

Bibliographical Remarks

The literature relevant to the topics treated in this book is vast and it would be an immense task to give a survey of it. Therefore here I only list sources that I used more extensively, the articles explicitly mentioned in the text and a few books that I either consider classical or find useful as further reading. In most cases I refer to the original publications, but the interested reader may find many old papers reprinted (and translated to English) in anthologies. The literature is commented in the main text and the notes after sections, so the purpose of the notes below is only to provide some additional information and suggest further reading.

Chapter 1

The approach to the foundations of mathematics based on mathematical structures is explained in the first volume of the Bourbaki series of monographs [32]. The standard reference for Ramsey theory is [107]. Cantor's most important paper about set theory is [36]. Paradoxes are treated at length in Fraenkel, Bar-Hillel and Levy [75], which is a classic in the literature about the foundations of set theory. Bertrand Russell wrote about the discovery of his paradox in [253]; Zermelo's discovery of this paradox is described in his biography written by Ebbinghaus [65].

To mention a few more classics in the foundations of mathematics, the two volumes of Hilbert and Bernays [128, 129] present Hilbert's proof-theoretical approach to the foundations, Beth [24] treats the foundations from a historical and philosophical standpoint, Kleene [154] focuses on computability and Feferman's book [72] is a more recent presentation of foundations from the position of a predicativist.

Chapter 2

There are many books devoted to formal language theory. The concept of a context-free grammar can be found in most textbooks about theoretical computer science.

Essentially the same concerns other concepts treated in this chapter: proofs, models and computations. Thus I only mention a few that are among the most popular ones. Shoenfield [267] and Manin [190] are general introductions to logic and set theory. Grzegorzczuk [110] is a readable introduction to logic. For further reading about proof theory, I recommend Takeuti [288], and the book by Troelstra and Schwichtenberg [291].

The history of first-order logic is treated in Moore's article [199]. The main part of Gödel's paper [96] is a proof of the First Incompleteness Theorem. The last section contains a sketch of a proof of the Second Incompleteness Theorem. Gödel intended to publish another paper on the subject with a detailed proof (with number II). That paper has not been written, probably because the sketch of the proof in the published paper turned out to be sufficiently clear. Three Brouwer's papers about intuitionism are reprinted in the anthology [118], which also contains other classical papers in the foundations of mathematics. The Church-Turing Thesis appeared for the first time as *Thesis I*. in Kleene's book [154, page 300]. A classical monograph on the λ -calculus is Barendregt [13]. For a brief presentation of Church's type theory, see Andrews [4]. Many mathematicians discovered parts of the Curry-Howard Isomorphism and often these ideas were published much later (see the history of the λ -calculus, including the Curry-Howard Isomorphism, described in [130]). The key publications are Curry and Feys [55] and Howard [133].

Chapter 3

The standard reference for set theory is Jech [138]. Kanamori [148] is a survey of the history of set theory. Part II of Boolos's book [30] contains 13 essays about Frege's work and some proposals how to fix his system in order to be consistent. For a brief presentation of Type Theory, see Coquand [52]. I am grateful to Ilan Vardi for drawing my attention to his paper *Archimedes, The Sand Reckoner* [296]. The theory of large cardinals is treated in Kanamori [147]. For a survey on large cardinals and algebra, see Dehornoy [62].

Chapter 4

My presentation of the Galois theory is inspired by the readable introduction to this theory by Stewart [285]. The sketch of the unsolvability of a concrete quintic equation is based on Stewart's elementary approach. An excellent exposition of Matyasevich's Theorem and related results in logical investigations of arithmetic is Smoryński [276]. In Table 4.1 the number $3 \cdot 2^{402653211} - 2$ is from [152]; I have just computed the sequence a few steps back to obtain some more values. The collection of articles about the Collatz problem, edited by Lagarias [177], is a useful overview of this area. It contains an article by Collatz describing the history of the problem; Conway's article [47] is reprinted there too. Kunen [173] is an outstanding introduction to the independence proofs in set theory.

Chapter 5

Two monographs on computational complexity have appeared recently: Arora and Barak [8] and Goldreich [101]. There are a number of books that cover special topics in computational complexity such as circuit complexity, algebraic complexity, randomized computations and cryptography, but somebody with little background in complexity theory should rather start with general introductions such as the two above. Some of the standard reference monographs are Bürgisser, Clausen, and Shokrollahi [31] in algebraic complexity, Goldreich [102, 103] in cryptography, Nielsen and Chuang [205] in quantum computing, and Li and Vitanyi [185] in Kolmogorov complexity.

Chapter 6

I have already mentioned some books about proof theory in the notes for Chap. 2. The standard reference for ordinal analysis is Pohlers's monograph [219] and I also recommend a more readable survey of Rathjen [237]. The first book about Bounded Arithmetic was Buss [34]. Krajíček's monograph [161] covers all main subjects in proof complexity. A more recent monograph of Cook and Nguyen [50] focuses on theories associated with complexity classes.

Conjecture 2 of Sect. 6.3 first appeared in print in [223]; Conjectures 1 and 4 and Conjectures 3 and 5 appeared in [227] and [164] respectively.

Chapter 7

The 26 chapters of *The Oxford Handbook of Philosophy of Mathematics and Logic* [265], edited by Shapiro, cover all main positions in the philosophy of mathematics and several other topics. An on-line source that I find very useful is *The Stanford Encyclopedia of Philosophy* [316], which contains many articles about the philosophy of mathematics and history of logic. For a survey on reflection principles, see Smoryński [273]. Readable surveys about the axioms providing invariance with respect to forcing and other results on the Continuum Hypothesis are Woodin [310, 311] and Dehornoy [61].

References

1. Ajtai, M.: Σ_1^1 formulae on finite structures. *Ann. Pure Appl. Log.* **24**, 1–48 (1983)
2. Agrawal, M., Kayal, N., Saxena, N.: PRIMES is in P. *Ann. Math.* **160**(2), 781–793 (2004)
3. Alekhnovich, M.: Mutilated chessboard problem is exponentially hard for resolution. *Theor. Comput. Sci.* **310**(1–3), 513–525 (2004)
4. Andrews, P.: Church’s type theory. In: Zalta, E.N. (ed.) *Stanford Encyclopedia of Philosophy*, Spring 2009 edn. (2009). <http://plato.stanford.edu/archives/spr2009/entries/type-theory-church>
5. Appel, K., Haken, W.: Every planar map is four colorable. Part I. Discharging. *Ill. J. Math.* **21**, 429–490 (1977)
6. Appel, K., Haken, W., Koch, J.: Every planar map is four colorable. Part II. Reducibility. *Ill. J. Math.* **21**, 491–567 (1977)
7. Arora, S., Lund, C., Motwani, R., Sudan, M., Szegedy, M.: Proof verification and the hardness of approximation problems. *J. ACM* **45**(3), 501–555 (1998)
8. Arora, S., Barak, B.: *Computational Complexity: A Modern Approach*. Cambridge University Press, Cambridge (2009)
9. Arora, S., Safra, S.: Probabilistic checking of proofs: A new characterization of NP. *J. ACM* **45**(1), 70–122 (1998)
10. Avigad, J., Sommer, R.: A model-theoretical approach to ordinal analysis. *Bull. Symb. Log.* **3**, 17–59 (1997)
11. Babai, L.: Trading group theory for randomness. In: *Proc. 17th ACM Symp. on Theory of Computing*, pp. 421–429 (1985)
12. Banach, S., Tarski, A.: Sur la décomposition des ensembles de points en parties respectivement congruentes. *Fundam. Math.* **6**, 244–277 (1924)
13. Barendregt, H.P.: *The Lambda Calculus: Its Syntax and Semantics*. North-Holland, Amsterdam (1984)
14. Barwise, J.: *Admissible Sets and Structures: An Approach to Definability Theory*. Springer, Berlin (1975)
15. Bernstein, A., Robinson, A.: Solution of an invariant subspace problem of K.T. Smith and P.R. Halmos. *Pac. J. Math.* **16**(3), 421–431 (1966)
16. Bachmann, H.: Die Normalfunktionen und das Problem der ausgezeichneten Folgen von Ordnungszahlen. *Vierteljschr. Naturforsch. Ges. Zürich* **95**, 115–147 (1950)
17. Baker, T.P., Gill, J., Solovay, R.: Relativizations of the $P = ? NP$ question. *SIAM J. Comput.* **4**(4), 431–442 (1975)
18. Beklemishev, L.D.: A proof-theoretic analysis of collection. *Arch. Math. Log.* **34**(4–5), 216–238 (1998)
19. Bennett, C.H.: Logical reversibility of computation. *IBM J. Res. Dev.* **17**(6), 525–532 (1973)

20. Bennett, C.H., Wiesner, S.J.: Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* **69**, 2881–2884 (1992)
21. Berger, R.: The undecidability of the domino problem. *Mem. Am. Math. Soc.* **66** (1966)
22. Bernays, P.: Sur le platonisme dans les mathématiques. *Enseign. Math.* **34**, 52–69 (1935)
23. Bernays, P.: A system of axiomatic set theory I. *J. Symb. Log.* **2**, 65–77 (1937)
24. Beth, E.W.: *The Foundations of Mathematics. A Study in the Philosophy of Science.* North-Holland, Amsterdam (1959)
25. Blum, L., Shub, M., Smale, S.: On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bull. Am. Math. Soc.* **21**, 1–46 (1989)
26. Blum, L., Cucker, F., Shub, M., Smale, S.: *Complexity and Real Computation.* Springer, Berlin (1997)
27. Blum, N.: A boolean function requiring $3n$ network size. *Theor. Comput. Sci.* **28**, 337–345 (1984)
28. Bolzano, B.: *Paradoxien des Unendlichen.* C.H. Reclam, Leipzig (1951)
29. Bonet, M.L., Pitassi, T., Raz, R.: On interpolation and automatization for Frege systems. *SIAM J. Comput.* **29**(6), 1939–1967 (2000)
30. Boolos, G.: *Logic, Logic, and Logic.* Harvard University Press, Cambridge (1998)
31. Bürgisser, P., Clausen, M., Shokrollahi, M.A.: *Algebraic Complexity Theory.* Springer, Berlin (1997)
32. Bourbaki, N.: *Theory of Sets. Elements of Mathematics, vol. 1.* Addison-Wesley, Reading (1974)
33. Bourgain, J.: On the Fourier-Walsh spectrum of the Moebius function (2011). <http://arxiv.org/pdf/1112.1423.pdf>, [arXiv:1112.1423](https://arxiv.org/abs/1112.1423)
34. Buss, S.R.: *Bounded Arithmetic.* Bibliopolis, Naples (1986)
35. Buss, S.R., Krajčček, J.: An application of boolean complexity to separation problems in bounded arithmetic. *Proc. Lond. Math. Soc.* **69**(3), 1–21 (1994)
36. Cantor, G.: *Grundlagen einer allgemeinen Mannichfaltigkeitslehre. Ein mathematisch-philosophischer Versuch in der Lehre des Unendlichen.* Teubner, Leipzig (1882)
37. Cantor, G.: Über eine elementare Frage der Mannichfaltigkeitslehre. *Jahresbericht der Deutsch. Math. Vereinig.* **1**, 75–78 (1890/91)
38. Carnap, R.: *Logische Syntax der Sprache.* Springer, Berlin (1934)
39. Chaitin, G.J.: On the simplicity and speed of programs for computing infinite sets of natural numbers. *J. ACM* **16**(3), 407–422 (1969)
40. Cheng, Q.: Straight-line programs and torsion points on elliptic curves. *Comput. Complex.* **12**(1), 150–161 (2003)
41. Cheyne, C.: *Knowledge, Cause, and Abstract Objects: Causal Objections to Platonism.* Kluwer Academic, Dordrecht (2001)
42. Church, A.: A set of postulates for the foundation of logic (1). *Ann. Math.* **33**, 346–366 (1932)
43. Church, A.: An unsolvable problem of elementary number theory. *Am. J. Math.* **58**, 345–363 (1936)
44. Church, A.: A formulation of the simple theory of types. *J. Symb. Log.* **5**, 56–68 (1940)
45. Chvátal, V.: Edmonds polytopes and a hierarchy of combinatorial problems. *Discrete Math.* **4**, 305–337 (1973)
46. Cohen, P.: *Set Theory and the Continuum Hypothesis,* Benjamin, New York (1963)
47. Conway J.H.: Unpredictable iterations. In: *Proc. 1972 Number Th. Conf*, pp. 49–52. University Press of Colorado, Boulder (1972)
48. Cook, S.A.: The complexity of theorem proving procedures. In: *Proc. 3rd Annual ACM Symposium on Theory of Computing*, pp. 151–158 (1971)
49. Cook, S.A.: Feasibly constructive proofs and the propositional calculus. In: *Proc. Seventh Annual ACM Symposium on Theory of Computing*, pp. 83–97. ACM, New York (1975)
50. Cook, S., Nguyen, P.: *Logical Foundations of Proof Complexity.* ASL Perspectives in Logic. Cambridge University Press, Cambridge (2010)

51. Cook, S.A., Reckhow, R.A.: The relative efficiency of propositional proof systems. *J. Symb. Log.* **44**(1), 36–50 (1979)
52. Coquand, T.: Type theory. In: Zalta, E.N. (ed.) *Stanford Encyclopedia of Philosophy*, Spring 2010 edn. (2010). <http://plato.stanford.edu/archives/spr2010/entries/type-theory/>
53. Craig, W.: Three uses of the Herbrand-Gentzen theorem in relating model theory and proof theory. *J. Symb. Log.* **22**(3), 269–285 (1957)
54. Curry, H.B.: *Outlines of a Formalist Philosophy of Mathematics*. Studies in Logic and Foundations of Mathematics. North-Holland, Amsterdam (1951)
55. Curry, H.B., Feys, R.: *Combinatory Logic*. Vol. I. North-Holland, Amsterdam (1958)
56. Davis, M., Putnam, H.: A computing procedure for quantification theory. *J. ACM* **7**(3), 201–215 (1960)
57. Davis, M., Putnam, H., Robinson, J.: The decision problem for exponential Diophantine equations. *Ann. Math. (2)* **74**(3), 425–436 (1961)
58. Dawson, J.W. Jr.: The reception of Gödel’s incompleteness theorems. In: Drucker, T. (ed.) *Perspectives on the History of Mathematical Logic*, pp. 84–100. Birkhäuser, Boston (1991)
59. Dedekind, R.: Was sind und was sollen die Zahlen? 1. Auflage. Vieweg, Braunschweig (1888)
60. Dehornoy, P.: Braid groups and left distributive operations. *Trans. Am. Math. Soc.* **345**(1), 115–150 (1994)
61. Dehornoy, P.: Recent progress about the Continuum Hypothesis (after Woodin). Séminaire Bourbaki, exposé 915, mars 2003 (2003)
62. Dehornoy, P.: Elementary embeddings and algebra. In: Foreman, M., Kanamori, A. (eds.) *Handbook of Set Theory*. Springer, Berlin (2010)
63. Detlefsen, M.: Formalism. In: Shapiro, S. (ed.) *The Oxford Handbook of Philosophy of Mathematics and Logic*, pp. 236–317. Oxford University Press, London (2005)
64. Dummett, M.: Realism. In: *Truth and Other Enigmas*, pp. 145–165. Harvard University Press, Cambridge (1978)
65. Ebbinghaus, H.-D., Peckhaus, V.: *Ernst Zermelo: An Approach to His Life and Work*. Springer, Berlin (2007)
66. Elitzur, A.C., Vaidman, L.: Quantum mechanical interaction-free measurements. *Found. Phys.* **23**, 987–997 (1993)
67. Erdős, P.: Some remarks on the theory of graphs. *Bull. Am. Math. Soc.* **53**, 292–294 (1947)
68. Erdős, P.: On a new method in elementary number theory which leads to an elementary proof of the prime number theorem. *Proc. Natl. Acad. Sci. USA* **35**, 374–384 (1949)
69. Erdős, P., Szekerés, G.: A combinatorial problem in geometry. *Compos. Math.* **2**, 463–470 (1935)
70. Feferman, S.: Transfinite recursive progressions of axiomatic theories. *J. Symb. Log.* **27**(3), 259–315 (1962)
71. Feferman, S.: Systems of predicative analysis. *J. Symb. Log.* **29**(1), 1–30 (1964)
72. Feferman, S.: *In the Light of Logic*. Oxford University Press, London (1998)
73. Feynman, R.: Simulating physics with computers. *Int. J. Theor. Phys.* **21**(6–7), 467 (1982)
74. Fraenkel, A.A.: Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre. *Math. Ann.* **86**, 230–237 (1922)
75. Fraenkel, A.A., Bar-Hillel, Y., Levy, A.: *Foundations of Set Theory*. North-Holland, Amsterdam (1973)
76. Franzén, T.: *Inexhaustibility: A Non-exhaustive Treatment*. Lecture Notes in Logic, vol. 16. Association for Symbolic Logic, AK Peters, Wellesley (2004)
77. Frege, G.: *Begriffsschrift: eine der arithmetischen nachgebildete Formelsprache des reinen Denkens*. Halle (1879)
78. Frege, G.: *Grundgesetze der Arithmetik I*. Hermann Pohle, Jena (1893)
79. Frege, G.: *Grundgesetze der Arithmetik II*. Hermann Pohle, Jena (1903)
80. Friedberg, R.M.: Two recursively enumerable sets of incomparable degrees of unsolvability. *Proc. Natl. Acad. Sci. USA* **43**, 236–238 (1957)

81. Friedman, H.: On the consistency, completeness and correctness. Unpublished typescript (1979)
82. Friedman, H.: Finite functions and the necessary use of large cardinals. *Ann. Math.* **148**, 803–893 (1998)
83. Furst, M.L., Saxe, J.B., Sipser, M.: Parity, circuits, and the polynomial-time hierarchy. *Math. Syst. Theory* **17**(1), 13–27 (1984)
84. Gaifman, H.: Ontology and conceptual framework part I. *Erkenntnis* **9**, 329–353 (1975)
85. Gaifman, H.: Ontology and conceptual framework part II. *Erkenntnis* **10**, 21–85 (1976)
86. Gaifman, H.: Ontology and realism in mathematics. *Rev. Symb. Log.* **5**(3), 480–512 (2012)
87. Gál, A., Hansen, K.A., Koucký, M., Pudlák, P., Viola, E.: Tight bounds on computing error-correcting codes by bounded-depth circuits with arbitrary gates. In: *Proc. STOC 2012*, pp. 479–494 (2012)
88. Galilei, G.: *Discorsi e dimostrazioni matematiche intorno a due nuove scienze attinenti la meccanica e i movimenti locali*. Elsevir, Leiden (1638)
89. Gentzen, G.: Untersuchungen über das logische Schließen I. *Math. Z.* **39**(2), 176–210 (1934)
90. Gentzen, G.: Untersuchungen über das logische Schließen II. *Math. Z.* **39**(3), 405–431 (1935)
91. Gentzen, G.: Die Widerspruchsfreiheit der reinen Zahlentheorie. *Math. Ann.* **112**, 493–565 (1936)
92. Gentzen, G.: Neue fassung des widerspruchsfreiheitsbeweises für die reine Zahlentheorie. *Forsch. Logik Grundlegung exakten Wiss.* **4**, 19–44 (1938)
93. Girard, J.-Y.: *Proof Theory and Logical Complexity*. Bibliopolis, Naples (1987)
94. Glaßer, C., Selman, A. A., Sengupta, S., Zhang, L.: Disjoint NP-pairs. *SIAM J. Comput.* **33**(6), 1369–1416 (2004)
95. Gödel, K.: Die Vollständigkeit der Axiome des logischen Funktionenkalküls. *Monatshefte Math. Phys.* **37**, 349–360 (1930)
96. Gödel, K.: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I. *Monatshefte Math. Phys.* **38**, 173–198 (1931)
97. Gödel, K.: The Consistency of the Axiom of Choice and of the Generalized Continuum Hypothesis with the Axioms of Set Theory. *Annals of Mathematical Studies*, vol. 3. Princeton University Press, Princeton (1940)
98. Gödel, K.: What is Cantor’s continuum problem? *Am. Math. Mon.* **54**(9), 515–525 (1947)
99. Gödel, K.: *Collected Works: Volume III. Unpublished Essays and Lectures*. Feferman, S., Dawson, J.W., Goldfarb, W., Parsons, C., Sieg, W. (eds.). Oxford University Press, London (1995)
100. Gödel, K. (ed.): *Collected Works: Volume V. Correspondence*, H.-Z. Feferman, S., Dawson, J.W., Goldfarb, W., Parsons, C., Sieg, W. (eds.). Oxford University Press, London (2003)
101. Goldreich, O.: *Computational Complexity, a Conceptual Perspective*. Cambridge University Press, London (2008)
102. Goldreich, O.: *The Foundations of Cryptography, Volume 1*. Cambridge University Press, London (2001)
103. Goldreich, O.: *The Foundations of Cryptography, Volume 2*. Cambridge University Press, London (2004)
104. Gomory, R.E.: Outline of an algorithm for integer solutions to linear programs. *Bull. Am. Math. Soc.* **64**, 275–278 (1958)
105. Goodstein, R.L.: On the restricted ordinal theorem. *J. Symb. Log.* **9**, 33–41 (1944)
106. Gonthier, G.: Formal proof—the four-color theorem. *Not. Am. Math. Soc.* **55**(11), 1382–1393 (2008)
107. Graham, R.L., Rothschild, B.L., Spencer, J.H.: *Ramsey Theory*. Wiley, New York (1990)
108. Green, B.: On (not) computing the Möbius functions using bounded depth circuits. *Comb. Probab. Comput.* **21**(6), 942–951 (2012)
109. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: *Proc. 28th Annual ACM Symposium on the Theory of Computing*, pp. 212–218 (1996)

110. Grzegorzcyk, A.: *An Outline of Mathematical Logic: Fundamental Results and Notions Explained with all Details*. Reidel, Dordrecht (1974)
111. Hájek, P., Pudlák, P.: *Metamathematics of First Order Arithmetic*. ASL Perspectives in Logic. Springer, Berlin (1993)
112. Hales, T.C.: A proof of the Kepler conjecture. *Ann. Math. (2)* **162**(3), 1065–1185 (2005)
113. Harrow, A.W., Hassidim, A., Lloyd, S.: Quantum algorithm for linear systems of equations. *Phys. Rev. Lett.* **103**, 150502 (2009)
114. Hartmanis, J., Stearns, R.E.: On the computational complexity of algorithms. *Trans. Am. Math. Soc.* **117**, 285–306 (1965)
115. Håstad, J.: Almost optimal lower bounds for small depth circuits. In: Micali, S. (ed.) *Randomness and Computation*, Advances in Computing Research, vol. 5, pp. 143–170. JAI Press, London (1989)
116. Hawking, S.: Godel and the end of physics. A public lecture held in 2002. <http://www.hawking.org.uk/godel-and-the-end-of-physics.html>
117. Heath, T.L.: *The Thirteen Books of Euclid's Elements*. Cambridge University Press, Cambridge (1908)
118. van Heijenoort, J.: *A Source Book in Mathematical Logic, 1879–1931*. Harvard University Press, Cambridge (1976)
119. Henkin, L., Monk, J.D., Tarski, A.: *Cylindric Algebras I*. North-Holland, Amsterdam (1975)
120. Henkin, L., Monk, J.D., Tarski, A.: *Cylindric Algebras II*. North-Holland, Amsterdam (1985)
121. Herbrand, J.: *Recherches sur la theorie de la demonstration*. Travaux de la Societe des Sciences et des Lettres de Varsovie, Class III, Sciences Mathematiques et Physiques 33, 33–160 (1930)
122. Heyting, A.: *Intuitionism: An introduction*. Studies in Logic and the Foundations of Mathematics, vol. 16. North-Holland, Amsterdam (1971)
123. Hilbert, D.: Über die Endlichkeit des Invariantensystems für binären Grundformen. *Math. Ann.* **33**, 223–226 (1889)
124. Hilbert, D.: *Grundlagen der Geometrie*. Teubner, Berlin (1899)
125. Hilbert, D.: Mathematical problems. *Bull. Am. Math. Soc.* **8**, 437–479 (1902)
126. Hilbert, D.: On the infinite. In: van Heijenoort, J. (ed.) *From Frege to Gödel: A Source Book in Mathematical Logic, 1879–1931*, pp. 367–392. Harvard University Press, Cambridge (1967)
127. Hilbert, D.: *Die Grundlagen der Mathematik* (a lecture given in Hamburg in 1927). English translation “The foundations of mathematics”. In: van Heijenoort, J. (ed.) *From Frege to Gödel: A Source Book in Mathematical Logic, 1879–1931*, pp. 464–479. Harvard University Press, Cambridge (1967)
128. Hilbert, D., Bernays, P.: *Grundlagen der Mathematik. I. Die Grundlehren der mathematischen Wissenschaften*, vol. 40. Springer, Berlin (1934)
129. Hilbert, D., Bernays, P.: *Grundlagen der Mathematik. II. Die Grundlehren der mathematischen Wissenschaften*, vol. 50. Springer, Berlin (1939)
130. Hindley, J.R., Cardone, F.: History of λ -calculus and combinatory logic. In: Gabbay, D.M., Woods, J. (eds.) *Handbook of the History of Logic*. Elsevier, Amsterdam (2006)
131. Hirschfeld, J.: The nonstandard treatment of Hilbert's fifth problem. *Trans. Am. Math. Soc.* **321**(1), 379–400 (1990)
132. Hopcroft, J., Paul, W.J., Valiant, L.G.: On time vs. space. *J. ACM* **24**(2), 332–337 (1977)
133. Howard, W.A.: The formulae-as-types notion of construction. In: Seldin, J.P., Hindley, J.R. (eds.) *To H.B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, pp. 479–490. Academic Press, Boston (1980)
134. Hrubeš, P.: A lower bound for intuitionistic logic. *Ann. Pure Appl. Log.* **146**, 72–90 (2007)
135. Impagliazzo, R.: A personal view of average-case complexity. In: *10th Annual Structure in Complexity Theory Conference (SCT'95)*, pp. 134–147 (1995)
136. Impagliazzo, R., Wigderson, A.: $P = BPP$ unless E has subexponential circuits: Derandomizing the XOR lemma. In: *Proc. 29th STOC*, pp. 220–229 (1997)

137. Jech, T.: OTTER experiments in a system of combinatory logic. *J. Autom. Reason.* **14**(3), 413–426 (1995)
138. Jech, T.: *Set Theory, the Third Millennium Edition*. Springer, Berlin (2003)
139. Jensen, R.B.: On the consistency of a slight(?) modification of Quine's NF. *Synthese* **19**, 250–263 (1969)
140. Jeřábek, E.: The strength of sharply bounded induction. *Math. Log. Q.* **52**(6), 613–624 (2006)
141. Jockusch, C.G., Jr.: Ramsey's theorem and recursion theory. *J. Symb. Log.* **37**, 268–280 (1972)
142. Jockusch, C.G., Soare, R.I.: Π_1^0 classes and degrees of theories. *Trans. Am. Math. Soc.* **173**, 33–56 (1972)
143. Jones, J.P.: Universal Diophantine equation. *J. Symb. Log.* **47**, 549–571 (1982)
144. Johnson, D., Papadimitriou, C., Yannakakis, M.: How easy is local search? *J. Comput. Syst. Sci.* **37**, 79–100 (1988)
145. Kabanets, V., Impagliazzo, R.: Derandomizing polynomial identity tests means proving circuit lower bounds. *Comput. Complex.* **13**(1–2), 1–46 (2004)
146. Kahr, A.S., Moore, E.F., Wang, H.: Entscheidungsproblem reduced to the AEA case. *Proc. Natl. Acad. Sci. USA* **48**(3), 365–377 (1962)
147. Kanamori, A.: *The Higher Infinite, Large Cardinals in Set Theory from Their Beginnings*. Springer, Berlin (1994)
148. Kanamori, A.: The mathematical development of set theory from Cantor to Cohen. *Bull. Symb. Log.* **2**, 1–71 (1996)
149. Kanamori, A., McAloon, K.: On Gödel incompleteness and finite combinatorics. *Ann. Pure Appl. Log.* **33**(1), 23–41 (1987)
150. Katz, V.J.: *A History of Mathematics – an Introduction*. Harper Collins, New York (1993)
151. Ketonen, J., Solovay, R.: Rapidly growing Ramsey functions. *Ann. Math.* **113**, 267–314 (1981)
152. Kirby, L., Paris, J.: Accessible independence results for Peano arithmetic. *Bull. Lond. Math. Soc.* **14**, 285–293 (1982)
153. Kleene, S.C.: General recursive functions of natural numbers. *Math. Ann.* **112**, 727–742 (1936)
154. Kleene, S.C.: *Introduction to Metamathematics*. Van Nostrand, New York (1952)
155. Kleene, S.C.: Extension of an effectively generated class of functions by enumeration. *Colloq. Math.* **6**(1), 67–78 (1958)
156. Koblitz, N.: *A Course in Number Theory and Cryptography*. Springer, New York (1987)
157. Koellner, P., Woodin, W.H.: Incompatible Omega-complete theories. *J. Symb. Log.* **74**(4), 1155–1170 (2009)
158. Kohlenbach, U.: *Applied Proof Theory: Proof Interpretations and Their Use in Mathematics*. Springer, Berlin (2008)
159. Kollár, J., Rónyai, L., Szabó, T.: Norm-graphs and bipartite Turán numbers. *Combinatorica* **16**(3), 399–406 (1996)
160. Kolmogorov, A.: On tables of random numbers. *Sankhya, Ser. A* **25**, 369–375 (1963)
161. Krajíček, J.: *Bounded Arithmetic, Propositional Logic, and Complexity Theory*. *Encyclopedia of Mathematics and Its Applications*, vol. 60. Cambridge University Press, Cambridge (1995)
162. Krajíček, J.: Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *J. Symb. Log.* **62**(2), 457–486 (1997)
163. Krajíček, J.: *Forcing with Random Variables*. *London Math. Soc. Lecture Note Series*, vol. 382. Cambridge University Press, Cambridge (2011)
164. Krajíček, J., Pudlák, P.: Propositional proof systems, the consistency of first order theories and the complexity of computations. *J. Symb. Log.* **54**(3), 1063–1079 (1989)
165. Krajíček, J., Pudlák, P.: On the structure of initial segments of models of arithmetic. *Arch. Math. Log.* **28**, 91–98 (1989)

166. Krajíček, J., Pudlák, P.: Some consequences of cryptographical conjectures for S_2^1 and EF . In: Leivant, D. (ed.) *Logic and Computational Complexity*, (Proceedings of Meeting Held in Indianapolis 1994). LNCS, vol. 960, pp. 210–220. Springer, Berlin (1995)
167. Krajíček, J., Pudlák, P., Takeuti, G.: Bounded arithmetic and polynomial hierarchy. *Ann. Pure Appl. Log.* **52**, 143–154 (1991)
168. Kreisel, G.: Ordinal logics and the characterization of informal concepts of proof. In: *Proc. of the 8th International Congress of Mathematicians*, pp. 289–299. Edinburgh University Press, Edinburgh (1958). 1960
169. Kreisel, G., Levy, A.: Reflection principles and their use for establishing the complexity of axiomatic systems. *Z. Math. Log. Grundle. Math.* **14**, 97–142 (1968)
170. Kripke, S.A.: A completeness theorem in modal logic. *J. Symb. Log.* **24**(1), 1–14 (1959)
171. Kruskal, J.B.: Well-quasi-ordering, the tree theorem, and Vázsonyi's conjecture. *Trans. Am. Math. Soc.* **95**, 210–225 (1960)
172. Kunen, K.: *Combinatorics*. In: Barwise, J. (ed.) *Handbook of Mathematical Logic*. North-Holland, Amsterdam (1977)
173. Kunen, K.: *Set Theory: An Introduction to Independence Proofs*. North-Holland, Amsterdam (1980)
174. Kuperberg, G.: A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.* **35**(1), 170–188 (2005)
175. Laczko, M.: *Conjecture and Proof*. TypoTeX, Budapest (1998)
176. Ladner, R.E.: On the structure of polynomial time reducibility. *J. ACM* **22**, 155–171 (1975)
177. Lagarias, G. (ed.): *The Ultimate Challenge: The $3x + 1$ Problem*. Am. Math. Soc., Providence (2010)
178. Lakatos, I.: *Proofs and Refutations*. Cambridge University Press, Cambridge (1976)
179. Laver, R.: The left-distributive law and the freeness of an algebra of elementary embeddings. *Adv. Math.* **91**, 209–231 (1992)
180. Laver, R.: On the algebra of elementary embeddings of a rank into itself. *Adv. Math.* **110**, 334–346 (1995)
181. Lawvere, F.W.: An elementary theory of the category of sets. *Proc. Natl. Acad. Sci. USA* **52**, 1506–1511 (1964)
182. Levin, L.: Universal'nye perebornye zadachi. *Probl. Inf. Transm.* **9**(3), 265–266 (1973). (Russian)
183. Levy, A., Solovay, R.M.: Measurable cardinals and the continuum hypothesis. *Isr. J. Math.* **5**, 234–248 (1967)
184. Linnebo, Ø.: Platonism in the philosophy of mathematics. In: Zalta, E.N. (ed.) *Stanford Encyclopedia of Philosophy* (2011). <http://plato.stanford.edu/entries/platonism-mathematics/>
185. Li, M., Vitanyi, P.: *An Introduction to Kolmogorov Complexity and Its Applications*. Springer, Berlin (2008)
186. Löwenheim, L.: Über Möglichkeiten im Relativkalkül. *Math. Ann.* **76**(4), 447–470 (1915)
187. Luckhardt, H.: Herbrand-Analysen Zweier Beweise Des Satzes von Roth: Polynomiale Anzahlschranken. *J. Symb. Log.* **54**(1) (1989)
188. Luminet, J.-P., Weeks, J., Riazuelo, A., Lehoucq, R., Uzan, J.-P.: Dodecahedral space topology as an explanation for weak wide-angle temperature correlations in the cosmic microwave background. *Nature* **425**(9), 593–595 (2003)
189. Mac Lane, S., Moerdijk, I.: *Sheaves in Geometry and Logic: A First Introduction to Topos Theory*. Springer, New York (1992)
190. Manin, Yu.I.: *A Course in Mathematical Logic for Mathematicians*. Springer, New York (2010)
191. Margulis, G.A.: Explicit constructions of expanders. *Probl. Pereda. Inf.* **9**(4), 71–80 (1973)
192. Martin, D.A., Solovay, R.M.: Internal Cohen extensions. *Ann. Math. Log.* **2**(2), 143–178 (1970)
193. Matiyasevich Yu, V.: Enumerable sets are Diophantine. *Dokl. Akad. Nauk SSSR* **191**(2), 279–282 (1970). (In Russian; English translation: *Sov. Math. Dokl.* **11**(2), 354–358)

194. Matoušek, J.: A combinatorial proof of Kneser's conjecture. *Combinatorica* **2**(1), 163–170 (2004)
195. McCarthy, J.: A tough nut for proof procedures. Stanford Artificial Intelligence Project, Memo No. 16 (1964)
196. McCarthy, C.: What does it take to prove Fermat's Last Theorem? Grothendieck and the logic of number theory. *Bull. Symb. Log.* **16**(3), 359–377 (2010)
197. McCune, W.: Solution of the Robbins problem. *J. Autom. Reason.* **19**(3), 263–276 (1997)
198. Miller, G.L.: Riemann's hypothesis and tests for primality. *J. Comput. Syst. Sci.* **13**(3), 300–317 (1976)
199. Moore, G.H.: The emergence of first-order logic. In: Aspray, W., Kitcher, P. (eds.) *Minnesota Studies of the Philosophy of Science, XI: History and Philosophy of Modern Mathematics*, pp. 95–135. University of Minnesota Press, Minneapolis (1988)
200. Mostowski, A.: Sentences Undecidable in Formalized Arithmetic: An Exposition of the Theory of Kurt Gödel. *Studies in Logic*. North-Holland, Amsterdam (1952)
201. Mostowski, A.: A generalization of the incompleteness theorem. *Fundam. Math.* **49**, 205–232 (1961)
202. Muchnik, A.A.: On the unsolvability of the problem of reducibility in the theory of algorithms. *Dokl. Akad. Nauk SSSR* **108**, 194–197 (1956) (Russian)
203. Mulmuley, K., Sohoni, M.: Geometric complexity theory I: An approach to the P vs. NP and related problems. *SIAM J. Comput.* **31**(2), 496–526 (2001)
204. Mycielski, J., Steinhaus, H.: A mathematical axiom contradicting the axiom of choice. *Bull. Acad. Pol. Sci., Sér. Sci. Math. Astron. Phys.* **10**, 1–3 (1962)
205. Nielsen, M.A., Chunag, I.L.: *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, Cambridge (2010)
206. Némethi, I., Dávid, Gy.: Relativistic computers and the Turing barrier. *Appl. Math. Comput.* **178**, 118–142 (2006)
207. von Neumann, J.: Eine Axiomatisierung der Mengenlehre. *J. Reine Angew. Math.* **154**, 219–240 (1925)
208. Newton, I.: *Universal Arithmetick: Or, a Treatise of Arithmetical Composition and Resolution*. J. Senex, London (1720)
209. Nisan, N., Wigderson, A.: Hardness vs. randomness. *J. Comput. Syst. Sci.* **49**(2), 149–167 (1994)
210. Odlyzko, A.M., te Riele, H.J.J.: Disproof of the Mertens conjecture. *J. Reine Angew. Math.* **357**, 138–160 (1985)
211. Parikh, R.: Existence and feasibility in arithmetic. *J. Symb. Log.* **36**(3), 494–508 (1971)
212. Paris, J.B.: Some independence results for Peano arithmetic. *J. Symb. Log.* **43**(4), 725–731 (1978)
213. Paris, J.B.: A hierarchy of cuts in models of arithmetic. In: *Model Theory of Algebra and Arithmetic*, Karpacz, 1979. Springer Lecture Notes in Math., vol. 834, pp. 312–337 (1980)
214. Paris, J., Harrington, L.: A mathematical incompleteness in Peano arithmetic. In: Barwise, J. (ed.) *Handbook of Mathematical Logic*, pp. 1133–1142. North-Holland, Amsterdam (1977)
215. Paris, J., Wilkie, A.: Δ_0 sets and induction. In: *Proc. Jadswin Logic Conference (Poland)*, pp. 237–248. Leeds University Press, Leeds (1981)
216. Peano, G.: *Arithmetices Principia, Nova Methodo Exposita*. Fratres Bocca, Torino (1889)
217. Peano, G., Cassina, U.: *Formulario Matematico*. Fratres Bocca, Torino (1908)
218. Planck, M.: *Where Is Science Going?* Norton, New York (1932)
219. Pohlers, W.: *Proof Theory. The First Step to Impredicativity*. Springer, Berlin (1989)
220. Poincaré, H.: *The Foundations of Science*. The Science Press, New York (1908)
221. Post, E.: Finite combinatory processes—formulation 1. *J. Symb. Log.* **1**(3), 103–105 (1936)
222. Pudlák, P.: Cuts, consistency statements and interpretations. *J. Symb. Log.* **50**(2), 423–441 (1985)
223. Pudlák, P.: On the length of proofs of finitistic consistency statements in first order theories. In: *Logic Colloquium*, vol. 84, pp. 165–196. North-Holland, Amsterdam (1986)

224. Pudlák, P.: Improved bounds to the length of proofs of finitistic consistency statements. In: *Contemporary Mathematics*, vol. 65, pp. 309–331. Am. Math. Soc., Providence (1987)
225. Pudlák, P.: Lower bounds for resolution and cutting planes proofs and monotone computations. *J. Symb. Log.* **62**(3), 981–998 (1997)
226. Pudlák, P.: Complexity theory and genetics: The computational power of crossing over. *Inf. Comput.* **171**, 201–223 (2001)
227. Pudlák, P.: Gödel and computations. *SIGACT News* **37**(4), 13–21 (2006)
228. Pudlák, P.: Quantum deduction rules. *Ann. Pure Appl. Log.* **157**, 16–29 (2009)
229. Pudlák, P.: Randomness, pseudorandomness and models of arithmetic. [arXiv:1210.4692](https://arxiv.org/abs/1210.4692)
230. Pudlák, P., Rödl, V., Sgall, J.: Boolean circuits, tensor ranks and communication complexity. *SIAM J. Comput.* **26**(3), 605–633 (1997)
231. Quine, W.V.: New foundations for mathematical logic. *Am. Math. Mon.* **44**, 70–80 (1937)
232. Quine, W.V.: *From a Logical Point of View: Nine Logico-Philosophical Essays*, 2nd edn. Harvard University Press, Cambridge (2003)
233. Quine, W.V.: *Mathematical Logic*. Norton, New York (1940)
234. Rabin, M.O.: Digital signatures and public-key functions as intractable as factorization. MIT Laboratory of Computer Science Technical Report 212, (1979).
235. Ramsey, F.P.: On a problem of formal logic. *Proc. Lond. Math. Soc.* **30**(1), 264–286 (1930)
236. Rathjen, M.: The higher infinite in proof theory. In: Makowsky, J., Ravve, E. (eds.) *Logic Colloquium '95*. Springer Lecture Notes in Logic, vol. 11, pp. 275–304 (1998)
237. Rathjen, M.: The realm of ordinal analysis. In: Cooper, S.B., Truss, J.K. (eds.) *Sets and Proofs*, pp. 219–279. Cambridge University Press, Cambridge (1999)
238. Razborov, A.: Lower bounds for the monotone complexity of some boolean functions. *Dokl. Akad. Nauk SSSR* **281**(4), 798–801 (1985). (In Russian; English translation in: *Sov. Math. Dokl.* **31**, 354–357 (1985))
239. Razborov, A.: Lower bounds on the size of bounded-depth networks over a complete basis with logical addition. *Mat. Zametki* **41**(4), 598–607 (1987). (In Russian; English translation in: *Math. Notes Acad. Sci. USSR* **41**(4), 333–338 (1987))
240. Razborov, A.: On the method of approximation. In: *Proc. of the 21st ACM STOC*, pp. 169–176 (1989)
241. Razborov, A.: Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic. *Izv. Math.* **59**(1), 201–224 (1995)
242. Razborov, A.: Bounded arithmetic and lower bounds in Boolean complexity. In: Clote, P., Remmel, J. (eds.) *Feasible Mathematics II*, pp. 344–386. Birkhauser, Basel (1995)
243. Razborov, A., Rudich, S.: Natural proofs. *J. Comput. Syst. Sci.* **55**(1), 24–35 (1997)
244. Reisch, S.: Hex ist PSPACE-vollständig (Hex is PSPACE-complete). *Acta Inform.* **15**, 167–191 (1981)
245. Rissanen, J.: Modeling by the shortest data description. *Automatica* **14**, 465–471 (1978)
246. Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**(2), 120–126 (1978)
247. Robinson, A.: *Non-standard Analysis*. North-Holland, Amsterdam (1966)
248. Robinson, J.A.: A machine-oriented logic based on the resolution principle. *J. ACM* **12**(1), 23–41 (1965)
249. Rosser, J.B.: Extensions of some theorems of Gödel and Church. *J. Symb. Log.* **1**, 87–91 (1936)
250. Rosser, J.B.: *Logic for Mathematicians*. McGraw-Hill, New York (1953)
251. Russell, B.: *The Principles of Mathematics*. Cambridge University Press, Cambridge (1903)
252. Russell, B.: Mathematical logic as based on the theory of types. *Am. J. Math.* **30**, 222–262 (1908)
253. Russell, B.: *My Philosophical Development*. Allen & Unwin, London (1959)
254. Russell, B.: *The Autobiography of Bertrand Russell*, vol. 1. Allen & Unwin, London (1967)
255. Savitch, W.J., Stimson, M.J.: Time bounded random access machines with parallel processing. *J. ACM* **26**(1), 103–118 (1979)

256. Schmerl, U.R.: A fine structure generated by reflection formulas over primitive recursive arithmetic. In: Boffa, M., van Dalen, D., McAloon, K. (eds.) *Proc. Logic Colloquium'78*, pp. 335–350. North-Holland, Amsterdam (1979)
257. Schönhage, A., Strassen V, V.: Schnelle multiplikation grosser Zahlen. *Computing* **7**, 281–292 (1971)
258. Schütte, K.: *Bewiestheorie*. Springer, Berlin (1960)
259. Schwartz, J.: Fast probabilistic algorithms for verification of polynomial identities. *J. ACM* **27**, 701–717 (1980)
260. Scott, D.: Measurable cardinals and constructible sets. *Bull. Acad. Pol. Sci.* **9**, 521–524 (1961)
261. Scott, D.: *Continuous Lattices*. Oxford Univ. Computing Lab. Technical Monograph PRG-7 (1971)
262. Scott, D., Solovay, R.: *Boolean-Valued Models for Set Theory*. Proc. AMS Summer Institute on Set Theory, Los Angeles. University of California, Berkeley (1967)
263. Selberg, A.: An elementary proof of the prime-number theorem. *Ann. Math. (2)* **50**, 305–313 (1949)
264. Shannon, C.E.: The synthesis of two-terminal switching circuits. *Bell Syst. Tech. J.* **28**, 59–98 (1949)
265. Shapiro, S. (ed.): *The Oxford Handbook of Philosophy of Mathematics and Logic*. Oxford University Press, London (2005)
266. Shelah, S.: Can you take Solovay's inaccessible away? *Isr. J. Math.* **48**(1), 1–47 (1984)
267. Shoenfield, J.R.: *Mathematical Logic*. Addison-Wesley, Reading (1967)
268. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**(5), 1484–1509 (1997)
269. Simpson, S.G.: Nonprovability of certain combinatorial properties of finite trees. In: Harrington, L.A., et al. (eds.) *Harvey's Friedman Research on the Foundations of Mathematics*, pp. 87–117. North-Holland, Amsterdam (1985)
270. Skolem, T.: Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit oder Beweisbarkeit mathematischer Sätze nebst einem Theoreme über dichte Mengen. *Videnskapsselskapet Skrifter, I. Mat.-Naturvidensk. Kl.* **6**, 1–36 (1920)
271. Skolem, T.: Einige Bemerkungen zur axiomatischen Begründung der Mengenlehre. In: *Fünften Kongress der Skandinavischen Mathematiker in Helsingfors 1922*. Helsingfors, pp. 217–232 (1923)
272. Smith, R.L.: The consistency strengths of some finite forms of the Higman and Kruskal theorems. In: Harrington, L.A., et al. (eds.) *Harvey's Friedman Research on the Foundations of Mathematics*, pp. 119–136. North-Holland, Amsterdam (1985)
273. Smoryński, C.: The incompleteness theorems. In: Barwise, J. (ed.) *Handbook of Mathematical Logic*, pp. 821–865. North-Holland, Amsterdam (1977)
274. Smoryński, C.: The varieties of arboreal experience. *Math. Intell.* **4**, 182–188 (1982)
275. Smoryński, C.: Nonstandard models and related developments. In: Harrington, L.A., et al. (eds.) *Harvey's Friedman Research on the Foundations of Mathematics*, pp. 179–229. North-Holland, Amsterdam (1985)
276. Smoryński, C.: *Logical Number Theory I, an Introduction*. Springer, Berlin (1991)
277. Solomonoff, R.: *A Preliminary Report on a General Theory of Inductive Inference*. Report V-131, Cambridge, Ma., Zator Co. (1960)
278. Solovay, R.M.: A model of set-theory in which every set of reals is Lebesgue measurable. *Ann. Math.* **92**(1), 1–56 (1970)
279. Solovay, R.M.: Real valued measurable cardinals. In: Scott, D.S. (ed.) *Axiomatic Set Theory*. Proc. Sym. in Pure Math. XIII, vol. 1, pp. 387–428 (1971)
280. Solovay, R.M.: Provability interpretations of modal logic. *Isr. J. Math.* **25**, 287–304 (1976)
281. Solovay, R.: Injecting inconsistencies into models of PA. *Ann. Pure Appl. Log.* **44**(1–2), 101–132 (1989)
282. Solovay, R.M., Strassen, V.: A fast Monte-Carlo test for primality. *SIAM J. Comput.* **6**(1), 84–85 (1977)

283. Specker, E.P.: Dualität. *Dialectica* **12**, 451–465 (1958)
284. Statman, R.: Proof-search and speed-up in the predicate calculus. *Ann. Math. Log.* **15**, 225–287 (1978)
285. Stewart, I.: *Galois Theory*. Chapman and Hall, New York (1998)
286. Strassen, V.: Gaussian elimination is not optimal. *Numer. Math.* **13**, 354–356 (1969)
287. Struik, D.J.: *A Concise History of Mathematics*. Dover, New York (1948)
288. Takeuti, G.: *Proof Theory*, 2nd. edn. North-Holland, Amsterdam (1987)
289. Tao, T.: Every odd number greater than 1 is the sum of at most five primes. *Math. Comput.* (to appear)
290. Tarski, A.: Der Wahrheitsbegriff in den formalisierten Sprachen. *Stud. Philos.* **1**, 261–405 (1936)
291. Troelstra, A., Schwichtenberg, H.: *Basic Proof Theory*, 2nd edn. Cambridge University Press, Cambridge (2000)
292. Tsfasman, M.A., Vlăduț, S.G., Zink T, T.: Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.* **104**, 13–28 (1982)
293. Turing, A.M.: On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc. (2)* **42**, 230–265 2(1937)
294. Turing, A.M.: Systems of logic based on ordinals. *Proc. Lond. Math. Soc.* **s2-45**(1), 161–228 (1939)
295. Uhlig, D.: On the synthesis of self-correcting schemes from functional elements with a small number of reliable elements. *Mat. Zametki* **15**(6), 937–944 (1974)
296. Vardi, I.: Archimedes, the Sand Reckoner. http://www.lix.polytechnique.fr/Labo/Ilan.Vardi/sand_reckoner.ps
297. Valiant, L.: The complexity of computing permanent. *Theor. Comput. Sci.* **8**, 189–201 (1979)
298. Vaught, R.L.: Axiomatizability by a schema. *J. Symb. Log.* **32**(4), 473–479 (1967)
299. Vinogradov, I.M.: Representation of an odd number as a sum of three primes. *C. R. Acad. Sci. USSR* **15**, 191–249 (1937)
300. Vopěnka, P.: On ∇ -model of set theory. *Bull. Acad. Pol. Sci., Sér. Sci. Math. Astron. Phys.* **13**, 267–272 (1965)
301. Vopěnka, P.: *Mathematics in the Alternative Set Theory*. Teubner, Leipzig (1979)
302. Wang, H.: The formalization of mathematics. *J. Symb. Log.* **19**, 241–266 (1954)
303. Wang, H.: Toward mechanical mathematics. *IBM J. Res. Dev.* **4**(1), 2–22 (1960)
304. Wang, H.: Proving theorems by pattern recognition–II. *Bell Syst. Tech. J.* **40**(1), 1–41 (1961)
305. Wang, H.: *A Survey of Mathematical Logic*. Science Press, Peking (1962)
306. Wang, H.: Some facts about Kurt Gödel. *J. Symb. Log.* **46**(3), 653–659 (1981)
307. Weyl, H.: *Das Kontinuum. Kritische Untersuchungen über die Grundlagen der Analysis*. Veit, Leipzig (1918)
308. Weyl, H.: Mathematics and logic. A brief survey serving as a preface to a review of “The philosophy of Bertrand Russell”. *Am. Math. Mon.* **53**, 2–13 (1946)
309. Woodin, W.H.: *The Axiom of Determinacy, Forcing Axioms, and the Nonstationary Ideal*. de Gruyter, Berlin (1999)
310. Woodin, W.H.: The continuum hypothesis, I. *Not. Am. Math. Soc.* **48**(6), 567–576 (2001)
311. Woodin, W.H.: The continuum hypothesis, II. *Not. Am. Math. Soc.* **48**(7), 681–690 (2001)
312. Woodin, W.H.: *The Continuum Hypothesis and the Ω -Conjecture*. Coxeter Lectures, Fields Institute, Toronto (2002)
313. Whitehead, A.N., Russell, B.: *Principia Mathematica, I*. Cambridge University Press, Cambridge (1910)
314. Whitehead, A.N., Russell, B.: *Principia Mathematica, II*. Cambridge University Press, Cambridge (1912)
315. Whitehead, A.N., Russell, B.: *Principia Mathematica, III*. Cambridge University Press, Cambridge (1913)
316. Zalta, E.N., Principal (eds.): *The Stanford Encyclopedia of Philosophy*. The Metaphysics Research Lab Center for the Study of Language and Information, Stanford University, Stanford. <http://plato.stanford.edu/>

317. Zermelo, E.: Beweis, dass jede Menge wohlgeordnet werden kann. *Math. Ann.* **59**(4), 514–516 (1904)
318. Zermelo, E.: Untersuchungen über die Grundlagen der Mengenlehre. I. *Math. Ann.* **65**, 261–281 (1908)
319. Zermelo, E.: Über Grenzzahlen und Mengenbereiche. *Fundam. Math.* **16**, 29–47 (1930)
320. Zippel, R.E.: Probabilistic algorithms for sparse polynomials. In: *Proc. EUROSAM'79*. Springer Lecture Notes in Computer Science, vol. 72, pp. 216–226 (1979)

Name Index

A

Abel, N.H., 263
Adleman, L., 430, 437
Al-Khwarizmi, 124
Alekhovich, M., 61
Appel, K., 13
Archimedes, 187
Aristarchus, 187
Aristotle, 44, 93, 177
Avigad, J., 120

B

Babai, L., 416
Bachmann, H., 209
Baker, T., 386
Banach, S., 218
Baranyi, I., 522
Beltrami, E., 86
Bennett, C.H., 462, 471
Berger, R., 303
Bernays, P., 101, 166, 586
Bernstein, A.R., 247
Blum, L., 408
Bolyai, J., 85
Bolzano, B., 39, 177
Boole, G., 111
Bourbaki, N., 2
Bourgain, J., 663
Brouwer, L.E.J., 108, 591
de Bruijn, N.G., 119
Buss, S.R., 523, 532, 539,
653

C

Cantor, G., 25, 157, 258
Cauchy, A.-L., 33
Chaitin, G.J., 480, 487

Church, A., 132, 146, 596
Chvátal, V., 558
Cohen, P.J., 183, 341
Collatz, L., 325
Conway, J., 327
Cook, S.A., 375, 523, 540, 552
Coquand, T., 120
Craig, W., 559
Curry, H.B., 146, 600

D

Davis, M., 119, 305
Dedekind, R., 30
Descartes, R., 11
Dummett, M., 589

E

Egan, G., 657
Erdős, P., 15, 61, 392
Euclid, 44, 178, 585
Euler, L., 62
Everet, H., 477

F

Feferman, S., 299, 620, 644
Fejes Tóth, L., 15
Ferguson, S.P., 15
de Fermat, P., 57
Feynman, R., 449
Fraenkel, A.A., 47
Franco, A.C., 299
Frege, G., 31, 93, 157, 586, 596
Freudenthal, H., 80
Friedberg, R.M., 311
Friedman, H., 299, 331, 339, 499,
565

G

Gaifman, H., 589
 Galileo Galilei, 176
 Galois, É., 9, 263
 Gauss, C.F., 85
 Gentzen, G., 118, 501
 Gill, J., 386
 Gilmore, P.C., 119
 Girard, J.-Y., 110
 Gödel, K., 99, 166, 183, 219, 276, 341, 342,
 375, 590, 591, 626, 630
 Gomory, R.E., 558
 Gonthier, G., 120
 Goodstein, R.L., 321
 Goppa, V.D., 407
 Gordan, P., 392
 Green, B., 663
 Grover, L.K., 450
 Guthrie, F., 13

H

Hadamard, J., 61
 Haken, W., 13
 Hales, T.C., 15
 Halmos, P.R., 237
 Harrington, L., 328
 Harrow, A.W., 471
 Hartmanis, J., 377
 Hassidim, A., 471
 Håstad, J., 540
 Hausdorff, F., 200
 Hawking, S., 659
 Herbrand, J., 500
 Hermite, C., 258
 Heyting, A., 592
 Hilbert, D., 25, 44, 104, 183, 304, 392,
 600–604
 Hirschfeld, J., 237
 Hogarth, M.L., 145
 Huet, G., 120

I

Impagliazzo, R., 426

J

Jaśkowski, S., 114
 Jensen, R., 242
 Jeřábek, E., 535
 Jockusch, C.G., 310
 Johnson, D.S., 532
 Jones, J.P., 305

K

Kahr, A.S., 312

Ketonen, J., 337
 Kirby, L., 323, 324
 Kleene, S.C., 133
 Klein, F., 90
 Knuth, D., 96
 Kohlenbach, U., 110
 Kolmogorov, A.N., 480
 Krajíček, J., 530, 559, 561
 Kreisel, G., 110, 617, 620
 Kripke, S.A., 121
 Kruskal, J., 330
 Kummer, E., 603
 Kuratowski, K., 14

L

Lakatos, I., 95
 Lambert, J.H., 258
 Laver, R., 205
 Lebesgue, H., 201
 Leibniz, G.W., 93, 111
 Levin, L., 375
 Levy, A., 617, 634
 von Lindemann, F., 258
 Liouville, J., 258, 266
 Lloid, S., 471
 Lobachevsky, N.I., 85
 Lovász, L., 522
 Löwenheim, L., 86
 Lucas, J., 621
 Luckhardt, H., 110, 501

M

Mahlo, P., 200
 Malament, D., 145
 Markov, A.A. Jr., 108
 Martin, D.A., 364
 Matiyasevich, Y., 305
 Matoušek, J., 522
 McCune, W., 119
 Miller, G.L., 429
 Mirimanoff, D., 41
 Moore, E.F., 312
 Mostowski, A., 286, 497
 Mučnik, A.A., 311
 Mulmuley, K., 409
 Mycielski, J., 223

N

Németi, I., 145
 von Neumann, J., 104, 165
 Newton, I., 585
 Nisan, N., 433

O

Odlyzko, A.M., 64, 660

P

Papadimitriou, C.H., 532
 Parikh, R., 497, 505, 523
 Paris, J.B., 320, 323, 324, 328, 523
 Peano, G., 30, 39, 93, 96
 Penrose, R., 303, 623
 Pierce, C.S., 111
 Pitowski, I., 145
 Planck, M., 284
 Poincaré, H., 108
 Popper, K., 95
 Post, E.L., 125
 Putnam, H., 119, 305
 Pythagoreans, 584

Q

Quine, W.V.O., 41, 232, 604, 605

R

Ramsey, F.P., 15
 Razborov, A.A., 386, 389
 te Riele, H.J.J., 64
 Riemann, B., 62
 Rissanen, J., 488
 Rivest, R.I., 430, 437
 Robinson, A., 237, 247
 Robinson, J.A., 60, 119
 Robinson, J.H.B., 305
 Robinson, R.M., 303
 Rosser, J.B., 233, 292
 Rudich, S., 389
 Ruffini, P., 263
 Russell, B., 43, 93, 157, 159, 596

S

Sarnak, P., 663
 Savitch, W.J., 446
 Schmerl, U.R., 619, 621
 Schönfinkel, M.I., 146
 Schröder, E., 111
 Schütte, K., 512
 Scott, D., 154, 215, 359
 Selberg, A., 61
 Shamir, A., 430, 437
 Shannon, C., 382, 394
 Shechtman, D., 304
 Shelah, S., 224
 Shor, P., 450
 Shub, M., 408
 Skolem, T., 86

Smale, S., 408
 Smith, K.T., 237
 Solomonoff, R.J., 480, 490
 Solovay, R.M., 202, 224, 229, 337, 359, 364,
 386, 428, 634, 664
 Specker, E., 233, 242
 Stearns, R.E., 377
 Steinhaus, H., 223
 Stimson, M.J., 446
 Strassen, V., 396, 428
 Szekerés, G., 15

T

Takeuti, G., 530
 Tao, T., 15
 Tarski, A., 81, 111, 218, 282
 Thomae, J., 600
 Thue, A., 392
 Tsfasman, M.A., 407
 Turing, A.M., 125, 132, 300, 618

V

Valiant, L., 409
 de la Vallée-Poussin, C., 61
 Vaught, R.L., 49
 Vinogradov, I.M., 14
 Visser, A., 299
 Vitali, G., 201
 Vlăduț, S.G., 407
 Vopěnka, P., 204, 237, 359

W

Wang, H., 94, 119, 243, 312
 Weierstrass, K.T.W., 39
 Werner, B., 120
 Weyl, H., 591
 Whitehead, A.N., 93
 Wiesner, S.J., 471
 Wigderson, A., 390, 426, 433
 Wiles, A., 57
 Wilkie, A., 523
 Woodin, W.H., 214, 223, 633

Y

Yannakakis, M., 532

Z

Žák, S., 41
 Zermelo, E., 37, 163, 165, 219
 Zink, T., 407

Subject Index

A

Algebra

- Boolean, 21, 111
 - complete, 360
- combinatory, 148
- cylindric, 111
- free, 91

Algorithm, 123

- probabilistic, 413
- quantum, 463–467
- Shore's, 464–467

Antinomy, 37

- Burali-Forti's, 42

Arithmetic

- Arithmetical Comprehension Axiom,
 ACA_0 , 643
- Arithmetical Transfinite Recursion, ATR_0 ,
643
- Cook's *PV*, 540
- Dedekind-Peano Arithmetic, 30, 146
- Elementary Arithmetic, *EA*, 617
- Peano Arithmetic, *PA*, 31, 60
- Peano Arithmetic, *PA*, 87, 505, 507, 510,
511, 524, 588, 614, 617, 619
 - axioms, 116
 - consistency of, 118
- Robinson Arithmetic, 116, 283, 294
- Second-Order Arithmetic, Z_2 , 295, 643
- True Arithmetic, 88

Arithmetic of infinite cardinals, 180

Arithmetization

- in Peano Arithmetic, 293
- of syntax, 276

Arity, 4

Artificial intelligence, 55

Automated theorem proving, 119

Autonomous progression, 620, 644

Axiom, 44

- forcing, 634
- higher axiom of infinity, 197
- independent, 50
- induction, 295
- large-cardinal, 197, 588, 629
- logical, 93
- Martin's, 363
- of choice, 173, 215–219
 - independence of, 352, 358
- of dependent choices, 224
- of determinacy, 219–221, 223
 - consistency, 230
- of feasible computations, 651
- of global choice, 175
- of infinity, 164, 173
- of limited universe, 651
- of projective determinacy, 633
- of solvability, 602, 655
- Tarski's, 208
- the strongest ever proposed, 214

Axiom schema, 48

- induction, 116
- replacement, 165
- restricted comprehension, 163
- typed comprehension, 159

B

Basis, *see* Connective, complete set of

Brute-force search, 368

C

Calculus

- functional, 74
- λ -calculus, *see* Lambda calculus
- propositional, 153

- Calculus (*cont.*)
 - Resolution, 60
 - sequent, 501, 516
 - Cardinal, 30, 178
 - inaccessible, 199
 - large, 197–215, 223, 339, 631–635
 - Mahlo, 200
 - measurable, 202, 634
 - Ramsey, 208
 - Vopěnka, 204, 214
 - weakly compact, 203
 - Woodin, 224, 229, 633
 - Cardinality, 178
 - Categorical foundations, 241
 - Category, 13, 22
 - Circuit
 - algebraic, 408
 - Boolean, 144, 380–385
 - quantum, 457, 468
 - randomized, 429
 - threshold, 440, 447
 - uniform, 384
 - Class, 166
 - nonelementary, 52
 - proper, 166
 - universal, 166
 - Clause, 60
 - Compactness, 115
 - Completeness, 50
 - relative, 50
 - Complexity
 - algebraic, 395–397
 - algorithmic, *see* Kolmogorov's
 - average case, 367
 - communication, 405
 - descriptive, 479
 - Kolmogorov's, 480–487
 - nondeterministic space, 402
 - of factoring, 398
 - of matrix multiplication, 396
 - of multiplication, 398
 - of primality, 374, 398, 428
 - of proof search, 371, 375
 - quantifier, 79
 - space, 378
 - time, 375
 - worst case, 367
 - Complexity class
 - algebraic, 408
 - bounded error probabilistic polynomial time **BPP**, 421
 - bounded error quantum polynomial time **BQP**, 470
 - co-nondeterministic polynomial time **coNP**, 376
 - nondeterministic polynomial time **NP**, 373
 - nonuniform, 384
 - polynomial local search **PLS**, 532
 - polynomial space **PSPACE**, 378
 - polynomial time **P**, 372
 - probabilistic, 421
 - quantum polynomial time **QP**, 470
 - relativized, 386
 - syntactical vs. semantical, 575
 - total polynomial search **TPS**, 530–534
 - Computability theory, 310
 - Computation
 - algebraic, 395
 - in the brain, 439–443
 - matrix model of, 137, 144, 383
 - parallel, 437–446
 - quantum, 448–479
 - relativistic, 145
 - reversible, 461–463
 - semantics of, 136
 - syntax of, 136
 - Conjecture
 - $3x + 1$, 325
 - Ω -conjecture, 635, 645
 - Goldbach, 14
 - Kepler, 15
 - PRG, 388, 435
 - Robbins', 119
 - Connective, 67, 68, 75
 - complete set of, 78, 382
 - Consistency, 49, 84, 103, 600
 - inner, 587
 - ω -consistency, 642
 - relative, 91
 - Consistency strength, 206, 612, 613
 - Constant, 69
 - Constructivism, 108
 - Cryptography, 418–421
 - public key, 430
 - quantum, 476
 - Curry-Howard isomorphism, 152, 598
 - Cut
 - Dedekind's, 34
 - in a model, 333
 - Cut-elimination, 501–504, 517
 - Cutting planes, *see* Proof system, cutting-planes
- D**
- Definition
 - impredicative, 161
 - predicative, 161, 166

- Derandomization, 425
- Diagonal argument, 41, 181
- Discrete logarithm, 427
- E**
- Echelon construction, 16
- Elementary embedding, 204, 212
- Elements*, 44, 93, 585
- Elitzur-Vaidman bomb test, 453
- Equality, 73
- Equation
 - algebraic, 262
 - Diophantine, 56, 304–308
 - quintic, 271
- Equinumerous, 31
- Error correcting code, 407
- Ex falso quodlibet, 36
- Excluded middle, 93
- F**
- Feasible interpolation, *see* Method, lower bound, feasible interpolation
- Field, 20
 - number field, 267
 - splitting, 268
- Field extension, 263
 - Galois, 268
 - radical, 269
- Finite automaton, 21
- Finitism, 600
 - objective, 650
- Forcing, 341–354, 631–635
- Forcing condition, 356
- Formal system, 49
- Formalism, 600–604
 - game, 600
- Formalized ω -rule, 642
- Formula, 72
 - atomic, 73
 - bounded arithmetical, 534
 - flexible, 286
- Frege's logical system, 170
- Function, 4
 - Ackermann, 336
 - Boolean, 21, 399
 - busy beaver, 129
 - collapsing, 209
 - computable, 142, 310
 - explicitly defined, 390
 - fast growing, 514
 - Möbius, 62
 - noncomputable, 128
 - one-way, 418
 - partial recursive, 141, 311
 - propositional, 74, 150
 - provably total, 514
 - recursive, 133, 310
 - definition of, 142
 - successor, 30
 - threshold, 440
 - time constructible, 377, 397
 - Veblen, 195
- Functional, 17
- G**
- Galois correspondence, 268
- Game, 219, 221, 379
- Geometric complexity theory, 409
- Geometry, 44, 584
 - Euclidean, 51
 - hyperbolic, 85
- Gödel's dichotomy, 626
- Gödel's Program, *see* Large-Cardinal Program
- Graph, 6
 - expander, 394
 - planar, 14, 18
 - Ramsey, 393
 - random, 393
- Grothendieck universe, 207
- Group, 7, 10, 18
 - abelian, 265
 - braid, 205
 - commutative, 265
 - simple, 9, 19
 - soluble, 270
- H**
- Halting problem, 128
- Hierarchy
 - arithmetical, 141
 - bounded arithmetic, 539
 - constructible, 343
 - cumulative, 168
 - of functions, 336
 - polynomial, 401
- Hilbert's Program, 100, 101, 118
- Holism, 604
- Human mind, 621–626
- Hypothesis
 - continuum, 183, 229, 341–344, 348, 635
 - extended Riemann's, 413, 429
 - generalized continuum, 183, 214
 - Mertens, 64
 - Riemann's, 62
 - Hilbert-Pólya's approach to, 660

I

- Ignorabimus, 602
- Incompressibility, 482
 - instead of randomness, 492
- Independence of $\mathbf{P} \neq \mathbf{NP}$, 639
- Induction
 - mathematical, 30
 - on notation, 543
 - transfinite, 192, 510
- Inductive reasoning, 490
- Infinity
 - actual, 178
 - potential, 177, 592
- Input length, 367
- Intuition, 606
- Intuitionism, 108, 591–595
- Isomorphism, 13

K

- Kripke semantics, 121

L

- Lambda calculus, 146–152, 162
 - model of, 154
 - type-free, 147
 - typed, 150, 598
- Language, 592
 - context-free, 76
 - higher-order, 78
 - logical, 72
 - metalanguage, 82
 - natural, 71
 - object, 82
 - of first-order logic, 76
 - of propositional logic, 75
 - programming, 73, 82, 127
- Large-Cardinal Program, 629–631
- Laver table, 215
- Lemma, 499
 - diagonal, 289, 291
 - König's, 24
- Logic
 - Ω -logic, 645
 - classical, 70
 - combinatory, 146, 152
 - first-order, 51, 74
 - undecidability of, 132
 - higher-order, 102
 - intuitionistic, 120, 151, 592
 - modal, 120
 - propositional, 78, 111, 545
 - provability, 297
 - second-order, 145
 - symbolic, 72

- Logic gates, 381
- Logic of relations, 111
- Logicism, 66, 595–599

M

- Mach-Zehnder interferometer, 451, 468
- Machine
 - parallel, 446
 - parallel random access, 446
 - random access, 377
 - Turing's, *see* Turing machine
- Mathematical realism, *see* Platonism
- Measure, 201
 - probability, 491
- Metalanguage, 82
- Method
 - feasible interpolation, 559
 - lower bound, 403–406
 - of ideal elements, 602
 - probabilistic, 392
- Modality, 68
- Model, 47, 82, 84
 - Beltrami-Klein, 90
 - Boolean valued, 359–362
 - inner, 354
 - nonstandard, 87, 91, 236
 - of set theory, 342–354
 - Solovay's, 229
 - standard, 88, 614
- Model theory, 82
- Modus ponens, 94

N

- Neural network, 448
- New Foundations, *see* Set theory
- Nonstandard analysis, 235, 244–250
- Normal subgroup, 268
- Normalization, 598
- \mathbf{NP} -completeness, 400
- Number
 - algebraic, 56, 257
 - cardinal, *see* Cardinal
 - irrational, 256–259
 - large cardinal, 197
 - natural, 30, 584, 592
 - nonstandard, 88
 - ordinal, *see* Ordinal
 - physical, 646
 - Ramsey, 16, 392, 406
 - real, 5, 33, 35
 - RSA-129, 368, 437
 - standard, 88
 - transcendental, 56, 266

O

- Operation, 4
- Ordinal, 26, 184–187
 - Bachmann–Howard, 210
 - Cantor normal form, 193
 - constructive, 193, 209, 619
 - Feferman–Schütte, 194
 - proof-theoretic, 521
 - definition of, 510
- Ordinal analysis, 510–514

P

- Pair, 34
- Pairs of disjoint **NP** sets, 576
- Paradox, 37, 592
 - Banach–Tarski’s, 218, 225–229
 - Berry’s, 38, 161, 486
 - Cantor’s, 41
 - Epimenides, 38
 - Hilbert’s, 42
 - liar’s, 38
 - Russell’s, 37, 40, 157
 - semantic, 38, 283
- Platonism, 586–591
 - degree of, 589
- Polynomially simulates, 551
- Positivism, 27
- Postulate, 44
 - Euclid’s fifth, 51, 85
- Power set, 12
- Predicate, 4
- Predicativism, 644
- Principle
 - comprehension, 28, 158
 - existence from consistency, 602, 611
 - extensionality, 26, 28
 - minimal changes, 605
 - minimum description length, 488, 605
 - Möbius randomness, 663
 - pigeonhole, 546
 - power and usefulness, 591
 - reflection, 296, 335, 498, 615, 642
 - in set theory, 645
 - Vopěnka’s, 204, 214
- Problem
 - algorithmically undecidable, 301–309
 - Collatz’s, 325–328
 - decision, 300
 - Entscheidungsproblem, 132, 306
 - feasible consistency, 564–566
 - graph isomorphism, 415
 - halting, 300
 - Hamiltonian cycle, 371
 - hidden subgroup, 475

- Hilbert’s fifth, 237
 - Hilbert’s tenth, 304
 - identity testing, 413
 - integer factoring, 368
 - integer linear programming, 557
 - linear programming, 533
 - Mutilated Chess-Board, 55
 - NP** versus **coNP**, 376, 408, 409, 551, 580
 - P** versus **NP**, 370–376, 566, 580
 - promise, 577
 - search, 530
 - $\Theta_{\mathbf{P}}$ versus $\Theta_{\mathbf{NP}}$, 626
 - total-measure, 201
 - Product of sets, 11
 - Program, 124
 - unpredictable, 287
 - Proof, 92
 - direct, 499
 - feasibly constructive, 540–545
 - holographic, 414, 429
 - interactive, 415
 - natural, 389
 - nonconstructive, 109, 382, 391–395
 - nonelementary, 522
 - probabilistic, 393, 406
 - purely existential, *see* Nonconstructive
 - quantum, 478
 - speed-up, 496–499, 515
 - zero-knowledge, 417
 - Proof checking, 94
 - Proof mining, 110, 501
 - Proof system
 - complete, 550
 - cutting-planes, 558
 - extended Frege, 552
 - Frege, 551
 - Hilbert style, 113
 - length-optimal, 568, 580
 - natural deduction, 97, 113
 - optimal, 571, 580
 - polynomially bounded, 551
 - propositional, 548–559
 - definition of, 550
 - sound, 550
 - Proof theory, 101
 - Pseudorandom generator, 423
 - Nisan–Wigderson’s, 433
- Q**
- Quantifier, 67, 68, 74
 - alternating, 74, 140
 - axioms and rules, 113
 - Quantum bit, 453

R

Radical, 262
 Realism, 586
 Recursion, 32
 on notation, 542
 Recursion theory, 310
 Relation, 4
 RSA, 430

S

Satisfaction, 81, 82
 definition of, 88
 Self-distributive system, 205
 Self-reference, 41, 273–275, 486
 Semiset, 238
 Sentence, 74
 combinatorial, 339
 empirically testable, 609
 Gödel's, 279, 308
 logically valid, 83
 Paris-Harrington's, 333
 Π_1 , 609
 Rosser's, 292
 universal finite, 609
 universal-finite, *see* Sentence, Π_1
 universal-P, 528, 541, 609
 unprovable in Θ_P , 560

Sequence

Cauchy, 33, 35
 Goodstein, 321–324, 327

Set, 25

constructible, 343, 355
 decidable, 310
 finite, 190
 generic, 346, 356
 nonmeasurable, 212
 ordered, 17
 random generic, 363
 recursive, 310
 recursively enumerable, 311

Set theory

Alternative Set Theory, 238
 axioms of, 250
 Finite Set Theory, ZF_{fin} , 117
 Finite Set Theory, ZF_{fin} , 323
 Gödel-Bernays Set Theory, 166
 axioms of, 174
 Kelly-Morse Set Theory, 174
 Kripke-Platek Set Theory, 195
 New Foundations, 232
 axioms of, 241
 von Neumann-Bernays Set Theory, *see*
 Gödel-Bernays Set Theory
 Zermelo Set Theory, 163

Zermelo-Fraenkel Set Theory, ZFC , 47,
 165, 613
 axioms of, 173

Zermelo-Fraenkel Set Theory without
 Axiom of Choice, ZF , 223

Σ -completeness, 290

Soundness, 98, 613
 arithmetical, 614

Structure, 82

algebraic, 10
 first-order, 10
 mathematical, 2
 second order, 10
 universe of, 4

Syllogisms, 44, 93

T

Tautology, 83

Term, 73

Theorem

Buss's, 532
 Cantor's, 182
 Church-Rosser's, 152
 completeness, 99, 114
 Craig's interpolation, 559
 Fermat's last, 208
 finite Ramsey's, 328
 first incompleteness, 101, 102
 proof of, 278
 fixed point, 149, 289
 four color, 13, 120
 Gödel-Tarski's, 283
 Herbrand's, 500, 501, 504, 518
 incompleteness, 273, 486
 infinite Ramsey's, 25
 Kruskal's, 330, 337
 Löb's, 616
 Łos's, 252
 Löwenheim-Skolem's, 89
 Matiyasevich's, 315–319
 Nullstellensatz, 549
 Paris-Harrington's, 328
 prime number, 61
 Ramsey's, 15, 203, 242, 309, 319, 339
 proof of, 23
 Roth's, 501
 second incompleteness, 103, 567
 proof of, 279
 space hierarchy, 378
 Thue-Siegel-Roth's, 392
 time hierarchy, 377

Theorem provers, 94
 Theory, 47, 84
 arithmetical, 87

Theory (*cont.*)

- arithmetically sound, 614
 - elementary, 48
 - empirical, 488
 - equational, 79
 - for a complexity class, 529
 - formal, 49
 - Galois, 263–266, 268–271
 - nonelementary, 48
 - relativized, 540
 - sound, 613–615
 - true, 613
 - useful inconsistent, 504
- Theory for a class C , 525
- Theory for \mathbf{NP} , $\Theta_{\mathbf{NP}}$, 536
- Theory for \mathbf{P} , $\Theta_{\mathbf{P}}$, 535
- Theory of Types, 159
- Ramified Class Calculus, 162
 - Simple Type Theory, 159, 242
 - axioms of, 171
- Thesis
- Church-Turing's, 134, 448
 - feasible incompleteness, 562
 - logician, 595
 - natural number, 649
 - parallel computation, 446
 - physical Church-Turing's, 136
 - quantum computing, 460
- Tiling, 302, 312
- aperiodic, 314

Transfinite progressions of theories, 618–621

- definition of, 642
- Tree, 24, 520
- Truth, 80
- undefinability of, 281
- Turing machine, 125
- definition of, 143
 - multitape, 377
 - nondeterministic, 375
 - probabilistic, 421, 429
 - universal, 131
- Type, 17, 150, 159
- Boolean, 150

U

- Ultrafilter, 208, 252
- Ultrafinitism, 506, 650, 652
- Ultrapower, 213, 251

V

- Variable, 69
- bound, 74
 - free, 74

W

- Wang's system Σ , 243
- Well-ordering, 191
- World
- Impagliazzo's, 579
 - inconsistent, 507

Symbols and Abbreviations

- 2^{\aleph_α} , 182
- ACA_0 , 643
- ATR_0 , 643
- $Con(T)$, 612
- Con_T , 280
- $Con_T(n)$, 564
- EA , 617
- FN , 239
- L , 214
- PA , 116
- PD , 633
- PHP_n , 546
- PV , 523
- $Pr_T(\phi)$, 497
- $S(x)$, 30
- T_α^{Con} , 618
- T_α^{RFN} , 621
- V , 166
- V_α , 169
- $X \times Y$, 11
- ZF , 223
- ZFC , 165
- ZF_{fin} , 117
- Z_2 , 643
- Γ_0 , 194
- Π_1 , 140
- Π_P , 528
- $\Sigma_1^0, \Pi_1^0, \Sigma_2^0, \Pi_2^0, \dots$, 141
- Σ_1 , 140
- Θ_{NP} , 526
- Θ_P , 526
- Θ_C , 525
- \aleph_α , 178
- FP**, 532
- PLS**, 532
- TPS**, 530
- \emptyset , 31
- ε_0 , 193
- \equiv , 75
- \exists , 74
- \forall , 74
- γ_T , 278
- \mathbb{L}_{phys} , 647
- \mathbb{N} , 10
- \mathbb{N}_{phys} , 647
- \mathbb{R} , 5, 10
- \neg , 75
- ω , 185
- ω_1^{CK} , 195
- $\psi(\varepsilon_{\Omega+1})$, 211
- \rightarrow , 75
- \vee , 75
- \wedge , 75
- $\{a_1, a_2, \dots, a_n\}$, 29
- $f : X \rightarrow Y$, 12
- $\mathcal{P}(A)$, 12
- BPP**, 421
- BQP**, 470
- EF**, 552
- EXPTIME**, 378
- NC^1 , 547
- NP**, 373
- $NP \cap coNP$, 402
- PSPACE**, 378
- P**, 372
- QP**, 470
- coNP**, 376
- nonuniformP**, 384
- $TPhN$, 650
- $RFN(T)$, 617
- $Rfn(T)$, 615