A Necessary and Sufficient Timing Assumption for Speed-Independent Circuits

Sean Keller\textsuperscript{1}, Michael Katelman\textsuperscript{2}, and Alain J. Martin\textsuperscript{1}

\textsuperscript{1} California Institute of Technology
\textsuperscript{2} University of Illinois at Urbana-Champaign

May 18, 2009
Introduction
  The Question
  Our Approach
  Real World Motivation

Formalization
  Syntax
  Semantics
  Timing Assumptions

Proof
  Overview

⇒

Conclusion
Overview of the Problem

- Gates: $O_x, O_u, O_v$

- Timing assumptions
  - Definition
  - What exactly are timing assumptions
Overview of the Problem

Gates: \( O_x, O_u, O_v \)

- Timing assumptions
  - Definition
  - What exactly are timing assumptions
- Forks
Overview of the Problem

Gates: $O_x, O_u, O_v$

- Timing assumptions
  - Definition
  - What exactly are timing assumptions
- Forks
- Two important assumptions
Overview of the Problem

Timing assumptions
- Definition
- What exactly are timing assumptions

Forks

Two important assumptions
- Strong fork timing assumption (SFTA)

Gates: $O_x, O_u, O_v$
Overview of the Problem

Gates: \( O_x, O_u, O_v \)

- Timing assumptions
  - Definition
  - What exactly are timing assumptions
- Forks
- Two important assumptions
  - Strong fork timing assumption (SFTA)
Overview of the Problem

Gates: $O_x, O_u, O_v$

- Timing assumptions
  - Definition
  - What exactly are timing assumptions
- Forks
- Two important assumptions
  - Strong fork timing assumption (SFTA)
Overview of the Problem

Gates: $O_x, O_u, O_v$

- Timing assumptions
  - Definition
  - What exactly are timing assumptions
- Forks
- Two important assumptions
  - Strong fork timing assumption (SFTA)
  - Adversary path timing assumption (APTA)
Overview of the Problem

Gates: $O_x, O_u, O_v$

- Timing assumptions
  - Definition
  - What exactly are timing assumptions
- Forks
- Two important assumptions
  - Strong fork timing assumption (SFTA)
  - Adversary path timing assumption (APTA)
Overview of the Problem

- Timing assumptions
  - Definition
  - What exactly are timing assumptions
- Forks
- Two important assumptions
  - Strong fork timing assumption (SFTA)
  - Adversary path timing assumption (APTA)
- SFTA and APTA are equivalent w.r.t hazards

Gates: $O_x, O_u, O_v$
A Formal Framework and a Proof

- Formally model digital switching networks directly
- Formal timing assumptions
- Rigorous proof: SFTA and APTA are equivalent
- APTA is the weakest SI timing assumption
- Formal framework: other comparisons, computerized proofs
- Existing work
Violating APTA

▶ Isn’t the SI/QDI timing assumption trivial to satisfy?
  ▶ In the past: yes
  ▶ Today:
Isn’t the SI/QDI timing assumption trivial to satisfy?
  ▶ In the past: yes
  ▶ Today: not always
    ▶ Subthreshold QDI circuits
    ▶ Adversary path length 5: Probability of failure \textit{greater} than 1 in 10K
Isn’t the SI/QDI timing assumption trivial to satisfy?

- In the past: yes
- Today: not always
  - Subthreshold QDI circuits
  - Adversary path length 5: Probability of failure \textit{greater than 1 in 10K}
  - Adversary path length 7: Probability of failure \textit{less than 1 in 2M}
Violating APTA (Continued)

Single Inverter - Delay Distribution - Subthreshold Operation
Extracted Layout in IBM 65nm CMOS10LPe
10,000 Monte Carlo Trials (Process Variation)
Violating APTA (Continued)

Chain of Five Inverters - Delay Distribution - Subthreshold Operation
Extracted Layout in IBM 65nm CMOS10LPe
10,000 Monte Carlo Trials (Process Variation)
Violating APTA (Continued)

Combined - Delay Distribution - Subthreshold Operation
Extracted Layout in IBM 65nm CMOS10LpE
10,000 Monte Carlo Trials (Process Variation)
PRS Syntax

- PRS, a familiar syntax: $g \leftrightarrow x \uparrow$ or $g \leftrightarrow x \downarrow$
- Operators: gates and wires
- An example:

$$\begin{align*}
\neg a'' \lor \neg b & \leftrightarrow x \uparrow \\
a \land b & \leftrightarrow x \downarrow \\
a & \leftrightarrow a' \uparrow \\
\neg a & \leftrightarrow a' \downarrow \\
a' & \leftrightarrow a'' \uparrow \\
\neg a' & \leftrightarrow a'' \downarrow
\end{align*}$$

- Properly structured PRS
A Mapping From PRS to Legal Computations

- An operational semantics
- Every gate and wire is an independent process
A Mapping From PRS to Legal Computations

- An operational semantics
- Every gate and wire is an independent process
- The state of every node is encoded as a function $\chi$
  - $\chi_i(y) = T$
  - The possible node states are $\{T, F, X\}$
A Mapping From PRS to Legal Computations

- An operational semantics
- Every gate and wire is an independent process
- The state of every node is encoded as a function $\chi$
  - $\chi_i(y) = T$
  - The possible node states are $\{T, F, X\}$
- Hazards
  - Instability and Interference
  - Hazards are kept track of with the $I$ set
  - $y \in I_j$ means that $y$ may take on the undefined value $X$ in a subsequent execution step, say $j + 1$
A Mapping From PRS to Legal Computations

- An operational semantics
- Every gate and wire is an independent process
- The state of every node is encoded as a function $\chi$
  - $\chi_i(y) = T$
  - The possible node states are $\{T, F, X\}$
- Hazards
  - Instability and Interference
  - Hazards are kept track of with the $I$ set
  - $y \in I_j$ means that $y$ may take on the undefined value $X$ in a subsequent execution step, say $j + 1$
- Execution Sequence: $\vec{\sigma} = (\chi_0, I_0), (\chi_1, I_1), ...$
Avoiding Hazards

- Intra-operator forks
Avoiding Hazards

- Intra-operator forks
- Acknowledgment: \( x \leftrightarrow_i y \)
Avoiding Hazards

- Intra-operator forks
- Acknowledgment: $x \leftrightarrow_i y$
Avoiding Hazards

- Intra-operator forks
- Acknowledgment: \( x \leftrightarrow_i y \)
Avoiding Hazards

- Intra-operator forks
- Acknowledgment: $x \leftrightarrow_i y$
Avoiding Hazards

- Intra-operator forks
- Acknowledgment: \( x \leftrightarrow_i y \)
Avoiding Hazards

- Intra-operator forks
- Acknowledgment: \( x \leftrightarrow_i y \)
Avoiding Hazards

- Intra-operator forks
- Acknowledgment: $x \leftrightarrow_i y$
- Instability hazard
Avoiding Hazards

- Intra-operator forks
- Acknowledgment: $x \leftrightarrow_i y$
- Instability hazard
- Strong fork timing assumption
Avoiding Hazards

- Intra-operator forks
- Acknowledgment: \( x \leftrightarrow_i y \)
- Instability hazard
- Strong fork timing assumption
- Adversary path timing assumption
Equivalence of SFTA and APTA

Theorem

Whenever SFTA excludes all execution sequences exhibiting hazards then so does APTA and vice versa
Equivalence of SFTA and APTA

Theorem
Whenever SFTA excludes all execution sequences exhibiting hazards then so does APTA and vice versa

Proof.
\(\Leftarrow\) Straightforward

- A hazard under SFTA implies a hazard under APTA
- Every SFTA sequence is also an APTA sequence
Equivalence of SFTA and APTA

Theorem
Whenever SFTA excludes all execution sequences exhibiting hazards then so does APTA and vice versa

Proof.
\(\iff\) Straightforward
- A hazard under SFTA implies a hazard under APTA
- Every SFTA sequence is also an APTA sequence

\(\Rightarrow\) Considerably more difficult
- A hazard under APTA implies a hazard under SFTA
- Take an arbitrary APTA sequence with a hazard and construct an SFTA sequence with a hazard
Constructing the Hazardous SFTA Sequence

- A variant sequence
  - $\vec{\sigma}$ is a hazardous APTA sequence
  - $\vec{\sigma}'$ is an SFTA variant of $\vec{\sigma}$
- $\vec{\sigma}'$ mimics $\vec{\sigma}$ as closely as possible
  - Forks must be handled specially
Fork Relaxations
Fork Relaxations

▶ Relaxation
Fork Relaxations

- Relaxation
- Suppress
Fork Relaxations

- Relaxation
- Suppress
- Force
Some Proof Details

- In a variant, each relaxation must be either *forced* or *suppressed*
- Consider the variant $\vec{\sigma}^+$ where all forks are forced
- Choose a partition of relaxations to generate the hazardous SFTA variant $\vec{\sigma}^-$
- Work out the details of exactly how and where $\vec{\sigma}$ and $\vec{\sigma}^-$ differ and why $\vec{\sigma}^-$ must also have a hazard
Variant $\vec{\sigma}^+$ Example
Variant $\vec{\sigma}^+$ Example
Variant $\vec{\sigma}^+$ Example
Variant $\vec{\sigma}^+$ Example
Variant $\bar{\sigma}^+$ Example

\[\bar{\sigma}\]

\[\bar{\sigma}^+\]
Variant $\bar{\sigma}^+$ Example

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{variant_example}
\caption{Variant $\bar{\sigma}^+$ Example}
\end{figure}
Variant $\bar{\sigma}^+$ Example
Variant $\vec{\sigma}^+$ Example
Variant $\vec{\sigma}^+$ Example
Conclusion

- A common mathematical framework
Conclusion

- A common mathematical framework
- A rigorous proof that SFTA and APTA are equivalent with respect to hazards
Conclusion

- A common mathematical framework
- A rigorous proof that SFTA and APTA are equivalent with respect to hazards
- The adversary path timing assumption is the weakest timing assumption