CSE 312

Foundations of Computing II

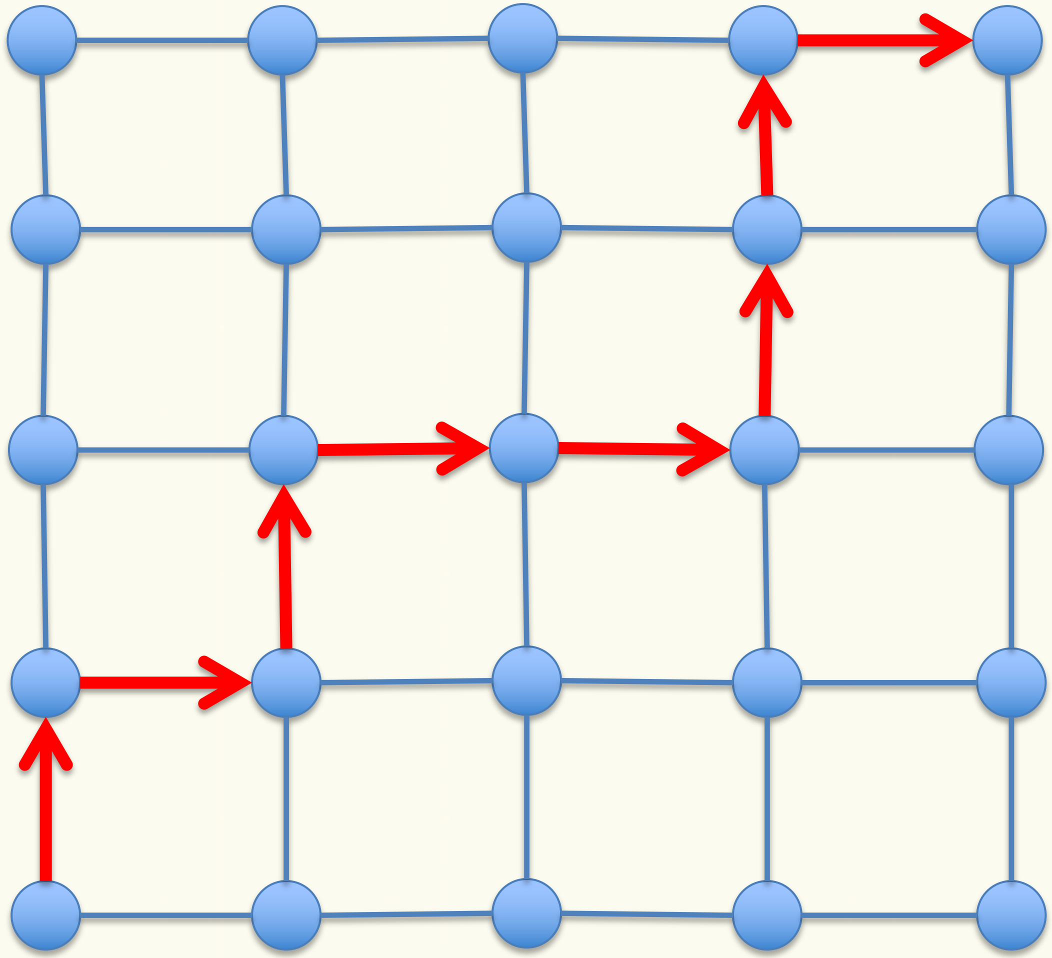
Lecture 3: Binomial Coefficients + Inclusion/exclusion

PAUL G. ALLEN SCHOOL
OF COMPUTER SCIENCE & ENGINEERING

Stefano Tessaro

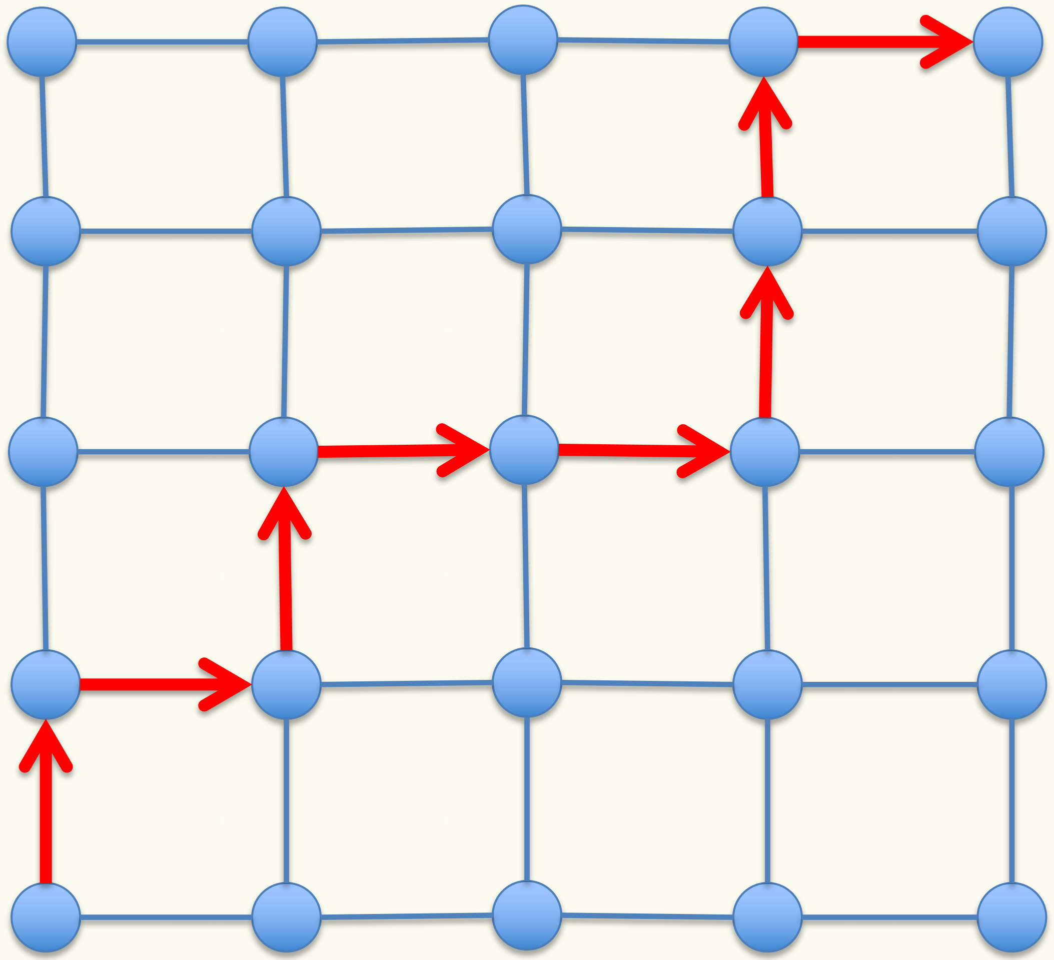
tessaro@cs.washington.edu

Example II – Counting Paths



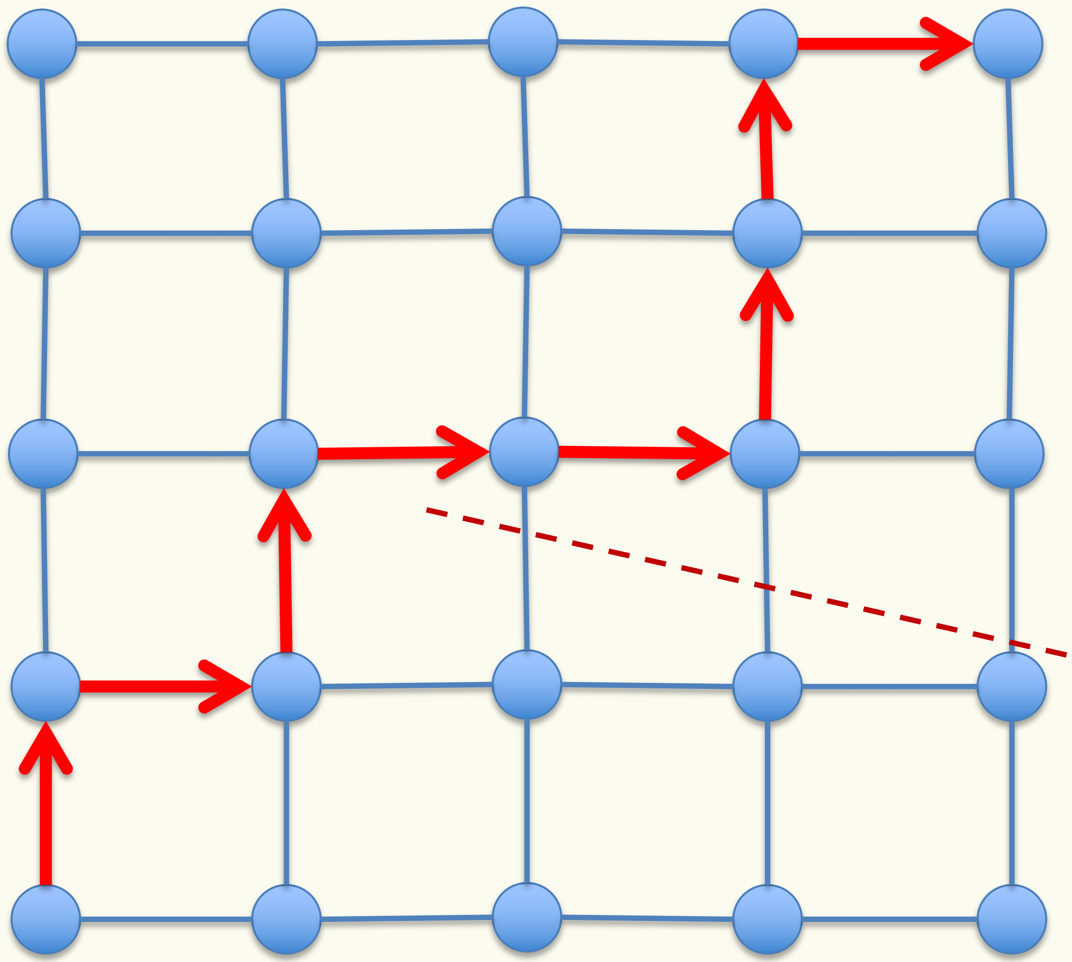
"How many shortest paths from bottom-left to top-right?"

Example II – Counting Paths



How do we represent a path?

Example II – Counting Paths

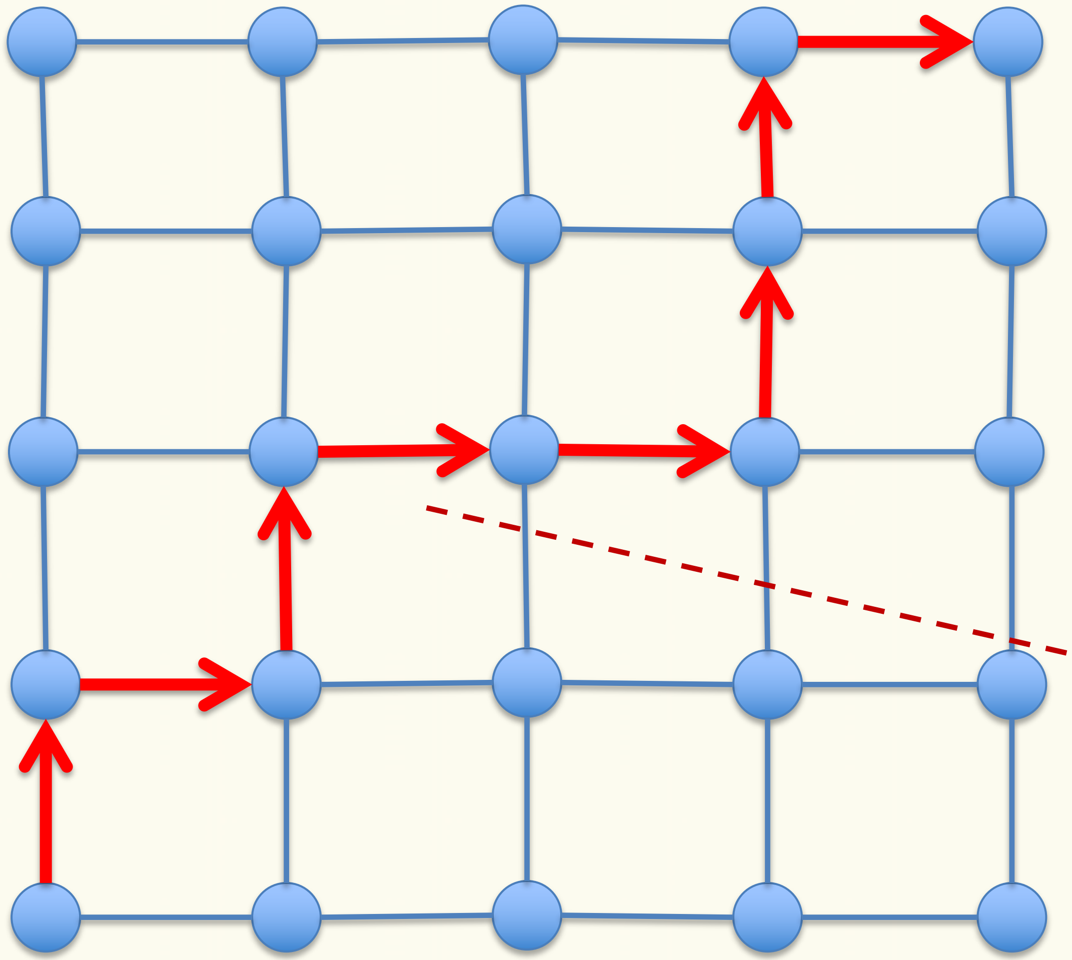


$$\text{Path} \in \{\uparrow, \rightarrow\}^8$$

$(\uparrow, \rightarrow, \uparrow, \rightarrow, \rightarrow, \uparrow, \uparrow, \rightarrow)$

$\#\uparrow\text{'s} = \#\rightarrow\text{'s}$

Example II – Counting Paths



Path <u>uniquely</u> defined by position of ↑'s

$$\# \text{ paths} = \binom{8}{4} = 70$$

(↑, →, ↑, →, →, ↑, ↑, →)

↑'s = # →'s

Example III – Word Permutations

"How many ways to re-arrange the letters in the word SEATTLE?

STALEET, TEALEST, LASTTEE, …

Guess: 7! Correct?!

No! e.g., leaving word unchanged / swapping two T's lead both to *SEATTLE*

Counted as separate permutations, but they lead to the same word.

Example III – Word Permutations

"How many ways to re-arrange the letters in the word SEATTLE?

STALEET, TEALEST, LASTTEE, …

Location of S

Location of A

$$\binom{7}{2} \times \binom{5}{2} \times 3 \times 2 \times 1$$

$\boxed{T}$ $\boxed{E}$ $\boxed{S}$ $\boxed{T}$ $\boxed{A}$ $\boxed{L}$ $\boxed{E}$

Location of L

Locations of E's

Locations of T's

Example III – Word Permutations

"How many ways to re-arrange the letters in the word SEATTLE?

STALEET, TEALEST, LASTTEE, …

$$\binom{7}{2} \times \binom{5}{2} \times 3 \times 2 \times 1 = \frac{7!}{2!\,\cancel{5}!} \times \frac{\cancel{5}!}{2!\,\cancel{3}!} \times \cancel{3}!$$

$$= \frac{7!}{2!\,2!} = 1260$$

Binomial Identities

Fact. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ **Pascal's Identity**

$$\binom{0}{0}$$
$$\binom{1}{0} \quad \binom{1}{1}$$
$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$
$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$
$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$
$$\dots$$

Pascal's triangle

$$1$$
$$1 \quad 1$$
$$1 \quad 2 \quad 1$$
$$1 \quad 3 \quad 3 \quad 1$$
$$1 \quad 4 \quad 6 \quad 4 \quad 1$$
$$\dots$$

Binomial Theorem

$(x+y)^2 = x^2 + 2xy + y^2$

$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$

$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^5$

...

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

...

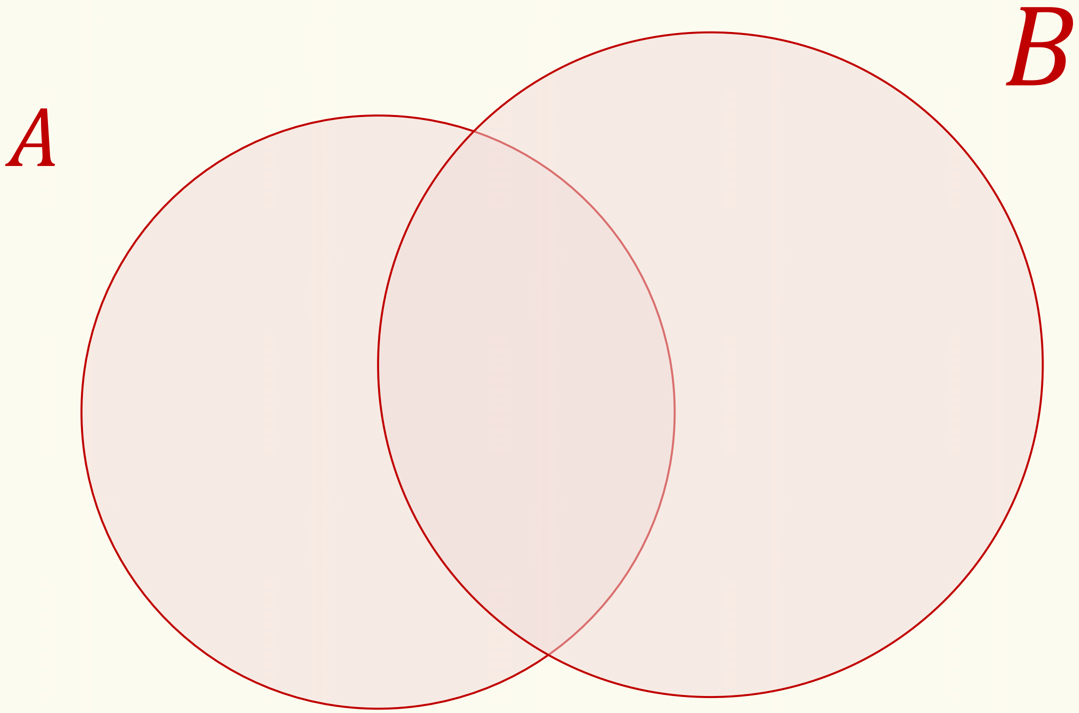
Theorem. $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

Corollary. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

Why?
Set $x = y = 1$

Inclusion-Exclusion

Sometimes, we want $|S|$, and $S = A \cup B$

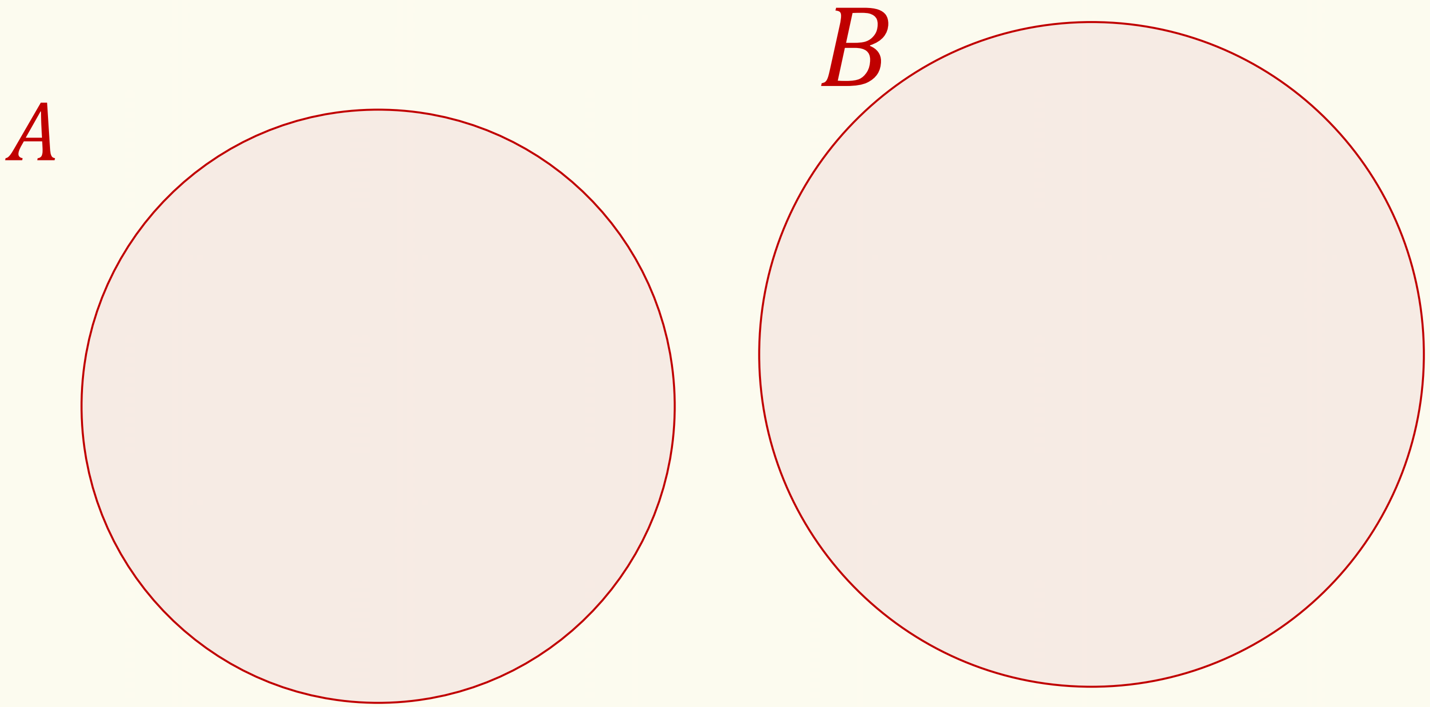


$\cancel{|A \cup B| = |A| + |B|}$?

Fact. $|A \cup B| = |A| + |B| - |A \cap B|$

Disjoint Sets

Sometimes, we want $|S|$, and $S = A \cup B$



Fact. $|A \cup B| = |A| + |B|$

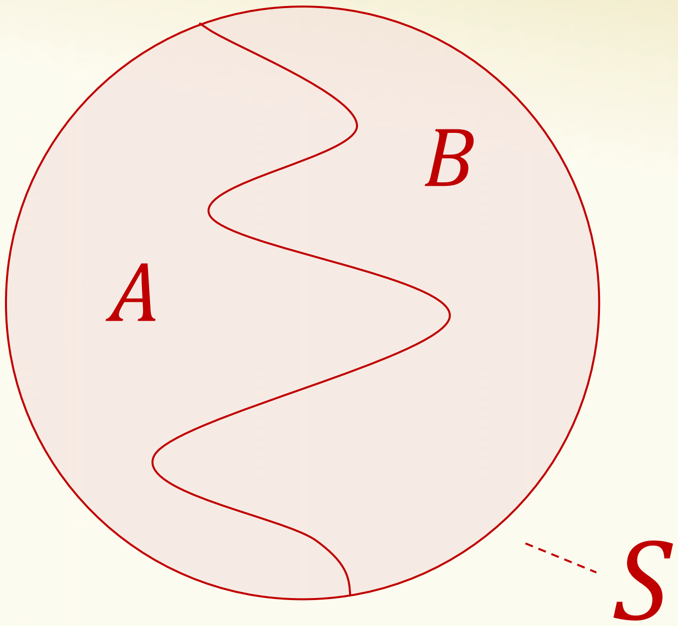
Example – Binomial Identity

B?

Fact. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

S

A?



$S = \binom{[n]}{k}$ $\quad |S| = \binom{n}{k}$

Example: $\binom{[4]}{2} = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$

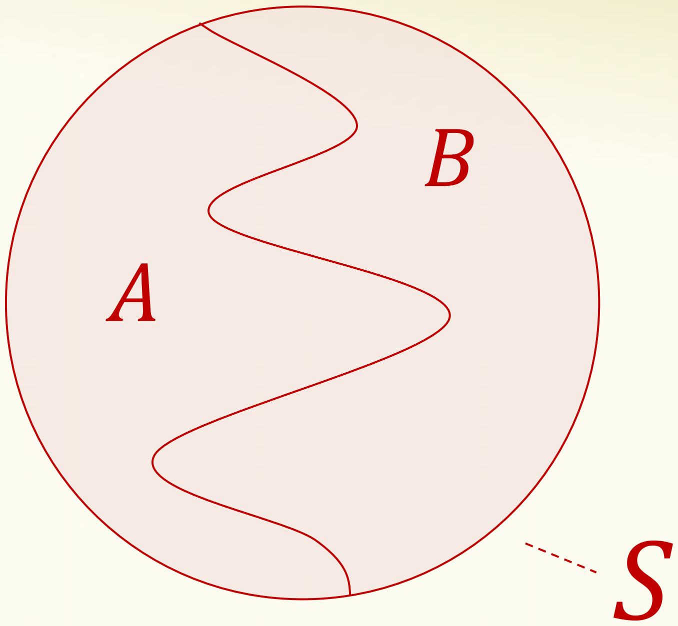
$A = ?$

$B = ?$

Example – Binomial Identity

Fact. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

S



$S = \binom{[n]}{k} \quad |S| = \binom{n}{k}$

Example: $\binom{[4]}{2} = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$

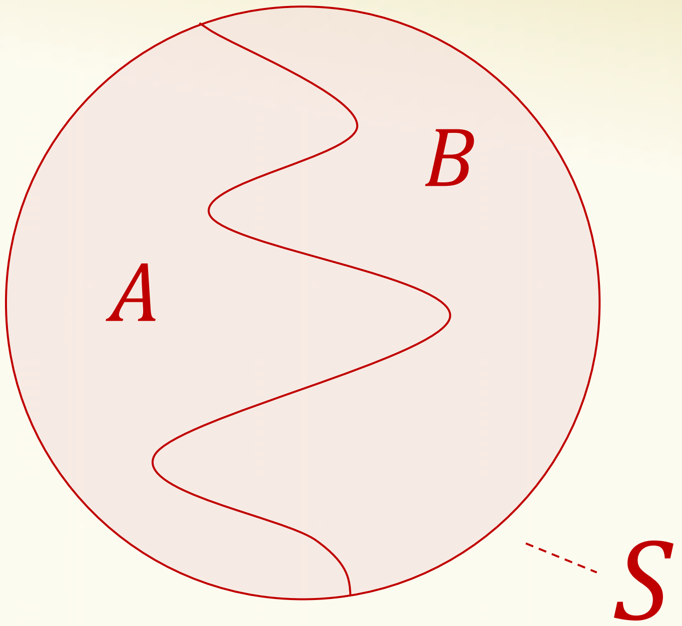
$A = \left\{X \in \binom{[n]}{k} \middle| \, n \in X\right\}$ $\{\{1,4\},\{2,4\},\{3,4\}\}$

$B = \left\{X \in \binom{[n]}{k} \mid n \notin X\right\}$ $\{\{1,2\},\{1,3\},\{2,3\}\}$

Example – Binomial Identity

Fact. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

S



n is in set, need to choose $k-1$ elements from $[n-1]$

$S = \binom{[n]}{k} \quad |S| = \binom{n}{k}$

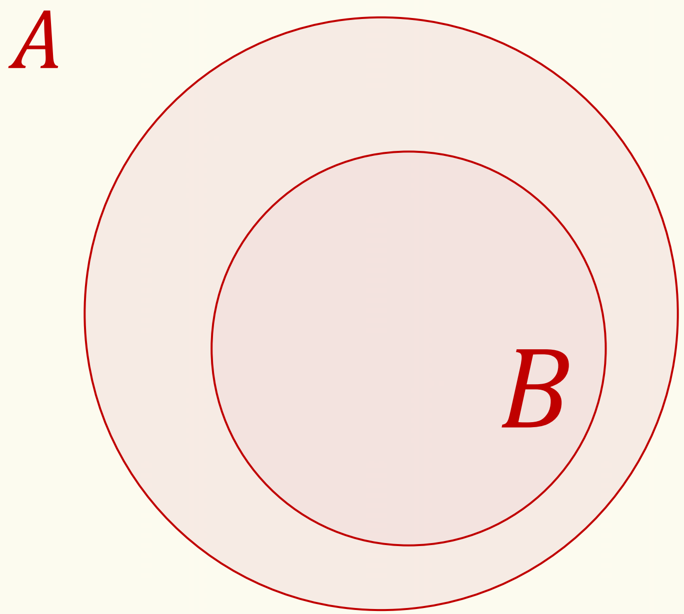
$A = \left\{X \in \binom{[n]}{k} \middle| \, n \in X\right\}$ $\qquad |A| = \binom{n-1}{k-1}$

$B = \left\{X \in \binom{[n]}{k} \,\middle|\, n \notin X\right\}$ $\qquad |B| = \binom{n-1}{k}$

n not in set, need to choose k elements from $[n-1]$

Also Useful: Set Difference

Sometimes, we want $|S|$, and $S = A \setminus B$ and $B \subseteq A$



Fact. $|A \setminus B| = |A| - |B|$

Example – Number of co-prime numbers

Definition. The **Euler's totient function** is defined as

$$\varphi(N) = |\{a \in \mathbb{N} \mid 1 \leq a \leq N \ \text{ and } \gcd(a, N) = 1\}|$$

"greatest common divisor"

Example.

$$\varphi(7) = |\{1,2,3,4,5,6\}| = 6$$

$$\varphi(15) = |\{1,2,4,7,8,11,13,14\}| = 8$$

Q: Which numbers did we exclude?

The multiples of 3 and 5

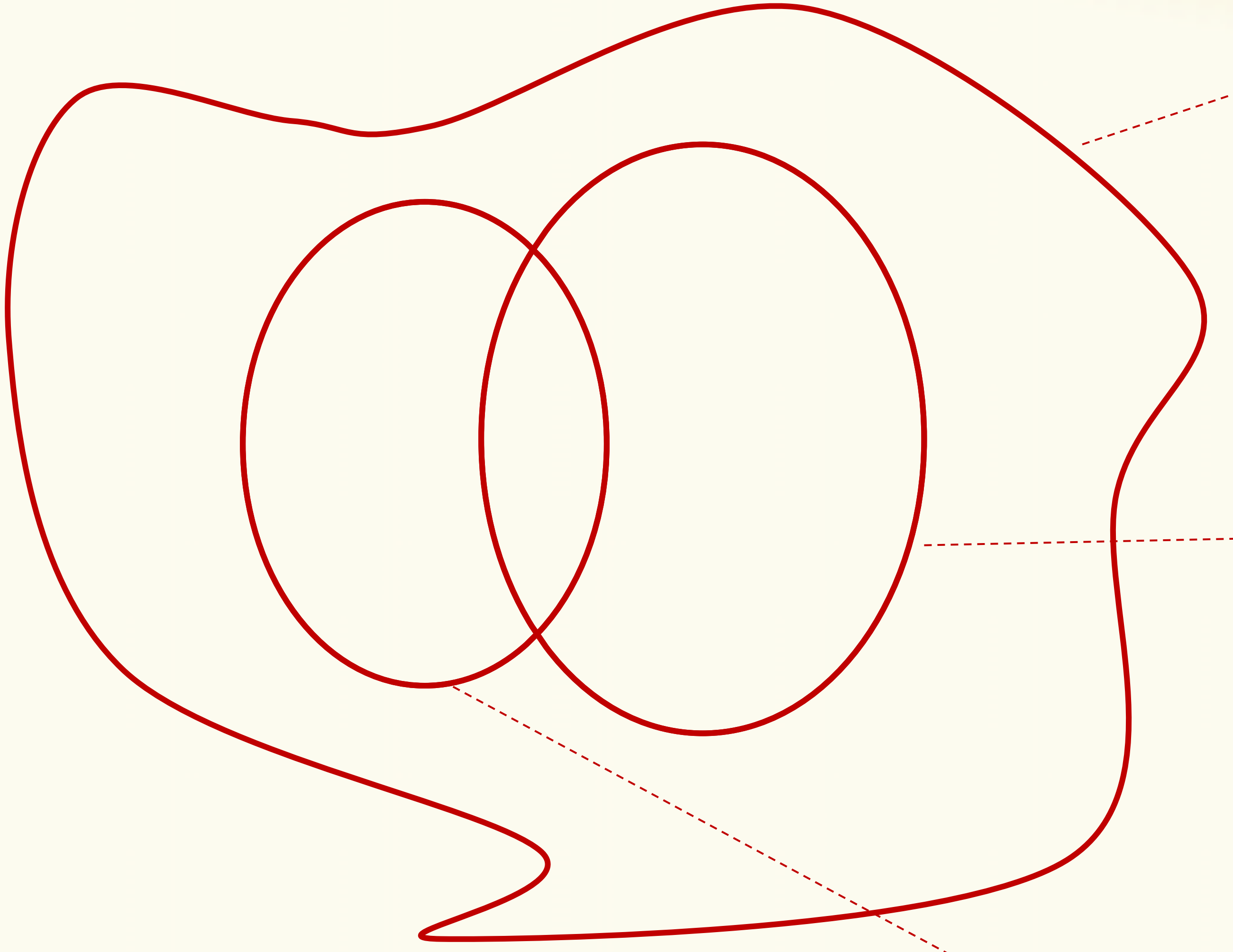
Special Case – Product of two Primes

Definition. The **Euler totient function** is defined as

$$\varphi(N) = |\{a \in \mathbb{N} \mid 1 \leq a \leq N \text{ and } \gcd(a, N) = 1\}|$$

Goal: For two distinct prime numbers P and Q, give a formula for $\varphi(N)$, where $N = P \times Q$.

Next time: General formula

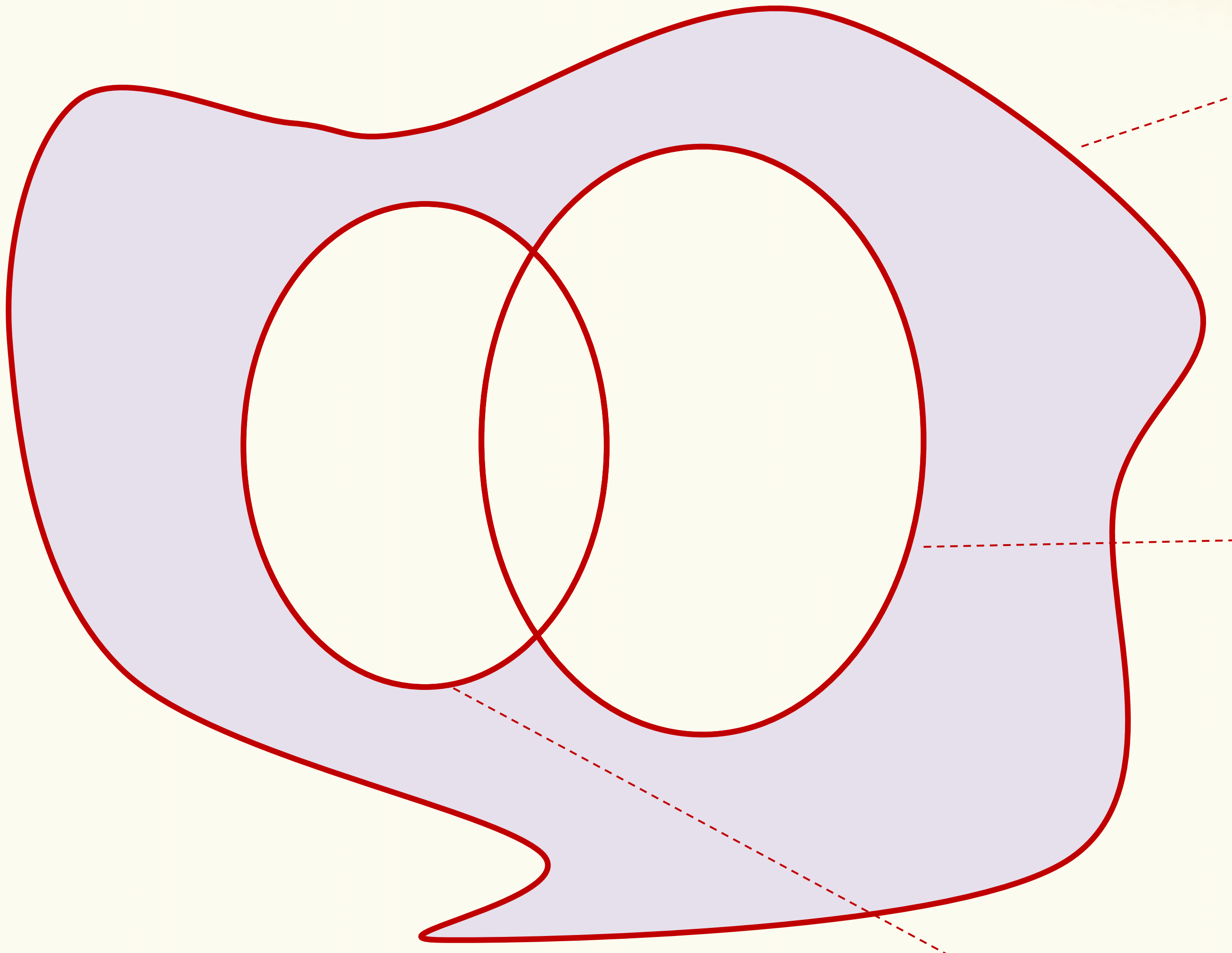


$C = \{1, \dots, N\}$

$A = \{P, 2P, \dots, PQ\}$

$\varphi(N) = ?$

$B = \{Q, 2Q, \dots, PQ\}$



$$C = \{1, \dots, N\}$$

$$|C| = N$$

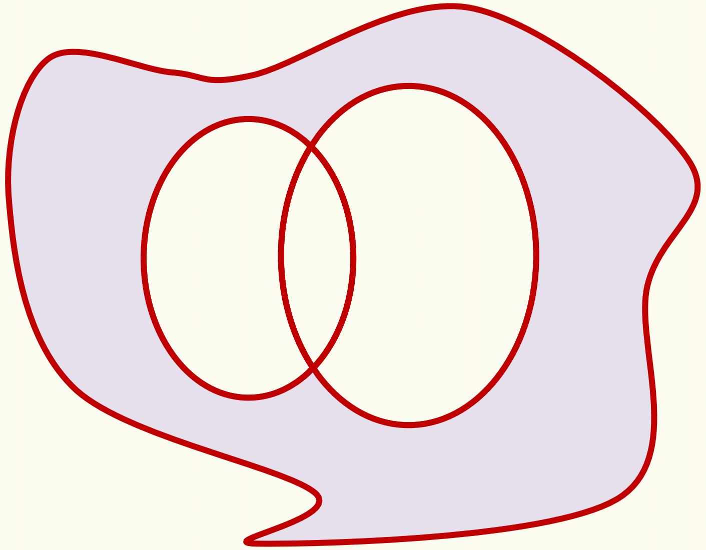
$$|A| = Q$$

$$A = \{P, 2P, \dots, PQ\}$$

$$\varphi(N) = |C \setminus (A \cup B)|$$

$$B = \{Q, 2Q, \dots, PQ\}$$

$$|B| = P$$



$$|A| = Q \qquad A = \{P, 2P, \dots, PQ\}$$

$$|B| = P \qquad B = \{Q, 2Q, \dots, PQ\}$$

$$|C| = N \qquad C = \{1, \dots, N\}$$

$$\varphi(N) = |C \setminus (A \cup B)|$$

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

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

???

$$A \cap B = \{N\}$$

$$= PQ - Q - P + 1 = (P-1)(Q-1)$$

RSA

Theorem. Computing $\varphi(N)$ when $N = P \times Q$ for two distinct (unknown) primes is equivalent to factoring N into P and Q.

- Very hard problem on computers, necessary for security of RSA encryption.
- ”Easy” on quantum computers.