Proof Techniques

- For correctness of algorithm we need proofs.
- Following are desirable characteristics
  - proofs must be logically correct,
  - brief, contains no meaningless statement,
  - self contained, references to other widely known results if used must be carefully cited,
  - should not be driven by intuition,
  - should not use any conjecture.
- Some of the powerful invalid proof techniques listed next.
- Lifted from a list displayed on an unknown professor's door.

Some Invalid Proof Techniques

1. Proof by cumbersome notation:
2. Proof by exhaustion : N number of cases delt separately.
3. Proof by omission : "The reader may easily supply the details."
4. Proof by obfuscation : A long plotless sequence of true and/or meaningless syntactically related statements.
5. Proof by eminent authority : "Knuth told me ..."

Invalid Proof Techniques

6. Proof by reduction to the wrong problem : This problem wrongly reduced some other known problem.
7. Proof by accumulated evidence : a counter example have not been found yet.
8. Proof by cosmology : The negation of the proposition is unimaginable or meaningless. Popular for proofs of the existence of God.

Invalid Proof Techniques

10. Proof by mutual reference : In reference A, Theorem 5 is said to follow from Theorem 3 in reference B, which is shown to follow from Corollary 6.2 in reference C, which is an easy consequence of Theorem 5 in reference A.
11. Proof by metaproof : A method is given to construct the desired proof. The correctness of the method is proved by any of these techniques.
12. Proof by picture : A more convincing form of proof by example. Combines well with proof by omission.

Invalid Proof Techniques

13. Proof by vehement assertion : It is useful to have some kind of authority relation to the audience.
14. Proof by ghost reference : Nothing even remotely resembling the cited theorem appears in the reference given.
15. Proof by appeal to intuition : Cloud-shaped drawings frequently help here.

Proof Techniques

- Indirect or by contradiction.
  - Assumes negation of what needs to be proved.
  - Then proves validity of some statement which is a contradiction of already known valid result.
  - So the assumption about negation becomes false, thus proving its complementary.
- Direct: dedactic including mathematical induction or constructive proof.
  - Induction is defined as "infering general from particular" whereas deduction is defined as "infering particular from general"
  - So, they appear to be different, but induction forms the basis. Nothing can be dedued if there are no examples.

Proof by Contradiction

- Consider the following

  There are infinitely many primes.

- Proof: Let P denote the set of all primes. Assume that P is finite. Since 2 is prime we know $P \neq \phi$.
  - Let $x = \prod_{p_i \in P} p_i$, since P is finite and nonempty, this is possible
  - Consider $y = x + 1$. We claim y to be prime.
  - y is not divisible by any of the primes in P.
  - So either y is a prime itself or is divisible by a prime number $p' \notin P$.
  - In either case we have proved existence of a prime not in P.
  - This is a contradiction. So, P is infinite.

Prime Number Generation

- On the basis of the proof we can develop a simple algorithm for prime generation

```
int newPrime(int_set P) {
    x = ∏_{p∈P} p;
    y = x+1;
    d = 1;
    repeat
        d++;
    until d divides y;
    return d;
}
```

- But a simpler algorithm would be

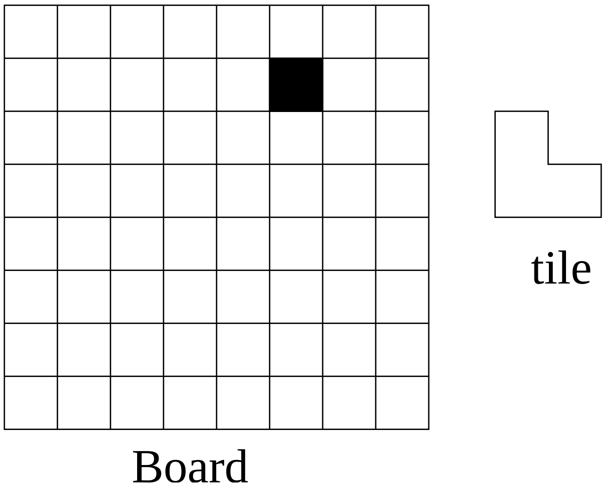
```
int newPrime(int_set P) {
    x = max{p ∈ P}
    repeat
        x++;
    until isPrime(x);
    return x;
}
```


Irrational Number

- There exist two irrational numbers x, y such that x^y is rational.
- Proof: Assume contradiction.
  - Let $x = \sqrt{2}$, which is irrational. Let $z = (\sqrt{2})^{\sqrt{2}}$.
  - z is irrational by assumption.
  - But
    $$z^{\sqrt{2}} = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\times\sqrt{2}} = (\sqrt{2})^2 = 2$$
  - This is a contradiction.

The Tiling Problem

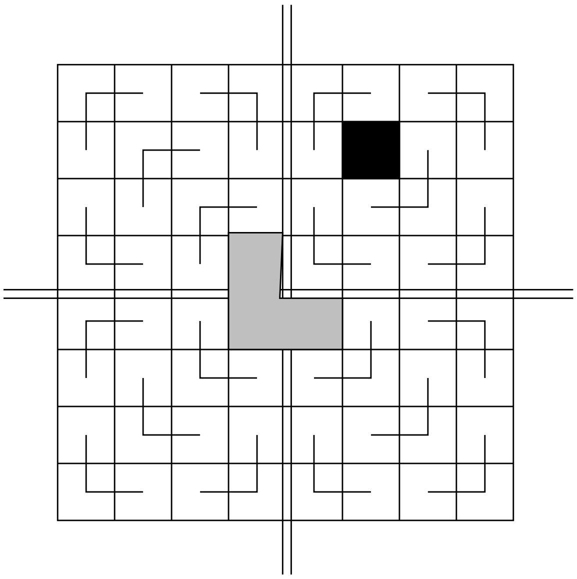
Problem: Consider the board and tile as shown below.



- One arbitrary square (in black) is a special.
- Tiles provided in only shape shown in figure.
- Task is to cover board by tiles leaving special square.

Induction Proof for Tiling

- Clearly solution exist.



Induction Proof for Tiling

- Basis: $n = 0$ trivially satisfied. For 1 square board only special square is there, using zero tiles the square can be covered. For 2×2 square board, if we remove special square then it looks exactly like tile.
- Hypothesis: Let the solution always exist for $2^k \times 2^k$ square board.
- Induction step: Partition the board $2^{k+1} \times 2^{k+1}$ into 4 $2^k \times 2^k$ square boards.
- Put one tile at the center covering three squares, one each from three sub-boards that do not have special square.
- Now consider each of these three sub-boards assuming the covered square as special.
- We have 4 sub-problems of size $2^k \times 2^k$ each. By induction hypothesis each one can be solved.
- So the 4 solutions combined to form solution for the whole.

Horses are of Same Color

- All horses are of same color.
- Basis: For $n = 0$, no horse $\Rightarrow$ it is true. For $n = 1$, the color of only horse is the color of all horses.
- Hypothesis: Let it be true for any number of horses less than n.
- Induction step: Let $\mathcal{H}$ be set $n + 1$ horses.
  - $\mathcal{H}_1$ be set obtained by removing horse h_1.
  - $\mathcal{H}_2$ be set obtained by removing horse h_2.
- Each sets $\mathcal{H}_1$, and $\mathcal{H}_2$ contains n horses. So by induction hypothesis $\mathcal{H}_1$ contains horse of same color, say c_1 and so is $\mathcal{H}_2$ of color c_2.
- Clearly, c_1 must be same as c_2.

Problem in Proof?

$\mathcal{H}_1$:		h_2	h_3	h_4	h_5
$\mathcal{H}_2$:	h_1		h_3	h_4	h_5

- h_{n+1} belongs to both $\mathcal{H}_1$ and $\mathcal{H}_2$.
- Induction step does not apply from n to $n+1$ if h_{n+1} must remain present in both.

Summary

- Powerful invalid proofs are discussed.
- Proofs by contradiction, induction (constructive) are discussed with example.

