L06

Tuesday, August 9, 2022 9:44 AM

* Algebraic Codes || Code constructions base on <u>finite algebra</u>.

* The most important class of codes before 2000.

* Even today, it is still the most widely used codes, especially when <u>complexity</u> and <u>speed</u> is the main concern.

  E.g. fiber-optic communication

  close to 100~400 G bps. $\boxed{\text{per channel}}$ for standard cable

  up to 600-1000 G bps per channel

* Extremely computationally efficient.

* Unfortunate, not <u>optimal</u> in the sense of MAP or ML decoder.

* Set: G, which many have finite, or countably infinite, or uncountably infinite number of elements.

* $G_1 \cup G_2$

  $G_1 \cap G_2$

  $G_1 \setminus G_2 = \{c : c \in G_1, c \notin G_2\}$

  $G_1 \times G_2 = \{(a, b) : a \in G_1, b \in G_2\}$

  $G_1 \subseteq G_2$

* A binary operation over G is a mapping $f : G \times G \longmapsto G$

  E.g. $G = \{\text{apple, orange}\}$.

  $f(\text{apple, apple}) = \text{apple}$.

  $f(\text{apple, orange}) = \text{apple}$.

  $f(\text{orange, apple}) = \text{orange}$.

$f(\text{orange}, \text{orange}) = \text{apple}$

Oftentimes, we use a symbol say $\bullet$ or $+$, or $\oplus$ or $\circ$, ... to represent a binary operator

E.g. apple $\bullet$ apple = apple.

apple $\bullet$ orange = apple

orange $\bullet$ apple = orange

orange $\bullet$ orange = apple

E.g. "Addition" is a binary operator over the set of integers.

"division" is Not a binary operator over the set of real numbers.

"vector inner product" $\vec{a} \cdot \vec{b}$ is not a binary operator over the $\mathbb{R}^n$ even though $\vec{a} \in \mathbb{R}^n$ and $\vec{b} \in \mathbb{R}^n$

* Suppose "$\bullet$" is defined over G.

* Suppose $\bullet$ is defined over G,
i.e. $\bullet : G \times G \mapsto G$.
then we say $\bullet$ is <u>closed</u> under $G_1 \subseteq G_2$
if $\forall a, b \in G_1$, $(a \bullet b) \in G_1$

* A set G is a <u>group</u> (with respect to a binary operation $\bullet$) if the following conditions are satisfied

① Associativity: $(a \circ b) \circ c$
$= a \circ (b \circ c)$

② Identity: there exists ($\exists$) $\boxed{1} \in G$
such that $a \cdot 1 = 1 \cdot a = a \quad \forall a \cdot G$
sometimes: $\exists e \in G$, s.t. $a \circ e = e \cdot a = a$

③ Inverse: $\forall a \in G$, there exists
$\boxed{a^{-1}} \in G$ such that

$$a \circ a^{-1} = a^{-1} \circ a = 1$$

The order of a Group $\Rightarrow$ the

* The <u>order</u> of a <u>Group</u> is the number of elements in G.
* If the order is <u>finite</u> $\Rightarrow (G, \circ)$ is a finite group

---

* A group does not require commutativity

$$a \circ b = b \circ a$$

* A group is called commutative (or Abelian) if $a \circ b = b \circ a \quad \forall a, b \in G$

Example: Say $G = \{0, 1, 2\}$.

define $a \bullet b = \text{mod}(a \boxplus b, 3)$

i.e. $1 \circ 2 = 0$,

$1 \circ 1 = 0$.

$2 \circ 2 = 1$, ...

Q: Prove G and $\bullet$ is a group.

Q: Prove G and $\circ$ is a group.

Ans: ① Associativity:

$$(a \circ b) \circ c$$

$$= \mathrm{mod}\left(\mathrm{mod}(a \boxplus b, 3) \boxplus c, 3\right)$$

$$= \mathrm{mod}(a \boxplus b \boxplus c, 3)$$

$$= a \circ (b \circ c)$$

② Identity: $e = 0$

$$a \circ e = \mathrm{mod}(a \boxplus 0, 3) = e \circ a$$

$$= a$$

③ Inverse:

	Inverse	
0	$0^{-1} = 0$	$0 \circ 0 = 0.$
1	$1^{-1} = 2$	$1 \circ 2 = 0$
2	$2^{-1} = 1$	$2 \circ 1 = 0$

$\Rightarrow$ G is a group.

Example $\quad G = \{0, 1, 2\}$.

$$a \circ b = \mathrm{mod}(a \boxplus b \boxplus 1, 3).$$

i.e. $\underline{1} \circ 1 = 0$.

$$1 \circ 2 = 1$$

$$0 \circ 0 = 1$$

Prove G and $\circ$ is a group.

Ans: Associativity.

$$(a \circ b) \circ c = \mathrm{mod}(a \boxplus b \boxplus c \boxplus 2, 3)$$

$$= a \circ (b \circ c)$$

Identity. $e = 2$.

$$e \circ a = a \circ e = a \quad \forall a \in G.$$

Invertibility:

	Inverse	
0	$0^{-1} = 1$	$0 \circ 1 = 2 = e$
$1.$	$1^{-1} = 0$	
2	$2^{-1} = 2$	

$2 \qquad 2^{-1} = 2$

Example: $G = \{1, 2, 3, 4\}$.

$a \circ b = mod(a \boxed{\cdot} b, 5)$.

Prove $(G, \circ)$ is a group.

Ans: Associativity

$(a \circ b) \circ c = mod(a \boxed{\cdot} b \boxed{\cdot} c, 5)$

$= a \circ (b \circ c)$

Identity: $e = 1$.

$e \circ a = a \circ e = a \quad \forall a \in G$.

Inverse:

$1 \qquad 1^{-1} = 1$

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

$3 \qquad 3^{-1} = 2$.

$4 \qquad 4^{-1} = 4$

$\Rightarrow$ It is a group.

Example: $G = \{1, 2, 3, 4\}$.

$$a \bullet b = \operatorname{mod}(a \boxed{\cdot} b, \underline{4}) \boxed{+} 1$$

$\hookrightarrow$ the only difference.

Prove: $(G, \bullet)$ is not a group.

Ans: Associativity:

$$(1 \cdot 3) \cdot 3 = 4 \cdot 3 = 1$$

$$1 \cdot (3 \cdot 3) = 1 \cdot 2 = 3$$

does not hold.

Theorem: If $(G, \bullet)$ is a group then e is unique.

proof: Suppose not. We have two $e \neq e'$ such that

$$\boxed{\begin{aligned} a \cdot e &= a \\ e' \cdot a &= a \end{aligned}} \begin{aligned} &= e \cdot a \\ &= a \cdot e' \end{aligned}$$

$$e' \cdot e = e' = e \quad \text{contradiction}$$

Theorem: If $(G, \circ)$ is a group.

then a^{-1} is unique for each a.

proof: suppose we have two distinct

a^{-1} and $a^{-1'}$ such that

$a \circ a^{-1} = e$ and $a^{-1'} \circ a = e$

then $a^{-1'} \cdot a \circ a^{-1} = e \cdot a^{-1} = a^{-1}$

$= a^{-1'} \circ e = a^{-1'}$

contradiction.

Theorem: If ① $(G_1, \circ_1)$ is a group.

② $|G_2| = |G_1|$,

then for any $\boxed{\text{one-to-one (bijective)}}$

mapping $f: G_1 \mapsto G_2$

mapping $f: G_1 \mapsto G_2$

We can define a new $\circ_2$ by

$$a \circ_2 b = f\left(f^{-1}(a) \circ_1 f^{-1}(b)\right).$$

and the resulting $(G_2, \circ_2)$ is also a group.

proof: Exercise.

Intuition: the labeling is <u>changed</u> but the underlying relationship is <u>preserved</u>.

Definition: Two groups $(G_1, \circ_1)$ $(G_2, \circ_2)$ are isomorphic if one can be <u>constructed</u> from the other by a relabeling <u>bijective</u> function $f: G_1 \mapsto G_2$

function $f: G_1 \mapsto G_2$

$\boxed{\text{carefully designing}}$

Example:

$G_1 = \{0, 1, 2\}$. $\quad a \circ_1 b = \operatorname{mod}(a \boxplus b, 3)$

and $G_2 = \{0, 1, 2\}$ $\quad a \circ_2 b = \operatorname{mod}(a \boxplus b \boxplus 1, 3)$

$(G_1, \circ_1)$ and $(G_2, \circ_2)$ are $\boxed{\text{isomorphic groups}}$.

Proof: exercise. Hint: find the bijective function $f: G_1 \mapsto G_2$.

Subgroups: Suppose $(G, \circ)$ is a group. We say a subset $G' \subseteq G$ is a <u>subgroup</u>

If ① $\circ$ is closed over G'.

(i.e. $a \in G'$, $b \in G'$
$\Rightarrow a \circ b \in G'$)

② $(G', \circ)$ is a group.

i.e. ① Associativity

② Identity

③ Inverse.

$\boxed{\text{Lagrange}}$ Theorem: $G_1 \subseteq G_2$ and G_1

is a subgroup of G_2

let $n = \text{order}(G_1)^{<\infty}$ and $m = \text{order}(G_2)^{<\infty}$

then $\frac{m}{n}$ is an integer

pf: Omitted.