Infinite abelian groups

Mihai Prunescu (* 1967)

For infinite abelian groups $G = \langle A, +, 0 \rangle$

$$\mathbf{P}_G \neq \mathbf{NP}_G$$

Infinite abelian groups

After Prunescu, JSL 2002

Theorem 1 (Bourgarde; Hemmerling and Gassner; Prunescu)
Let $G = (A, +_A, 0_A)$ be an infinite abelian group. Then $\mathbf{P}_G \neq \mathbf{NP}_G$.

This generalizes K. Meer's Theorem $\mathbf{P}_{lin} \neq \mathbf{NP}_{lin}$ for the additive group of $\mathbb{R}$ stated in Lecture 1.

For the ordered abelian group of the reals $\mathbb{R}_{ovs}$,
considered as an ordered vector space (ovs) over $\mathbb{R}$ we have

Theorem 2 (H. Fournier and P. Koiran 2001)
$\mathbf{P}_{ovs} = \mathbf{NP}_{ovs}$ *iff* $\mathbf{P}/poly = \mathbf{NP}/poly$,
resp. $\mathbf{P}^0_{ovs} = \mathbf{NP}^0_{ovs}$ *iff* $\mathbf{P} = \mathbf{NP}$, *for the parameter-free case.*

We shall read Prunescu's proof carefully to see why

it does not work in the ordered case.

The Nullsack problem

We call the problem $NS_G \subseteq G^\infty$ below the **Nullsack** problem:

$$NS_G = \{(x_1, \ldots, x_n) : n \in \mathbb{N} \text{ and } \exists J \neq \emptyset, J \subseteq [n] \text{ with } \sum_{j \in J} x_j = 0\}$$

- $NS_G \in \mathbf{NP}_G$ with boolean guesses and parameter-free.
- NS_G is computable in exponential time deterministically.

Fundamental theorems on abelian groups

AG-1: Every finitely generated abelian group G is isomorphic to

$$\mathbb{Z}^n \oplus \mathbb{Z}_{q_1} \oplus \ldots \oplus \mathbb{Z}_{q_t}$$

where n is its rank and $q_s, s \leq t$ are powers of primes.

AG-2: G is torsion-free if $t = 0$.

AG-3: F.W. Levi (1942):
An abelian group is orderable iff it is torsion-free.

AG-4: O. Hölder:
Every archimedian abelian ordered group is an ordered subgroup of the reals $\langle \mathbb{R}, +_R, <_R, 0_R, \rangle$.

Prüfer's theorems on abelian groups

Ernst Paul Heinz Prüfer (1896–1934)

PT-1: Every finite abelian group is isomorphic to the direct sum of cyclic gropus of prime order.

PT-2: E. Prüfer: An abelian group of bounded exponent is isomorphic to a direct sum of cyclic groups.

PT-3: Let G be infinite abelian group of bounded exponent.
There is a prime number p, such that there infinitely many elements on G of order p.

p-elementary abelian groups

- Let $\mathbb{H}_p = \bigoplus_{i \in \mathbb{N}} \mathbb{Z}_p$, where the elements are infinite sequences of elements of $\mathbb{Z}_p$ where all but finitely many are 0.
- $\mathbb{H}_p = \bigoplus_{i \in \mathbb{N}} \mathbb{Z}_p$ is an infinite dimensional, countable vector space over the field $GF(p)$, the Galois field of order p.
- Let $\mathcal{H} = \{\mathbb{Z}\} \cup \{\mathbb{H}_p : p \text{ a prime}\}$.
- the groups $\mathbb{H}_p$ are **not finitely generated**.

Prunescu's Theorem: For G an abelian group $\mathbf{P}_G \neq \mathbf{NP}_G$.

Step 1

The following was proved by K. Meer for the additive group on $\mathbb{R}$, and by B. Poizat for $\mathbb{H}_2$.

We first generalize this to groups in $\mathcal{H}$:

Proposition 3 (M. Prunescu)
Let $H \in \mathcal{H}$. Then $NS_H \notin \mathbf{P}_H$, hence $\mathbf{P}_H \neq \mathbf{NP}_H$.

Proof of $NS_H \notin \mathbf{P}_H$, I

- Let $m, n \in \mathbb{N}$ and $m, n \geq 1$, and $\bar{a} \in \{0,1\}^n$, $\bar{b}_1, \ldots, \bar{b}_m \in \mathbb{Z}^n$.
- The system

$$\begin{aligned} \bar{a} \cdot \bar{x} &= 0 \\ \bar{b}_1 \cdot \bar{x} &\neq 0 \\ &\vdots \\ \bar{b}_m \cdot \bar{x} &\neq 0 \end{aligned} \tag{1}$$

  has infinitely many solutions in H^n, provided that no $\bar{b}_i$ is a multiple of $\bar{a}$, and in case that $H = \mathbb{H}_p$, no inequation reduces to $0 \neq 0$ modulo p.

Proof of $NS_H \notin \mathbf{P}_H$, II

- Assume NS_H can be solved deterministically in polynomial time $p(n)$.
- Choose n such that $2^n - 1 > p(n)$.
- Using that the system (1) has infinitely many solutions, we construct $Y, N \in H^n$ such that $Y \in NS_H, N \notin NS_H$, but both traverse the same set of $< p(n)$ non-trivial tests negatively.
- Thus we reach a contradiction.

Q.E.D.

What happens here in the case of **ordered abelian groups**?

Strategy for the proof of $NS_G \notin \mathbf{P}_G$, for any abelian group G.

We proceed as follows:

- We look at **ultraproducts** of G.
- We show that every (non-trivial) ultrapower G^* of G is elementarily equivalent to G.

Lemma 4

- *We show that every (non-trivial) ultrapower G^* of G contains both G and some $H \in \mathcal{H}$, such that $G \cap H = \{0\}$.*
- Then we show that $NS_{G^*} \notin \mathbf{P}_{G^*}$.
- Using that $G^* \equiv G$ we conclude that $NS_G \notin \mathbf{P}_G$.

Short course on ultraproducts

More details on the blackboard.

(i) Filters and ultrafilters.

(ii) Non-principal ultrafilters.

(iii) Ultraproducts and ultrapowers.

(iv) Proof of Lemma 4.

Filters and ultrafilters

Let I be an infinite set.

Intuitively, a filter $\mathcal{F}$ is a collection of large subsets of I.

A filter $\mathcal{F}$ is a family of subsets of I such that

1. The empty set $\emptyset$ is not an element of $\mathcal{F}$.

2. If A and B are subsets of I, A is a subset of B, and A is an element of $\mathcal{F}$, then B is also an element of $\mathcal{F}$.

3. If A and B are elements of I, then so is the intersection of A and B.

$\mathcal{F}$ is an ultrafilter if additionally

4. If A is a subset of I, then either A or $I - A$ is an element of $\mathcal{F}$.

Properties 1 and 3 imply that A and $I - A$ cannot both be elements of $\mathcal{F}$.

Examples of filters and ultrafilters, I.

Let $I = \mathbb{N}$.

- Let $A \subseteq \mathbb{N}$. $\mathcal{F}_A = \{B \subseteq \mathbb{N} : A \subseteq B\}$.
  $\mathcal{F}_A$ is an ultrafilter.

- A filter $\mathcal{F}$ on a set I is principal if it is of the form $\mathcal{F}_A = \{B \subseteq \mathbb{N} : A \subseteq B\}$. for some subset $A \subseteq I$.

  Every principal filter is an ultrafilter.

- $\mathcal{F}_1$ be the family of co-finite sets.
  $\mathcal{F}_1$ is a non-principal filter but not an ultrafilter.
  Neither the set of even numbers nor the set of odd numbers is in $\mathcal{F}_1$.

Examples of filters and ultrafilters, II

Let $I = \mathbb{R}$ and

- $\mathcal{F}_2$ be the set of uncountable sets.
- $\mathcal{F}_3$ be the set of co-countable sets.
- $\mathcal{F}_4$ be the set of dense subsets of $\mathbb{R}$.

Discuss the filter properties of $\mathcal{F}_i$ for $i = 2, 3, 4$.

Discuss ultrafilters on finite sets I.

Ultraproducts and ultrapowers

Let I be set, serving as an index set,
and $\mathcal{F}$ be a non-principal ultrafilter on I.

Let $\mathfrak{A}_i : i \in I$ a family of τ-structures.

- $\mathfrak{A} = \prod_{i \in I} \mathfrak{A}_i$ is the cartesian product of these structures.
- For $\bar{a}, \bar{b}$ we define $\bar{a} \sim_{\mathcal{F}} \bar{b}$ iff $\{i \in I : a_i = b_i\} \in \mathcal{F}$.
- The ultraproduct $\prod_{i \in I} \mathfrak{A}_i / \mathcal{F}$ is the quotient structure $\mathfrak{A} / \sim_{\mathcal{F}}$.
- In case all the structures $\mathfrak{A}_i$ are the same
  we speak of the ultrapower $\prod_I \mathfrak{A} / \mathcal{F}$.

The Ultrafilter Theorem

Theorem 5
Every filter $\mathcal{F}$ over a set I is contained in some ultrafilter $\mathcal{U}$ over I.

Proof: We use the well-ordering theorem, that every set can be well-ordered.

Let $U_\alpha : \alpha < \beta$ be a well-ordering of the powerset of I.

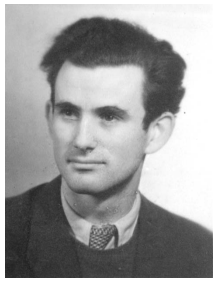
We put $\mathcal{F}_0 = \mathcal{F}$. For each $0 < \alpha < \beta$ we check whether $U_\alpha \in \mathcal{F}_\alpha$ or $I - U_\alpha \in \mathcal{F}_\alpha$.

If yes, we put $\mathcal{F}_{\alpha^+} = \mathcal{F}_\alpha$.

If no, we put $\mathcal{F}_{\alpha^+} = \mathcal{F}_\alpha[U_\alpha]$, which is the smallest filter containing $\mathcal{F}_\alpha$ and U_α.

If $\delta < \beta$ is a limit ordinal, we put $\mathcal{F}_\delta = \bigcup_{\alpha<\delta} \mathcal{F}_\alpha$.

It is now easy to check that $\mathcal{U} = \mathcal{F}_\beta$ is an ultrafilter. Q.E.D.



Łos' Theorem

J. Łos, 1920-1998

Theorem 6 (Fundamental Theorem of Ultraproducts)

Let $\prod_{i\in I}\mathfrak{A}_i/\mathcal{F}$ *be an ultraproduct of* τ*-structures* $\mathfrak{A}_i : i \in I$*, and* $\phi(x_1,\ldots,x_n) \in \mathsf{FOL}(\tau)$ *be a first order formula. Let* $\bar{a}_j : j \in [n]$*.*

$$\prod_{i\in I}\mathfrak{A}_i/\mathcal{F} \models \phi(\bar{a}_1,\ldots,\bar{a}_n)$$

iff

$$\{i \in I : \mathfrak{A}_i \models \phi(a_{i,1},\ldots,a_{i,n})\} \in \mathcal{F}$$

The proof is by induction.

What we need for Prunescu's Theorem

Let $\mathfrak{A}$ be a τ-structure.

- Then $\mathfrak{A} \equiv \prod_I \mathfrak{A}/\mathcal{F}$.
  In particular, this holds for $\mathfrak{A} = G$, an abelian group.

Let G be an abelian group,and $G^* = \prod_I \mathfrak{A}/\mathcal{F}$ an ultrapower of G.

- Then G^* contains a group G' which is an isomorphic copy of G.

  We map $a \in G$ into the constant sequence $a_i = a$.

- Then G^* contains an isomorphic copy of H
  for some $H \in \mathcal{H}$ with $H \cap G = \{0\}$.

  Let $\bar{a}$ consist of infinitely many different coordinates a_i.
  If the a_i's have unbounded order, we take the H to be the subgroup of G^* generated by $\bar{a}$, which is isomorphic to $\mathbb{Z}$ and 0 is the only element also in G'.

  If all the a_i's have order bounded by m, we use Prüfer's Theorem.

Outline of the ESSLLI-course given by

J.A. Makowsky (Haifa) and K. Meer (Cottbus)

LECTURE 1 (JAM): Introduction INTRO (5 slides)
Turing machines over relational structures, NEWBSS, (19 slides)
Short quantifier elimination. SHORTQE (16 slides)

LECTURE 2 (JAM): Introduction to quantifier elimination QE (26 slides)
Fields, rings and other structures TABLE (incomplete, 20 slides)

LECTURE 3 (JAM): Computing with the reals: Removing order or multiplication;
Adding `Fortran`-libraries. FORTRAN (24 slides)
Comparing Poizat's Theorem with descriptive complexity FAGIN (20 slides)

LECTURE 4 (KM): Inside $\mathbf{NP}_{\mathbb{R}}$ and analogues to Ladner's Theorem, Meer-1 (149 slides)

LECTURE 5 (KM): PCP-Theorem over $\mathbb{R}$, Meer-2 (139 slides)

ADDITIONAL MATERIAL see next slide.

Additional material for the ESSLLI-course

LECTURE 6 (JAM): Quantifier elimination in algebraically closed fields, ACF-0 (21 slides)
By JAM after Kreisel and Krivine.

LECTURE 7 (JAM): $\mathbf{P}_G \neq \mathbf{NP}_G$ for all abelian groups. ABELIAN (18 slides)
By JAM After M. Prunescu

LECTURE 8 (JAM): $\mathbf{P}_G \neq \mathbf{NP}_G$ for all boolean algebras. BOOLEAN (23 slides)
By I. Bentov after M. Prunescu

LECTURE 9 (JAM): $\mathbf{P}_G \neq \mathbf{NP}_G$ for all real matrix rings. MATRIX (70 slides)
By N. Labai after A. Rybalov