CSE 312

Foundations of Computing II

Lecture 1: Welcome & Introduction

PAUL G. ALLEN SCHOOL OF COMPUTER SCIENCE & ENGINEERING

Stefano Tessaro

tessaro@cs.washington.edu

Foundations of Computing II

=

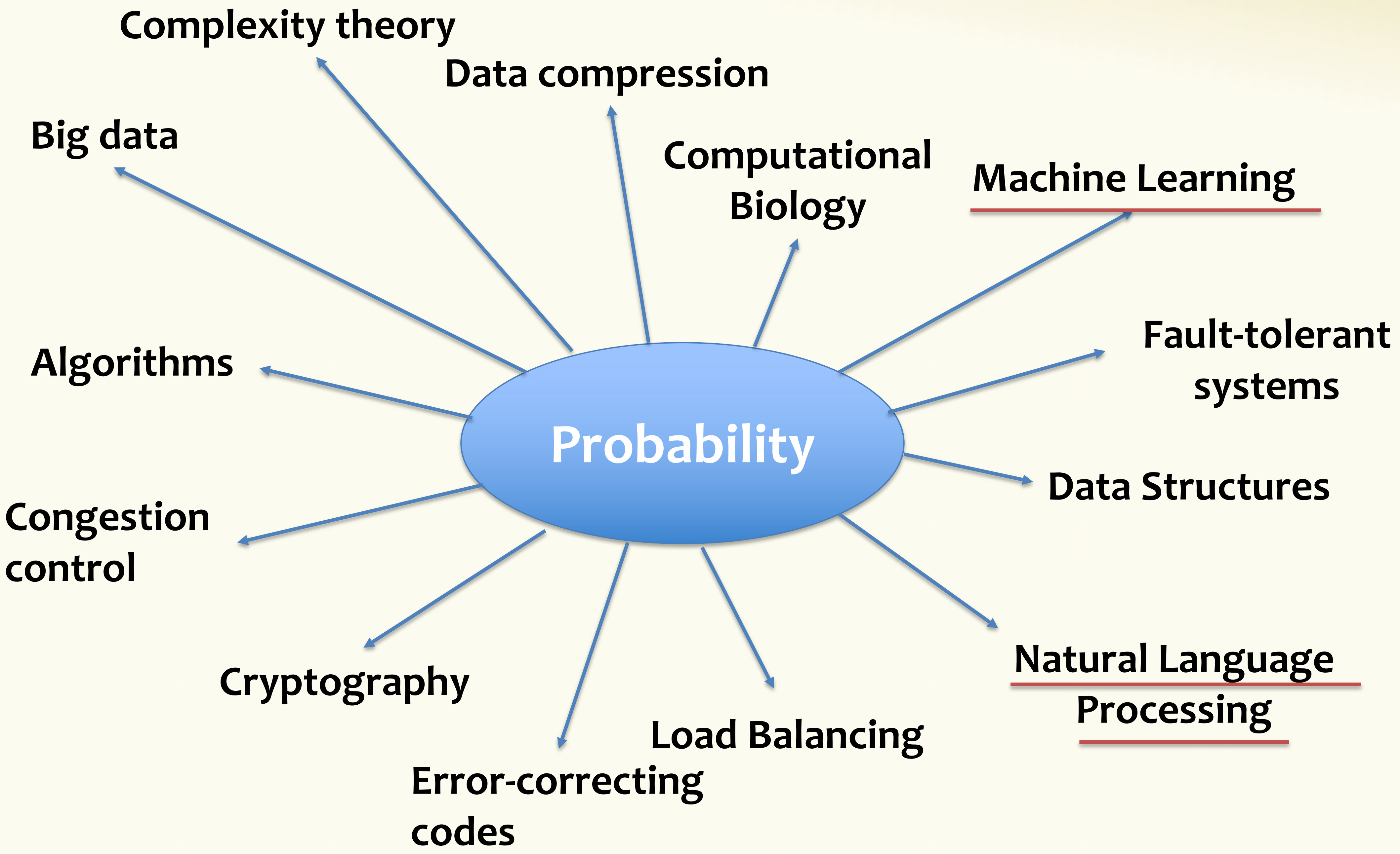
Introduction to Probability & Statistics

for computer scientists

What is probability??

Why probability?!

+ much more!



Complexity theory
Data compression
Big data
Computational Biology
Machine Learning
Algorithms
Fault-tolerant systems
Probability
Data Structures
Congestion control
Natural Language Processing
Cryptography
Load Balancing
Error-correcting codes

CSE 312 team

Cryptographer, Associate Professor @ Allen School since Jan 2019.

Stefano Tessaro
tessaro@cs

Leonid Baraznenok
barazl@cs

Duowen (Justin) Chen
chendw98@cs

Kushal Jhunjhunwalla
kushaljh@cs

Tina Kelly Li
tinakli@cs

Siva N. Ramamoorthy
sivanr@cs

Su Ye
yes23@cs

Zhanhao Zhang
zhangz73@cs

Most important info

https://courses.cs.washington.edu/courses/cse312/19au/

tl;dr:

- **Weekly Homework,** starting next week, Wed – Wed schedule. Submissions via Gradescope only, individual submissions.
- **Weekly Quiz Sessions**, starting tomorrow. Short review + in-class assignment, posted one day in advance. Do attend them.
- Office hours on M/T/W.
- Midterm on **Friday 11/1**.
- Grade (approx.): 50% HW, 15% midterm, 35% final
- **Panopto is activated – not a replacement for class attendance!**

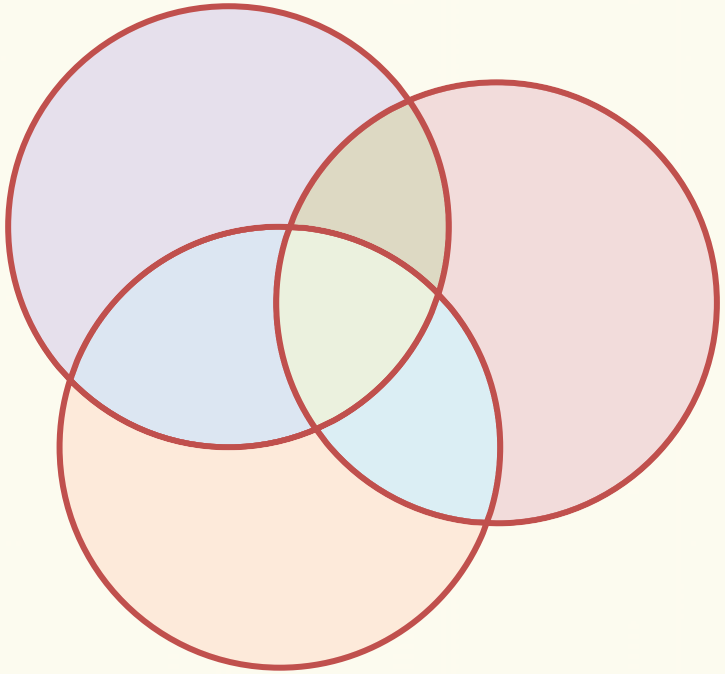
Class materials + textbook

Mandatory textbook: Dimitri P. Bertsekas and John N. Tsitsiklis, *Introduction to Probability*, First Edition, Athena Scientific, 2000. [Available for free!]

Optional: Kenneth H. Rosen, *Discrete Mathematics and Its Applications*, McGraw-Hill, 2012.

I will use slides. These will be available online.

Review: Sets and Sequences



Sets

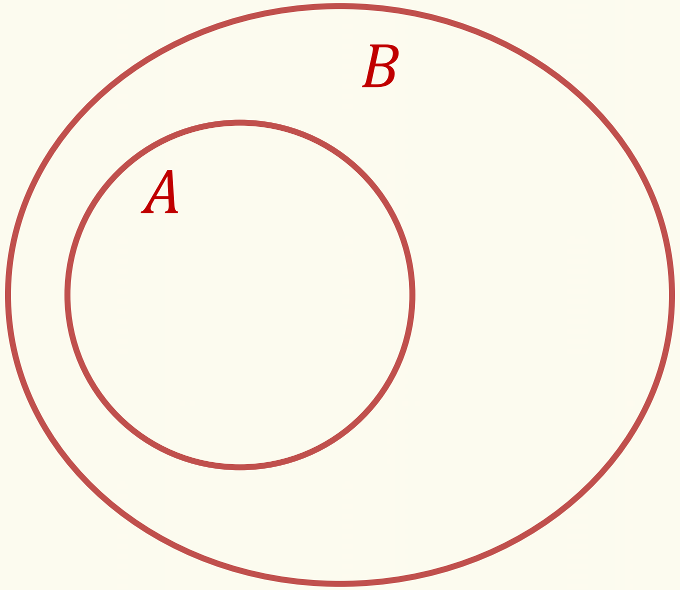
"Definition." A **set** is a collection of (distinct) elements from a **universe** Ω.

Order irrelevant: $\{1,2,3\} = \{3,1,2\} = \{3,2,1\} = \{1,3,2\} = \cdots$
No repetitions: $\{1,2,2,3\} = \{1,2,3\}$

Notation:

- $x \in S$: x belongs to / is an element of S
- $x \notin S$: x does not belong to / is not an element of S
- $|S|$: size / cardinality of S

Subsets / set inclusion



Definition. $A \subseteq B$ if $\forall x: x \in A \Rightarrow x \in B$

Examples:
- $\{1,2,3\} \subseteq \{1,2,3,5\}$
- $\{1,2,3\} \subseteq \{1,2,3\}$
- $\{1,2,3\} \nsubseteq \{1,2,4\}$

Definition. $A \subset B$ if $A \subseteq B \wedge A \neq B$

Examples:
- $\{1,2,3\} \subset \{1,2,3,5\}$
- $\{1,2,3\} \not\subset \{1,2,3\}$
- $\{1,2,3\} \not\subset \{1,2,4\}$

Common sets

- **Empty set:** $\emptyset$
- **First n integers:** $[n] = \{1,2, \dots, n\}$
- **Integers:** $\mathbb{Z} = \{\dots, -3, -2, -1,0,1,2,3, \dots\}$
- **Naturals:** $\mathbb{N} = \{0,1,2,3, \dots\}$
- **Reals:** $\mathbb{R}$ (aka. points on the real line)
- **Rationals:** $\mathbb{Q} = \left\{ \frac{a}{b} \in \mathbb{R} \,\middle|\, a, b \in \mathbb{Z}, b \neq 0 \right\}$

finite sets

countable

infinite sets

uncountable

Implicit descriptions

Often, sets are described implicitly.

$$S_1 = \{a \in \mathbb{N} \mid 1 \leq a \leq 7\}$$

unambiguous

What is this set? $S_1 = \{1,2,3,4,5,6,7\}$

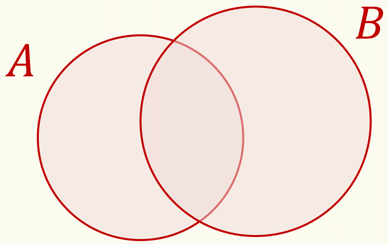
$$S_2 = \{a \in \mathbb{N} \mid \exists k \in \mathbb{N} : a = 2k + 1\}$$

What is this set? $S_2 = \{1,3,5,7,\ldots\}$ = the odd naturals

ambiguous

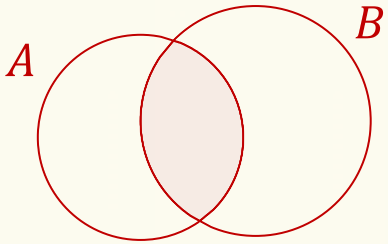
Set operations

$$A \cup B = \{x \mid x \in A \lor x \in B\}$$



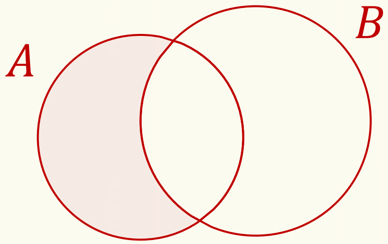
set union

$$A \cap B = \{x \mid x \in A \land x \in B\}$$



set intersection

$$A \setminus B = \{x \mid x \in A \land x \notin B\}$$



set difference

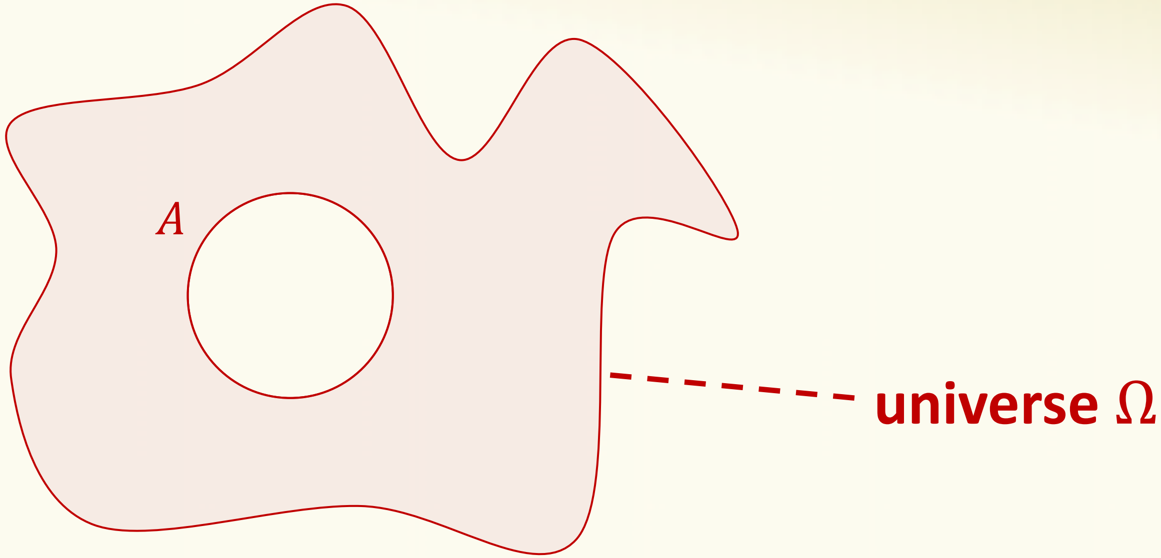
[Sometimes also: $A - B$]

Set operations (cont'd)

$$A^c = \{x \mid x \notin A\} = \Omega \setminus A$$

set complement

[Sometimes also: $\bar{A}$]



Fact 1. $(A^c)^c = A$.

Fact 2. $(A \cup B)^c = A^c \cap B^c$.

Fact 3. $(A \cap B)^c = A^c \cup B^c$.

"De Morgan's Laws"

Sequences

A (finite) **sequence** (or **tuple**) is an (ordered) list of elements.

Order matters: $(1,2,3) \neq (3,2,1) \neq (1,3,2)$
Repetitions matter: $(1,2,3) \neq (1,2,2,3) \neq (1,1,2,3)$

Definition. The **cartesian product** of two sets S, T is

$$S \times T = \{(a, b) : a \in S, b \in T\}$$

Equivalent naming: 2-sequence = 2-tuple = ordered pair.

Cartesian product – cont'd

Definition. The **cartesian product** of two sets S, T is

$$S \times T = \{(a, b) : a \in S, b \in T\}$$

Example.

$$\{1,2,3\} \times \{\bigstar, \spadesuit\} = \{(1,\bigstar), (2,\bigstar), (3,\bigstar), (1, \spadesuit), (2, \spadesuit), (3, \spadesuit)\}$$

Cartesian product – even more notation

$S \times T \times U = \{(a, b, c) : a \in S, b \in T, c \in U\}$

$S \times T \times U \times V$

…

Notation. $S^k = \underbrace{S \times S \times \cdots \times S}_{k \text{ times}}$

Next – Counting (aka ”combinatorics”)

We are interested in counting the number of objects with a certain given property. [Weeks 0-1]

"How many ways are there to assign 7 TAs to 5 sections, such that each section is assigned to two TAs, and no TA is assigned to more than two sections?"

"How many integer solutions $(x, y, z) \in \mathbb{Z}^3$ *does the equation* $x^3 + y^3 = z^3$ *have?"*

Generally: Question boils down to computing cardinality $|S|$ of some given (implicitly defined) set S.

Example – Strings

How many string of length 5 over the alphabet $\{A, B, C, \ldots, Z\}$ are there?

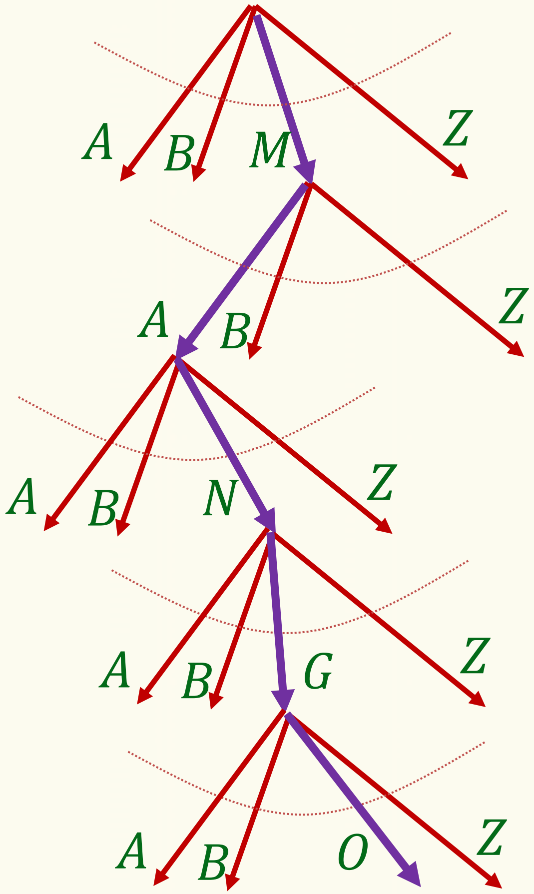
- E.g., AZURE, BINGO, TANGO, STEVE, SARAH, …

26 options 26 options

String = $\boxed{M}\ \boxed{A}\ \boxed{N}\ \boxed{G}\ \boxed{O}$

26 options

26 options 26 options



Answer: $26^5 = 11881376$

Product rule – Generally

$$\boxed{|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \times |A_2| \times \cdots \times |A_n|}$$

Example – Strings

How many string of length 5 over the alphabet $\{A, B, C, \dots, Z\}$ are there?

- E.g., AZURE, BINGO, TANGO, STEVE, SARAH, …

$$\left|\{A, B, C, \dots, Z\}^5\right| = |\{A, B, C, \dots, Z\}|^5 = 26^5.$$

Product rule

Example – Laptop customization

Alice wants to buy a new laptop:

- The laptop can be **blue**, **orange**, **purple**, or **silver**.
- The SSD storage can be **128GB**, **256GB**, and **512GB**
- The available RAM can be **8GB** or **16GB.**
- The laptop comes with a **13"** or with a **15"** screen.

How many different laptop configurations are there?

Example – Laptop customization (cont'd)

$C = \{$**blue**, **orange**, **purple**, **silver**$\}$

$D = \{$**128GB, 256GB, 512GB**$\}$

$R = \{$**8GB, 16GB**$\}$

$S = \{$**13", 15"**$\}$

Configuration = element of $C \times D \times R \times S$

$$\# \text{ configurations} = |C \times D \times R \times S|$$

Product rule

$$= |C| \times |D| \times |R| \times |S|$$

$$= 4 \times 3 \times 2 \times 2 = 48.$$

Example – Power set

Definition. The **power set** of S is

$$2^S = \{X \mid X \subseteq S\}.$$

Example. $2^{\{\bigstar,\spadesuit\}} = \{\emptyset, \{\bigstar\}, \{\spadesuit\}, \{\bigstar, \spadesuit\}\}$

$2^{\emptyset} = \{\emptyset\}$

…

Proposition. $|2^S| = 2^{|S|}$.

Proof of proposition

(Case $S = \emptyset$ needs to be handled separately)

Proposition. $|2^S| = 2^{|S|}$.

Let $S = \{s_1, \ldots, s_n\}$ (i.e., $|S| = n \geq 1$)

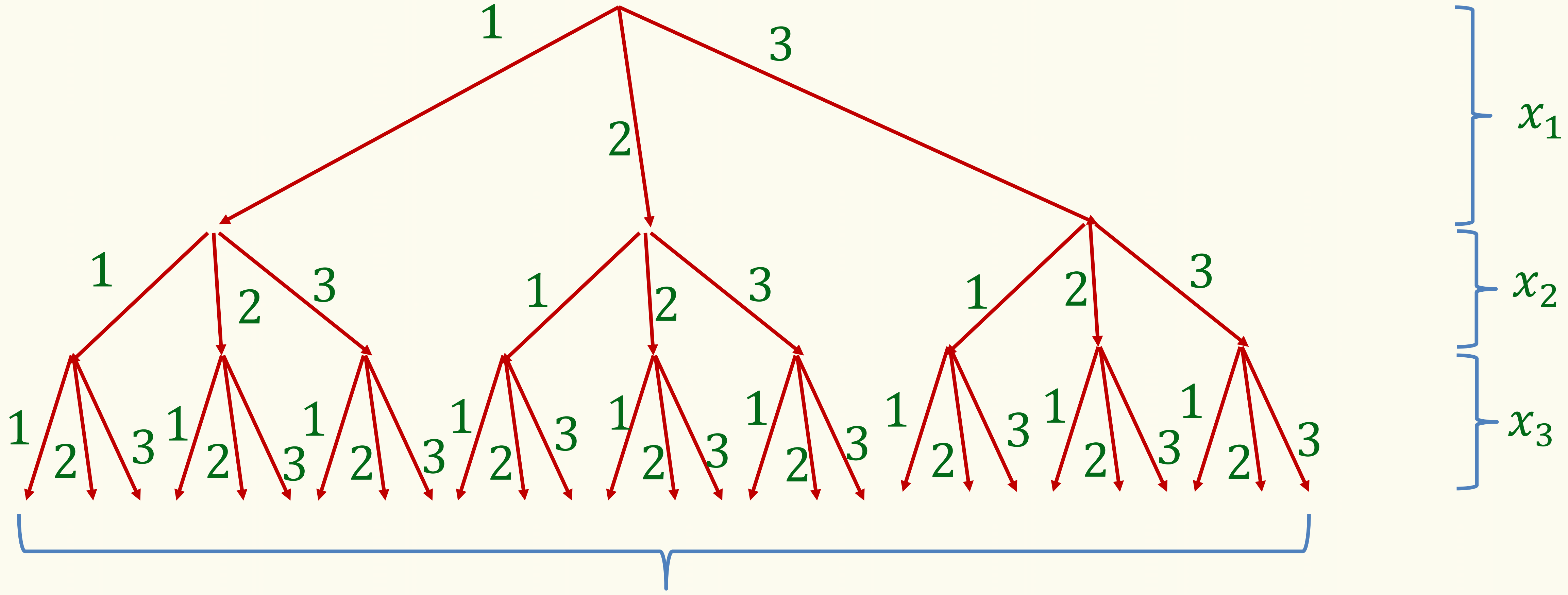
subset $X \subseteq S$ $\xleftrightarrow{\text{1-to-1 correspondence}}$ <u>sequence</u> $1_X \in \{0,1\}^n$

$$1_X = (x_1, \ldots, x_n) \text{ where } x_i = \begin{cases} 1 & \text{if } s_i \in X \\ 0 & \text{if } s_i \notin X \end{cases}$$

Therefore: $|2^S| = |\{0,1\}^n| \underbrace{=}_{\text{Product rule}} |\{0,1\}|^n = 2^n$ ∎

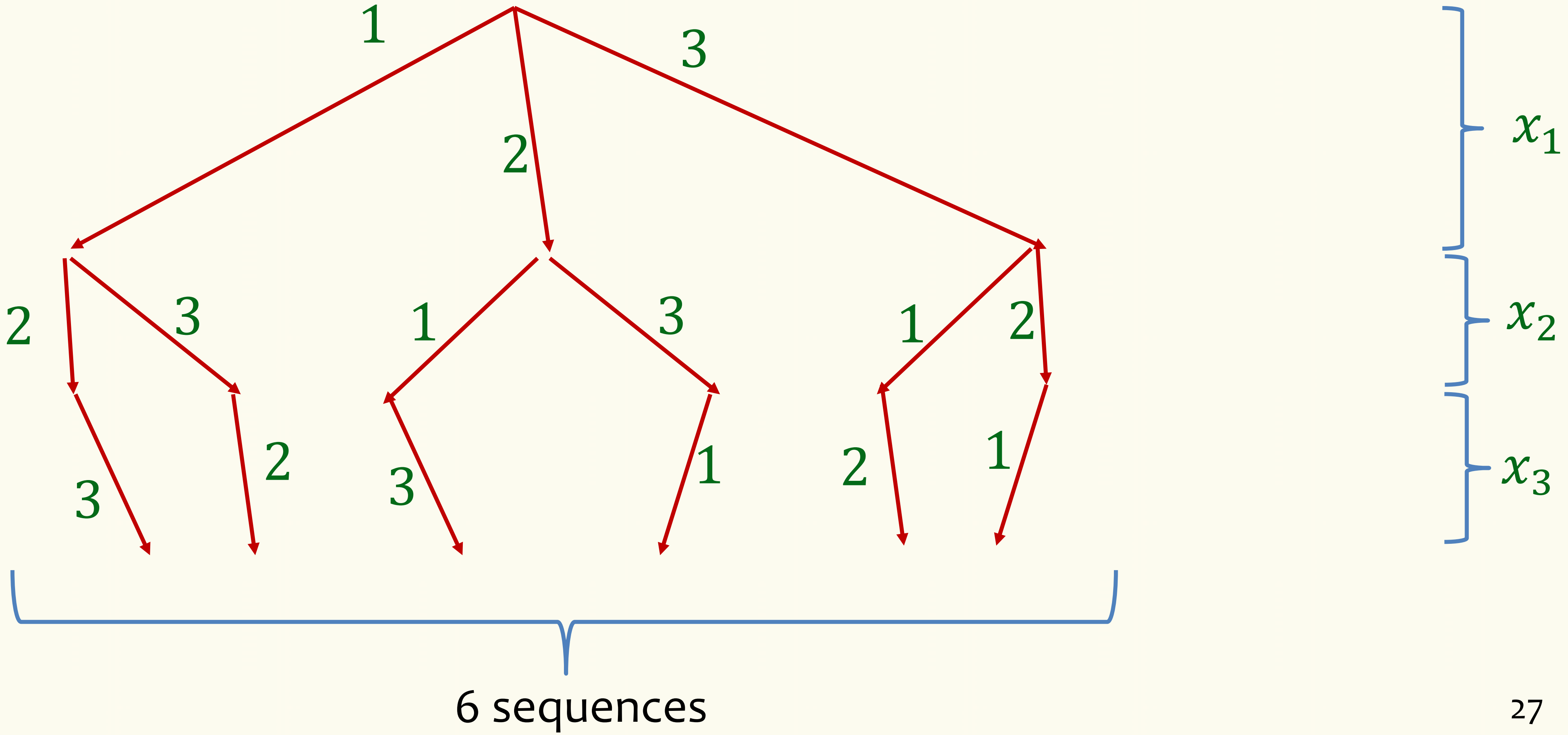
Sequential process: We fix elements in a sequence one by one, and see how many possibilities we have at each step.

Example: "How many sequences are there in $\{1,2,3\}^3$?"



27 paths = 27 sequences

Example: "How many sequences are there in $\{1,2,3\}^3$ with no repeating elements?"



Factorial

"How many sequences in $[n]^n$ with no repeating elements?" **"Permutations"**

Answer = $n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1$

Definition. The **factorial function** is

$$n! = n \times (n-1) \times \cdots \times 2 \times 1\,.$$

Theorem. (Stirling's approximation)

$$\underbrace{\sqrt{2\pi}}_{=\,2.5066} \cdot n^{n+\frac{1}{2}} \cdot e^{-n} \le n! \le \underbrace{e}_{=\,2.7183} \cdot n^{n+\frac{1}{2}} \cdot e^{-n}\,.$$