LinuxTesting.org

Symbolic Memory Graphs invariant and corresponding optimizations for SMGCPA

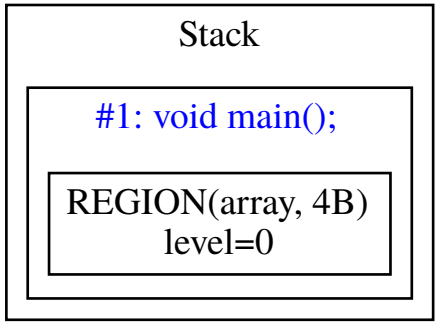
Anton Vasilyev

ISP RAS

Ivannikov Institute for System Programming of the RAS

Symbolic Memory Graph

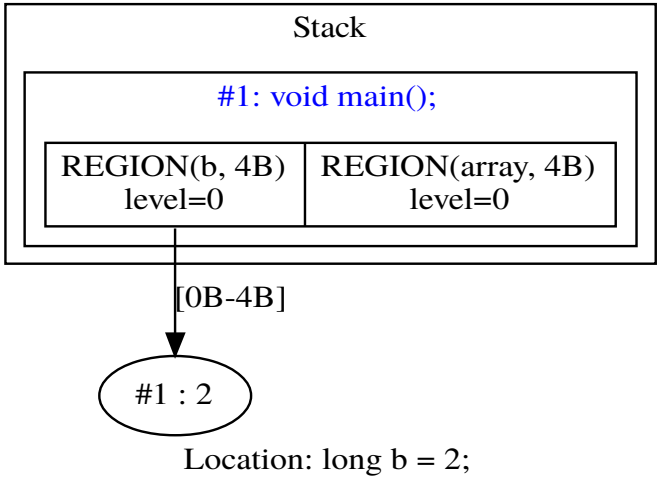
```
void main() {
    void *array;
    long b = 2;
    long c = 3;
    array = calloc(1, 16);
    memcpy(&array[4], &b, 4);
    memcpy(&array[5], &c, 4);
}
```



Location: void *array;

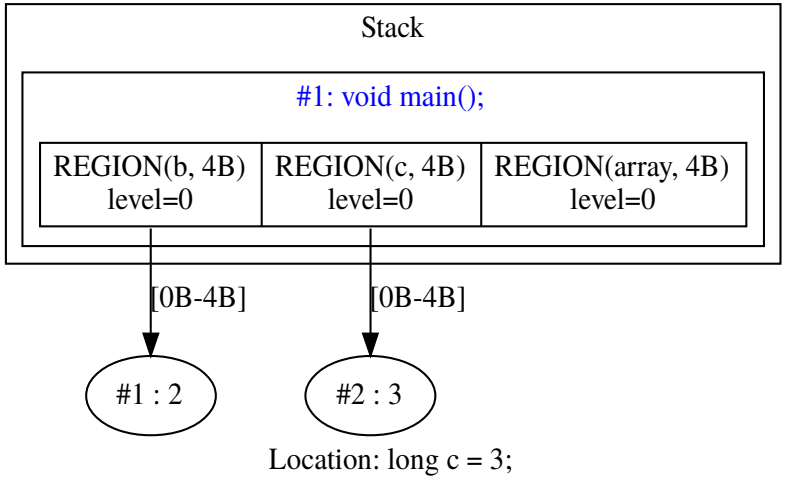
Symbolic Memory Graph

```
void main() {
    void *array;
    long b = 2;
    long c = 3;
    array = calloc(1, 16);
    memcpy(&array[4], &b, 4);
    memcpy(&array[5], &c, 4);
}
```



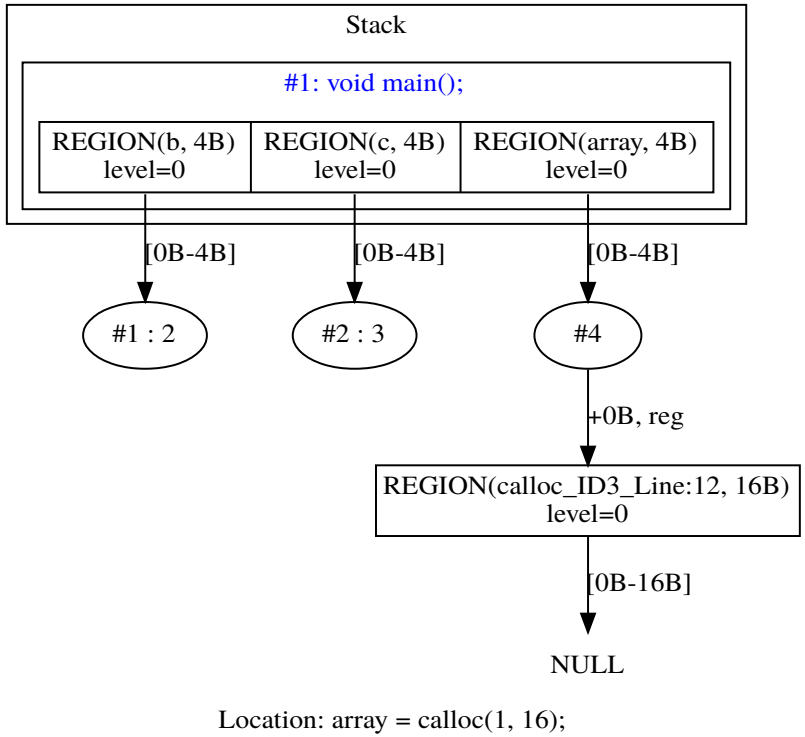
Symbolic Memory Graph

```
void main() {
    void *array;
    long b = 2;
    long c = 3;
    array = calloc(1, 16);
    memcpy(&array[4], &b, 4);
    memcpy(&array[5], &c, 4);
}
```



Symbolic Memory Graph

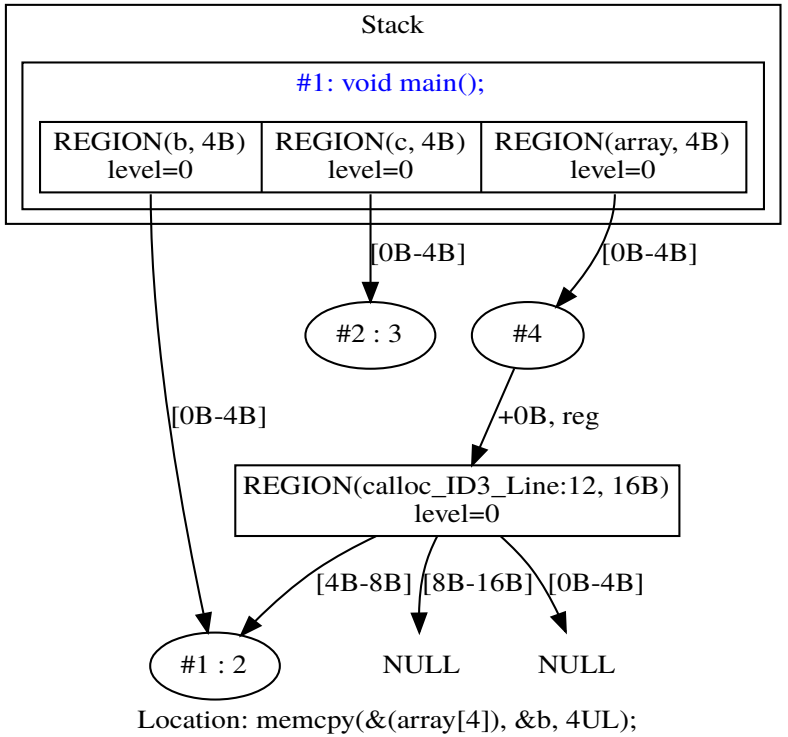
```
void main() {
    void *array;
    long b = 2;
    long c = 3;
    array = calloc(1, 16);
    memcpy(&array[4], &b, 4);
    memcpy(&array[5], &c, 4);
}
```



Location: array = calloc(1, 16);

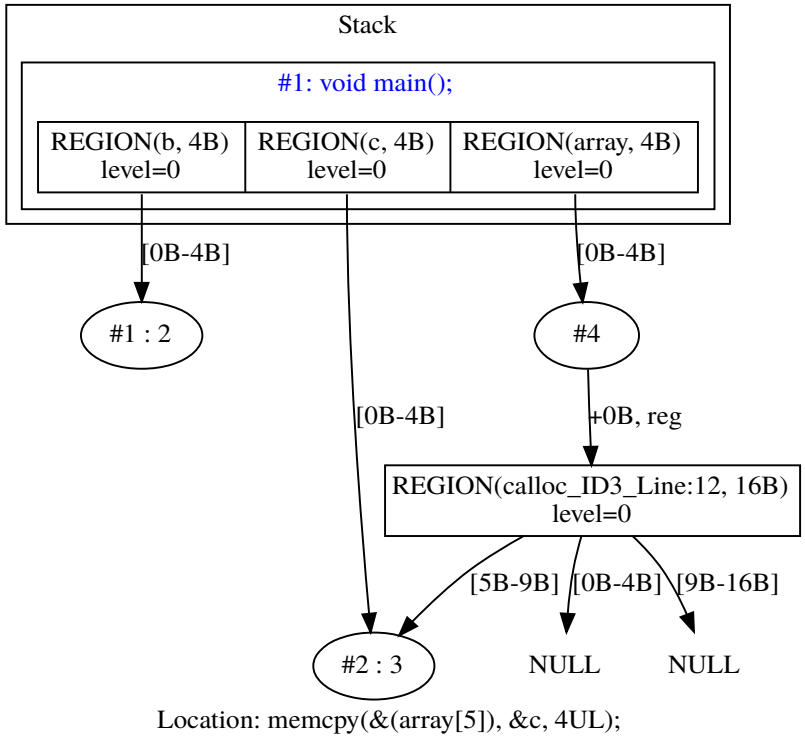
Symbolic Memory Graph

```
void main() {
    void *array;
    long b = 2;
    long c = 3;
    array = calloc(1, 16);
    memcpy(&array[4], &b, 4);
    memcpy(&array[5], &c, 4);
}
```



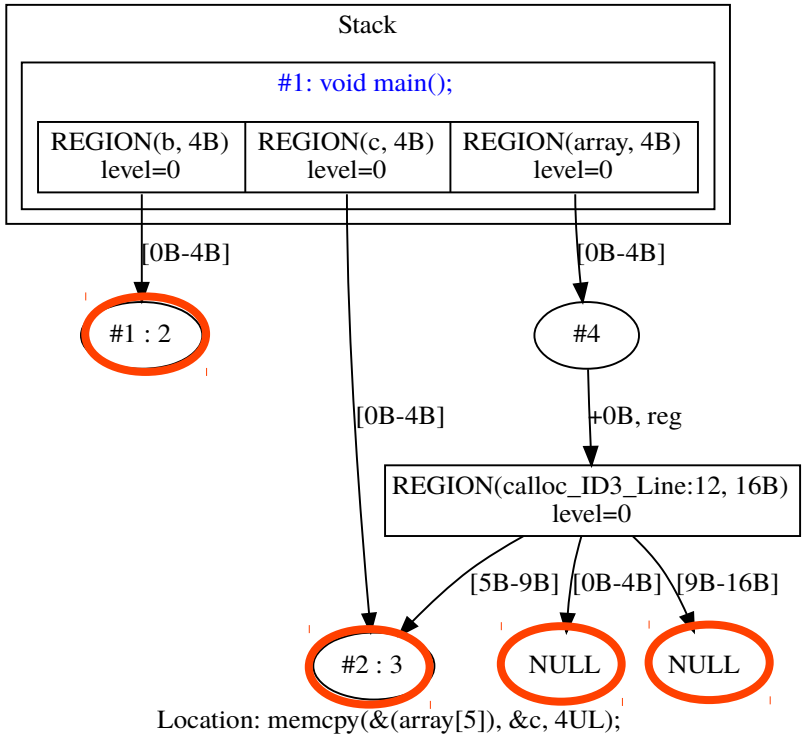
Symbolic Memory Graph

```
void main() {
    void *array;
    long b = 2;
    long c = 3;
    array = calloc(1, 16);
    memcpy(&array[4], &b, 4);
    memcpy(&array[5], &c, 4);
}
```



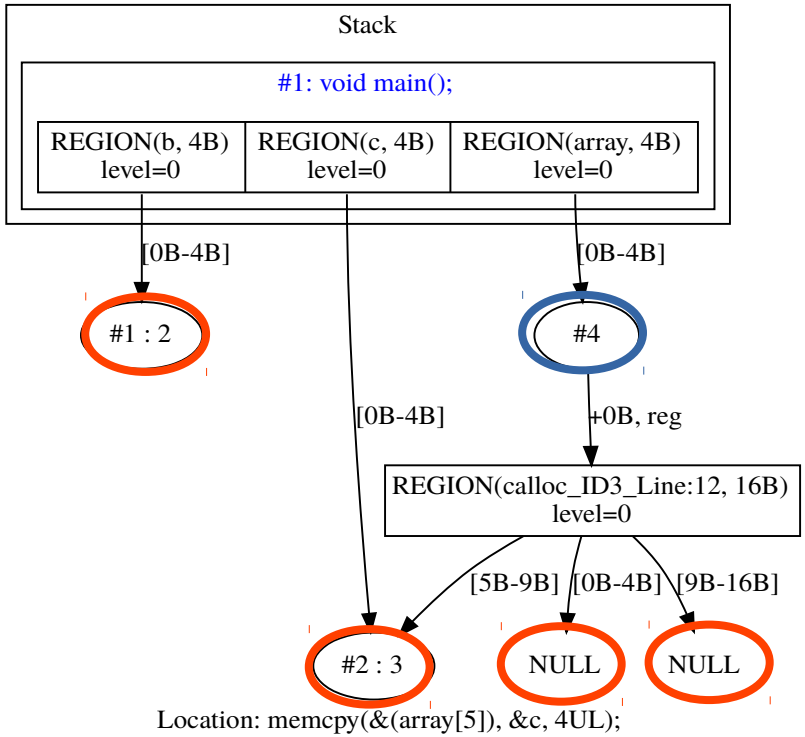
Symbolic Values

- Values



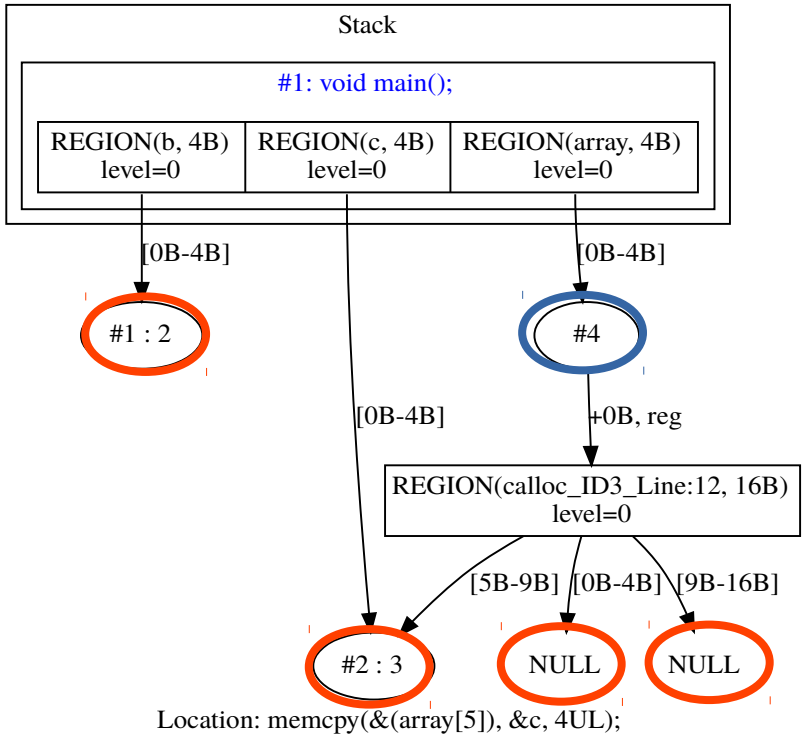
Symbolic Values

- Values
- Pointers



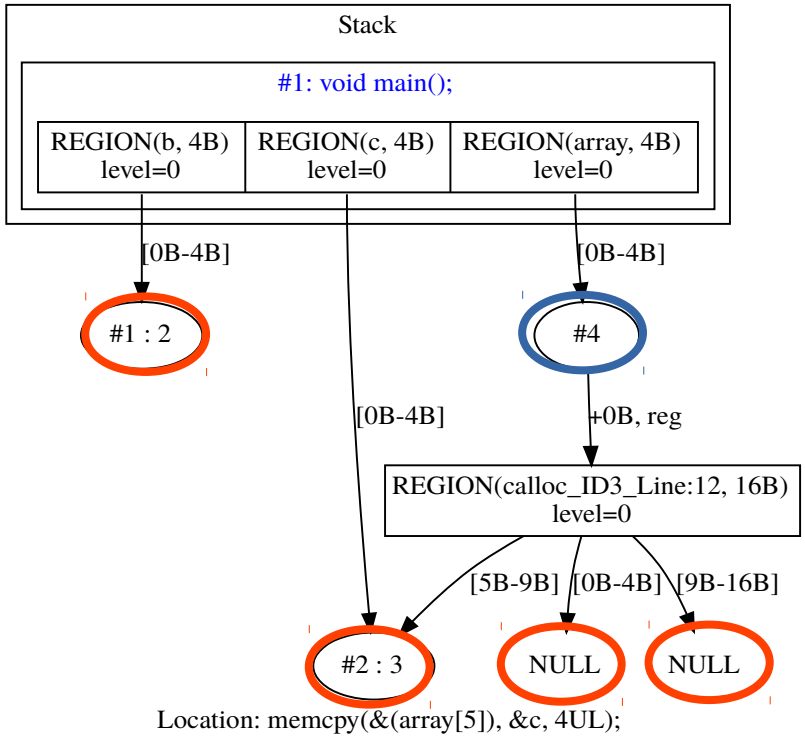
Invariant of Memory Graph

- Separate values for object don`t intesect

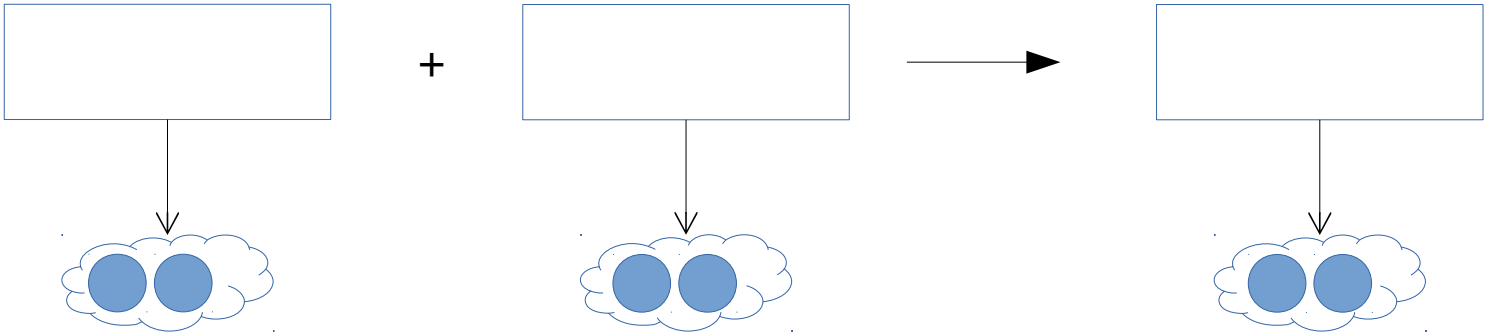


Invariant of Memory Graph

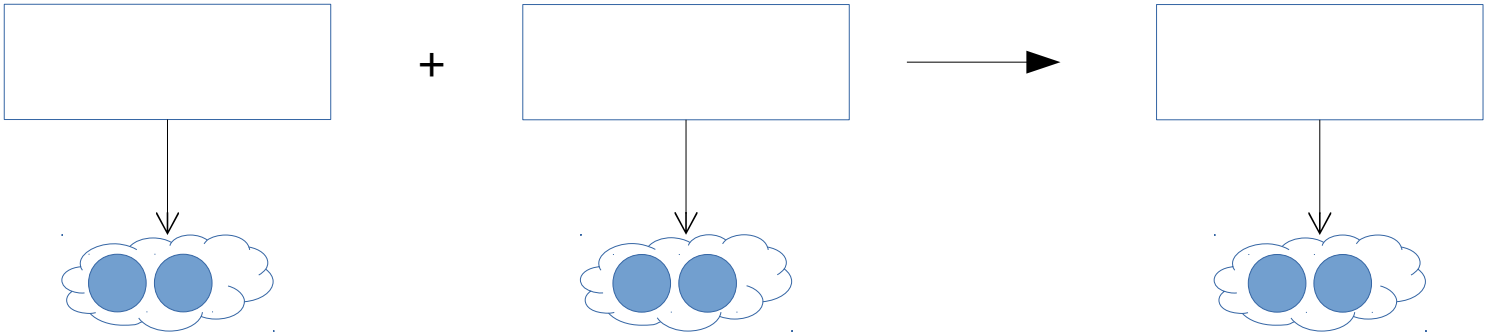
- Separate values for object don`t intesect
- Use immutable collection with sort by objects and offsets



Join based on object



Join based on object

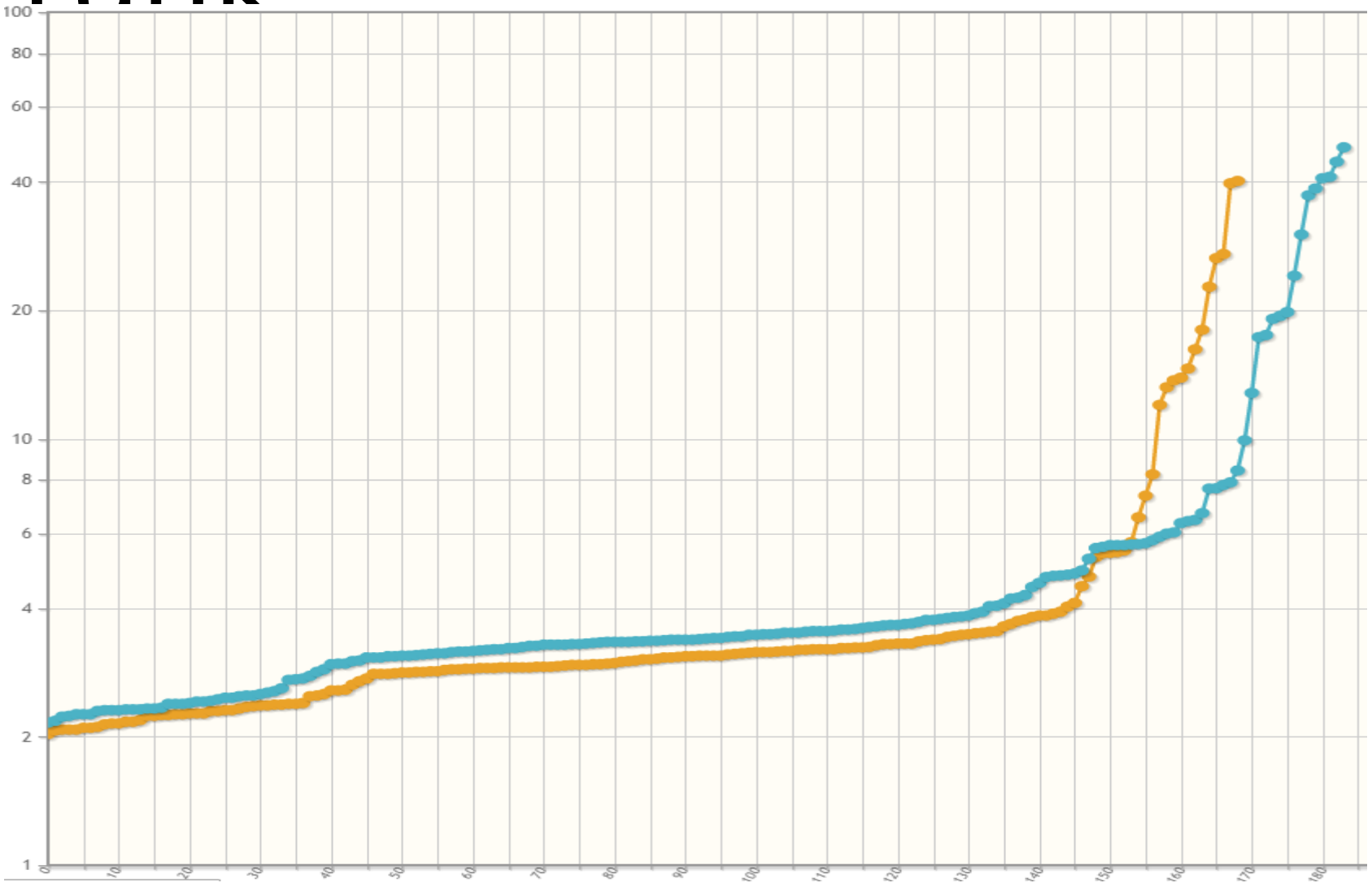


- Fast check on equivalense of HasValueEdgeSet on selected objects

Results

	Trunk	Trunk soundness	Branch
Correct true	147	76	69
Correct false	115	108	100
Incorrect true	6	1	0
Incorrect false	28	22	83
Timeouts	81	147	108
Exceptions	4	26	1

Results. Branch vs fixed Trunk



Future work

- Mathematical prove of correctness
- Abstractions for strings, arrays, set of values, work with loops
- Symbolic size and offset
- Refactore predicate extention
- Refactore storage of pointers
- Repair comunication explicit and symbolic values
- Merge branches