LECTURE 1
9/2/2019

ADMINISTRIVIA:

LECTURER: MADHU SUDAN
TAS: CHRISTINA ILVENTO
SANTHOSHI VELUSAMY

ONLINE SUF:

- http://madhu.seas.harvard.edu/courses/Fall2019:
  handouts, notes, etc. — please bookmark.

- links also to Piazza — most announcements + discussion
  Canvas — to submit PSETs.

- Sign up on Piazza; verify Canvas site award

OH:
- First week: Madhu — 1-2pm on Friday

Special section: First week only
F 11am — Northwest B150
F 2pm — MD 123
Course Overview

- Applied Algebra
  - Standard: as in Math 122, 123
  - More algorithmic, constructive.

Example: \[ 3x^5 + 2x^2 - 27 = 0 \]

- Usual Algebra: "Has at most 5 real roots" or even "Has 1, 3, 5 roots".

- Constructive question: How many?
  How to find them (starting from coefficients)

- Motivated by applications.
  - Crystallography \( \subseteq \) group theory
  - Cryptography \( \subseteq \) group theory
  - Error-correcting \( \subseteq \) Ring theory

= Algebra =? study of sets + operations on sets (esp. binary)

  eg. Integers: Addition
  Integers: Multiplication
Many other such:
- (Integers, Add II Mult.)
- \( \mathbb{R} \) ?
- Matrices ;
- Polynomials ;
- Vectors ; Add.
- Binary strings ; Bitwise XOR
- Permutations ; Composition

\[
\begin{array}{c|c|c|c}
+ & 0 & 1 \\
\hline
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array}
\]

Power of abstraction: (Assume few properties, some others follow).

- e.g. How many solutions to

\[
\begin{array}{c}
X_1 \oplus X_2 \oplus X_3 \oplus X_4 \oplus X_5 = 0 \\
X_1 \oplus X_2 \oplus X_5 = 1 \\
X_2 \oplus X_3 = 0 \\
\end{array}
\]

(\text{with } X_1 \ldots X_5 \in \{0,1\})

- Answer: \( \boxed{4} \). How? Why?

\text{Warning/Encouragement: Poor based cause !!}!!!
Administrivia

Grading: 
- Weekly Psets: 45%
- 4 psets, 1 drop.
- Lateness, Collaboration - see announcements.
  * Not including P50 - 0 points.
- PSETS typically out Friday; Due 7 weeks later.
- Rest of grade
  - 3 Exams: 
    - Q1 10/3/19 - In class 15%
    - Q2 11/12/19 - In class 15%
    - Final 12/12 - up to registrar, 20%
- Participation - lectures, OIT, Plaza - 5%

Warning/Encouragement: Some coding on PSETS.
Quick outline:

- 3 lectures: Preliminaries: Induction, Integers, Algorithms
  - 1 section: Coding, Oh notation.
  - this Friday

- 9 lectures: Groups (Sets w. one binary op.)

- 9 lectures: Rings/Fields (Set w. two binary op.)

Side Outcomes:
- Solidify your "proof-based math"
- Start more "coding"
Induction:

- Key proof technique in discrete math.
- How to prove that some statement holds for all integers?
- Example: "for every positive integer \( n \),
  \[
  1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}
  \]"

[Notational aside:
- \( \mathbb{N} = \{0, 1, 2, \ldots \} \rightarrow \) "natural numbers"
  (in this class)
  sometimes \( \mathbb{N}^* \)
- \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots \} \rightarrow \) integers
- "\( \forall \) \( x \in S \)" for every \( x \) in \( S \)...
- "\( \exists \) \( x \in S \)" there exists (at least one) \( x \) in \( S \)"

Prop: \( \forall n \in \mathbb{N} \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \)

Prop: \( \forall n \in \mathbb{N} \sum_{i=0}^{n} i = \frac{n(n+1)(n+2)}{2} \)
Induction: 3 related statements.

1. Standard Induction
   a. \( o \in S \)
   b. \( \forall n \in \mathbb{N} \; n \notin S \Rightarrow (n+1) \in S \)
   \( \Rightarrow \) c. \( \mathbb{N} \subseteq S \) [if presence of \( n \) in \( S \) implies presence of \( n+1 \), then \( \mathbb{N} \subseteq S \)]

2. Strong Induction
   a. \( o \in S \)
   b. \( \exists n \in \mathbb{N} \; (\exists o, \ldots, n \in S \Rightarrow (n+1) \in S) \)
   \( \Rightarrow \) c. \( \mathbb{N} \subseteq S \) [if presence of all numbers less than \( n \) in \( S \) implies \( n \) in \( S \), then \( \mathbb{N} \subseteq S \)]

3. Well-ordering Principle
   "\( \forall T \subseteq \mathbb{N} \) \( \exists m \in T \) s.t. \( \forall n \in T \) \( m \leq n \)
   [every non-empty set of \( \mathbb{N} \) has a minimum element]

\( 1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1 \)
Application of Induction

Prop: \[ \sum_{i=0}^{n} i = \frac{n(n+1)}{2} \]

\[ \text{Induction: } S \equiv \text{all } n \text{ for which statement holds} \]
\[ \text{Strong Induction: } S \equiv \]
\[ \text{Well-ordering: } T \equiv \text{all } n \text{ for which statement does NOT hold.} \]

Proof: Base Case: \( n=0 \); \[ \sum_{i=0}^{0} i = 0 = 0 \cdot (0+1) \]

Inductive Step: Assume \[ \sum_{i=0}^{n} i = \frac{n(n+1)}{2} \quad [n \in S] \]

Want to Prove \[ \sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2} \]

\[ \sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1) = \frac{n(n+1)}{2} + (n+1) \]

\[ = \left( \frac{n+1}{2} \right) \left[ n + 2 \right] \]