SOME SUGGESTED ARGUMENTS FOR THE FINAL PRESENTATION EXAM

MATHEMATICAL LOGIC FOR COMPUTER SCIENCE - 2020/2021

ABSTRACT. The following is a commented list of suggested topic for final presentation, with some bibliographical pointer. Please feel free to select and propose your own logic topic! Topics for final will be assigned on a first come, first served policy.

Consistency of the Predicate Calculus

We proved that the Predicate Calculus is consistent using a semantic argument ($\vdash E$ implies $\models E$). There exist more informative proofs of this result that use only syntactical methods.

References: Shoenfield, Mathematical Logic, pp. 48-52

Consistency of Peano Arithmetic

As discussed in class Gentzen gave a proof of the consistency of Peano Arithmetic using induction over some countable (computable) ordinals.

References: Gaisi Takeuti, Proof Theory (Springer 1987, Dover 2013), Chapter II.

Herbrand's Theorem

Herbrand's Theorem is a fundamental result with many consequences in theory and applications. The theorem reduces provability in the Predicate Calculus to propositional provability: a formula $\exists x F(x)$ is provable if and only if a disjunction $F(t_1) \vee \cdots \vee F(t_n)$ is provable, where every t_i is a term in the language of F.

References: Shoenfield, Mathematical Logic, pp. 52-55

Cut-Elimination Theorem

The Sequent Calculus is a formalism for first-order logic proofs introduced by Gerhard Gentezen that has many applications in automated deduction. The most important theorem about the Sequent Calculus is the the Cut Elimination Theorem which shows, essentially that every proof can be transformed in a completely explicit proof in which no formula disappears from the premises to the conclusion. This helps in automatic theorem proving.

References: Gentzen, Investigations into logical deduction; Takeuti, Proof Theory.

Gödel's Second Incompleteness Theorem, new proof

This paper gives a new proof of Gödel's Second Incompleteness Theorem using methods of Kolmogorov Complexity.

References: S. Kritchman and R. Raz, The surprise examination paradox and the Second Incompleteness Theorem. (5 pages)

Provably total functions of formal arithmetic

A (computable) function is provably total in a theory T if there exists a formal proof of totality of the function from axioms of T. The provably total functions of first-order Peano Arithmetic can be fully characterized in terms of growth-rate using an appropriate hierarchy of fast-growing functions indexed by transfinite ordinals. This characterizations is a powerful tool for obtaining unprovability results of combinatorial principles.

References: Andreas Weiermann, Classifying the provably total function of PA. Bulletin of Symbolic Logic, 12:2, 177-190, 2006.

Paris-Harrington's Theorem (original proof)

Gödel's Theorem shows that any reasonable formal theory of arithmetic is incomplete. Yet the witnesses of incompleteness are coded logical statements, not natural propositions about natural numbers. It took thirty years to find the first examples of concrete mathematical principles that are (true but) neither provable nor disprovable from the formal system of arithmetic known as Peano Arithmetic. The Paris-Harrington principle is the first such example and is a slight variant of Ramsey's Theorem. The original proof uses model theory.

Jeff Paris and Leo Harrington: A mathematical incompleteness in Peano Arithmetic. In Jon Barwise (editor) Hanbook of Mathematical Logic.

Paris-Harrington's Theorem (combinatorial proof)

In this paper the authors give a concise elegant combinatorial proof of this result. The proof is based on the characterization of the provably total functions of arithmetic. The proof uses transfinite ordinals.

References: Martin Loebl, Jaroslav Nešetril. An unprovable Ramsey-type theorem. Proceedings of the American Mathematical Society, 116:3, 819-824, 1992. Abstract: We present a new proof of the Paris-Harrington unprovable (in PA) version of Ramsey's theorem. This also yields a particularly short proof of the Ketonen-Solovay result on rapidly growing Ramsey functions.

Goodstein Sequences

Goodstein sequences are one of the first examples of natural mathematical theorems unprovable in formal theories such as Peano Arithmetic. The proof uses transfinite ordinals.

References:
A. Caicedo, Goodstein functions (expository article: `http://emis.impa.br/EMIS/journals/RCM/Articulos/878.pdf`.
M. Rathjen, Goodstein's Theorem Revisited, `http://www1.maths.leeds.ac.uk/ rathjen/Goodstein-rev.pdf`.

Ultrafilters, ultraproducts and Compactness

Ultrafilters are a very powerful tool in many areas of maths and computer science. In particular they can be used to give a proof of the Compactness Theorem that does not use the Completeness Theorem. Ultrafilters and the related notion of ultraproduct allows to build a model from an infinite sequence of models by taking a sort of majority vote to decide which sentences hold in the new structure.

References: Handouts.

Ultrafilters and Ramsey Theorem

Ultrafilters can be used in Combinatorics to give elegant proofs of theorems. In particular they can be applied to give a proof of Ramsey's Theorem.

References: Handouts.

Intractability of the theory of addition on N (Presburger Arithmetic)

The first-order theory of addition is decidable but intractable. The result can be established using the method of encoding the Limited Halting Problem in the theory.

References: Michael J. Fischer and Michael O. Rabin, Super-Exponential Complexity of Presburger Arithmetic. Proceedings of the SIAM-AMS Symposium in Applied Mathematics 7: 27-41. Michael Machtey and Paul Young, Introduction to the General Theory of Algorithms, Elsevier 1978.

Intractability of the theory of real addition

The first-order theory of real addition is decidable but intractable (any decision procedure has double exponential lower bounds). We have proved decidability by quantifier elimination in class, but the result can also be established using Ehrenfeucht-Fraissé games.

References: Devdatt P. Dubhashi, Complexity of Logical Theories, pp. 13-31.

Kleene's Recursion Theorem

Kleene's Theorem shows that there exist self-referential programs. For every algorithmic task p there exists a program e that makes a copy of its own code and applies p to its self-copy and to any external

input. Furthermore, a code for program e can be obtained uniformly and algorithmically from program p. It is an interesting and complex task to investigate the effective programming systems that satisfy various (constructive and non-constructive) forms of the Kleene Recursion Theorem with the goal of obtaining a mathematical characterization of self-reference.

References: Selected sections from Samuel Moelius, Program Self-Reference. PhD Thesis, 2008.

Ultrafilters in Combinatorics

Ultrafilters are a powerful tool for proving results in combinatorics. In particular they can be used to obtain elegant proofs in Ramsey's Theory.

References: Luigi Di Nasso, Dispense del corso di Logica Matematica, University of Pisa, Dipartimento di Matematica. (In Italian).

0-1 Laws for First-Order Logic

Properties expressible in many logics are almost surely true or almost surely false; that is, either they hold for almost all structures, or they fail for almost all structures. This phenomenon is known as the zero-one law. In particular, it holds for First-Order Logic.

References: Leonid Libkin, Elements of Finite Model Theory, pp. 247-254.

Locality of First-Order Logic

Gaifman showed that every first-order sentence is equivalent to a combination of so-called local sentences.

References: Leonid Libkin, Elements of Finite Model Theory, pp. 55-60.

Büchi's Theorem

The theorem characterizes the class or regular languages using a fragment of second-order logic, Monadic Second-Order Logic. The proof is based on description of computations of non-deterministic Turing Machines.

References: Chapter in Libkin, Elements of Finite Model Theory.

Immerman-Vardi Theorem

Even though the problem of finding a logic that captures polynomial time **P** is still open, Immerman and Vardi showed that the complexity class **P** is captured *over ordered structures* by a logic extended with least fix-point operators.

References: Leonid Libkin, Elements of Finite Model Theory, pp. 171-188.

Size of propositional proofs of the Pigeonhole Principle

Propositional Proof Complexity studies the length of proofs of tautologies in propositional proof systems. This problem is strictly connected to the P vs NP problem. A fundamental result in the area is that proofs of exponential size are necessary for proving tautologies expressing the Pigeonhole Principle in the proof system known as Resolution.

References: S. Jukna, Extremal Combinatorics with applications in Computer Science, pp. 47-51.

Reverse Mathematics

Reverse Mathematics is concerned with the question of which set-existence axioms are necessary and sufficient for proving mathematical theorems. Five systems of (second-order arithmetic) have been isolated and a vast number of mathematical theorems have been proved to be equivalent to one of these systems. The systems are formalized in the language of second-order arithmetic and are strictly related to closure under computability-theoretic operations (e.g. Turing jump).

References: Selected reading from S. J. Simpson, Subsystems of Second Order Arithmetic.

The strength of Hindman's Theorem

Hindman's Theorem is a famous combinatorial theorem stating that for every finite coloring of the positive integers there exists an infinite set of numbers such that all the numbers in the set and all finite unions of

finitely many distinct numbers from the set have the same color. Measuring the complexity of the solution for computable colorings is a major open problem. Blass, Hirst and Simpson showed in 1987 that there is a computable coloring such that all solutions to Hindman's Theorem compute the Halting Set. This has been recently refined by Dzhafarov, Jockusch, Solomon and Westrick to the restriction of Hindman's Theorem to sums of one, two or three distinct terms.

References: Andreas R. Blass, Jeffry L. Hirst, and Stephen G. Simpson, Logical analysis of some theorems of combinatorics and topological dynamics, in Stephen G. Simpson, ed., Logic and Combi- natorics, Contemporary Mathematics 65, American Mathematical Society, Providence, RI, 1987, 125-156.

Damir D. Dzhafarov, Carl G. Jockusch, Jr., Reed Solomon, and Linda Brown Westrick, Effectiveness of Hindman's Theorem for bounded sums, in Adam Day, Michael Fellows, Noam Greenberg, Bakhadyr Khoussainov, Alexander Melnikov, and Frances Rosamond, eds., Computability and Complexity: Essays Dedicated to Rodney G. Downey on the Occasion of His 60th Birthday, Lecture Notes in Computer Science 10010, Springer, Cham, 2017, 134-142.

Tennenbaum's Theorem

Tennenbaum's Theorem shows that the standard model is (modulo isomorphism) the unique countable computable model of Peano Arithmetic. In all countable non-standard model either addition or multiplication have to be non computable.

References: Richard Kaye, Models of Peano Arithmetic, Richard Kaye, Tennebaum's Theorem for Models of Arithmetic, in Juliette Kennedy and Roman Kossak, Set theory, Arithmetic, and Foundations of Mathematics - Theorems, Philosophies (`http://web.mat.bham.ac.uk/R.W.Kaye/papers/tennenbaum/tennenbaum.pdf`), Peter Smith, Tennenbaum's Theorem (`http://www.logicmatters.net/resources/pdfs/TennenbaumTheorem.pdf`).

Monadic Second-order logic

Second-order logic is an extension of first-order logic which allows quantification over sets and relations. Monadic second-order logic is fragment of second-order logic in which only unary predicates are allowed. This logic is more expressive than first-order logic and can express some NP-complete problems. Extensions of Ehrenfeucht-Fraïssé games and other tools are used to study expressibility and inexpressibility of queries in Monadic Second-Order Logic.

References: A selection from Chapter 7 of Libkin's *Elements of Finite Model Theory* book.

Logic with counting

First-order logic has some severe limitations with respect to counting. For example, no formula of degree n can distinguish two linear order of cardinality above 2^n. Extensions of first-order logic exist that have some counting power and tools can be developed to study expressibility and inexpressibility of queries in these logics.

References: selection from Chapter 8 of Libkin's *Elements of Finite Model Theory* book.

Friedberg-Muchnik's Theorem

The theorem solves Post's problem in the positive: there exists a c.e. set that is neither computable nor complete, i.e. there exists an intermediate degree of complexity with c.e. instances between the computable sets and the halting problem.

References: R. Soare, Recursively Enumerable Sets and Degrees, Part B, Chapter VII, pp. 110-121.

Provability Logic and Modal Logic

The the predicate "E is provable in T" for a formal theory of arithmetic T behave in a similar way to the modal operator $\Box$ (necessity) and to the temporal logic operator "forever". The semantics of this kind of logic uses so-called Kripke frames. An introduction to the syntax, semantics and basic properties of this kind of logic is of interest for Logic, Proof Theory and Computer Science.

References: Handouts.

Completeness of Provability Logic for Arithmetic

The logic of the provability predicate $\Box$ for arithmetical theories can be finitely axiomatized. A completeness theorem is provable with respect to so-called Kripke semantics of frames for these systems.

References: Handouts.

Solovay's Arithmetical Completeness Theorem (original proof)
If T is a formal theory of arithmetic one can consider the behaviour of the provability predicate $Prov_T(n)$, expressing the fact that the formula with code n is provable from the axioms of T. Solovay proved a surprising theorem showing that the behaviour of this predicate for Peano Axioms for arithmetic is completely described by a system of Modal Logic. The proof is complex and makes use of fixed-point theorems.

References: Robert M. Solovay. Provability interpretations of modal logic. Israel Journal of Mathematics, 25:287-304, 1976.

Solovay's Arithmetical Completeness Theorem (new proof)
A new proof of Solovay's Completeness Theorem has been recently given that does not use fixed-points.

References: Fedor Pakhomov, Solovay Completeness without Fixed Points.
Preprint: `https://arxiv.org/pdf/1703.10262.pdf`.

Satisfiability Modulo Theories
Some applications in artificial intelligence and hardware and software development sometimes require determining the satisfiability of a first-order formula with respect to some background theory fixing the intepretation of some symbols in the formula. Satisfiability Modulo Theories research points at developing decision procedures (solvers) to use in these situations.

References: Clark Barrett, Roberto Sebastiani, Sanjit A. Seshia and Cesare Tinelli, Satisfiability Modulo Theories, in Handbook of Satisfiability Armin Biere, Marijn Heule, Hans van Maaren and Toby Walsh (Eds.) IOS Press, 2009, 825-885. Available online.

Temporal Logic(s)
Different systems of Temporal Logic are widely used in formal verification. A variety of systems exist (Interval, Linear, Computation tree, modal mu-calculus, etc.), each suitable for different applications.

References: Mordechai Ben-Ari, Mathematical Logic for Computer Science, Third Edition, Springer 2012 chapter 13 containes the basics of TL and pointers to further bibliography.

Natural Proofs
The paper provides foundations for a class of heuristics currently used in automated rasoning for program verification to reason with quantified logics in practice, based on quantifier instantiation and recursive definitions.

References: Löding, Madhusudan, Pena, Foundations for natural proofs and quantifier instantiation; Proceedings of the ACM on Programming Languages, (2018), Proceedings of the ACM on Programming Languages, vol. 2 (availabel at: `http://publications.rwth-aachen.de/record/713651/files/713651.pdf`)