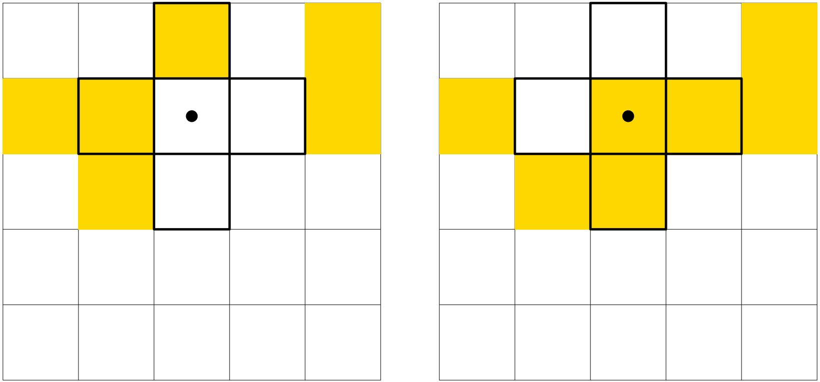
$$\begin{bmatrix} 1 & & & & \\ 1 & 1 & & & \\ 0 & 1 & 1 & & \\ 0 & 0 & 1 & 1 & \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Take columns $1, 3, 5$

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Application: Game "Lights out!"

$n \times n$ grid of buttons (original game: 5×5), some are on (yellow):

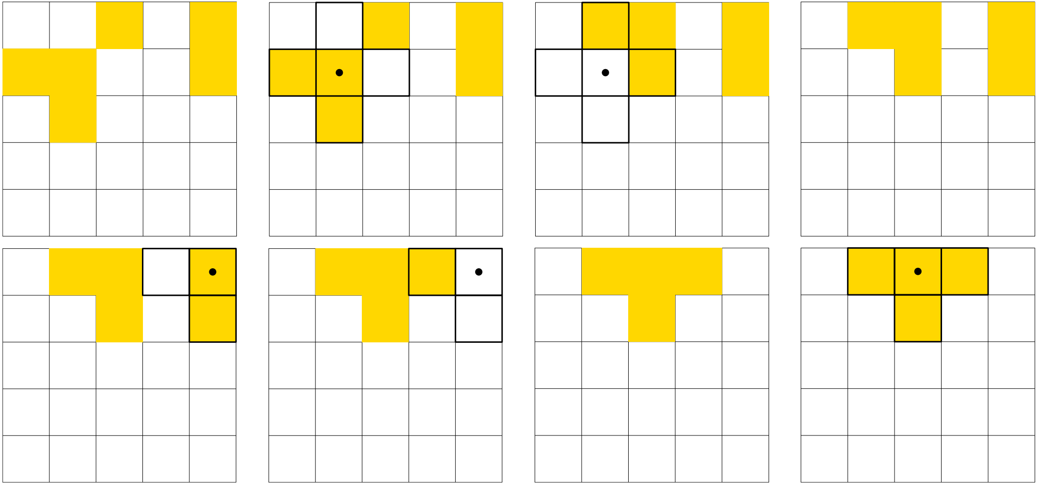


Pressing a button... switches it (on $\leftrightarrow$ off) and all its neighbors.

Goal: Repeatedly press buttons until all are off!

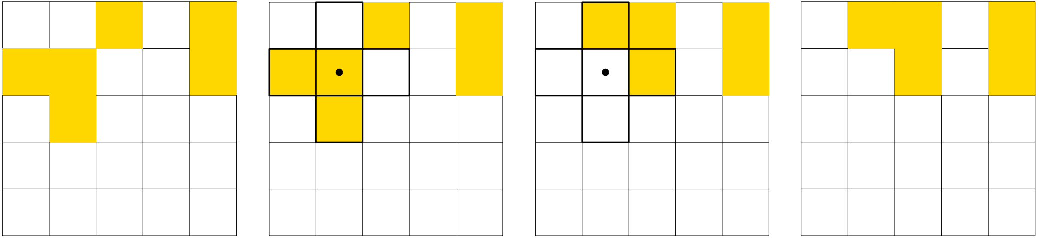
Lights Out!

Solution



Done after this button!

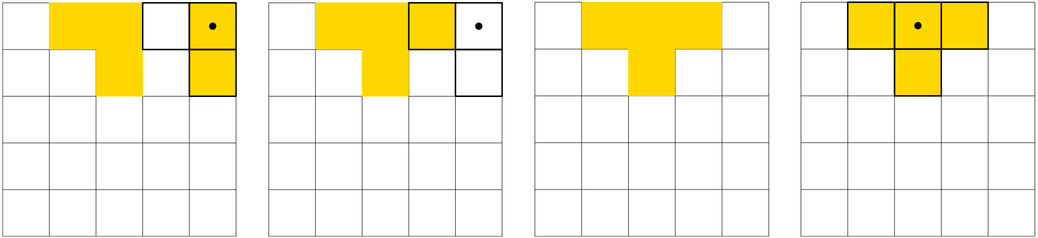
First solution step, mathematically



$$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

vector in $\mathbb{F}_2^{25}$ | “button vector” $\mathbf{b}_7$ in $\mathbb{F}_2^{25}$ | vector in $\mathbb{F}_2^{25}$

Second solution step, mathematically



$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

vector in $\mathbb{F}_2^{25}$ | “button vector” $\mathbf{b}_5$ in $\mathbb{F}_2^{25}$ | vector in $\mathbb{F}_2^{25}$

Lights Out, mathematically

Given a vector $\mathbf{v} \in \mathbb{F}_2^{25}$, produce $\mathbf{0} \in \mathbb{F}_2^{25}$ by adding suitable button vectors!

Same problem ("play the game backwards"): starting from $\mathbf{0}$, produce $\mathbf{v}$ by adding suitable button vectors!

$$\underset{\mathbf{v}}{\begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}} = \underset{\mathbf{b}_7}{\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}} + \underset{\mathbf{b}_5}{\begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}} + \underset{\mathbf{b}_3}{\begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}}$$

No button vector is needed twice ($\mathbf{b}_i + \mathbf{b}_i = \mathbf{0}$, no effect).

Order of button vectors doesn't matter (commutativity)!

Lights Out: A system of linear equations in $\mathbb{F}_2^{25}$!

To win the game with initial configuration $\mathbf{v} \in \mathbb{F}_2^{25}$, solve

$$\mathbf{v} = x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + \cdots x_{25}\mathbf{b}_{25}$$

with all $x_i \in \mathbb{F}_2$ (0 or 1).

This is a system of linear equations with 25 equations in 25 unknowns:

$$\underbrace{\begin{bmatrix} | & | & & | \\ \mathbf{b}_1 & \mathbf{b}_2 & \cdots & \mathbf{b}_{25} \\ | & | & & | \end{bmatrix}}_{\text{matrix A,}25\times 25} \mathbf{x} = \mathbf{v}$$

This system has been analyzed [AF98]:

- The matrix A is quadratic but *not* invertible.
- In Chapter 3, we will learn how to solve systems of equations with non-invertible matrices.
- This allows you to win Lights Out whenever this is possible (it isn't always)!

References

Marlow Anderson and Todd Feil.
Turning lights out with linear algebra.
Mathematics Magazine, 71(4):300–303, 1998.
https://doi.org/10.1080/0025570X.1998.11996658.