Noncomputable Functions in the Blum-Shub-Smale Model

Russell Miller

Queens College & CUNY Graduate Center
New York, NY

Logical Approaches to Computational Barriers
Greifswald, Germany, 18 Feb. 2010

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

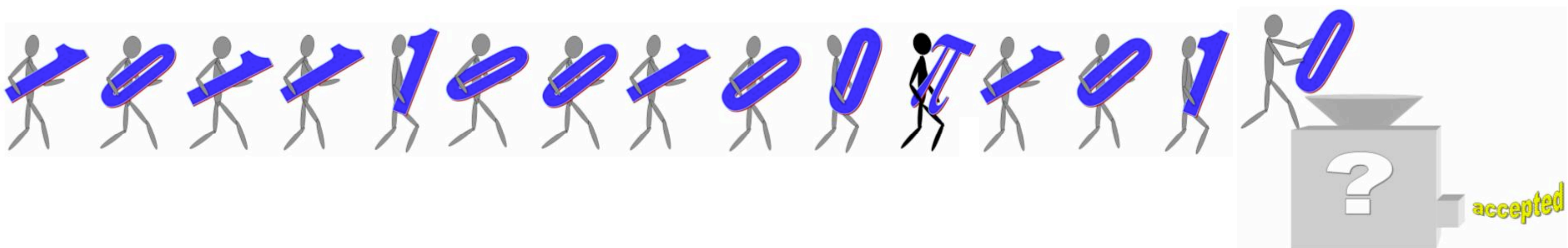
Slides available at
`qc.edu/~rmiller/slides.html`

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.


1 0 1 1 1 0 0 1 0 0 π 1 0 1 0
?
accepted

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 any $\vec{x} \in \mathbb{R}^n$ in an ϵ-ball around $\vec{y}$, 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 any $\vec{x} \in \mathbb{R}^n$ in an ϵ-ball around $\vec{y}$, 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* $A \subseteq \mathbb{R}$, we would have to ensure that $|\vec{x} - \vec{y}| < \epsilon$ and also, for all $f_{i,s}$,

$$f_{i,s}(\vec{x}) \in A \iff f_{i,s}(\vec{y}) \in A.$$

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* $A \subseteq \mathbb{R}$, we would have to ensure that $|\vec{x} - \vec{y}| < \epsilon$ and also, for all $f_{i,s}$,

$$f_{i,s}(\vec{x}) \in A \iff f_{i,s}(\vec{y}) \in A.$$

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

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

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

Proving the Theorem for $d = 1$: $\mathbb{A}_{=2} \not\leq_{BSS} \mathbb{A}_{=1} = \mathbb{Q}$

For any machine M with parameters $\vec{z}$, fix $y \in \mathbb{R}$ transcendental over $\mathbb{Q}(\vec{z})$. Let F be the finite set of rational functions $f(Y)$ over $\mathbb{Q}(\vec{z})$ such that $f(y)$ appears in a cell during this computation.
We pick $x = b + \sqrt{u}$ for some $b, u \in \mathbb{Q}$ with

- $|x - y| < \epsilon$;
- $f'(b) \neq 0$ for all nonconstant $f \in F$, and $u > 0$ small enough that $f(b + \sqrt{u}) \neq f(b - \sqrt{u})$; and
- $\sqrt{u} \notin \mathbb{Q}(\vec{z})$.

So $x = b + \sqrt{u}$ has minimal polynomial $p(X) = X^2 - 2bX + (b^2 - u)$ over $\mathbb{Q}(\vec{z})$, with conjugate $(b - \sqrt{u})$.

Proving the Theorem for $d = 1$: $\mathbb{A}_{=2} \not\leq_{BSS} \mathbb{A}_{=1} = \mathbb{Q}$

For each $f(Y) = \frac{g(Y)}{h(Y)} \in F$, write

$$f(X) = \frac{g(X)}{h(X)} = \frac{q_g(X) \cdot p(X) + r_g(X)}{q_h(X) \cdot p(X) + r_h(X)}$$

with $r_g(X)$ and $r_h(X)$ both linear polynomials. Then

$$\frac{r_g(x)}{r_h(x)} = f(x) = f(b + \sqrt{u}) \neq f(b - \sqrt{u}) = \frac{r_g(b - \sqrt{u})}{r_h(b - \sqrt{u})},$$

so $r_g(X)$ is not a constant multiple of $r_h(X)$ whenever f is nonconstant.

Proving the Theorem for $d = 1$: $\mathbb{A}_{=2} \not\leq_{BSS} \mathbb{A}_{=1} = \mathbb{Q}$

But if $a = f(x) = \frac{r_g(x)}{r_h(x)} = \frac{g_1 \cdot (b+\sqrt{u})+g_0}{h_1(b+\sqrt{u})+h_0}$, then

$$\sqrt{u} = \frac{g_1 b + g_0 - ah_1 b - ah_0}{-(g_1 - ah_1)} \text{ or } g_1 = ah_1.$$

In the first case, $f(x) = a \notin \mathbb{Q}(\vec{z})$ since $\sqrt{u} \notin \mathbb{Q}(\vec{z})$. In the second case, $a = \frac{ah_1 \cdot (b+\sqrt{u})+g_0}{h_1(b+\sqrt{u})+h_0}$, forcing $g_0 = ah_0$, so that

$$r_g(X) = g_1 X + g_0 = ah_1 X + ah_0 = a \cdot r_h(X)$$

and f must have been constant. So

$$f(x) \in \mathbb{Q}(\vec{z}) \iff f \text{ is constant} \iff f(y) \in \mathbb{Q}(\vec{z})$$

and specifically $f(x) \in \mathbb{Q} \iff f(y) \in \mathbb{Q}$.

Proving the Theorem for $d = 1$: $\mathbb{A}_{=2} \not\leq_{BSS} \mathbb{A}_{=1} = \mathbb{Q}$

But if $a = f(x) = \frac{r_g(x)}{r_h(x)} = \frac{g_1 \cdot (b+\sqrt{u})+g_0}{h_1(b+\sqrt{u})+h_0}$, then

$$\sqrt{u} = \frac{g_1 b + g_0 - ah_1 b - ah_0}{-(g_1 - ah_1)} \text{ or } g_1 = ah_1.$$

In the first case, $f(x) = a \notin \mathbb{Q}(\vec{z})$ since $\sqrt{u} \notin \mathbb{Q}(\vec{z})$. In the second case, $a = \frac{ah_1 \cdot (b+\sqrt{u})+g_0}{h_1(b+\sqrt{u})+h_0}$, forcing $g_0 = ah_0$, so that

$$r_g(X) = g_1 X + g_0 = ah_1 X + ah_0 = a \cdot r_h(X)$$

and f must have been constant. So

$$f(x) \in \mathbb{Q}(\vec{z}) \iff f \text{ is constant} \iff f(y) \in \mathbb{Q}(\vec{z})$$

and specifically $f(x) \in \mathbb{Q} \iff f(y) \in \mathbb{Q}$. So the oracle computation on inputs x and y follows the same path and outputs the same answer. But $y \notin \mathbb{A}_{=2}$ and $x = b + \sqrt{u} \in \mathbb{A}_{=2}$.

Other Results

- **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

- **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

- **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 $(\mathcal{L}, \leq_{BSS}) \cong (\mathcal{P}(\omega), \subseteq)$.

Other Results

- **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 $(\mathcal{L}, \leq_{BSS}) \cong (\mathcal{P}(\omega), \subseteq)$.
- **Thm.:** If $C \subseteq \mathbb{R}^\infty$ is a set such that the BSS Halting Problem H satisfies $H \leq_{BSS} C$, then $|C| = 2^\omega$. Indeed $\mathbb{R}$ must have finite transcendence degree over the field generated by the coordinates of the tuples in C.

Other Results

- **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 $(\mathcal{L}, \leq_{BSS}) \cong (\mathcal{P}(\omega), \subseteq)$.
- **Thm.:** If $C \subseteq \mathbb{R}^\infty$ is a set such that the BSS Halting Problem H satisfies $H \leq_{BSS} C$, then $|C| = 2^\omega$. Indeed $\mathbb{R}$ must have finite transcendence degree over the field generated by the coordinates of the tuples in C.
- **Thm.:** If $C \subseteq \mathbb{R}^\infty$ is an oracle set of infinite cardinality $\kappa < 2^\omega$, and $S \subseteq \mathbb{R}$ is a set with $S \leq_{BSS} C$, then S must be locally of bicardinality $\leq \kappa$.

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`