A model-theoretic proof for $P \neq NP$ over all infinite abelian groups

Mihai Prunescu *

Abstract

We give a model-theoretic proof of the fact that for all infinite Abelian groups $P \neq NP$ in the sense of binary nondeterminism. This result has been announced 1994 by Christine Gaßner.

Key Words: BSS-model, $P \neq NP$, abelian group, ultraproduct.

A.M.S.-Classification: 03C60.

Introduction: The result proven in this note was announced in a private communication hold by Christine Gaßner in 1994 at the University of Greifswald. When this note was in preparation, the result appeared also in a preprint of Menard Bourgade concerning the polynomial hierarchy over infinite abelian groups. All proofs known so far are complicated and contain a lot of calculations. We will show here a uniform model-theoretic proof.

Our work is compatible with approaches did independently by Poizat [P] and Hemmerling [H] in order to generalize the framework of Blum, Shub and Smale [BSS], [BCSS].

Problems: Given an infinite abelian group $G$, we call input over $G$ a finite non-empty sequence of elements of $G$. Let $G^\infty$ be the set of all inputs. A problem $\Pi$ over $G$ is any set of inputs ($\Pi \subset G^\infty$). A $G$-machine is a computation system given by a finite description and able to work out inputs of arbitrary length according to a program. The length of an input is the measure of its (algebraic) complexity. By polynomial time we mean that the time of computation has at most a polynomial increment rate in the length of the input.

Nondeterminism: In the binary (called also boolean -, ramification -, or simply first kind of -) nondeterminism situations in which the machine can continue the computation in two different ways are allowed. The second kind of nondeterministic machines have guess instructions, assigning to some register any value picked up arbitrarily from the group. If one algebraic structure contains at least

*Universität Greifswald, Germany and IMAR, Romania. The author thanks Christine Gaßner and Günter Asser for their work concerning this problem. See [A].
two elements and possess equality one can simulate any binary nondeterministic machine using a guess nondeterministic one.

Let $K$ be an abstract set of constants. We consider an interpretation $(k^G \in G)_{k \in K}$ of $K$ in $G$ and the structure $(G; (k^G)_{k \in K}; +, -, =)$.

**Complexity:** If we interpret the structure above as a model of computation, we can define the class $P_G$ of problems decided by deterministic machines in polynomial time and the classes $N_i P_G$ ($i \in \{1, 2\}$) of problems recognized by the eventually halting of nondeterministic machines of the $i$-th kind in polynomial time. As we have seen, $P_G \subseteq N_1 P_G \subseteq N_2 P_G$.

**Nullsack:** We call Nullsack the following problem $\Sigma_G \subset G^\infty$:

$$\Sigma_G := \{(x_1, \ldots, x_n) \mid n \in \mathbb{N} \text{ and } \exists J \neq \emptyset; J \subseteq \{1, \ldots, n\} \text{ so that } \sum_{j \in J} x_j = 0\}.$$ 

$\Sigma_G \in N_1 P_G$ parameter-free. We will show that $\Sigma_G \notin P_G$.

**Lemma 1:** Assume that $G_1$ and $G_2$ are infinite abelian groups such that for a given set of constants $K$ and fixed interpretations $(k^{G_1})_{k \in K}$ of the constants, the resulting structures $(G_i; (k^{G_i})_{k \in K}; +, -, =)$ are elementary equivalent. Then $\Sigma_{G_1} \in P_{G_1}$ iff $\Sigma_{G_2} \in P_{G_2}$.

**Proof:** Assume that $\Sigma_{G_1} \in P_{G_1}$. There is a deterministic machine which decides $\Sigma_{G_1}$ in a time given by a polynomial $\text{pol}$ in the length $n$ of the input. All the possible paths of computation have a length $\leq \text{pol}(n)$, just some of them end with a positive answer. Any test performed along such a path has the form ”Is $\vec{a} \cdot \vec{x} = c$?” where all $\vec{a} \in \mathbb{Z}^n$ and $c$ is a linear combination of constants $(k^{G_1})_{k \in K}$. We denote by $\psi_n$ the universal proposition which states that for all $n$-tuple of elements of the group, being a solution of the problem $\Sigma$ is equivalent to traversing an accepting path. The left hand side of this equivalence should be a disjunction taken over all accepting paths consisting of conjunctions of $\leq \text{pol}(n)$ (negated, if necessary) tests along a given path.

If $\Sigma_{G_1} \in P_{G_1}$, then for all $n \in \mathbb{N}$, $G_1 \models \psi_n$. So also $G_2 \models \psi_n$ for all $n$, thus the machine obtained by substituting the parameters $(k^{G_1})_{k \in K}$ with corresponding parameters $(k^{G_2})_{k \in K}$ will decide $\Sigma_{G_2}$ in polynomial time.

This proof does not use the fact that the sequence $(\psi_n)$ is recursive. Thus Lemma 1 is also true for the non-uniform computation class $\mathbb{P}_G$.

**Definition:** Let $p \in \mathbb{N}$ be a prime. We recall the notation $\mathbb{Z}_p$ for the unique group with $p$ elements. Let $\mathbb{H}_p$ be the $p$-elementary group:

$$\mathbb{H}_p := \bigoplus_\omega \mathbb{Z}_p.$$
The group \( \mathbb{H}_p \) is an infinitely dimensional vector space over the field \( \mathbb{F}_p \) with \( p \) elements. We denote by \( \mathcal{H} \) the following set of infinite abelian groups:

\[ \mathcal{H} := \{ \mathbb{Z}, \mathbb{H}_2, \mathbb{H}_3, \mathbb{H}_5, \ldots, \mathbb{H}_p, \ldots \} \]

The following result was proved by Klaus Meer [M] for the additive group of \( \mathbb{R} \) and by Bruno Poizat [P] for the group \( \mathbb{H}_2 \):

**Lemma 2:** Let \( H \in \mathcal{H} \) be a group. If we consider the complexity classes defined according to the structure \((H; 0; +, -; =)\) then \( \Sigma_H \notin P_H \). Consequently, \( P_H \neq N_1 P_H \).

**Proof:** For \( m, n \geq 1 \) we fix arbitrary numerical vectors \( \vec{a} \in \{0, 1\}^n, \vec{b}_1, \ldots, \vec{b}_m \in \mathbb{Z}^n \setminus \vec{0} \). For all \( H \in \mathcal{H} \), if no \( \vec{b}_i \) is a multiple of \( \vec{a} \) and, in case that \( H = \mathbb{H}_p \), no unequation reduces to 0 \( \neq 0 \) because of the characteristic \( p \), then the system:

\[ \vec{a} \cdot \vec{x} = 0, \vec{b}_1 \cdot \vec{x} \neq 0, \ldots, \vec{b}_m \cdot \vec{x} \neq 0. \]

has infinitely many solutions \( \vec{x} \in H^n \).

If we suppose that a deterministic machine decides \( \Sigma_H \) in a polynomial time \( pol(n) \), we choose an \( n \) such that \( 2^n - 1 > pol(n) \) and we use the observation above for constructing inputs \( Y \) and \( N \) of length \( n \) with the following properties:

\( Y \in \Sigma_H, N \notin \Sigma_H \), but both inputs traverse the unique computation path defined by a sequence of \( \leq pol(n) \) negative answers to all non-trivial tests. This is a contradiction. \( \square \)

**Lemma 3:** Let \( G \) be an infinite abelian group and \( G^* \) its classical ultrapower. There is a group \( H \in \mathcal{H} \) and an embedding of \( H \) in \( G^* \) which makes \( H \leq G^* \) so that \( H \cap G = \{0\} \).

**Proof:** If \( G \) contains an element of infinite order or if the set of orders for elements in \( G \) is unbounded, then \( G^* \) contains a non-standard element of infinite order. This element generates a subgroup of \( G^* \) that is isomorphic with \( \mathbb{Z} \) and has the desired property. If all orders are finite and their set is also finite, a theorem of Prüfer implies that there is a prime number \( p \) such that the set of all elements of order \( p \) is infinite. Then there are infinitely many non-standard elements of order \( p \) and we can find a copy of \( \mathbb{H}_p \) whose non-zero elements are such non-standard elements. \( \square \)

**Main result:** If \( G \) is an infinite abelian group and the class \( P_G \) is defined according to the structure

\[ (G; (g)_{g \in G}; +, -; =), \]

then the problem \( \Sigma_G \in N_1 P_G \setminus P_G \). Consequently is \( P_G \neq N_1 P_G \).

**Proof:** Let \( G^* \) be the classical ultrapower of \( G \). We define \( P_{G^*} \) to be the polynomial class over \( (G^*; (g)_{g \in G}; +, -; =) \). We prove that \( \Sigma_{G^*} \notin P_{G^*} \) and we use the elementary equivalence with \( (G; (g)_{g \in G}; +, -; =) \) to get \( \Sigma_G \notin P_G \).
We assume for the sake of contradiction that $\Sigma_{G^*} \in P_{G^*}$. Thus there is a $G^*$-machine $M$ with parameters in $G$ and a polynomial $pol$ such that for inputs $I$ of length $n$, $M$ decides if $I \in \Sigma_{G^*}$ in a time $\leq pol(n)$.

There is a $H \in \mathcal{H}$ such that $H \leq G^*$ and $H \cap G = \{0\}$. Of course $\Sigma_H \subset \Sigma_{G^*}$.

Any test done by $M$ looks like "Is $\vec{a} \cdot \vec{x} = c$?" with $\vec{a} \in \mathbb{Z}^n$, $\vec{x} \in H^n$ and $c \in G$.

Because $H \cap G = \{0\}$, one has for inputs $I \in H^\infty$:

$$\vec{a} \cdot \vec{x} = c \iff \vec{a} \cdot \vec{x} = 0 \text{ and } c = 0;$$
$$\vec{a} \cdot \vec{x} \neq c \iff \vec{a} \cdot \vec{x} \neq 0 \text{ or } c \neq 0.$$

Let $M_0$ be the machine obtained from $M$ by substituting all parameters occurring in the finite description of $M$ by 0. For the inputs $I \in H^\infty$, $M_0$ works like $M$, thus it should decide $\Sigma_H$ in time $pol(n)$. This is a contradiction. \hfill \Box

**Corollary:** The stronger inequality $\mathbb{P}_G \neq N_1 \mathbb{P}_G$ is also true for all infinite abelian groups $G$.

**References**


