On Time and Space in Higher Order Boolean Circuits

Damiano Mazza
CNRS – Université Paris 13

LCC 2016
Marseille, 2–3 September 2016

Time and Size, Space and Depth

- $(C_n)_{n\in\mathbb{N}}$ circuit family (on $\{\neg, \wedge^2, \vee^2\}$):
  - *size* $s(n) =$ number of gates of C_n;
  - *depth* $d(n) =$ longest path in C_n (seen as a dag).
- Time/size and space/depth are polynomially related:

Theorem (Fisher and Pippenger, 1974; Borodin 1977)

1. $\mathsf{TIME}(f) \subseteq \mathsf{SIZE}(O(f \log f))$
2. $\mathsf{SIZE}(s) \subseteq \mathsf{TIME}(O(s))^*$
3. $\mathsf{NSPACE}(f) \subseteq \mathsf{DEPTH}(O(f^2))$
4. $\mathsf{DEPTH}(d) \subseteq \mathsf{SPACE}(O(d))^*$

*Under some uniformity assumption.

Time and Size, Space and Depth

- $(C_n)_{n\in\mathbb{N}}$ circuit family (on $\{\neg, \wedge^2, \vee^2\}$):
  - *size* $s(n) =$ number of gates of C_n;
  - *depth* $d(n) =$ longest path in C_n (seen as a dag).
- Time/size and space/depth are polynomially related:

Theorem (Fisher and Pippenger, 1974; Borodin 1977)

1. $\mathsf{TIME}(f) \subseteq \mathsf{SIZE}(O(f \log f))$
2. $\mathsf{SIZE}(s) \subseteq \mathsf{TIME}(O(s))^*$
3. $\mathsf{NSPACE}(f) \subseteq \mathsf{DEPTH}(O(f^2))$
4. $\mathsf{DEPTH}(d) \subseteq \mathsf{SPACE}(O(d))^*$

*Under some uniformity assumption.

- What happens in the higher-order world?

Why Do We Care?

- Quantitative program analysis:
  - approximations, CFA;
  - non-idempotent intersection types;
  - implicit computational complexity;
  - higher order circuits?

- The crazy idea that we should be able to study complexity directly in the λ-calculus:
  - cost models;
  - structure vs. efficiency?

Higher-Order Boolean Circuits

- What should a **higher-order Boolean circuit** be?

$$\frac{???}{\lambda\text{-terms}} = \frac{\text{Boolean circuits}}{\text{Turing machines}}$$

Higher-Order Boolean Circuits

- What should a **higher-order Boolean circuit** be?

$$\frac{\text{(affine) linear } \lambda\text{-terms}}{\lambda\text{-terms}} = \frac{\text{Boolean circuits}}{\text{Turing machines}}$$

- Why?
  - May only compute finite functions (like Boolean circuits);
  - runtime is the size (like Boolean circuits);
  - free SMC vs. free SMCC (the meaning of higher-order).

The Polyadic Affine Lambda-Calculus

- A fragment of multiplicative linear logic:

$$A, B ::= \alpha \mid (A_1 \,\&\, 1) \otimes \cdots \otimes (A_n \,\&\, 1) \multimap B$$

- Terms (via Curry-Howard): $t, u ::= x_i \mid \lambda x.t \mid t\mathbf{u}$
  - $i \in \mathbb{N}$, pairwise distinct (linearity);
  - $\mathbf{u} : \mathbb{N} \rightharpoonup \mathrm{Terms}$, of finite domain.

- Reduction: $(\lambda x.t)\mathbf{u} \to t\{\mathbf{u}(i)/x_i\}$ provided $\mathrm{occ}_x(t) \subseteq \mathrm{dom}\,\mathbf{u}$.

- Strongly confluent, strongly terminating (but there may be clashes).

Approximations

- Affine terms may approximate ordinary λ-terms:

$$\frac{}{x_i \sqsubset x} \qquad \frac{t \sqsubset M}{\lambda x.t \sqsubset \lambda x.M} \qquad \frac{t \sqsubset M \quad \mathbf{u}(i) \sqsubset N \quad \forall i \in \mathrm{dom}\,\mathbf{u}}{t\mathbf{u} \sqsubset MN}$$

- Basic properties:
  - **bounded completeness**: $t, t' \sqsubset M$ implies $t \sqcup t' \sqsubset M$ exists;
  - **monotonicity:** $M \sqsupset t \to u$ implies $M \to N \sqsupset u$
  - **continuity**: if $M \to N$ then $\forall u \sqsubset N,\ \exists t \sqsubset M.\ t' \to^* u'$.
  - **fwd. simulation**: $t \sqsubset M \to N$, t clash-free implies $t \to^* u \sqsubset N$.

What Is Time in the λ-calculus?

- Is counting head reduction steps reasonable?
  In spite of size explosion, the answer is **yes**!

  Theorem (Accattoli and Dal Lago, 2012)
  1. $\mathsf{TIME}(f) \subseteq \lambda\mathsf{TIME}(O(f))$
  2. $\lambda\mathsf{TIME}(f) \subseteq \mathsf{TIME}(O(\mathsf{poly}(f))$

  $\lambda\mathsf{TIME}(f) =$ languages decided by λ-terms in $\leq f(n)$ head reduction steps.

- Unfortunately, size explosion is a problem for approximations:

$$\underline{w} : \mathsf{Str} \quad M\underline{w} \to^{l(|w|)} \underline{b} : \mathsf{Bool} \quad \Longrightarrow \quad \exists t \sqsubset M,\ t\underline{w} \to^{*} \underline{b}$$

  but sometimes $|t| = \Theta(2^l)$!

Enter Parsimony

- The parsimonious λ-calculus:

$$M, N ::= a \mid \lambda a.M \mid MN \mid x_i \mid !M \mid \mathsf{let}\, !x = N \,\mathsf{in}\, M$$

$$\mathsf{let}\, !x = !N \,\mathsf{in}\, M\langle x_0 \rangle \quad \to \quad \mathsf{let}\, !x = !N^{++} \,\mathsf{in}\, M^{x--}\langle N \rangle$$

- Intuition: only *linear recursive definitions* available ($e.g.$ `while` loops):

$$\texttt{let rec fun(x)} \;=\; \Phi \quad \longleftarrow \text{ one occurrence of } \texttt{fun}$$

Theorem (M. 2016)

1. $\mathrm{p}\lambda\mathsf{TIME}(f) \subseteq \lambda\mathsf{SIZE}(O(\mathsf{poly}(f)))$
2. $\lambda\mathsf{SIZE}(s) \subseteq \mathsf{TIME}(O(s))^*$

*Under some uniformity assumption.

What About Space?

- Need to account for sublinear complexity $\Rightarrow$ rewriting is useless.
- Ideally: abstract measures, implementation-independent.
- Non-examples: Spoonhower et al. 2008, Blelloch and Harper 2014: need low-level description of λ-terms.
- Our proposal: a mixture of
  - approximations;
  - (non-idempotent) intersection types;
  - geometry of interaction (GoI), as suggested by Schöpp and Dal Lago.

Intersection Types come From Approximations!

¬i,¬c intersection types	polyadic simple types
$A, B ::= \alpha \mid A_1 \cap \cdots \cap A_n \to B$	$A, B ::= \alpha \mid A_1^\bullet \otimes \cdots \otimes A_n^\bullet \multimap B$

- M *intersection-typable iff* M *has a simply-typable linear approximation*.

- **Curry style:**

$$\Gamma \vdash M : A \quad \Longleftrightarrow \quad \exists t \sqsubset M \text{ s.t. } \Gamma \vdash t : A$$

- **Church style:**

$$\delta :: M \quad \Longleftrightarrow \quad \delta^- \sqsubset M$$

Intersection Types come From Approximations!

¬i,¬c intersection types	polyadic simple types
$A, B ::= \alpha \mid A_1 \cap \cdots \cap A_n \to B$	$A, B ::= \alpha \mid A_1^\bullet \otimes \cdots \otimes A_n^\bullet \multimap B$

$$\frac{}{\vec{y} : \langle\rangle, x : \langle \underbrace{*, \ldots, *}_{i}, A\rangle \vdash \qquad x : A}$$

$$\frac{\Gamma, x : \mathbf{A} \vdash \qquad M : B}{\Gamma \vdash \qquad \lambda x.M : \mathbf{A} \to B}$$

$$\frac{\Gamma \vdash \qquad M : \mathbf{A} \to B \qquad \Delta_i \vdash \qquad N : \mathbf{A}(i) \quad \forall i \in \mathrm{dom}\,\mathbf{u} = \mathrm{dom}\,\mathbf{A}}{\Gamma \uplus \biguplus \Delta_i \vdash \qquad MN : B}$$

Intersection Types come From Approximations!

¬i,¬c intersection types	polyadic simple types
$A, B ::= \alpha \mid A_1 \cap \cdots \cap A_n \to B$	$A, B ::= \alpha \mid A_1^\bullet \otimes \cdots \otimes A_n^\bullet \multimap B$

$$\frac{}{\vec{y} : \langle\rangle, x : \langle \underbrace{*, \ldots, *}_{i}, A\rangle \vdash x_i \quad : A}$$

$$\frac{\Gamma, x : \mathbf{A} \vdash t \quad : B}{\Gamma \vdash \lambda x.t \quad : \mathbf{A} \to B}$$

$$\frac{\Gamma \vdash t \quad : \mathbf{A} \to B \qquad \Delta_i \vdash \mathbf{u}(i) \quad : \mathbf{A}(i) \quad \forall i \in \operatorname{dom} \mathbf{u} = \operatorname{dom} \mathbf{A}}{\Gamma \uplus \biguplus \Delta_i \vdash t\mathbf{u} \quad : B}$$

Intersection Types come From Approximations!

¬i,¬c intersection types	polyadic simple types
$A, B ::= \alpha \mid A_1 \cap \cdots \cap A_n \to B$	$A, B ::= \alpha \mid A_1^\bullet \otimes \cdots \otimes A_n^\bullet \multimap B$

$$\frac{}{\vec{y} : \langle\rangle, x : \langle \underbrace{*, \ldots, *}_{i}, A\rangle \vdash x_i \sqsubset x : A}$$

$$\frac{\Gamma, x : \mathbf{A} \vdash t \sqsubset M : B}{\Gamma \vdash \lambda x.t \sqsubset \lambda x.M : \mathbf{A} \to B}$$

$$\frac{\Gamma \vdash t \sqsubset M : \mathbf{A} \to B \qquad \Delta_i \vdash \mathbf{u}(i) \sqsubset N : \mathbf{A}(i) \quad \forall i \in \operatorname{dom} \mathbf{u} = \operatorname{dom} \mathbf{A}}{\Gamma \uplus \biguplus \Delta_i \vdash t\mathbf{u} \sqsubset MN : B}$$

Higher Order Depth and Space

Theorem. *Let*

$$(t_w :: \vdash M : \mathsf{Str}_w \multimap \mathsf{Bool})_{w \in \{0,1\}^*}$$

– Str_w *are instances of* Str *"corresponding" to* w*;*
– $\max_{|w|=n} |t_w| = O(s(n))$, $\max_{|w|=n} \mathrm{depth}(\mathsf{Str}_w) = O(d(n))$.
Then, $\mathrm{lang}(M) \in \mathsf{TIME}(O(|t_n|)) \cap \mathsf{SPACE}(O(d(n) \log |t_n|))$.

Proof. Use the GoI. □

- HO circuit $= t : \mathsf{Str}[] \multimap \mathsf{Bool}$, size $= |t|$, depth $= \mathrm{depth}(\mathsf{Str}[])$.
- Consistent with Terui, 2004; similar to Borodin 1977:

$$\mathsf{DEPTH/SIZE}(d, s) \subseteq \mathsf{TIME}(O(s)) \cap \mathsf{SPACE}(O(d + \log s))$$

Perspectives

- Space in λ-calculus $\sim$ height of intersection types times log of size.
- Pros:
  - yields simply-typed parsimonious terms = L;
  - non-uniformity (novelty in PL);
  - may yield definition of λSPACE (Borodin's theorem $\rightarrow$ definition).
- Cons:
  - need to find *canonical* derivations;
  - dependency on size = time. . .