

# Fundamentals of Computing

Leonid A. Levin (<https://www.cs.bu.edu/fac/1nd/>)

## Abstract

These are notes for the course CS-172 I first taught in the Fall 1986 at UC Berkeley and subsequently at Boston University. The goal was to introduce students to basic concepts of Theory of Computation and to provoke their interest in further study. Model-dependent effects were systematically ignored. Concrete computational problems were considered only as illustrations of general principles.

The notes are skeletal: they do have (terse) proofs, but exercises, references, intuitive comments, examples are missing or inadequate. The notes can be used for designing a course or by students who want to refresh the known material or are bright and have access to an instructor for questions.

Each subsection takes about a week of the course. Versions of these notes appeared in [Levin 91].

**Acknowledgments.** I am grateful to the University of California at Berkeley, its MacKey Professorship fund and Manuel Blum who made possible for me to teach this course. The opportunity to attend lectures of M. Blum and Richard Karp and many ideas of my colleagues at BU and MIT were very beneficial for my lectures. I am also grateful to the California Institute of Technology for a semester with light teaching load in a stimulating environment enabling me to rewrite the students' notes. NSF grants #DCR-8304498, DCR-8607492, CCR-9015276 also supported the work. And most of all I am grateful to the students [see 6.3] who not only have originally written these notes, but also influenced the lectures a lot by providing very intelligent reactions and criticism.

## Contents

<b>I</b>	<b>Basics</b>	<b>2</b>
<b>1</b>	<b>Deterministic Models; Polynomial Time &amp; Church's Thesis</b>	<b>2</b>
1.1	Rigid Models . . . . .	3
1.2	Pointer Machines . . . . .	4
1.3	Simulation . . . . .	5
<b>2</b>	<b>Universal Algorithm; Diagonal Results</b>	<b>6</b>
2.1	Universal Turing Machine . . . . .	6
2.2	Uncomputability; Goedel Theorem . . . . .	7
2.3	Intractability; Compression and Speed-up Theorems . . . . .	8
<b>3</b>	<b>Games; Alternation; Exhaustive Search; Time vs. Space</b>	<b>9</b>
3.1	How to Win . . . . .	9
3.2	Exponentially Hard Games . . . . .	10
3.3	Reductions; Non-Deterministic and Alternating TM; Time and Space . . . . .	11
<b>II</b>	<b>Mysteries</b>	<b>12</b>
<b>4</b>	<b>Nondeterminism; Inverting Functions; Reductions</b>	<b>12</b>
4.1	An Example of a Narrow Computation: Inverting a Function . . . . .	12
4.2	Complexity of NP Problems . . . . .	13
4.3	An NP-Complete Problem: Tiling . . . . .	14
<b>5</b>	<b>Probability in Computing</b>	<b>15</b>
5.1	A Monte-Carlo Primality Tester . . . . .	15
5.2	Randomized Algorithms and Random Inputs . . . . .	16
5.3	Arithmetization: One-Player Games with Randomized Transition . . . . .	17
<b>6</b>	<b>Randomness</b>	<b>18</b>
6.1	Randomness and Complexity . . . . .	18
6.2	Pseudo-randomness . . . . .	19
6.3	Cryptography . . . . .	20
	<b>References</b>	<b>21</b>