Proof Strategies

CMSC 27230: Honors Theory of Algorithms

1 Proofs by Contradiction

In a proof by contradiction, we prove that a statement is true by assuming it is false and deriving a contradiction. The assumption that our statement is false can be very useful as it can give us something concrete to work with.

Two excellent examples of proofs by contradiction are the proof that $\sqrt{2}$ is irrational and a direct proof that there are infinitely many primes.

Theorem 1.1. *$\sqrt{2}$ is irrational.*

Proof. We assume that $\sqrt{2}$ is rational and obtain a contradiction as follows:

1. If $\sqrt{2}$ is rational, we can write $\sqrt{2} = \frac{p}{q}$ where $p, q \in \mathbb{Z}$ have no common factors.

2. Squaring this equation and rearranging it, we obtain that $2q^2 = p^2$. This implies that p is even so we have that $p = 2r$ for some integer r.

3. Now $2q^2 = 4r^2$ so $q^2 = 2r^2$. This implies that q is even so we have that $q = 2s$ for some integer s.

4. We now have that both p and q are divisible by 2 which contradicts our assumption that p and q have no common factors.

□

Theorem 1.2. *There are an infinite number of primes.*

Proof. We need the following elementary proposition. For a brief proof of this proposition (which also uses a proof by contradiction), see the appendix.

Proposition 1.3. *If $n \in \mathbb{N}$ is not divisible by any prime p such that $1 < p < n$ then n is prime.*

With this proposition in hand, we assume that there are are only finitely primes $p_1, \ldots, p_k$ and obtain a contradiction as follows.

1. Let $m = \left(\prod_{i=1}^{k} p_i\right) + 1$.

2. Observe that if we divide m by any of the p_i, the remainder will be 1. Thus, m is not divisible by any prime less than m so by Proposition 1.3, m is prime.

3. $\forall i \in [k](m \neq p_i)$ so m is a new prime which contradicts the assumption that $p_1, \ldots, p_k$ are the only primes.

□

2 Proof by Induction

In a proof by induction, we prove that a statement holds for all integers $n \geq n_0$ as follows:

1. Base case: We prove that the statement holds for $n = n_0$

2. Inductive step: We prove that for all $k \geq n_0$, if the statement holds for $n = k$ then the statement holds for $n = k + 1$.

We can then reason as follows:

1. We proved the statement holds for $n = n_0$.

2. Since the statement holds for $n = n_0$, it holds for $n = n_0 + 1$ as well.

3. Since the statement holds for $n = n_0 + 1$, it holds for $n = n_0 + 2$ as well.

4. Since the statement holds for $n = n_0 + 2$, it holds for $n = n_0 + 3$ as well.

5. Continuing in this way, the statement must hold for all integers $n \geq n_0$.

Proofs by induction are ubiquitous in mathematics and theoretical computer science. One class of problems where they are very effective is evaluating series.

Theorem 2.1. *For all* $n \geq 1$, $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$

Proof. Base case: If $n = 1$ then the equation is true because $\sum_{j=1}^{1} j = \frac{1(1+1)}{2} = 1$.

Inductive step: Assume the equation is true for $n = k$ and consider $n = k + 1$. We have that

$$\sum_{j=1}^{k+1} j = \sum_{j=1}^{k} j + (k+1) = \frac{k(k+1)}{2} + (k+1) = (k+1)\left(\frac{k}{2} + 1\right) = \frac{(k+1)(k+2)}{2}$$

so the equation is true for $n = k+1$ as well. Thus, the equation is true for all $n \geq 1$, as needed. □

Theorem 2.2. *For all* $n \geq 1$, $\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$

Proof. Base case: If $n = 1$ then the equation is true because $\sum_{j=1}^{1} j^2 = \frac{1(1+1)(2*1+1)}{6} = 1$.

Inductive step: Assume the equation is true for $n = k$ and consider $n = k + 1$. We have that

$$\begin{aligned}\sum_{j=1}^{k+1} j^2 &= \sum_{j=1}^{k} j^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= (k+1)\left(\frac{k(2k+1)}{6} + (k+1)\right) = (k+1)\frac{2k^2+k+6k+6}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6}\end{aligned}$$

so the equation is true for $n = k+1$ as well. Thus, the equation is true for all $n \geq 1$, as needed. □

3 Invariants

It can be extremely useful to find invariants which remain the same as we run our algorithms. A classic example where an invariant is very useful is domino tilings.

Problem 3.1. *The domino tiling problem asks whether it is possible to completely cover a shape with 2×1 dominos without having any overlap or going outside of the shape.*

Definition 3.2. *The mutilated chessboard is a chessboard where two opposite corners have been removed.*

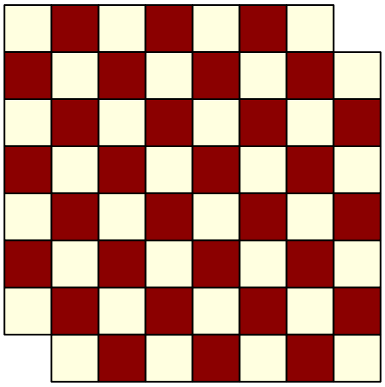

Figure 1: The mutilated chessboard

Theorem 3.3. *It is impossible to cover the mutilated chessboard with 2×1 dominos.*

Proof. We use the following invariant

Definition 3.4. *Let w be the number of white squares which are still uncovered and let b be the number of black squares which are still uncovered.*

Proposition 3.5. *Whenever we place a 2×1 domino, $w - b$ remains the same.*

This invariant immediately implies that we cannot cover the mutilated chessboard with 2×1 dominos. To see this, assume that we had such a domino tiling. If so, we must have that $w - b = 0$ because $w - b = 0$ once everything is covered and $w - b$ remains unchanged as dominos are placed. However, counting directly we see that $w - b = 2$, which is a contradiction. □

4 Advanced Topic: Potential Functions

Potential functions can be very useful for ensuring that our algorithm is making progress and will eventually terminate. A simple example where a potential function is useful is as follows:

Problem 4.1. *There are n people and the ith person starts out with x_i candies. The people decide to share the candies more evenly, so they do the following repeatedly:*

1. *The people look for an i and a j such that person i has at least two more candies than person j.*
2. *If such a pair i, j is found then person i gives a candy to person j.*
3. *If no such pair exists then the process terminates.*

Theorem 4.2. *This process will terminate with everyone having roughly the same number of candies. More precisely, if person i ends up with y_i candies then we will have that $\forall i, j \, (|y_j - y_i| \leq 1)$. Moreover, this process takes at most $\frac{1}{2}\sum_{i=1}^{n} x_i^2$ steps before terminating.*

Proof. We take the potential function $\phi(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^2$.

Lemma 4.3. *At each step, $\phi(x_1, \ldots, x_n)$ decreases by at least 2.*

Proof. We need to show that if $x_i - x_j \geq 2$ then $x_i^2 + x_j^2 \geq (x_i - 1)^2 + (x_j + 1)^2 + 2$. To see this, observe that

$$(x_i - 1)^2 + (x_j + 1)^2 + 2 = x_i^2 - 2x_i + 1 + x_j^2 + 2x_j + 1 + 2 = x_i^2 + x_j^2 - 2(x_i - x_j - 2) \leq x_i^2 + x_j^2$$

□

Using this lemma, note that the potential function $\phi(x_1, \ldots, x_n)$ starts at $\sum_{i=1}^{n} x_i^2$, goes down by at least 2 at each step, and is always non-negative. Thus, there can be at most $\frac{1}{2}\sum_{i=1}^{n} x_i^2$ steps before the process terminates.

Finally, observe that when the process terminates, there cannot be an i and a j such that person i has at least 2 more candies than person j. Thus, we must have that $\forall i, j \, (|y_j - y_i| \leq 1)$, as needed. □

Remark 4.4. *A slightly better potential function would have been $\phi(x_1, \ldots, x_n) = \sum_{i=1}^{n} (x_i - \bar{x})^2$ where $\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n}$, but we took the potential function $\phi(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^2$ for simplicity.*

A Proof of Proposition 1.3

For convenience, we recall the statement of Proposition 1.3 here.

Proposition A.1. *If $n \in \mathbb{N}$ is not divisible by any prime p such that $1 < p < n$ then n is prime.*

Proof. Let p be the smallest integer such that $p > 1$ and n is divisible by p. We claim that p is prime.

To see this, assume that p is not prime. If so, then there exists an integer x such that $1 < x < p$ and p is divisible by x. But then n is divisible by x because n is divisible by p and p is divisible by x. Since $x > 1$, which contradicts the definition of p as the smallest integer such that $p > 1$ and n is divisible by p.

Thus, p must be prime. Since n is not divisible by any prime p such that $1 < p < n$, we must have that $p = n$ and thus n is prime, as needed. □