TECHNISCHE UNIVERSITÄT DARMSTADT

Mathematik

Satisfiability over Cross Product is $\mathcal{NP}_{\mathbb{R}}^{\circ}$-complete

TECHNISCHE UNIVERSITÄT DARMSTADT

Christian Herrmann, Johanna Sokoli, Martin Ziegler

Reminder: Complexity Theory

$\mathcal{P} := \{ L \subseteq \{0,1\}^* \text{ decidable in polynomial time } \}$
$\subseteq \mathcal{NP} := \{ L \textbf{ verifiable} \text{ in polynomial time } \}$
$\subseteq \mathcal{PSPACE} := \{ L \text{ decidable in polyn. space } \}$

Def: Call L verifiable in polynomial time if

$$L = \{ \underline{x} \in \{0,1\}^n \mid n \in \mathbb{N}, \exists \underline{y} \in \{0,1\}^{q(n)} : \langle \underline{x}, \underline{y} \rangle \in V \}$$

discrete *"witness"*

for some $V \in \mathcal{P}$ and $q \in \mathbb{N}[N]$.

Examples:

2SAT = { $\langle \Phi \rangle$: Boolean formula Φ in **2**-CNF admits a satisfying assignment } $\in \mathcal{P} \in \mathcal{NP}$

3COL = { $\langle G \rangle$: graph G admits a 3-coloring} $\in \mathcal{NP}$

HC = {$\langle G \rangle$: G has a Hamiltonian cycle} $\in \mathcal{NP}$

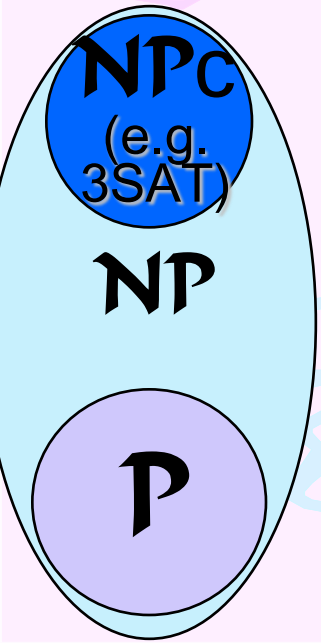
EC = {$\langle G \rangle$: G has a Eulerian cycle } $\in \mathcal{P} \in \mathcal{NP}$

Reminder: $\mathcal{NP}$-completeness

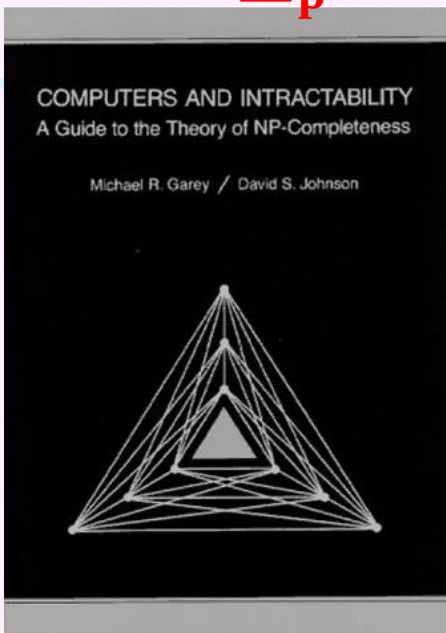
$\mathcal{P} := \{ L \subseteq \{0,1\}^* \text{ decidable in polynomial time } \}$
$\subseteq \mathcal{NP} := \{ L \textbf{ verifiable} \text{ in polynomial time } \}$

Def: Polynom. reduction from A to $B \subseteq \{0,1\}^*$ is a $f: \{0,1\}^* \to \{0,1\}^*$ computab. in polytime such that $x \in A \Leftrightarrow f(x) \in B$.

Write $A \preceq_p B$.



- $A \preceq_p B,\ B \preceq_p C \Rightarrow A \preceq_p C$
- $A \preceq_p B,\ B \in \mathcal{P} \Rightarrow A \in \mathcal{P}$
- For any $L \in \mathcal{NP}$, $L \preceq_p$ SAT (S. Cook / L. Levin 70ies)
- SAT $\preceq_p$ 3SAT, HC, 3COL...



Turing vs. BSS Machine

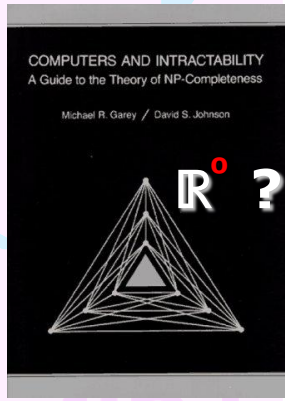
Discrete: Turing Machine / Random-Access Machine (TM/RAM)

Input/output: finite sequence of bits $\{0,1\}^*$ or integers $\mathbb{Z}^*$

Each memory cell holds one element of $R=\{0,1\}$ / $R=\mathbb{Z}$

~~`Program' can store finitely many constants from R~~

operates on R (for TM: $\vee, \wedge, \neg$; for RAM: $+, -, \times, <$)



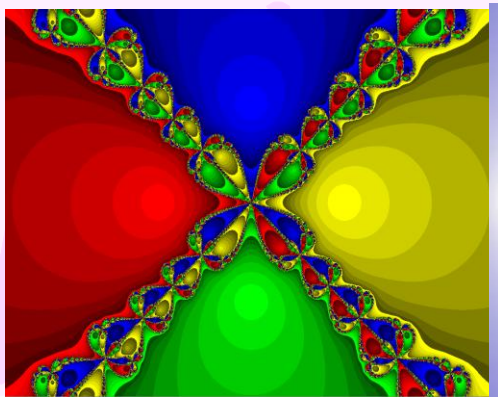
Computation on algebras/structures **[Tucker&Zucker], [Poizat]**

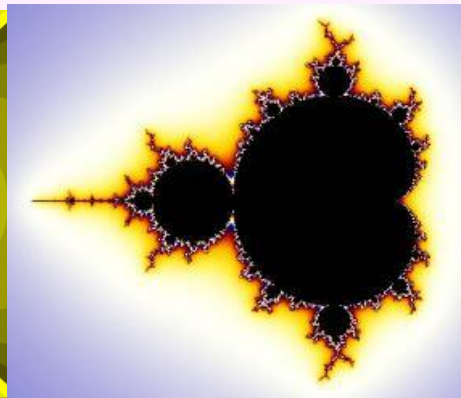
on $\mathbb{R}^* := \bigcup_k \mathbb{R}^k$: Algebra $(\mathbb{R},+,-,\times,\div,<)$ → real-RAM, BSS-machine

[Blum&Shub&Smale'89], [Blum&Cucker&Shub&Smale'98]

$\mathcal{P}^o_{\mathbb{R}} \subseteq \mathcal{NP}^o_{\mathbb{R}} \subseteq \mathcal{EXP}^o_{\mathbb{R}}$ (Tarski Quantifier Elimination) strict?

$\mathcal{NP}^o_{\mathbb{R}}$-complete: *Does a given real polynom.system have a real root?*





$\mathbb{H} \subseteq \mathbb{R}^*$ real Halting problem

Undecidable, too: Mandelbrot Set, Newton starting points

Turing vs. BSS Complexity

$\mathcal{NP}_{\mathbb{R}}^{\circ}$-complete: *Does a given multivariate integer polynomial have a real root?*

Theorem [Canny'88, Grigoriev'88, Heintz&Roy&Solerno'90, Renegar'92]: $\mathcal{NP}_{\mathbb{R}}^{\circ} \subseteq \mathcal{PSPACE}$ ("efficient real quantifier elimination")

No 'better' (e.g. in $\mathcal{PH}$) algorithm known to-date!

(Allender, Bürgisser, Kjeldgaard-Pedersen, Miltersen'06: $\mathcal{P}_{\mathbb{R}}^{\circ} \subseteq \mathcal{CH}$)

Similarly with integer root: undecidable (Matiyasevich'70)

Similarly with rational root: unknown (e.g. Poonen'09)

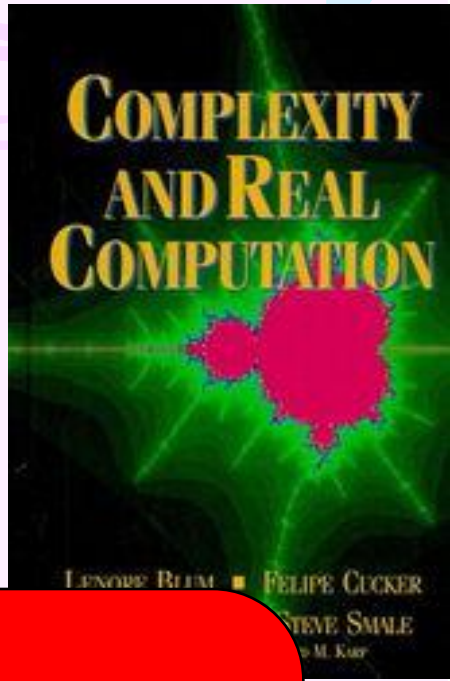
Simil. with complex root: $coRP^{NP}$ mod **GRH** (Koiran'96)

$\mathcal{NP}^0_{\mathbb{R}}$–Completeness

$\mathbf{QSAT}^0_{\mathbb{R}}$: Given a term $t(X_1,..X_n)$ over $\vee,\wedge,\neg$, does it have a satisfying assignment over subspaces of $\mathbb{R}^3/\mathbb{C}^3$? C.Herrmann& M.Z. 2011

$\mathbf{FEAS}^0_{\mathbb{R}}$: Given a system of n-variate integer polynomial in-/equalities, does it have a real solution?

$\mathbf{CONV}^0_{\mathbb{R}}$: …, is the solution set convex?



DI

Q

Today:

The following problem is $\mathcal{NP}^0_{\mathbb{R}}$-complete:

Given a term $t(X_1,\ldots X_n)$ over × only,

does the equation $t(X_1,\ldots X_n) = X_1$

have a solution over $\mathbb{R}^3\backslash\{0\}$?

t'99

r'91

- Certain geometric properties of graphs … 2010

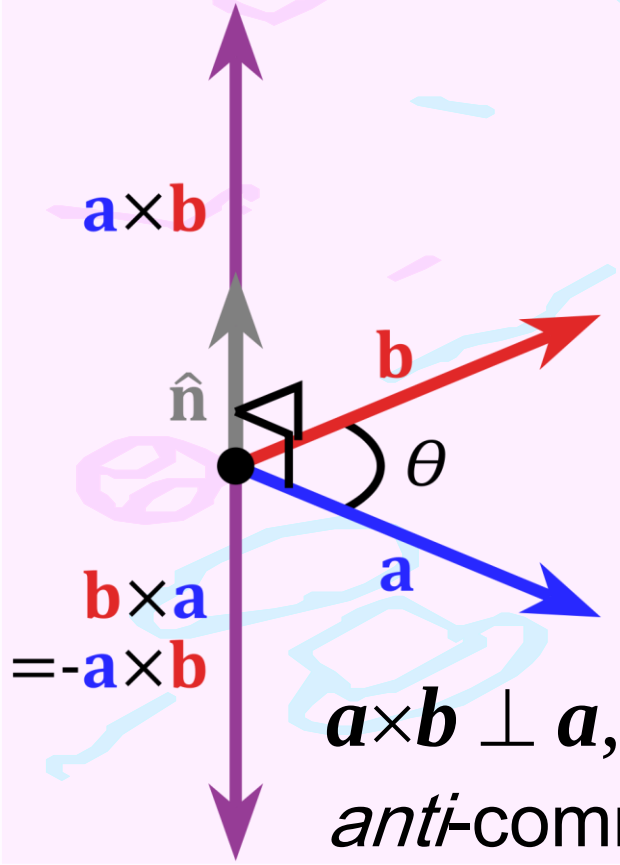
Cross Product in $\mathbb{R}^3$

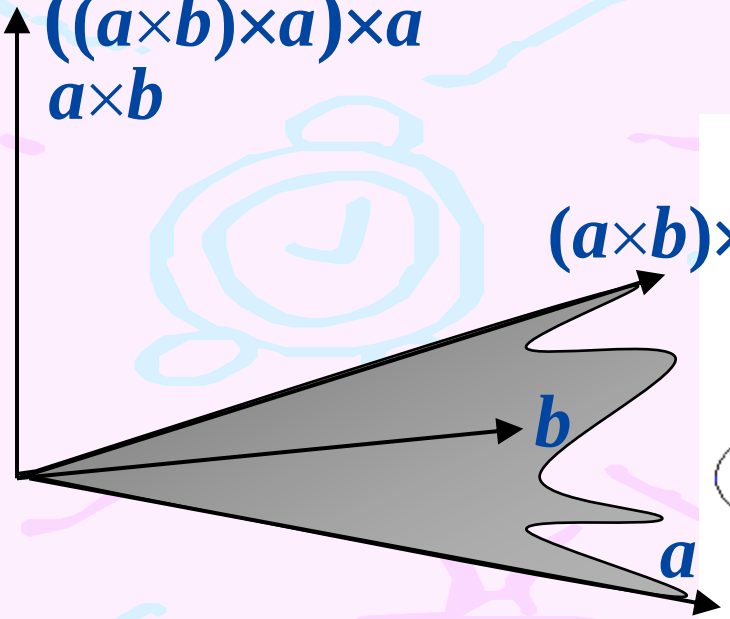
$$(a_x,a_y,a_z)\times(b_x,b_y,b_z) = (a_y\cdot b_z - a_z\cdot b_y,\ a_z\cdot b_x - a_x\cdot b_z,\ a_x\cdot b_y - a_y\cdot b_z)$$

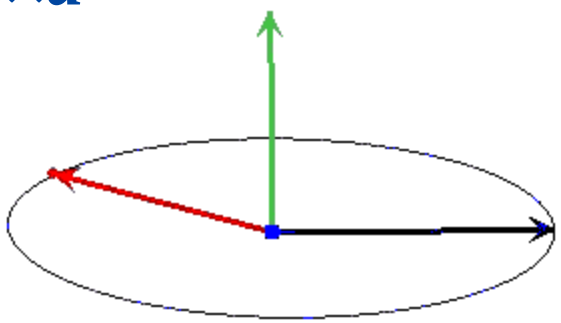
$\boldsymbol{a}\approx\boldsymbol{b}$ (parallel)

$\Rightarrow\ \boldsymbol{a}\times\boldsymbol{b} = \boldsymbol{0}$

$$(((a\times b)\times a)\times a)\times(a\times b) = 0$$







$\boldsymbol{a}\times\boldsymbol{b} \perp \boldsymbol{a}$, $|\boldsymbol{a}\times\boldsymbol{b}| = |\boldsymbol{a}|\cdot|\boldsymbol{b}|\cdot\sin\angle(\boldsymbol{a},\boldsymbol{b})$

anti-commutative, *non*-associative.

Decision Problems with Cross Product

Theorem: a) to c) and a') to b') are all equivalent to **Polynomial Identity Testing** $\in \mathcal{RP}$ (*randomized polytime with one-sided error,* Schwartz-Zippel)

d) to f) are all $\mathcal{NP}^0_{\mathbb{R}}$-complete

d') to f') are equivalent to Hilbert's 10th Problem over $\mathbb{Q}$

In particular there exists a cross product equation $t(\boldsymbol{v}_1,..\boldsymbol{v}_n)=\boldsymbol{v}_1\neq\mathbf{0}$ satisfiable over $\mathbb{R}^3$ but not over $\mathbb{Q}^3$.

c) Is there an assignment $\boldsymbol{v}_j\in\mathbb{R}^3$ s.t. $t(\boldsymbol{v}_1,..\boldsymbol{v}_n)=\mathbf{e}_z$?

d) Is there an assignment $\boldsymbol{v}_j\in\mathbb{R}^3$ s.t. $t(\boldsymbol{v}_1,..\boldsymbol{v}_n)=\boldsymbol{v}_1\neq\mathbf{0}$?

e) Is there an assignment $\boldsymbol{v}_j\in\mathbb{R}^3$ s.t. $t(\boldsymbol{v}_1,..)\approx\boldsymbol{v}_1\neq\mathbf{0}$?

f) Is there an assignment $\boldsymbol{v}_j\in\mathbb{R}^3$ s.t. $t(\boldsymbol{v}_1,..\boldsymbol{v}_n)\approx s(\boldsymbol{v}_1,..\boldsymbol{v}_n)$?

a') to f') similarly but for assignments $\in\mathbb{Q}^3$

Proof (Sketch, hardness)

$\mathrm{QUAD}^0_{\mathbb{R}}$ (Does given $p \in \mathbb{Z}[X_1,..X_n]$ have a real root?) $\preceq_p$ e)

e) Is there an assignment $\boldsymbol{v}_j \in \mathbb{F}^3$ s.t. $t(\boldsymbol{v}_1,..\boldsymbol{v}_n) \approx \boldsymbol{v}_1 \neq \mathbf{0}$?

For any right-handed ortho*g*onal basis $\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3$ of $\mathbb{F}^3$ and for $r,s \in \mathbb{F}$, the following are easily verified:

- $(\mathbf{e}_1 - r\cdot s\,\mathbf{e}_2) = \mathbf{e}_3 \times [\,(\mathbf{e}_3 - r\cdot\mathbf{e}_2) \times (\mathbf{e}_1 - s\cdot\mathbf{e}_3)\,]$
- $(\mathbf{e}_1 - s\cdot\mathbf{e}_3) = \mathbf{e}_2 \times [\,(\mathbf{e}_2 - \mathbf{e}_3) \times (\mathbf{e}_1 - s\cdot\mathbf{e}_2)\,]$
- $-(\mathbf{e}_3 - s\cdot\mathbf{e}_2) = \mathbf{e}_1 \times [\,(\mathbf{e}_1 - \mathbf{e}_3) \times (\mathbf{e}_1 - r\cdot\mathbf{e}_2)\,]$
- $\mathbf{e}_1 - (r-s)\cdot\mathbf{e}_2 = \mathbf{e}_3 \times [\,(\,[(\mathbf{e}_2 - \mathbf{e}_3) \times (\mathbf{e}_1 - r\cdot\mathbf{e}_2)] \times [\,\mathbf{e}_2 \times (\mathbf{e}_1 - s\,\mathbf{e}_3)\,]\,) \times \mathbf{e}_3]$
- $(\mathbf{e}_1 - \mathbf{e}_3) = \mathbf{e}_2 \times [\,-(\mathbf{e}_1 - \mathbf{e}_2) \times (\mathbf{e}_2 - \mathbf{e}_3)\,]$

Encode $s \in \mathbb{F}$ as projective point $\mathbb{F}(\mathbf{e}_1 - s\cdot\mathbf{e}_2)$

Can thus express the arithmetic operations $\cdot$ and $-$ using the cross product and $\mathbf{e}_1$ and $\mathbf{e}_2$ and $(\mathbf{e}_1 - \mathbf{e}_2)$ and $(\mathbf{e}_2 - \mathbf{e}_3)$.

Proof (Sketch, hardness)

$\mathrm{QUAD}^0_{\mathbb{R}}$ (Does given $p \in \mathbb{Z}[X_1,..X_n]$ have a real root?) $\preceq_p$ e)

e) Is there an assignment $\boldsymbol{v}_j \in \mathbb{F}^3$ s.t. $t(\boldsymbol{v}_1,..\boldsymbol{v}_n) \approx \boldsymbol{v}_1 \neq \mathbf{0}$?

For any right-handed orthogonal basis $\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3$ of $\mathbb{F}^3$, can express $-$ and $\cdot$ using cross product and $\mathbb{F}\mathbf{e}_1$ and $\mathbb{F}\mathbf{e}_2$ and $\mathbb{F}(\mathbf{e}_1\text{-}\mathbf{e}_2)$ and $\mathbb{F}(\mathbf{e}_2\text{-}\mathbf{e}_3)$.

Encode $s \in \mathbb{F}$ as projective point $\mathbb{F}(\mathbf{e}_1\text{-}s\cdot\mathbf{e}_2)$

→ terms $V_1(A,B,C)$, $V_2(A,B,C)$, $V_{12}(A,B,C)$, $V_{23}(A,B,C)$ that for any assignment $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C} \in \mathbf{P}^2\mathbb{F}$, *either* coincide with $\mathbb{F}\mathbf{e}_1=\boldsymbol{A}$ and $\mathbb{F}\mathbf{e}_2$ and $\mathbb{F}(\mathbf{e}_1\text{-}\mathbf{e}_2)$ and $\mathbb{F}(\mathbf{e}_2\text{-}\mathbf{e}_3)$ for *some* right-handed orthogonal basis $\mathbf{e}_i$ – *or* evaluate to $\mathbf{0}$.

Using these terms, one can express (in polytime) any given $p \in \mathbb{Z}[X_1,\ldots,X_n]$ as term $t_p(Y_1,\ldots,Y_n;A,B,C)$ over $\times$ s.t. $p(s_1,\ldots,s_n)=0 \Leftrightarrow t_p(\mathbb{F}(\mathbf{e}_1\text{-}s_1\cdot\mathbf{e}_2),\ldots,\mathbb{F}(\mathbf{e}_1\text{-}s_n\cdot\mathbf{e}_2);\boldsymbol{A},\boldsymbol{B},\boldsymbol{C})=\boldsymbol{A}$

Conclusion

- Identified a new problem complete for $\mathcal{NP}^{0}_{\mathbb{R}}$
- defined over $\times$ only, i.e. conceptionally simplest
- normal form for equations over $\times$: $t(Z_1,\ldots,Z_n)=Z_1$

$\mathcal{NP}^{0}_{\mathbb{R}}$ is an important Turing (!) complexity class as $\mathcal{NP}$ currently developping into similarly rich structural theory
[Baartse&Meer'13] *PCP Theorem for $\mathcal{NP}$ over the Reals*

Question: **Graph Coloring** being $\mathcal{NP}$-complete, how about ***Quantum* Graph Coloring**? [LeGall'13]

Using these terms, one can express (in polytime) any given $p\in\mathbb{Z}[X_1,\ldots,X_n]$ as term $t_p(Y_1,\ldots,Y_n;A,B,C)$ over $\times$ s.t. $p(s_1,\ldots,s_n)=0 \;\Leftrightarrow\; t_p(\mathbb{F}(\mathbf{e}_1\text{-}s_1\cdot\mathbf{e}_2),\ldots,\mathbb{F}(\mathbf{e}_1\text{-}s_n\cdot\mathbf{e}_2);\boldsymbol{A},\boldsymbol{B},\boldsymbol{C})=\boldsymbol{A}$