Lecture Notes for CS 313H, Fall 2011

August 25.

We start by examining *triangular numbers*:

$$T(n) = 1 + 2 + \cdots + n \qquad (n = 0, 1, 2, \ldots).$$

Triangular numbers can be also defined recursively:

$$\begin{aligned}&T(0) = 0,\\ &T(n+1) = T(n) + n + 1,\end{aligned}$$

or using sigma-notation:

$$T(n) = \sum_{i=1}^{n} i.$$

Topics for discussion:

- A closed-form expression for $T(n)$ and various ways of proving it.
- The rate of growth of $T(n)$.
- Combinatorial problems related to triangular numbers.
- A generalization of triangular numbers:

$$S_k(n) = 1^k + 2^k + \cdots + n^k.$$

- A related concept—*factorials*:

$$n! = 1 \cdot 2 \cdot \ldots \cdot n.$$

Here is a closed-form expression for $T(n)$:

$$T(n) = \frac{n^2 + n}{2}.$$

This formula can be also written as

$$T(n) = \frac{n(n+1)}{2}. \tag{1}$$

We will see that it can be proved in many different ways.

Problem 1. By $S_3(n)$ we denote the sum $1^3+2^3+\cdots+n^3$. Calculate $S_3(n)$ for several values of n and guess what a general formula for $S_3(n)$ may look like.

August 30.

One possible approach to proving formula (1) is based on induction. When we want to prove by induction that some statement containing a variable n is true for all nonnegative integers n, we do two things. First we prove the statement when $n = 0$; this part of the proof is called the *basis*. Then we prove the statement for $n + 1$ assuming that it is true for n; this part of the proof is called the *induction step*. (The assumption that the statement is true for n, which is used in the induction step, is called the *induction hypothesis*.)

Once we have completed both the basis and the induction step, we can conclude that the statement holds for all nonnegative integers n. Indeed, according to the basis, in holds for $n = 0$. From this fact, according to the induction step, we can conclude that it holds for $n = 1$. From this fact, according to the induction step, we can conclude that it holds for $n = 2$. And so on.

Here is a proof of formula (1) by induction. *Basis*. When $n = 0$, the formula turns into

$$0 = \frac{0(0+1)}{2},$$

which is correct. *Induction step*. Assume that

$$1+2+\ldots+n = \frac{n(n+1)}{2}.$$

We need to show that

$$1+2+\ldots+n+(n+1) = \frac{(n+1)(n+2)}{2}.$$

Using the induction hypothesis, we calculate:

$$\begin{aligned}
1+2+\ldots+n+(n+1) &= \frac{n(n+1)}{2}+(n+1) \\
&= \frac{n(n+1)+2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}.
\end{aligned}$$

This is the end of the proof.

Problem 2. Prove that for any nonnegative integer n, $7^n + 5$ is a multiple of 6.

Our work on Problem 1 has led us to the conjecture that for any nonnegative integer n

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}. \tag{2}$$

We have also conjectured that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{3}$$

Problem 3. Find a closed-form expression for $1^2+2^2+\cdots+n^2$ geometrically.

Problem 4. Use induction to prove formula (3).

Problem 5. Use induction to prove formula (2).

Problem 6. Use induction to solve Problem 2.

September 1.

Here is another proof of formula (1). Consider the formulas

$$\begin{array}{rcccccc}
(1+1)^2 & = & 1^2 & + & 2\cdot 1\cdot 1 & + & 1^2 \\
(2+1)^2 & = & 2^2 & + & 2\cdot 2\cdot 1 & + & 1^2 \\
(3+1)^2 & = & 3^2 & + & 2\cdot 3\cdot 1 & + & 1^2 \\
 & & & \cdots & & & \\
(n+1)^2 & = & n^2 & + & 2\cdot n\cdot 1 & + & 1^2.
\end{array}$$

By adding the left-hand sides and the right-hand sides, we get:

$$2^2 + 3^2 + 4^2 + \cdots + (n+1)^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 + 2\cdot T(n) + n,$$

or, after subtracting $2^2 + 3^2 + \cdots + n^2$ from both sides,

$$(n+1)^2 = 1^2 + 2\cdot T(n) + n.$$

Solving this equation for $T(n)$ gives formula (1).

Problem 7. Use this method to prove formula (3).

So far we used induction to prove assertions about nonnegative integers. More generally, induction can be used to prove an assertion about all integers that are $\geq n_0$ for some initial value n_0. First we prove the statement when $n = n_0$. Then we prove the statement for $n+1$ assuming that it is true for n, for an arbitrary $n \geq n_0$. Once this is done, we can conclude that the statement holds for all $n \geq n_0$.

Problem 8. Prove that for every $n \geq 4$, $n! > 2^n$.

September 6.

Problem 9. Use calculus to find the smallest value of $2^x - x$.

Problem 10. Find a closed-form expression for

$$\left(1-\frac{1}{4}\right)\left(1-\frac{1}{9}\right)\left(1-\frac{1}{16}\right)\cdots\left(1-\frac{1}{n^2}\right).$$

September 8.

By $P_2(n)$ we denote the number of parts into which a plane is divided by n lines, provided that these lines are in a general position. Similarly, $P_3(n)$ is the number of parts into which space is divided by n planes in a general position.

Problem 11. Find $P_3(4)$.

Problem 12. Find a general formula for $P_2(n)$.

September 13.

Problem 13. Find a closed-form expression for $P_3(n)$.

The following approximate formula is often useful: for large values of n,

$$f(1) + f(2) + \cdots + f(n) \approx \int_0^n f(x)dx. \tag{4}$$

It shows, for instance, that for large values of n

$$S_k(n) \approx \frac{1}{k+1} n^{k+1}.$$

The *n-th harmonic number* is defined by the formula

$$H(n) = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}.$$

In application to harmonic numbers, formula (4) tells us that for large values of n

$$H(n) \approx \ln n.$$

Problem 14. Use formula (4) to estimate $n!$.

September 15.

Problem 15. A slow but persistent worm, W, starts at one end of a foot-long rubber band and crawls one inch per minute toward the other end. At the end of each minute an equally persistent keeper of the band, K, whose sole purpose in life is to frustrate W, stretches it one foot. Thus after one minute of crawling, W is 1 inch from the start and 11 from the finish; then K stretches the band one foot. During the stretching operation W maintains his relative position, so that W is now 2 inches from the starting point and 22 inches from the goal. After W crawls for another minute the score is 3 inches traveled and 21 to go; but K stretches, and the distances become 4.5 and 31.5. And so on. Does the worm ever reach the finish? (We are assuming an infinite longevity for W and K, an infinite elasticity of the band, and an infinitely tiny worm.)

As we have seen, the claim that some statement is true for all nonnegative integers can be sometime proved by induction. In some cases, *strong* induction is more useful. In a proof by strong induction we show that the statement is true for a nonnegative integer n assuming that it is true for each nonnegative integer that is $< n$. As in the case of simple ("weak") induction, we can talk about the integers beginning with some initial value n_0, instead of nonnegative integers.

September 20.

Fibonacci numbers are defined by the formulas

$$\begin{aligned}&Fib(0) = 0,\\&Fib(1) = 1,\\&Fib(n+2) = Fib(n) + Fib(n+1) \qquad (n \geq 0).\end{aligned}$$

Problem 16. Prove that

$$Fib(1) + Fib(2) + \ldots + Fib(n) = Fib(n+2) - 1.$$

Problem 17. Prove that

$$Fib(1)^2 + Fib(2)^2 + \ldots + Fib(n)^2 = Fib(n)Fib(n+1).$$

September 22.

Problem 18. Find all values of n such that $Fib(n) < 1.1^n$.

About a function f defined on nonnegative integers we say that it is a *generalized Fibonacci function* if it satisfies the equation

$$f(n+2) = f(n) + f(n+1).$$

Problem 19. A generalized Fibonacci function f satisfies the conditions $f(0) = 1$, $f(6) = 3$. Find $f(3)$.

Problem 20. Find a formula that expresses $f(n)$ for any generalized Fibonacci function f in terms of $f(0)$, $f(1)$, and n. The formula may use the standard Fibonacci function Fib.

Problem 21. Find a number c such that the sequence of its powers $f(n) = c^n$ is a generalized Fibonacci function.

September 27.

Problem 22. Find numbers a, b such that

$$Fib(n) = a\left(\frac{1+\sqrt{5}}{2}\right)^n + b\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

October 4.

Problem 23. Function f is defined by the formula

$$f(n) = \begin{cases} n-10, & \text{if } n > 100, \\ f(f(n+11)), & \text{otherwise.} \end{cases}$$

Find $f(98)$.

For any nonnegative integers m, n, the *binomial coefficient* $\binom{n}{m}$ (read "n choose m") is the number ways to choose an m-element subset from an n-element set. Binomial coefficients can be calculated using the formula

$$\binom{n}{m} = \frac{n(n-1)\cdots(n-m+1)}{m!}.$$

When $m \leq n$, this formula can be rewritten as

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}.$$

Problem 24. Prove that

$$\binom{n+1}{m+1} = \binom{n}{m} + \binom{n}{m+1}.$$

This formula, combined with the initial conditions

$$\binom{n}{0} = 1, \quad \binom{0}{m+1} = 0,$$

provides a recursive definition of binomial coefficients.

Problem 25. Prove the binomial theorem:

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n}b^n.$$

October 6.

Problem 26. Prove by induction:

$$0 \cdot \binom{n}{0} + 1 \cdot \binom{n}{1} + 2 \cdot \binom{n}{2} + \cdots + n \cdot \binom{n}{n} = n \cdot 2^{n-1}.$$

Stirling numbers (of the first kind) are coefficients in the expansion of the polynomial $x(x+1)(x+2)\cdots(x+n-1)$:

$$x(x+1)(x+2)\cdots(x+n-1) = \begin{bmatrix} n \\ 0 \end{bmatrix} + \begin{bmatrix} n \\ 1 \end{bmatrix} x + \begin{bmatrix} n \\ 2 \end{bmatrix} x^2 + \cdots \begin{bmatrix} n \\ n \end{bmatrix} x^n.$$

For instance,

$$x(x+1)(x+2)(x+3) = 6x + 11x^2 + 6x^3 + x^4;$$

consequently,

$$\begin{bmatrix} 4 \\ 0 \end{bmatrix} = 0, \quad \begin{bmatrix} 4 \\ 1 \end{bmatrix} = 6, \quad \begin{bmatrix} 4 \\ 2 \end{bmatrix} = 11, \quad \begin{bmatrix} 4 \\ 3 \end{bmatrix} = 6, \quad \begin{bmatrix} 4 \\ 4 \end{bmatrix} = 1.$$

Problem 27. Find a formula expressing $\left[\begin{smallmatrix} n+1 \\ m+1 \end{smallmatrix}\right]$ in terms of $\left[\begin{smallmatrix} n \\ m \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} n \\ m+1 \end{smallmatrix}\right]$.

October 11.

Problem 28. Prove that for all $n > 0$

$$\begin{bmatrix} n \\ 1 \end{bmatrix} = (n-1)!.$$

Problem 29. Prove that for all $n > 0$

$$\begin{bmatrix} n \\ n-1 \end{bmatrix} = T(n-1).$$

Problem 30. Prove that for all $n > 0$

$$\begin{bmatrix} n \\ 2 \end{bmatrix} = (n-1)! \cdot H(n-1).$$

October 13.

Problem 31. Prove that for all $n \geq 0$

$$0 \cdot \begin{bmatrix} n \\ 0 \end{bmatrix} + 1 \cdot \begin{bmatrix} n \\ 1 \end{bmatrix} + 2 \cdot \begin{bmatrix} n \\ 2 \end{bmatrix} + \cdots + n \cdot \begin{bmatrix} n \\ n \end{bmatrix} = n! \cdot H(n).$$

October 18.

A *set* is a collection of objects. We write $x \in A$ if object x is an element of set A, and $x \notin A$ otherwise.

The set whose elements are $x_1, \ldots, x_n$ is denoted by $\{x_1, \ldots, x_n\}$. The set $\{\,\}$ is called *empty* and denoted also by $\emptyset$. The set of nonnegative integers is denoted by $\mathbf{N}$:

$$\mathbf{N} = \{0, 1, 2, \ldots\}.$$

When we specify which objects belong to a set, this defines the set completely; there is no such thing as the order of elements in a set or the number of repetitions of an element in a set. For instance,

$$\{2, 3\} = \{3, 2\} = \{2, 2, 3\}.$$

If C is a condition, then by $\{x \;:\; C\}$ we denote the set of all objects x satisfying this condition. For instance,

$$\{x \;:\; x = 2 \text{ or } x = 3\}$$

is the same set as $\{2, 3\}$.

If A is a set and C is a condition, then by $\{x \in A \;:\; C\}$ we denote the set of all elements of A satisfying condition C. For instance, $\{2, 3\}$ can be also written as

$$\{x \in \mathbf{N} \;:\; 1 < x < 4\}.$$

If a set A is finite then the number of elements of A is also called the *cardinality* of A and denoted by $|A|$. For instance,

$$|\emptyset| = 0,\ |\{2, 3\}| = 2.$$

We say that a set A is a *subset* of a set B, and write $A \subseteq B$, if every element of A is an element of B. For instance,

$$\emptyset \subseteq \mathbf{N},\ \{2, 3\} \subseteq \mathbf{N},\ \mathbf{N} \subseteq \mathbf{N}.$$

For any sets A and B, by $A \cup B$ we denote the set

$$\{x \;:\; x \in A \text{ or } x \in B\},$$

called the *union* of A and B. By $A \cap B$ we denote the set

$$\{x \;:\; x \in A \text{ and } x \in B\},$$

called the *intersection* of A and B. For instance,

$$\{2,3\} \cup \{3,5\} = \{2,3,5\},$$
$$\{2,3\} \cap \{3,5\} = \{3\}.$$

Problem 32. For any sets A, B, C, if

$$A \cap B \neq \emptyset,\ A \cap C \neq \emptyset,\ B \cap C \neq \emptyset$$

then $A \cap B \cap C \neq \emptyset$. True or false?

Problem 33. Let $|A| = 3$, $|B| = 4$. What can you say about the cardinalities of $A \cup B$ and $A \cap B$?

By $A \setminus B$ we denote the set

$$\{x \ :\ x \in A \text{ and } x \notin B\},$$

called the *difference* of A and B. For instance,

$$\{2,3\} \setminus \{3,5\} = \{2\}.$$

Problem 34. Let $|A| = 3$, $|B| = 4$. What can you say about the cardinalities of $A \setminus B$ and $B \setminus A$?

The *Cartesian product* of sets A and B is the set of ordered pairs $\langle x, y\rangle$ such that $x \in A$ and $y \in B$:

$$A \times B = \{\langle x, y\rangle \mid x \in A \text{ and } \ y \in B\}.$$

For instance,

$$\begin{aligned}\{1,2\} \times \{2,3,4,5,6\} \quad = \quad & \{\langle 1,2\rangle,\ \langle 1,3\rangle,\ \langle 1,4\rangle,\ \langle 1,5\rangle,\ \langle 1,6\rangle, \\ & \ \langle 2,2\rangle,\ \langle 2,3\rangle,\ \langle 2,4\rangle,\ \langle 2,5\rangle,\ \langle 2,6\rangle\}.\end{aligned}$$

Problem 35. Determine whether the following assertions are true. (a) For any sets A and B, $A \times B = B \times A$. (b) For any sets A and B, if A is infinite then $A \times B$ is infinite too. (c) For any sets A and B, if $|A \times B| = 91$ then one of the sets A, B is a singleton.

October 20.

The cardinality of the union of two sets can be determined if we know their cardinalities and the cardinality of their intersection:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

This formula is called the *inclusion-exclusion principle*. Similar formulas can be written for the union of several sets.

Problem 36. Use a set diagram to simplify the expression

$$(A \setminus B) \cup (B \setminus C) \cup (C \setminus A) \cup (A \cap B \cap C).$$

October 25.

By $\mathcal{P}(A)$ we denote the *power set* of a set A, that is, the set of all subsets of A. The cardinality of $\mathcal{P}(A)$ is $2^{|A|}$.

Problem 37. For any sets A, B,

$$\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B).$$

True or false?

Problem 38. For any pair of different sets A and B, $\mathcal{P}(A)$ is different from $\mathcal{P}(B)$. True or false?

Set-theoretic notation can be used to represent some English phrases by mathematical formulas. For instance, the assertion

"A is the set of roots of the polynomial $x^2 + px + q$"

can be written as

$$A = \{x \in \mathbf{R} : x^2 + px + q = 0\}.$$

Instead of

"All elements of A are roots of the polynomial $x^2 + px + q$"

we can write

$$A \subseteq \{x \in \mathbf{R} : x^2 + px + q = 0\}.$$

November 3.

A *binary relation* on a set A is a subset of $A \times A$. If R is a binary relation then we write xRy instead of $\langle x, y \rangle \in R$.

A relation R on a set A is said to be

- *reflexive* if, for all $x \in A$, xRx;
- *symmetric* if, for all $x, y \in A$, xRy implies yRx;
- *transitive* if, for all $x, y, z \in A$, xRy and yRz imply xRz.

Problem 39. There are 2^{16} binary relations on the set $\{1, 2, 3, 4\}$. How many of them are reflexive? Symmetric? Both reflexive and symmetric?

Problem 40. (a) Consider the relation R on the set $\mathbf{N}$ of nonnegative integers defined by the condition: xRy if $x \geq y + 5$. Is it reflexive? Is it symmetric? Is it transitive? (b) Answer the same questions for the relation: xRy if $|x - y| < 5$.

November 8.

A binary relation R on a set A can be visualized as the directed graph with the set of vertices A that has an edge from a vertex x to a vertex y whenever xRy.

A binary relation on a finite set $\{a_1, \ldots, a_n\}$ can be represented by its *adjacency matrix*— an $n \times n$ matrix such that the entry at the intersection of column i and row j is

$$\begin{array}{l} 1 \text{ if } a_i R a_j, \\ 0 \text{ otherwise.} \end{array}$$

If a relation is reflexive, symmetric, and transitive, then we say that it is an *equivalence relation*. If R is an equivalence relation on a set A, and x is an element of A, then the set $\{y \in A : xRy\}$ is called the *equivalence class* of x and is denoted by $[x]$. The set of all equivalence classes of an equivalence relation R is called the *quotient set* of R.

Problem 41. Prove that the equivalence classes of any equivalence relation are pairwise disjoint.

A *partition* of a set A is a set P of non-empty subsets of A such that each element of A belongs to a unique element of P. The quotient set of any equivalence relation is a partition. The other way around, any partition is the quotient set of some equivalence relation.

Problem 42. Find all partitions of the set $\{1, 2, 3\}$. For each of them, represent the corresponding equivalence relation as a graph and as an adjacency matrix.

Problem 43. Does there exist a partition of $\mathbf{N}$ with infinitely many equivalence classes such that all of them are infinite?

A relation R on a set A is *antisymmetric* if, for all $x, y \in A$, xRy and yRx imply $x = y$. A *partial order* is a relation that is reflexive, antisymmetric, and transitive. A *total order* on a set A is a partial order R on A such that for all $x, y \in A$, xRy or yRx.

November 10.

A *function* from a set A to a set B is a subset f of $A \times B$ satisfying the following condition: for every element x of A there exists a unique element y of B such that $\langle x, y\rangle \in f$. This element y is called the *value* of f at x and is denoted by $f(x)$. Set A is called the *domain* of f, and B is called the *co-domain* of f. The subset of the co-domain B consisting of the values $f(x)$ for all $x \in A$ is called the *range* of f.

Problem 44. Let $A = \{1, 2, 3\}$, $B = \{2, 3, 4, 5\}$. Find the number of functions from A to B and the number of functions from B to A.

In the following examples, the domain of each function is the set $\mathbf{S}$ of all bit strings:

$$\mathbf{S} = \{\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, \ldots\}.$$

1. Function l from $\mathbf{S}$ to $\mathbf{N}$: $l(x)$ is the length of x. For instance, $l(00110) = 5$.

2. Function z from $\mathbf{S}$ to $\mathbf{N}$: $z(x)$ is the number zeroes in x. For instance, $z(00110) = 3$.

3. Function n from $\mathbf{S}$ to $\mathbf{N}$: $n(x)$ is the number represented by x in binary notation. For instance, $n(00110) = 6$.

4. Function e from $\mathbf{S}$ to $\mathbf{S}$: $e(x)$ is the string $1x$. For instance, $t(00110) = 100110$.

5. Function r from $\mathbf{S}$ to $\mathbf{S}$: $r(x)$ is the string x reversed. For instance, $r(00110) = 01100$.

6. Function p from $\mathbf{S}$ to $\mathcal{P}(\mathbf{S})$: $p(x)$ is the set of prefixes of x. For instance, $p(00110) = \{\epsilon, 0, 00, 001, 0011, 00110\}$.

If the range of f is the whole co-domain B then we say that f is a function *onto* B. A function f from A to B is called *one-to-one* if, for any pair of different elements x, y of A, $f(x)$ is different from $f(y)$. If a function f is both onto and one-to-one then we say that f is a *bijection*.

November 17.

Problem 45. Which of the functions l, z, n, e, r, p defined above are one-to-one?

If f is a function from A to B, and g is a function from B to C, then the *composition* of these functions is the function h from A to C defined by the formula $h(x) = g(f(x))$. This function is denoted by $g \circ f$.

Problem 46. For the functions l, z, n, e and r defined above, which of the following formulas are true?

- $l \circ r = l$,
- $z \circ r = z$,
- $n \circ r = n$,
- $e \circ r = r \circ e$.

If f is a bijection from A to B then the *inverse* of f is the function g from B to A such that, for every $x \in A$, $g(f(x)) = x$. This function is denoted by f^{-1}.

Problem 47. Find all bijections f from $\{1,2,3\}$ to $\{1,2,3\}$ such that $f^{-1} \neq f$.

Now we turn to the study of logical notation, the last topic in this course.

Truth values are the symbols F ("false") and T ("true"). *Propositional connectives* are functions that are applied to truth values and return truth values. We will use these propositional connectives:

$\neg$	"not" (negation)
$\wedge$	"and" (conjunction)
$\vee$	"or" (disjunction)
$\rightarrow$	"implies" (implication)
$\leftrightarrow$	"is equivalent to" (equivalence)

Negation is a unary connective (takes one argument); the others are binary (take two arguments). Here are the tables of values for these connectives:

p	$\neg p$
F	T
T	F

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
F	F	F	F	T	T
F	T	F	T	T	F
T	F	F	T	F	F
T	T	T	T	T	T

Propositional variables are variables for truth values, such as p and q in the tables above. *Propositional formulas* are built from truth values and propositional variables using propositional connectives. For instance,

$$\neg(p \vee q) \rightarrow (r \leftrightarrow \mathsf{F})$$

is a propositional formula.

November 22.

The *truth table* of a propositional formula shows its truth values for all possible combinations of values of its variables. For instance:

p	q	r	$\neg(p \vee q) \rightarrow (r \leftrightarrow \mathsf{F})$
F	F	F	T
F	F	T	F
F	T	F	T
F	T	T	T
T	F	F	T
T	F	T	T
T	T	F	T
T	T	T	T

Problem 48. Find a propositional formula that gets the value T in two cases: when $p = \mathsf{T}$, $q = \mathsf{F}$, $r = \mathsf{T}$ and when $p = \mathsf{T}$, $q = \mathsf{T}$, $r = \mathsf{F}$.

About propositional formulas F and G we say that they are *equivalent* to each other if, for each combination of the values of their variables, the truth value of F equals the truth value of G. For example,

$$\begin{array}{rll} p \rightarrow q & \text{is equivalent to} & \neg p \vee q, \\ p \leftrightarrow q & \text{is equivalent to} & (p \wedge q) \vee (\neg p \wedge \neg q), \\ \mathsf{F} & \text{is equivalent to} & p \wedge \neg p, \\ \mathsf{T} & \text{is equivalent to} & p \vee \neg p. \end{array}$$

Using these four facts, we can eliminate from any propositional formula the connectives $\rightarrow$ and $\leftrightarrow$ and the constants F and T. In other words, any propositional formula can be equivalently rewritten as a formula formed from variables using the connectives $\neg$, $\wedge$ and $\vee$.

Here are two other useful facts about the equivalence of propositional formulas:

$$\begin{array}{lll} \neg(p \vee q) & \text{is equivalent to} & \neg p \wedge \neg q, \\ \neg(p \wedge q) & \text{is equivalent to} & \neg p \vee \neg q. \end{array}$$

These facts are called *De Morgan's laws*.

Propositional variables are also called *atoms*. Atoms and negated atoms, such as p and $\neg p$, are called *literals*. A propositional formula is said to be in *negation normal form* if it is formed from literals using conjunctions ($\wedge$) and disjunctions ($\vee$). Any propositional formula can be equivalently rewritten in negation normal form in two steps:

- eliminate $\rightarrow$, $\leftrightarrow$, F, T, as described above;
- use De Morgan's laws to push the negations inside.

A propositional formula is said to be in *conjunctive normal form (CNF)* if it is a conjunction of disjunctions of literals. A propositional formula is said to be in *disjunctive normal form (DNF)* if it is a disjunction of conjunctions of literals. For instance, the formula

$$\neg p \vee (p \wedge q) \vee (\neg q \wedge r \wedge \neg s)$$

is in disjunctive normal form.

A formula in negation normal form can be turned into CNF by distributing disjunction over conjunction, and to DNF by distributing conjunction over disjunction.

Problem 49. Convert the formulas

$$(p \rightarrow q) \rightarrow r$$

and

$$p \leftrightarrow (q \wedge r)$$

to CNF and DNF.

A propositional formula is called a *tautology* if each of its truth values is T.

Problem 50. Determine which of these formulas are tautologies:

$$\begin{gathered}(p \rightarrow q) \vee (q \rightarrow p), \\ ((p \rightarrow q) \rightarrow p) \rightarrow p, \\ (p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r)).\end{gathered}$$

November 22.

In logical formulas, we use the propositional connectives introduced above and the *quantifiers* $\forall$ ("for all") and $\exists$ ("exists").

Problem 51. Express in logical notation:

1. $A \subseteq B \cup C$
2. $A = B \cup C$
3. $A = \{a, b\}$

Problem 52. Express in logical notation using variables for nonnegative integers:

1. Number n can be represented as the sum of two complete squares.
2. Number n is composite.