Math 231, Fall 2014 — Boris Botvinnik

Summary on Lecture 5, October 13, 2014

- **Logical equivalence.** Recall that two propositions $s_1$ and $s_2$ are logically equivalent if $s_1$ is true if and only if $s_2$ is true. We use the notation: $s_1 \Longleftrightarrow s_2$ **Examples:**

  (a) $(p \to q) \Longleftrightarrow (\neg p \vee q)$,

  (b) $(p \to q) \Longleftrightarrow (\neg q \to \neg q)$.

- **The Laws of logic.**

  (1) $\neg\neg p \Longleftrightarrow p$ — Double negation

  (2) $\neg(p \vee q) \Longleftrightarrow (\neg p \wedge \neg q)$
  $\neg(p \wedge q) \Longleftrightarrow (\neg p \vee \neg q)$ — DeMorgan Laws

  (3) $(p \vee q) \Longleftrightarrow (q \vee p)$
  $(p \wedge q) \Longleftrightarrow (q \wedge p)$ — Commutativity Laws

  (4) $(p \vee q) \vee r \Longleftrightarrow p \vee (q \vee r)$
  $(p \wedge q) \wedge r \Longleftrightarrow p \wedge (q \wedge r)$ — Associativity Laws

  (5) $[p \vee (q \wedge r)] \Longleftrightarrow [(p \vee q) \wedge (p \vee r)]$
  $[p \wedge (q \vee r)] \Longleftrightarrow [(p \wedge q) \vee (p \wedge r)]$ — Distributive Laws

  (6) $p \wedge p \Longleftrightarrow p$
  $p \vee p \Longleftrightarrow p$ — Idempotent Laws

  (7) $p \vee \mathbf{F}_0 \Longleftrightarrow p$
  $p \wedge \mathbf{T}_0 \Longleftrightarrow p$ — Identity Laws

  (8) $p \wedge \neg p \Longleftrightarrow \mathbf{F}_0$
  $p \vee \neg p \Longleftrightarrow \mathbf{T}_0$ — Inverse Laws

  (9) $p \wedge \neg \mathbf{F}_0 \Longleftrightarrow \mathbf{F}_0$
  $p \vee \neg \mathbf{T}_0 \Longleftrightarrow \mathbf{T}_0$ — Domination Laws

  (10) $[p \vee (p \wedge q)] \Longleftrightarrow p$
  $[p \wedge (p \vee q)] \Longleftrightarrow p$ — Absorbtion Laws

(10)

| $p$ | $q$ | $p \vee (p \wedge q)$ | $p \wedge (p \vee q)$ |
|---|---|---|---|
| 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 |

(5)

| $p$ | $q$ | $r$ | $p \vee (q \wedge r)$ | $(p \vee q) \wedge (p \vee r)$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 |

(a) Show that the implication $[p \wedge (p \to q)] \to q$ is a tautology.

(b) Show that $(p \to q) \Longleftrightarrow (p \wedge q)$ is not a tautology.

(c) Show that the implication $(p \wedge q) \to (p \vee q)$ is a tautology.

- **First examples of proofs.**

  (a) *If $n^2$ is even, then $n$ is even.*
  **Proof.** Indeed, assume that $n$ is odd, i.e., $n = 2k + 1$, then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$ is odd. We showed that the implication

  $$\{ n \text{ is odd}\} \to \{ n^2 \text{ is odd}\} \quad (\neg q \to \neg p)$$

  is true. It is equivalent to the implication

  $$\{ n^2 \text{ is even}\} \to \{ n \text{ is even}\} \quad (p \to q)$$

  which is true as well.

  (b) *$\sqrt{2}$ is irrational number.*
  **Proof.** Assume that $\sqrt{2} = \frac{m}{n}$, where $m, n \in \mathbf{Z}_+$, $n \neq 0$, and $m$, $n$ do not have common divisors, i.e., $\gcd(m,n) = 1$. Then we have: $2n^2 = m^2$. Thus $m^2$ is even, then by (a), $m$ is even, i.e., $m = 2k$. We obtain $2n^2 = 4k^2$ or $n^2 = 2k^2$, i.e., $n$ is even as well. We obtain that $m$, $n$ do have a common divisor 2. Contradiction. Thus $\sqrt{2}$ is irrational number.

Let $n, k \in \mathbf{Z}_+$. Recall that $k$ divides $n$ if $n = k \cdot i$ for some $i \in \mathbf{Z}_+$. We denote $k|n$ if $k$ divides $n$. Then a number $p \in Z_+$ is *prime* if it has no divisors other than 1 and $p$. Here is the list of first few prime numbers:

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 83, 89, 97, 101, \ldots$

The closest two prime numbers to 2014 are 2011 and 2017.

There is a remarkable property of positive integers: *Let $S \subset \mathbf{Z}_+$ be a non-empty subset. Then $S$ has a minimal element, i.e. such $n_0 \in S$ that $n_0 \leq n$ for any $n \in S$.* We will return this later on, this property is called *Well Ordering Principle,* see Chapter 3 of the textbook.

  (c) Let $n \in \mathbf{Z}_+$. Then $n$ is either a prime number or there exists a prime $p$ such that $p$ divides $n$.
  **Proof.** Assume there are integers $n$ which are not primes and no prime $p$ divides $n$. Let $S$ be a set of such integers, and $n_0 \in S$ is a minimal number. Since $n_0$ is not a prime, there exists $n_1 < n_0$ with divides $n_0$. Since $n_1 < n_0$, $n_1$ is either prime or it is divisible by a prime. We arrive to a contradiction in both cases.

  (d) Now we can follow Euclid (who notice that more than 2500 years ago) to prove the following
  **Theorem.** *There is infinite number of primes.*
  **Proof.** Assume there exist only finite number of primes. Let $P = \{p_1, p_2, \ldots, p_k\}$ is the set of all prime numbers, $|P| = k$. Consider the integer: $p_{k+1} = p_1 \cdot p_2 \cdots p_k + 1$. The integer $p_{k+1}$ is either pime or not. If $p_{k+1}$ is not a prime, then it has to be divisible by some prime $p_j$, $j = 1, \ldots, k$, but it is not since the remainder will be 1. Thus $p_{k+1}$ is a prime, and $p_{k+1} \in P$. Then $|P| = k + 1$, not $|P| = k$. This two properties cannot hold together. Contradiction.

- **Contradiction and other rules of inference.** Above we followed the same scheam: we assume that a statement $p$ is wrong, or $\neg p$ is correct, and then we derived a contradiction. This is justified by the tautology $(\neg p \to \mathbf{F}_0) \to p$. This can be written as $$\begin{array}{l} \neg p \to \mathbf{F}_0 \\ \hline \therefore \quad p \end{array}$$

  Here $\neg p \to \mathbf{F}_0$ is a *premise*, and $p$ is a *conclusion*. The sign "$\therefore$" means *therefore*, and the formula above reads "$\neg p \to \mathbf{F}_0$ is true, therefore, $p$ true."

There are several standard rules of inference:

(1) $$\begin{array}{ll} & p \\ & p \to q \\ \hline \therefore & p \end{array}$$ Modus Ponens or Rule of Detachment

(2) $$\begin{array}{ll} & p \to q \\ & q \to r \\ \hline \therefore & r \end{array}$$ Law of Syllogism

(2) $$\begin{array}{ll} & p \to q \\ & \neg q \\ \hline \therefore & \neg p \end{array}$$ Modus Tollens

(3) $$\begin{array}{ll} & p \\ & q \\ \hline \therefore & p \wedge q \end{array}$$ Rule of Conjunction

(4) $$\begin{array}{ll} & p \vee q \\ & \neg q \\ \hline \therefore & p \end{array}$$ Rule of Disjunctive Syllogism

(5) $$\begin{array}{ll} & \neg p \to \mathbf{F}_0 \\ \hline \therefore & p \end{array}$$ Rule of Contradiction

(6) $$\begin{array}{ll} & p \wedge q \\ \hline \therefore & p \end{array}$$ Rule of Disjunctive Amplification

(7) $$\begin{array}{ll} & p \\ \hline \therefore & p \vee q \end{array}$$ Rule of Conjunctive Simplification

(8) $$\begin{array}{ll} & p \wedge q \\ & p \to (q \to r) \\ \hline \therefore & r \end{array}$$ Rule of Conditional Proof

(9) $$\begin{array}{ll} & p \to r \\ & q \to r \\ \hline \therefore & (p \vee q) \to r \end{array}$$ Rule of Proof by Cases

(10) $$\begin{array}{ll} & p \to q \\ & r \to s \\ & p \vee r \\ \hline \therefore & q \vee s \end{array}$$ Constructive Dilemma

(11) $$\begin{array}{ll} & p \to q \\ & r \to s \\ & \neg q \vee \neg r \\ \hline \therefore & \neg p \vee \neg r \end{array}$$ Destructive Dilemma