Lecture 22: GCD and linear combinations. Induction proof practice.

Dave Naumann

Department of Computer Science
Stevens Institute of Technology

CS 135 Discrete Structures Spring 2015

Review: Euclid's algorithm

Using { this notation } for assertions.

```
{a>0 and b>0 }
x := a; y := b;
while x ≠ y {
   { invariant: gcd(x,y) = gcd(a,b) }
   if x > y then x := x - y;
              else y := y - x;
} { gcd(x,y) = gcd(a,b) ∧ x=y }
{ x = gcd(a,b) }
```

Terminates because every iteration decreases $abs(x-y)$, and ...

Invariant maintained because
$\forall a, b.\ (\ a > b \rightarrow gcd(a, b) = gcd(a-b, b)\ )$

Last assertion follows using $\forall a.\ gcd(a, a) = a$

GCD and linear combinations

Thm: For any integers a, b there are integers s, t such that $gcd(a, b) = sa + tb$.

Proof idea: Add variables s, t to Euclid's algorithm, maintaining the invariant that $x = sa + tb$.

```
{a>0 and b>0 }
x := a; y := b;
s := 1; t := 0;
while x ≠ y {
  { gcd(x,y) = gcd(a,b) ∧ x = s a + t b }
  if x > y then { x := x - y; "update s,t — how?" }
            else { y := y - x; }
}
{ x = gcd(a,b) ∧ x = s a + t b }
```

GCD and linear combinations

Thm: For any integers a, b there are integers s, t such that $gcd(a, b) = sa + tb$.

Proof idea: Add variables s, t to Euclid's algorithm, maintaining the invariant that $x = sa + tb$.

```
{a>0 and b>0 }
x := a; y := b;
s := 1; t := 0;
while x ≠ y {
  { gcd(x,y) = gcd(a,b) ∧ x = s a + t b }
  if x > y then { x := x - y; "update s,t — how?" }
              else { y := y - x; }
}
{ x = gcd(a,b) ∧ x = s a + t b }
```

One solution

Given precondition $x > y \wedge x = sa + tb$, how to update s, t following assignment $x := x - y$ to restore invariant $x = sa + tb$?

After $x := x - y$ we have $x + y = sa + tb$ (why?), so $x = sa + tb - y$.

Add variables s', t' and invariant $y = s'a + t'b$. Now

$$\begin{aligned} x &= sa + tb - y && \text{following } x := x - y \\ &= sa + tb - (s'a + t'b) && \text{using new invariant} \\ &= (s - s')a + (t - t')b && \text{by algebra} \end{aligned}$$

So update $s := s - s'$; $t := t - t'$.

The case $y > x$ is symmetric.

The algorithm finds x, s, t such that $x = gcd(a, b)$ and $x = sa + tb$.

One solution

Given precondition $x > y \wedge x = sa + tb$, how to update s, t following assignment $x := x - y$ to restore invariant $x = sa + tb$?

After $x := x - y$ we have $x + y = sa + tb$ (why?), so $x = sa + tb - y$.

Add variables s', t' and invariant $y = s'a + t'b$. Now

$$
\begin{array}{lll}
x & = sa + tb - y & \text{following } x := x - y \\
 & = sa + tb - (s'a + t'b) & \text{using new invariant} \\
 & = (s - s')a + (t - t')b & \text{by algebra}
\end{array}
$$

So update $s := s - s'$; $t := t - t'$.

The case $y > x$ is symmetric.
The algorithm finds x, s, t such that $x = gcd(a, b)$ and $x = sa + tb$.

Review

If $a \mid b$ and $a \mid c$ then $a \mid (mb + nc)$ for $a, b, c, m, n \in \mathbf{Z}$

For $m \in \mathbf{Z}^+$, $a = (a \textbf{ div } m) \cdot m + (a \textbf{ mod } m)$

If $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$ (for positive integer m) then $a + c \equiv b + d (\text{mod } m)$ and $ac \equiv bd (\text{mod } m)$

$(a + b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$

$ab \textbf{ mod } m = ((a \textbf{ mod } m)(b \textbf{ mod } m)) \textbf{ mod } m$

If $gcd(a, b) = 1$ then a, b are called *relatively prime*

NEW: Linear combination Thm:
$\forall a, b \in \mathbf{Z}^+. \exists s, t \in \mathbf{Z}. \; gcd(a, b) = sa + tb$

Pedestrian proof style

(Be good at this, before indulging in discursive style of textbook.)

Lemma: for $a, b, c \in \mathbf{Z}^+$, if $gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.

Proof: (Assume antecedents, prove consequence.)

1.	$sa + tb = 1$	(for some s, t) by $gcd(a, b) = 1$, Lin Comb Thm
2.	$sac + tbc = c$	from step 1 using arith
3.	$a \mid tbc$	by $a \mid bc$ and property of $\mid$ (what property?)
4.	$a \mid sac$	by $\mid$ property (which?)
5.	$a \mid (sac + tbc)$	from 3 and 4 by a property of $\mid$
6.	$a \mid c$	from 5 and 2

Not just one thing after another. Step 3 is from an assumption. So to be utterly clear we're numbering the reasoning steps to make the logical connections clear.

Pedestrian proof style

(Be good at this, before indulging in discursive style of textbook.)

Lemma: for $a, b, c \in \mathbf{Z}^+$, if $gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.

Proof: (Assume antecedents, prove consequence.)

1.	$sa + tb = 1$	(for some s, t) by $gcd(a, b) = 1$, Lin Comb Thm
2.	$sac + tbc = c$	from step 1 using arith
3.	$a \mid tbc$	by $a \mid bc$ and property of $\mid$ (what property?)
4.	$a \mid sac$	by $\mid$ property (which?)
5.	$a \mid (sac + tbc)$	from 3 and 4 by a property of $\mid$
6.	$a \mid c$	from 5 and 2

Not just one thing after another. Step 3 is from an assumption. So to be utterly clear we're numbering the reasoning steps to make the logical connections clear.

Pedestrian proof style

(Be good at this, before indulging in discursive style of textbook.)

Lemma: for $a, b, c \in \mathbf{Z}^+$, if $gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.

Proof: (Assume antecedents, prove consequence.)

1. $sa + tb = 1$ (for some s, t) by $gcd(a, b) = 1$, Lin Comb Thm
2. $sac + tbc = c$ from step 1 using arith
3. $a \mid tbc$ by $a \mid bc$ and property of $\mid$ (what property?)
4. $a \mid sac$ by $\mid$ property (which?)
5. $a \mid (sac + tbc)$ from 3 and 4 by a property of $\mid$
6. $a \mid c$ from 5 and 2

Not just one thing after another. Step 3 is from an assumption. So to be utterly clear we're numbering the reasoning steps to make the logical connections clear.

Another proof of same lemma

Lemma: for $a, b, c \in \mathbf{Z}^+$, if $gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.

Proof: (Assume antecedents, prove consequence.)

1. $sa + tb = 1$ (for some s, t) by $gcd(a, b) = 1$, Lin Comb Thm
2. $a \mid tbc$ by $a \mid bc$ and first property of $\mid$ on review slide
3. $a \mid sac$ by $\mid$ property (which?)
4. $a \mid (sac + tbc)$ from 2 and 3 by $\mid$ property
5. $a \mid c(sa + tb)$ from 4 by arith.
6. $a \mid c$ from 5 and 1 by arith.

Meticulous but more relaxed proof style

(Only mark things than need to be referred to.)

Lemma: for $a, b, c \in \mathbf{Z}^+$, if $gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.
Proof:
$sa + tb = 1$ . . . (for some s, t) by $gcd(a, b) = 1$, Lin Comb Thm
(*) $sac + tbc = c$ . . . from preceding using arith
$a \mid tbc$ . . . by $a \mid bc$ and property of $\mid$
$a \mid sac$ . . . by another $\mid$ property
$a \mid (sac + tbc)$ . . . by preceding two lines and $\mid$ property
$a \mid c$ . . . from preceding and (*)

Induction exercise

We just proved: If $gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.

Lemma: If p is prime and $p \mid a_1 a_2 \ldots a_n$ then $p \mid a_i$ for some i.

Proof by induction on n.

Base case $n = 1$: If $p \mid a_1$ then $p \mid a_1$. (It's "immediate".)

Case $n > 1$. Hyp: $p \mid a_1 a_2 \ldots a_{n-1} \rightarrow \exists i \ (i \in 1..n-1 \wedge (p \mid a_i))$.

Suppose $p \mid a_1 a_2 \ldots a_n$, to show $p \mid a_i$ for some i.

Subcase $gcd(p, a_n) = 1$: Then by previous lemma, $p \mid a_1 a_2 \ldots a_{n-1}$ so we can use the induction hypothesis and get $i \in 1..n-1$.

Subcase $gcd(p, a_n) \neq 1$: Then since p is prime we have $p \mid a_n$.

Aside: If needed, we could have assumed that $\forall b \ (p \mid b_1 b_2 \ldots b_{n-1} \rightarrow \exists i \ (p \mid b_i))$ (induct "on length of product")

Induction exercise

We just proved: If $gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.

Lemma: If p is prime and $p \mid a_1 a_2 \dots a_n$ then $p \mid a_i$ for some i.
Proof by induction on n.
Base case $n = 1$: If $p \mid a_1$ then $p \mid a_1$. (It's "immediate".)
Case $n > 1$. Hyp: $p \mid a_1 a_2 \dots a_{n-1} \to \exists i \ (i \in 1..n-1 \wedge (p \mid a_i))$.
Suppose $p \mid a_1 a_2 \dots a_n$, to show $p \mid a_i$ for some i.
Subcase $gcd(p, a_n) = 1$: Then by previous lemma,
$p \mid a_1 a_2 \dots a_{n-1}$ so we can use the induction hypothesis and get $i \in 1..n-1$.
Subcase $gcd(p, a_n) \neq 1$: Then since p is prime we have $p \mid a_n$.

Aside: If needed, we could have assumed that
$\forall b \ (p \mid b_1 b_2 \dots b_{n-1} \to \exists i \ (p \mid b_i))$ (induct "on length of product")

Induction exercise

We just proved: If $gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.

Lemma: If p is prime and $p \mid a_1 a_2 \ldots a_n$ then $p \mid a_i$ for some i.
Proof by induction on n.
Base case $n = 1$: If $p \mid a_1$ then $p \mid a_1$. (It's "immediate".)
Case $n > 1$. Hyp: $p \mid a_1 a_2 \ldots a_{n-1} \rightarrow \exists i\ (i \in 1..n-1 \wedge (p \mid a_i))$.
Suppose $p \mid a_1 a_2 \ldots a_n$, to show $p \mid a_i$ for some i.
Subcase $gcd(p, a_n) = 1$: Then by previous lemma,
$p \mid a_1 a_2 \ldots a_{n-1}$ so we can use the induction hypothesis and get
$i \in 1..n-1$.
Subcase $gcd(p, a_n) \neq 1$: Then since p is prime we have $p \mid a_n$.

Aside: If needed, we could have assumed that
$\forall b\ (p \mid b_1 b_2 \ldots b_{n-1} \rightarrow \exists i\ (p \mid b_i))$ (induct "on length of product")

Induction exercise

We just proved: If $gcd(a, b) = 1$ and $a \mid bc$ then $a \mid c$.

Lemma: If p is prime and $p \mid a_1 a_2 \ldots a_n$ then $p \mid a_i$ for some i.
Proof by induction on n.
Base case $n = 1$: If $p \mid a_1$ then $p \mid a_1$. (It's "immediate".)
Case $n > 1$. Hyp: $p \mid a_1 a_2 \ldots a_{n-1} \rightarrow \exists i \; (i \in 1..n-1 \wedge (p \mid a_i))$.
Suppose $p \mid a_1 a_2 \ldots a_n$, to show $p \mid a_i$ for some i.
Subcase $gcd(p, a_n) = 1$: Then by previous lemma,
$p \mid a_1 a_2 \ldots a_{n-1}$ so we can use the induction hypothesis and get $i \in 1..n-1$.
Subcase $gcd(p, a_n) \neq 1$: Then since p is prime we have $p \mid a_n$.

Aside: If needed, we could have assumed that
$\forall b \; (p \mid b_1 b_2 \ldots b_{n-1} \rightarrow \exists i \; (p \mid b_i))$ (induct "on length of product")

Induction exercises

Exercises 31–34 in sect 4.1 of Rosen.

Prove that 2 divides $n^2 + n$ whenever n is a positive integer. (Can also be proved for any integer n, by cases on whether n is even: do the even case first.)

Prove that 3 divides $n^3 + 2n$ whenever n is a positive integer.

Prove that 5 divides $n^5 - n$ whenever n is a nonnegative integer.

Prove that 6 divides $n^3 - n$ whenever n is a nonnegative integer.

One solution

Thm: $2 \mid n^2 + n$ for all $n \in \mathbf{Z}^+$

Proof by induction on n. (By Natalie Barillaro.)

Base case $n = 1$. To prove $2 \mid 1^2 + 1$. Equivalent to $2 \mid 2$, an instance of the lemma $\forall a.\ a \mid a$.

Induction case. To prove: $2 \mid (n+1)^2 + (n+1)$.

1. $2 \mid n^2 + n$ assume induction hypothesis
2. $(n+1)^2 + (n+1) = (n^2 + n) + (2n + 2)$ by algebra
3. $2 \mid 2n + 2$ by property of $\mid$ (i.e., $a \mid a$, lin. comb. thm.)
4. $2 \mid (n^2 + n) + (2n + 2)$ from 1 and 3 by lin. comb.
5. $2 \mid (n+1)^2 + (n+1)$ from 4 using 2