Automatic Device Driver Synthesis with Termite

Leonid Ryzhyk, Peter Chubb, Ihor Kuz, Etienne Le Sueur, Gernot Heiser
UNSW, NICTA, Open Kernel Labs (Australia),

John Keys, Intel
Conventional driver development

OS interface spec

device spec
Conventional driver development

OS interface spec

device spec
Conventional driver development

OS interface spec

requests

driver.c

device commands

device spec
Driver synthesis: high-level view

Formal OS interface spec

requests

driver.c

device commands

Formal device spec
Driver synthesis: high-level view

- Formal OS interface spec
  - requests
  - driver.c
    - device commands
  - Formal device spec
Driver synthesis: high-level view

Advantages

- Separation of concerns
  - Know one thing well
- Reuse
  - Specify once, synthesise many

Formal OS interface spec

requests

driver.c

device commands

Formal device spec
Driver synthesis by example

Formal OS interface spec

Formal device spec

GPIO controller

ctrl, data

GPIO line
Driver synthesis by example

Formal OS interface spec

Formal device spec

GPIO controller registers

<table>
<thead>
<tr>
<th>ctrl</th>
<th>data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0=off</td>
<td>0=low</td>
</tr>
<tr>
<td>1=on</td>
<td>1=high</td>
</tr>
</tbody>
</table>

GPIO controller

GPIO line
Driver synthesis by example view

**Formal OS interface spec**

**Formal device spec**

- off
- on

- !ctrlWrite(1)
- !ctrlWrite(0)
- !dataWrite/changeLevel

**GPIO controller registers**

<table>
<thead>
<tr>
<th>ctrl</th>
<th>data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0=off</td>
<td>0=low</td>
</tr>
<tr>
<td>1=on</td>
<td>1=high</td>
</tr>
</tbody>
</table>

**GPIO controller**

GPIO line
Driver synthesis by example view

Formal
OS interface
spec

Formal device spec

GPIO controller registers

<table>
<thead>
<tr>
<th>ctrl</th>
<th>data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0=off</td>
<td>0=low</td>
</tr>
<tr>
<td>1=on</td>
<td>1=high</td>
</tr>
</tbody>
</table>

GPIO line
Driver synthesis by example view

Formal OS interface spec

GPIO controller registers

<table>
<thead>
<tr>
<th>ctrl</th>
<th>data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0=off</td>
<td>0=low</td>
</tr>
<tr>
<td>1=on</td>
<td>1=high</td>
</tr>
</tbody>
</table>

Formal device spec

- !ctrlWrite(1)
- !ctrlWrite(0)
- !dataWrite/changeLevel

GPIO controller

GPIO line
Driver synthesis by example view

**Formal OS interface spec**

- !ctrlWrite(1)
- !ctrlWrite(0)
- !dataWrite/changelvel

**GPIO controller registers**

<table>
<thead>
<tr>
<th>ctrl</th>
<th>data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0=off</td>
<td>0=low</td>
</tr>
<tr>
<td>1=on</td>
<td>1=high</td>
</tr>
</tbody>
</table>

**Formal device spec**

- off
- on

**GPIO controller**

- GPIO line
**Driver synthesis by example view**

**Formal OS interface spec**

**GPIO controller registers**

<table>
<thead>
<tr>
<th>ctrl</th>
<th>data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0=off</td>
<td>0=low</td>
</tr>
<tr>
<td>1=on</td>
<td>1=high</td>
</tr>
</tbody>
</table>

**Formal device spec**

- off
- on

- `!ctrlWrite(1)`
- `!ctrlWrite(0)`
- `!dataWrite/changeLevel`
Driver synthesis by example

Formal OS interface spec

?set \rightarrow \text{changeLevel} \rightarrow \text{!setComplete}

Formal device spec

\text{off} \rightarrow \text{!ctrlWrite}(1) \rightarrow \text{!ctrlWrite}(0) \rightarrow \text{on} \rightarrow \text{!dataWrite/\text{changeLevel}}

GPIO controller registers

<table>
<thead>
<tr>
<th>ctrl</th>
<th>data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0=off</td>
<td>0=low</td>
</tr>
<tr>
<td>1=on</td>
<td>1=high</td>
</tr>
</tbody>
</table>

GPIO controller

!ctrlWrite(1)

!dataWrite/\text{changeLevel}

GPIO line
Driver synthesis by example

Formal OS interface spec

Formal device spec

GPIO controller registers

ctrl  data
0=off  0=low
1=on   1=high

GPIO controller

GPIO line
Driver synthesis by example

**Formal OS interface spec**

- ?set
- changeLevel
- !setComplete

**GPIO controller registers**

<table>
<thead>
<tr>
<th>ctrl</th>
<th>data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0=off</td>
<td>0=low</td>
</tr>
<tr>
<td>1=on</td>
<td>1=high</td>
</tr>
</tbody>
</table>

**Formal device spec**

- off
- on

- !ctrlWrite(1)
- !ctrlWrite(0)
- !dataWrite/changeLevel

**GPIO controller**

- ctrl
- data

**GPIO line**
Driver synthesis by example

**Formal OS interface spec**

- ?set
- changeLevel
- !setComplete

**GPIO controller registers**

<table>
<thead>
<tr>
<th>ctrl</th>
<th>data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0=off</td>
<td>0=low</td>
</tr>
<tr>
<td>1=on</td>
<td>1=high</td>
</tr>
</tbody>
</table>

**Formal device spec**

- off
- on
- !ctrlWrite(1)
- !ctrlWrite(0)
- !dataWrite/changeLevel

**GPIO controller**

- ctrl
- data

**GPIO line**
Driver synthesis by example

Formal OS interface spec

Formal device spec

GPIO controller registers

<table>
<thead>
<tr>
<th>ctrl</th>
<th>data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0=off</td>
<td>0=low</td>
</tr>
<tr>
<td>1=on</td>
<td>1=high</td>
</tr>
</tbody>
</table>
Driver synthesis by example

**Formal OS interface spec**

- `?set` to `changeLevel`
- `!setComplete`

**Formal device spec**

- `off`
- `!ctrlWrite(1)` to `!ctrlWrite(0)`
- `on`
- `!dataWrite/changeLevel`
Driver synthesis by example

Formal OS interface spec

Formal device spec

OS spec || Device spec
Driver synthesis by example

Formal OS interface spec

Formal device spec

OS spec || Device spec
Driver synthesis by example

Formal OS interface spec
?set changeLevel
!setComplete

Formal device spec
off
!ctrlWrite(1) !ctrlWrite(0)
on
!dataWrite/changeLevel

OS spec || Device spec
?set
!ctrlWrite(1)
Driver synthesis by example

Formal OS interface spec

Formal device spec

OS spec || Device spec
Driver synthesis by example

Formal OS interface spec

?set \rightarrow \text{changeLevel} \rightarrow \exists\text{setComplete}

Formal device spec

\text{off} \rightarrow \neg\text{ctrlWrite(1)} \rightarrow \neg\text{ctrlWrite(0)} \rightarrow \text{on} \rightarrow \text{dataWrite/\text{changeLevel}}

OS spec \parallel \text{Device spec}

?set \rightarrow \exists\text{ctrlWrite(1)} \rightarrow \neg\text{ctrlWrite(1)}
Driver synthesis by example

Formal OS interface spec

Formal device spec

OS spec ∥ Device spec
Driver synthesis by example

**Formal OS interface spec**

- `?set changeLevel`
- `!setComplete`

**Formal device spec**

- `off`:
  - `!ctrlWrite(1)`
  - `!ctrlWrite(0)`
- `on`:
  - `!dataWrite/changeLevel`

**OS spec || Device spec**

- `?set`
- `!ctrlWrite(1)`
- `!ctrlWrite(0)`
- `!dataWrite/changeLevel`
Driver synthesis by example

Formal OS interface spec

Formal device spec

OS spec || Device spec
Driver synthesis by example

Formal OS interface spec

Formal device spec

OS spec \parallel Device spec
Driver synthesis by example

Formal OS interface spec
- `?set`
- `changeLevel`
- `!setComplete`

Formal device spec
- `off`
- `on`
- `!ctrlWrite(1)`
- `!ctrlWrite(0)`
- `!dataWrite/ changeLevel`

OS spec || Device spec
- `?set`
- `!ctrlWrite(1)`
- `!ctrlWrite(0)`
- `!ctrlWrite(1)`
- `!ctrlWrite(0)`
- `!ctrlWrite(0)`
- `!setComplete`
- `!dataWrite/ changeLevel`
Driver synthesis by example

Formal OS interface spec

Formal device spec

OS spec  Device spec
Driver synthesis by example

Formal OS interface spec

Formal device spec

OS spec || Device spec
Driver synthesis by example

Formal OS interface spec

Formal device spec

OS spec \parallel Device spec
Driver synthesis by example

Formal OS interface spec

- ?set
- changeLevel
- !setComplete

Formal device spec

- off
- !ctrlWrite(1)
- !ctrlWrite(0)
- on
- !dataWrite/changeLevel

OS spec || Device spec

- ?set
- !ctrlWrite(1)
- !dataWrite/changeLevel
- !setComplete
Driver synthesis by example

Formal OS interface spec

Formal device spec

OS spec || Device spec
Driver synthesis by example

Formal OS interface spec

Formal device spec

OS spec \parallel Device spec
Driver synthesis by example

Formal OS interface spec

Formal device spec

OS spec || Device spec
Driver synthesis by example

Formal OS interface spec

Formal device spec

??set changeLevel
!setComplete

?set changeLevel

Formal device spec

!ctrlWrite(1)
!ctrlWrite(0)
off
on
!dataWrite/changeLevel

?set changeLevel

!ctrlWrite(1)

OS spec || Device spec

!setComplete

?set changeLevel

!dataWrite/changeLevel

!setComplete
Modelling real device interfaces

SD host controller device

REGISTERS
- ARG
- CMD
- STAT
- RESP
- ISR
- DIV
- RST
- DISR
- BDST
- BDRX
- BDTX

CMD_MASTER

CLK DIVIDER

DATA_MASTER
Modelling real device interfaces

SD host controller device

REGISTERS
- ARG
- CMD
- STAT
- RESP
- ISR

CMD_MASTER

CLK DIVIDER

DATA_MASTER

Multiple functional units
Modelling real device interfaces

Multiple functional units

REGISTERS
|||  
CLOCK_DIVIDER
|||  
(COMMAND_MASTER |[class.off]| DATA_MASTER)
Modelling real device interfaces

Data

REGISTERS

CLOCK_DIVIDER

Multiple functional units

CMD_MASTER

DATA_MASTER

CLK DIVIDER

ARG

CMD

STAT

RESP

ISR

DIV

RST

DISR

BDST

BDRX

BDTX

SD host controller device

REGISTER

CLOCK_DIVIDER

COMMAND_MASTER |[class.off]| DATA_MASTER

(Data)
comand_reg m_command_reg;
...
write_reset_reg
/m_command_reg = 0

Modelling real device interfaces

Multiple functional units

REGISTERS
|||
CLOCK_DIVIDER
|||
(COMMAND_MASTER |[class.off]| DATA_MASTER)
The synthesis algorithm

• The state explosion problem
  - **Problem:** The product state space can be huge
  - **Solution:** Explore the product state space incrementally

• Dealing with data
  - **Problem:** Enumerating all variable assignments is infeasible
  - **Solution:** Manipulate data symbolically
Results

- Successfully synthesised drivers for real devices:
  - Asix AX88772 USB-to-Ethernet adapter
    - Linux
  - Ricoh R5C822 SD host controller
    - Linux
    - FreeBSD
# Results

<table>
<thead>
<tr>
<th></th>
<th>USB-to-Ethernet</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS interface spec</td>
<td>309 loc</td>
<td>641 loc</td>
</tr>
<tr>
<td>Device spec</td>
<td>463 loc</td>
<td>653 loc</td>
</tr>
<tr>
<td>Synthesised driver</td>
<td>2620 loc</td>
<td>4667 loc</td>
</tr>
<tr>
<td>Linux driver</td>
<td>1200 loc</td>
<td>1174 loc</td>
</tr>
</tbody>
</table>
## Results

<table>
<thead>
<tr>
<th></th>
<th>USB-to-Ethernet</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS interface spec</td>
<td>309 loc</td>
<td>641 loc</td>
</tr>
<tr>
<td>Device spec</td>
<td>463 loc</td>
<td>653 loc</td>
</tr>
<tr>
<td>Synthesised driver</td>
<td>2620 loc</td>
<td>4667 loc</td>
</tr>
<tr>
<td>Linux driver</td>
<td>1200 loc</td>
<td>1174 loc</td>
</tr>
</tbody>
</table>
## Results

<table>
<thead>
<tr>
<th></th>
<th>USB-to-Ethernet</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS interface spec</td>
<td>309 loc</td>
<td>641 loc</td>
</tr>
<tr>
<td>Device spec</td>
<td>463 loc</td>
<td>653 loc</td>
</tr>
<tr>
<td>Synthesised driver</td>
<td>2620 loc</td>
<td>4667 loc</td>
</tr>
<tr>
<td>Linux driver</td>
<td>1200 loc</td>
<td>1174 loc</td>
</tr>
</tbody>
</table>
The Termite Debugger
Performance of the AX88772 USB-to-Ethernet adapter driver

CPU Utilisation (%)

Packet size (bytes)

Throughput (Mbit/s)

Packet size (bytes)
Limitations of Termite

- Cannot specify constraints on data in memory
  - alignment, fragmentation, etc
- Complex relations among variables are not supported
- Restrictions on the structure of specifications
- Termite drivers require runtime support
Ongoing work

- Formal OS interface spec
- driver.c
- Formal device spec
Ongoing work

1. **HDL**
2. **Formal device spec**
3. **Formal OS interface spec**
4. **driver.c**
Ongoing work

HDL

Formal OS interface spec

driver.c

Formal device spec
Conclusions

• Driver synthesis is possible
  - Device experts provide device specs
  - OS experts provide OS specs
  - Termite does the rest

• Still work-in-progress
  - Addressing current limitations
  - Driver synthesis from HDL