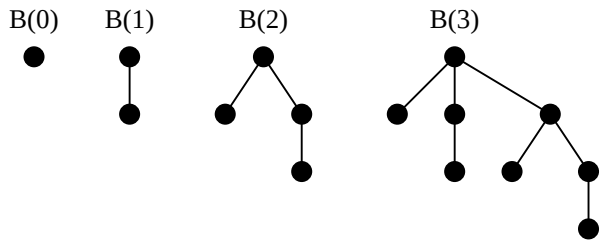
# CS21201 Discrete Structures

## Tutorial 4

### Recursive Constructions, Loop Invariance, Properties of Integers

**1.** Binomial trees $B(n)$ are recursively defined for all $n \in \mathbb{N}_0$ as follows. $B(0)$ is a single node. For $n \geqslant 1$, $B(n)$ consists of a root with $n$ subtrees. The $i$-th subtree of the root is the tree $B(i)$ for $i = 0, 1, 2, \ldots, n-1$. The first four binomial trees are given below.




Prove the following assertions.

**(a)** $B(n)$ contains exactly $2^n$ nodes for all $n \geqslant 0$.

*Solution* Proceed by strong induction on $n$. For $n = 0$, $B(n)$ contains only $2^0 = 1$ node. For $n \geqslant 1$, note that $1 + (2^0 + 2^1 + 2^2 + \cdots + 2^{n-1}) = 2^n$.

**(b)** $B(n)$ contains exactly $2^{n-1}$ leaf nodes for all $n \geqslant 1$.

*Solution* Similar to Part (a).

**(c)** $B(n)$ contains exactly $\binom{n}{i}$ nodes at level $i$ for all $n \geqslant 0$ and for all $i$ (take $\binom{n}{i} = 0$ for $i < n$).

*Solution* Again proceed by strong induction on $n$. For $n = 0$, the statement is obviously true. So let $n \geqslant 1$. The number of nodes in $B(n)$ at level 0 is 1 (only the root), whereas $\binom{n}{0} = 1$. At a level $i \geqslant 1$, the number of nodes in $B(n)$ is $\binom{0}{i-1} + \binom{1}{i-1} + \binom{2}{i-1} + \cdots + \binom{n-1}{i-1}$. On the other hand, $\binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i} = \binom{n-1}{i-1} + \binom{n-2}{i-1} + \binom{n-2}{i} = \binom{n-1}{i-1} + \binom{n-2}{i-1} + \binom{n-3}{i-1} + \binom{n-3}{i} = \cdots = \binom{n-1}{i-1} + \binom{n-2}{i-1} + \binom{n-3}{i-1} + \cdots + \binom{0}{i-1}$.

**2.** *Stirling numbers $S(m,n)$ of the second kind* is the number of ways of partitioning an $m$-set into exactly $n$ non-empty parts. For example, for $m = 4$ and $n = 2$, we have only the following partitions of $\{1,2,3,4\}$ into two subsets: $(\{1\},\{2,3,4\})$, $(\{2\},\{1,3,4\})$, $(\{3\},\{1,2,4\})$, $(\{4\},\{1,2,3\})$, $(\{1,2\},\{3,4\})$, $(\{1,3\},\{2,4\})$, and $(\{1,4\},\{2,3\})$. Therefore $S(4,2) = 7$. Prove that the Stirling numbers $S(m,n)$ of the second kind can be recursively defined as follows.

$$\begin{aligned} S(0,0) &= 1, \\ S(m,0) &= 0 \text{ for } m > 0, \\ S(m,n) &= 0 \text{ for } n > m, \\ S(m,n) &= S(m-1,n-1) + nS(m-1,n) \text{ for } m \geqslant n \geqslant 1. \end{aligned}$$

*Solution* The first three equations follow from the definition. For the last equation, consider the set to be $\{1,2,3,\ldots,m\}$. The element $n$ can itself form a part (a singleton subset) in the partition. In this case, the remaining $m-1$ elements should be partitioned into $n-1$ parts. Otherwise, if $n$ appears in a part with other element(s), then removing $n$ gives a partition of $m-1$ elements into $n$ parts. Finally, note that given such a partition, $n$ can be added to any of the $n$ parts.

**3.** Let us define *falling factorials* as

$$x^{\underline{n}} = x(x-1)(x-2)\cdots(x-n+1).$$

Treat $x$ as a variable here. Prove the polynomial identity $x^m = \sum_{n=0}^{m} S(m,n)x^{\underline{n}}$ for all $m \geqslant 0$.

*Solution* Proceed by induction on $m$. For $m=0$, both sides of the identity evaluate to 1. So take $m \geqslant 1$. Since $S(m,0)=0$ in this case, we have

$$\begin{aligned}\sum_{n=0}^{m} S(m,n)x^{\underline{n}} &= \sum_{n=1}^{m} S(m,n)x^{\underline{n}} \\ &= \sum_{n=1}^{m} \big[S(m-1,n-1)+nS(m-1,n)\big]x^{\underline{n}} \\ &= \sum_{n=1}^{m} S(m-1,n-1)x^{\underline{n}} + \sum_{n=1}^{m} nS(m-1,n)x^{\underline{n}}.\end{aligned}$$

Replacing $n-1$ by $n$ in the first subsum gives

$$\sum_{n=1}^{m} S(m-1,n-1)x^{\underline{n}} = \sum_{n=0}^{m-1} S(m-1,n)x^{\underline{n+1}} = \sum_{n=0}^{m-1} (x-n)S(m-1,n)x^{\underline{n}}.$$

Since $S(m-1,m)=0$, the second subsum is

$$\sum_{n=1}^{m} nS(m-1,n)x^{\underline{n}} = \sum_{n=0}^{m} nS(m-1,n)x^{\underline{n}} = \sum_{n=0}^{m-1} nS(m-1,n)x^{\underline{n}}.$$

Therefore by induction we have

$$\sum_{n=0}^{m} S(m,n)x^{\underline{n}} = \sum_{n=0}^{m-1} (x-n+n)S(m-1,n)x^{\underline{n}} = x\sum_{n=0}^{m-1} S(m-1,n)x^{\underline{n}} = x \times x^{m-1} = x^{m}.$$

**4.** You have six integers $a_1,a_2,a_3,a_4,a_5,a_6$ arranged in the clockwise fashion on a circle. Their initial values are $1,0,1,0,0,0$, respectively. You then run a loop, each iteration of which takes two consecutive integers (that is, $(a_1,a_2)$ or $(a_2,a_3)$ or $\cdots$ or $(a_6,a_1)$), and increments both the chosen integers by 1. Your goal is to make all the six integers equal. Propose a way to achieve this using the above loop (that is, specify which pairs you choose in different iterations), or prove that this cannot be done.

*Solution* Look at the alternating sum $a_1-a_2+a_3-a_4+a_5-a_6$. This is initially 2. The given operation does not change this sum, so it can never attain the value 0.

**5.** What does the following function return upon the input of two positive integers $a,b$? Prove it.

```
int f ( int a, int b )
{
   int x, y, u, v;

   x = u = a; y = v = b;
   while (x != y) {
      if (x > y) {
         x = x - y;
         u = u + v;
      } else {
         y = y - x;
         v = u + v;
      }
   }
   return (u + v)/2;
}
```

*Solution* The function returns $\operatorname{lcm}(a,b)$. The loop maintains the two invariances

$$\begin{aligned}\gcd(x,y) &= \gcd(a,b), \\ vx+uy &= 2ab.\end{aligned}$$

Show that this is true at all the times when the loop condition is checked. The loop terminates when $x=y$. At that time, $\gcd(a,b)=\gcd(x,y)=x=y$, and so $(v+u)\gcd(a,b)=2ab$. But then $(u+v)/2 = ab/\gcd(a,b) = \operatorname{lcm}(a,b)$.

**6.** Let $A$ be a sorted array of $n \geqslant 2$ integers with repetitions allowed. Consider the following variant of binary search for $x$ in $A$. Prove by an invariance property of the loop that the function returns the index of the *first* occurrence of $x$ in $A$ (or $-1$ if $x$ is not present in $A$).

```
int first ( int A[], int n, int x )
{
   int L, R, M;

   if ( (A[0] > x) || (A[n-1] < x) ) return -1;
   if (A[0] == x) return 0;
   L = 0; R = n-1;
   while (R - L > 1) {
      M = (L + R + 1) / 2;
      if (A[M] >= x) R = M; else L = M;
   }
   if (A[R] == x) return R;
   else return -1;
}
```

*Solution* The loop maintains the invariance $A[L] < x \leqslant A[R]$.

**7.** Let $a, b, c$ be non-zero integers. Prove that the equation $ax + by = c$ has integer-valued solutions for $x, y$ if and only if $\gcd(a,b) | c$.

*Solution* [If] Let $d = \gcd(a,b)$, and $c = \gamma d$. By the extended gcd theorem, there exist integers $u, v$ such that $ua + vb = d$. But then, $a(u\gamma) + b(v\gamma) = d\gamma = c$, that is, $x = u\gamma$ and $y = v\gamma$ are integers satisfying $ax + by = c$.

[Only if] For any integer-valued solution $x, y$ of $ax + by = c$, both $ax$ and $by$ are multiples of $\gcd(a,b)$. So their sum $c$ must also be a multiple of $\gcd(a,b)$.

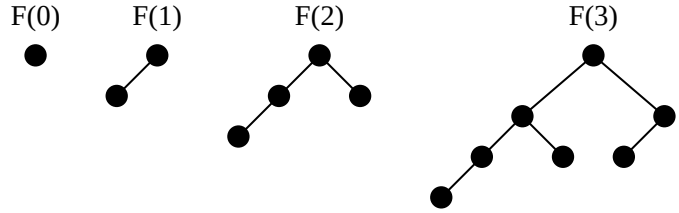
**8.** Let $n \in \mathbb{N}$. Prove that if $2^n - 1$ is prime, then $n$ must be prime. What about the converse?

*Solution* If $n$ is not prime, it has a non-trivial divisor $a$. But then, $2^a - 1$ is a non-trivial divisor of $2^n - 1$.

The converse of the statement is false. For example, $2^{11} - 1 = 2047 = 23 \times 89$.

## Additional Exercises

**9.** Fibonacci trees $F(n)$ are recursively defined for $n \geqslant 0$ as follows. $F(0)$ is a single node. $F(1)$ has two nodes with the root having only a left child. For $n \geqslant 2$, the tree $F(n)$ consists of a root. Its left subtree is $F(n-1)$, and its right subtree is $F(n-2)$. The following figure shows the first four Fibonacci trees.




Prove the following assertions for all $n \geqslant 0$.

**(a)** $F(n)$ contains $F_{n+3} - 1$ nodes (where $F_i$ is the $i$-th Fibonacci number).

**(b)** $F(n)$ contains $F_{n+1}$ leaf nodes.

**(c)** The height of $F(n)$ is $n$.

**(d)** At every non-leaf node $v$ of $F(n)$, the height of the left subtree of $v$ is one more than the height of the right subtree of $v$. (Note that the empty tree has height $-1$, and a single-node tree has height 0.)

**10.** Assume that $m \geqslant n \geqslant 1$. Prove the identity $S(m,n) = \sum_{r=n-1}^{m-1} \binom{m-1}{r} S(r, n-1)$.

**11.** The $n$-th *Bell number* is defined as the total number of partitions of an $n$-set (into any number of parts), so

$$B_n = \sum_{k=0}^{n} S(n,k).$$

Prove the identity $B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$.

**12.** Let $s(n,m)$ denote the number of permutations of $1,2,3,\ldots,n$, that have exactly $m$ cycles. For example, the permutation $3,1,6,8,2,5,7,4$ (for $n=8$) has three cycles $(1,3,6,5,2),(4,8),(7)$. The numbers $s(n,m)$ are called *Stirling numbers of the first kind*. Prove that $s(m,n) = s(m-1,n-1)+(m-1)s(m-1,n)$.

**13.** Define the *rising factorials* as

$$x^{\overline{m}} = x(x+1)(x+2)\cdots(x+m-1).$$

Prove the polynomial identity $x^{\overline{m}} = \sum_{n=0}^{m} s(m,n)x^n$ for all $m \geqslant 0$. How can you express the falling factorial $x^{\underline{m}}$ in terms of the Stirling numbers of the first kind?

**14.** A box contains 100 red marbles, 101 green marbles, and 102 blue marbles. You also have an unlimited external store of marbles of each of these colors. As long as the box contains marbles of at least two different colors, repeat the following: Move two marbles of *different* colors from the box to the store, and then move one marble of the *remaining* color from the store to the box. You stop when all the marbles in the box are of the same color. What is this color?

**15.** Prove using the theory of loop invariance that the following function prints $d,u,v$, where $d = \gcd(x,y) = ux+vy$ with $d \in \mathbb{N}$ and $u,v \in \mathbb{Z}$. Assume that both the arguments $x$ and $y$ are supplied *positive* values.

```
void egcd ( unsigned int x, unsigned int y )
{
   int a1, a2, u1, u2;

   a1 = x; a2 = y; u1 = 1; u2 = 0;
   while (a1 != a2) {
      if (a1 > a2) { a1 = a1 - a2; u1 = u1 - u2; }
      else         { a2 = a2 - a1; u2 = u2 - u1; }
   }
   printf("%d, %d, %d\n", a1, u1, (a1 - u1 * x) / y);
}
```

(**Hint:** There exist *integers* $v_1, v_2$ such that $a_1 = u_1x + v_1y$ and $a_2 = u_2x + v_2y$.)

**16.** Write a modified binary-search function that returns the index of the *last* occurrence of $x$ in an array $A$ (or $-1$ if the search fails). Prove its correctness.

**17.** Let $A$ be an array of $n$ integers with $p_1 = A[0] < A[n-1] = p_2$. We want to make an in-place partitioning of $A$ of the form $LE_1IE_2G$, where the five blocks consist of the following elements of $A$.

1. $L$ consists of elements less than both $p_1$ and $p_2$.
2. $E_1$ consists of elements equal to $p_1$.
3. $I$ consists of elements strictly between $p_1$ and $p_2$.
4. $E_2$ consists of elements equal to $p_2$.
5. $G$ consists of elements greater than both $p_1$ and $p_2$.

Propose an algorithm to solve this problem.

**18.** A positive integer is called a *perfect number* if it is equal to the sum of its positive proper divisors. For example, $6 = 1+2+3$ and $28 = 1+2+4+7+14$ are perfect numbers.

**(a)** Find another perfect number.

**(b)** Let $p$ be a prime such that $2^p - 1$ is prime. Prove that $2^{p-1}(2^p-1)$ is a perfect number.

**19.** Let $n \in \mathbb{N}$ be such that $2^n + 1$ is prime. Prove that $n$ must be a power of 2. What about the converse?

**20.** Let $n \in \mathbb{N}$, $n \geqslant 2$, and $a_1, a_2, \ldots, a_n$ positive integers with $d = \gcd(a_1, a_2, \ldots, a_n)$. Prove that there exist *integers* $u_1, u_2, \ldots, u_n$ such that $u_1a_1 + u_2a_2 + \cdots + u_na_n = d$.

## Hard Exercise

**** 21.** Let $n$ be an *even* perfect number. Prove that $n = 2^{p-1}(2^p-1)$ for a prime $p$ for which $2^p - 1$ is prime.