MAU22C00 Lecture 23

John Stalker

Trinity College Dublin

Generalised associative law

Binary operations allow us to take a list of two elements of A and combine them to get a list with just one element of A.

Given a list of three elements of A we can combine two successive elements to get a list of two, then combine those to get a list with just one.

There are two ways to do this. The operation is associative if both give the same result, since $f(f(x,y),z) = f(x,f(y,z))$.

Given a list of four elements of A we can combine two successive elements to get a list of three, then two of those to get a list of two, then those to get a list with just one element.

There are five ways to do this. Do they give the same result?

We expect to need (simple) associativity, but do we need to impose any further conditions?

Products of length 4

Start with the list (w,x,y,z).

We can combine the first two to get $(f(w,x),y,z)$.

Next we can combine the first two or the last two of the new list to get $(f(f(w,x),y),z)$ or $(f(w,x),f(y,z))$.

There is only one way to combine each of these, which gives $(f(f(f(w,x),y),z))$ or $(f(f(w,x),f(y,z)))$.

These are lists with a single item, $f(f(f(w,x),y),z)$ or $f(f(w,x),f(y,z))$.

I could have started by combining the middle two instead, to get $(w,f(x,y),z)$.

From there I can get to $(f(w,f(x,y)),z)$ or $(w,f(f(x,y),z))$.

Combining these lists of two items gives lists of one item. That item is $f(f(w,f(x,y)),z)$ or $f(w,f(f(x,y),z))$.

Products of length 4, continued

Or I could have started by combining the last two, i.e. $(w,x,f(y,z))$.

I have two options for the next step, $(f(w,x),f(y,z))$ and $(w,f(x,f(y,z)))$.

We've already considered the first of these.

The second one leads to the list with the single item $f(w,f(x,f(y,z)))$.

We have five possible results, $f(f(f(w,x),y),z)$, $f(f(w,x),f(y,z))$, $f(f(w,f(x,y)),z)$, $f(w,f(f(x,y),z))$, or $f(w,f(x,f(y,z)))$.

We'll call all of these "products" of length four.

This terminology makes sense when the operation is multiplication. Then the five products are $((w \cdot x) \cdot y) \cdot z$, $(w \cdot x) \cdot (y \cdot z)$, $(w \cdot (x \cdot y)) \cdot z$, $w \cdot ((x \cdot y) \cdot z)$, and $w \cdot (x \cdot (y \cdot z))$.

This terminology can be confusing when the operation is not multiplication. For addition, for example, the "products" are $((w + x) + y) + z$, $(w + x) + (y + z)$, $(w + (x + y)) + z$, $w + ((x + y) + z)$, and $w + (x + (y + z))$.

Products of length 4, continued

Assuming the simple version of the associative law, i.e. that $f(f(x,y),z) = f(x,f(y,z))$ for all x, y and z, is it true that $f(f(f(w,x),y),z)$, $f(f(w,x),f(y,z))$, $f(f(w,f(x,y)),z)$, $f(w,f(f(x,y),z))$, and $f(w,f(x,f(y,z)))$ are all equal for all w, x, y and z?

Yes, by repeated application of the (simple) associative law.

For example,

$$f(f(f(w,x),y),z) = f(f(w,x),f(y,z))$$

and

$$f(f(f(w,x),y),z) = f(f(w,f(x,y)),z)$$

by applying the associative law to either the first or second f in $f(f(f(w,x),y),z)$.

Applying the associative law to either the first or second f in $f(w,f(x,f(y,z)))$ give

$$f(w,f(x,f(y,z))) = f(f(w,x),f(y,z)),$$

and

$$f(w,f(x,f(y,z))) = f(w,f(f(x,y),z)).$$

One way to visualise the product is with trees.

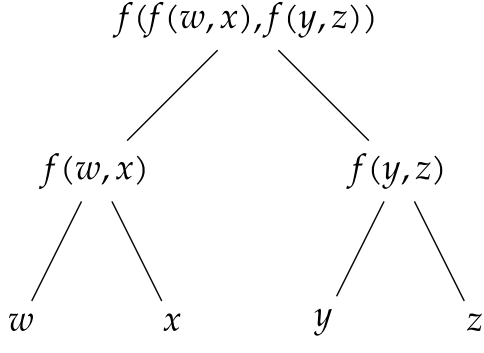

Figure 1: A tree for $f(f(w,x),f(y,z))$

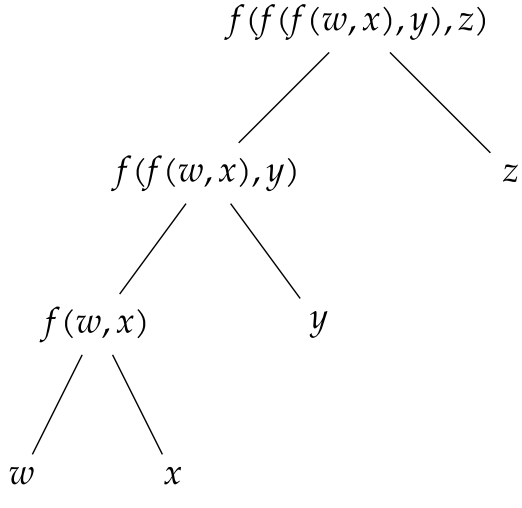

Figure 2: A tree for $f(f(f(w,x),y),z)$

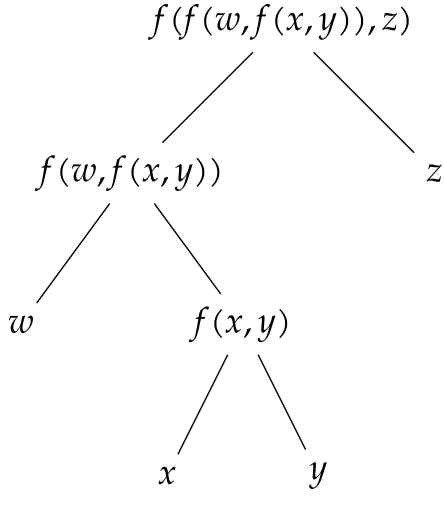

Figure 3: A tree for $f(f(w,f(x,y)),z)$

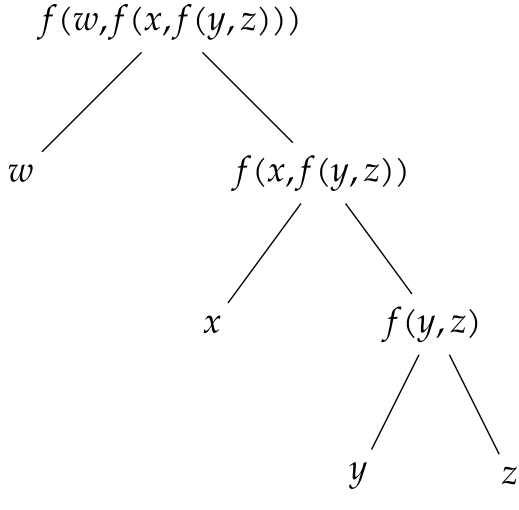

Figure 4: A tree for $f(w,f(x,f(y,z)))$

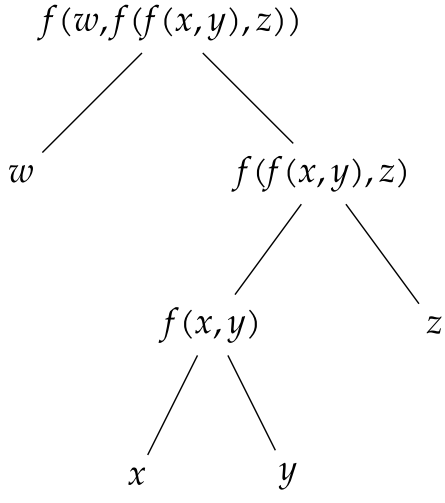

Figure 5: A tree for $f(w,f(f(x,y),z))$

These trees should look familiar from Assignment 0.

Another way to visualise this is with graphs. There's a graph whose vertices are the different "products" and whose edges are the ones which can be shown to be equal with a single application of the associative law.

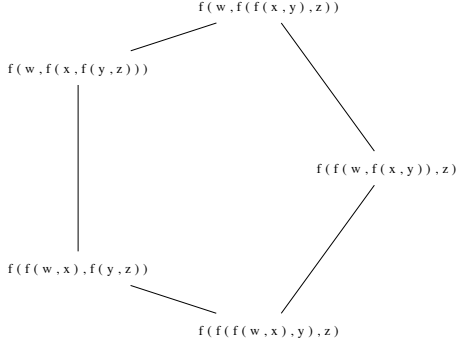

Figure 6: A graph for products of length 4

The fact that this graph is connected implies that the "products" are all equal.

Products of arbitrary length

Can we do this for "products" of length greater than 4?

Can we avoid doing this for "products" of length 4?

Yes, it is possible to prove that all "products" of a non-empty list are equal.

The restriction to non-empty lists is there because we don't have a good way to define the product of the empty list.

For monoids actually we do, the product is the identity, but otherwise we don't.

The details are in the notes, but here are the ideas:

- It suffices to show that every "product" is equal to the "leftmost product".
- One shows that the "product" of "leftmost products" is a "leftmost product" by induction on the length of the second "factor", using the (simple) associative law.
- The general case is by induction on the length, again using the (simple) associative law.
- We use the fact that any "product" is a (simple) "product" of two shorter "factors".

The bicyclic semigroup

A useful example of a monoid is the bicyclic semigroup. Despite the name it is actually a monoid.

The set is N^2, the set of pairs of natural numbers.

The operation is

$$f((a,b),(c,d)) = (a + c - \min(b,c), b + d - \min(b,c)).$$

The identity is $(0,0)$.

It's easy to check that

$$f((a,b),(0,0)) = (a,b)$$

and

$$f((0,0),(c,d)) = (c,d).$$

It's less easy, but straightforward, to check that this operation is associative.

The bicyclic semigroup, continued

What are the invertible elements of the bicyclic semigroup?

The product is $f((a,b),(c,d)) = (a + c - \min(b,c), b + d - \min(b,c))$ and the identity is $(0,0)$.

If $f((a,b),(c,d)) = (0,0)$ and $f((c,d),(a,b)) = (0,0)$ then

$$(a+c-\min(b,c), b+d-\min(b,c)) = (0,0), \quad (c+a-\min(d,a), d+b-\min(d,a)) = (0,0)$$

so

$$(a + c - \min(b,c)) + (b + d - \min(b,c)) + (c + a - \min(d,a)) + (b + d - \min(d,a)) = 0.$$

The left hand side is equal to $2(\max(a,d) + \max(b,c))$.

The only way for this to be zero is if a, b, c and d are all zero.

So the identity is the only invertible element.

Subsemigroups, submonoids, subgroups

If (A,f) is a semigroup, $B \subseteq A$, and $f(x,y) \in B$ whenever $x \in B$ and $y \in B$ then (B,g) is a semigroup, where g is the restriction of f to B^2.

In this case (B,g) is said to be a subsemigroup of (A,f).

Often we just say B is a subsemigroup of A.

If (A,f) is a monoid with identity i, $B \subseteq A$, $i \in B$, and $f(x,y) \in B$ whenever $x \in B$ and $y \in B$ then (B,g) is a monoid, where g is the restriction of f to B^2. Its identity is i.

In this case (B,g) is said to be a submonoid of (A,f). Often we just say B is a submonoid of A.

If (A,f) is a group with identity i, $B \subseteq A$, $i \in B$, the inverse of x is in B for every $x \in B$ and $f(x,y) \in B$ whenever $x \in B$ and $y \in B$ then (B,g) is a group, where g is the restriction of f to B^2. Its identity is i.

In this case (B,g) is said to be a subgroup of (A,f). Often we just say B is a subgroup of A.

Examples

Every semigroup is a subsemigroup of itself; every monoid is a submonoid of itself; every group is a subgroup of itself.

In each monoid the set containing just the identity element is a submonoid, and similarly for subgroups.

The set of powers of two is a submonoid of the natural numbers, with multiplication as the operation. It's not a submonoid if addition is the operation.

Every subset of the natural numbers is a subsemigroup of the natural numbers is a subsemigroup, if the operation is maximum or minimum. For the maximum it's also a submonoid if 0 is a member.

The bicyclic semigroup has several interesting submonoids:

- The set of all pairs of the form $(n, 0)$. We have $f((m, 0), (n, 0)) = (m + n, 0)$.
- The set of all pairs of the form $(0, n)$. We have $f((0, m), (0, n)) = (0, m + n)$.
- The set of all pairs of the form (n, n). We have $f((m, m), (n, n)) = (\max(m, n), \max(m, n))$.