$P \neq NP$ für eine endliche Gruppe

Christine Gaßner

Inhalt

- Berechnungen über algebraischen Strukturen
- Das uniforme Berechnungsmodell und die Klassen P_G und NP_G für Gruppen G
- Die Bewegungsgruppe des Quadrates B_{2Q}
- Ein Problem in $NP_{B_{2Q}} \setminus P_{B_{2Q}}$

Probleme und Klassen

- Probleme:
  - Mengen von endlichen Folgen über einem Grundbereich.
  - Beispiele:

    A = $(A, \cup_{n\geq 1}\mathbb{R}^n)$ mit $A \subseteq \cup_{n\geq 1}\mathbb{R}^n$,

    B = $(B, \cup_{n\geq 1}\mathbb{N}^n)$ mit $B \subseteq \cup_{n\geq 1}\mathbb{N}^n$.

- Klassen von Problemen für eine Struktur Σ:
  - Mengen von Problemen.
  - Beispiele: P_Σ, NP_Σ, DNP_Σ.

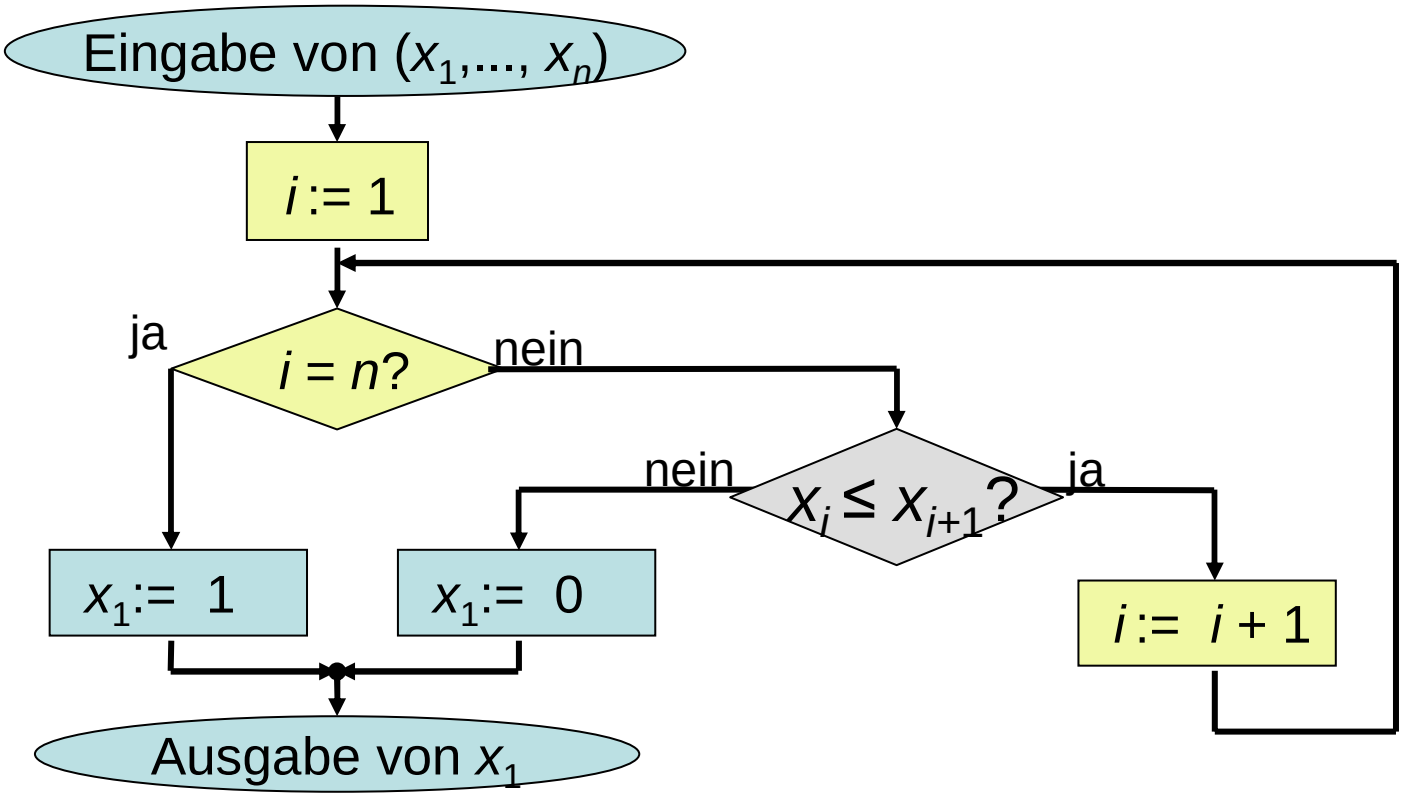
- P_Σ-NP_Σ-Problem: $P_\Sigma = NP_\Sigma$ oder $P_\Sigma \neq NP_\Sigma$?

Ein Problem (Beispiel)

Gegeben: Endliche Folgen von Zahlen $(x_1,..., x_n)$, $n \in \mathbb{N}^+$.

Problem: Menge der geordneten Folgen.

Entscheidbarkeit des Problems:



Eine Struktur

$$\Sigma = (S;\ \underbrace{c_1, \ldots, c_l}_{\text{Konstanten}};\ \underbrace{f_1, \ldots, f_n}_{\text{Operationen}};\ \underbrace{r_1, \ldots, r_m}_{\text{Relationen}})$$

nichtleere Trägermenge (Universum)

Beispiele:

- $(\{0, 1\}; 0, 1; ;\ =)$ ($\triangleq$ Turing-Maschine)
- $(\mathbb{R}; 0, 1;\ \cdot, +, -;\ \leq)$ ($\triangleq$ Blum-Shub-Smale-Modell)
- Gruppen $(G;\ e;\ \circ; =)$:
  - $(\mathbb{Z}; 0; +; =)$,
  - $(\mathbb{Q}; 1; \cdot; =)$,…

Das Berechnungsmodell für Σ

- Variablen (oder Register) für die Elemente der Struktur:

  $z_1,\ldots, z_n , z_{n+1},\ldots$

- Variablen (Indexregister) für natürliche Zahlen (Indizes, Adressen):

  $i_1,\ldots, i_k$

- Programme (Σ-Programme):

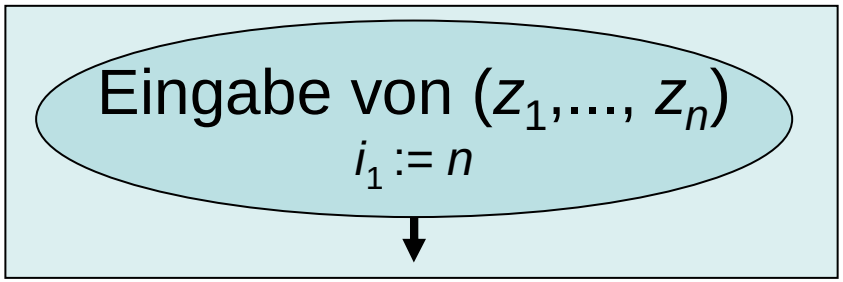
  1: Anweisung Nr.1;

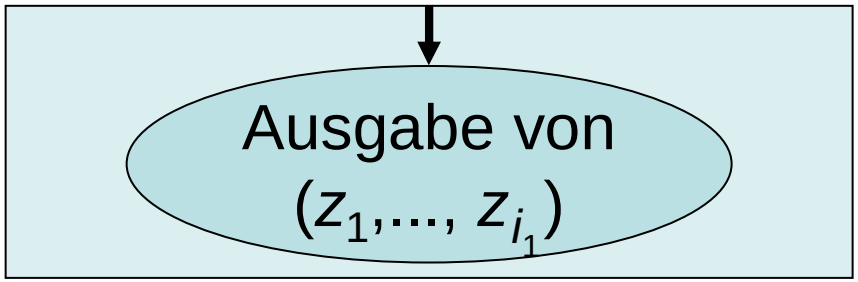
  …

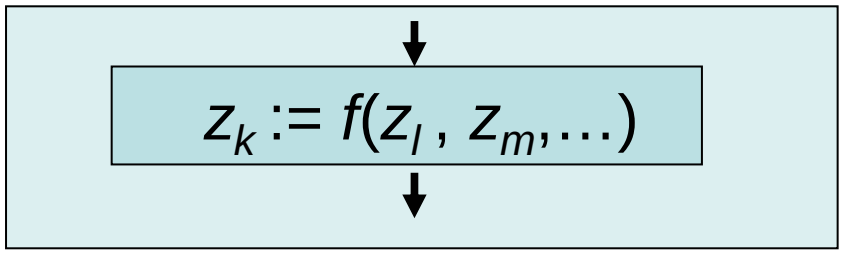
  m: Anweisung Nr. m.

  Programme können durch Flussdiagramme beschrieben werden.

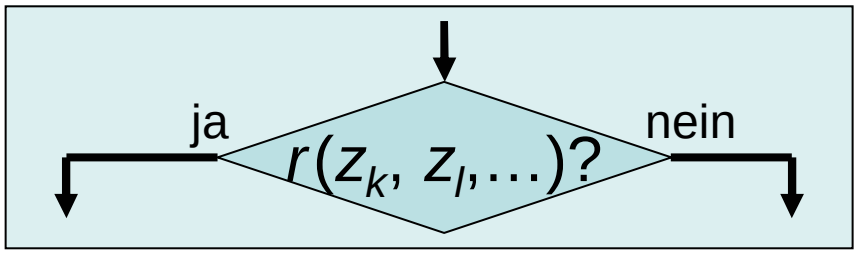
Die Anweisungen



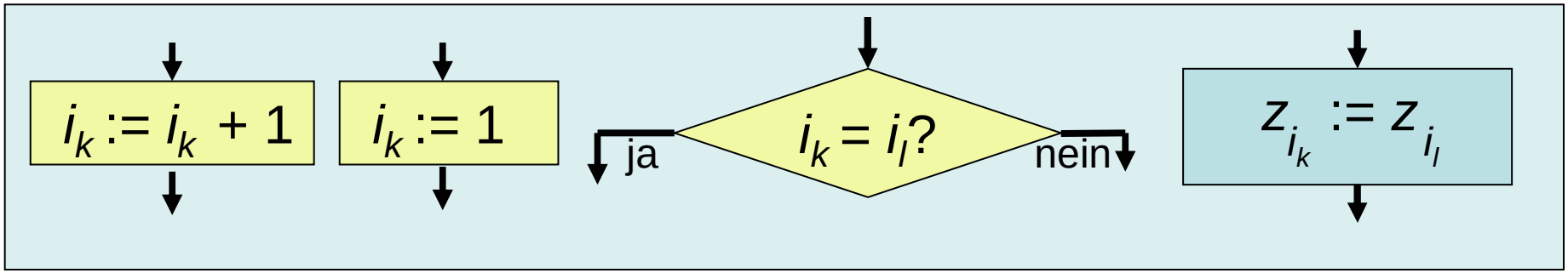




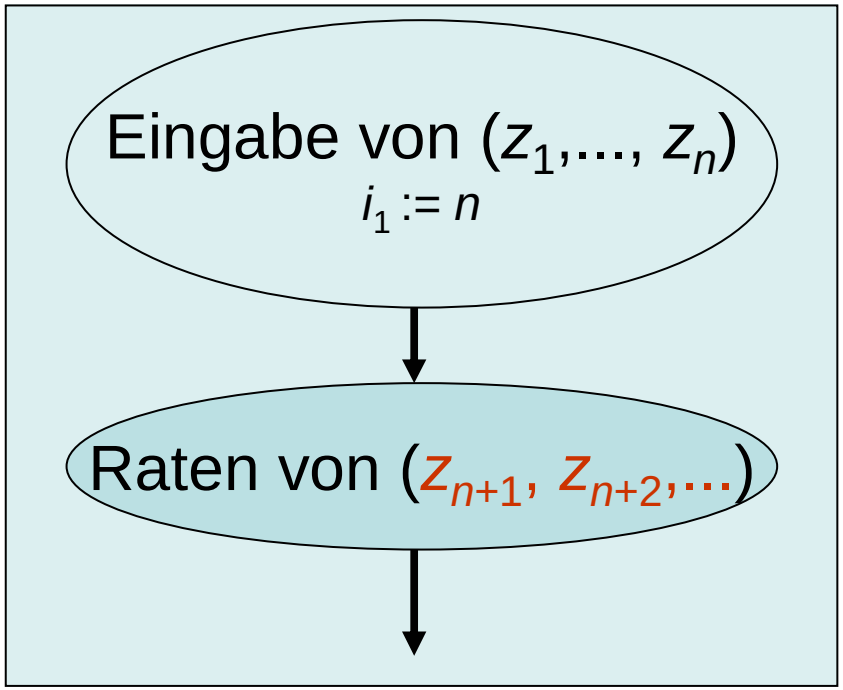
$z_k := f(z_l, z_m,\ldots)$; $z_k := c_m$;



if $r(z_k, z_l,\ldots)$ then goto m_1 else goto m_2 ;

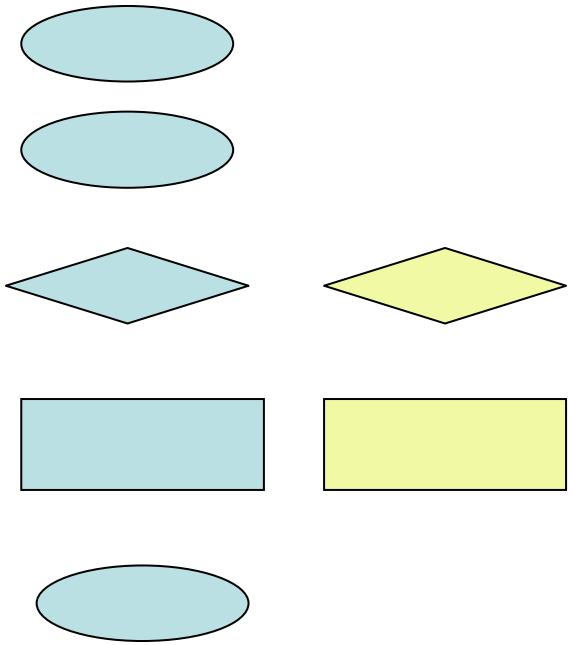


Das Raten – Nichtdeterministische Programme



Die Berechnungszeit für eine Anweisung
(für das uniforme Modell)

- Die Eingabe
- Das Raten
- 1 Anfrage (ein Test)
- 1 Berechnung
- Die Ausgabe



≙ 1 Berechnungseinheit

≙ 1 Berechnungsschritt

Entscheidbarkeit eines Problems für Gruppen $(G;\ e;\ \circ;=)$

- Problem: A= $(A, \cup_{n\geq 1} G^n)$, $A \subseteq \cup_{n\geq 1} G^n$.

Dieses Problem ist *entscheidbar*, wenn es zwei deterministische Programme M_1 und M_2 gibt, so dass

– M_1 für alle Eingaben aus A hält (und e ausgibt)

und

– M_2 für alle Eingaben aus $\cup_{n\geq 1} G^n \setminus A$ hält (und e ausgibt).

Nichtdeterministische Erkennbarkeit eines Problems

- Problem: A= $(A, \cup_{n\geq 1} G^n)$, $A \subseteq \cup_{n\geq 1} G^n$.

Dieses Problem wird mit Hilfe eines *nichtdeterministischen* Programms M *erkannt*, wenn es

für jede Eingabe $(x_1,\ldots, x_n)$ aus A

ein geratenes Tupel $(y_1,\ldots, y_m) \in \cup_{n\geq 1} G^n$

gibt, so dass M für $(x_1,\ldots, x_n, y_1,\ldots, y_m)$ die Konstante e ausgibt (beziehungsweise hält).

Entscheidbarkeit in Polynomialzeit
(für das uniforme Modell)

- Problem: A= $(A, \cup_{n\geq 1} G^n)$, $A \subseteq \cup_{n\geq 1} G^n$.

A ist *in Polynomialzeit* entscheidbar,

wenn für jede n-dimensionale Eingabe aus G^n

die Ausgabe von e (das Halten)
für M_1 bez. M_2

nach höchstens $p_A(n)$ Berechnungsschritten

für ein Polynom p_A (nur abhängig von A) erfolgt.

Nichtdeterministische Erkennbarkeit in Polynomialzeit (für das uniforme Modell)

- Problem: A= $(A, \cup_{n\geq 1} G^n)$, $A \subseteq \cup_{n\geq 1} G^n$.

A ist *in Polynomialzeit* nichtdeterministisch erkennbar,

wenn für jede n-dimensionale Eingabe aus $A \cap G^n$

eine Ausgabe von e
(das Halten für eine Kombination von Ratewerten)

nach höchstens $p_A(n)$ Berechnungsschritten

für ein Polynom p_A (nur abhängig von A) erfolgt.

Die Klassen P_G und NP_G für eine Gruppe G

P_G

= Klasse der Probleme, die in Polynomialzeit mit Hilfe von deterministischen G-Programmen entscheidbar sind.

NP_G

= Klasse der Probleme, die in Polynomialzeit mit Hilfe von nichtdeterministischen G-Programmen nichtdeterministisch erkennbar sind.

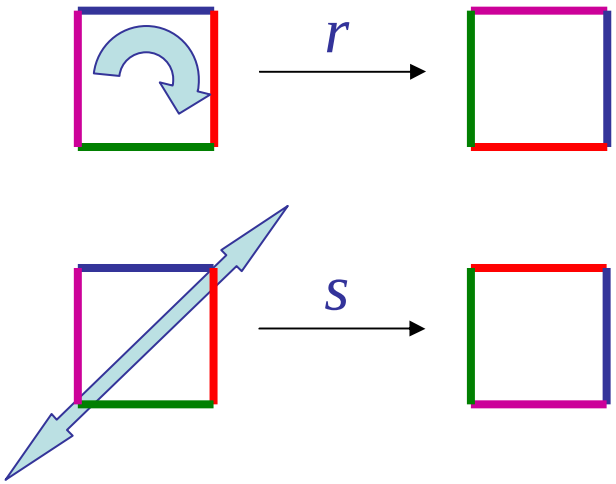
Die Bewegungsgruppe des Quadrates (Die Diedergruppe)

$$B_{2Q} = (\{e, r, r^2, r^3, s, rs, r^2s, r^3s\}, \circ)$$

erzeugt durch

eine Drehung um 90° und

eine Spiegelung



Die Bewegungsgruppe des Quadrates (Gruppentafel)

$x \circ y$ (y / x)	e	r	$p=r^2$	$q=r^3$	s	$u=rs$	$v=r^2s$	$w=r^3s$
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
$p=r^2$	r^2	r^3	e	r	r^2s	r^3s	s	rs
$q=r^3$	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
$u=rs$	rs	s	r^3s	r^2s	r	e	r^3	r^2
$v=r^2s$	r^2s	rs	s	r^3s	r^2	r	e	r^3
$w=r^3s$	r^3s	r^2s	rs	s	r^3	r^2	r	e

Die Bewegungsgruppe des Quadrates

$x \circ y$ (y \ x)	e O2	r	$p=r^2$ O2	$q=r^3$	s O2	$u=rs$ O2	$v=r^2s$ O2	$w=r^3s$ O2
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
$p=r^2$	r^2	r^3	e	r	r^2s	r^3s	s	rs
$q=r^3$	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
$u=rs$	rs	s	r^3s	r^2s	r	e	r^3	r^2
$v=r^2s$	r^2s	rs	s	r^3s	r^2	r	e	r^3
$w=r^3s$	r^3s	r^2s	rs	s	r^3	r^2	r	e

Die Elemente der Ordnung 2.

Die Bewegungsgruppe des Quadrates

$x \circ y$ (y / x)	e O2, Z	r	$p=r^2$ O2, Z	$q=r^3$	s O2	$u=rs$ O2	$v=r^2s$ O2	$w=r^3s$ O2
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
$p=r^2$	r^2	r^3	e	r	r^2s	r^3s	s	rs
$q=r^3$	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
$u=rs$	rs	s	r^3s	r^2s	r	e	r^3	r^2
$v=r^2s$	r^2s	rs	s	r^3s	r^2	r	e	r^3
$w=r^3s$	r^3s	r^2s	rs	s	r^3	r^2	r	e

Die Elemente der Ordnung 2. Das Zentrum $Z = \{e, p\}$.

Die Bewegungsgruppe des Quadrates

$x \circ y$ / y / x	e O2, Z	r K	$p=r^2$ O2, Z	$q=r^3$ K	s O2, K	$u=rs$ O2, K	$v=r^2s$ O2, K	$w=r^3s$ O2, K
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
$p=r^2$	r^2	r^3	e	r	r^2s	r^3s	s	rs
$q=r^3$	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r^3	r^2	r
$u=rs$	rs	s	r^3s	r^2s	r	e	r^3	r^2
$v=r^2s$	r^2s	rs	s	r^3s	r^2	r	e	r^3
$w=r^3s$	r^3s	r^2s	rs	s	r^3	r^2	r	e

Die Elemente der Ordnung 2. Das Zentrum $Z = \{e, p\}$. Das Komplement K von Z.

$NP_{B_{2Q}} \neq P_{B_{2Q}}$ (Ein Problem in $NP_{B_{2Q}} \setminus P_{B_{2Q}}$)

- $A = (A, \cup_{n \geq 1}(B_{2Q})^n)$

mit $A = \{(x_1, x_2, \ldots, x_n) \mid n \in \mathbb{N}^+ \;\&\; \exists y\,(y \circ x_1 \neq x_1 \circ y)\}$

$\triangleq$ x_1 gehört nicht zum Zentrum von B_{2Q},

d. h.

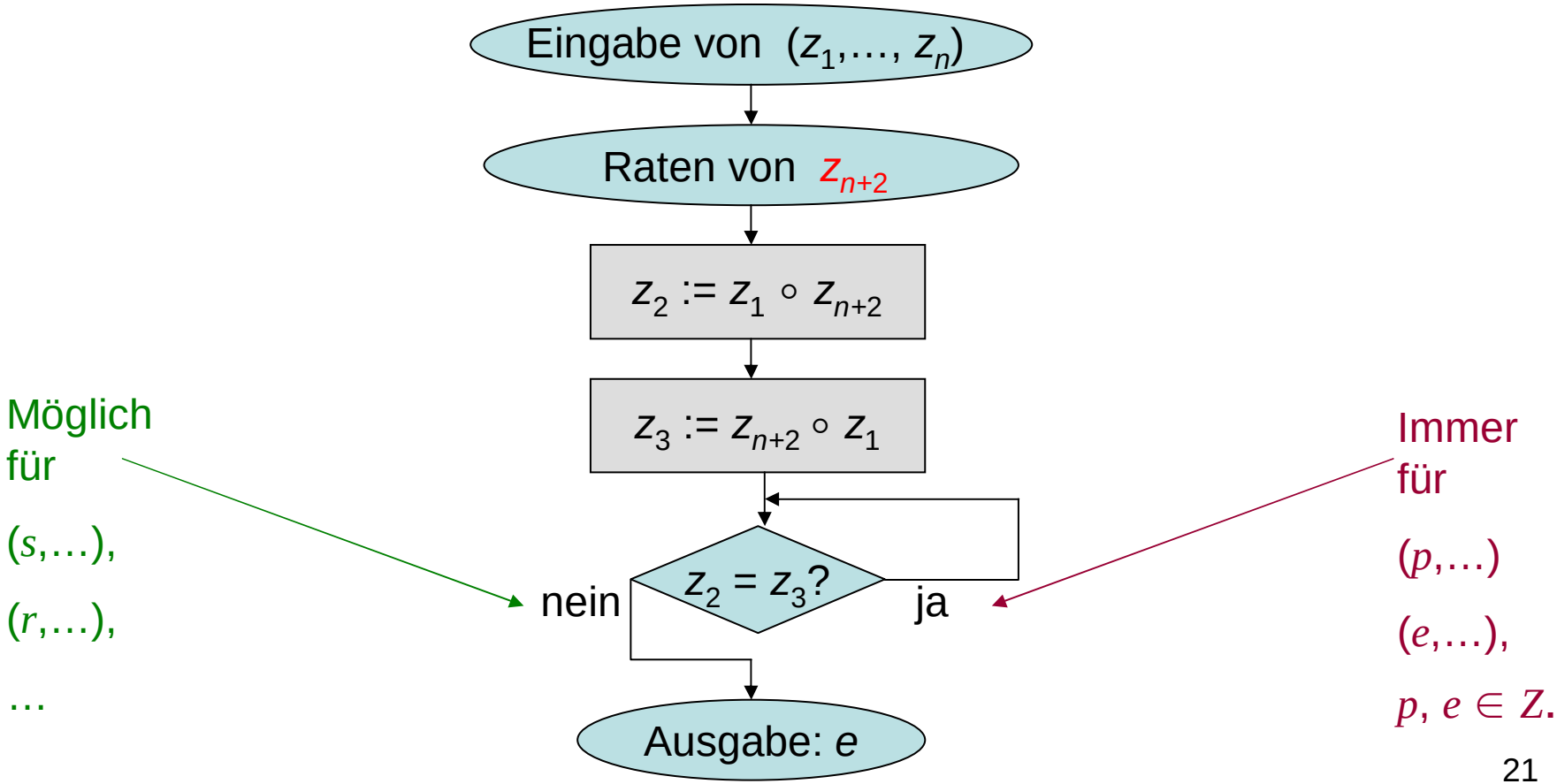
$K = \{r, q, s, u, v, w\} \Rightarrow (s, s, \ldots, s) \in A$

$Z = \{e, p\} \Rightarrow (p, p, \ldots, p) \notin A$

Elemente der Ordnung 2.

$A \in NP_{B_{2Q}}$

- $A = (A, \cup_{n \geq 1}(B_{2Q})^n)$ mit $A = \{(x_1, \ldots, x_n) \mid \exists y (y \circ x_1 \neq x_1 \circ y)\}$



$A \notin P_{B_{2Q}}$

- $A = (A, \cup_{n \geq 1}(B_{2Q})^n)$ mit $A = \{(x_1, x_2, \ldots, x_n) \mid \exists y(y \circ x_1 \neq x_1 \circ y)\}$,
- $n \in \mathbb{N}^+$.

Angenommen:

Es existiert B_{2Q}-Programm M, das für die Eingabe

$$(x_1, \ldots, x_1) \in (B_{2Q})^n$$

die Konstante e ausgibt, wenn $(x_1, \ldots, x_1) \in A$ gilt.

$A \notin P_{B_{2Q}}$

⇒ Alle Eingaben $(x_1,..., x_1)$ durchlaufen die gleichen Anweisungen von M, bis es zu einem Test kommt.

Der Test hat die Form

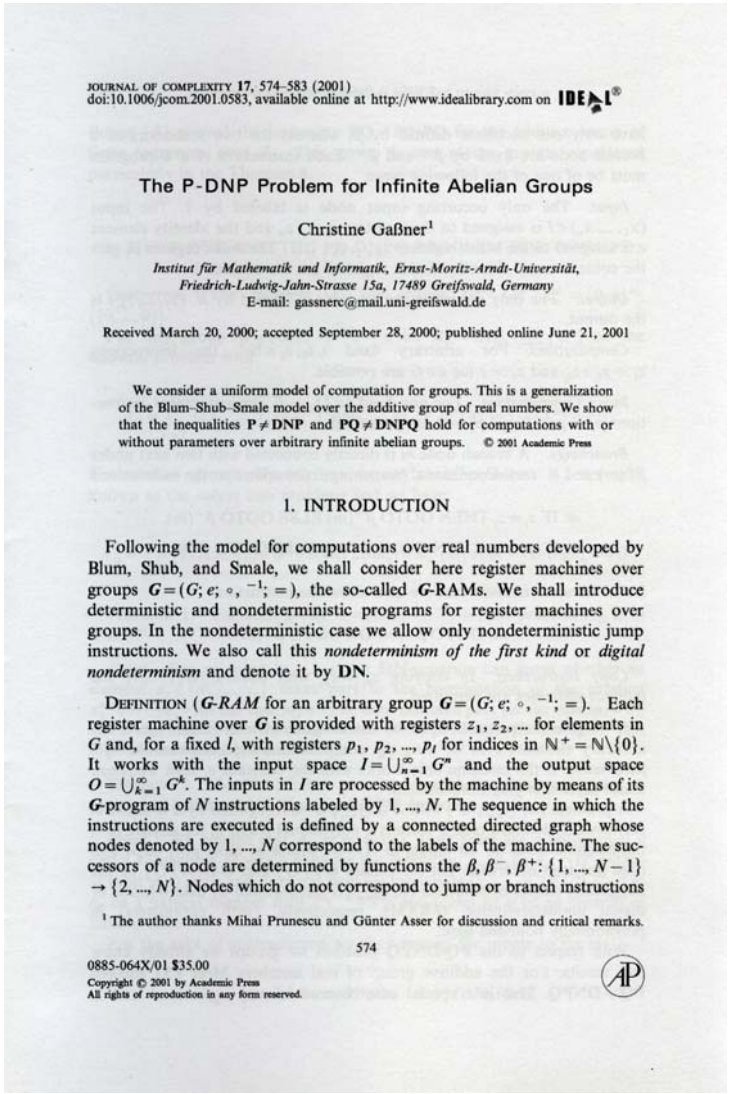
$$x_1{}^k = x_1{}^m.$$

⇒ Für alle Eingaben mit $x_1{}^2 = e$ erhalten wir das gleiche Testergebnis

- für den ersten Test,
- für alle weiteren Tests.

⇒ Wenn M für $(p,\ldots, p)$ die Konstante e ausgibt, so gibt M auch für $(s,\ldots, s)$ die Konstante e nach genauso vielen Schritten aus.

Einige weitere Ergebnisse



JOURNAL OF COMPLEXITY 17, 574–583 (2001)
doi:10.1006/jcom.2001.0583, available online at http://www.idealibrary.com on IDEAL®

The P-DNP Problem for Infinite Abelian Groups

Christine Gaßner[1]

Institut für Mathematik und Informatik, Ernst-Moritz-Arndt-Universität, Friedrich-Ludwig-Jahn-Strasse 15a, 17489 Greifswald, Germany
E-mail: gassnerc@mail.uni-greifswald.de

Received March 20, 2000; accepted September 28, 2000; published online June 21, 2001

We consider a uniform model of computation for groups. This is a generalization of the Blum–Shub–Smale model over the additive group of real numbers. We show that the inequalities **P** ≠ **DNP** and **PQ** ≠ **DNPQ** hold for computations with or without parameters over arbitrary infinite abelian groups.

1. INTRODUCTION

Following the model for computations over real numbers developed by Blum, Shub, and Smale, we shall consider here register machines over groups $G=(G; e; \circ, ^{-1}; =)$, the so-called *G*-RAMs. We shall introduce deterministic and nondeterministic programs for register machines over groups. In the nondeterministic case we allow only nondeterministic jump instructions. We also call this *nondeterminism of the first kind* or *digital nondeterminism* and denote it by **DN**.

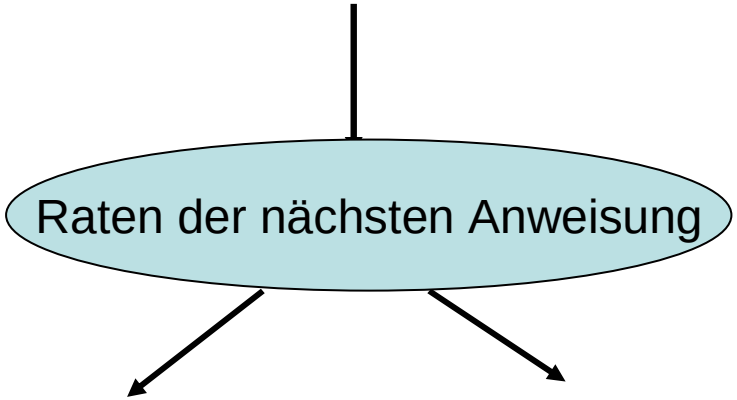
DEFINITION (*G-RAM* for an arbitrary group $G=(G; e; \circ, ^{-1}; =)$. Each register machine over *G* is provided with registers $z_1, z_2, \ldots$ for elements in *G* and, for a fixed *l*, with registers $p_1, p_2, \ldots, p_l$ for indices in $\mathbb{N}^+ = \mathbb{N}\backslash\{0\}$. It works with the input space $I=\bigcup_{n=1}^{\infty} G^n$ and the output space $O=\bigcup_{k=1}^{\infty} G^k$. The inputs in *I* are processed by the machine by means of its *G*-program of *N* instructions labeled by $1, \ldots, N$. The sequence in which the instructions are executed is defined by a connected directed graph whose nodes denoted by $1, \ldots, N$ correspond to the labels of the machine. The successors of a node are determined by functions the $\beta, \beta^-, \beta^+: \{1, \ldots, N-1\} \to \{2, \ldots, N\}$. Nodes which do not correspond to jump or branch instructions

[1] The author thanks Mihai Prunescu and Günter Asser for discussion and critical remarks.

0885-064X/01 $35.00

Für DNP_{Σ}:

- kein beliebiges Raten,
- nur digitales Raten:
  - von c_1 ($\triangleq 1$) und c_2 ($\triangleq 0$),
  - der nächsten Anweisung.



Einige weitere Ergebnisse

Ernst-Moritz-Arndt-Universität Greifswald

Preprint-Reihe Mathematik

A Structure of Finite Signature with Identity Relation and with P = NP – A Formal Proof with More Details

Christine Gaßner

Nr. 9/2005

Beratung: Prof. R. Schimming

Vielen Dank!