Static Reference Analysis for GUI Objects in Android Software

Atanas Rountev, Dacong (Tony) Yan

Ohio State University

PRESTO: Program Analyses and Software Tools Research Group, Ohio State University

Motivation and Background

- Android software is used by millions of users
  - Requires foundational program analyses for improved performance and quality
- Static reference analysis for Java
  - What is the set of run-time objects?
  - Which variables contain references to which objects?
  - Critical component of data- and control-flow analysis
  - Prerequisite for many other techniques
- Existing work cannot be applied directly to Android
- Goal: develop a precise and efficient static reference analysis for Android-specific features

Static Reference Analysis for Android Features

- Android application
  - Driven by a graphical user interface (GUI)
  - *Activity*: on-screen window with GUI elements (*views*)
  - *Event handlers*: defined in *listeners* and associated with views to respond to user actions
- Need to model statically
  - Views and their hierarchical structure
  - Association of views with activities
  - Association of views with listeners
  - Variables that refer to views, activities, and listeners

Example

MyActivity.java:

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

ButtonListener.java:

```
class ButtonListener implements OnClickListener {
  void onClick(View d) { ... }  }
```

main.xml:

```
<RelativeLayout ...>
  <Button android:id=“@+id/my_btn” ... />
</RelativeLayout>
```

Example

MyActivity.java:

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

ButtonListener.java:

```
class ButtonListener implements OnClickListener {
  void onClick(View d) { ... }  }
```

main.xml:

```
<RelativeLayout ...>
  <Button android:id="@+id/my_btn" ... />
</RelativeLayout>
```

Example

MyActivity.java:

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

ButtonListener.java:

```
class ButtonListener implements OnClickListener {
  void onClick(View d) { ... }  }
```

main.xml:

```
<RelativeLayout ...>
  <Button android:id="@+id/my_btn" ... />
</RelativeLayout>
```

Example

MyActivity.java:

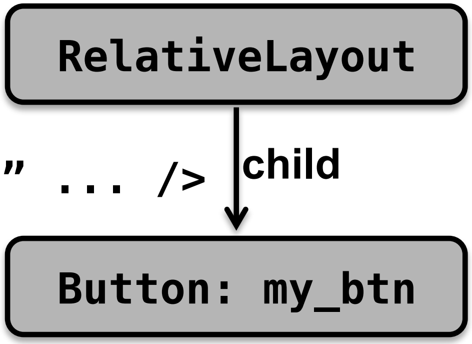
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

ButtonListener.java:

```
class ButtonListener implements OnClickListener {
  void onClick(View d) { ... }  }
```

main.xml:

```
<RelativeLayout ...>
  <Button android:id=“@+id/my_btn” ... />
</RelativeLayout>
```



Example

MyActivity.java:

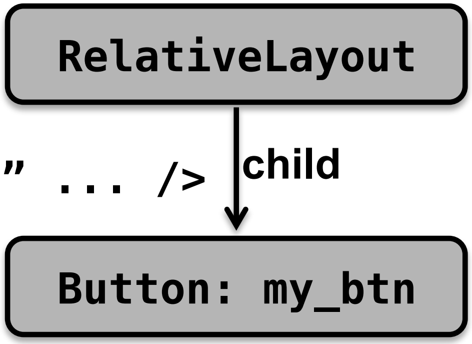
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

ButtonListener.java:

```
class ButtonListener implements OnClickListener {
  void onClick(View d) { ... }  }
```

main.xml:

```
<RelativeLayout ...>
  <Button android:id=“@+id/my_btn” ... />
</RelativeLayout>
```



RelativeLayout

child

Button: my_btn

Example

MyActivity.java:

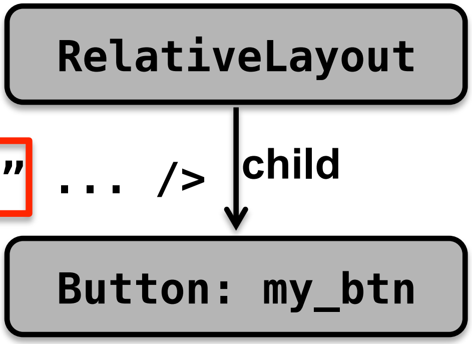
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

ButtonListener.java:

```
class ButtonListener implements OnClickListener {
  void onClick(View d) { ... }  }
```

main.xml:

```
<RelativeLayout ...>
  <Button android:id="@+id/my_btn" ... />
</RelativeLayout>
```



Example

MyActivity.java:

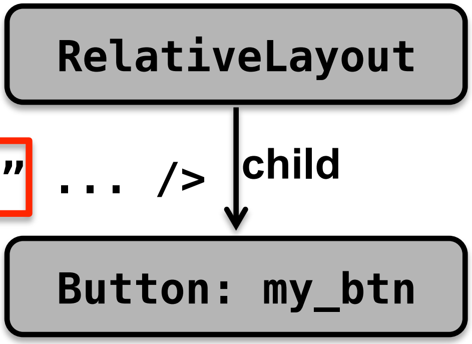
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

ButtonListener.java:

```
class ButtonListener implements OnClickListener {
  void onClick(View d) { ... }  }
```

main.xml:

```
<RelativeLayout ...>
  <Button android:id="@+id/my_btn" ... />
</RelativeLayout>
```



RelativeLayout

child

Button: my_btn

Example

MyActivity.java:

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

ButtonListener.java:

```
class ButtonListener implements OnClickListener {
  void onClick(View d) { ... }  }
```

main.xml:

```
<RelativeLayout ...>
  <Button android:id=“@+id/my_btn” ... />
</RelativeLayout>
```

Example

MyActivity.java:

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

ButtonListener.java:

```
class ButtonListener implements OnClickListener {
  void onClick(View d) { ... }  }
```

main.xml:

```
<RelativeLayout ...>
  <Button android:id="@+id/my_btn" ... />
</RelativeLayout>
```

Example

MyActivity.java:

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

ButtonListener.java:

```
class ButtonListener implements OnClickListener {
  void onClick(View d) { ... }  }
```

main.xml:

```
<RelativeLayout ...>
  <Button android:id=“@+id/my_btn” ... />
</RelativeLayout>
```

Example

MyActivity.java:

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

ButtonListener.java:

```
class ButtonListener implements OnClickListener {
  void onClick(View d) { ... }  }
```

main.xml:

```
<RelativeLayout ...>
  <Button android:id="@+id/my_btn" ... />
</RelativeLayout>
```

Example

MyActivity.java:

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

ButtonListener.java:

```
class ButtonListener implements OnClickListener {
  void onClick(View d) { ... } }
```

main.xml:

```
<RelativeLayout ...>
  <Button android:id="@+id/my_btn" ... />
</RelativeLayout>
```

Modeled Android Operations

- **Inflate**
  - Create GUI structure from XML and attach to activity/view
- **CreateView**
  - Programmatically create a view through **new V**
- **FindView**
  - Lookup a view from activity or ancestor view (e.g., by ID)
- **SetListener**
  - Associate view and listener
- **AddView**
  - Establish parent-child relationship between two views
- **SetId**
  - Programmatically set the ID of a view

Our Proposal

- Define *formal semantics* of GUI-related Android constructs
- Encode semantics of an Android application in a *constraint graph*
- Perform constraint-based static reference analysis

Example

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
   ...    ...    ...
  void onClick(View d) { ... }  }
```

Propagation edges and relevant nodes

Example

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
  ...    ...    ...
  void onClick(View d) { ... }  }
```

MyActivity

Propagation edges and relevant nodes

Example

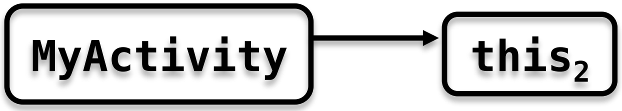
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
   ...    ...    ...
  void onClick(View d) { ... }  }
```

MyActivity

Propagation edges and relevant nodes

Example

```
1  class MyActivity extends Activity {
2    void onCreate() {
3      this.setContentView(R.layout.main);  // Inflate
4      View a = this.findViewById(R.id.my_btn);  // FindView
5      Button b = (Button) a;
6      ButtonListener c = new ButtonListener();
7      b.setOnClickListener(c);  // SetListener  }  }
     ...    ...    ...
9    void onClick(View d) { ... }  }
```



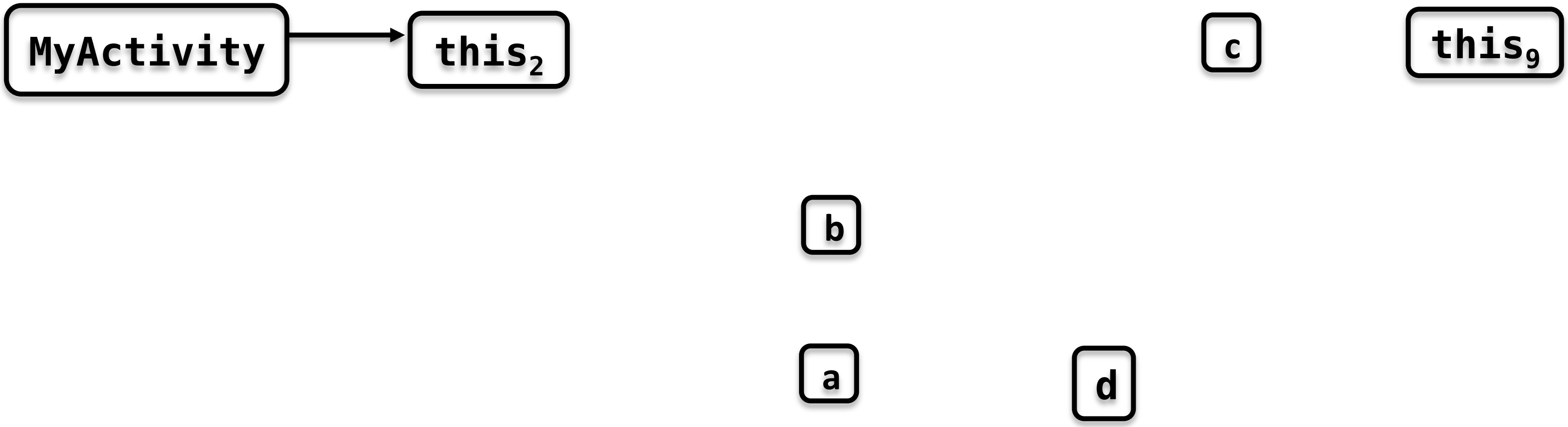
MyActivity

this_2

Propagation edges and relevant nodes

Example

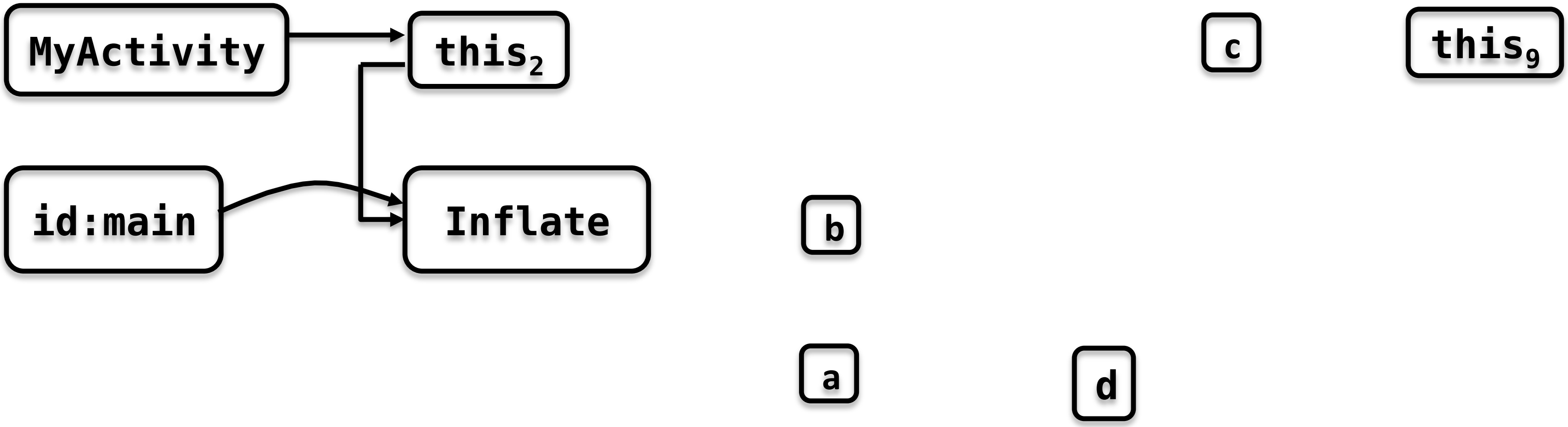
```
1  class MyActivity extends Activity {
2    void onCreate() {
3      this.setContentView(R.layout.main);  // Inflate
4      View a = this.findViewById(R.id.my_btn);  // FindView
5      Button b = (Button) a;
6      ButtonListener c = new ButtonListener();
7      b.setOnClickListener(c);  // SetListener  }  }
     ...     ...     ...
9    void onClick(View d) { ... }  }
```



Propagation edges and relevant nodes

Example

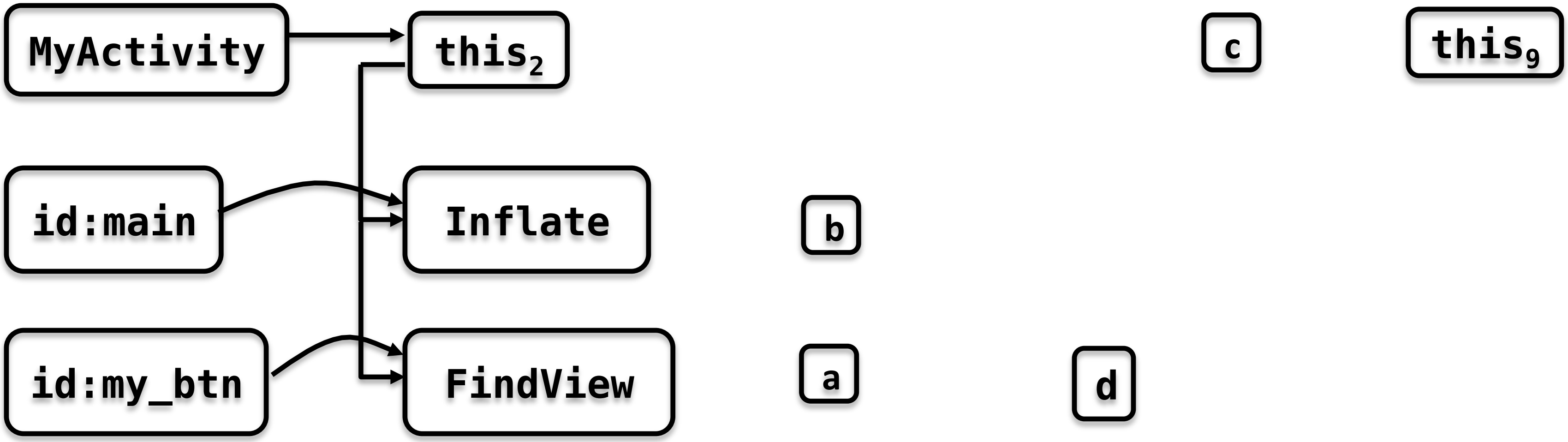
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
 ...    ...    ...
  void onClick(View d) { ... }  }
```



Propagation edges and relevant nodes

Example

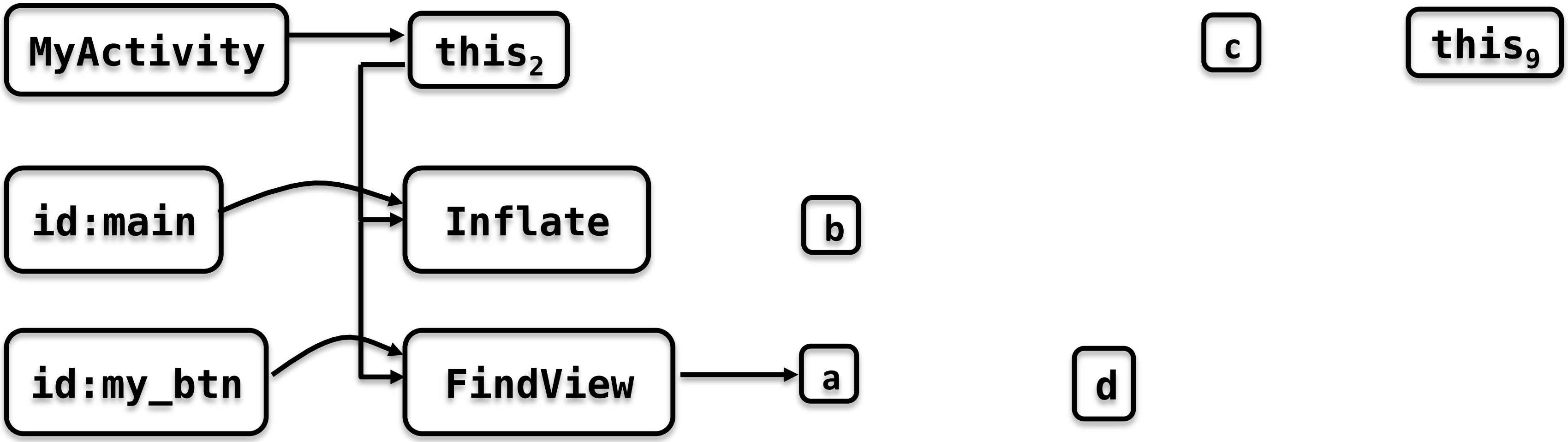
```
1   class MyActivity extends Activity {
2     void onCreate() {
3       this.setContentView(R.layout.main);  // Inflate
4       View a = this.findViewById(R.id.my_btn);  // FindView
5       Button b = (Button) a;
6       ButtonListener c = new ButtonListener();
7       b.setOnClickListener(c);  // SetListener  }  }
     ...    ...    ...
9     void onClick(View d) { ... }  }
```



Propagation edges and relevant nodes

Example

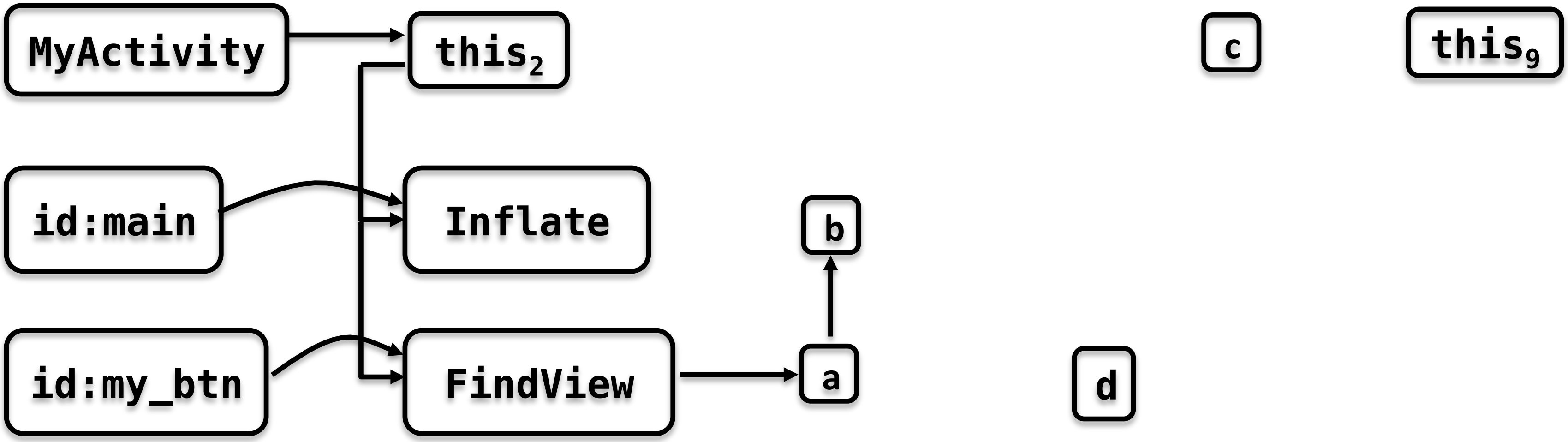
```
1  class MyActivity extends Activity {
2    void onCreate() {
3      this.setContentView(R.layout.main);  // Inflate
4      View a = this.findViewById(R.id.my_btn);  // FindView
5      Button b = (Button) a;
6      ButtonListener c = new ButtonListener();
7      b.setOnClickListener(c);  // SetListener  }  }
     ...    ...    ...
9    void onClick(View d) { ... }  }
```



Propagation edges and relevant nodes

Example

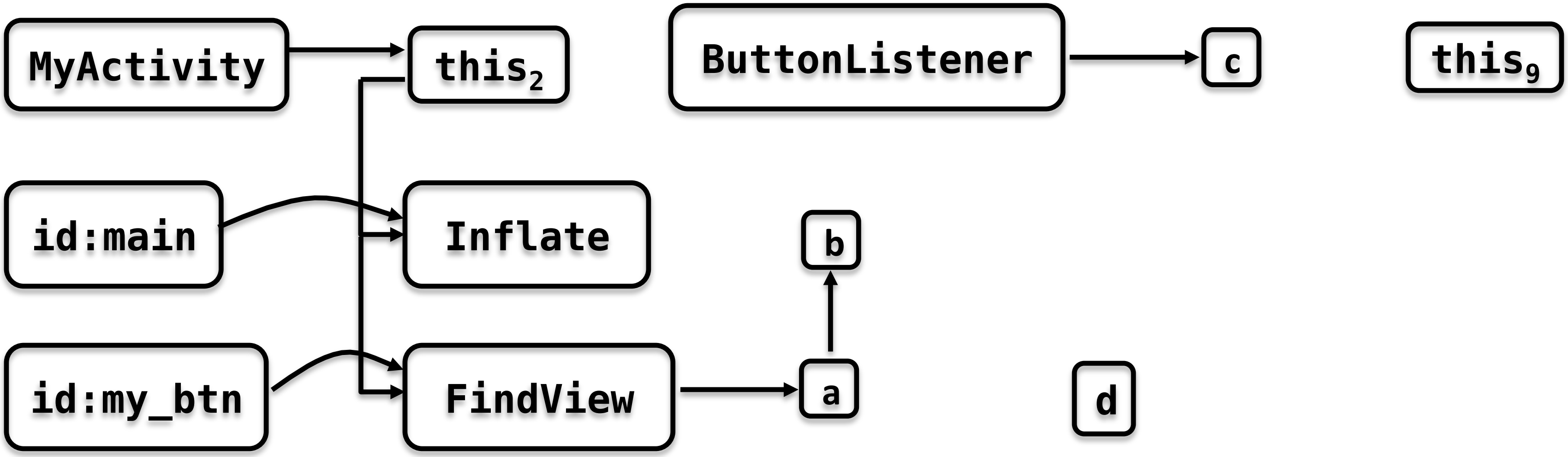
```
1  class MyActivity extends Activity {
2    void onCreate() {
3      this.setContentView(R.layout.main);  // Inflate
4      View a = this.findViewById(R.id.my_btn);  // FindView
5      Button b = (Button) a;
6      ButtonListener c = new ButtonListener();
7      b.setOnClickListener(c);  // SetListener  }  }
     ...    ...    ...
9    void onClick(View d) { ... }  }
```



Propagation edges and relevant nodes

Example

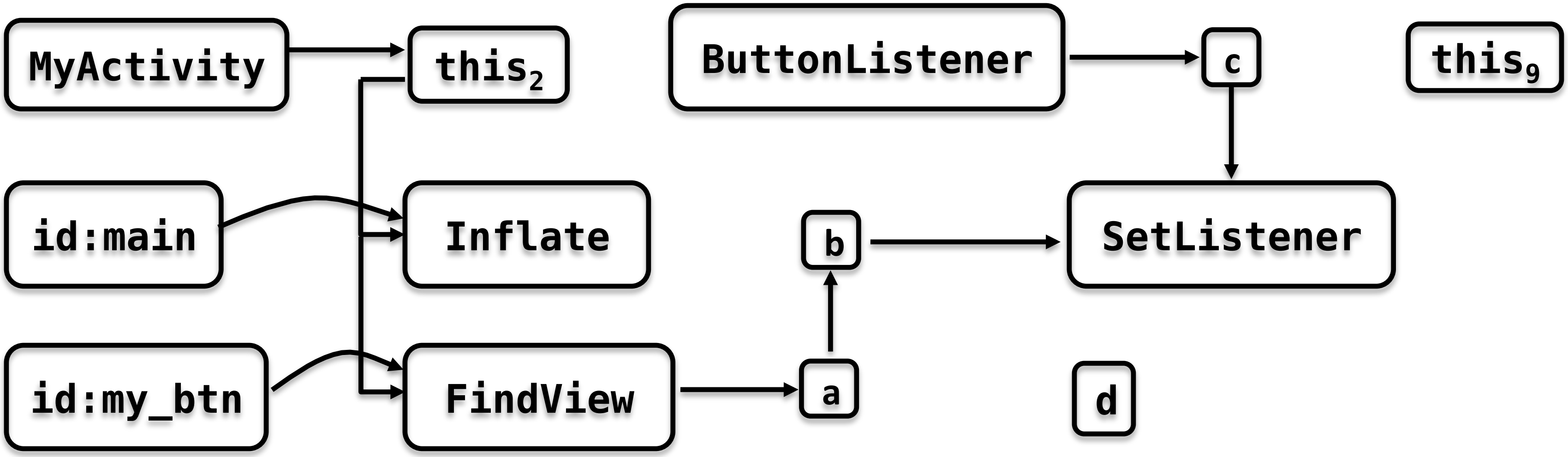
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
  ...    ...    ...
  void onClick(View d) { ... }  }
```



Propagation edges and relevant nodes

Example

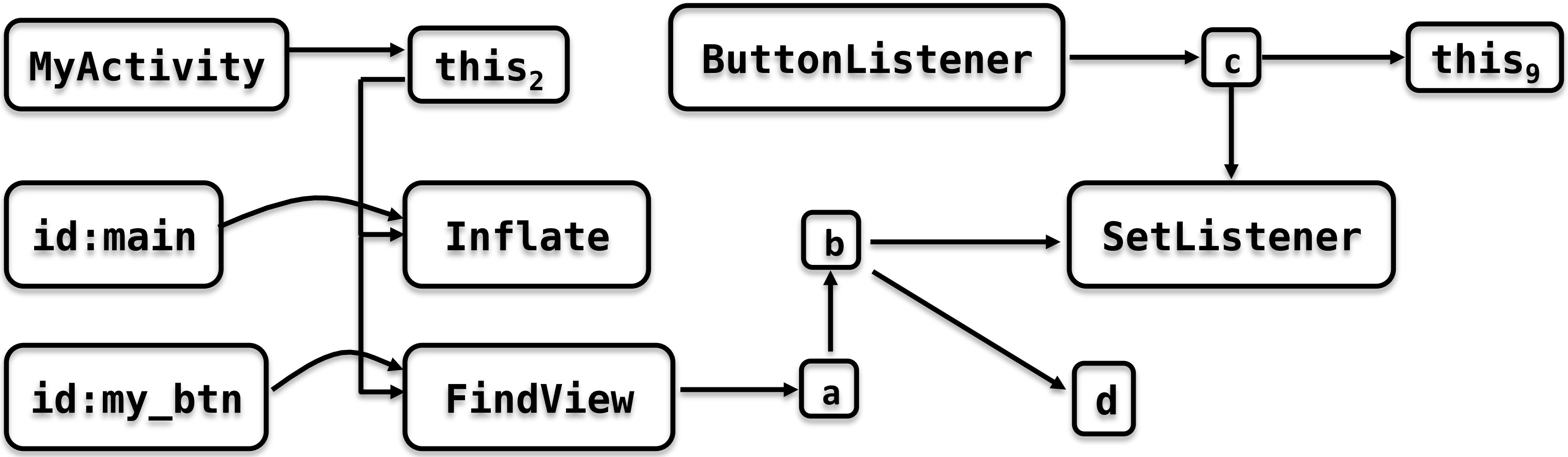
```
1  class MyActivity extends Activity {
2    void onCreate() {
3      this.setContentView(R.layout.main);  // Inflate
4      View a = this.findViewById(R.id.my_btn);  // FindView
5      Button b = (Button) a;
6      ButtonListener c = new ButtonListener();
7      b.setOnClickListener(c);  // SetListener  }  }
     ...    ...    ...
9    void onClick(View d) { ... }  }
```



Propagation edges and relevant nodes

Example

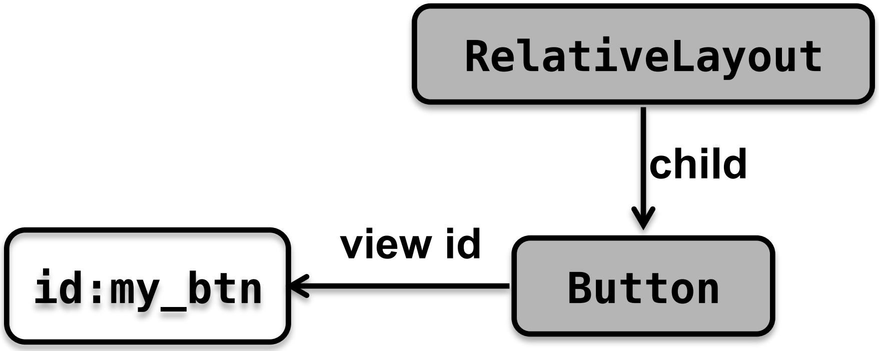
```
1  class MyActivity extends Activity {
2    void onCreate() {
3      this.setContentView(R.layout.main);  // Inflate
4      View a = this.findViewById(R.id.my_btn);  // FindView
5      Button b = (Button) a;
6      ButtonListener c = new ButtonListener();
7      b.setOnClickListener(c);  // SetListener  }  }
     ...    ...    ...
9    void onClick(View d) { ... }  }
```



Propagation edges and relevant nodes

Example

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```



RelativeLayout

child

Button

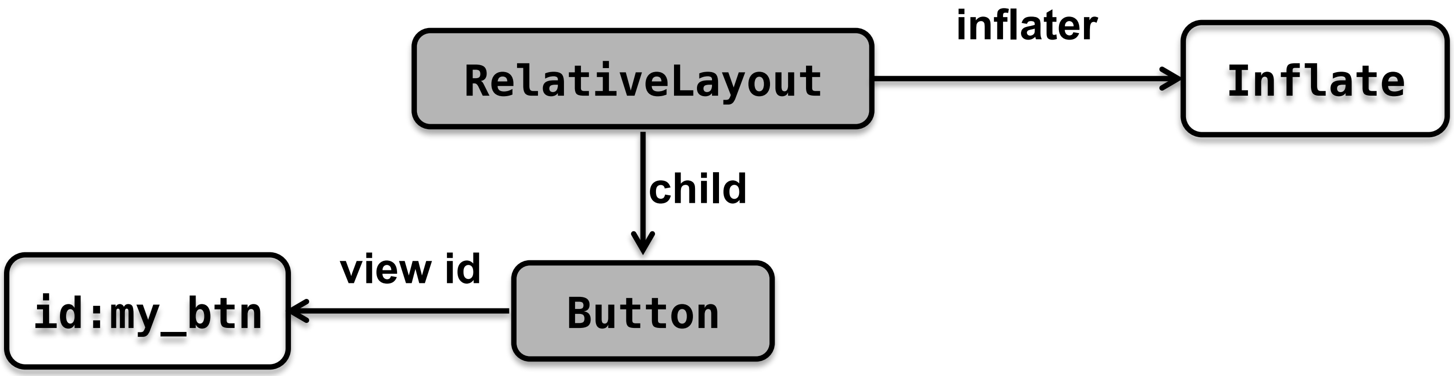
view id

id:my_btn

Property edges and relevant nodes

Example

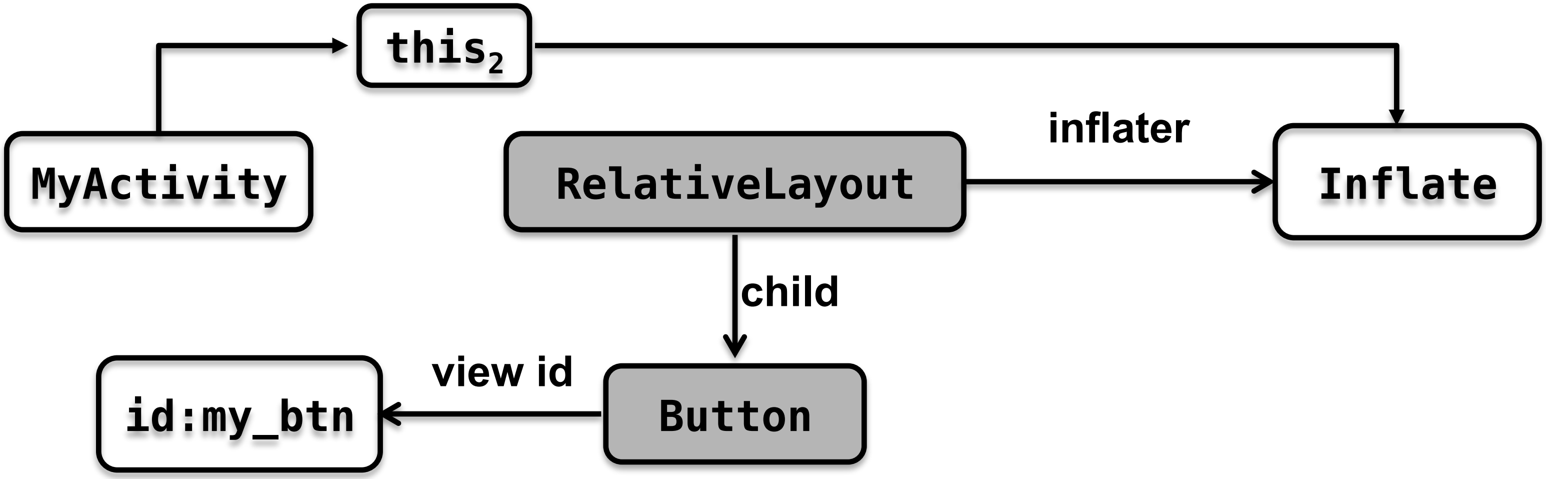
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```



Property edges and relevant nodes

Example

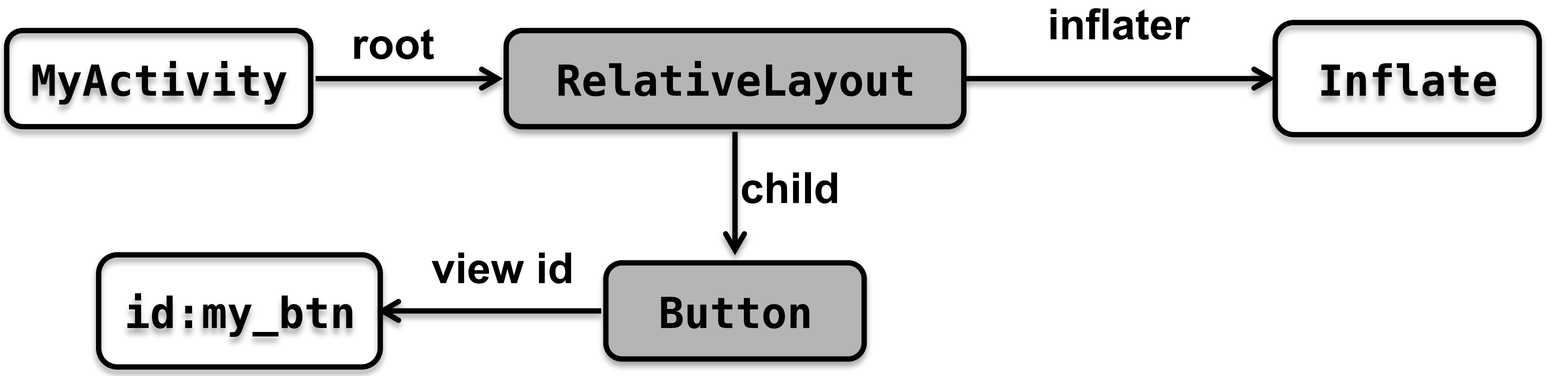
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```



Property edges and relevant nodes

Example

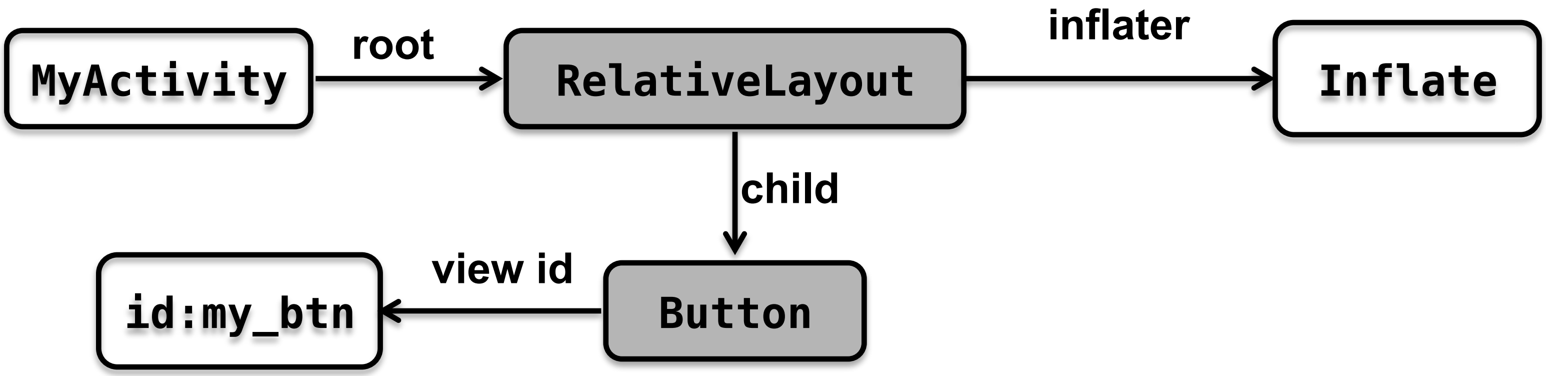
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```



Property edges and relevant nodes

Example

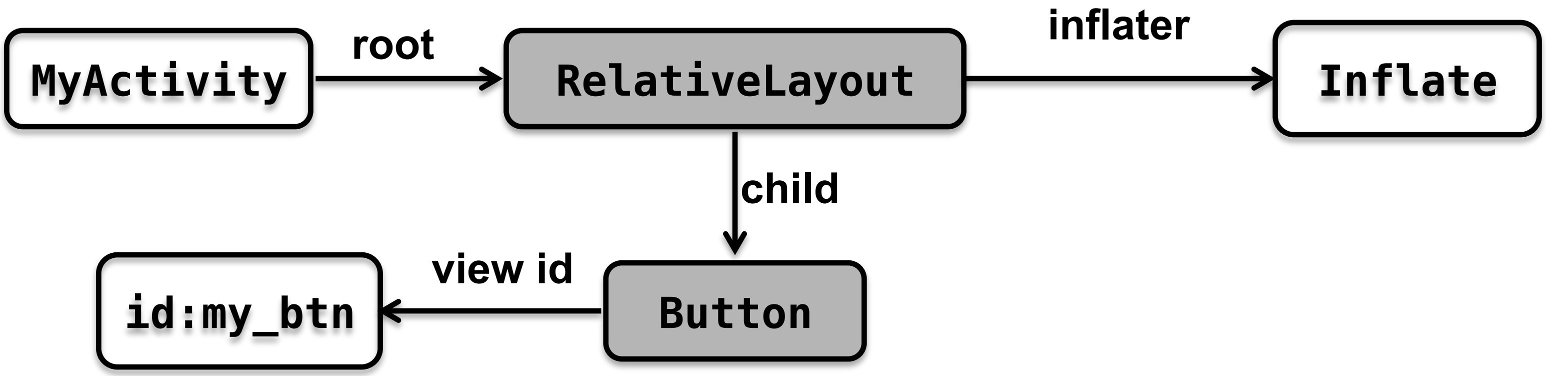
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```



Property edges and relevant nodes

Example

```
class MyActivity extends Activity {
 void onCreate() {
  this.setContentView(R.layout.main);  // Inflate
  View a = this.findViewById(R.id.my_btn);  // FindView
  Button b = (Button) a;
  ButtonListener c = new ButtonListener();
  b.setOnClickListener(c);  // SetListener  }  }
```



MyActivity

root

RelativeLayout

inflater

Inflate

child

Button

view id

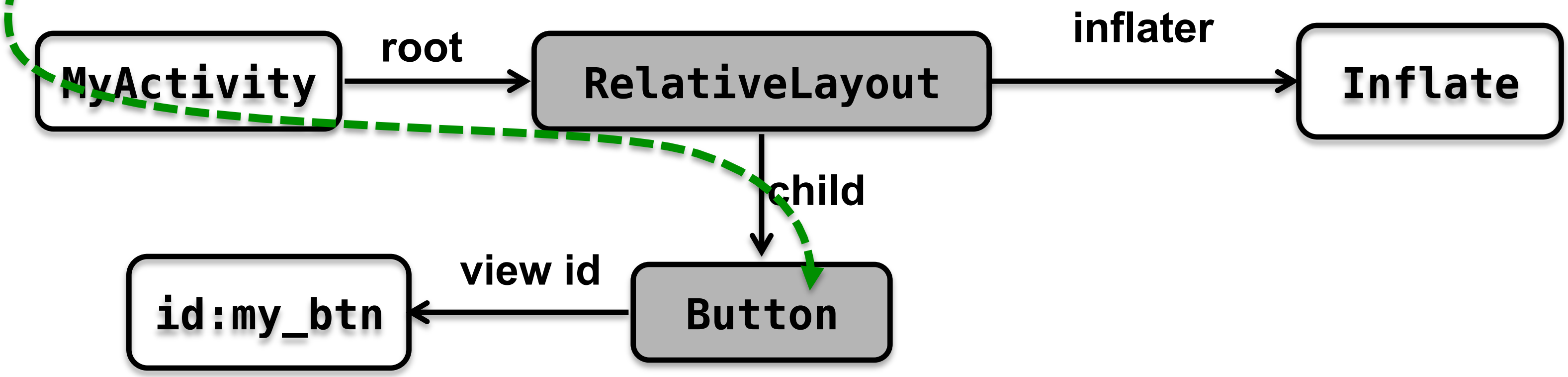
id:my_btn

Property edges and relevant nodes

Example

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```

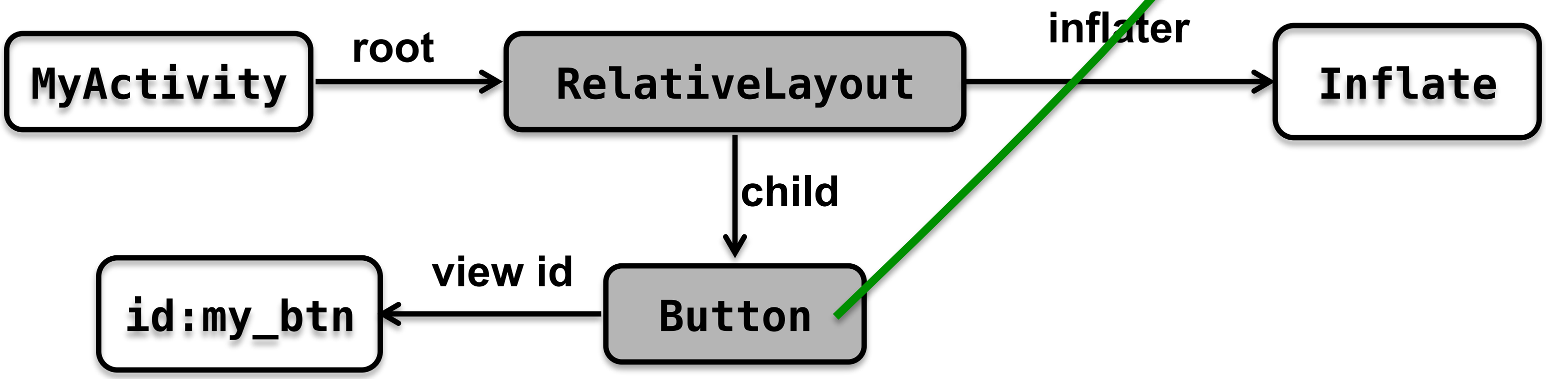
lookup performed by **FindView**



Property edges and relevant nodes

Example

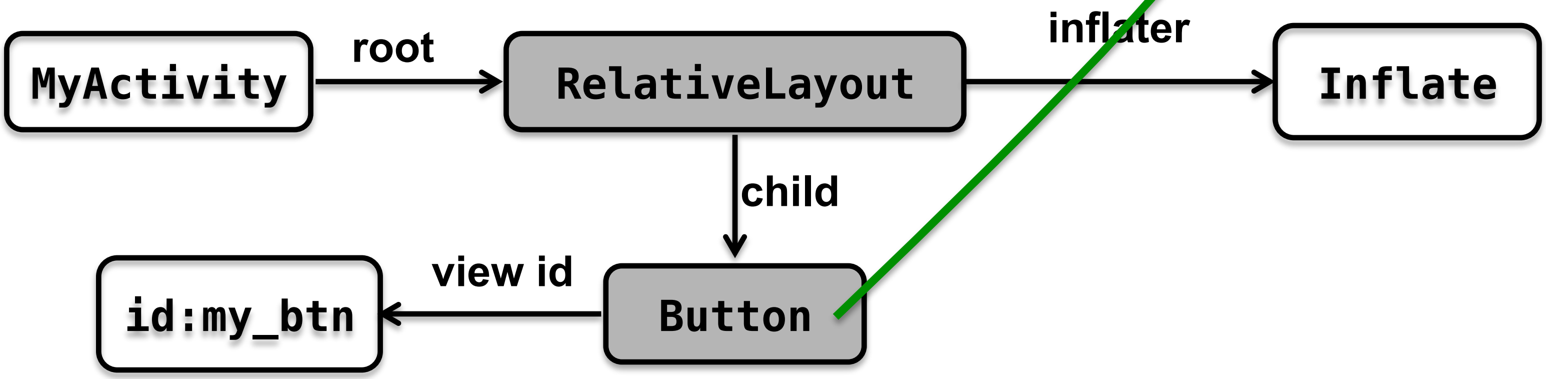
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```



Property edges and relevant nodes

Example

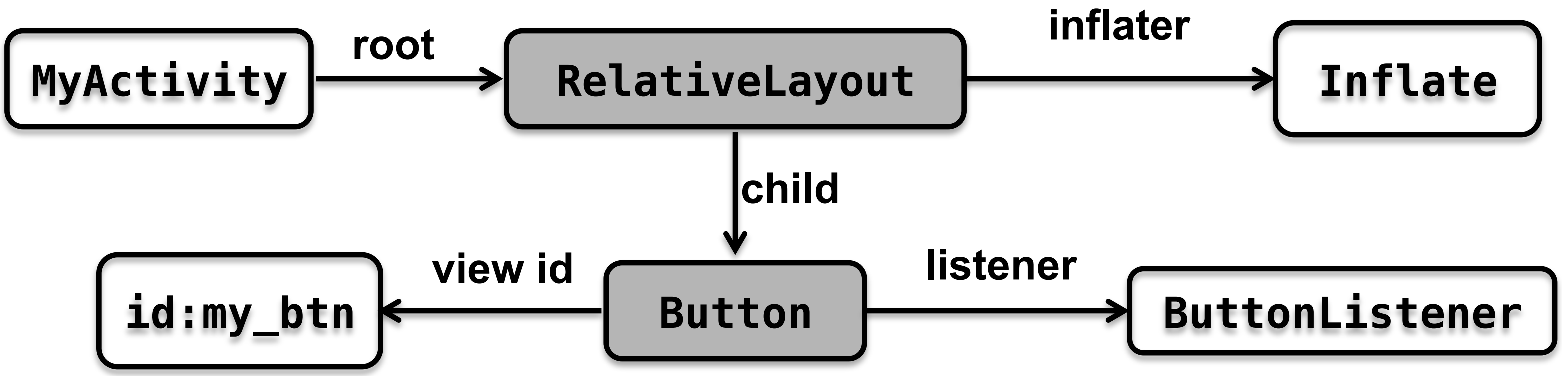
```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = ButtonListener
    b.setOnClickListener(c);  // SetListener  }  }
```



Property edges and relevant nodes

Example

```
class MyActivity extends Activity {
  void onCreate() {
    this.setContentView(R.layout.main);  // Inflate
    View a = this.findViewById(R.id.my_btn);  // FindView
    Button b = (Button) a;
    ButtonListener c = new ButtonListener();
    b.setOnClickListener(c);  // SetListener  }  }
```



Property edges and relevant nodes

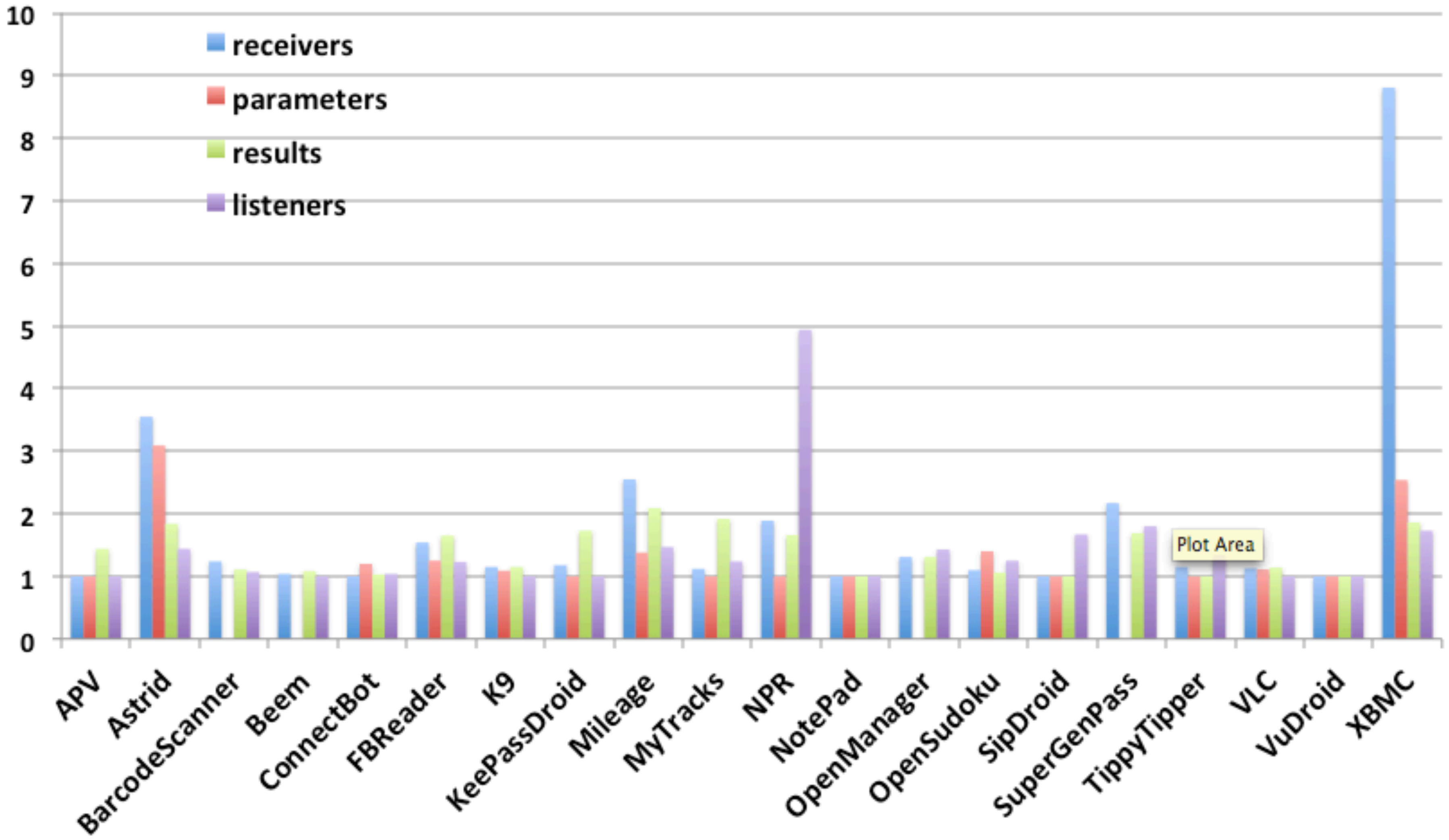
Implementation

- Input
  - Java bytecode of the application
  - Relevant XML files
- Output
  - Parent-child relationships between views
  - Association of activities with root views
  - Association of views with listeners
  - Variables and fields referring to views, activities, listeners
- Analysis algorithm
  1. Create initial constraint graph from app code
  2. Solve propagation constraints for IDs, activities, listeners
  3. Fixed-point computation for flow of views between operation nodes

Evaluation

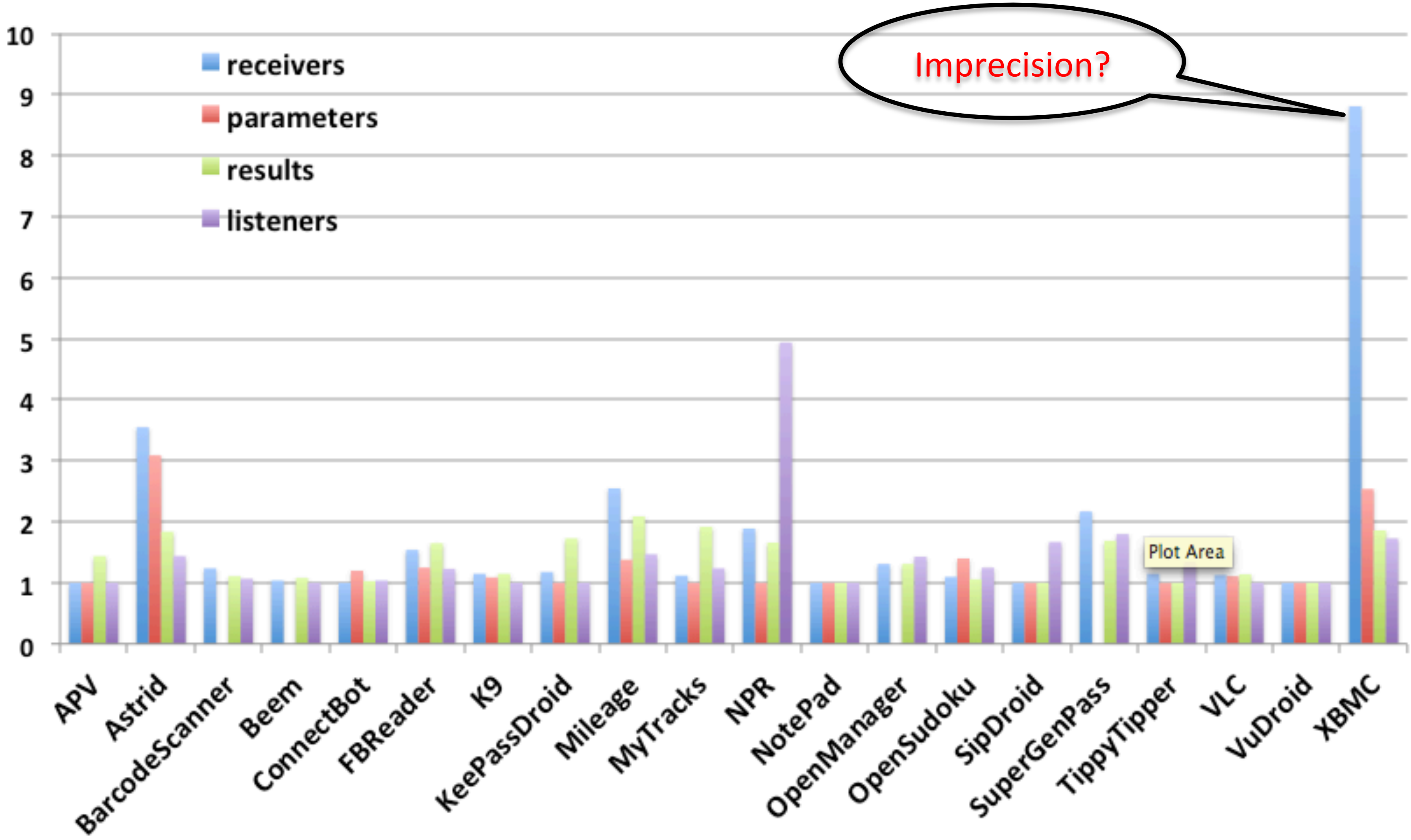
- Experiments on 20 open-source Android apps
- Experiment I – application characterization
    - Constraint graph: number of various types of nodes
    - Result: Android-specific features are widely used
- Experiment II – analysis performance and precision
    - Running time to perform the constraint analysis
        - Less than 5 seconds for each app
    - Average number of objects for variables at relevant operations – e.g.
        - v1.addChild(v2) – receiver v1, parameter v2
        - v = x.findViewById(…) – result v
        - v.setListener(m) – receiver v, listener m

Precision Measurements



Average number of objects for variables at relevant operations

Precision Measurements



Average number of objects for variables at relevant operations

Conclusions

- First static analysis to focus on GUI-related Android constructs
- Proposed constraint-based algorithm exhibits high precision and low cost
- Critical building block for other analyses and tools for Android
- Software release
  - GATOR: Pro***g***ram ***A***nalysis ***T***oolkit F***o***r And***r***oid
  - http://www.cse.ohio-state.edu/presto/software/

Thank you