Polynomial Hierarchy, Betti Numbers and a real analogue of Toda's Theorem

Saugata Basu

Purdue/Georgia Tech

IIT Kharagpur, Jan 13, 2009

Outline

Outline

Outline

1. (Discrete) Polynomial Hierarchy
2. Blum-Shub-Smale Models of Computation
3. Algorithmic Semi-algebraic Geometry
4. Real Analogue of Toda's Theorem
5. Proof Idea

Outline

1. (Discrete) Polynomial Hierarchy
2. Blum-Shub-Smale Models of Computation
3. Algorithmic Semi-algebraic Geometry
4. Real Analogue of Toda's Theorem
5. Proof Idea

Outline

A quick primer of basic definitions and notation

- Initially let $k = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$.
- A *language* L is a set

$$\bigcup_{n>0} L_n, \quad L_n \subset k^n$$

(abusing notation a little we will identify L with the sequence $(L_n)_{n>0}$).

- A language

$$L = (L_n)_{n>0} \in \mathbf{P}$$

if there exists a Turing machine M (or equivalently a C program) that given $\mathbf{x} \in k^n$ decides whether $\mathbf{x} \in L_n$ or not in $n^{O(1)}$ time.

A quick primer of basic definitions and notation

- Initially let $k = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$.
- A *language* L is a set

$$\bigcup_{n>0} L_n, \quad L_n \subset k^n$$

(abusing notation a little we will identify L with the sequence $(L_n)_{n>0}$).

- A language

$$L = (L_n)_{n>0} \in \mathbf{P}$$

if there exists a Turing machine M (or equivalently a C program) that given $\mathbf{x} \in k^n$ decides whether $\mathbf{x} \in L_n$ or not in $n^{O(1)}$ time.

A quick primer of basic definitions and notation

- Initially let $k = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$.
- A *language* L is a set

$$\bigcup_{n>0} L_n, \quad L_n \subset k^n$$

(abusing notation a little we will identify L with the sequence $(L_n)_{n>0}$).

- A language

$$L = (L_n)_{n>0} \in \mathbf{P}$$

if there exists a Turing machine M (or equivalently a C program) that given $\mathbf{x} \in k^n$ decides whether $\mathbf{x} \in L_n$ or not in $n^{O(1)}$ time.

Primer (cont.)

- A language
$$L = (L_n)_{n>0} \in \mathbf{NP}$$
if there exists a language $L' = (L'_n)_{n>0} \in \mathbf{P}$ such that
$$\mathbf{x} \in L_n \iff (\exists \mathbf{y} \in k^{m(n)})\ \ (\mathbf{y}, \mathbf{x}) \in L'_{m+n}$$
where $m(n) = n^{O(1)}$ (such a $\mathbf{y}$ is usually called a "certificate" or a "witness" for $\mathbf{x}$).
- A language
$$L = (L_n)_{n>0} \in \mathbf{coNP}$$
if there exists a language $L' = (L'_n)_{n>0} \in \mathbf{P}$ such that
$$\mathbf{x} \in L_n \iff (\forall \mathbf{y} \in k^{m})\ \ (\mathbf{y}, \mathbf{x}) \in L'_{m+n}$$
where $m(n) = n^{O(1)}$.

Primer (cont.)

- A language
$$L = (L_n)_{n>0} \in \mathbf{NP}$$
if there exists a language $L' = (L'_n)_{n>0} \in \mathbf{P}$ such that
$$\mathbf{x} \in L_n \iff (\exists \mathbf{y} \in k^{m(n)}) \;\; (\mathbf{y}, \mathbf{x}) \in L'_{m+n}$$
where $m(n) = n^{O(1)}$ (such a $\mathbf{y}$ is usually called a "certificate" or a "witness" for $\mathbf{x}$).
- A language
$$L = (L_n)_{n>0} \in \mathbf{coNP}$$
if there exists a language $L' = (L'_n)_{n>0} \in \mathbf{P}$ such that
$$\mathbf{x} \in L_n \iff (\forall \mathbf{y} \in k^{m}) \;\; (\mathbf{y}, \mathbf{x}) \in L'_{m+n}$$
where $m(n) = n^{O(1)}$.

Discrete Polynomial Time Hierarchy– A Quick Reminder

A language

$$L = (L_n)_{n>0} \in \Sigma_\omega$$

if there exists a language $L' = (L'_n)_{n>0} \in \mathbf{P}$ such that

$$\mathbf{x} \in L_n$$
$$\Updownarrow$$
$$(Q_1 \mathbf{y}^1 \in k^{m_1})(Q_2 \mathbf{y}^2 \in k^{m_2}) \ldots (Q_\omega \mathbf{y}^\omega \in k^{m_\omega})$$
$$(\mathbf{y}^1, \ldots, \mathbf{y}^\omega, \mathbf{x}) \in L'_{m+n}$$

where $m(n) = m_1(n) + \cdots + m_\omega(n) = n^{O(1)}$ and for $1 \le i \le \omega$, $Q_i \in \{\exists, \forall\}$, and $Q_j \neq Q_{j+1}, 1 \le j < \omega$, $Q_1 = \exists$.

Discrete Polynomial Time Hierarchy– A Quick Reminder

A language

$$L = (L_n)_{n>0} \in \Sigma_\omega$$

if there exists a language $L' = (L'_n)_{n>0} \in \mathbf{P}$ such that

$$\mathbf{x} \in L_n$$

$$\Updownarrow$$

$$(Q_1 \mathbf{y}^1 \in k^{m_1})(Q_2 \mathbf{y}^2 \in k^{m_2}) \ldots (Q_\omega \mathbf{y}^\omega \in k^{m_\omega})$$
$$(\mathbf{y}^1, \ldots, \mathbf{y}^\omega, \mathbf{x}) \in L'_{m+n}$$

where $m(n) = m_1(n) + \cdots + m_\omega(n) = n^{O(1)}$ and for $1 \leq i \leq \omega$, $Q_i \in \{\exists, \forall\}$, and $Q_j \neq Q_{j+1}, 1 \leq j < \omega$, $Q_1 = \exists$.

Discrete Polynomial Time Hierarchy– A Quick Reminder

A language

$$L = (L_n)_{n>0} \in \Sigma_\omega$$

if there exists a language $L' = (L'_n)_{n>0} \in \mathbf{P}$ such that

$$\mathbf{x} \in L_n$$
$$\Updownarrow$$
$$(Q_1 \mathbf{y}^1 \in k^{m_1})(Q_2 \mathbf{y}^2 \in k^{m_2}) \ldots (Q_\omega \mathbf{y}^\omega \in k^{m_\omega})$$
$$(\mathbf{y}^1, \ldots, \mathbf{y}^\omega, \mathbf{x}) \in L'_{m+n}$$

where $m(n) = m_1(n) + \cdots + m_\omega(n) = n^{O(1)}$ and for $1 \leq i \leq \omega$, $Q_i \in \{\exists, \forall\}$, and $Q_j \neq Q_{j+1}, 1 \leq j < \omega$, $Q_1 = \exists$.

Reminder (cont.)

Similarly a language

$$L = (L_n)_{n>0} \in \Pi_\omega$$

if there exists a language $L' = (L'_n)_{n>0} \in \mathbf{P}$ such that

$$\mathbf{x} \in L_n$$
$$\Updownarrow$$
$$(Q_1 \mathbf{y}^1 \in k^{m_1})(Q_2 \mathbf{y}^2 \in k^{m_2}) \cdots (Q_\omega \mathbf{y}^\omega \in k^{m_\omega})$$
$$(\mathbf{y}^1, \ldots, \mathbf{y}^\omega, \mathbf{x}) \in L'_{m+n}$$

where $m(n) = m_1(n) + \cdots + m_\omega(n) = n^{O(1)}$ and for $1 \le i \le \omega$, $Q_i \in \{\exists, \forall\}$, and $Q_j \neq Q_{j+1}, 1 \le j < \omega$, $Q_1 = \forall$. Notice that

$$\mathbf{P} = \Sigma_0 = \Pi_0,$$

$$\mathbf{NP} = \Sigma_1, \quad \mathbf{coNP} = \Pi_1.$$

Reminder (cont.)

Similarly a language

$$L = (L_n)_{n>0} \in \Pi_\omega$$

if there exists a language $L' = (L'_n)_{n>0} \in \mathbf{P}$ such that

$$\mathbf{x} \in L_n$$

$$\Updownarrow$$

$$(Q_1 \mathbf{y}^1 \in k^{m_1})(Q_2 \mathbf{y}^2 \in k^{m_2}) \cdots (Q_\omega \mathbf{y}^\omega \in k^{m_\omega})$$
$$(\mathbf{y}^1, \ldots, \mathbf{y}^\omega, \mathbf{x}) \in L'_{m+n}$$

where $m(n) = m_1(n) + \cdots + m_\omega(n) = n^{O(1)}$ and for $1 \leq i \leq \omega$, $Q_i \in \{\exists, \forall\}$, and $Q_j \neq Q_{j+1}$, $1 \leq j < \omega$, $Q_1 = \forall$. Notice that

$$\mathbf{P} = \Sigma_0 = \Pi_0,$$

$$\mathbf{NP} = \Sigma_1, \quad \mathbf{coNP} = \Pi_1.$$

Reminder (cont.)

Similarly a language

$$L = (L_n)_{n>0} \in \Pi_\omega$$

if there exists a language $L' = (L'_n)_{n>0} \in \mathbf{P}$ such that

$$\mathbf{x} \in L_n$$

$$\Updownarrow$$

$$(Q_1 \mathbf{y}^1 \in k^{m_1})(Q_2 \mathbf{y}^2 \in k^{m_2}) \cdots (Q_\omega \mathbf{y}^\omega \in k^{m_\omega})$$
$$(\mathbf{y}^1, \ldots, \mathbf{y}^\omega, \mathbf{x}) \in L'_{m+n}$$

where $m(n) = m_1(n) + \cdots + m_\omega(n) = n^{O(1)}$ and for $1 \leq i \leq \omega$, $Q_i \in \{\exists, \forall\}$, and $Q_j \neq Q_{j+1}, 1 \leq j < \omega$, $Q_1 = \forall$. Notice that

$$\mathbf{P} = \Sigma_0 = \Pi_0,$$

$$\mathbf{NP} = \Sigma_1, \quad \mathbf{coNP} = \Pi_1.$$

Reminder (cont.)

Similarly a language

$$L = (L_n)_{n>0} \in \Pi_\omega$$

if there exists a language $L' = (L'_n)_{n>0} \in \mathbf{P}$ such that

$$\mathbf{x} \in L_n$$

$$\Updownarrow$$

$$(Q_1 \mathbf{y}^1 \in k^{m_1})(Q_2 \mathbf{y}^2 \in k^{m_2}) \cdots (Q_\omega \mathbf{y}^\omega \in k^{m_\omega})$$
$$(\mathbf{y}^1, \ldots, \mathbf{y}^\omega, \mathbf{x}) \in L'_{m+n}$$

where $m(n) = m_1(n) + \cdots + m_\omega(n) = n^{O(1)}$ and for $1 \leq i \leq \omega$, $Q_i \in \{\exists, \forall\}$, and $Q_j \neq Q_{j+1}, 1 \leq j < \omega$, $Q_1 = \forall$. Notice that

$$\mathbf{P} = \Sigma_0 = \Pi_0,$$

$$\mathbf{NP} = \Sigma_1, \quad \mathbf{coNP} = \Pi_1.$$

The polynomial time hierarchy

- Also, notice the inclusions

$$\Sigma_i \subset \Pi_{i+1}, \Sigma_i \subset \Sigma_{i+1}$$
$$\Pi_i \subset \Sigma_{i+1}, \Pi_i \subset \Pi_{i+1}$$

- The *polynomial time hierarchy* is defined to be

$$\mathbf{PH} \stackrel{\text{def}}{=} \bigcup_{\omega \geq 0} (\Sigma_\omega \cup \Pi_\omega) = \bigcup_{\omega \geq 0} \Sigma_\omega = \bigcup_{\omega \geq 0} \Pi_\omega.$$

- *Central problem of CS is to prove that* **PH** *is a proper hierarchy (as is widely believed), and in particular to prove* $\mathbf{P} \neq \mathbf{NP}$.

The polynomial time hierarchy

- Also, notice the inclusions

$$\Sigma_i \subset \Pi_{i+1}, \Sigma_i \subset \Sigma_{i+1}$$
$$\Pi_i \subset \Sigma_{i+1}, \Pi_i \subset \Pi_{i+1}$$

- The *polynomial time hierarchy* is defined to be

$$\mathbf{PH} \overset{\text{def}}{=} \bigcup_{\omega \geq 0} (\Sigma_\omega \cup \Pi_\omega) = \bigcup_{\omega \geq 0} \Sigma_\omega = \bigcup_{\omega \geq 0} \Pi_\omega.$$

- *Central problem of CS is to prove that* **PH** *is a proper hierarchy (as is widely believed), and in particular to prove* **P** $\neq$ **NP**.

The polynomial time hierarchy

- Also, notice the inclusions

$$\Sigma_i \subset \Pi_{i+1}, \Sigma_i \subset \Sigma_{i+1}$$
$$\Pi_i \subset \Sigma_{i+1}, \Pi_i \subset \Pi_{i+1}$$

- The *polynomial time hierarchy* is defined to be

$$\mathbf{PH} \stackrel{\text{def}}{=} \bigcup_{\omega \geq 0} (\Sigma_\omega \cup \Pi_\omega) = \bigcup_{\omega \geq 0} \Sigma_\omega = \bigcup_{\omega \geq 0} \Pi_\omega.$$

- *Central problem of CS is to prove that* **PH** *is a proper hierarchy (as is widely believed), and in particular to prove* $\mathbf{P} \neq \mathbf{NP}$*.*

The Class $\#\mathbf{P}$

- A sequence of functions $(f_n : k^n \to \mathbb{N})_{n>0}$ is said to be in the class $\#\mathbf{P}$ if there exists $L = (L_n)_{n>0} \in \mathbf{P}$ such that for $\mathbf{z} \in k^n$

$$f_n(\mathbf{z}) = \#\{\mathbf{y} \in k^{m(n)} \mid (\mathbf{y}, \mathbf{z}) \in L_{m+n}\}.$$

The Class $\#\mathbf{P}$

- A sequence of functions $(f_n : k^n \rightarrow \mathbb{N})_{n>0}$ is said to be in the class $\#\mathbf{P}$ if there exists $L = (L_n)_{n>0} \in \mathbf{P}$ such that for $\mathbf{z} \in k^n$

$$f_n(\mathbf{z}) = \#\{\mathbf{y} \in k^{m(n)} \mid (\mathbf{y}, \mathbf{z}) \in L_{m+n}\}.$$

Toda's Theorem

Toda's theorem is a seminal result in discrete complexity theory and gives the following inclusion.

Theorem (Toda (1989))

$$\mathbf{PH} \subset \mathbf{P}^{\#\mathbf{P}}$$

"illustrates the power of counting"

Toda’s Theorem

Toda’s theorem is a seminal result in discrete complexity theory and gives the following inclusion.

Theorem (Toda (1989))

$$\mathbf{PH} \subset \mathbf{P}^{\#\mathbf{P}}$$

“illustrates the power of counting”

Toda's Theorem

Toda's theorem is a seminal result in discrete complexity theory and gives the following inclusion.

Theorem (Toda (1989))

$$\mathbf{PH} \subset \mathbf{P}^{\#\mathbf{P}}$$

"illustrates the power of counting"

Toda's Theorem

Toda's theorem is a seminal result in discrete complexity theory and gives the following inclusion.

Theorem (Toda (1989))

$$\mathbf{PH} \subset \mathbf{P}^{\#\mathbf{P}}$$

"illustrates the power of counting"

Blum-Shub-Smale model

- Generalized TM where k is allowed to be any ring (we restrict ourseleves to the cases $k = \mathbb{C}$ or $\mathbb{R}$).
- Setting $k = \mathbb{Z}/2\mathbb{Z}$ (or any finite field) recovers the classical complexity classes.
- Informally, such a TM should be thought of as a program that accepts as input $\mathbf{x} \in k^n$, and at each step
  1. either makes a ring computation $z_i \leftarrow z_j * z_\ell$;
  2. or branches according to a test $z_j\{=, \neq\}0$ in case $k = \mathbb{C}$, or the test $z_j\{>, <, =\}0$ in case $k = \mathbb{R}$;
  3. or accepts/rejects.
- A B-S-S TM accepts for every n a subset of $S_n \subset k^n$.
  1. In case $k = \mathbb{C}$, each such S_n [illegible]
  2. In case $k = \mathbb{R}$, each S_n [illegible]

Blum-Shub-Smale model

- Generalized TM where k is allowed to be any ring (we restrict ourseleves to the cases $k = \mathbb{C}$ or $\mathbb{R}$).
- Setting $k = \mathbb{Z}/2\mathbb{Z}$ (or any finite field) recovers the classical complexity classes.
- Informally, such a TM should be thought of as a program that accepts as input $\mathbf{x} \in k^n$, and at each step
  1. either makes a ring computation $z_i \leftarrow z_j * z_\ell$;
  2. or branches according to a test $z_j\{=,\neq\}0$ in case $k = \mathbb{C}$, or the test $z_j\{>,<,=\}0$ in case $k = \mathbb{R}$;
  3. or accepts/rejects.
- A B-S-S TM accepts for every n a subset of $S_n \subset k^n$.
  1. In case $k = \mathbb{C}$, each such S_n is a constructible subset of $\mathbb{C}^n$;
  2. in case $k = \mathbb{R}$, each S_n is a semi-algebraic subset of $\mathbb{R}^n$.

Blum-Shub-Smale model

- Generalized TM where k is allowed to be any ring (we restrict ourseleves to the cases $k = \mathbb{C}$ or $\mathbb{R}$).
- Setting $k = \mathbb{Z}/2\mathbb{Z}$ (or any finite field) recovers the classical complexity classes.
- Informally, such a TM should be thought of as a program that accepts as input $\mathbf{x} \in k^n$, and at each step
    1. either makes a ring computation $z_i \leftarrow z_j * z_\ell$;
    2. or branches according to a test $z_j\{=, \neq\}0$ in case $k = \mathbb{C}$, or the test $z_j\{>, <, =\}0$ in case $k = \mathbb{R}$;
    3. or accepts/rejects.
- A B-S-S TM accepts for every n a subset of $S_n \subset k^n$.
    1. In case $k = \mathbb{C}$, each such S_n is a constructible subset of $\mathbb{C}^n$.
    2. In case $k = \mathbb{R}$, each S_n is a semi-algebraic subset of $\mathbb{R}^n$.

Blum-Shub-Smale model

- Generalized TM where k is allowed to be any ring (we restrict ourseleves to the cases $k = \mathbb{C}$ or $\mathbb{R}$).
- Setting $k = \mathbb{Z}/2\mathbb{Z}$ (or any finite field) recovers the classical complexity classes.
- Informally, such a TM should be thought of as a program that accepts as input $\mathbf{x} \in k^n$, and at each step
  1. either makes a ring computation $z_i \leftarrow z_j * z_\ell$;
  2. or branches according to a test $z_j\{=,\neq\}0$ in case $k = \mathbb{C}$, or the test $z_j\{>,<,=\}0$ in case $k = \mathbb{R}$;
  3. or accepts/rejects.
- A B-S-S TM accepts for every n a subset of $S_n \subset k^n$.
  1. In case $k = \mathbb{C}$, each such S_n is a constructible subset of $\mathbb{C}^n$.
  2. In case $k = \mathbb{R}$, each S_n is a semi-algebraic subset of $\mathbb{R}^n$.

Blum-Shub-Smale model

- Generalized TM where k is allowed to be any ring (we restrict ourseleves to the cases $k = \mathbb{C}$ or $\mathbb{R}$).
- Setting $k = \mathbb{Z}/2\mathbb{Z}$ (or any finite field) recovers the classical complexity classes.
- Informally, such a TM should be thought of as a program that accepts as input $\mathbf{x} \in k^n$, and at each step
    1. either makes a ring computation $z_i \leftarrow z_j * z_\ell$;
    2. or branches according to a test $z_j\{=,\neq\}0$ in case $k = \mathbb{C}$, or the test $z_j\{>,<,=\}0$ in case $k = \mathbb{R}$;
    3. or accepts/rejects.
- A B-S-S TM accepts for every n a subset of $S_n \subset k^n$.
    1. In case $k = \mathbb{C}$, each such S_n is a constructible subset of $\mathbb{C}^n$.
    2. In case $k = \mathbb{R}$, each S_n is a *semi-algebraic* subset of $\mathbb{R}^n$.

Blum-Shub-Smale model

- Generalized TM where k is allowed to be any ring (we restrict ourseleves to the cases $k = \mathbb{C}$ or $\mathbb{R}$).
- Setting $k = \mathbb{Z}/2\mathbb{Z}$ (or any finite field) recovers the classical complexity classes.
- Informally, such a TM should be thought of as a program that accepts as input $\mathbf{x} \in k^n$, and at each step
  1. either makes a ring computation $z_i \leftarrow z_j * z_\ell$;
  2. or branches according to a test $z_j \{=, \neq\} 0$ in case $k = \mathbb{C}$, or the test $z_j \{>, <, =\} 0$ in case $k = \mathbb{R}$;
  3. or accepts/rejects.
- A B-S-S TM accepts for every n a subset of $S_n \subset k^n$.
  1. In case $k = \mathbb{C}$, each such S_n is a constructible subset of $\mathbb{C}^n$.
  2. In case $k = \mathbb{R}$, each S_n is a semi-algebraic subset of $\mathbb{R}^n$.

Blum-Shub-Smale model

- Generalized TM where k is allowed to be any ring (we restrict ourseleves to the cases $k = \mathbb{C}$ or $\mathbb{R}$).
- Setting $k = \mathbb{Z}/2\mathbb{Z}$ (or any finite field) recovers the classical complexity classes.
- Informally, such a TM should be thought of as a program that accepts as input $\mathbf{x} \in k^n$, and at each step
    1. either makes a ring computation $z_i \leftarrow z_j * z_\ell$;
    2. or branches according to a test $z_j \{=, \neq\} 0$ in case $k = \mathbb{C}$, or the test $z_j \{>, <, =\} 0$ in case $k = \mathbb{R}$;
    3. or accepts/rejects.
- A B-S-S TM accepts for every n a subset of $S_n \subset k^n$.
    1. In case $k = \mathbb{C}$, each such S_n is a *constructible* subset of $\mathbb{C}^n$,
    2. in case $k = \mathbb{R}$, each S_n is a *semi-algebraic* subset of $\mathbb{R}^n$.

Blum-Shub-Smale model

- Generalized TM where k is allowed to be any ring (we restrict ourseleves to the cases $k = \mathbb{C}$ or $\mathbb{R}$).
- Setting $k = \mathbb{Z}/2\mathbb{Z}$ (or any finite field) recovers the classical complexity classes.
- Informally, such a TM should be thought of as a program that accepts as input $\mathbf{x} \in k^n$, and at each step
  1. either makes a ring computation $z_i \leftarrow z_j * z_\ell$;
  2. or branches according to a test $z_j\{=,\neq\}0$ in case $k = \mathbb{C}$, or the test $z_j\{>,<,=\}0$ in case $k = \mathbb{R}$;
  3. or accepts/rejects.
- A B-S-S TM accepts for every n a subset of $S_n \subset k^n$.
  1. In case $k = \mathbb{C}$, each such S_n is a *constructible* subset of $\mathbb{C}^n$,
  2. in case $k = \mathbb{R}$, each S_n is a *semi-algebraic* subset of $\mathbb{R}^n$.

Blum-Shub-Smale model

- Generalized TM where k is allowed to be any ring (we restrict ourseleves to the cases $k = \mathbb{C}$ or $\mathbb{R}$).
- Setting $k = \mathbb{Z}/2\mathbb{Z}$ (or any finite field) recovers the classical complexity classes.
- Informally, such a TM should be thought of as a program that accepts as input $\mathbf{x} \in k^n$, and at each step
  1. either makes a ring computation $z_i \leftarrow z_j * z_\ell$;
  2. or branches according to a test $z_j\{=, \neq\}0$ in case $k = \mathbb{C}$, or the test $z_j\{>, <, =\}0$ in case $k = \mathbb{R}$;
  3. or accepts/rejects.
- A B-S-S TM accepts for every n a subset of $S_n \subset k^n$.
  1. In case $k = \mathbb{C}$, each such S_n is a *constructible* subset of $\mathbb{C}^n$,
  2. in case $k = \mathbb{R}$, each S_n is a *semi-algebraic* subset of $\mathbb{R}^n$.

Blum-Shub-Smale model

- Generalized TM where k is allowed to be any ring (we restrict ourseleves to the cases $k = \mathbb{C}$ or $\mathbb{R}$).
- Setting $k = \mathbb{Z}/2\mathbb{Z}$ (or any finite field) recovers the classical complexity classes.
- Informally, such a TM should be thought of as a program that accepts as input $\mathbf{x} \in k^n$, and at each step
  1. either makes a ring computation $z_i \leftarrow z_j * z_\ell$;
  2. or branches according to a test $z_j\{=,\neq\}0$ in case $k = \mathbb{C}$, or the test $z_j\{>,<,=\}0$ in case $k = \mathbb{R}$;
  3. or accepts/rejects.
- A B-S-S TM accepts for every n a subset of $S_n \subset k^n$.
  1. In case $k = \mathbb{C}$, each such S_n is a *constructible* subset of $\mathbb{C}^n$,
  2. in case $k = \mathbb{R}$, each S_n is a *semi-algebraic* subset of $\mathbb{R}^n$.

Complexity Classes

- Complexity classes $\mathbf{P}_k, \mathbf{NP}_k, \mathbf{coNP}_k$ and more generally $\mathbf{PH}_k$ are defined as before (for $k = \mathbb{C}, \mathbb{R}$).
- B-S-S developed a theory of **NP**-completeness.
- In case, $k = \mathbb{C}$ the problem of determining if a system of $n+1$ polynomial equations in n variables has a common zero in $\mathbb{C}^n$ is $\mathbf{NP}_{\mathbb{C}}$-complete.
- In case, $k = \mathbb{R}$ the problem of determining if a quartic polynomial in n variables has a common zero in $\mathbb{R}^n$ is $\mathbf{NP}_{\mathbb{R}}$-complete.
- It is unknown if $\mathbf{P}_{\mathbb{C}} = \mathbf{NP}_{\mathbb{C}}$ (respectively, $\mathbf{P}_{\mathbb{R}} = \mathbf{NP}_{\mathbb{R}}$) just as in the discrete case.

Complexity Classes

- Complexity classes $\mathbf{P}_k, \mathbf{NP}_k, \mathbf{coNP}_k$ and more generally $\mathbf{PH}_k$ are defined as before (for $k = \mathbb{C}, \mathbb{R}$).
- B-S-S developed a theory of **NP**-completeness.
- In case, $k = \mathbb{C}$ the problem of determining if a system of $n+1$ polynomial equations in n variables has a common zero in $\mathbb{C}^n$ is $\mathbf{NP}_{\mathbb{C}}$-complete.
- In case, $k = \mathbb{R}$ the problem of determining if a quartic polynomial in n variables has a common zero in $\mathbb{R}^n$ is $\mathbf{NP}_{\mathbb{R}}$-complete.
- It is unknown if $\mathbf{P}_{\mathbb{C}} = \mathbf{NP}_{\mathbb{C}}$ (respectively, $\mathbf{P}_{\mathbb{R}} = \mathbf{NP}_{\mathbb{R}}$) just as in the discrete case.

Complexity Classes

- Complexity classes $\mathbf{P}_k, \mathbf{NP}_k, \mathbf{coNP}_k$ and more generally $\mathbf{PH}_k$ are defined as before (for $k = \mathbb{C}, \mathbb{R}$).
- B-S-S developed a theory of **NP**-completeness.
- In case, $k = \mathbb{C}$ the problem of determining if a system of $n + 1$ polynomial equations in n variables has a common zero in $\mathbb{C}^n$ is $\mathbf{NP}_{\mathbb{C}}$-complete.
- In case, $k = \mathbb{R}$ the problem of determining if a quartic polynomial in n variables has a common zero in $\mathbb{R}^n$ is $\mathbf{NP}_{\mathbb{R}}$-complete.
- It is unknown if $\mathbf{P}_{\mathbb{C}} = \mathbf{NP}_{\mathbb{C}}$ (respectively, $\mathbf{P}_{\mathbb{R}} = \mathbf{NP}_{\mathbb{R}}$) just as in the discrete case.

Complexity Classes

- Complexity classes $\mathbf{P}_k, \mathbf{NP}_k, \mathbf{coNP}_k$ and more generally $\mathbf{PH}_k$ are defined as before (for $k = \mathbb{C}, \mathbb{R}$).
- B-S-S developed a theory of **NP**-completeness.
- In case, $k = \mathbb{C}$ the problem of determining if a system of $n+1$ polynomial equations in n variables has a common zero in $\mathbb{C}^n$ is $\mathbf{NP}_{\mathbb{C}}$-complete.
- In case, $k = \mathbb{R}$ the problem of determining if a quartic polynomial in n variables has a common zero in $\mathbb{R}^n$ is $\mathbf{NP}_{\mathbb{R}}$-complete.
- It is unknown if $\mathbf{P}_{\mathbb{C}} = \mathbf{NP}_{\mathbb{C}}$ (respectively, $\mathbf{P}_{\mathbb{R}} = \mathbf{NP}_{\mathbb{R}}$) just as in the discrete case.

Complexity Classes

- Complexity classes $\mathbf{P}_k, \mathbf{NP}_k, \mathbf{coNP}_k$ and more generally $\mathbf{PH}_k$ are defined as before (for $k = \mathbb{C}, \mathbb{R}$).
- B-S-S developed a theory of **NP**-completeness.
- In case, $k = \mathbb{C}$ the problem of determining if a system of $n + 1$ polynomial equations in n variables has a common zero in $\mathbb{C}^n$ is $\mathbf{NP}_\mathbb{C}$-complete.
- In case, $k = \mathbb{R}$ the problem of determining if a quartic polynomial in n variables has a common zero in $\mathbb{R}^n$ is $\mathbf{NP}_\mathbb{R}$-complete.
- It is unknown if $\mathbf{P}_\mathbb{C} = \mathbf{NP}_\mathbb{C}$ (respectively, $\mathbf{P}_\mathbb{R} = \mathbf{NP}_\mathbb{R}$) just as in the discrete case.

Semi-algebraic sets

- From now we assume $k = \mathbb{R}$, and restrict ourselves to real TM in the sense of B-S-S.
- Such a machine accepts a sequence $(S_n \subset \mathbb{R}^n)_{n>0}$ where each S_n is a semi-algebraic subset of $\mathbb{R}^n$.
- A semi-algebraic set, $S \subset \mathbb{R}^n$, is a subset of $\mathbb{R}^n$ defined by a Boolean formula whose atoms are polynomial equalities and inequalities.

Semi-algebraic sets

- From now we assume $k = \mathbb{R}$, and restrict ourselves to real TM in the sense of B-S-S.
- Such a machine accepts a sequence $(S_n \subset \mathbb{R}^n)_{n>0}$ where each S_n is a semi-algebraic subset of $\mathbb{R}^n$.
- A semi-algebraic set, $S \subset \mathbb{R}^n$, is a subset of $\mathbb{R}^n$ defined by a Boolean formula whose atoms are polynomial equalities and inequalities.

Semi-algebraic sets

- From now we assume $k = \mathbb{R}$, and restrict ourselves to real TM in the sense of B-S-S.
- Such a machine accepts a sequence $(S_n \subset \mathbb{R}^n)_{n>0}$ where each S_n is a semi-algebraic subset of $\mathbb{R}^n$.
- A semi-algebraic set, $S \subset \mathbb{R}^n$, is a subset of $\mathbb{R}^n$ defined by a Boolean formula whose atoms are polynomial equalities and inequalities.

Two classes of problems

The most important algorithmic problems studied in this area fall into two broad sub-classes:

1. the problem of quantifier elimination, and its special cases such as *deciding* a sentence in the first order theory of reals, or deciding emptiness of semi-algebraic sets.
2. the problem of *computing* topological invariants of semi-algebraic sets, such as the number of connected components, Euler-Poincaré characteristic, and more generally all the Betti numbers of semi-algebraic sets.

Two classes of problems

The most important algorithmic problems studied in this area fall into two broad sub-classes:

1. the problem of quantifier elimination, and its special cases such as *deciding* a sentence in the first order theory of reals, or deciding emptiness of semi-algebraic sets.
2. the problem of *computing* topological invariants of semi-algebraic sets, such as the number of connected components, Euler-Poincaré characteristic, and more generally all the Betti numbers of semi-algebraic sets.

Two classes of problems

The most important algorithmic problems studied in this area fall into two broad sub-classes:

1. the problem of quantifier elimination, and its special cases such as *deciding* a sentence in the first order theory of reals, or deciding emptiness of semi-algebraic sets.
2. the problem of *computing* topological invariants of semi-algebraic sets, such as the number of connected components, Euler-Poincaré characteristic, and more generally all the Betti numbers of semi-algebraic sets.

Analogy with Toda's Theorem

- The classes **PH** and $\#$**P** appearing in the two sides of the inclusion in Toda's Theorem can be identified with the two broad classes of problems in algorithmic semi-algebraic geometry;
- the class **PH** with the problem of deciding sentences with a fixed number of quantifier alternations;
- the class $\#$**P** with the problem of computing topological invariants of semi-algebraic sets, namely their Betti numbers which generalize the notion of cardinality for finite sets.
- It is thus quite natural to seek a real analogue of Toda's theorem.

Analogy with Toda's Theorem

- The classes **PH** and $\#$**P** appearing in the two sides of the inclusion in Toda's Theorem can be identified with the two broad classes of problems in algorithmic semi-algebraic geometry;
- the class **PH** with the problem of deciding sentences with a fixed number of quantifier alternations;
- the class $\#$**P** with the problem of computing topological invariants of semi-algebraic sets, namely their Betti numbers which generalize the notion of cardinality for finite sets.
- It is thus quite natural to seek a real analogue of Toda's theorem.

Analogy with Toda's Theorem

- The classes **PH** and $\#$**P** appearing in the two sides of the inclusion in Toda's Theorem can be identified with the two broad classes of problems in algorithmic semi-algebraic geometry;
- the class **PH** with the problem of deciding sentences with a fixed number of quantifier alternations;
- the class $\#$**P** with the problem of computing topological invariants of semi-algebraic sets, namely their Betti numbers which generalize the notion of cardinality for finite sets.
- It is thus quite natural to seek a real analogue of Toda's theorem.

Analogy with Toda's Theorem

- The classes **PH** and $\#$**P** appearing in the two sides of the inclusion in Toda's Theorem can be identified with the two broad classes of problems in algorithmic semi-algebraic geometry;
- the class **PH** with the problem of deciding sentences with a fixed number of quantifier alternations;
- the class $\#$**P** with the problem of computing topological invariants of semi-algebraic sets, namely their Betti numbers which generalize the notion of cardinality for finite sets.
- It is thus quite natural to seek a real analogue of Toda's theorem.

Real Analogue of $\#\mathbf{P}$

- In order to define real analogues of counting complexity classes of discrete complexity theory, it is necessary to identify the proper notion of "counting" in the context of semi-algebraic geometry.
- Counting complexity classes over the reals have been defined previously by Meer (2000) and studied extensively by other authors Burgisser, Cucker et al (2006). These authors used a straightforward generalization to semi-algebraic sets of counting in the case of finite sets; namely

$$\begin{aligned} f(S) &= \mathrm{card}(S) \text{ if } \mathrm{card}(S) < \infty \\ &= \infty \text{ otherwise.} \end{aligned}$$

Real Analogue of $\#\mathbf{P}$

- In order to define real analogues of counting complexity classes of discrete complexity theory, it is necessary to identify the proper notion of “counting” in the context of semi-algebraic geometry.
- Counting complexity classes over the reals have been defined previously by Meer (2000) and studied extensively by other authors Burgisser, Cucker et al (2006). These authors used a straightforward generalization to semi-algebraic sets of counting in the case of finite sets; namely

$$\begin{aligned} f(S) &= \mathrm{card}(S) \text{ if } \mathrm{card}(S) < \infty \\ &= \infty \text{ otherwise.} \end{aligned}$$

Criticism and an alternative

- In our view this is not fully satisfactory, since the count gives no information when the semi-algebraic set is infinite, and *most interesting semi-algebraic sets are infinite*.
- If one thinks of "counting" a semi-algebraic set $S \subset \mathbb{R}^k$ as computing certain discrete invariants, then a natural mathematical candidate is its sequence of Betti numbers, $b_0(S), \ldots, b_{k-1}(S)$.
- In case $\mathrm{card}(S) < \infty$, we have that $b_0(S) = \mathrm{card}(S)$.

Criticism and an alternative

- In our view this is not fully satisfactory, since the count gives no information when the semi-algebraic set is infinite, and *most interesting semi-algebraic sets are infinite*.
- If one thinks of "counting" a semi-algebraic set $S \subset \mathbb{R}^k$ as computing certain discrete invariants, then a natural mathematical candidate is its sequence of Betti numbers, $b_0(S), \ldots, b_{k-1}(S)$.
- In case $\mathrm{card}(S) < \infty$, we have that $b_0(S) = \mathrm{card}(S)$.

Criticism and an alternative

- In our view this is not fully satisfactory, since the count gives no information when the semi-algebraic set is infinite, and *most interesting semi-algebraic sets are infinite*.
- If one thinks of "counting" a semi-algebraic set $S \subset \mathbb{R}^k$ as computing certain discrete invariants, then a natural mathematical candidate is its sequence of Betti numbers, $b_0(S), \ldots, b_{k-1}(S)$.
- In case $\mathrm{card}(S) < \infty$, we have that $b_0(S) = \mathrm{card}(S)$.

Definition of $\#\mathbf{P}_{\mathbb{R}}^{\dagger}$

Definition (The class $\#\mathbf{P}_{\mathbb{R}}^{\dagger}$)

We call a sequence of functions

$$(f_n : \mathbb{R}^n \to \mathbb{N}^{m(n)})_{n>0}$$

with $m = n^{O(1)}$, to be in class $\#\mathbf{P}_{\mathbb{R}}^{\dagger}$ if there exists a sequence $(S_n \subset \mathbb{R}^n)_{n>0} \in \mathbf{P}_{\mathbb{R}}$ such that

$$f_{n,i}(\mathbf{z}) = b_i(\{\mathbf{y} \in \mathbb{R}^{m(n)} \mid (\mathbf{y}, \mathbf{z}) \in S_{m+n}\}), 0 \leq i \leq m.$$

Counting and Betti numbers

- The connection between counting points of varieties and their Betti numbers is more direct over fields of positive characteristic via the zeta function.
- The zeta function of a variety defined over $\mathbb{F}_p$ is the exponential generating function of the sequence whose n-th term is the number of points in the variety over $\mathbb{F}_{p^n}$.
- The zeta function depends on the Betti numbers of the variety with respect to a certain (ℓ-adic) co-homology theory.
- Thus, the problems of "counting" varieties and computing their Betti numbers, are connected at a deeper level, and thus our definition of $\#\mathbf{P}^{\dagger}_{\mathbb{R}}$ is not entirely ad hoc.

Counting and Betti numbers

- The connection between counting points of varieties and their Betti numbers is more direct over fields of positive characteristic via the zeta function.
- The zeta function of a variety defined over $\mathbb{F}_p$ is the exponential generating function of the sequence whose n-th term is the number of points in the variety over $\mathbb{F}_{p^n}$.
- The zeta function depends on the Betti numbers of the variety with respect to a certain (ℓ-adic) co-homology theory.
- Thus, the problems of "counting" varieties and computing their Betti numbers, are connected at a deeper level, and thus our definition of $\#\mathbf{P}^{\dagger}_{\mathbb{R}}$ is not entirely ad hoc.

Counting and Betti numbers

- The connection between counting points of varieties and their Betti numbers is more direct over fields of positive characteristic via the zeta function.
- The zeta function of a variety defined over $\mathbb{F}_p$ is the exponential generating function of the sequence whose n-th term is the number of points in the variety over $\mathbb{F}_{p^n}$.
- The zeta function depends on the Betti numbers of the variety with respect to a certain (ℓ-adic) co-homology theory.
- Thus, the problems of "counting" varieties and computing their Betti numbers, are connected at a deeper level, and thus our definition of $\#\mathbf{P}^{\dagger}_{\mathbb{R}}$ is not entirely ad hoc.

Counting and Betti numbers

- The connection between counting points of varieties and their Betti numbers is more direct over fields of positive characteristic via the zeta function.
- The zeta function of a variety defined over $\mathbb{F}_p$ is the exponential generating function of the sequence whose n-th term is the number of points in the variety over $\mathbb{F}_{p^n}$.
- The zeta function depends on the Betti numbers of the variety with respect to a certain (ℓ-adic) co-homology theory.
- Thus, the problems of "counting" varieties and computing their Betti numbers, are connected at a deeper level, and thus our definition of $\#\mathbf{P}_{\mathbb{R}}^{\dagger}$ is not entirely ad hoc.

Real analogue of Toda's theorem

It is now natural to formulate the following conjecture.

Conjecture

$$\mathbf{PH}_{\mathbb{R}} \subset \mathbf{P}^{\#\mathbf{P}^{\dagger}_{\mathbb{R}}}$$

For technical reasons we are unable to prove this without a further compactness hypothesis on the left hand-side.

Real analogue of Toda's theorem

It is now natural to formulate the following conjecture.

Conjecture

$$\mathbf{PH}_{\mathbb{R}} \subset \mathbf{P}^{\#\mathbf{P}^{\dagger}_{\mathbb{R}}}$$

For technical reasons we are unable to prove this without a further compactness hypothesis on the left hand-side.

Real analogue of Toda's theorem

It is now natural to formulate the following conjecture.

Conjecture

$$\mathbf{PH}_{\mathbb{R}} \subset \mathbf{P}^{\#\mathbf{P}^{\dagger}_{\mathbb{R}}}$$

For technical reasons we are unable to prove this without a further compactness hypothesis on the left hand-side.

The compact real polynomial hierarchy

We say that a sequence of semi-algebraic sets

$$(S_n \subset \mathbf{S}^n)_{n>0} \in \Sigma^c_{\mathbb{R},\omega}$$

with each S_n compact if there exists another sequence $(S'_n)_{n>0} \in \mathbf{P}_{\mathbb{R}}$ such that

$$x \in S_n$$

if and only if

$$(Q_1 y^1 \in \mathbf{S}^{m_1})(Q_2 y^2 \in \mathbf{S}^{m_2}) \ldots (Q_\omega y^\omega \in \mathbf{S}^{m_\omega})$$

$$(y^1, \ldots, y^\omega, x) \in S'_{m+n}$$

where $m(n) = m_1(n) + \cdots + m_\omega(n) = n^{O(1)}$ and for $1 \leq i \leq \omega$, $Q_i \in \{\exists, \forall\}$, and $Q_j \neq Q_{j+1}, 1 \leq j < \omega$, $Q_1 = \exists$. The compact class $\Pi^c_{\mathbb{R},\omega}$ is defined analogously.

The compact real polynomial hierarchy

We say that a sequence of semi-algebraic sets

$$(S_n \subset \mathbf{S}^n)_{n>0} \in \Sigma^{c}_{\mathbb{R},\omega}$$

with each S_n compact if there exists another sequence $(S'_n)_{n>0} \in \mathbf{P}_{\mathbb{R}}$ such that

$$x \in S_n$$

if and only if

$$(Q_1 y^1 \in \mathbf{S}^{m_1})(Q_2 y^2 \in \mathbf{S}^{m_2}) \ldots (Q_\omega y^\omega \in \mathbf{S}^{m_\omega})$$

$$(y^1, \ldots, y^\omega, x) \in S'_{m+n}$$

where $m(n) = m_1(n) + \cdots + m_\omega(n) = n^{O(1)}$ and for $1 \leq i \leq \omega$, $Q_i \in \{\exists, \forall\}$, and $Q_j \neq Q_{j+1}, 1 \leq j < \omega$, $Q_1 = \exists$. The compact class $\Pi^{c}_{\mathbb{R},\omega}$ is defined analogously.

The compact real polynomial hierarchy

We say that a sequence of semi-algebraic sets

$$(S_n \subset \mathbf{S}^n)_{n>0} \in \Sigma^c_{\mathbb{R},\omega}$$

with each S_n compact if there exists another sequence $(S'_n)_{n>0} \in \mathbf{P}_{\mathbb{R}}$ such that

$$x \in S_n$$

if and only if

$$(Q_1 y^1 \in \mathbf{S}^{m_1})(Q_2 y^2 \in \mathbf{S}^{m_2}) \dots (Q_\omega y^\omega \in \mathbf{S}^{m_\omega})$$
$$(y^1, \dots, y^\omega, x) \in S'_{m+n}$$

where $m(n) = m_1(n) + \cdots + m_\omega(n) = n^{O(1)}$ and for $1 \leq i \leq \omega$, $Q_i \in \{\exists, \forall\}$, and $Q_j \neq Q_{j+1}, 1 \leq j < \omega$, $Q_1 = \exists$. The compact class $\Pi^c_{\mathbb{R},\omega}$ is defined analogously.

The compact real polynomial hierarchy

We say that a sequence of semi-algebraic sets

$$(S_n \subset \mathbf{S}^n)_{n>0} \in \Sigma^c_{\mathbb{R},\omega}$$

with each S_n compact if there exists another sequence $(S'_n)_{n>0} \in \mathbf{P}_{\mathbb{R}}$ such that

$$x \in S_n$$

$$\text{if and only if}$$

$$(Q_1 y^1 \in \mathbf{S}^{m_1})(Q_2 y^2 \in \mathbf{S}^{m_2}) \ldots (Q_\omega y^\omega \in \mathbf{S}^{m_\omega})$$
$$(y^1, \ldots, y^\omega, x) \in S'_{m+n}$$

where $m(n) = m_1(n) + \cdots + m_\omega(n) = n^{O(1)}$ and for $1 \leq i \leq \omega$, $Q_i \in \{\exists, \forall\}$, and $Q_j \neq Q_{j+1}, 1 \leq j < \omega$, $Q_1 = \exists$. The compact class $\Pi^c_{\mathbb{R},\omega}$ is defined analogously.

The compact real polynomial hierarchy (cont.)

We define

$$\mathbf{PH}^{c}_{\mathbb{R}} \overset{\text{def}}{=} \bigcup_{\omega\geq 0} (\Sigma^{c}_{\mathbb{R},\omega} \cup \Pi^{c}_{\mathbb{R},\omega}) = \bigcup_{\omega\geq 0} \Sigma^{c}_{\mathbb{R},\omega} = \bigcup_{\omega\geq 0} {}^{c}_{\mathbb{R},\omega}.$$

Notice that the semi-algebraic sets belonging to any language in $\mathbf{PH}^{c}_{\mathbb{R}}$ are all semi-algebraic compact (in fact closed semi-algebraic subsets of spheres). Also, notice the inclusion

$$\mathbf{PH}^{c}_{\mathbb{R}} \subset \mathbf{PH}_{\mathbb{R}}.$$

The compact real polynomial hierarchy (cont.)

We define

$$\mathbf{PH}^{c}_{\mathbb{R}} \overset{\text{def}}{=} \bigcup_{\omega\geq 0} (\Sigma^{c}_{\mathbb{R},\omega} \cup \Pi^{c}_{\mathbb{R},\omega}) = \bigcup_{\omega\geq 0} \Sigma^{c}_{\mathbb{R},\omega} = \bigcup_{\omega\geq 0} {}^{c}_{\mathbb{R},\omega}.$$

Notice that the semi-algebraic sets belonging to any language in $\mathbf{PH}^{c}_{\mathbb{R}}$ are all semi-algebraic compact (in fact closed semi-algebraic subsets of spheres). Also, notice the inclusion

$$\mathbf{PH}^{c}_{\mathbb{R}} \subset \mathbf{PH}_{\mathbb{R}}.$$

Main theorem

Theorem (B-Zell,2008)

$$\mathbf{PH}_{\mathbb{R}}^{c} \subset \mathbf{P}_{\mathbb{R}}^{\#\mathbf{P}_{\mathbb{R}}^{\dagger}}.$$

Remark about the compactness assumption

- Even though the restriction to compact semi-algebraic sets might appear to be only a technicality at first glance, this is actually an important restriction.
- For instance, it is a long-standing open question in real complexity theory whether there exists an $\mathbf{NP}_{\mathbb{R}}$-complete problem which belongs to the class $^{\circ}{}^{c}_{1}$ (the compact version of the class $\mathbf{NP}_{\mathbb{R}}$ i.e. where the certificates are constrained to come from a compact set).

Remark about the compactness assumption

- Even though the restriction to compact semi-algebraic sets might appear to be only a technicality at first glance, this is actually an important restriction.
- For instance, it is a long-standing open question in real complexity theory whether there exists an $\mathbf{NP}_{\mathbb{R}}$-complete problem which belongs to the class $^{\circ c}_{1}$ (the compact version of the class $\mathbf{NP}_{\mathbb{R}}$ i.e. where the certificates are constrained to come from a compact set).

Summary of the Main Idea

- Our main tool is a topological construction which given a semi-algebraic map $f : A \to B$ (satisfying a mild hypothesis) and $p \geq 0$, constructs *efficiently* a semi-algebraic set, $D_f^p(A)$, such that

$$b_i(f(A)) = b_i(D_f^p(A)), 0 \leq i < p.$$

- Notice that even if there exists an efficient (i.e. polynomial time) algorithm for checking membership in A, the same need not be true for the image $f(A)$.
- A second topological ingredient is *Alexander-Lefshetz duality* which relates the Betti numbers of a compact subset K of the sphere $\mathbf{S}^n$ with those of $\mathbf{S}^n - K$.

Summary of the Main Idea

- Our main tool is a topological construction which given a semi-algebraic map $f : A \to B$ (satisfying a mild hypothesis) and $p \geq 0$, constructs *efficiently* a semi-algebraic set, $D_f^p(A)$, such that

$$b_i(f(A)) = b_i(D_f^p(A)), 0 \leq i < p.$$

- Notice that even if there exists an efficient (i.e. polynomial time) algorithm for checking membership in A, the same need not be true for the image $f(A)$.
- A second topological ingredient is *Alexander-Lefshetz duality* which relates the Betti numbers of a compact subset K of the sphere $\mathbf{S}^n$ with those of $\mathbf{S}^n - K$.

Summary of the Main Idea

- Our main tool is a topological construction which given a semi-algebraic map $f : A \to B$ (satisfying a mild hypothesis) and $p \geq 0$, constructs *efficiently* a semi-algebraic set, $D_f^p(A)$, such that

$$b_i(f(A)) = b_i(D_f^p(A)), 0 \leq i < p.$$

- Notice that even if there exists an efficient (i.e. polynomial time) algorithm for checking membership in A, the same need not be true for the image $f(A)$.
- A second topological ingredient is *Alexander-Lefshetz duality* which relates the Betti numbers of a compact subset K of the sphere $\mathbf{S}^n$ with those of $\mathbf{S}^n - K$.

The case $\Sigma^c_{\mathbb{R},1}$

- Consider a closed semi-algebraic set $S \subset \mathbf{S}^k \times \mathbf{S}^\ell$ be defined by a quantifier free formula $\phi(Y, X)$ and let

$$\pi_Y : \mathbf{S}^k \times \mathbf{S}^\ell \to \mathbf{S}^k$$

  be the projection map along the Y coordinates.
- Then the formula $\Phi(X) = \exists Y \phi(X, Y)$ is satisfied by $\mathbf{x} \in \mathbf{S}^k$ if and only if $b_0(S_\mathbf{x}) \neq 0$, where $S_\mathbf{x} = S \cap \pi_Y^{-1}(\mathbf{x})$. Thus, the problem of deciding the truth of $\Phi(\mathbf{x})$ is reduced to computing a Betti number (the 0-th) of the fiber of S over $\mathbf{x}$.

The case $\Sigma^c_{\mathbb{R},1}$

- Consider a closed semi-algebraic set $S \subset \mathbf{S}^k \times \mathbf{S}^\ell$ be defined by a quantifier free formula $\phi(Y, X)$ and let

$$\pi_Y : \mathbf{S}^k \times \mathbf{S}^\ell \to \mathbf{S}^k$$

be the projection map along the Y coordinates.

- Then the formula $\Phi(X) = \exists Y \phi(X, Y)$ is satisfied by $\mathbf{x} \in \mathbf{S}^k$ if and only if $b_0(S_\mathbf{x}) \neq 0$, where $S_\mathbf{x} = S \cap \pi_Y^{-1}(\mathbf{x})$. Thus, the problem of deciding the truth of $\Phi(\mathbf{x})$ is reduced to computing a Betti number (the 0-th) of the fiber of S over $\mathbf{x}$.

The case $\Pi^{c}_{\mathbb{R},1}$

- Using the same notation as before we have that the formula $\Psi(X) = \forall Y \phi(X, Y)$ is satisfied by $\mathbf{x} \in \mathbf{S}^k$ if and only if $b_0(\mathbf{S}^\ell \setminus S_{\mathbf{x}}) = 0$ which is equivalent to $b_\ell(S_{\mathbf{x}}) = 1$ (by Alexander duality).
- Notice, that as before the problem of deciding the truth of $\Psi(\mathbf{x})$ is reduced to computing a Betti number (the ℓ-th) of the fiber of S over $\mathbf{x}$.

The case $\Pi^c_{\mathbb{R},1}$

- Using the same notation as before we have that the formula $\Psi(X) = \forall Y \phi(X,Y)$ is satisfied by $\mathbf{x} \in \mathbf{S}^k$ if and only if $b_0(\mathbf{S}^\ell \setminus S_\mathbf{x}) = 0$ which is equivalent to $b_\ell(S_\mathbf{x}) = 1$ (by Alexander duality).
- Notice, that as before the problem of deciding the truth of $\Psi(\mathbf{x})$ is reduced to computing a Betti number (the ℓ-th) of the fiber of S over $\mathbf{x}$.

Slightly more non-trivial case: $\Pi^c_{\mathbb{R},2}$

- Let $S \subset \mathbf{S}^k \times \mathbf{S}^\ell \times \mathbf{S}^m$ be a closed semi-algebraic set defined by a quantifier-free formula $\phi(X, Y, Z)$ and let

  $$\pi_Z : \mathbf{S}^k \times \mathbf{S}^\ell \times \mathbf{S}^m \to \mathbf{S}^k \times \mathbf{S}^\ell$$

  be the projection map along the Z variables, and

  $$\pi_Y : \mathbf{S}^k \times \mathbf{S}^\ell \to \mathbf{S}^k$$

  be the projection map along the Y variables as before.
- Consider the formula $\Phi(X) = \forall Y \exists Z \phi(X, Y, Z)$.
- For $\mathbf{x} \in \mathbf{S}^k$, $\Phi(\mathbf{x})$ is true if and only if $\pi_Z(S)_\mathbf{x} = \mathbf{S}^\ell$, which is equivalent to $b_\ell(D^{\ell+1}_{\pi_Z}(S)_\mathbf{x}) = 1$.

Slightly more non-trivial case: $\Pi^c_{\mathbb{R},2}$

- Let $S \subset \mathbf{S}^k \times \mathbf{S}^\ell \times \mathbf{S}^m$ be a closed semi-algebraic set defined by a quantifier-free formula $\phi(X, Y, Z)$ and let

$$\pi_Z : \mathbf{S}^k \times \mathbf{S}^\ell \times \mathbf{S}^m \to \mathbf{S}^k \times \mathbf{S}^\ell$$

be the projection map along the Z variables, and

$$\pi_Y : \mathbf{S}^k \times \mathbf{S}^\ell \to \mathbf{S}^k$$

be the projection map along the Y variables as before.

- Consider the formula $\Phi(X) = \forall Y \exists Z \phi(X, Y, Z)$.
- For $\mathbf{x} \in \mathbf{S}^k$, $\Phi(\mathbf{x})$ is true if and only if $\pi_Z(S)_\mathbf{x} = \mathbf{S}^\ell$, which is equivalent to $b_\ell(D^{\ell+1}_{\pi_Z}(S)_\mathbf{x}) = 1$.

Slightly more non-trivial case: $\Pi^c_{\mathbb{R},2}$

- Let $S \subset \mathbf{S}^k \times \mathbf{S}^\ell \times \mathbf{S}^m$ be a closed semi-algebraic set defined by a quantifier-free formula $\phi(X, Y, Z)$ and let

$$\pi_Z : \mathbf{S}^k \times \mathbf{S}^\ell \times \mathbf{S}^m \to \mathbf{S}^k \times \mathbf{S}^\ell$$

  be the projection map along the Z variables, and

$$\pi_Y : \mathbf{S}^k \times \mathbf{S}^\ell \to \mathbf{S}^k$$

  be the projection map along the Y variables as before.
- Consider the formula $\Phi(X) = \forall Y \exists Z \phi(X, Y, Z)$.
- For $\mathbf{x} \in \mathbf{S}^k$, $\Phi(\mathbf{x})$ is true if and only if $\pi_Z(S)_{\mathbf{x}} = \mathbf{S}^\ell$, which is equivalent to $b_\ell(D^{\ell+1}_{\pi_Z}(S)_{\mathbf{x}}) = 1$.

The case : $\Pi^{c}_{\mathbb{R},2}$ (cont.)

- Thus for any $\mathbf{x} \in \mathbf{S}^k$, the truth or falsity of $\Phi(\mathbf{x})$ is determined by a certain Betti number of the fiber $D^{\ell+1}_{\pi_Z}(S)_{\mathbf{x}}$ over $\mathbf{x}$ of a certain semi-algebraic set $D^{\ell+1}_{\pi_Z}(S)$ which can be constructed efficiently in terms of the set S.

In general ...

The idea behind the proof of the main theorem is a recursive application of the above argument in case when the number of quantifier alternations is larger (but still bounded by some constant) while keeping track of the growth in the sizes of the intermediate formulas and also the number of quantified variables.