Testing for Compositeness

Miguel Amezola

Department of Mathematics
Pacific Lutheran University

April 21, 2017

Overview

- Miller-Rabin vs Support Vector Machine Classification

Prime and Composite Numbers

Definition (Prime)

Let $p \in \mathbb{Z}$, $p > 1$. Then p is prime if and only if for every $a, b \in \mathbb{Z}$, $p = ab$ implies $a = 1$ or $b = 1$. [**?**]

Definition (Composite)

Let $n \in \mathbb{Z}, n > 1$. Then n is composite if and only if there exists $a, b \in \mathbb{Z}$ such that $n = ab, 1 < a, b < n$. [**?**]

Divisibility

Definition (Divide [?])

Let $a, d \in \mathbb{Z}$. We say that d divides a if there exists $q \in \mathbb{Z}$ such that $a = qd$. We express this in symbols as $d \mid a$ (which is read "d divides a").

The Set of All Congruence Classes I

Definition (Congruent [?])

Let $a, b, n \in \mathbb{Z}$ with $n > 0$. We say that a is congruent to b modulo n if $n \mid (a - b)$, denoted $a \equiv b \pmod{n}$.

Example

Is it true that 34 is congruent to 144 modulo 10? Subtracting 144 from 34, we have $34 - 144 = -110$. Now, does 10 divide this difference? Yes, since $-110 = -11 \cdot 10$. Thus, $34 \equiv 144 \pmod{10}$.

The Set of All Congruence Classes II

Definition (Congruence Class)

Let $a, n \in \mathbb{Z}$ with $n > 0$. We define the congruence class of a modulo n as the set of all integers congruent to a modulo n; that is,

$$\bar{a} := \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}.$$

Definition ($\mathbb{Z}_n$)

Let $n > 0$ be any integer. We define $\mathbb{Z}_n$ to be the set of all congruence classes modulo n, i.e.

$$\mathbb{Z}_n := \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}.$$

Algebraic Structures I

Definition (Binary operation)

Let S be a set. We define a binary operation on S to be a function $f : S \times S \to S$ that assigns to each pair $(a, b) \in S \times S$ a unique element $a \circ b \in S$.
A binary operation $\circ$ with the property that $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in S$ is called associative.

	Associative	**Identity**	**Inverses**	**Commutative**
Magma	Unneeded	Unneeded	Unneeded	Unneeded
Semigroup	Required	Unneeded	Unneeded	Unneeded
Monoid	Required	Required	Unneeded	Unneeded
Group	Required	Required	Required	Unneeded

Algebraic Structures II

Definition (Ring)

Let R be an abelian group. Then R is a ring if it satisfies the following axioms:

1. R forms a monoid under a second binary operation $\circ$ that distributes over the group operation, and
2. the additive identity $0 \in R$ satisfies $0 \circ a = 0$ for all $a \in R$.

Definition (Field)

Let F be a ring under two commutative binary operations. If every nonzero element in R has a multiplicative inverse, then we say F is a field.

The Structure of $\mathbb{Z}_n$ I

Table: Multiplication in $\mathbb{Z}_7$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Table: Multiplication in $\mathbb{Z}_8$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Fermat's Little Theorem I

Theorem (Fermat's Little Theorem [?])

Let p be prime, and let $\bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}$. Then

$$\bar{a}^{p-1} = \bar{1}.$$

Fermat's Little Theorem II

Proof.

Let p be prime, and let $\bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}$. By **??**, we know that $\mathbb{Z}_p$ contains a unique inverse for each of its elements. Furthermore, $\bar{1}^{-1} = \bar{1}$ and $\overline{p-1}^{-1} = \overline{p-1}$ by **??**. Thus, $\bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{p-1} = \bar{1} \cdot \overline{p-1} = \overline{p-1}$. Then

$$
\begin{aligned}
(\bar{a} \cdot \bar{1})(\bar{a} \cdot \bar{2}) \cdots (\bar{a} \cdot \overline{p-1}) &= \underbrace{\bar{a} \cdot \bar{a} \cdots \bar{a}}_{p-1 \text{ times}} \cdot \bar{1} \cdot \bar{2} \cdots \bar{a} \cdots \bar{a}^{-1} \cdots \overline{p-1} \\
&= \bar{a}^{p-1} \cdot \overline{p-1}.
\end{aligned}
$$

Moreover, since this multiplication is a binary operation, we know that each product is equal to a unique element in $\mathbb{Z}_p$. Thus, $(\bar{a} \cdot \bar{1})(\bar{a} \cdot \bar{2}) \cdots (\bar{a} \cdot \overline{p-1}) = \bar{1} \cdot \bar{2} \cdots \overline{p-1}$, where the right-hand side is some permutation of the elements in $\mathbb{Z}_p$.

Fermat's Little Theorem III

Proof (Cont.)

Hence,

$$
\begin{aligned}
\bar{a}^{p-1} \cdot \overline{p-1} &= \bar{1} \cdot \bar{2} \cdots \overline{p-1} \\
\bar{a}^{p-1} \cdot \overline{p-1} &= \overline{p-1} \\
\bar{a}^{p-1} \cdot \overline{p-1} \cdot \overline{p-1} &= \overline{p-1} \cdot \overline{p-1} \\
\bar{a}^{p-1} \cdot \bar{1} &= \bar{1} \\
\bar{a}^{p-1} &= \bar{1}.
\end{aligned}
$$

Therefore, if p is prime, then $\bar{a}^{p-1} = \bar{1}$ for all $\bar{a} \in \mathbb{Z}_p, \bar{a} \neq \bar{0}$.

Miller-Rabin Test for Compositeness I

Algorithm (Miller-Rabin Test for Compositeness)

Let $n > 0$ be any odd integer. Then there exists an integer $k > 0$ such that 2^k is that largest power of two that divides $n - 1$. If there exists $\bar{a} \in \mathbb{Z}_n$ such that

$$\bar{a}^{\frac{n-1}{2^k}} \neq \bar{1}$$

and

$$\bar{a}^{\frac{n-1}{2^h}} \neq -\bar{1},$$

for all $h \in \mathbb{Z} : 1 \leq h \leq k$, then n is composite. In this case, the integer a is called a Miller-Rabin witness to the compositeness of n.

Miller-Rabin Test for Compositeness II

Example

We would like to test the compositeness of 169. Since 2^3 is the largest power of two that divides 168, we must find an $\bar{a} \in \mathbb{Z}_{169}$ such that $\bar{a}^{\frac{168}{2^3}} \neq \bar{1}$ and $\bar{a}^{\frac{168}{2^h}} \neq -\bar{1}$ for all h, $h = 1, 2, 3$. So, we randomly choose $\overline{19} \in \mathbb{Z}_{169}$ and find that

$$\overline{19}^{\frac{168}{2^3}} = \overline{70}$$

$$\overline{19}^{\frac{168}{2^2}} = -\bar{1}$$

$$\overline{19}^{\frac{168}{2^1}} = \bar{1}.$$

Miller-Rabin Test for Compositeness III

Example

Because $\overline{19}^{\frac{168}{2^2}} = -\overline{1}$, we cannot conclude that 169 is composite. So we randomly select a different $\overline{a} \in \mathbb{Z}_{169}$, namely $\overline{a} = \overline{145}$, and this time discover that

$$\overline{145}^{\frac{168}{2^3}} = \overline{18}$$
$$\overline{145}^{\frac{168}{2^2}} = \overline{155}$$
$$\overline{145}^{\frac{168}{2^1}} = \overline{27}.$$

Hence, 145 is a Miller-Rabin witness to the compositeness of 169 and we conclude that 169 is not prime.

Effectiveness of the Miller-Rabin Test

Machine Learning Algorithms

- Target function — underlying function that maps inputs to outputs (if it exists)
- Solution — estimate of the target function by learning algorithm (also called the decision function in classification algorithms)
- Hypothesis space — a set or class of candidate solutions (known as hypotheses)
- Learning algorithm — uses training data to select a hypothesis
- Features — the quantities used to describe the data
- Attributes — original quantities from data

Linear Classification

Support Vector Machine

Feature Space

Let $b \in \mathbb{Z} : b \geq 2$. Then every $N \in \mathbb{Z} : N > 0$ can be expressed uniquely in the form $N = a_k b^k + a_{k-1} b^{b-1} + \cdots + a_1 b + a_0$, where $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b, $a_k \neq 0$, and $k \geq 0$. [**?**]

Training Methodology

Definition (Training Set)

A **training set** is a collection of training examples, which are also called training data. It is usually denoted by $S = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\} \subset X \times Y$, where n is the number of examples. We refer to x_i as examples or instances and y_i as their labels.[**?**]

Comparison

References

Acknowledgements