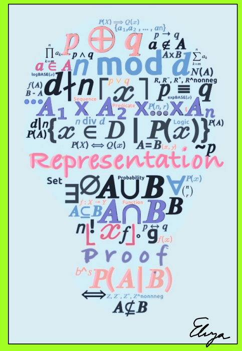
Discrete Structures



Lecture 22: Polynomial counting

Susan L. Epstein

HUNTER

1

Last time

★ **Counting supports function theory**

- Repetition counting employs identical objects
- Repetition in combinations produces a multiset

2

Review: questions to ask when you count

- How big are the sets that are involved?
- Are the sets involved disjoint?
- Is there inherent order? ≡ is this a permutation or a combination?
- What process would construct an arbitrary element?
- Would the complement be easier to count?
- Does the inclusion / exclusion rule apply?

Review: counting rules (1)

Multiplication rule: If a process consists of k steps that can be performed respectively in n_1, n_2,⋯, n_k ways, then the entire process can be performed in $n_1 n_2 \cdots n_k$ ways

For any integer $n \geq 1$ and any set S of n elements,

$P(n, r)$: there are $\frac{n!}{(n-r)!}$ permutations of r distinct elements from S

$C(n, r)$: there are $\frac{n!}{(n-r)!r!}$ combinations (ways to select) r elements from S

Addition rule: For any partition $\{A_1, A_2, \dots, A_n\}$ of a finite set A,

$$|A| = |A_1| + |A_2| + \cdots + |A_n|$$

Difference rule: For any finite set A and any subset B of A, $|A - B| = |A| - |B|$

Complement rule: For any finite set $A \subseteq U$, $|A^C| = |U| - |A|$

Review: counting rules (2)

Inclusion/exclusion rules: $|A \cup B| = |A| + |B| - |A \cap B|$ and

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

$$\left|\bigcup_{i=1}^{n} A_i\right| =$$

$$\sum_{i=1}^{n}|A_i| - \sum_{\text{distinct } i,j=1}^{n}|A_i \cap A_j| +$$

$$\sum_{\text{distinct } i,j,k=1}^{n}|A_i \cap A_j \cap A_{kj}| + \cdots + (-1)^{n-1}\left|\bigcap_{i=1}^{n} A_i\right|$$

Pigeonhole principles:

For any function *f* from a finite set X with n elements to a finite set Y with m elements, if $n > m$, then f is not 1-to-1.

Let f be a function from a finite set X of n elements to a finite set Y of m elements, and $k \in \boldsymbol{Z}^+$. If $k < \frac{n}{m}$, then there is some $y \in Y$ that is the image of at least $k+1$ elements of X.

5

Review: counting rules (3)

Order matters

- n items of r kinds with repetition: n^r
- n items of r kinds without repetition: $P(n,r) = \frac{n!}{(n-r)!}$
- n items of k kinds with q_i indistinguishable copies of the ith kind:
  $P(n;\ q_1, q_2, \dots, q_k) = \frac{n!}{q_1!q_2!\dots q_k!}$

Order does not matter

- n items of r kinds without repetition: $C(n,r) = \frac{n!}{(n-r)!r!}$
- n items of r kinds with repetition (aka stars and bars):
  $V(n,r) = C(n+r-1, n)$

6

Today's outline

- Pascal's triangle
- The binomial theorem
- Some important results

Proofs may reason combinatorically

Fall 2023 CSCI 150 7/24

7

Properties of $C(n, r)$

$$C(n,r) = \frac{n!}{(n-r)!\,r!}$$

- $C(n,n) = \frac{n!}{(n-n)!\,n!} = \frac{n!}{0!\,n!} = 1$
- If $n \geq 1$, $C(n, n-1) = \frac{n!}{(n-(n-1))!\,(n-1)!} = \frac{n!}{1!\,(n-1)!} = n$
- If $n \geq 2$, $C(n, n-2) = \frac{n!}{(n-(n-2))!\,(n-2)!} = \frac{n!}{2!\,(n-2)!} = \frac{n(n-1)}{2}$
- If $n \geq r$, $C(n, n-r) = C(n, r)$

Fall 2023 CSCI 150 8/24

8

2 proofs of $C(n, n-r) = C(n, r)$

Algebraic proof

Right side: $C(n,r) = \frac{n!}{(n-r)!r!}$

Left side: $C(n, n-r) = \frac{n!}{(n-(n-r))!(n-r)!} = \frac{n!}{r!(n-r)!} = \frac{n!}{(n-r)!r!}$

Combinatorial proof: We must show that $C(n,r) = C(n, n-r)$.

Let S be a set of n elements with exactly k distinct subsets of size r: $A_1, A_2, \ldots, A_k$.

Each subset of size r can be specified either by which elements are in it or which are not in it.

By definition of complement, each subset A_i has a unique complement $S - A_i$ of size $n - r$. This forms a 1-to-1 correspondence from $\{A_1, A_2, \ldots, A_k\}$, the set of all subsets of size r, to $\{S - A_1, S - A_2, \ldots, S - A_k\}$, the set of all subsets of size $n - r$, that is, $C(n,r) = C(n, n-r)$.

QED

Pascal's triangle [1654]

For $n, r \in \boldsymbol{Z}^+, r \le n,\ \ C(n+1.r) = C(n, r-1) + C(n,r)$

The sum of any 2 consecutive entries appears in the row below it.

$n \backslash r$	0	1	2		3	4	5	$\cdots$	$r-1$		r	$\cdots$
0	1								.		.	…
1	1	1							.		.	…
2	1	2	1						.		.	…
3	1	3	3		1				.		.	…
4	1	4	6	+	4	1			.		.	…
5	1	5	10	=	10	5	1		.		.	…
⋮	⋮	⋮	⋮		⋮	⋮	⋮		⋮		⋮	⋮
n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$		$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\cdots$	$\binom{n}{r-1}$	+	$\binom{n}{r}$	$\cdots$
$n+1$	$\binom{n+1}{0}$	$\binom{n+1}{1}$	$\binom{n+1}{2}$		$\binom{n+1}{3}$	$\binom{n+1}{4}$	$\binom{n+1}{5}$	$\cdots$		=	$\binom{n+1}{r}$	$\cdots$
.		.	.		.	.	.		.		.	…
.		.	.		.	.	.		.		.	…
.		.	.		.	.	.		.		.	…

$C(6,2) = C(5,1) + C(5,2) = 5 + 10$

A proof of Pascal's formula

Pascal's formula: $C(n+1.r) = C(n,r-1) + C(n,r)$

Theorem: For $n,r \in \boldsymbol{Z}^{+}, r \le n,\ \ C(n+1.r) = C(n,r-1) + C(n,r)$

Proof (algebraic):

Right side is $C(n,r-1) + C(n,r) = \frac{n!}{(n-(r-1))!(r-1)!} + \frac{n!}{(n-r)!r!} =$

$$\frac{n!}{(n-r+1)!\,(r-1)!} \cdot \frac{r}{r} + \frac{n!}{(n-r)!\,r!} \cdot \frac{(n-r+1)}{(n-r+1)} =$$

$$\frac{n!r}{(n-r+1)!r!} + \frac{n \cdot n! - n!r + n!}{(n-r+1)!r!} = \frac{n!r + n \cdot n! - n!r + n!}{(n+1-r)!r!} = \frac{n!(n+1)}{(n-r+1)!r!}$$

Left side is $C(n+1.r) = \frac{(n+1)!}{(n+1-r)!r!}$

QED

There is also a combinatoric proof in your text

11

Today's outline

- ✓ Pascal's triangle
- The binomial theorem
- Some important results

12

Binomials and exponents

- Term = product of a number and at least one variable
- Monomial = 1 term ab $3ab^2$
- Binomial = sum of 2 terms $a+b$ $13-2z$

$(a+b)^0 = 1$

$(a+b)^1 = 1a + 1b$

$(a+b)^2 = (a+b)\cdot(a+b) = aa + ab + ba + bb = 1a^2 + 2ab + 1b^2$

$(a+b)^3 = (a+b)\cdot(a+b)\cdot(a+b) =$

$= aaa + aab + aba + abb + baa + bab + bba + bbb$

$= a^3 + ab^2 + a^2b + ab^2 + a^2b + ab^2 + ab^2 + b^3$

$= a^3 + 3a^2b + 3ab^2 + b^3$

				1				
			1		1			
		1		2		1		
	1		3		3		1	
1		4		6		4		1

$(a+b)^4 = (a+b)\cdot(a+b)\cdot(a+b)\cdot(a+b)$

$= aaaa + aaab + aaba + aabb + abaa + abab + abba + abbb +$
$baaa + baab + baba + babb + bbaa + bbab + bbba + bbbb$

$= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^3$

- How many terms in $(a+b)^1$? in $(a+b)^2$? in $(a+b)^3$? in $(a+b)^4$?

Binomials and that triangle

$(a+b)^0 = 1$

$(a+b)^1 = 1a + 1b$

$(a+b)^2 = 1a^2 + 2ab + 1b^2$

$(a+b)^3 = 1a^3 + 3a^2b + 3ab^2 + 1b^3$

$(a+b)^4 = 1a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1b^3$

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1

- How many terms would you expect in the expansion of $(a+b)^n$?
- What do you notice about the exponents in any one term?
- A term is produced by selecting either a or b from each $(a+b)$ factor
- How many ways can you do that from n factors so that you have k b's and $n-k$ a's?

$C(n,k)$

- And when you do that, what does a term in the full product look like?

$C(n,k)a^{n-k}b^k$

- That's why $C(n,k)$ is also known as a binomial coefficient

Binomial theorem

Binomial theorem: Given any $a, b \in \boldsymbol{R}$ and any $n \in \boldsymbol{Z}^{nonneg}$,

$$(a+b)^n = \sum_{k=0}^{n} C(n,k)a^{n-k}b^k$$

$$= a^n + C(n,1)a^{n-1}b^1 + C(n,2)a^{n-2}b^2 + \ldots + C(n,n-1)a^1b^{n-1} + b^n$$

Proof (combinatorial version): Let a, b be real numbers. There are 2 cases: $n = 0$ and $n \geq 1$.

Case 1: $n = 0$. The left side is $(a+b)^0 = 1$. The right side is shown to also be 1 by $\sum_{k=0}^{0} C(n,k)a^{n-k}b^k = C(0,k)a^{0-0}b^0 = \frac{0!}{0!(0-0)!} \cdot 1 \cdot 1 = \frac{1}{1 \cdot 1} = 1$

Case 2: $n \geq 1$. The expression $(a+b)^n$ can be expanded into products of n letters, each of which is either a or b.

For each $k = 0,1,2,\ldots,n$, the product $a^{n-k}b^k$ occurs as a term in the sum as many times as there are ways to order $n-k$ a's and k b's. This is the same as $C(n,k)$ to select the k b's and then fill the other positions with a's. Hence, when like terms are combined, the coefficient of $a^{n-k}b^k$ in the sum is $C(n,k)$.

Thus the theorem is true regardless of which is the case.

QED

There is also an algebraic proof in your text

Fall 2023 CSCI 150 15/24

15

Applications (1)

$$(a+b)^n = \sum_{k=0}^{n} C(n,k)a^{n-k}b^k$$

$$(a+b)^5 = \sum_{k=0}^{5} C(5,k)a^{5-k}b^k$$

$$= a^5 + C(5,1)a^{5-1}b^1 + C(5,2)a^{5-2}b^2 + C(5,3)a^{5-3}b^3 + C(5,4)a^1b^{5-1} + b^5$$

$$= a^5 + 5a^4b^1 + 10a^3b^2 + 10a^2b^3 + 5a^1b^4 + b^5$$

$$(x-4y)^4 = \sum_{k=0}^{4} C(4,k)x^{4-k}(-4y)^k$$

$$= x^4 + C(4,1)x^{4-1}(-4y)^1 + C(4,2)x^{4-2}(-4y)^2 + C(4,3)x^{4-3}(-4y)^3 + (-4y)^4$$

$$= x^4 + 4x^3(-4y)^1 + 6x^2(-4y)^2 + 4x^1(-4y)^3 + (-4y)^4$$

$$= x^4 - 16x^3y^1 + 96x^2y^2 - 256x^1y^3 + 256y^4$$

Since $2 = 1 + 1$,

$2^n = \sum_{k=0}^{n} C(n,k)1^{5-k}1^k = \sum_{k=0}^{n} C(n,k) \cdot 1 \cdot 1 = \sum_{k=0}^{n} C(n,k)$

And now you know why

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

Fall 2023 CSCI 150 16/24

16

Applications (2)

- How many terms in the expansion of $(2s-3y)^{17}$

  18

$$(a+b)^n = \sum_{k=0}^{n} C(n,k)a^{n-k}b^k$$

- What is the 6th term in that expansion?

  $C(17,5)\cdot(2s)^{17-5}\cdot(-3y)^5$

- Sum of the binomial coefficients

  Substitute $a=1, b=1$

  $\sum_{k=0}^{n} C(n,k)1^{n-k}1^k = \sum_{k=0}^{n} C(n,k) = (1+1)^2 = 2^n$

- Find a closed form (without Σ or Π or ellipses) for $\sum_{k=0}^{n} C(n,k)9^k$

  Since $1^k = 1$, $\sum_{k=0}^{n} C(n,k)\, 9^k 1^{n-k} = (9+1)^n = 10^n$

  Rather than code a loop that iterates over values of k, you can just code a single exponential!

But the triangle is not Pascal's alone

- In the 11th century Persian mathematician Omar Khayyam built a similar triangle (and wrote and collected poetry attributed to him in 1859)
- Also in the 11th century Chinese mathematician Jia Xian developed it but by the 13th century it was known as known as Yang Hui's triangle
- And even in Europe, Pascal was not the first
  - Jordanus de Nemore in the late 12th or early 13th century
  - Levi ben Gershon in France in the early 14th century
  - Other latecomers include Petrus Apianus [1527] and Michael Stifei [1544] in Germany, and Niccolo Tartaglia [1556] and Gerolamo Cardano [1570] in Italy
- Mathematical attribution requires both discovery and dissemination

https://en.wikipedia.org/wiki/Pascal%27s_triangle

Today's outline

- ✓ Pascal's triangle
- ✓ The binomial theorem
- Some important results

The hairdresser's puzzle

In the tiny town of Weirdville there is a hairdresser who cuts the hair of all people, and only those people, who do not cut their own hair.

Does the hairdresser cut their own hair?
Neither yes nor no. Why?
There are 2 possibilities: either the hairdresser cuts their own hair or does not.
Possibility 1: The hairdresser cuts their own hair, That's a contradiction because that service is only for people who do not cut their own hair.
Possibility 2: The hairdresser does not cut their own hair. But the hairdresser is a person in the town and therefore must have their hair cut by the hairdresser. Another contradiction.

What's wrong here?
The assumption that such a situation can exist.

(Bertrand) Russell's Paradox (part 1)

Consider $S = \{A \mid A$ is a set and $A \notin A\}$, the set of all sets that are not elements of themselves.

Is S an element of itself?

Neither yes nor no. Why?

There are 2 possibilities: $S \in S$ or $S \notin S$.

Possibility 1: If $S \in S$ it contradicts its definition.

Possibility 2: If $S \notin S$ then by definition of S, $S \in S$

Neither possibility can be true…

Again the error is allowing such a situation to exist

21

(Bertrand) Russell's Paradox (part 2)

In CSCI 150 we avoid this by specifying that all sets are subsets of $\boldsymbol{U}$.

Assume there is a set $S = \{A \mid A \subseteq \boldsymbol{U}$ and $A \notin A\}$.

There are 2 cases: $S \in S$ or $S \notin S$.

Case 1: If $S \in S$ then $S \subseteq \boldsymbol{U}$ and $S \notin S$ by definition of S, so $S \in S \rightarrow S \notin S$.

Contradiction.

Case 2: If $S \notin S$ then not ($S \subseteq \boldsymbol{U}$ and $S \notin S$), so by DeMorgan's laws

either $S \nsubseteq \boldsymbol{U}$ or $S \in S$.

Since $S \in S$ would be a contradiction, the only remaining possibility is that

$S \nsubseteq \boldsymbol{U}$, that is, that no such set S exists!

QED

An entire branch of mathematics now exists to identify Russell's paradox.
https://en.wikipedia.org/wiki/Non-well-founded_set_theory

22

The halting problem (Alan Turing)

Halt = terminate in finitely many steps

Can infinite loops during execution be predicted?

Theorem: No algorithm can check whether or not any program X with data D will halt before you execute it.

Proof:

Assume there is some algorithm $Check$ such that, given program X and dataset D, $Check(X, D)$ prints "halts" if X on D will halt else it prints "never."

Since the sequence of characters that compose $Check$ can also be considered a dataset, we could run $Check(X, X)$.

Let $Test$ be another algorithm that runs on any algorithm X. If $Check(X, X)$ prints "halts," then $Test(X)$ loops forever. If $Check(X, X)$ prints "never, " then $Test(X)$ halts. Now consider 2 cases: either $Test(Test)$ halts or it doesn't.

Case 1: $Test(Test)$ halts, so $Check(Test, Test)$ outputs "halts" and $Test(Test)$ loops forever. Contradiction.

Case 2: $Test(Test)$ does not halt, so $Check(Test, Test)$ outputs "never" and $Test(Test)$ halts. Contradiction.

Thus our assumption was wrong and $Check$ does not exist. QED

23

What you should know

★ **Proods may reason combinatorially**

- How to efficiently generate polynomials
- Russell's paradox
- The halting problem

Next up: *Graphs*

Time to finish up that Opening sheet!

Any questions?

Problem set 21,22 is due on Thursday, November 30 at 11PM

24

Multinomials

- Multinomial = sum of algebraic terms binomial

Multinomial theorem: Given any $m \in \boldsymbol{Z}^{+}$and any $n \in \boldsymbol{Z}^{nonneg}$,

$$(x_1 + x_2 + \cdots x_m)^n = \sum_{\substack{k_1+k_2+\cdots+k_m=n \\ k_1,k_2,\ldots,k_m \geq 0}}^{n} C(n; k_1, k_2, \ldots, k_m) \prod_{t=1}^{m} x_t^{k_t}$$

where $C(n; k_1, k_2, \ldots, k_m) = \frac{n!}{k_1! k_2! \cdots k_m!}$ is a multinomial coefficient

$(a+b+c)^3 = \sum_{\substack{k_1+k_2+k_3=3 \\ k_1,k_2,k_3 \geq 0}} C(3; k_1, k_2, k_3) \prod_{t=1}^{3} x_t^{k_t}$

$= C(3;3,0,0)a^3 + C(3;2,1,0)a^2 b + C(3;2,0,1)a^2 c + C(3;1,2,0)ab^2 + C(3;1,1,1)abc + C(3;1,0,2)ac^2 + C(3;0,3,0)b^3 + C(3;0,2,1)\, b^2 c + C(3;0,1,2)bc^2 + C(3;0,0,3)c^3$

$C(3;2,1,0) = \frac{3!}{2!\,1!\,0!} = 3,\ C(3;1,1,1) = \frac{3!}{1!\,1!\,1!} = 6,\ C(3;3,0,0) = \frac{3!}{3!\,1!\,1!} = 1$

So $(a+b+c)^3 =$

$a^3 + 3a^2 b + 3a^2 c + 3ab^2 + 6abc + 3ac^2 + b^3 + 3b^2 c + 3bc^2 + c^3$

Fall 2023 CSCI 150

25

Multinomial coefficients

- To find the sum of multinomial coefficients, substitute $x_i = 1$ for $1 \leq i \leq m$

$$(x_1 + x_2 + \cdots x_m)^n = \sum_{\substack{k_1+k_2+\cdots+k_m=n \\ k_1,k_2,\ldots,k_m \geq 0}}^{n} C(n; k_1, k_2, \ldots, k_m) \prod_{t=1}^{m} x_t^{k_t} =$$

$\sum_{\substack{k_1+k_2+\cdots+k_m=n \\ k_1,k_2,\ldots,k_m \geq 0}}^{n} C(n; k_1, k_2, \ldots, k_m) \prod_{t=1}^{m} 1^{k_t} =$

$\sum_{\substack{k_1+k_2+\cdots+k_m=n \\ k_1,k_2,\ldots,k_m \geq 0}}^{n} C(n; k_1, k_2, \ldots, k_m) = (x_1 + x_2 + \cdots x_m)^n = m^n$

- Number of terms in the expansion = number of monomials of degree n on m variables $V(m,n) = C(n+m-1, m-1)$

Fall 2023 CSCI 150

26