The Cardinality of an Oracle in Blum-Shub-Smale Computation

Russell Miller

Queens College & CUNY Graduate Center
New York, NY.

Seventh International CCA Conference
Jiangsu University
Zhenjiang, China, 23 June 2010

(Joint work with Wesley Calvert, Murray State University, and Ken Kramer, CUNY.)

Slides available at
`qc.edu/~rmiller/slides.html`

BSS Computation on $\mathbb{R}$

Roughly, a BSS machine M on $\mathbb{R}$ operates like a Turing machine, but with a real number in each cell, rather than a bit.

- M can compute full-precision $+$. $-$. $\cdot$, and $\div$ on numbers in its cells.
- M can compare 0 to the number in any cell, using $=$ or $<$, and fork according to the answer.
- M is allowed finitely many real numbers $z_0, \ldots, z_m$ as *parameters* in its program. The input and output (if M halts) are tuples $\vec{y} \in \mathbb{R}^\infty = \{$ finite tuples from $\mathbb{R}$ $\}$.

A subset $S \subseteq \mathbb{R}^\infty$ is BSS-*decidable* iff its characteristic function χ_S is computable by a BSS machine, and BSS-*semidecidable* iff S is the domain of some BSS-computable function.

Basic Facts about BSS Computation

For a machine M with parameters $\vec{z}$, running on input $\vec{y}$, only elements of the field $\mathbb{Q}(\vec{z}, \vec{y})$ can ever appear in the cells of M.

Cell: 0	$\cdots$	m	$m+1$	$\cdots$	$m+n$	$m+n+1$	$\cdots$
z_0	$\cdots$	z_m	y_1	$\cdots$	y_n		
z_0	$\cdots$	z_m	y_1	$\cdots$	y_n	$z_m + y_n$	
$\vdots$		$\vdots$	$\vdots$		$\vdots$	$\vdots$	
$f_{0,s}(\vec{y})$	$\cdots$	$f_{m,s}(\vec{y})$	$f_{m+1,s}(\vec{y})$	$\cdots$	$f_{m+n,s}(\vec{y})$	$f_{m+n+1,s}(\vec{y})$	$\cdots$
$\vdots$		$\vdots$	$\vdots$		$\vdots$	$\vdots$	

Basic Facts about BSS Computation

For a machine M with parameters $\vec{z}$, running on input $\vec{y}$, only elements of the field $\mathbb{Q}(\vec{z}, \vec{y})$ can ever appear in the cells of M.

Cell: 0	$\cdots$	m	$m+1$	$\cdots$	$m+n$	$m+n+1$	$\cdots$
z_0	$\cdots$	z_m	y_1	$\cdots$	y_n		
z_0	$\cdots$	z_m	y_1	$\cdots$	y_n	$z_m + y_n$	
$\vdots$		$\vdots$	$\vdots$		$\vdots$	$\vdots$	
$f_{0,s}(\vec{y})$	$\cdots$	$f_{m,s}(\vec{y})$	$f_{m+1,s}(\vec{y})$	$\cdots$	$f_{m+n,s}(\vec{y})$	$f_{m+n+1,s}(\vec{y})$	$\cdots$
$\vdots$		$\vdots$	$\vdots$		$\vdots$	$\vdots$	

For each input $\vec{y}$, every $f_{i,s}(Y_1, \ldots, Y_n)$ is a rational function with coefficients from the field $\mathbb{Q}(\vec{z})$. If the input $\{y_1, \ldots, y_n\}$ is algebraically independent over $\mathbb{Q}(\vec{z})$, then each $f_{i,s}(\vec{Y})$ is uniquely defined.

Restrictions on BSS Computation

Given a machine M with parameters $\vec{z}$, choose any input $\vec{y}$ algebraically independent over $\mathbb{Q}(\vec{z})$. If $M(\vec{y})$ halts after t steps, then only finitely many functions $f_{i,s}$ appear. So there is an $\epsilon > 0$ such that for all inputs $\vec{x}$ within ϵ of $\vec{y}$, M at stage s contains:

$f_{0,s}(\vec{x})$	$\cdots$	$f_{m,s}(\vec{x})$	$f_{m+1,s}(\vec{x})$	$\cdots$	$f_{m+n,s}(\vec{x})$	$f_{m+n+1,s}(\vec{x})$	$\cdots$

with the same functions $f_{i,s}$ as for $\vec{y}$.
Therefore, on an ϵ-ball around $\vec{y}$ in $\mathbb{R}^n$, M always halts after t steps, and computes the function $\langle f_{0,t}(\vec{x}), \ldots, f_{m+n+t,t}(\vec{x})\rangle$.

Restrictions on BSS Computation

Given a machine M with parameters $\vec{z}$, choose any input $\vec{y}$ algebraically independent over $\mathbb{Q}(\vec{z})$. If $M(\vec{y})$ halts after t steps, then only finitely many functions $f_{i,s}$ appear. So there is an $\epsilon > 0$ such that for all inputs $\vec{x}$ within ϵ of $\vec{y}$, M at stage s contains:

$f_{0,s}(\vec{x})$	$\cdots$	$f_{m,s}(\vec{x})$	$f_{m+1,s}(\vec{x})$	$\cdots$	$f_{m+n,s}(\vec{x})$	$f_{m+n+1,s}(\vec{x})$	$\cdots$

with the same functions $f_{i,s}$ as for $\vec{y}$.
Therefore, on an ϵ-ball around $\vec{y}$ in $\mathbb{R}^n$, M always halts after t steps, and computes the function $\langle f_{0,t}(\vec{x}), \ldots, f_{m+n+t,t}(\vec{x})\rangle$.

Corollary: No BSS-decidable set can be dense and codense within any nonempty open subset of $\mathbb{R}^n$.

Oracle BSS-Machines

To do the same for a machine M with parameters $\vec{z}$ and an *oracle* $C \subseteq \mathbb{R}^\infty$, we would have to ensure that $|\vec{x} - \vec{y}| < \epsilon$ and also, for all s,

$$(\forall i_0, \ldots, i_m) \left[\langle f_{i_k,s}(\vec{x}) \ : \ k \leq m \rangle \in C \iff \langle f_{i_k,s}(\vec{y}) \ : \ k \leq m \rangle \in C \right].$$

Then the computation will fork exactly the same for $\vec{x}$ as for $\vec{y}$, and will output $\langle f_{i,t}(\vec{x}) \rangle$.

Oracle BSS-Machines

To do the same for a machine M with parameters $\vec{z}$ and an *oracle* $C \subseteq \mathbb{R}^\infty$, we would have to ensure that $|\vec{x} - \vec{y}| < \epsilon$ and also, for all s,

$$(\forall i_0, \ldots, i_m)\left[\langle f_{i_k,s}(\vec{x}) \ : \ k \leq m\rangle \in C \iff \langle f_{i_k,s}(\vec{y}) \ : \ k \leq m\rangle \in C\right].$$

Then the computation will fork exactly the same for $\vec{x}$ as for $\vec{y}$, and will output $\langle f_{i,t}(\vec{x})\rangle$.

Theorem: Let

$$\mathbb{H} = \{\langle \vec{p}; \vec{x}\rangle : \text{Program } \vec{p} \text{ halts on input } \vec{x}\}$$

be the BSS Halting Problem. If $\chi_{\mathbb{H}}$ is computable by a BSS program with oracle $C \subseteq \mathbb{R}^\infty$, then $|C| = 2^{\aleph_0}$.

This answers a question from Meer and Ziegler.

Proving the Theorem

Assume that the oracle $C \subseteq \mathbb{R}^\infty$ has $|C| < 2^{\aleph_0}$. For any oracle machine M with parameters $\vec{z}$ and oracle C, we claim that M^C does not compute $\chi_{\mathbb{H}}$.

Let p be the program which, on input $\langle a, b \rangle$, halts iff b is algebraic over $\mathbb{Q}(a)$. Fix any $y_0, y_1 \in \mathbb{R}$ algebraically independent over the field E (of size $< 2^{\aleph_0}$) generated by $\vec{z}$ and p and all tuples in C. Let R be the finite set of rational functions $f \in E(Y_0, Y_1)$ such that $f(y_0, y_1)$ appears in a cell during this computation. Fix $n \in \mathbb{N}$ such that each $f \in R$ is a quotient of polynomials of degree $< n$.

Proving the Theorem

Assume that the oracle $C \subseteq \mathbb{R}^\infty$ has $|C| < 2^{\aleph_0}$. For any oracle machine M with parameters $\vec{z}$ and oracle C, we claim that M^C does not compute $\chi_{\mathbb{H}}$.

Let p be the program which, on input $\langle a, b \rangle$, halts iff b is algebraic over $\mathbb{Q}(a)$. Fix any $y_0, y_1 \in \mathbb{R}$ algebraically independent over the field E (of size $< 2^{\aleph_0}$) generated by $\vec{z}$ and p and all tuples in C. Let R be the finite set of rational functions $f \in E(Y_0, Y_1)$ such that $f(y_0, y_1)$ appears in a cell during this computation. Fix $n \in \mathbb{N}$ such that each $f \in R$ is a quotient of polynomials of degree $< n$.

Now $\langle p, y_0, y_1 \rangle \notin \mathbb{H}$, by algebraic independence, so $M^C(p, y_0, y_1) = 0$. We want to choose $\langle p, x_0, x_1 \rangle \in \mathbb{H}$ close to $\langle p, y_0, y_1 \rangle$ to fool M^C into computing $M^C(p, x_0, x_1) = 0$ as well.

Proving the Theorem

Recall: $y_0, y_1 \in \mathbb{R}$ independent over E; finite set $R \subset E(Y_0, Y_1)$; all $f \in R$ have $f = \frac{g}{h}$ of degree $< n$.

Now choose x_0 transcendental over E, and $x_1 = \sqrt[m]{x_0} + q$, with $m > n$ prime and $q \in \mathbb{Q}$ so that x_0, x_1 are sufficiently close to y_0, y_1. So x_1 has degree m over $E(x_0)$. Now for $f = \frac{g}{h} \in R$,

$$f(\vec{x}) = c \in E \implies g(\vec{x}) - ch(\vec{x}) = 0 \implies (g - ch) = 0 \text{ in } E[Y_0, Y_1].$$

So $f = \frac{g}{h} = c$ is constant. Thus

$$f(x_0, x_1) \in E \iff f \text{ is constant} \iff f(y_0, y_1) \in E.$$

So the computation by M^C on input $\langle p, x_0, x_1 \rangle$ follows the same path as on $\langle p, y_0, y_1 \rangle$, and outputs the same answer: $\langle p, x_0, x_1 \rangle \notin \mathbb{H}$. This is wrong!

Shall We Generalize?

When can a countable set decide an uncountable (and co-uncountable) set?

Shall We Generalize?

When can a countable set decide an uncountable (and co-uncountable) set?

Easy answer: $\{x \in \mathbb{R} : x > 0\}$ is BSS-decidable.
(Is there a similar subset of $\mathbb{C}$, for BSS-computation on $\mathbb{C}$?)

Shall We Generalize?

When can a countable set decide an uncountable (and co-uncountable) set?

Easy answer: $\{x \in \mathbb{R} : x > 0\}$ is BSS-decidable.
(Is there a similar subset of $\mathbb{C}$, for BSS-computation on $\mathbb{C}$?)

Indeed, $\{x \in \mathbb{R} : x \in (0, 1]$ & x begins with an even number of 0's$\}$ is BSS-decidable. This is the set

$$\cdots \left[\frac{1}{32}, \frac{1}{16}\right] \cup \left[\frac{1}{8}, \frac{1}{4}\right] \cup \left[\frac{1}{2}, 1\right].$$

Local Bicardinality

Defn.: A set $S \subseteq \mathbb{R}$ is *locally of bicardinality* $\leq \kappa$ if there exist two open subsets U and V of $\mathbb{R}$ with $|\mathbb{R} - (U \cup V)| \leq \kappa$ and $|U \cap S| \leq \kappa$ and $|V \cap \overline{S}| \leq \kappa$.
The *local bicardinality of S* is the least cardinal κ such that S is locally of bicardinality $\leq \kappa$.

So both S and $\overline{S}$ are open, up to a set of size κ. Notice that the open set $(U \cap V)$ is empty, since

$$|U \cap V| \leq |U \cap S| + |V \cap \overline{S}| \leq \kappa.$$

(Question: is there an equivalent but simpler definition?)

Example: The Cantor middle-thirds set has local bicardinality $2^{\aleph_0}$.

Local Bicardinality and Oracle Computation

Thm.: If $C \subseteq \mathbb{R}^\infty$ is an oracle set of infinite cardinality $\kappa < 2^{\aleph_0}$, and $S \subseteq \mathbb{R}$ is a set with $S \leq_{BSS} C$, then S must be locally of bicardinality $\leq \kappa$. The same holds for oracles C of infinite co-cardinality $\kappa < 2^{\aleph_0}$.

Proof: Consider $\chi_S(y) = M^C(y)$ for any y transcendental over the subfield E generated by C. On some open interval $B(y)$, $\chi_s(x) = \chi_s(y)$ for every $x \in B(y)$ transcendental over E, so either $|S \cap B(y)| \leq \kappa$ or $|\overline{S} \cap B(y)| \leq \kappa$. Also, if $B(y) \cap B(y') \neq \emptyset$, then $\chi_S(y) = \chi_S(y')$. So let

$$U = \cup\{B(y) : y \notin S\} \qquad V = \cup\{B(y) : y \in S\}.$$

So $|\overline{U \cup V}| \leq |E| = \kappa$. If we assume all $B(y)$ to have rational end points, then these are both countable unions, and hence $(U \cap S)$ is a countable union of sets $(B(y) \cap S)$ of size $\leq \kappa$; likewise for $(V \cap \overline{S})$.

Complex Numbers

A BSS-machine on $\mathbb{C}$ can perform the field operations, but there is no instruction for deciding whether "$z > 0$." Here the theorem is nicer (and easily proven):

Thm.: If $C \subseteq \mathbb{C}^\infty$ is an oracle set of infinite cardinality κ, and $S \subseteq \mathbb{C}$ with $S \leq_{BSS} C$, then either $|S| \leq \kappa$ or $|\overline{S}| \leq \kappa$. In particular, for all x, y transcendental over C, we have

$$x \in S \iff y \in S.$$

This fails for sets $S \subseteq \mathbb{C}^2$: just consider the BSS-decidable set $\{\langle z, z\rangle : z \in \mathbb{C}\}$. Similarly for subsets of $\mathbb{R}^2$, the theorem on local bicardinality fails. We believe that this can be fixed by considering size-κ unions of Zariski-closed subsets of $\mathbb{C}^2$ and $\mathbb{R}^2$, and generally for $\mathbb{C}^\infty$ and $\mathbb{R}^\infty$.

Other Results

- **Thm.:** Let

$$\mathbb{A}_{=d} = \{y \in \mathbb{R} : y \text{ is algebraic of degree } d \text{ over } \mathbb{Q}\}.$$

Then for all $d \geq 0$, $\mathbb{A}_{=d+1} \not\leq_{BSS} \mathbb{A}_{=d}$. Indeed $\mathbb{A}_{=d+1} \not\leq_{BSS} \cup_{c \leq d} \mathbb{A}_c$.

Other Results

- **Thm.:** Let

$$\mathbb{A}_{=d} = \{y \in \mathbb{R} : y \text{ is algebraic of degree } d \text{ over } \mathbb{Q}\}.$$

  Then for all $d \geq 0$, $\mathbb{A}_{=d+1} \not\leq_{BSS} \mathbb{A}_{=d}$. Indeed $\mathbb{A}_{=d+1} \not\leq_{BSS} \cup_{c \leq d} \mathbb{A}_c$.
- **Prop.:** Let p and r be any positive integers. Then $\mathbb{A}_{=p} \leq_{BSS} \mathbb{A}_{=r}$ if and only if p divides r.

Other Results

- **Thm.:** Let

$$\mathbb{A}_{=d} = \{y \in \mathbb{R} : y \text{ is algebraic of degree } d \text{ over } \mathbb{Q}\}.$$

  Then for all $d \geq 0$, $\mathbb{A}_{=d+1} \not\leq_{BSS} \mathbb{A}_{=d}$. Indeed $\mathbb{A}_{=d+1} \not\leq_{BSS} \cup_{c \leq d} \mathbb{A}_c$.

- **Prop.:** Let p and r be any positive integers. Then $\mathbb{A}_{=p} \leq_{BSS} \mathbb{A}_{=r}$ if and only if p divides r.

- **Prop.:** Let P be the set of all prime numbers in ω and let $S \subseteq P$ and $T \subseteq P$, Then $A_S \leq_{BSS} A_T$ if and only if $S \subseteq T$.
  (Here $\mathbb{A}_S = \cup_{d \in S} \mathbb{A}_{=d}$.)

Other Results

- **Thm.:** Let
$$\mathbb{A}_{=d} = \{y \in \mathbb{R} : y \text{ is algebraic of degree } d \text{ over } \mathbb{Q}\}.$$
Then for all $d \geq 0$, $\mathbb{A}_{=d+1} \not\leq_{BSS} \mathbb{A}_{=d}$. Indeed $\mathbb{A}_{=d+1} \not\leq_{BSS} \cup_{c\leq d}\mathbb{A}_c$.
- **Prop.:** Let p and r be any positive integers. Then $\mathbb{A}_{=p} \leq_{BSS} \mathbb{A}_{=r}$ if and only if p divides r.
- **Prop.:** Let P be the set of all prime numbers in ω and let $S \subseteq P$ and $T \subseteq P$, Then $A_S \leq_{BSS} A_T$ if and only if $S \subseteq T$.
(Here $\mathbb{A}_S = \cup_{d\in S}\mathbb{A}_{=d}$.)
- **Cor.:** There exists a subset $\mathcal{L}$ of the BSS-semidecidable degrees such that $(\mathcal{L}, \leq_{BSS}) \cong (\mathcal{P}(\omega), \subseteq)$.

Online Help

- Introduction to BSS computation:
  L. Blum, F. Cucker, M. Shub, and S. Smale; *Complexity and Real Computation* (Berlin: Springer-Verlag, 1997).
- Relevant papers:
  C. Gassner; A hierarchy below the halting problem for additive machines, *Theory of Computing Systems* **43** (2008) 3–4, 464–470.
  K. Meer & M. Ziegler; An explicit solution to Post's Problem over the reals, *Journal of Complexity* **24** (2008) 3–15.
- Full version of these results, joint with Calvert & Kramer, available at `qc.edu/~rmiller/BSSfull.pdf`
- These slides available at `qc.edu/~rmiller/slides.html`