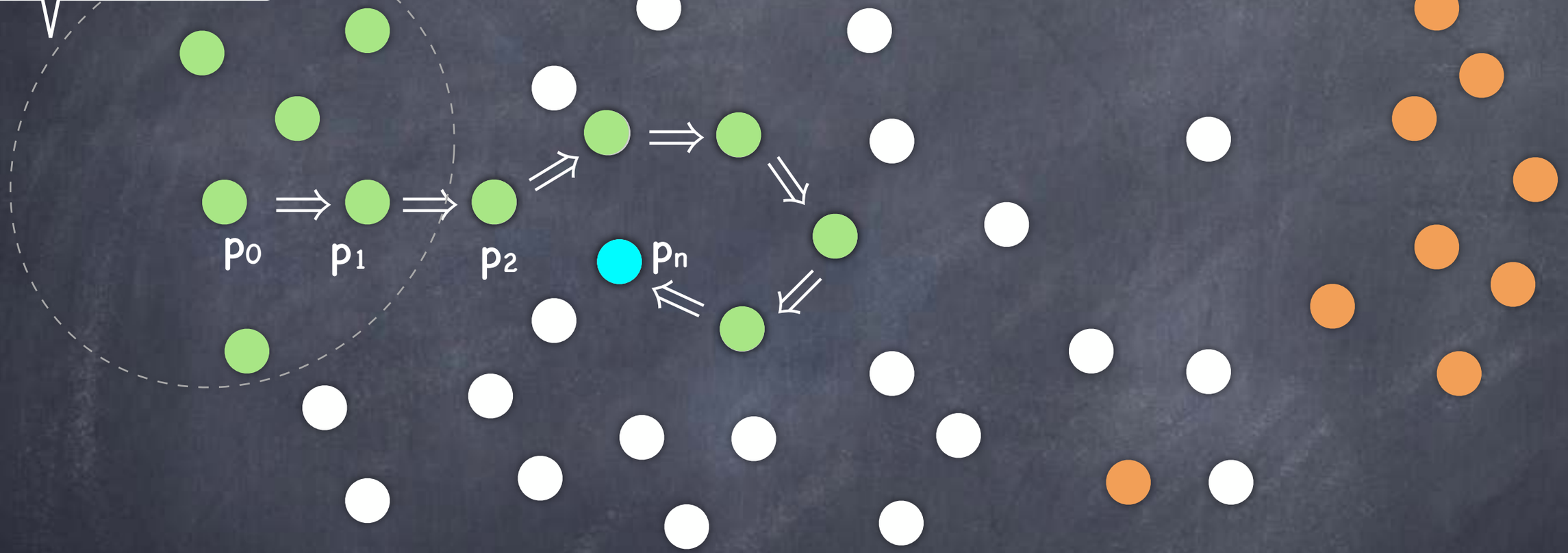
Some Proof Templates

A Mental Picture

Axioms, definitions, already proven propositions



Template for $p \rightarrow q$

- To prove $p \rightarrow q$:
  - May set p_0 as p (even though we don't know if p is True), and proceed to prove q
    - Proof starts with "Suppose p."
  - Why is this a proof of $p \rightarrow q$?
    - If p is True, the above is a valid proof that q holds. And if q holds, $p \rightarrow q$ holds.
    - If p is False, the above proof is not valid. But we already have that $p \rightarrow q$ is vacuously true.
    - In either case $p \rightarrow q$ holds
  - Or, could rewrite the proof as $(p \rightarrow p_1) \Rightarrow (p \rightarrow p_2) \Rightarrow \ldots \Rightarrow (p \rightarrow q)$

Rephrasing

- Often it is helpful to first rewrite the proposition into an equivalent proposition and prove that.

  $p_{orig} \leftrightarrow p_{equiv}$
  $p_0 \Rightarrow p_1 \Rightarrow \ldots \Rightarrow p_{equiv} \Rightarrow p_{orig}$

- Should clearly state this if you are doing this.

- An important example: contrapositive
  - $p \rightarrow q \equiv \neg q \rightarrow \neg p$
    - Both equivalent to $\neg p \vee q$

Contrapositive

- $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- An example:
  - Proposition: $\forall x,y \in \mathbb{Z}^+ \;\; x \cdot y > 25 \rightarrow (x \geq 6) \vee (y \geq 6)$

Positive integers

  - Enough to prove that: $\forall x,y \in \mathbb{Z}^+ \;\; (x<6) \wedge (y<6) \rightarrow x \cdot y \leq 25$
- Another example:
  - If function f is "hard" then crypto scheme S is "secure"
    ≡ If crypto scheme S is not "secure," then function f is not "hard"
  - To prove the former, we can instead show how to transform any attack on S into an efficient algorithm for f

Rephrasing

- Often it is helpful to first rewrite the proposition into an equivalent proposition and prove that.

$P_{orig} \leftrightarrow P_{equiv}$

$P_0 \Rightarrow P_1 \Rightarrow \ldots \Rightarrow P_{equiv} \Rightarrow P_{orig}$

- Should clearly state this if you are doing this.

- An important example: contrapositive
  - $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- Another instance: proof by contradiction
  - $p \equiv \neg p \rightarrow \text{False}$
  - So, to prove p, enough to show that $\neg p \rightarrow$ False.

Contradiction

- To prove p, enough to show that ¬p → False.
- Recall: To prove ¬p → False, we can start by assuming ¬p
  - Can start the proof directly by saying "Suppose for the sake of contradiction, ¬p" (instead of saying we shall prove ¬p → False)
- p_n is simply "False"
  - E.g., we may have ¬p ⇒ ... ⇒ q ... ⇒ ¬q ⇒ False
    - "But that is a contradiction! Hence p holds."

Example

- Claim: There's a village barber who gives haircuts to exactly those in the village who don't cut their own hair
- Proposition: The claim is false
- Proposition, formally: $\neg(\exists B \forall x \;\; \neg\text{cut-hair}(x,x) \longleftrightarrow \text{cut-hair}(B,x))$
- Suppose for the sake of contradiction,
  $\exists B \;\forall x \;\; \neg\text{cut-hair}(x,x) \longleftrightarrow \text{cut-hair}(B,x)$
- $(\exists B \;\forall x \;\; \neg\text{cut-hair}(x,x) \longleftrightarrow \text{cut-hair}(B,x)\;)$

  $\Rightarrow (\exists B \;\neg\text{cut-hair}(B,B) \longleftrightarrow \text{cut-hair}(B,B)\;)$

  $\Rightarrow \exists B$ False

  $\Rightarrow$ False, which is a contradiction!

Example

- For every pair of distinct primes p,q, $\log_p(q)$ is irrational
- (Will use basic facts about log and primes from arithmetic.)
- Suppose for the sake of contradiction that there exists a pair of distinct primes (p,q), s.t. $\log_p(q)$ is rational.
- $\Rightarrow \log_p(q) = a/b$ for positive integers a,b.

  (Note, since $q>1$, $\log_p(q) > 0$.)
- $\Rightarrow \quad p^{a/b} = q \quad \Rightarrow p^a = q^b$.
- But p, q are distinct primes. Thus p^a and q^b are two distinct prime factorisations of the same integer!
- Contradicts the Fundamental Theorem of Arithmetic!

Will prove later

Reduction

- Often it is helpful to break up the proof into two parts
- To prove p, show $r \rightarrow p$ and separately show r
  - The proof $r \rightarrow p$ is said to "reduce" the task of proving p to the task of proving r
- Many sophisticated proofs are carried out over several works, each one reducing it to a simpler problem

$$p_0 \Rightarrow \ldots \Rightarrow r' \Rightarrow \ldots \Rightarrow r \Rightarrow \ldots \Rightarrow p$$

- Proving $r \rightarrow p$ leaves open the possibility that $\neg p$ will be proven later, which will yield a proof for $\neg r$ instead

Template for $\exists x\ P(x)$

- To prove $\exists x\ P(x)$
  - Demonstrate a particular value of x s.t. P(x) holds
- e.g. to prove $\exists x\ P(x) \rightarrow Q(x)$
  - find an x s.t. $P(x) \rightarrow Q(x)$ holds
    - if you can find an x s.t. P(x) is false, done!
    - or, you can find an x s.t. Q(x) is true, done!
    - (May not be easy to show either, but still may be able to find an x and argue $\neg P(x) \vee Q(x)$)
  - (May not be able to find one, but still show one exists!)

Template for ¬(∀x P(x))

- To prove ¬(∀x P(x))
  - ≡ ∃x ¬P(x)
  - Demonstrate a particular value of x s.t. P(x) doesn't hold
  - Proof by counterexample
- e.g. to disprove the claim that all odd numbers > 1 are prime
  - i.e., to prove ¬(∀x∈S, Prime(x)) where S is the set of all odd numbers > 1
  - Enough to show that ∃x∈S ¬Prime(x)
    - take x = 9 = 3×3 (or, say, x = 207 = 9×23)

Template for $\forall x\ P(x)$

- To prove $\forall x\ P(x)$
  - Let x be an arbitrary element (in the domain of the predicate P)
  - Now prove P(x) holds
  - x is arbitrary: the proof applies to every x. Hence $\forall x\ P(x)$

- e.g., To prove $\forall x\ \underline{Q(x) \rightarrow R(x)}$
  - To prove $Q(x) \rightarrow R(x)$ for an arbitrary x
    - Assume Q(x) holds, i.e., set p_0 to be Q(x). Then prove R(x) using a sequence, $p_0 \Rightarrow p_1 \Rightarrow \ldots \Rightarrow p_n$, where p_n is R(x)
  - Caution: You are not proving $(\forall x\ Q(x)) \rightarrow (\forall x\ R(x))$. So to prove R(x), may only assume Q(x), and not Q(x′) for $x' \neq x$.

Cases

- Often it is helpful to break a proposition into various "cases" and prove them one by one
- e.g., To prove q, prove the following
  - $c_1 \vee c_2 \vee c_3$
  - $c_1 \rightarrow q$
  - $c_2 \rightarrow q$
  - $c_3 \rightarrow q$
  - $\Rightarrow (c_1 \vee c_2 \vee c_3) \rightarrow q$
  - $\Rightarrow q$

$$(c_1 \rightarrow q) \wedge (c_2 \rightarrow q) \wedge (c_3 \rightarrow q)$$

$$\equiv$$

$$(c_1 \vee c_2 \vee c_3) \rightarrow q$$

$$c \wedge (c \rightarrow q) \Rightarrow q$$

Cases

- Often it is helpful to break a proposition into various "cases" and prove them one by one
- e.g., To prove $p \rightarrow q$, prove the following
  - $p \rightarrow c_1 \vee c_2 \vee c_3$
  - $c_1 \rightarrow q$
  - $c_2 \rightarrow q$
  - $c_3 \rightarrow q$
  - $\Rightarrow (c_1 \vee c_2 \vee c_3) \rightarrow q$
  - $\Rightarrow p \rightarrow q$

$$(c_1 \rightarrow q) \wedge (c_2 \rightarrow q) \wedge (c_3 \rightarrow q)$$
$$\equiv$$
$$(c_1 \vee c_2 \vee c_3) \rightarrow q$$

$$((p \rightarrow c) \wedge (c \rightarrow q)) \Rightarrow (p \rightarrow q)$$

Cases: Example

- Proving equivalences of logical formulas
- To prove: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
  - $\forall p,q,r \in \{T,F\} \quad (p \vee (q \wedge r)) \longleftrightarrow ((p \vee q) \wedge (p \vee r))$
- Two cases: $p \vee \neg p$
- Case p: $p \vee (q \wedge r) \equiv T$

  $(p \vee q) \wedge (p \vee r) \equiv T$
- Case ¬p: $p \vee (q \wedge r) \equiv (q \wedge r)$

  $(p \vee q) \wedge (p \vee r) \equiv (q \wedge r)$

Cases: Example

- $\forall a,b,c,d \in \mathbb{Z}^+$ If $a^2+b^2+c^2 = d^2$, then d is even iff a,b,c are all even.
- Suppose $a,b,c,d \in \mathbb{Z}^+$ s.t. $a^2+b^2+c^2 = d^2$. Will show d is even iff a,b,c are all even.
- 4 cases based on number of a,b,c which are even.
- Case 1: a,b,c all even $\Rightarrow d^2 = a^2+b^2+c^2$ even $\Rightarrow$ d even.
- Case 2: Of a,b,c, 2 even, 1 odd. Without loss of generality, let a be odd and b, c even. i.e., $a=2x+1$, $b=2y$, $c=2z$ for some x,y,z. Then, $d^2 = a^2+b^2+c^2 = 2(2x^2+2x+2y^2+2z^2) + 1 \Rightarrow d^2$ odd $\Rightarrow$ d odd.
- Case 3: Of a,b,c, 1 even, 2 odd. W.l.o.g, $a=2x+1, b=2y+1, c=2z$. Then, $d^2=a^2+b^2+c^2 = 4(x^2+x+y^2+y+4z^2) + 2$. Contradiction! (why?)
- Case 4: a,b,c all odd $\Rightarrow d^2 = a^2+b^2+c^2 = 4w+3 \Rightarrow$ d odd.