Vector spaces over finite fields (class)

Our examples so far, like $\mathbb{R}^n$, $\mathbb{R}^{m\times n}$ ($m\times n$ matrices), or their subspaces, have been "over $\mathbb{R}$" (real numbers, $\mathbb{R}=(-\infty,\infty)$), meaning that the spaces have to be closed under multiplication by arbitrary real numbers $(0, 1, \frac{1}{2}, \sqrt{2}, \pi, \dots)$.

But linear algebra makes sense over other fields, too, and some are very important!

Example: $\mathbb{C} = \{a+bi \mid a,b\in\mathbb{R}\}$ complex numbers

$i^2=-1$

$(a+bi)(c+di) = (ac-bd)+(ad+bc)i$

What is a field? $\mathbb{R}$, $\mathbb{C}$

Essentially, a set with
- addition ✓
- subtraction ✓
- multiplication ✓
- division ✓

https://en.wikipedia.org/wiki/Field_(mathematics)#Classic_definition

Formally, a field is a set together with two operations called *addition* and *multiplication*.[1] An operation is a mapping that associates an element of the set to *every* pair of its elements. The result of the addition of a and b is called the *sum* of a and b and denoted $a+b$. Similarly, the result of the multiplication of a and b is called the *product* of a and b, and denoted ab or $a\cdot b$. These operations are required to satisfy the following properties, referred to as *field axioms*. In the sequel, a, b and c are arbitrary elements of F.

- *Associativity* of addition and multiplication: $a+(b+c)=(a+b)+c$ and $a\cdot(b\cdot c)=(a\cdot b)\cdot c$.
- *Commutativity* of addition and multiplication: $a+b=b+a$ and $a\cdot b=b\cdot a$.
- *Additive* and *multiplicative identity*: there exist two different elements 0 and 1 in F such that $a+0=a$ and $a\cdot 1=a$.
- *Additive inverses*: for every a in F, there exists an element in F, denoted $-a$, called *additive inverse* of a, such that $a+(-a)=0$.
- *Multiplicative inverses*: for every $a\neq 0$ in F, there exists an element in F, denoted by a^{-1}, $1/a$, or $\frac{1}{a}$, called the *multiplicative inverse* of a, such that $a\cdot a^{-1}=1$.
- *Distributivity* of multiplication over addition: $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$.

$2\cdot 2=1 \bmod 3 \Rightarrow 2^{-1}=2 \bmod 3$

$2=0 \bmod 2 \Rightarrow 2^{-1}$ doesn't exist mod 2

Example:

$\mathbb{Z}$ = set of integers $\dots,-2,-1,0,1,2,\dots$ is not a field

addition ✓, subtraction ✓, multiplication ✓, ~~division~~ $\frac{1}{2}\notin\mathbb{Z}$

Linear algebra over $\mathbb{Z}$ doesn't really work

$$\begin{pmatrix}2&3\\3&2\end{pmatrix}\vec{x}=\vec{0} \qquad \begin{pmatrix}6&9\\0&-5\end{pmatrix}\vec{x}=\vec{0}$$

$$\left\{\begin{pmatrix}x_1\\x_2\end{pmatrix} \,\middle|\, x_1+x_2=0\right\} \;\text{ ⫲ }\; \left\{\begin{pmatrix}x_1\\x_2\end{pmatrix} \,\middle|\, 3x_1+3x_2=0\right\}$$

We need division!

Example:

$\mathbb{Q}=\{a/b \mid a,b\in\mathbb{Z}, b\neq 0\}$ is a field

rational numbers

Example: $\mathbb{F}_2=\{0,1\}$ is a finite field

Mathematica

```
A = (1 0 1
     1 1 0
     0 1 1);
RowReduce[A, Modulus → 2] // MatrixForm
```

$$\begin{pmatrix}1&0&1\\0&1&1\\0&1&1\end{pmatrix} \to \begin{pmatrix}1&0&1\\0&1&1\\0&0&0\end{pmatrix}$$

$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$; $\longrightarrow \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

```
RowReduce[A, Modulus → 2] // MatrixForm
```

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

$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$; $\longrightarrow \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 2 \end{pmatrix}$ $\cdot\frac{1}{2}$

```
RowReduce[A] // MatrixForm
```

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

$\mathbb{R} = \mathbb{R}^1 \qquad \mathbb{R}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \middle| \, x, y \in \mathbb{R} \right\}$

$\mathbb{F}_2 \qquad \mathbb{F}_2^2$

Vector spaces over $\mathbb{F}_2 = \{0, 1\}$

Bit strings of length n form a vector space over $\mathbb{F}_2$

eg., $n=2$: $\mathbb{F}_2^2$ $\qquad$ $n=3$: $\mathbb{F}_2^3$

$(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ $\qquad$ $(0,0,0), (0,0,1), (0,1,0), (0,1,1)$, $(1,0,0), (1,0,1), (1,1,0), (1,1,1)$

coordinate-wise addition mod 2,

$(0,1,1) + (1,1,0) = (1,0,1)$.

Linear operators make sense:

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

Subspaces make sense:

$\{(0,0), (0,1)\}$ is a subspace of $\{0,1\}^2$

Why?

closure under addition:

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

closure under multiplication by 0 or 1 ($\mathbb{F}_2$): ✓

Exercise: How many subspaces are there of $\{0,1\}^2$ over $\mathbb{F}_2$?

Answer: $\boxed{5}$

$\left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}$ ✓ $\qquad \mathbb{F}_2^2 = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$

$\left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$ ✓, $\left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$, $\left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$

$V = \left\{ \begin{pmatrix} 0\\0\\0 \end{pmatrix}, \begin{pmatrix} 0\\0\\1 \end{pmatrix}, \begin{pmatrix} 1\\0\\1 \end{pmatrix} \right\}$ is not a subspace

not closed under addition

$\begin{pmatrix} 0\\0\\1 \end{pmatrix} + \begin{pmatrix} 1\\0\\1 \end{pmatrix} = \begin{pmatrix} 1\\0\\0 \end{pmatrix} \notin V$

Exercise: Span$\left(\left\{ \begin{pmatrix} 0\\0\\1 \end{pmatrix}, \begin{pmatrix} 1\\0\\1 \end{pmatrix} \right\} \right) = \left\{ a\begin{pmatrix} 0\\0\\1 \end{pmatrix} + b\begin{pmatrix} 1\\0\\1 \end{pmatrix} \;\middle|\; a, b \in \mathbb{F}_2 = \{0,1\} \right\}$

over $\mathbb{F}_2$

$= \left\{ \begin{pmatrix} 0\\0\\0 \end{pmatrix}, \begin{pmatrix} 0\\0\\1 \end{pmatrix}, \begin{pmatrix} 1\\0\\1 \end{pmatrix}, \begin{pmatrix} 1\\0\\0 \end{pmatrix} \right\}$

How many subspaces are there of $\{0,1\}^3$?
$\{0,1\}^n$?

More finite fields

$\mathbb{F}_3 = \{0, 1, 2\}$ is a field ✓

$1^{-1} = 1$, $2^{-1} = 2$

$2^{-1} 2 = 1 \mod 3$

$\Updownarrow$

$2^{-1} = 2$

$\frac{a}{b} = a \cdot b^{-1}$

$\{0, 1, 2, 3\}$ is not a field

$1^{-1} = 1$, $3^{-1} = 3$ $(3 \times 3 = 1 \mod 4)$

but you can't divide by 2!

2^{-1} does not exist in $\{0,1,2,3\}$

$2x = 1 \mod 4$

no answer

$x = 2^{-1} \mod p$

$\{0, 1, 2, 3, 4\}$ is a field (mod 5, $\mathbb{F}_5$)

$1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$

Def: Inverse of x

$x^{-1} \cdot x = 1$

$\{0, 1, 2, \dots, p-1\}$ is a field if and only if p is prime!

$2^{-1} \cdot 2 = 1 \mod 5$

$\Rightarrow 2^{-1} = 3$

$2^{-1} \mod 7 = 4$

"$a - b$" $= a + (-b)$

where "$-b$" satisfies

$b + (-b) = 0$

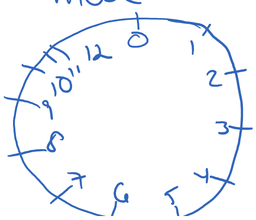
$-b$ is the additive inverse of b

"a/b" $= a \cdot b^{-1}$

where b^{-1} is the multiplicative inverse of b

$b \cdot b^{-1} = 1$

mod 13



$15 = 2 \mod 13$

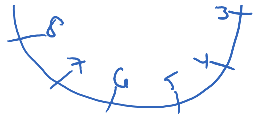
$15 \cdot 2 = 2 \cdot 2 = 4 \mod 13$

$12 = -1 \mod 13$

$\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$

field $\Leftrightarrow p$ is prime

over $\mathbb{R}$



$\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ is a field $\iff p$ is prime

Other important finite fields

Any finite field must have p^k elements for a prime p.

Example: x^2+x+1 is "irreducible" over $\mathbb{F}_2$ (can't be factored)

Consider all polynomials modulo x^2+x+1

$\underbrace{0,\ 1,}_{\text{degree } 0}\ \underbrace{x,\ x+1}_{\text{degree } 1}$ $\quad ``x^2"$

$x^2+x+1 = 0$

$+(x+1) \Downarrow \quad +(x+1)$

$x^2+2(x+1) = x+1$

$= x^2$

multiplication

	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

inverses:

$1^{-1} = 1$

$x^{-1} = x+1$

$(x+1)^{-1} = x$

$x^3 = x^2 \cdot x$
$= (x+1)\cdot x$
$= x^2 + x$
$= (x+1) + x$
$= 2x + 1 = 1$

$(x+1)(x+1) = (x+1)\cdot x + (x+1)\cdot 1 = 1 + x+1 = x$

addition

	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

$-1 = 1 \bmod 2$

over $\mathbb{F}_2$

x^2+1 reducible

$= (x+1)(x+1)$

$= x^2+1 + 1\cdot x + x\cdot 1$

$= x^2+1+2\cdot x$

$= x^2+1$ ✓

x^2+1 over $\mathbb{F}_3$?

over $\mathbb{R}$

$x^2-1 = (x-1)(x+1)$

reducible $\quad$ irreducible

$x^2+1 = (x-i)(x+i)$

x^2+1 is irreducible over $\mathbb{R}$

reducible over $\mathbb{C}$

https://en.wikipedia.org/wiki/Finite_field

Applications [edit]

In cryptography, the difficulty of the discrete logarithm problem in finite fields or in elliptic curves is the basis of several widely used protocols, such as the Diffie–Hellman protocol. For example, in 2014 a secure internet connection to Wikipedia involved the elliptic curve Diffie–Hellman protocol (ECDHE) over a large finite field.[5] In coding theory, many codes are constructed as subspaces of vector spaces over finite fields.

:

Reed–Solomon codes are a group of error-correcting codes that were introduced by Irving S. Reed and Gustave Solomon in 1960.[1] They have many applications, the most prominent of which include consumer technologies such as CDs, DVDs, Blu-ray Discs, QR Codes, data transmission technologies such as DSL and WiMAX, broadcast systems such as DVB and ATSC, and storage systems such as RAID 6. They are also used in satellite communication.

In coding theory, the Reed–Solomon code belongs to the class of non-binary cyclic error-correcting codes. The Reed–Solomon code is based on univariate polynomials over finite fields.

Data storage [edit]

Reed–Solomon coding is very widely used in mass storage systems to correct the burst errors associated with media defects.

Reed–Solomon coding is a key component of the compact disc. It was the first use of strong error correction coding in a mass-produced consumer product, and DAT and DVD use similar schemes. In the CD, two layers of Reed–Solomon coding separated by a 28-way convolutional interleaver yields a scheme called Cross-Interleaved Reed–Solomon Coding (CIRC). The first element of a CIRC decoder is a relatively weak inner (32,28) Reed–Solomon code, shortened from a (255,251) code with 8-bit symbols. This code can correct up to 2 byte errors per 32-byte block. More importantly, it flags as erasures any uncorrectable blocks, i.e., blocks with more than 2 byte errors. The decoded 28-byte blocks, with erasure indications, are then spread by the deinterleaver to different blocks of the (28,24) outer code. Thanks to the deinterleaving, an erased 28-byte block from the inner code becomes a single erased byte in each of 28 outer code blocks. The outer code easily corrects this, since it can handle up to 4 such erasures per block.

$\mathbb{F}_{2^8}$

The result is a CIRC that can completely correct error bursts up to 4000 bits, or about 2.5 mm on the disc surface. This code is so strong that most CD playback errors are almost certainly caused by tracking errors that cause the laser to jump track, not by uncorrectable error bursts.[5]

DVDs use a similar scheme, but with much larger blocks, a (208,192) inner code, and a (182,172) outer code.

Reed–Solomon error correction is also used in parchive files which are commonly posted accompanying multimedia files on USENET. The Distributed online storage service Wuala (discontinued in 2015) also used to make use of Reed–Solomon when breaking up files.

Example: Over $\mathbb{F}_2$.

Example: Over $\mathbb{F}_2$,

$x^{2^n}+1$ is reducible for $n \geq 0$

```
FactorList[x^4 + 1, Modulus -> 2]
{{1, 1}, {1 + x, 4}}
```

Proof: $(x+1)\cdot(x+1) = x^2+2x+1 = x^2+1$

$(x^2+1)(x^2+1) = x^4+1 \quad (x+1)^{2^n} = x^{2^n}+1$

x^4+x+1 is irreducible

```
IrreduciblePolynomialQ[x^4 + x + 1, Modulus -> 2]
True
```

$\Rightarrow$ gives a field with 2^4 elements

$0, 1, x, x+1, x^2, \ldots, x^3+x^2+x+1$

Multiplication mod x^4+x+1, $x^4 = x+1$

e.g., $x^3 \cdot (x^2+1) = x^5+x^3$

$= x^4 \cdot x + x^3$

$= (x+1)\cdot x + x^3$

$= x^3+x^2+x$

polynomial addition

$$\begin{array}{r} 1001 \\ +\,0101 \\ \hline 1100 \end{array}$$

= exor of binary strings

Represented in binary:

$$\underset{x^3\ x^2\ x\ 1}{1000} \cdot \underset{\underbrace{x^3\ x^2}\ x\ 1}{0101} = \underset{x^3\ x^2\ x\ 1}{1110}$$

$\updownarrow$ $\qquad x^2+1$

$x^3+0x^2+0\cdot x+0\cdot 1$