Discrete Structures

Lecture 17: Counting and probability

Susan L. Epstein

HUNTER

1

Last time

★ **Simple examples yield intuition for hypotheses**

- How compositionality works
- How to build proofs with 1-to-1 functions, onto functions, and 1-to-1 correspondences
- What cardinality is
- How to measure the size of infinite sets

2

Today's outline

- Sample spaces and probability
- Learning to count
- The multiplication rule

Sequential decisions multiply possibilities

3

Useful facts

A coin has 2 sides: heads and tails 

A standard die has 6 sides numbered from 1 to 6 

A standard deck has 52 cards in 4 suits
Hearts and diamonds are red suits
Clubs and spades are black suits
13 cards in a suit
Face values (aka denominations) in every suit: 2,3,4,5,6,7,8,9,10,J,Q,K,A
There are 4 different cards with each face value
J(ack),Q(ueen),K(ing) are picture cards

4

Events and sample spaces

- Experiment may have happened (and produced an outcome) or may have not yet occurred but will produce an outcome

roll a die   pick a card   flip a coin



- Sample space S = set of all possible distinct outcomes of an experiment
- Event E = any subset of sample space

roll a 3   pick a diamond   heads

- Random variable = function defined on a sample space

5

Fundamentals

- CSCI 150 assumes sample space S is finite

$\{1,2,3,4,5,6\}$



{heads,tails}

6   52   2

- How many possible outcomes are there in S?

$|S|$ size of sample space

- Event space $\mathcal{P}(S)$ is the set of all possible events in S

{5, even, <3,…}   {red,diamond,picture,…}   {∅,heads,tails,both}

- How many possible events are there in S?

$|\mathcal{P}(S)|$ size of event space

$|\mathcal{P}(S)| =$ 2^6 2^{52} 2^2

- Each outcome $s \in S$ has some likelihood that it will occur

6

Kolmogorov's axioms

- Probability function $P: \mathcal{P}(S) \rightarrow [0,1]$ assigns some $r \in [0,1]$ to each possible event
- E is impossible iff $P(E) = 0$
- E is certain iff $P(E) = 1$

For all events A and B in S

No rational agent violates these axioms
[De Finetti, Cox, and Carnap]

- $0 \leq P(A) \leq 1$
- $P(\emptyset) = 0$ and $P(S) = 1$

Experiment is "flip a coin" $S =$ {heads, tails}
Probability of getting no outcome is 0
Probability of getting some outcome is 1

- If A and B are disjoint ($A \cap B = \emptyset$) then $P(A \cup B) = P(A) + P(B)$

Probability of getting heads or tails is P(heads) + P(tails)
Disjoint events in roll 1 die: $A =$ even number, $B =$ odd number
Not disjoint in roll a die: $A \geq 3, B \leq 3$
Disjoint in pick a card: $A =$ red, $B =$ black
Not disjoint in pick a card: $A =$ red, $B =$ picture

7

Using the axioms

- Each outcome $s \in S$ has some likelihood that it will
- Outcomes are by definition disjoint $S = \{A_1, A_2, \ldots, A_n\}$ so
  If $A \cap B = \emptyset$ then $P(A \cup B) = P(A) + P(B)$ and $P(S) = 1$ implies
  $\sum_{i=1}^{n} P(A_i) = 1$
- If all outcomes $s \in S$ have the same likelihood, they are equally likely (aka object is fair)

$S =$ {heads, tails}   A fair coin has P(heads) = P(tails)
Kolmogorov: $P(\emptyset) = 0$, P({heads, tails}) = 1
so P(heads) + P(tails) = 1 and P(heads) = P(tails) = $\frac{1}{2}$

Fair die has $P(1) = P(2) = P(3) = P(4) = P(5) = P(6) = \frac{1}{6}$

- Probability $P(E)$ of any event $E \subseteq S$ with equally likely outcomes = $\frac{|E|}{|S|}$

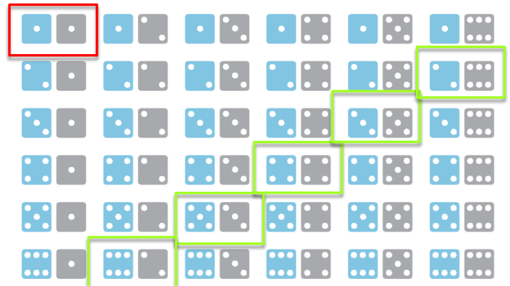
P(roll < 3)	P(pick diamond)	P(pick even red card)
$\frac{2}{6}$	$\frac{13}{52}$	$\frac{10}{52}$

If you really care about what number results, use a computer.
What CSCI cares about is your thought process

8

A more interesting experiment

- Roll a pair of fair dice, one blue and one gray, and add their values
- $|S|$=?
- What is the probability of rolling a 2?
- If E ={8}, $|E|$ =?
- What is the probability of rolling an 8?



Today's outline

- ✓ Sample spaces and probability
- Learning to count
- The multiplication rule

Introduction to counting

- Combinatorics = the branch of mathematics concerned with counting
- Assume that the available items are distinct unless told otherwise
- Think about the counted items as constructed one part at a time
- What's the set you can choose from?
- Can you reuse an item?

How many numbers?

- How many integers are there from 1 to 10?
- How many from 31 to 35?
- How many from 122 to 133?
- For integers $m \leq n$ how many integers are there from m to n?

Theorem: Let $P(n)$ be for $m, n \in \boldsymbol{Z}, m \leq n$, there are $n - m + 1$ integers from m to n inclusive.
Proof by induction after the closing slide in this slide set.

Counting the elements of a sublist

Find a pattern that can be placed in 1-to-1 correspondence with the elements of the sublist

How many 3-digit integers are divisible by 5?

100	101	102	103	104	105	106	107	108	109	110	$\cdots$	994	995	996	997	998	999
$\updownarrow$					$\updownarrow$					$\updownarrow$			$\updownarrow$				
$5\cdot 20$					$5\cdot 21$					$5\cdot 22$			$5\cdot 199$				

Why do the arrows stop at 995?

Now how many integers are between 20 and 199 inclusive?

$$199 - 20 + 1$$

What is the probability that a 3-digit integer is divisible by 5?

$$\frac{199 - 20 + 1}{999 - 100 + 1}$$

If you really care about what number results, use a computer.
What CSCI cares about is your thought process

Application: counting for an array

- Subdivide array A with elements $A[1], A[2], \ldots, A[n]$ at midpoint m
  $A[1], A[2], \ldots, A[m]$ and $A[m+1], A[m+2], \ldots, A[n]$
  To code this, why can't we just take $m = \frac{n}{2}$?
- For efficiency, algorithms often put their data in an array
- Items in an array are indexed, so can count them as if they were a list
  What is the probability that n is even?

1	2	3	4	5	6	7	8	9	10	$\cdots$	n
	$\updownarrow$		$\updownarrow$		$\updownarrow$		$\updownarrow$		$\updownarrow$		$\updownarrow$
	$2\cdot 1$		$2\cdot 2$		$2\cdot 3$		$2\cdot 4$		$2\cdot 5$		$2\cdot n/2$

$$\frac{\frac{n}{2} - 1 + 1}{n} = \frac{n/2}{n}$$

What is the probability that n is odd?

1	2	3	4	5	6	$\cdots$	$n-1$	n
	$\updownarrow$		$\updownarrow$		$\updownarrow$		$\updownarrow$	
	$2\cdot 1$		$2\cdot 2$		$2\cdot 3$	$\cdots$	$2\cdot(n-1)/2$	

$$\frac{\frac{n-1}{2} - 1 + 1}{n} = \frac{(n-1)/2}{n}$$

Can combine these as $\frac{\lfloor n/2 \rfloor}{n}$

Any questions?

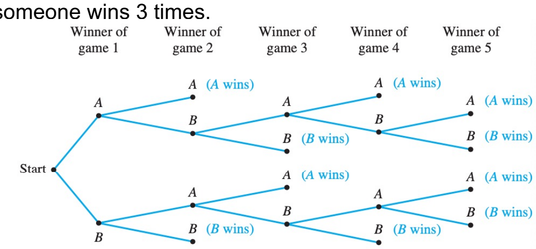
Today's outline

- ✓ Sample spaces and probability
- ✓ Learning to count
- The multiplication rule

15

Example 1

In a tournament, 2 players, A and B, play a game until someone wins 2 in a row or someone wins 3 times.

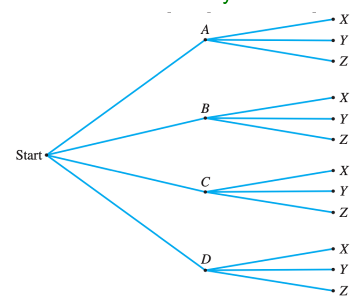


This **possibility** tree clarifies the ways the tournament can happen
How many ways can the tournament end?
What's the probability that they play 5 games? $\frac{4}{10}$
In how many 5-game tournaments does A win? $\frac{2}{10}$

16

Example 2

A restaurant offers 4 main courses (A, B, C, D) and 3 desserts (X, Y, Z).
How many different 2-course meals can you order there?



There's a rule to shortcut this variety of possibility tree…

Strings

- Character = element in a set of symbols
  - There are 10 digits (aka numeric characters) $\{0,1,2,3,4,5,6,7,8,9\}$
  - There are 26 letters in the alphabet used in CSCI 150: $\{A, B, C, \dots, Z\}$
  - For our purposes, there are 5 vowels $\{A, E, I, O, U\}$
  - There are 36 alphanumeric characters
    $\{0,1,2,3,4,5,6,7,8,9, A, B, C, \dots, Z\}$

- If S is a non-empty finite set of characters, then a string is a finite sequence of elements of S rabbit ILoveCSCI
  - The length of the sequence is the length of the string
  - The null string has no characters and length 0

Multiplication rule

If a process consists of k steps and
- the first step can be performed in n_1 ways
- the second step can be performed in n_2 ways (no matter what step 1 was)
- …
- the kth step can be performed in n_k ways (no matter what the earlier steps were)

Then the entire process can be performed in $n_1 n_2 \cdots n_k$ ways

Think about what items to count as the result of a process that builds them

letters in a name	How many 10 letter first names are there? 26^{10}
digits in your CUNYFirst ID	How many students can there be? 10^{8}
Alphanumeric characters on a license plate	How many 7-character plates can there be? 36^{7}

Practice

A store carries 8 styles of pants. For each style there are 10 different waist sizes, 6 pants lengths, and 4 color choices. What is the minimum number of different pants the store must have in stock?

$$8 \cdot 10 \cdot 6 \cdot 4$$

How many election outcomes are possible with 20 people each voting for one of 7 candidates? (The outcome includes not just the totals but also who voted for each candidate.)

Imagine them arriving at the polling place one at a time.

$$7^{20}$$

How many if only one person votes for candidate A and only one person votes for candidate D?

Get the votes for A and D in first.

$$20 \cdot 19 \cdot 5^{18}$$

$|\mathcal{P}(S)|$

- How many subsets of a set S are there?
- Think of it as a counting problem that builds a subset
- You could do that by asking if each element of the set is in or out of the subset you are building
- If $|S| = n$ then how many times would you have to ask that question?
- And how many answers could you get to each question?

That is why

$$|\mathcal{P}(S)| = 2^n$$

21

More counting examples

How many 5-place alphanumeric PINs are there?

$$36^5$$

How many passwords of length 10 are there, using alphanumeric characters and the special characters @?#$%& ?

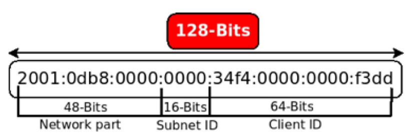
$$42^{10}$$

How many elements are there in the Cartesian product $A_1 \times A_2 \times \ldots \times A_n$?

$$|A_1| \cdot |A_2| \cdots |A_n|$$

IPv6 addresses are 128 bits long.

How many different networks can they support? 2^{48}



How many subnets per network?

2^{16}

How many clients per subnet?

2^{64}

How many addresses?

$2^{48} \cdot 2^{16} \cdot 2^{64}$

22

Avoiding duplicates (aka without repetition)

To avoid duplicates, temporarily remove a choice from a set to build the rest of the item

There were 36^5 5-place alphanumeric PINs. What would that count be if no duplicate characters were allowed? Hint: _ _ _ _ _

$$36 \cdot 35 \cdot 34 \cdot 33 \cdot 32$$

What's the probability that one of those PINs has no duplicate characters?

$$\frac{36 \cdot 35 \cdot 34 \cdot 33 \cdot 32}{36^5}$$

There were 42^{10} passwords of length 10, using alphanumeric characters and the special characters @?#$%& What would that count be if no duplicate characters were allowed?

$$42 \cdot 41 \cdot 40 \cdot 39 \cdot 38 \cdot 37 \cdot 36 \cdot 35 \cdot 34 \cdot 33$$

What's the probability that one of those has no duplicate characters?

$$\frac{42 \cdot 41 \cdot 40 \cdot 39 \cdot 38 \cdot 37 \cdot 36 \cdot 35 \cdot 34 \cdot 33}{42^{10}}$$

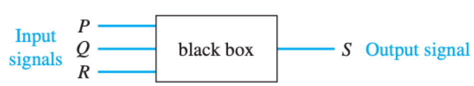
If you really care about what number results, use a computer.
What CSCI cares about is your thought process

Fall 2023 CSCI 150 23/26

23

How many circuits can we build with 3 inputs?

- Recall that we built an input/output table to describe the way a black box behaved
- Circuits that are distinct must have a different Output column for Input columns in the usual (binary countdown) order
- So the number of circuits on 3 binary inputs is the number of wavs we can write an 8-place binary number 2^3



Input			Output
P	*Q*	*R*	*S*
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	0

- How many truth table are there on 3 variables? 2^3
- How many boolean functions are there on 3 arguments? 2^3
- How many boolean functions are there on n arguments? 2^n

Fall 2023 CSCI 150a 24/26

24

Iterations in a nested loop

How many times do the statements in the inner loop execute?

for *i* := 1 to 4
  for *j* := 1 to 3
    [*Statements in body of inner loop. None contain branching statements that lead out of the inner loop.*]
  next *j*
next *i*

i	1 →		→	2 →		→	3 →		→	4 →		→
j	1	2	3	1	2	3	1	2	3	1	2	3

3 + 3 + 3 + 3 = 12

Proof methods (so far)

Truth table
Sequence of statements with reasons
Logic (modus ponens, modus tollens,…)
Predicate logic (quantification, vacuous truth)
Generalization from the generic particular
Proof by contradiction
Proof by contraposition
Proof by cases
Mathematical induction
Strong mathematical induction
Proof by set element
Algebraic set proof
Algebraic proof by properties of functions
Cardinality proof by one-to-one correspondence
Algebraic proof by combinatorics

What you should know

Sequential decisions multiply possibilities

- What a sample space is and how it affects probabilities
- How to construct items for counting
- The multiplication rule and when to use it

Next up: *Permutations and combinations*

Time to finish up that Opening sheet!

Problem set 17,18 is due on Thursday, November 16 at 11PM


Any questions?

A counting proof

Theorem: Let $P(n)$ be for $m, n \in \boldsymbol{Z}, m \leq n$, there are $n - m + 1$ integers from m to n inclusive.
Proof by mathematical induction: There are 2 cases: $m \geq 0$ and $m < 0$.
Case 1: $m \geq 0$. Since $m \leq n$, we must show that $P(n)$ is true for all $n \geq 0$.
Basis: $P(0)$ counts the non-negative integers ≤ 0, that is $\{0\}$.
Since $0 - 0 + 1 = 1$ and $|\{0\}| = 1, P(0)$ is true.
Inductive step: Assume for some k that $P(k)$ is true, that is, there are $k - m + 1$ non-negative integers $\leq k$: $\{m, m+1, \ldots, k\}$.
We must show $P(k+1)$ is true, that is, that there are $k + 1 - m + 1$ integers $\leq k+1$: $\{m, m+1, \ldots, k, k+1\}$.
But $\{m, m+1, \ldots, k\} \cap \{k+1\} = \emptyset$
and $\{m, m+1, \ldots, k, k+1\} = \{m, m+1, \ldots, k\} \cup \{k+1\}$.
Thus, $\{m, m+1, \ldots, k\}$ and $\{k+1\}$ partition $\{m, m+1, \ldots, k, k+1\}$, and $|\{m, m+1, \ldots, k, k+1\}| = |\{m, m+1, \ldots, k\}| + |\{k+1\}| = k + 1$ and $P(k+1)$ is true.
Since we have proved the basis step and the inductive step, Case 1 is true. (continued)

Proof (continued)

Theorem: Let $P(n)$ be for $m, n \in \boldsymbol{Z}, m \leq n$, there are $n - m + 1$ integers from m to n inclusive. (continued)

Case 2: We must show that $P(n)$ is true for all $n \geq m, m \leq 0$.

Case 2a: $n \geq 0$. The integers to be counted $\{m, m+1, \dots, -1, 0, 1, 2, \dots n\}$ can be partitioned as $\{m, m+1, \dots, -1\}$ and $\{0, 1, 2, \dots n\}$.

The negative numbers $\{m, m+1, \dots, -2, -1\}$ can be placed in one-to-one correspondence with $\{1, 2, \dots m\}$.

By Case 1, $|\{1, 2, \dots m\}| = m - 1 + 1 = m$ so $|\{m, m+1, \dots, -1\}| = -m$

And also by Case 1 $|\{0, 1, 2, \dots n\}| = n - 0 + 1 = n + 1$.

Thus $|\{m, m+1, \dots, -1, 0, 1, 2, \dots n\}| = -m + n + 1 = n - m + 1$.

Case 2b: $n < 0$. The integers to be counted $\{m, m+1, \dots, \dots n\}$ are all negative and thus can be placed in one-to-one correspondence with the positive integers $\{-n, -n+1, \dots - m\}$ which by Case 1 are counted as $-m - (-n) + 1 = n - m + 1$.

Thus the theorem is true in all cases.

QED