Discrete Mathematics

Instructor: Alexander Razborov, University of Chicago.
razborov@cs.uchicago.edu
Course Homepage:
http://people.cs.uchicago.edu/~razborov/teaching/autumn13.html

Autumn Quarter, 2013

Contents

Lecture 1

Scribe: Andrew Ding, University of Chicago.
Date: September 30, 2013

Discrete Mathematics is the branch of mathematics focusing on finite objects. During this week, we will discuss a few interesting examples.

1 Euclidean Algorithm

Let a, b be positive integers. We want to find integers x, y such that $ax+by = 1$.

Example 1. $1x + 1y = 1 : (1, 0)$ *is a solution.*
$2x + 3y = 1 : (2, -1)$ *is a solution.*
$5x + 7y = 1 : (3, -2)$ *is a solution.*
$6x + 8y = 1$: *No solution because* 6 *and* 8 *are even.*
$3x + 6y = 1$: *No solution because* 3 *and* 6 *are divisble by 3, but* 1 *is not.*

Definition 2. The **greatest common divisor** of a, b, called $\gcd(a, b)$, is the largest positive integer d such that $d|a$ and $d|b$. ($d|a$ means d divides a).

Strictly speaking, we have to prove that any bounded set of integers has the largest element. But in this introductory course we will not be that fussy and will take things like that "for granted".

We observe that $\gcd(a, b) > 1$ implies no integer solutions to $ax+by = 1$. This is an obstacle. It turns out that this is the only obstacle.

Theorem 3 (Bezout's Theorem)**.** *Let a, b be positive integers such that $\gcd(a, b) = 1$. Then there exist integers x, y such that $ax + by = 1$.*

Proof. We give an algorithm. We take as given the Division Algorithm, which states that for any two positive integers a, b, there exist nonnegative integers q, r such that $a = qb + r$ and $0 \leq r < b$.

```
Bezout(a,b: non-negative, a > b)
  if b=0 and a>1 then {FAIL}
  if b=0 and a=1 then {(1,0)}
  if b>0 then
    a = bq+r
    (x,y) := Bezout(b,r)
    end {(y,x-yq)}
```

Three things can go wrong in an algorithm:

1. Does not halt (i.e. infinite loop).
2. Fails when it is not supposed to fail.
3. Wrong answer.

Now we check each of these:

1. It does not halt because the second term of Bezout strictly decreases, that is, $a > b > r > r' > \cdots \geq 0$, and this chain is finite. This uses the principle called well-foundedness.
2. Lemma: $\gcd(a, b) = gcd(b, r)$, where $a = bq + r$. This is an example of an invariant.
3. If we are given $bx + ry = 1$ and $a = bq + r$, then we can check that $ay + b(x - yq) = 1$. Thus, we can prove that the answer is correct by induction.

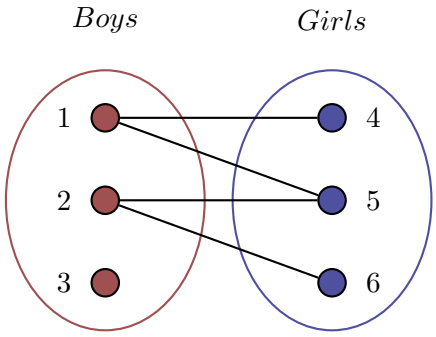

Figure 1: M1

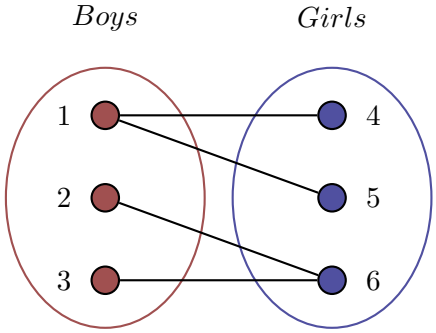

Figure 2: M2

□

This proof is a constructive mathematical proof.

We can modify this algorithm to return $\gcd(a, b)$. This would be the Euclidean Algorithm. The Euclidean algorithm is remarkable because it is fast. It is hard to find the prime divisors of a number, but it is easy to find the shared divisors of two numbers.

2 Perfect Matching Theorem

A village has n boys and n girls. There exists an edge between a boy and a girl if they are willing to marry one another.

Question 4. *Is there a way to match people so everyone is married?*

It is impossible in Figure 1, since there is one boy unwilling to marry.

It is impossible in Figure 2, since the two boys collectively only want to marry one girl.

Obstacle: For $k < n$, if a set of k boys collectively like $k - 1$ or fewer girls, then we are in trouble (Or if k girls collectively like $k-1$ or fewer boys: it is a good exercise to prove that these two conditions are equivalent.)

However, without this obstacle, this problem can be solved (Hall's Theorem, Augmenting Path Algorithm).