Formalisation of Additive Combinatorics in Isabelle/HOL

Angeliki Koutsoukou-Argyraki
University of Cambridge, UK

Abstract

In this talk, I will present an overview of recent formalisations, in the interactive theorem prover Isabelle/HOL, of significant theorems in additive combinatorics, an area of combinatorial number theory. The formalisations of these theorems were the first in any proof assistant to my knowledge. For each of these theorems, I will discuss selected aspects of the formalisation process, focussing on observations on our treatment of certain mathematical arguments when translated into Isabelle/HOL and our overall formalisation experience with Isabelle/HOL for this area of mathematics.

2012 ACM Subject Classification Mathematics of computing → Combinatorics; Theory of computation → Logic and verification

Keywords and phrases Additive combinatorics, additive number theory, combinatorial number theory, formalisation of mathematics, interactive theorem proving, proof assistants, Isabelle/HOL

Digital Object Identifier 10.4230/LIPIcs.ITP.2023.1

Category Invited Talk

Funding Angeliki Koutsoukou-Argyraki is funded by the ERC Advanced Grant ALEXANDRIA (Project GA 742178, European Research Council) led by Lawrence C. Paulson (University of Cambridge, Department of Computer Science and Technology). The Cambridge Mathematics Placements (CMP) Programme has been supporting and (partially) funding summer internships contributing to (ongoing) formalisations: Mantas Bakšys (2022); three more internships to contribute to Isabelle/HOL formalisations of material in a related area to be supported in 2023.

1 Summary

Additive combinatorics studies the properties of sumsets of subsets of groups, often employing proof techniques from other mathematical areas. In 2022 I initiated a line of formalisations of results in this area of mathematics using Isabelle/HOL [11], one of my main goals being the formalisation of advanced course material from the Cambridge Mathematical Tripos. My collaborators and I achieved the formalisation of a number of profound theorems in this area. A first project involved the formalisation of a proof of the Plünnecke–Ruzsa Inequality [9], an inequality giving information on the size (cardinality) of sumsets (and difference sets) of finite subsets of an abelian group. To this end, Lawrence Paulson and I, building on an algebra library by Clemens Ballarin [2], introduced the basics of sumset theory in Isabelle/HOL including basic results such as the Ruzsa Triangle Inequality [9]. Our source was the set of the 2022 lecture notes by Timothy Gowers for Part III of the Cambridge Mathematical Tripos [5]. Building on our formalisation of the basics [9] and again following [5], Lawrence Paulson and I went on to formalise Khovanskii's Theorem [8], which attests that for all sufficiently large n, the cardinality of the n-iterated sumset of a finite subset of an abelian group is polynomial in n. Continuing to follow [5], Mantas Bakšys, Chelsea Edmonds and I, formalised the Balog–Szemerédi–Gowers Theorem [7, 6], a profound result which played a central role in Gowers's proof deriving the first effective bounds for Szemerédi's Theorem. The Balog–Szemerédi–Gowers Theorem attests that every finite subset (of given additive energy) of an abelian group must contain a large subset whose sumset (difference set) is small, and gives bounds on these cardinalities depending on the given additive energy. The proof is of great mathematical interest in itself given that it involves an interplay between graph theory, probability theory and additive combinatorics. This interplay made the formalisation process more rich and technically challenging, and was handled by an appropriate use of locales, Isabelle's module system. To treat the graph-theoretic aspects of the proof, we made use of a new, more general undirected graph theory library by Chelsea Edmonds [4]. Another subsequent formalisation project, this time involving proofs of purely combinatorial and algebraic flavour, was the formalisation of Kneser's Theorem (following a paper by Matt DeVos [3]) and the Cauchy–Davenport Theorem as its corollary by Mantas Bakšys and myself [1]. Both theorems give information on various estimates on the cardinality of sumsets of finite subsets of abelian groups under certain conditions. Lastly, I will very briefly comment on a new line of ongoing formalisation work that I initiated, currently in progress by my students from the Computer Science Department and my interns from the Mathematics Department at Cambridge: formalising material in additive number theory, a related research area involving combinatorial tools. In particular, this line of work involves material related to Waring's problem and follows Nathanson's book [10].

References

1. Mantas Bakšys and Angeliki Koutsoukou-Argyraki. Kneser's Theorem and the Cauchy–Davenport Theorem. *Archive of Formal Proofs*, November 2022. Formal proof development. URL: `https://isa-afp.org/entries/Kneser_Cauchy_Davenport.html`.
2. Clemens Ballarin. A Case Study in Basic Algebra. *Archive of Formal Proofs*, August 2019. Formal proof development. URL: `https://isa-afp.org/entries/Jacobson_Basic_Algebra.html`.
3. Matt DeVos. A Short Proof of Kneser's Addition Theorem for Abelian Groups. In *Springer Proceedings in Mathematics and Statistics, vol 101*, pages 39–41, New York, NY, USA, 2014. Springer New York. `doi:10.1007/978-1-4939-1601-6_3`.
4. Chelsea Edmonds. Undirected Graph Theory. *Archive of Formal Proofs*, September 2022. Formal proof development. URL: `https://isa-afp.org/entries/Undirected_Graph_Theory.html`.
5. Timothy Gowers. *Introduction to Additive Combinatorics.* Online course notes for Part III of the Mathematical Tripos, University of Cambridge, 2022.
6. Angeliki Koutsoukou-Argyraki, Mantas Bakšys, and Chelsea Edmonds. The Balog–Szemerédi–Gowers Theorem. *Archive of Formal Proofs*, November 2022. Formal proof development. URL: `https://isa-afp.org/entries/Balog_Szemeredi_Gowers.html`.
7. Angeliki Koutsoukou-Argyraki, Mantas Bakšys, and Chelsea Edmonds. A Formalisation of the Balog–Szemerédi–Gowers Theorem in Isabelle/HOL. In *Proceedings of the 12th ACM SIGPLAN International Conference on Certified Programs and Proofs, Boston, MA, USA*, pages 225–238, New York, NY, USA, 2023. Association for Computing Machinery. `doi:10.1145/3573105.3575680`.
8. Angeliki Koutsoukou-Argyraki and Lawrence C. Paulson. Khovanskii's Theorem. *Archive of Formal Proofs*, September 2022. Formal proof development. URL: `https://isa-afp.org/entries/Khovanskii_Theorem.html`.
9. Angeliki Koutsoukou-Argyraki and Lawrence C. Paulson. The Plünnecke–Ruzsa Inequality. *Archive of Formal Proofs*, May 2022. Formal proof development. URL: `https://isa-afp.org/entries/Pluennecke_Ruzsa_Inequality.html`.
10. Melvyn B. Nathanson. *Additive Number Theory: The Classical Bases.* Springer-Verlag New York, 1996.
11. Tobias Nipkow, Markus Wenzel, and Lawrence C. Paulson. *Isabelle/HOL, A Proof Assistant for Higher-Order Logic.* Springer-Verlag Berlin Heidelberg, 2002. Updated online tutorial on `https://isabelle.in.tum.de/dist/Isabelle/doc/tutorial.pdf`.