Query-Directed Adaptive Heap Cloning for Optimizing Compilers

Yulei Sui, Yue Li, Jingling Xue

Programming Languages and Compilers Group
School of Computer Science and Engineering
University of New South Wales, Australia

April 3, 2013
Program execution

Heap cloning

Statically distinguishing heap objects by call paths

```c
int main()
{
    int* buffer1 = getMem();
    int* buffer2 = getMem();
}

int* getMem()
{
    return malloc(10);
}
```

Points-to relations without heap cloning

Points-to relations with heap cloning
Heap cloning

Statically distinguishing heap objects by call paths

```c
int main()
{
    int* buffer1 = getMem();
    int* buffer2 = getMem();
}

test* getMem()
{
    return malloc(10);
}
```
Heap cloning

Statically distinguishing heap objects by call paths

```c
int main()
{
    int* buffer1 = getMem();
    int* buffer2 = getMem();
}

int* getMem()
{
    return malloc(10);
}
```

Program execution
Heap cloning

Statically distinguishing heap objects by call paths

```c
int main()
{
    int* buffer1 = getMem();
    int* buffer2 = getMem();
}

int* getMem()
{
    return malloc(10);
}
```

Program execution
Heap cloning

Statically distinguishing heap objects by call paths

```c
int main()
{
    int* buffer1 = getMem();
    int* buffer2 = getMem();
}

int* getMem()
{
    return malloc(10);
}
```

Program execution
Heap cloning

Statically distinguishing heap objects by call paths

```c
int main()
{
    int* buffer1 = getMem();
    int* buffer2 = getMem();
}

int* getMem()
{
    return malloc(10);
}
```

Program execution

Points-to relations without heap cloning
Heap cloning

Statically distinguishing heap objects by call paths

```c
int main()
{
    int* buffer1 = getMem();
    int* buffer2 = getMem();
}
```

```c
int* getMem()
{
    return malloc(10);
}
```

Program execution

Points-to relations without heap cloning

Points-to relations with heap cloning
Call graph of 176.gcc (230.4KLOC)

#Procedures: 2256  #Pointers: 134380  #Calling Contexts: 1.2*10^5

Context-sensitive heap cloning can be costly!

© Yulei Sui, CGO 2013, 25/02/2013
PLC, UNSW
K-callsite-sensitive heap cloning

Call Graph with K-callsite-sensitive heap cloning

[Nystrom-SAS’04, Nystrom-PASTE’04, Lhotak-CC’06, Xu-ISSTA’08]
K-callsite-sensitive heap cloning

Call Graph with K-callsite-sensitive heap cloning

[Nystrom-SAS’04, Nystrom-PASTE’04, Lhotak-CC’06, Xu-ISSTA’08]
K-callsite-sensitive heap cloning

Call Graph with K-callsite-sensitive heap cloning

[Nystrom-SAS’04, Nystrom-PASTE’04, Lhotak-CC’06, Xu-ISSTA’08]
K-callsite-sensitive heap cloning

Call Graph with K-callsite-sensitive heap cloning

[Nystrom-SAS’04, Nystrom-PASTE’04, Lhotak-CC’06, Xu-ISSTA’08]
K-callsite-sensitive heap cloning

Call Graph with K-callsite-sensitive heap cloning

[Nystrom-SAS’04, Nystrom-PASTE’04, Lhotak-CC’06, Xu-ISSTA’08]
K-callsite-sensitive heap cloning

Call Graph with K-callsite-sensitive heap cloning
[Nystrom-SAS’04, Nystrom-PASTE’04, Lhotak-CC’06, Xu-ISSTA’08]
K-callsite-sensitive heap cloning

Analysis time of 176.gcc with Andersen-style context sensitive heap cloning 22x slower than Open64 "-O2" compile time

[Nystrom-SAS’04, Nystrom-PASTE’04, Lhotak-CC’06, Xu-ISSTA’08]
• Is full heap cloning overkill (relative to a client’s needs)?
• Is full heap cloning overkill (relative to a client’s needs)?

• Is k-callsite sensitive cloning the best solution?
Alias Query

• Whether two expressions may represent the same memory location.
Alias Query

• Whether two expressions may represent the same memory location.
• For example: \( \langle *\text{buffer1}, *\text{buffer2} \rangle \)
  • Alias Without Heap Cloning
Alias Query

- Whether two expressions may represent the same memory location.
- For example: \langle *buffer1, *buffer2 \rangle
  - Alias Without Heap Cloning
  - Not-Alias Heap Cloning
Analysis precision for answering alias queries

Percentage of must-not aliases disambiguated among the queries issued by WOPT with k-callsite-sensitive heap cloning
A close look at 255.vortex’s call graph
Goal

- Can we enable heap cloning only where it is necessary?
- Can we achieve the same precision as full heap cloning according to a client’s needs?
Our QUDA framework
QUery-Directed Adaptive heap cloning

- Alias Queries
- Heap-Aware Pointer Solver
- Selecting Candidate Heap Objects
- Adaptive Update

Cloning Level K
K++
Query-directed adaptive heap cloning

Query-Directed Adaptive Heap Cloning

procedure
heap object
k=0
k=1
k=2
k=3
bb
<p,q>

Alias Query

must-not-alias

not heap-related

heap-related

All done
Can't clone further

Query-Directed Adaptive Heap Cloning
Query-directed adaptive heap cloning

procedure
heap object
k=0
k=1
k=2
k=3
bb
<*p,*q>
Alias Query
must-not-alias

Query-Directed Adaptive Heap Cloning

procedure
heap object
k=0
k=1
k=2
k=3
bb
<*p,*q>
Alias Query
may-alias
not heap-related

Query-Directed Adaptive Heap Cloning

procedure
heap object
k=0
k=1
k=2
k=3
bb
<*p,*q>
Alias Query
may-alias
heap-related

Query-Directed Adaptive Heap Cloning

procedure
heap object
k=0
k=1
k=2
k=3
bb
<*p,*q>
Alias Query
may-alias
heap-related

Query-Directed Adaptive Heap Cloning

procedure
heap object
k=0
k=1
k=2
k=3
bb
<*p,*q>
Alias Query
All done
Can't clone further
Query-directed adaptive heap cloning

Query-Directed Adaptive Heap Cloning

procedure
heap object
k=0
k=1
k=2
k=3
bb
<*p,*q>
Alias Query

must-not-alias

may-alias
not heap-related

heap-related

All done
Can't clone further
Query-directed adaptive heap cloning

Query-Directed Adaptive Heap Cloning

procedure
heap object
k=0
k=1
k=2
k=3
bb
<*p,*q>
Alias Query
must-not-alias

<*>p,*q>
Alias Query
may-alias
not heap-related

heap-related

All done
Can't clone further

11 / 20

YG Sui, CGO 2013, 25/02/2013
PLC, UNSW
Query-directed adaptive heap cloning

procedure
heap object

k=0

k=1

k=2

k=3

bb

Alias Query

<*p,*q>

may-alias

not heap-related

heap-related

All done

Can't clone further

Query-Directed Adaptive Heap Cloning
Query-directed adaptive heap cloning

Query-Directed Adaptive Heap Cloning

Alias Query

must-not-alias

may-alias

not heap-related

heap-related

All done

Can't clone further

procedure

heap object

k=0

Query-Directed Adaptive Heap Cloning

@ Yulei Sui, CGO 2013, 25/02/2013
PLC, UNSW
Query-directed adaptive heap cloning

Query-Directed Adaptive Heap Cloning

procedure
heap object
k=0
k=1
k=2
k=3
bb

Alias Query
<*p,*q>

may-alias
not heap-related

All done
Can't clone further

Query-Directed Adaptive Heap Cloning
Query-directed adaptive heap cloning

Alias Query

<*p,*q>

may-alias

heap-related

All done

Can't clone further
Query-directed adaptive heap cloning

```
procedure
heap object
k=0
k=1
k=2
k=3
bb
<*p,*q>
Alias Query
must-not-alias

procedure
heap object
k=0
k=1
k=2
k=3
bb
<*p,*q>
Alias Query
may-alias
not heap-related

procedure
heap object
k=0
k=1
k=2
k=3
bb
<*p,*q>
Alias Query
may-alias
heap-related

All done
Can't clone further
```
Query-directed adaptive heap cloning

**Alias Query**

<*p,*q>

- **must-not-alias**
- **may-alias**
- **heap-related**
- **not heap-related**

**Query-Directed Adaptive Heap Cloning**
Query-directed adaptive heap cloning

Alias Query

must-not-alias

may-alias

not heap-related

heap-related

All done

Can't clone further

procedure

heap object

k=0

k=1

k=2

k=3

<*p,*q>

p

q

p

q

k=0

k=1

Query-Directed Adaptive Heap Cloning
Query-directed adaptive heap cloning

procedure
heap object
k=0
k=1
k=2
k=3
bb
<*p,*q>
Alias Query
must-not-alias

<*>p,*q>
Alias Query
may-alias
not heap-related
heap-related

All done
Can't clone further

Query-Directed Adaptive Heap Cloning
Query-directed adaptive heap cloning

Alias Query

<*p,*q>

may-alias

not heap-related

heap-related

All done

Can't clone further

Query-Directed Adaptive Heap Cloning

procedure

heap object

k=0

k=1

k=2

k=3
Query-directed adaptive heap cloning

Alias Query

<*p,*q>

may-alias

not heap-related

heap-related

All done
Can't clone further

Query-Directed Adaptive Heap Cloning
Query-directed adaptive heap cloning

Alias Query

must-not-alias

may-alias

not heap-related

heap-related

All done
Can't clone further

Query-Directed Adaptive Heap Cloning

procedure
heap object
k=0
k=1
k=2
k=3
bb
<*p,*q>

Alias Query

may-alias

not heap-related

heap-related
Query-directed adaptive heap cloning

procedure
heap object
k=0
k=1
k=2
k=3

bb
<*p,*q>
Alias Query

P
Q
must-not-alias

All done
Can't clone further

procedure
heap object

Query-Directed Adaptive Heap Cloning

Alias Query

<*p,*q>

k=2
k=1
k=0
QUDA: QUery-Directed Adaptive heap cloning

Alias Queries

Heap-Aware Pointer Solver

Selecting Candidate Heap Objects

Adaptive Update

Cloning Level $K$

$K++$
Heap-aware pointer analysis

\[ x \rightarrow g \]
\[ p \rightarrow o \]
Heap-aware pointer analysis

\[ x \rightarrow (\text{true, } g) \]
\[ p \rightarrow (h_o, \ o) \]
Heap-aware pointer analysis

\begin{align*}
x & \rightarrow \text{(true, } g) \\
p & \rightarrow \text{(} h_o, \quad o \text{)} \\
q & \rightarrow \text{(} h_o, \quad o \text{)} \\
\end{align*}

\begin{align*}
* p &= x; \\
y &= * q; \\
\end{align*}
Heap-aware pointer analysis

Constraint Graph:

Copy ← Store ← = Load →

\[
\begin{align*}
x & \rightarrow \text{(true, } g) \\
p & \rightarrow \text{(} h_o, \ o) \\
q & \rightarrow \text{(} h_o, \ o)
\end{align*}
\]

\[
\begin{align*}
*p & = x; \\
y & = *q;
\end{align*}
\]
Heap-aware pointer analysis

Constraint Graph:

\[
\begin{align*}
x & \rightarrow (\text{true, } g) \\
p & \rightarrow (h_o, \ o) \\
q & \rightarrow (h_o, \ o) \\
*p & = x; \\
y & = *q;
\end{align*}
\]
Heap-aware pointer analysis

Constraint Graph:

Copy ← Store ← = Load ←

\[
\begin{align*}
x & \rightarrow (\text{true, } g) \\
p & \rightarrow (h_o, \ o) \\
q & \rightarrow (h_o, \ o)
\end{align*}
\]

\[
\begin{align*}
*p & = x; \\
y & = *q;
\end{align*}
\]
Candidate heap objects selection

Constraint Graph:

Copy ← Store ← Load

Alias Query

\[ \langle \ast x, \ast y \rangle \]
Candidate heap objects selection

Constraint Graph:

Copy ← Store ← Load

Alias Query

\langle \ast x, \ast y \rangle

\text{pts}(x) = \{\text{true}, g\}
\text{pts}(y) = \{h_0, g\}

Candidate Heap Object \{o\}
Adaptive update

Candidate Heap Object \( \{ o \} \)

Constraint Graph:

Copy ← Store ← = Load ← →

\[ *vec = x; \]
\[ y = *map; \]
\[ *arr = y; \]

\[ z = *arr; \]
Adaptive update

Constraint Graph:

Candidate Heap Object \{o\}

\[\text{vec} = x;\]
\[y = \text{map};\]
\[\text{arr} = y;\]

\[z = \text{arr};\]
Next round resolution

Constraint Graph:

Copy ← Store ← Load

Alias Query

\langle \ast x, \ast y \rangle

Not-alias!
QUDA framework in Open64
Analysis times of FULCRA and QUDA

Analysis time normalized with respect to Open64’s compile times (-O2)
Heap objects reduced by QUDA over FULCRA

Number of heap objects reduced by QUDA over FULCRA in percentage terms
Heap distribution with full heap cloning (175.vpr)
Heap distribution with QUDA (175.vpr)
Alias queries to be answered at each iteration

% of Queries to Be Answered

% of Analysis Time

k-Callsite-Sensitivity Heap Cloning

@ Yulei Sui, CGO 2013, 25/02/2013
PLC, UNSW
Analysis time per iteration over the total

![Graph showing analysis time per iteration for various benchmarks. The graph plots the percentage of analysis time against the k-Callsite-Sensitivity Heap Cloning iteration number. Different benchmarks such as gcc, hmmer, jpeg, mesa, perlbmk, rasta, sendmail, and vortex are represented by distinct markers and lines. The x-axis represents the iteration number (1 to 6), and the y-axis shows the percentage of analysis time (0% to 14%).]
Conclusion

Novel heap cloning approach: same precision as full heap cloning but significantly more scalable

- Heap-aware analysis
- Query-directed
- Adaptive

Challenges and opportunities:

- Iterative compilation (prioritising queries in hot functions)
- Bug detection (scaling precise pointer analysis)