DOM: Towards a Formal Specification

Author: Mark Wheelhouse

Supervisor: Dr. Philippa Gardner

Thanks to: Gareth Smith, Uri Zarfaty, Ian Hodkinson

DOM (Document Object Model)

Current Spec.

- English
  - Verbose
  - Ambiguous
- Automated Verification
  - Not Possible
- Extensions
  - Hard
  - Time-consuming

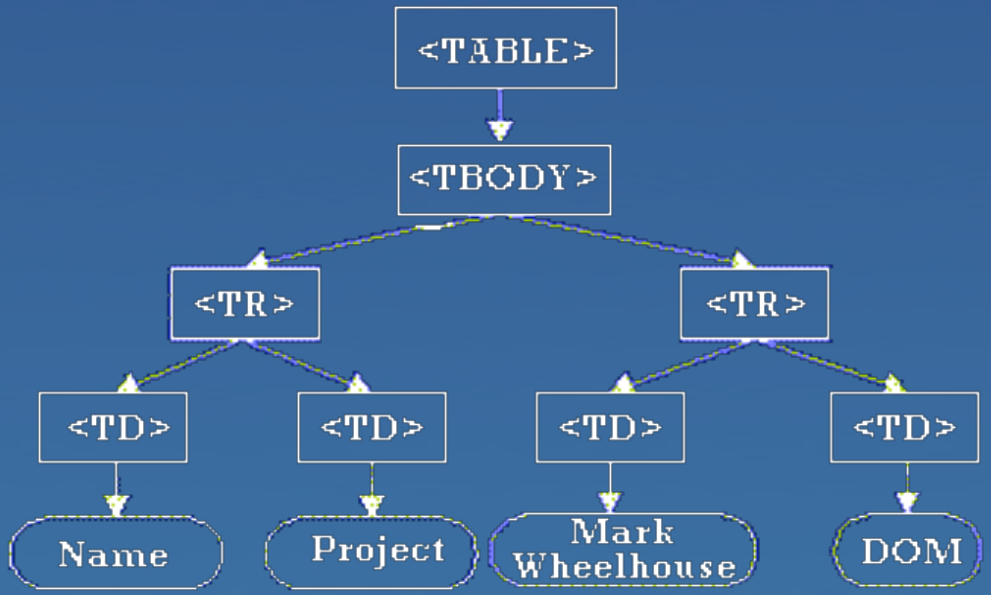
What We Want

- Formalism
  - Data Structure
  - Logical Framework
- Automated Verification
  - Possible
- Extensions
  - Easier
  - Quicker

What is DOM?

- High Level XML Update
- W3C
- Aimed at Object Orientated Programmers
- Stores XML in Tree Structure

DOM Tree



Minimal DOM

DOM Core Level 3

DOM Core Level 2

} Application Based

DOM Core Level 1 – Consider Structural Behaviour Only

Minimal DOM

createNode

getNodeName

getChildNodes

getParentNode

insertBefore

removeChild

append

getLength

getItem

Minimal DOM

createNode

getNodeName

getChildNodes

getParentNode

insertBefore

removeChild

append

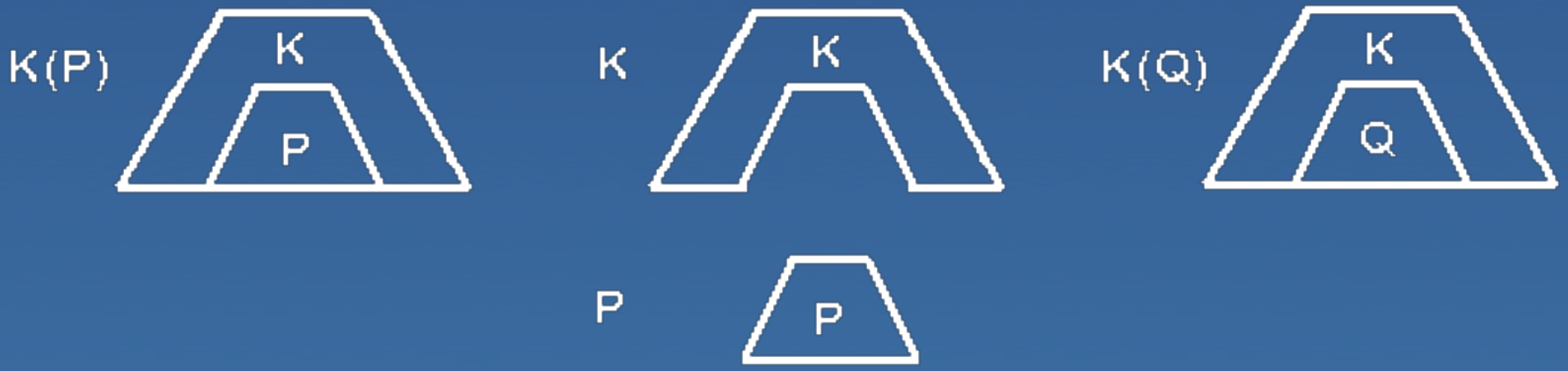
getLength

getItem

Context Logic

- Local Reasoning Tool for Tree Update
- Proved Correct
- Used on Toy Examples
- Provides Compositional Reasoning
- First Real-World Test

Context Logic - Application



Pre: P

Command: C

Post: Q

Context Logic – Right Triangle

$$K = (P \triangleright Q)$$

Data Structure

$$\begin{aligned}
\text{Grove } G &::= \emptyset \mid G \oplus G \mid T \\
\text{Tree } T &::= \mathrm{tag}_{\mathrm{id}}[F]_{\mathrm{fid}} \\
\text{Forest } F &::= \emptyset \mid F \times F \mid T
\end{aligned}$$

$$\begin{aligned}
\text{Grove Context } CG &::= _ \mid CG \oplus G \mid CT \\
\text{Tree Context } CT &::= \mathrm{tag}_{\mathrm{id}}[CF]_{\mathrm{fid}} \\
\text{Forest Context } CF &::= _ \mid CF \times F \mid F \times CF \mid CT
\end{aligned}$$

Command Axioms

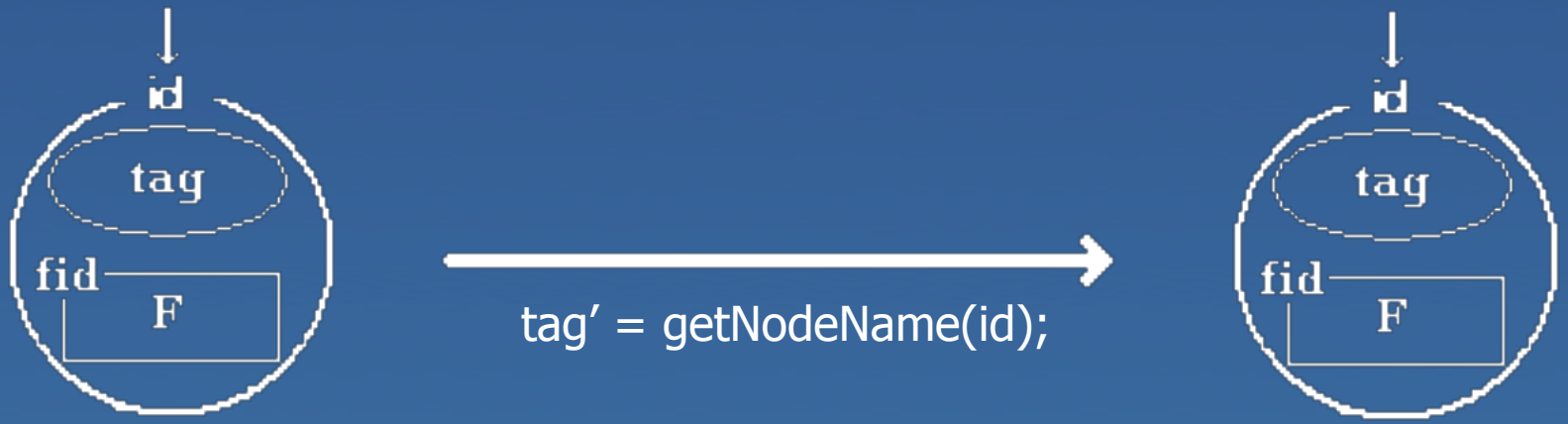
Specifying the Local Behaviour of the commands:

{ Pre-condition }

Command

{ Post-condition }

getNodeName



tag' = tag

getNodeName - Small Axiom

$$\{\mathbf{tag_{node}}[\mathbf{F}]_{\mathbf{fid}}\}$$

$$\mathbf{tag}' = \mathrm{getNodeName}(\mathbf{node});$$

$$\{\mathbf{tag_{node}}[\mathbf{F}]_{\mathbf{fid}} \wedge \mathbf{tag}' = \mathbf{tag}\}$$

Weakest Pre-condition

$$\{\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathfrak{fid}}\}$$

$$\mathrm{tag}' = \mathrm{getNodeName}(\mathrm{node});$$

$$\{\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathfrak{fid}} \wedge \mathrm{tag}' = \mathrm{tag}\}$$

$$\{(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathfrak{fid}} \triangleright P[\mathrm{tag}/\mathrm{tag}'])(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathfrak{fid}})\}$$

$$\mathrm{tag}' = \mathrm{getNodeName}(\mathrm{node});$$

$$\{(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathfrak{fid}} \triangleright P[\mathrm{tag}/\mathrm{tag}'])(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathfrak{fid}} \wedge \mathrm{tag}' = \mathrm{tag})\}$$

Weakest Pre-condition

$$\{(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}} \triangleright P[\mathrm{tag}/\mathrm{tag}'])(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}})\}$$

$$\mathrm{tag}' = \mathrm{getNodeName}(\mathrm{node});$$

$$\{(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}} \triangleright P[\mathrm{tag}/\mathrm{tag}'])(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}} \wedge \mathrm{tag}' = \mathrm{tag})\}$$

$$\{(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}} \triangleright P[\mathrm{tag}/\mathrm{tag}'])(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}})\}$$

$$\mathrm{tag}' = \mathrm{getNodeName}(\mathrm{node});$$

$$\{(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}} \triangleright P[\mathrm{tag}/\mathrm{tag}'])(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}}) \wedge (\mathrm{tag}' = \mathrm{tag})\}$$

Weakest Pre-condition

$$\{(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}} \triangleright P[\mathrm{tag}/\mathrm{tag}'])(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}})\}$$

$$\mathrm{tag}' = \mathrm{getNodeName}(\mathrm{node});$$

$$\{(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}} \triangleright P[\mathrm{tag}/\mathrm{tag}'])(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}}) \wedge (\mathrm{tag}' = \mathrm{tag})\}$$

$$\{\mathrm{True}(\mathrm{tag}_{\mathrm{node}}[\mathbf{F}]_{\mathrm{fid}}) \wedge P[\mathrm{tag}/\mathrm{tag}']\}$$

$$\mathrm{tag}' = \mathrm{getNodeName}(\mathrm{node});$$

$$\{P[\mathrm{tag}/\mathrm{tag}'] \wedge (\mathrm{tag}' = \mathrm{tag})\}$$

Weakest Pre-condition

$$\{\mathrm{True}(\mathrm{tag}_{\mathrm{node}}[\mathrm{F}]_{\mathrm{fid}}) \wedge P[\mathrm{tag}/\mathrm{tag}']\}$$

$$\mathrm{tag}' = \mathrm{getNodeName}(\mathrm{node});$$

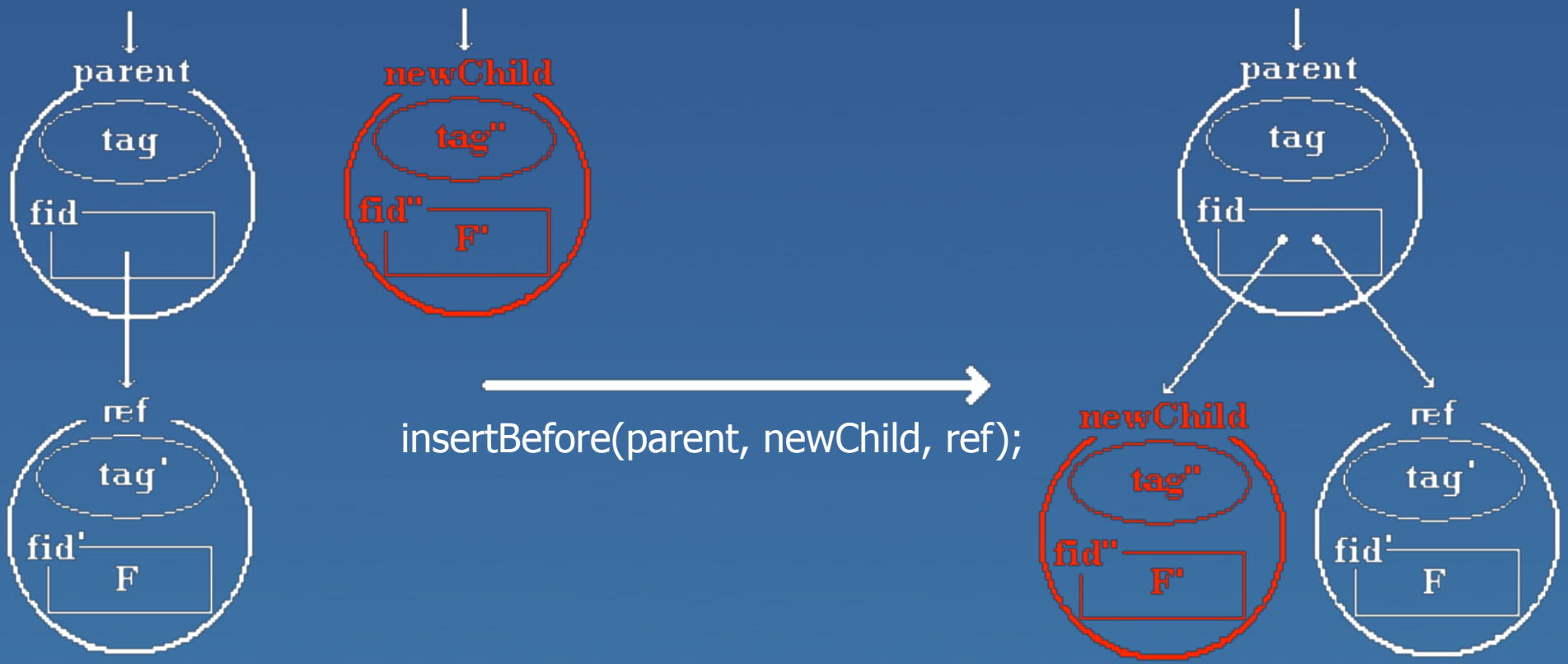
$$\{P[\mathrm{tag}/\mathrm{tag}'] \wedge (\mathrm{tag}' = \mathrm{tag})\}$$

$$\{\exists \mathrm{tag}(\mathrm{True}(\mathrm{tag}_{\mathrm{node}}[\mathrm{F}]_{\mathrm{fid}}) \wedge P[\mathrm{tag}/\mathrm{tag}'])\}$$

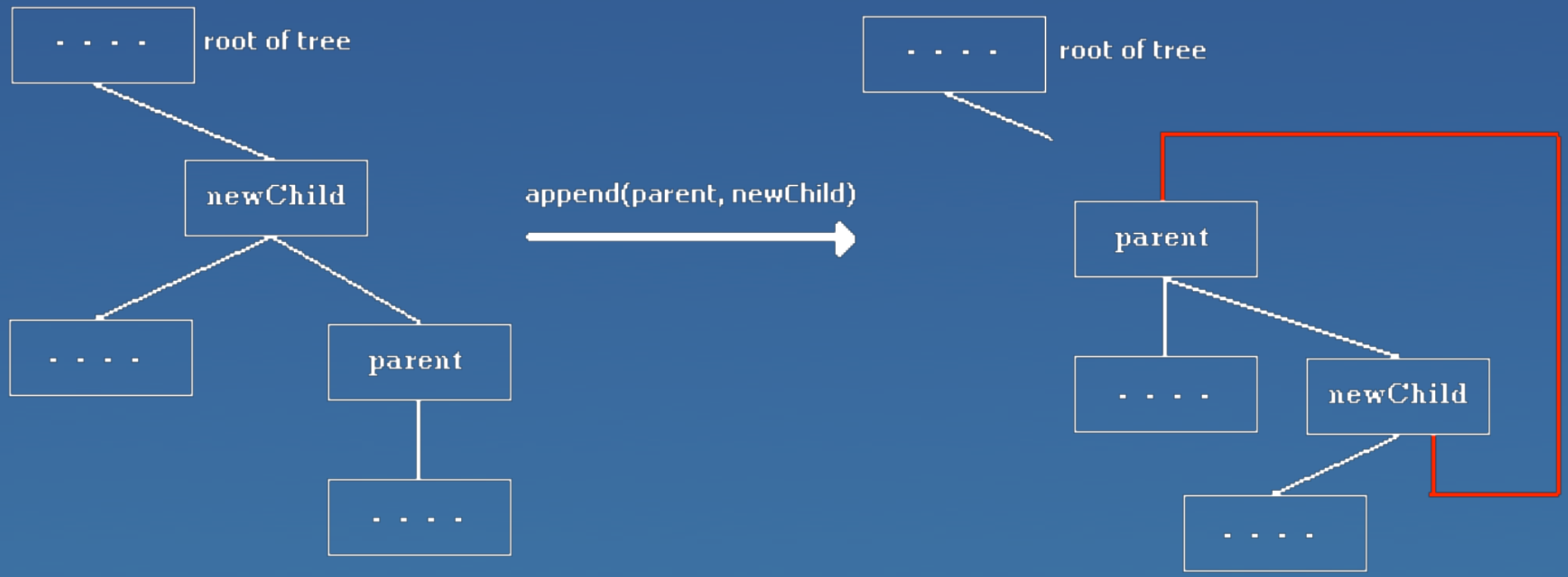
$$\mathrm{tag}' = \mathrm{getNodeName}(\mathrm{node});$$

$$\{\mathrm{P}\}$$

insertBefore



Ancestor Issue



insertBefore - Axiom

$$\{(\emptyset \triangleright \mathbf{CG}(\mathbf{tag}_{\mathbf{parent}}[\mathbf{F}_1 \times \mathbf{tag}'_{\mathbf{ref}}[\mathbf{F}]_{\mathbf{fid}'} \times \mathbf{F}_2]_{\mathbf{fid}}))(\mathbf{tag}''_{\mathbf{newChild}}[\mathbf{F}']_{\mathbf{fid}''})\}$$

$$\mathbf{insertBefore}(\mathbf{parent}, \mathbf{newChild}, \mathbf{ref});$$

$$\{\mathbf{CG}(\mathbf{tag}_{\mathbf{parent}}[\mathbf{F}_1 \times \mathbf{tag}''_{\mathbf{newChild}}[\mathbf{F}']_{\mathbf{fid}''} \times \mathbf{tag}'_{\mathbf{ref}}[\mathbf{F}]_{\mathbf{fid}'} \times \mathbf{F}_2]_{\mathbf{fid}})\}$$

Why not Small ?

Weakest Pre-condition

$$\{(\emptyset \triangleright \mathbf{CG}(\mathrm{tag}_{\mathrm{parent}}[\mathbf{F}_1 \times \mathrm{tag}'_{\mathrm{ref}}[\mathbf{F}]_{\mathrm{fid}'} \times \mathbf{F}_2]_{\mathrm{fid}}))(\mathrm{tag}''_{\mathrm{newChild}}[\mathbf{F}']_{\mathrm{fid}''})\}$$

$$\mathrm{insertBefore}(\mathrm{parent}, \mathrm{newChild}, \mathrm{ref});$$

$$\{\mathbf{CG}(\mathrm{tag}_{\mathrm{parent}}[\mathbf{F}_1 \times \mathrm{tag}''_{\mathrm{newChild}}[\mathbf{F}']_{\mathrm{fid}''} \times \mathrm{tag}'_{\mathrm{ref}}[\mathbf{F}]_{\mathrm{fid}'} \times \mathbf{F}_2]_{\mathrm{fid}})\}$$

$$\{(\mathbf{CG}(\mathrm{tag}_{\mathrm{parent}}[\mathbf{F}_1 \times \mathrm{tag}''_{\mathrm{newChild}}[\mathbf{F}']_{\mathrm{fid}''} \times \mathrm{tag}'_{\mathrm{ref}}[\mathbf{F}]_{\mathrm{fid}'} \times \mathbf{F}_2]_{\mathrm{fid}}) \triangleright P)$$

$$((\emptyset \triangleright \mathbf{CG}(\mathrm{tag}_{\mathrm{parent}}[\mathbf{F}_1 \times \mathrm{tag}'_{\mathrm{ref}}[\mathbf{F}]_{\mathrm{fid}'} \times \mathbf{F}_2]_{\mathrm{fid}}))(\mathrm{tag}''_{\mathrm{newChild}}[\mathbf{F}']_{\mathrm{fid}''}))\}$$

$$\mathrm{insertBefore}(\mathrm{parent}, \mathrm{newChild}, \mathrm{ref});$$

$$\{(\mathbf{CG}(\mathrm{tag}_{\mathrm{parent}}[\mathbf{F}_1 \times \mathrm{tag}''_{\mathrm{newChild}}[\mathbf{F}']_{\mathrm{fid}''} \times \mathrm{tag}'_{\mathrm{ref}}[\mathbf{F}]_{\mathrm{fid}'} \times \mathbf{F}_2]_{\mathrm{fid}}) \triangleright P)$$

$$(\mathbf{CG}(\mathrm{tag}_{\mathrm{parent}}[\mathbf{F}_1 \times \mathrm{tag}''_{\mathrm{newChild}}[\mathbf{F}']_{\mathrm{fid}''} \times \mathrm{tag}'_{\mathrm{ref}}[\mathbf{F}]_{\mathrm{fid}'} \times \mathbf{F}_2]_{\mathrm{fid}}))\}$$

Weakest Pre-condition

$$\{(\mathrm{CG}(\mathrm{tag}_{\mathrm{parent}}[\mathbf{F}_1 \times \mathrm{tag}''_{\mathrm{newChild}}[\mathbf{F}']_{\mathrm{fid}''} \times \mathrm{tag}'_{\mathrm{ref}}[\mathbf{F}]_{\mathrm{fid}'} \times \mathbf{F}_2]_{\mathrm{fid}}) \triangleright P)$$
$$((\emptyset \triangleright \mathrm{CG}(\mathrm{tag}_{\mathrm{parent}}[\mathbf{F}_1 \times \mathrm{tag}'_{\mathrm{ref}}[\mathbf{F}]_{\mathrm{fid}'} \times \mathbf{F}_2]_{\mathrm{fid}}))(\mathrm{tag}''_{\mathrm{newChild}}[\mathbf{F}']_{\mathrm{fid}''}))\}$$

$$\mathrm{insertBefore}(\mathrm{parent}, \mathrm{newChild}, \mathrm{ref});$$

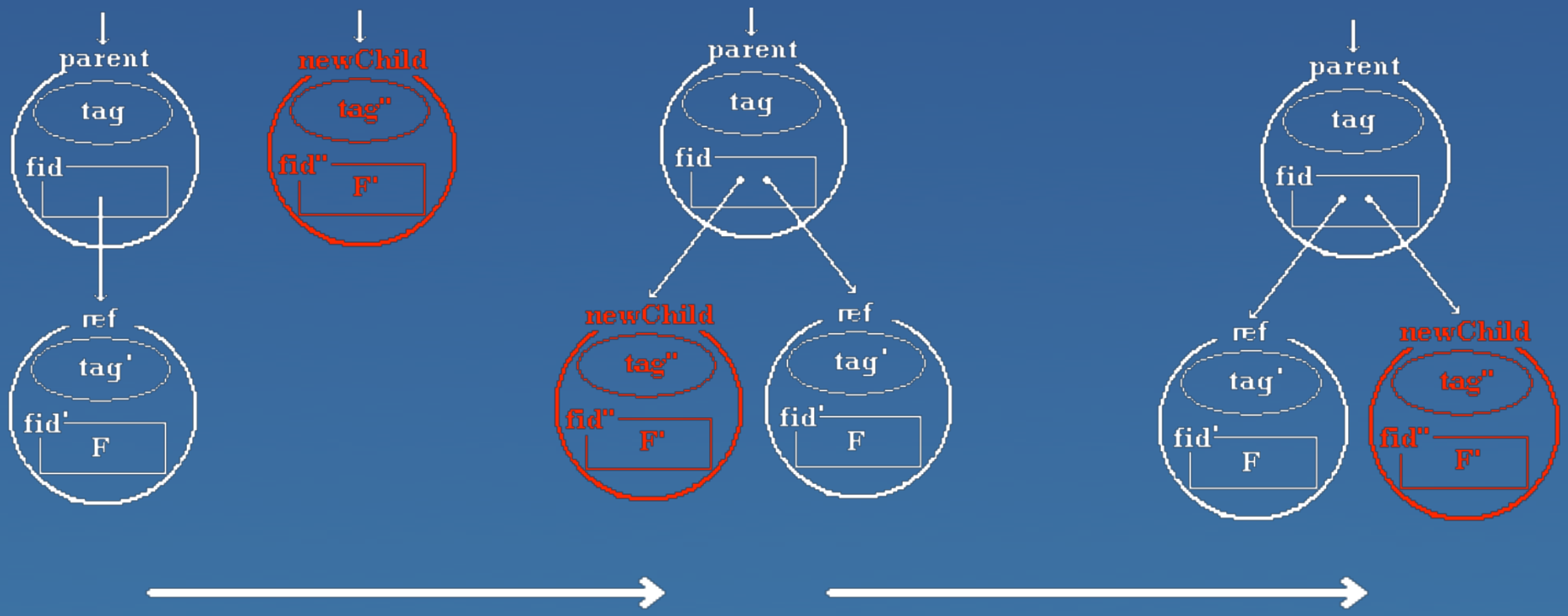
$$\{(\mathrm{CG}(\mathrm{tag}_{\mathrm{parent}}[\mathbf{F}_1 \times \mathrm{tag}''_{\mathrm{newChild}}[\mathbf{F}']_{\mathrm{fid}''} \times \mathrm{tag}'_{\mathrm{ref}}[\mathbf{F}]_{\mathrm{fid}'} \times \mathbf{F}_2]_{\mathrm{fid}}) \triangleright P)$$
$$(\mathrm{CG}(\mathrm{tag}_{\mathrm{parent}}[\mathbf{F}_1 \times \mathrm{tag}''_{\mathrm{newChild}}[\mathbf{F}']_{\mathrm{fid}''} \times \mathrm{tag}'_{\mathrm{ref}}[\mathbf{F}]_{\mathrm{fid}'} \times \mathbf{F}_2]_{\mathrm{fid}}))\}$$

$$\{(\mathrm{CG}(\mathrm{tag}_{\mathrm{parent}}[\mathbf{F}_1 \times \mathrm{tag}''_{\mathrm{newChild}}[\mathbf{F}']_{\mathrm{fid}''} \times \mathrm{tag}'_{\mathrm{ref}}[\mathbf{F}]_{\mathrm{fid}'} \times \mathbf{F}_2]_{\mathrm{fid}}) \triangleright P)$$
$$((\emptyset \triangleright \mathrm{CG}(\mathrm{tag}_{\mathrm{parent}}[\mathbf{F}_1 \times \mathrm{tag}'_{\mathrm{ref}}[\mathbf{F}]_{\mathrm{fid}'} \times \mathbf{F}_2]_{\mathrm{fid}}))(\mathrm{tag}''_{\mathrm{newChild}}[\mathbf{F}']_{\mathrm{fid}''}))\}$$

$$\mathrm{insertBefore}(\mathrm{parent}, \mathrm{newChild}, \mathrm{ref});$$

$$\{P\}$$

Axiom Composition - insertAfter



insertBefore(parent, newChild, ref);

insertBefore(parent, ref, newChild);

Axiom Composition - insertAfter

$$\{(\emptyset \triangleright \mathbf{CG}(\mathbf{tag}_{\mathbf{parent}}[\mathbf{F}_1 \times \mathbf{tag}'_{\mathbf{ref}}[\mathbf{F}]_{\mathbf{fid}'} \times \mathbf{F}_2]_{\mathbf{fid}}))(\mathbf{tag}''_{\mathbf{newChild}}[\mathbf{F}']_{\mathbf{fid}''})\}$$

$$\mathrm{insertBefore}(\mathbf{parent}, \mathbf{newChild}\ , \mathbf{ref});$$

$$\{\mathbf{CG}(\mathbf{tag}_{\mathbf{parent}}[\mathbf{F}_1 \times \mathbf{tag}''_{\mathbf{newChild}}[\mathbf{F}']_{\mathbf{fid}''} \times \mathbf{tag}'_{\mathbf{ref}}[\mathbf{F}]_{\mathbf{fid}'} \times \mathbf{F}_2]_{\mathbf{fid}})\}$$

$$\{(\emptyset \triangleright \mathbf{CG}(\mathbf{tag}_{\mathbf{parent}}[\mathbf{F}_1 \times \mathbf{tag}''_{\mathbf{newChild}}[\mathbf{F}']_{\mathbf{fid}''} \times \emptyset \times \mathbf{F}_2]_{\mathbf{fid}}))(\mathbf{tag}'_{\mathbf{ref}}[\mathbf{F}]_{\mathbf{fid}'})\}$$

$$\{(\emptyset \triangleright \mathbf{CG}(\mathbf{tag}_{\mathbf{parent}}[\mathbf{F}_1 \times \mathbf{tag}''_{\mathbf{newChild}}[\mathbf{F}']_{\mathbf{fid}''} \times \mathbf{F}_2]_{\mathbf{fid}}))(\mathbf{tag}'_{\mathbf{ref}}[\mathbf{F}]_{\mathbf{fid}'})\}$$

$$\mathrm{insertBefore}(\mathbf{parent}, \mathbf{ref}, \mathbf{newChild});$$

$$\{\mathbf{CG}(\mathbf{tag}_{\mathbf{parent}}[\mathbf{F}_1 \times \mathbf{tag}'_{\mathbf{ref}}[\mathbf{F}]_{\mathbf{fid}'} \times \mathbf{tag}''_{\mathbf{newChild}}[\mathbf{F}']_{\mathbf{fid}''} \times \mathbf{F}_2]_{\mathbf{fid}})\}$$

More than Minimal DOM

DOM Core Level 1:

- cloneNode
- replaceChild
- hasChildNodes

- insertAfter
- nodeEquality

Conclusion

- Complete Spec. for Minimal DOM
- Complete Spec. for Structural DOM Core Level 1
- Highly Extendable
- Automated Verification now possible

Future Work

- Automated Verification Tool
- Getting it Small
- The Rest of Core Level 1
- Higher Levels of DOM
- Concurrent DOM