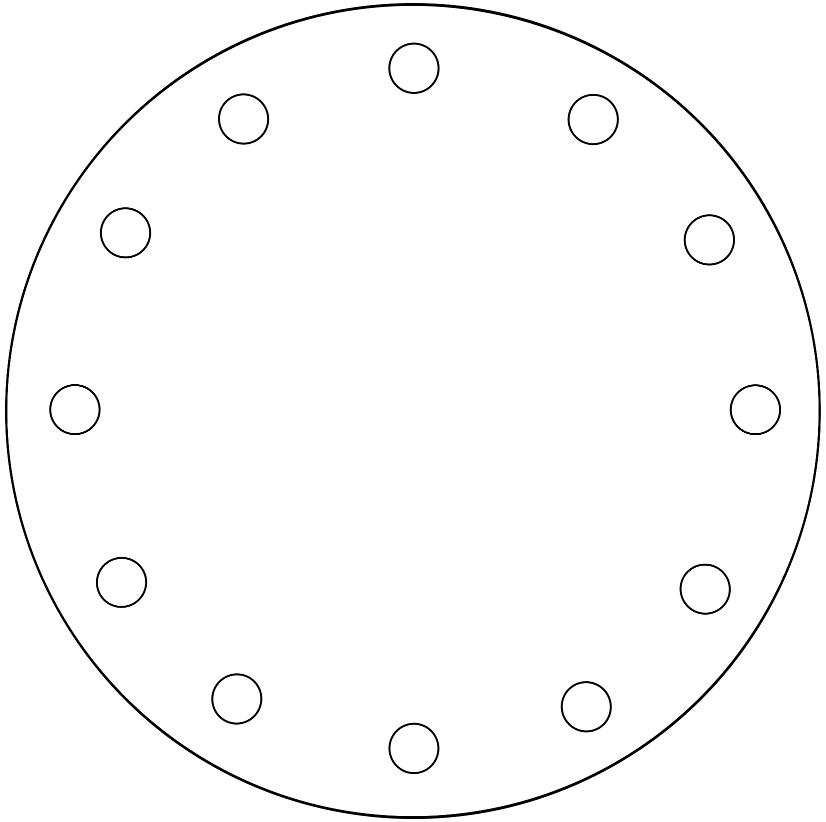
CS3102 Theory of Computation

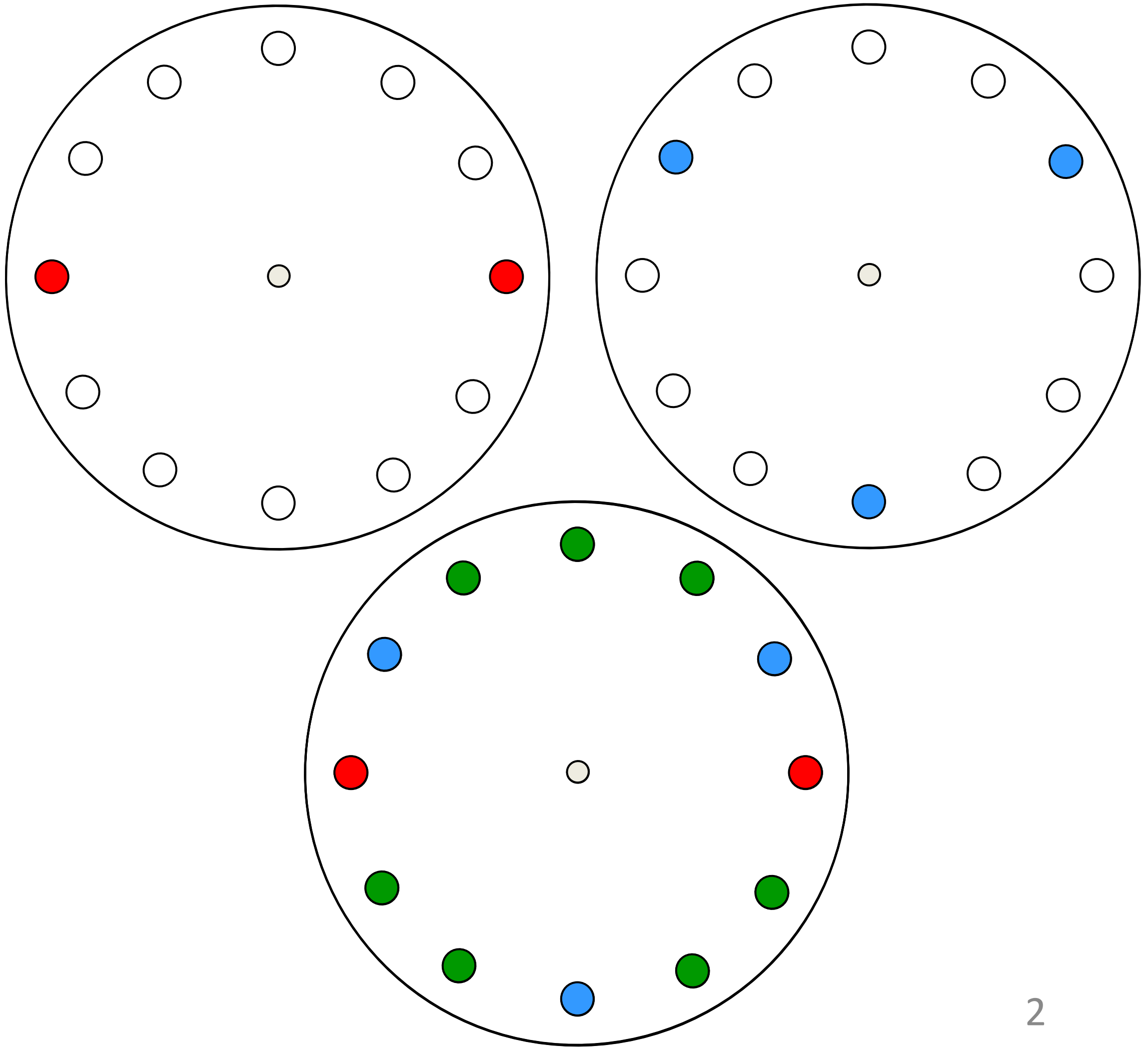
www.cs.virginia.edu/~njb2b/cs3102

Can 5 test tubes be spun simultaneously in a 12-hole centrifuge in a balanced way?



Can 5 test tubes be spun simultaneously in a 12-hole centrifuge in a balanced way?

- What does "balanced" mean?
- Symmetry
- Superposition
- Complementarity



What makes a proof “good”?

Finite Geometric Series

- $1 + 2 + 4 + 8 + 16 + 32 + \cdots + 256 = ?$
  - $\frac{2^{8+1} - 1}{2 - 1} = 511$
- $3 + 12 + 48 + 192 + \cdots + 12288 = ?$
  - $3\,\frac{\left(4^{6+1} - 1\right)}{4 - 1} = 16383$
- $a(1 + r + r^2 + r^3 + r^4 + \cdots + r^n) = ?$
  - $a\,\frac{r^{n+1} - 1}{r - 1}$
  - How could I show this?

Finite Geometric Series

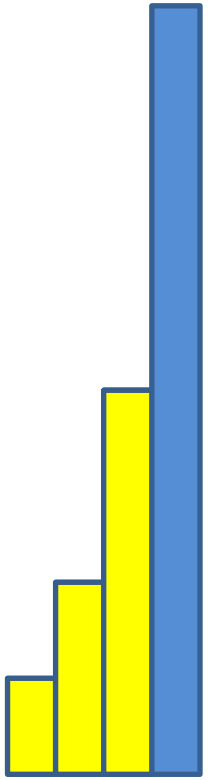
$$a(1 + r + r^2 + r^3 + r^4 + \cdots + r^n)(r - 1) = ?$$

$$a(\cancel{r} + \cancel{r^2} + \cancel{r^3} + \cancel{r^4} + \cancel{r^5} + \cdots + \cancel{r^n} + r^{n+1}) +$$
$$a(-\cancel{r} - \cancel{r^2} - \cancel{r^3} - \cancel{r^4} - \cancel{r^5} - \cdots - \cancel{r^n} - 1) =$$
$$a(r^{n+1} - 1)$$

$$\sum_{i=0}^{n} ar^i = a\frac{r^{n+1} - 1}{r - 1}$$

Finite Geometric Series

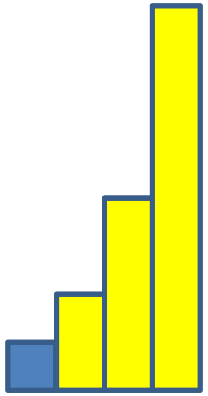
$r > 1$



The series multiplied by r

$(a + ar + \cdots + ar^n)r$

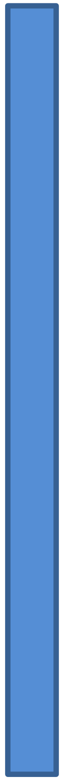
$-$



The series

$(a + ar + \cdots + ar^n)1$

$=$



The next term in the series

ar^{n+1}

$-$

The first term

a

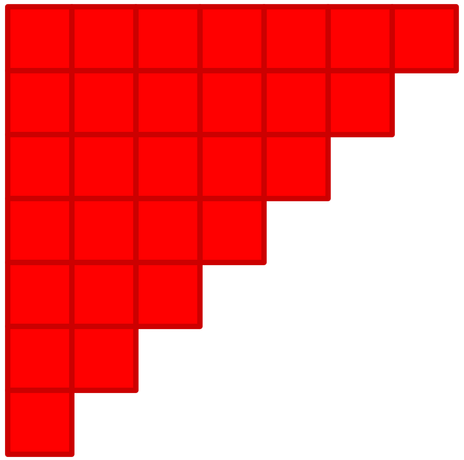
Finite Arithmetic Series

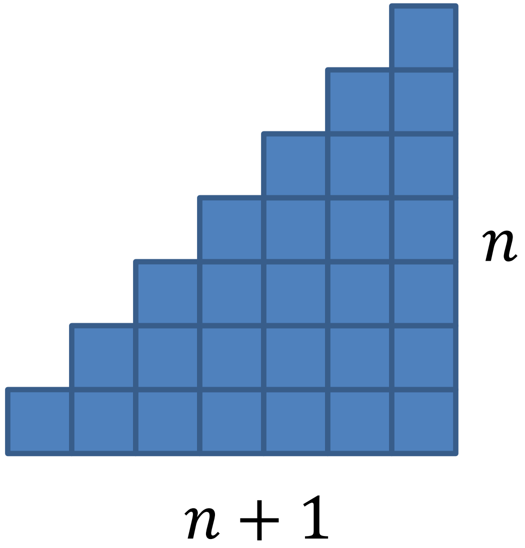
- $1 + 2 + 3 + \cdots + 100 = ?$
  - $\frac{100(100+1)}{2} = 5050$
- $4 + 7 + 10 + 13 + 16 + \cdots + 37 = ?$
  - $(1 + 1 \cdot 3) + (1 + 2 \cdot 3) + \cdots + (1 + 12 \cdot 3) =$
  - $(12) + 3(1 + 2 + 3 + \cdots + 12)$
  - $12 + 3(\frac{12(12+1)}{2})$
- $1 + 2 + 3 + 4 + \cdots + n = \frac{n(n+1)}{2}$

Finite Arithmetic Series

$$1 + 2 + 3 + \cdots + (n - 1) + n =$$

$$\frac{n(n+1)}{2}$$





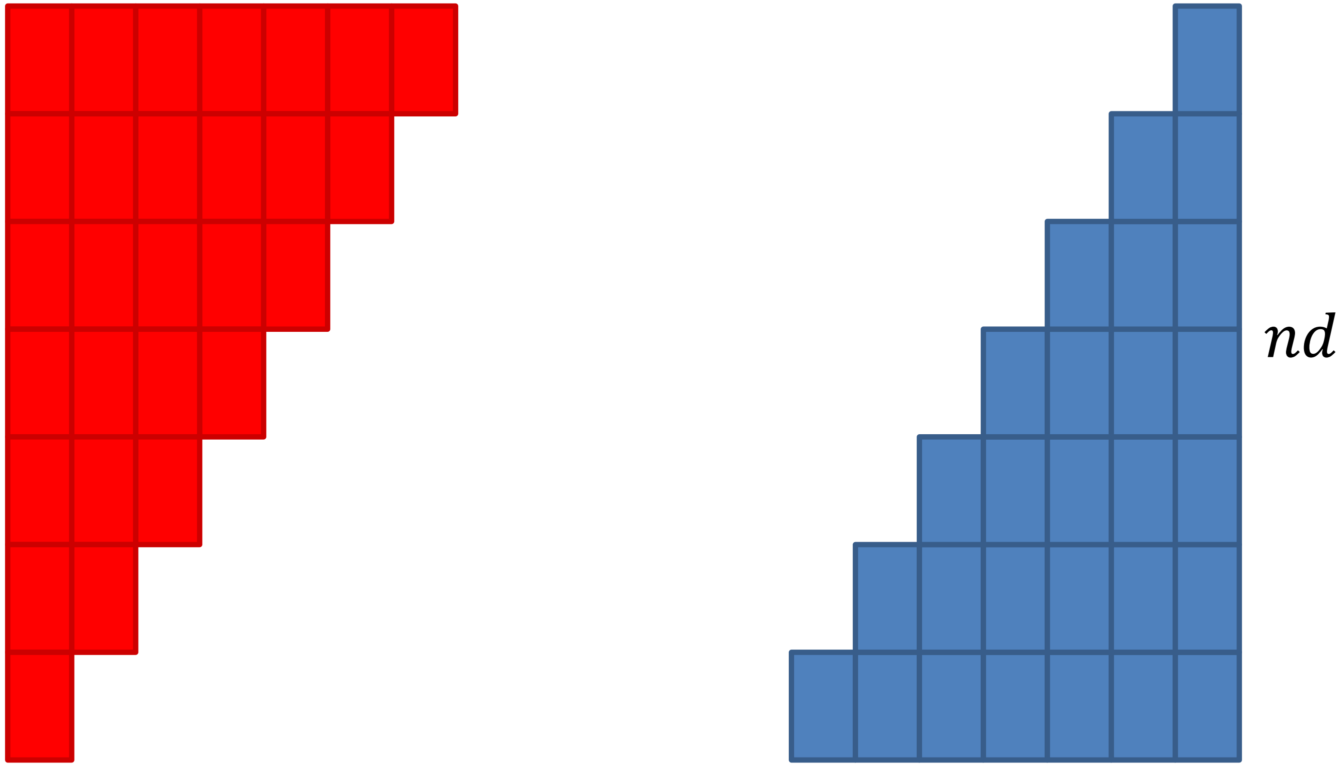
Finite Arithmetic Series

$$a(n+1) + (0d + 1d + 2d + \cdots + nd) =$$

$$a(n+1) + \frac{nd(n+1)}{2} = (n+1)\left(\frac{a + (a + nd)}{2}\right)$$

Number of terms

Average term value



How to prove $p \to q$

- Direct Proof ($p \to q$)
  - Start with premise
  - Repeatedly apply definitions, equivalences, and inferences
  - End with conclusion
- Indirect Proof ($\neg q \to \neg p$) AKA, proof by contrapositive
  - Start with negation of the conclusion
  - Repeatedly apply definitions, equivalences, and inferences
  - End with negation of the premise
- Proof by Contradiction $\left(\neg(p \wedge \neg q)\right)$
  - Start with $p \wedge \neg q$
  - Repeatedly apply definitions, equivalences, and inferences
  - End with False

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Proofs Techniques Cont.

- Construction
  - Shows: $\exists x \in S, P(x)$
  - Give an example which works
- Proof by Cases
  - Shows: $\forall x \in S, P(x)$
  - Show $\left(\forall x \in S_1, P(x)\right) \wedge \left(\forall x \in S_2, P(x)\right) \wedge (S_1 \cup S_2 = S)$
- Induction
  - Shows: $\forall x \in \mathbb{N}, P(x)$
  - Show $P(0)$, then show $P(k) \rightarrow P(k+1)$ for $k \geq 0$

Proof: n^2 is even $\leftrightarrow n$ is even

- How would we prove this?
- Recall: $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
  - Suffice to show both of:
    - $p \rightarrow q$
    - $q \rightarrow p$

Proof: if n^2 is even $\leftarrow$ n is even

- Direct Proof :
  - Start with premise
  - Repeatedly apply definitions, equivalences, and inferences
  - End with conclusion

Show that $n = 2k$ implies $n^2 = 2k'$

Start with $n = 2k$

1. $n = 2k$
2. $n^2 = (2k)(2k)$
3. $n^2 = 4k^2$
4. $n^2 = 2(2k^2)$
5. Let $k' = 2k^2$, n^2 is even

Proof: if n^2 is even $\rightarrow n$ is even

- Indirect Proof (proof by contrapositive):
  - Start with negation of the conclusion
  - Repeatedly apply definitions, equivalences, and inferences
  - End with negation of the premise

<u>Show</u> that $n = 2k + 1$ implies $n^2 = 2k' + 1$

<u>Start with</u> $n = 2k + 1$

1. $n = 2k + 1$

2. $n^2 = (2k + 1)(2k + 1)$

3. $n^2 = 4k^2 + 4k + 1$

4. $n^2 = 2(2k^2 + 2k) + 1$

5. Let $k' = 2k^2 + 2k$, n^2 is odd

Proof: $5n + 6$ even $\leftrightarrow n$ even

Proof: √2 is not rational

- Proof by contradiction
  - Start with $p \land \neg q$
  - Repeatedly apply definitions, equivalences, and inferences
  - End with False

<u>Show</u> that $\left(\frac{a}{b}\right)^2 = 2$ and $a, b \in \mathbb{N}$ is impossible

<u>Start with</u>$\left(\frac{a}{b}\right)^2 = 2 \land a, b \in \mathbb{N} n = 2k + 1$

1. Assume toward reaching a contradiction that $\left(\frac{a}{b}\right)^2 = 2$ and a, b are integers, and $\frac{a}{b}$ is in simplest terms (i.e. $\gcd(a, b) = 1$)
2. Since a^2 is even, it must be that a is even, so a^2 is divisible by 4
3. For $\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} = 2$, it must then be that b^2 is even, meaning b is also even
4. Since a, b are both even, $\gcd(a, b) \geq 2$, which is a contradiction

Proof: $n^4 - 4n^2$ is divisible by 3

- **Proof by Cases:**
  1. Enumerate all possible circumstances for the given
  2. Show that each circumstance results in the conclusion

1. $n^4 - 4n^2$
2. $n^2(n^2 - 4)$
3. $n \cdot n(n-2)(n+2)$
4. Cases: $n \equiv 0 \bmod 3$, $n \equiv 1 \bmod 3$, $n \equiv 2 \bmod 3$
   1. $n \equiv 0 \bmod 3$: $3|n$, thus $3|(n^4 - 4n^2)$
   2. $n \equiv 1 \bmod 3$: $3|(n+2)$, thus $3|(n^4 - 4n^2)$
   3. $n \equiv 2 \bmod 3$: $3|(n-2)$, thus $3|(n^4 - 4n^2)$

Proof: $\min(x, y) \cdot \max(x, y) = x \cdot y$

Mathematical Induction

- We what to show $\forall x \in \mathbb{N}, P(x)$ for some proposition $P(x)$
  - E.g. $\forall x \in \mathbb{N}$, Domino x will fall
- Base Case: First show $P(0)$
  - Show that Domino 0 (the first domino) will fall
- Inductive Hypothesis: Assume $P(k)$ for an arbitrary $k \geq 0$.
  - Assume arbitrary domino k will fall
- Inductive Step: Show $P(k) \rightarrow P(k+1)$
  - Show that when arbitrary domino k falls, then the next domino $k+1$ will fall.

Mathematical Induction

- Base Case: The first domino will fall
- Inductive step: If any domino k falls, then domino $k+1$ will fall

Falls because of base Case

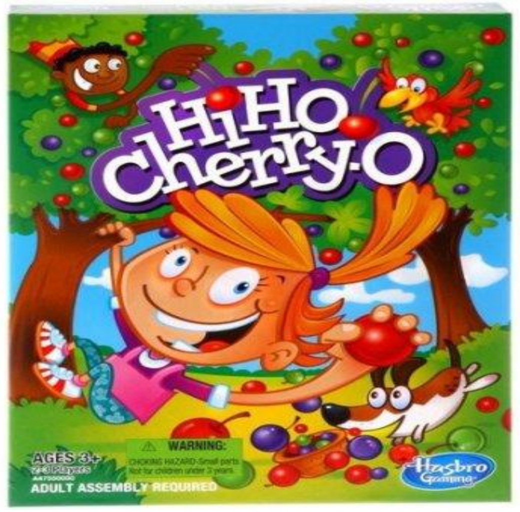
Falls because of Inductive Step

Falls because of Inductive Step

Falls because of Inductive Step

All dominos fall!!

Hi-Ho-Cherry-O



- Each Player takes turns removing 1, 2, 3, or 4 cherries from play
- First player unable to pick a cherry loses

Player 2 always wins

- If number of cherries is a multiple of 5, then player 2 always wins.
  - $\forall x \in \mathbb{N}$, Player 2 wins for $5x$ cherries
- Base Case: when $x = 0$, player 2 wins
  - Proof: when there are 0 cherries, player 1 has none to take, so player 2 wins
- Inductive Hypothesis: Assume player 2 wins when there are $5k$ cherries
- Inductive Step: Show that if player 2 wins with $5k$ cherries, then player 2 wins with $5(k+1)$ cherries
  - Proof: By construction: If player 1 takes n cherries, where $1 \leq n \leq 4$, then player 2 can take $5 - n$ cherries. If we had $5(k+1)$ cherries, then we now have $5(k+1) - n - (5 - n) = 5k$ cherries. Therefore player 2 wins by the inductive hypothesis

Problems with induction

- Useless for helping you to find the answer
- You have to know the answer first
- Does not provide insights into why something is true
- Does not give any clues on how to correct if you're wrong