ISE SRA

Leibniz Universität Hannover

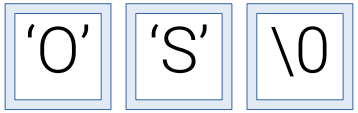
Multivariant ELF Executables for Dynamic Variability via Address-Space Views

Dominik Töllner, Leibniz Universität Hannover

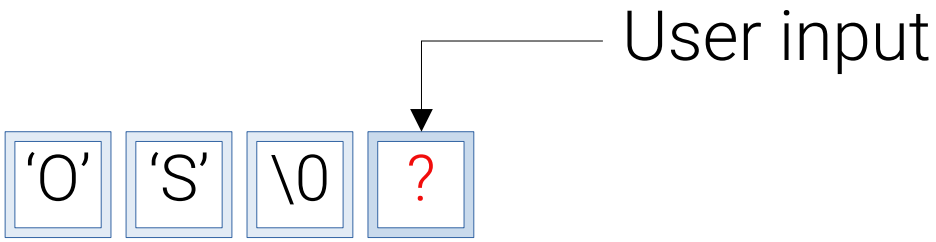
Fachgruppentreffen Betriebssysteme der Gesellschaft für Informatik

16.03.2022

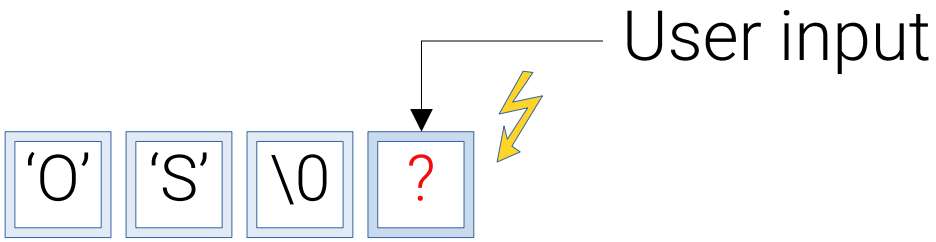
Motivation: ASan – What we got



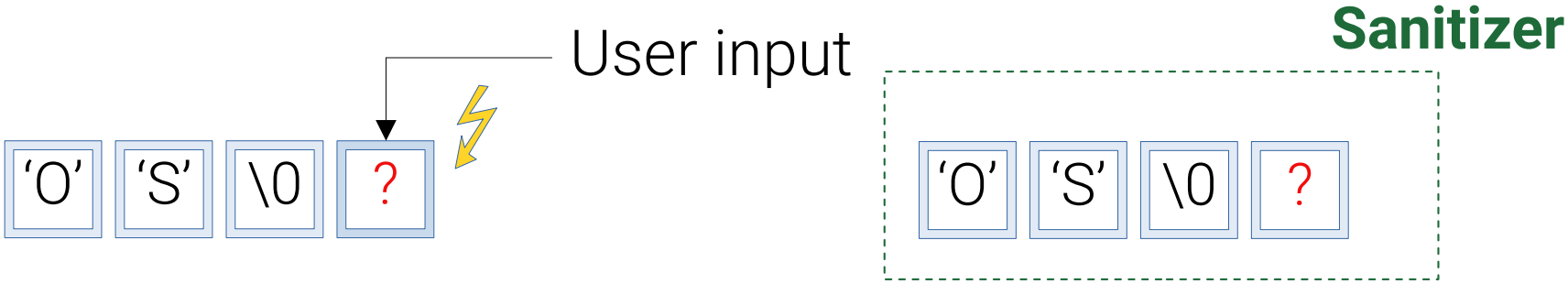
Motivation: ASan – What we got



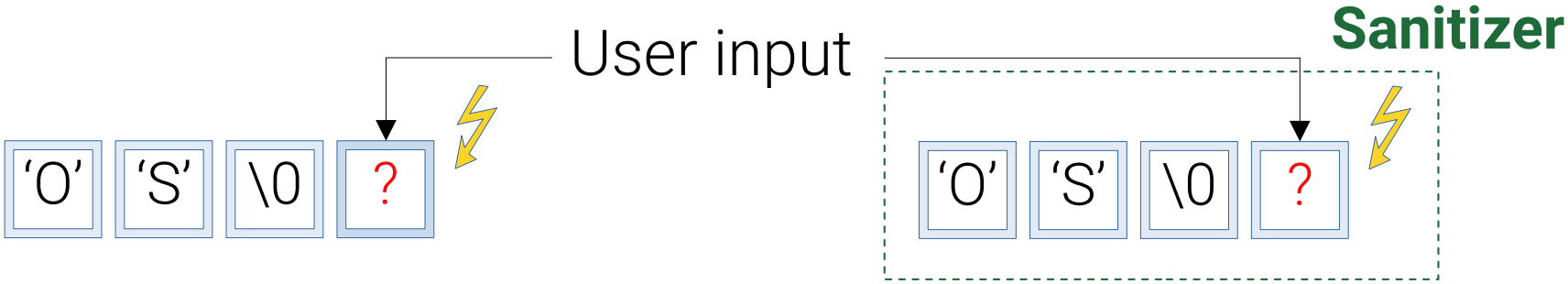
Motivation: ASan – What we got



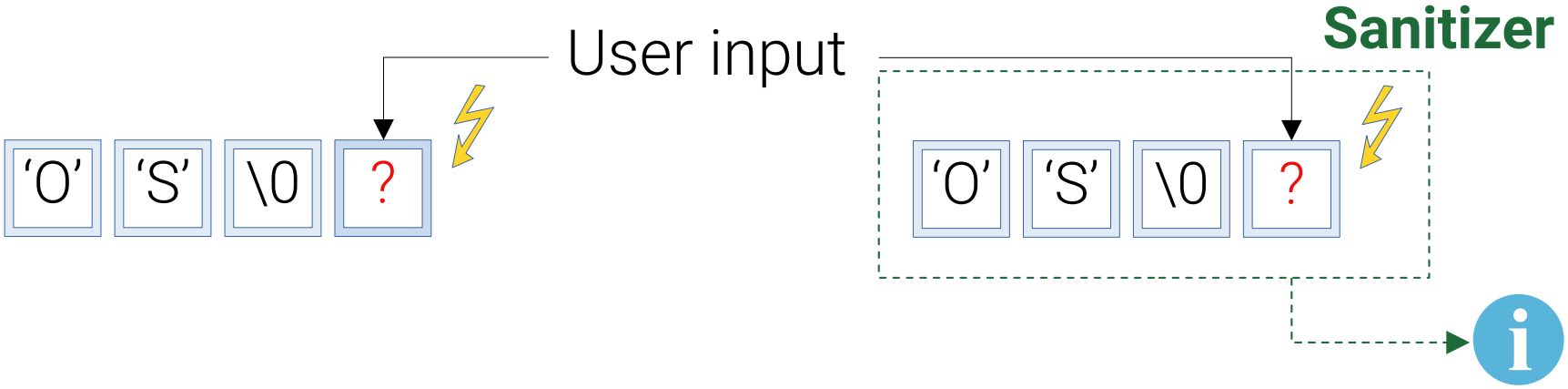
Motivation: ASan – What we got



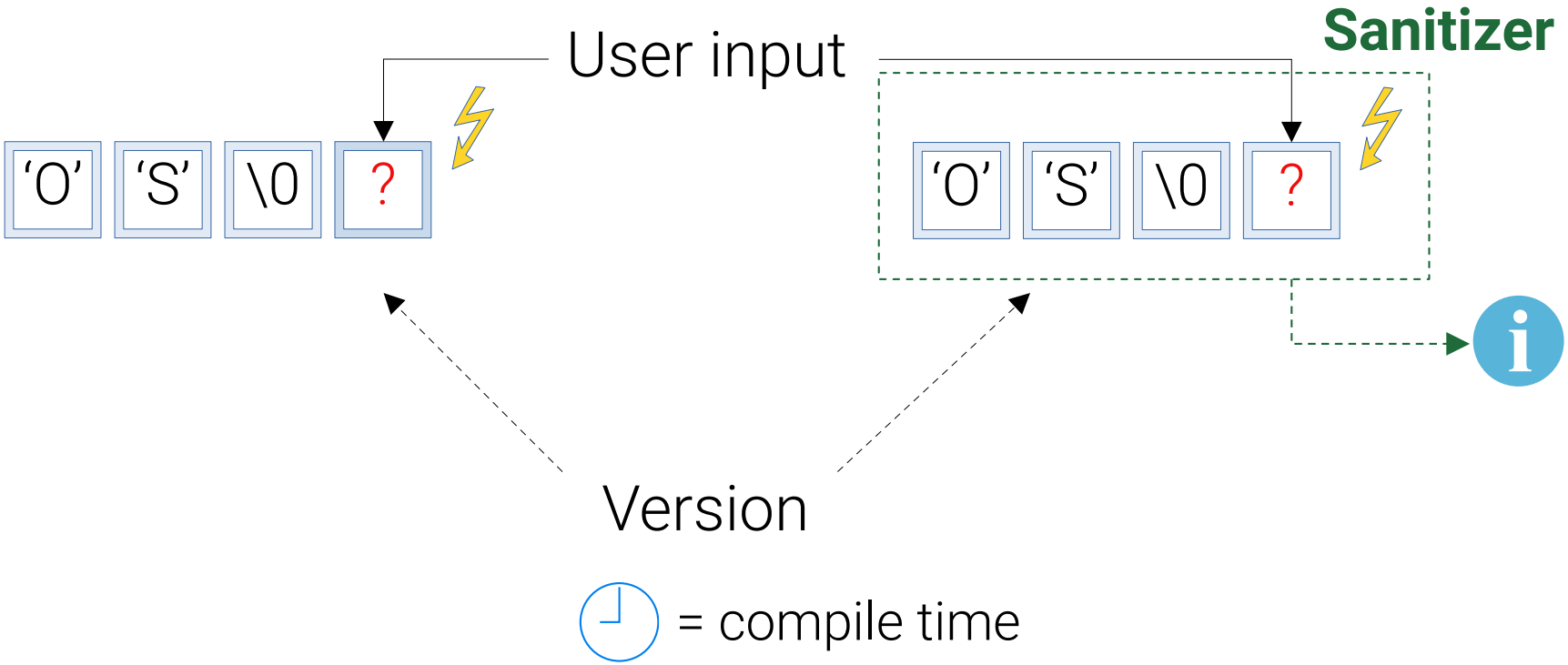
Motivation: ASan – What we got



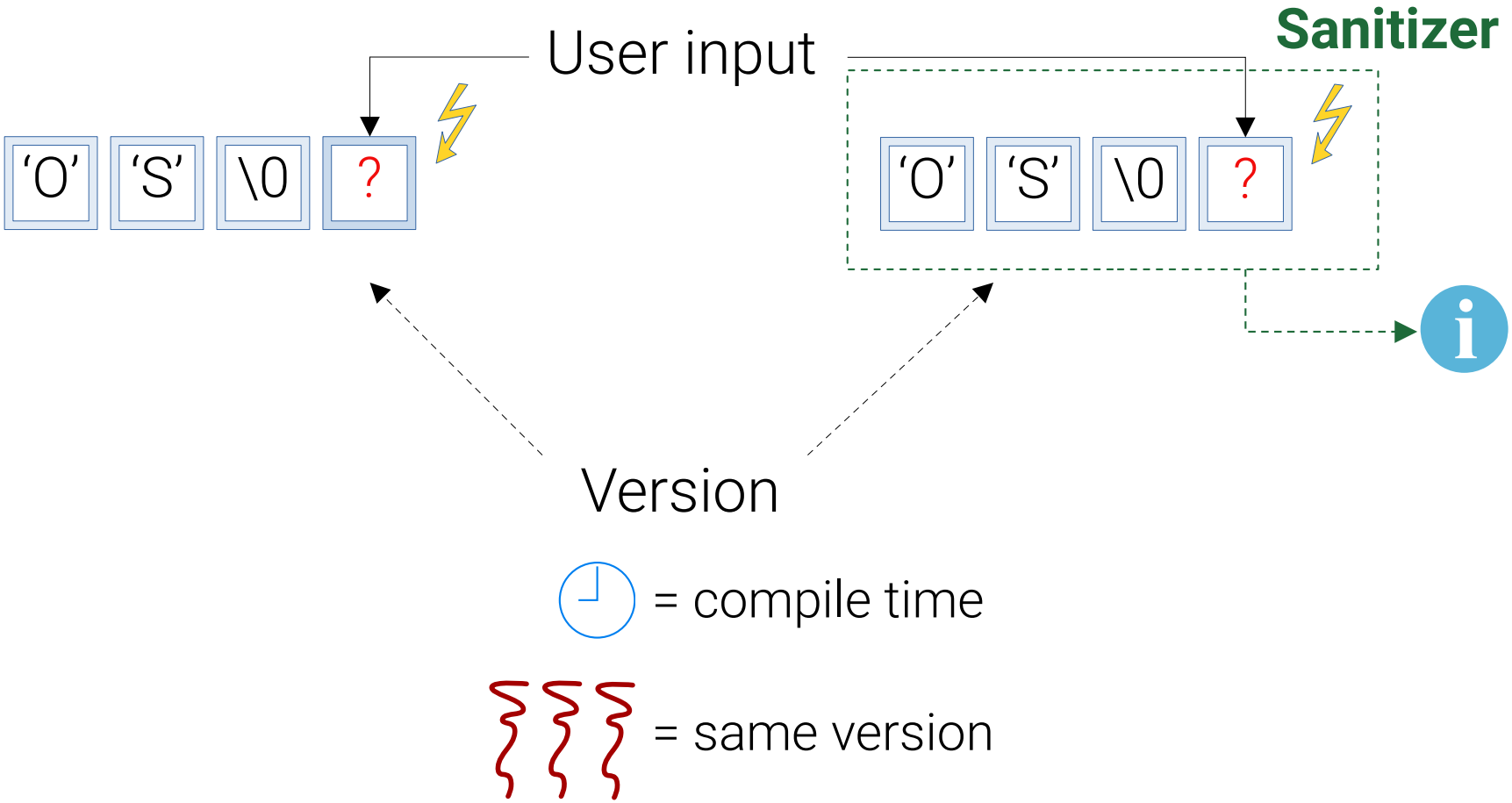
Motivation: ASan – What we got



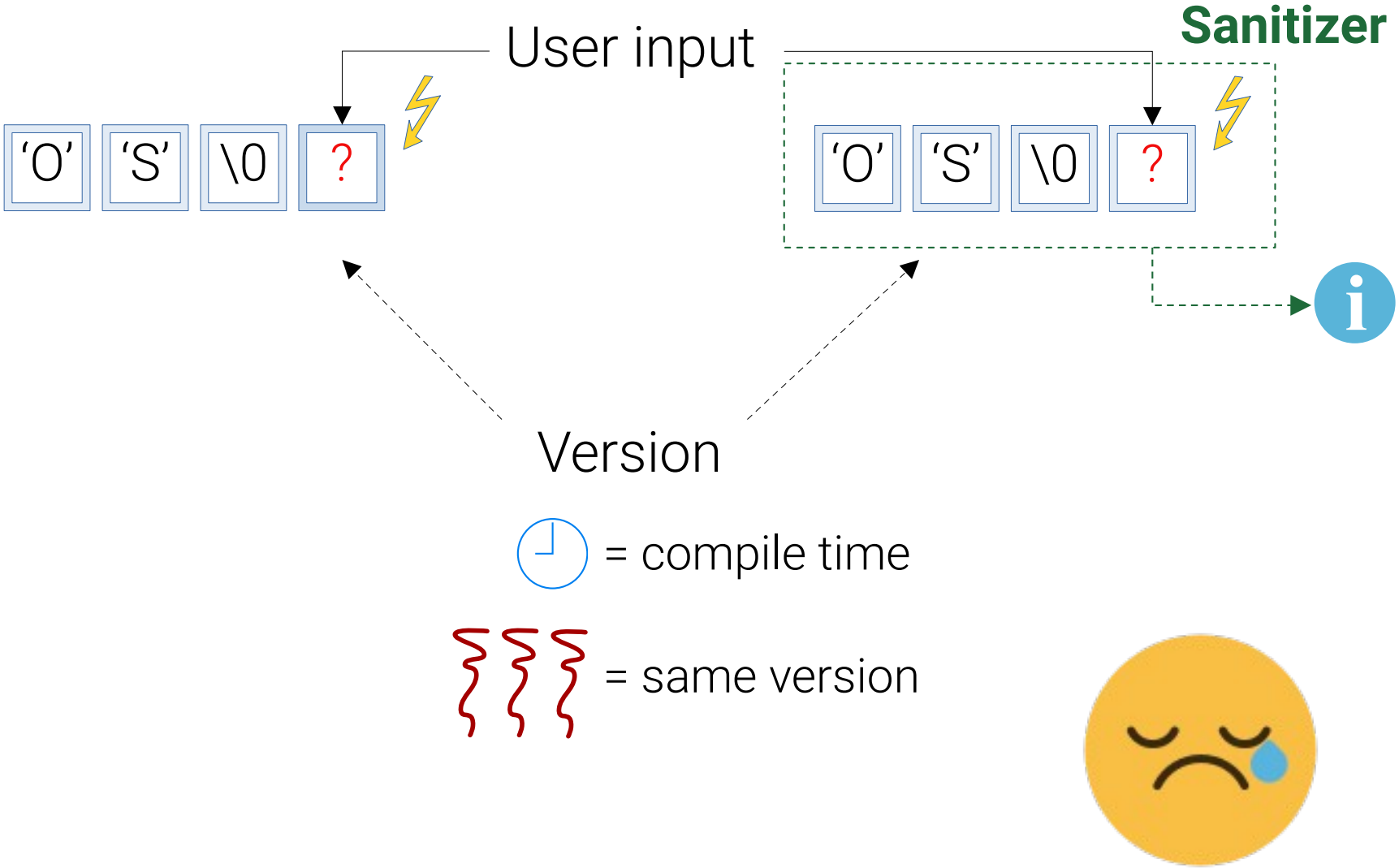
Motivation: ASan – What we got



Motivation: ASan – What we got



Motivation: ASan – What we got

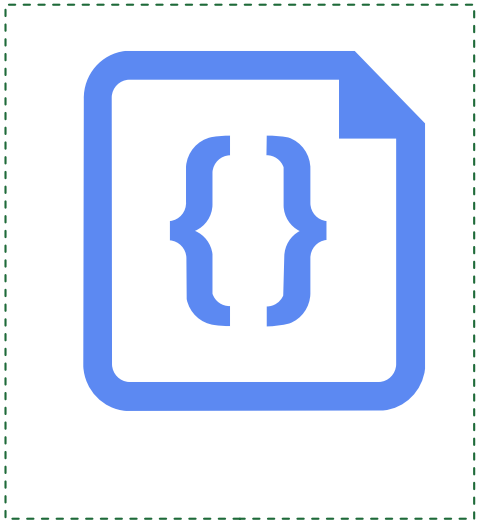


Motivation: ASan – What we want

Not sanitized

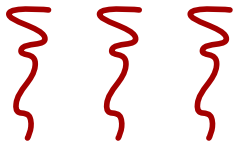
T1 T2 T3

Sanitized



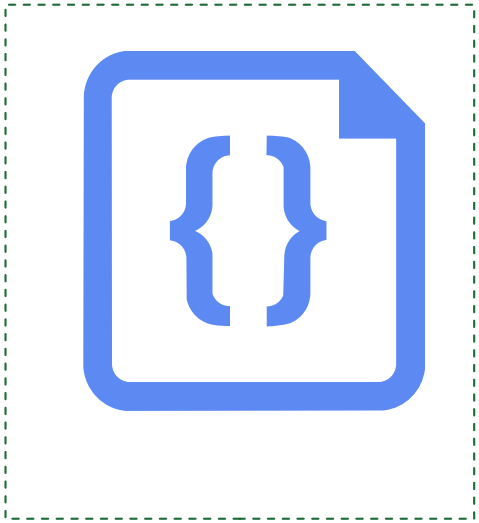
Motivation: ASan – What we want

Not sanitized



T1 T2 T3

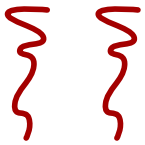
Sanitized



= run time

Motivation: ASan – What we want

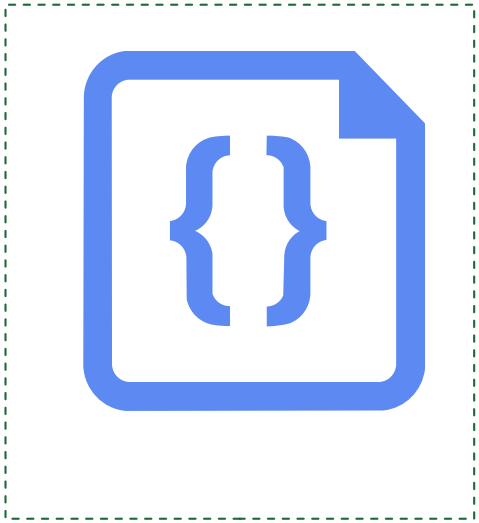
Not sanitized



T2 T3

= run time

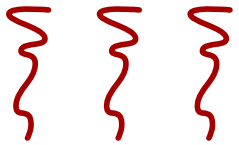
Sanitized



T1

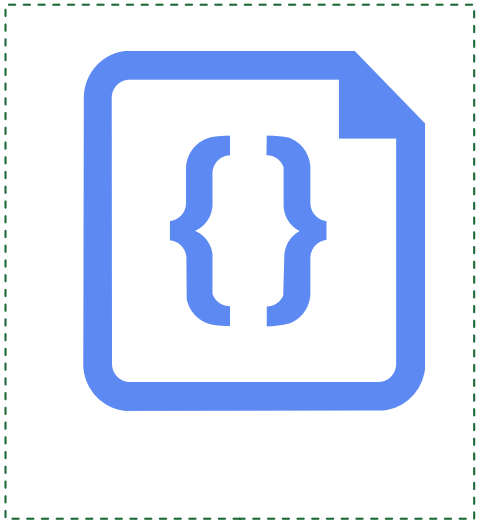
Motivation: ASan – What we want

Not sanitized



T1 T2 T3

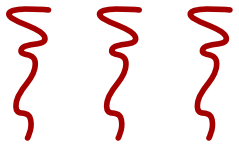
Sanitized



= run time

Motivation: ASan – What we want

Not sanitized

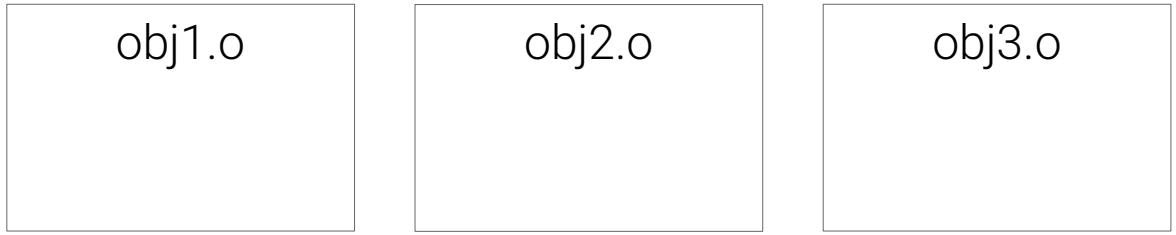


T1 T2 T3

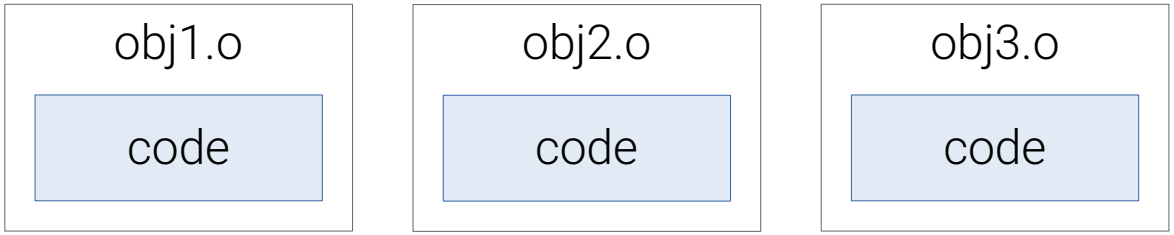
= run time

Sanitized

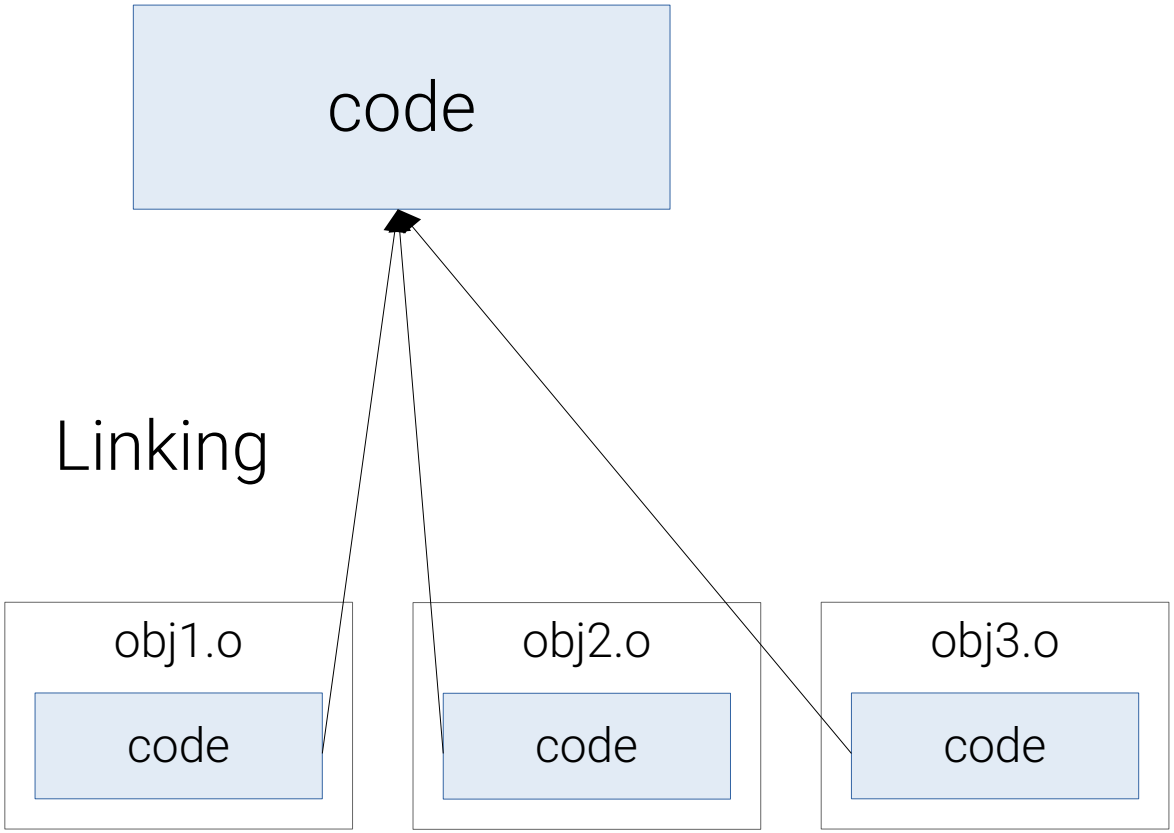
Fundamentals



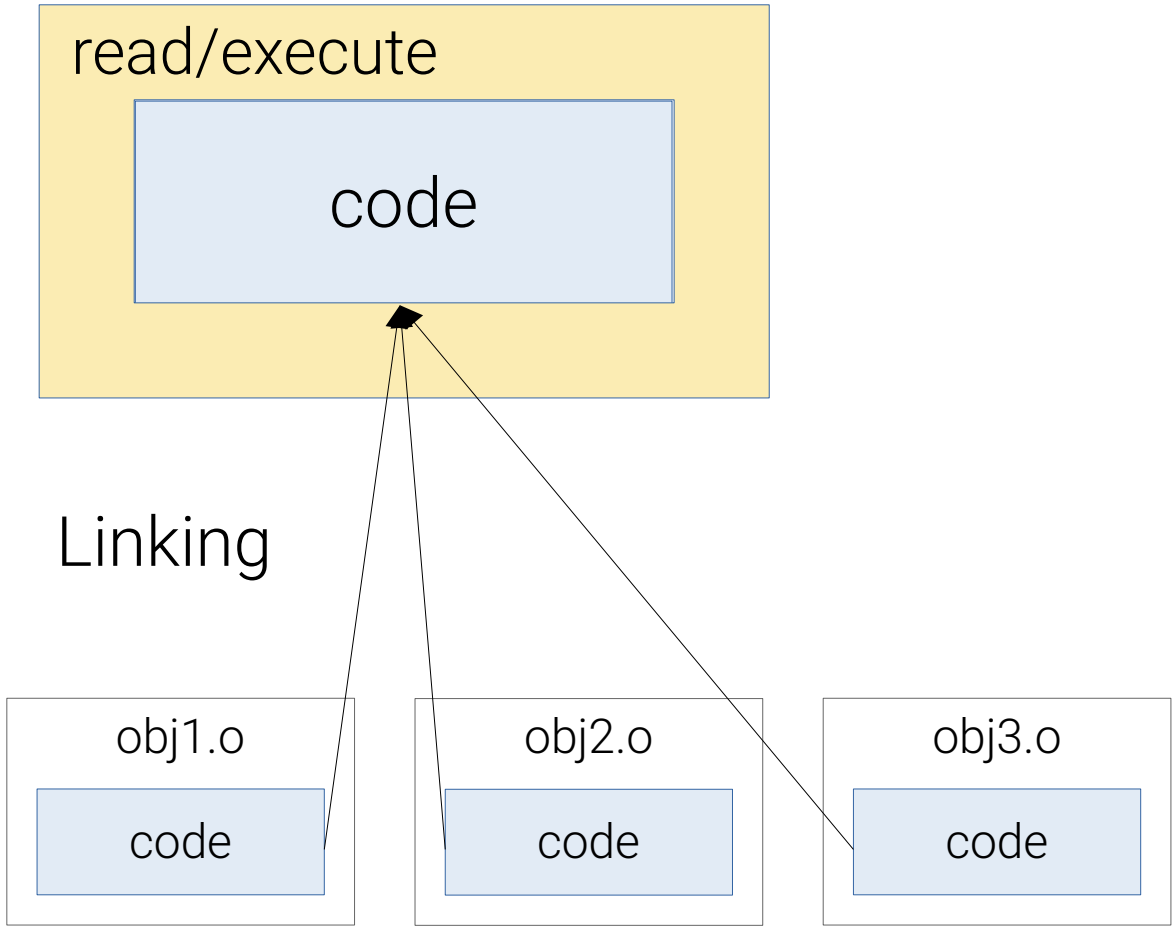
Fundamentals



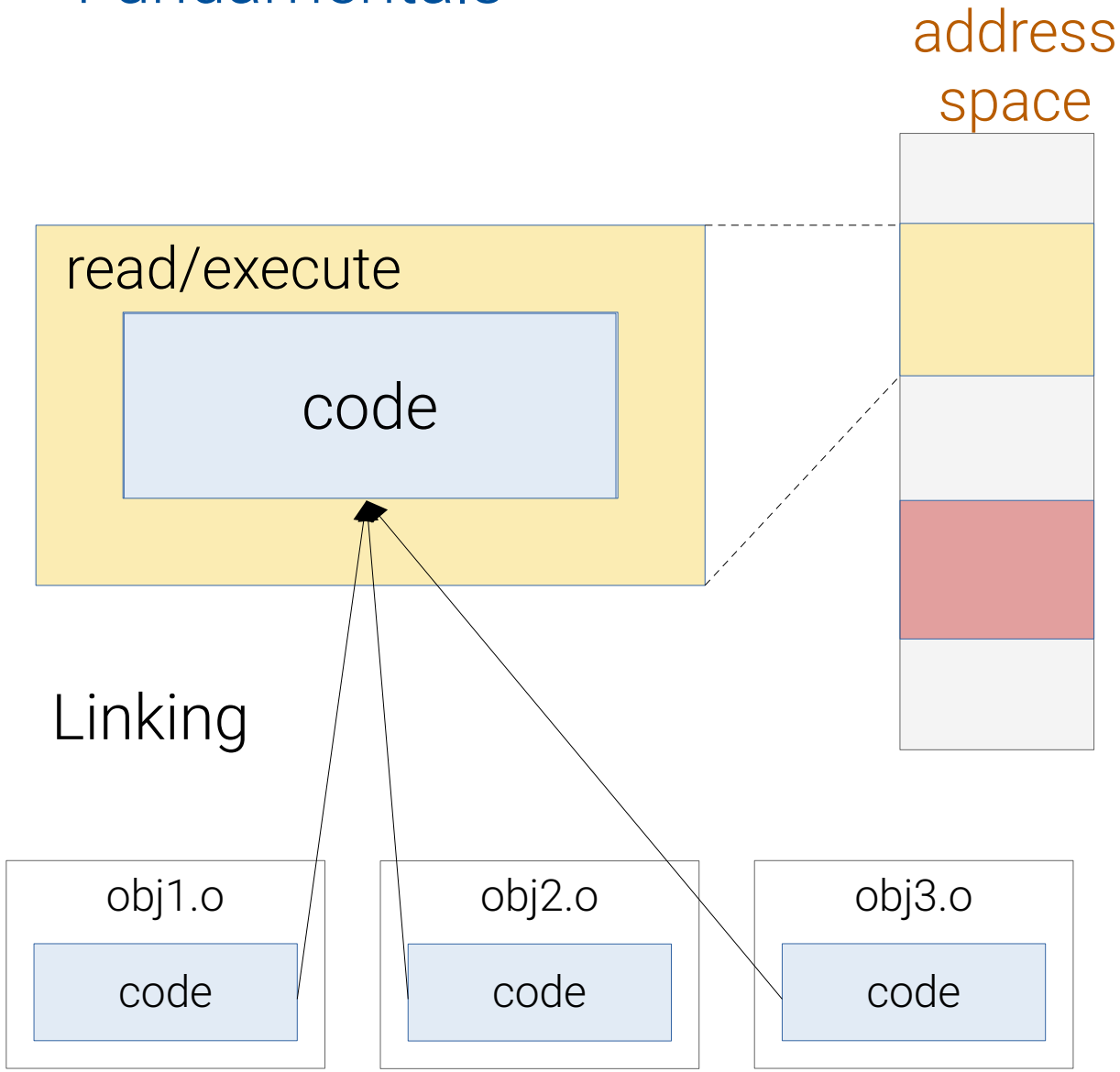
Fundamentals



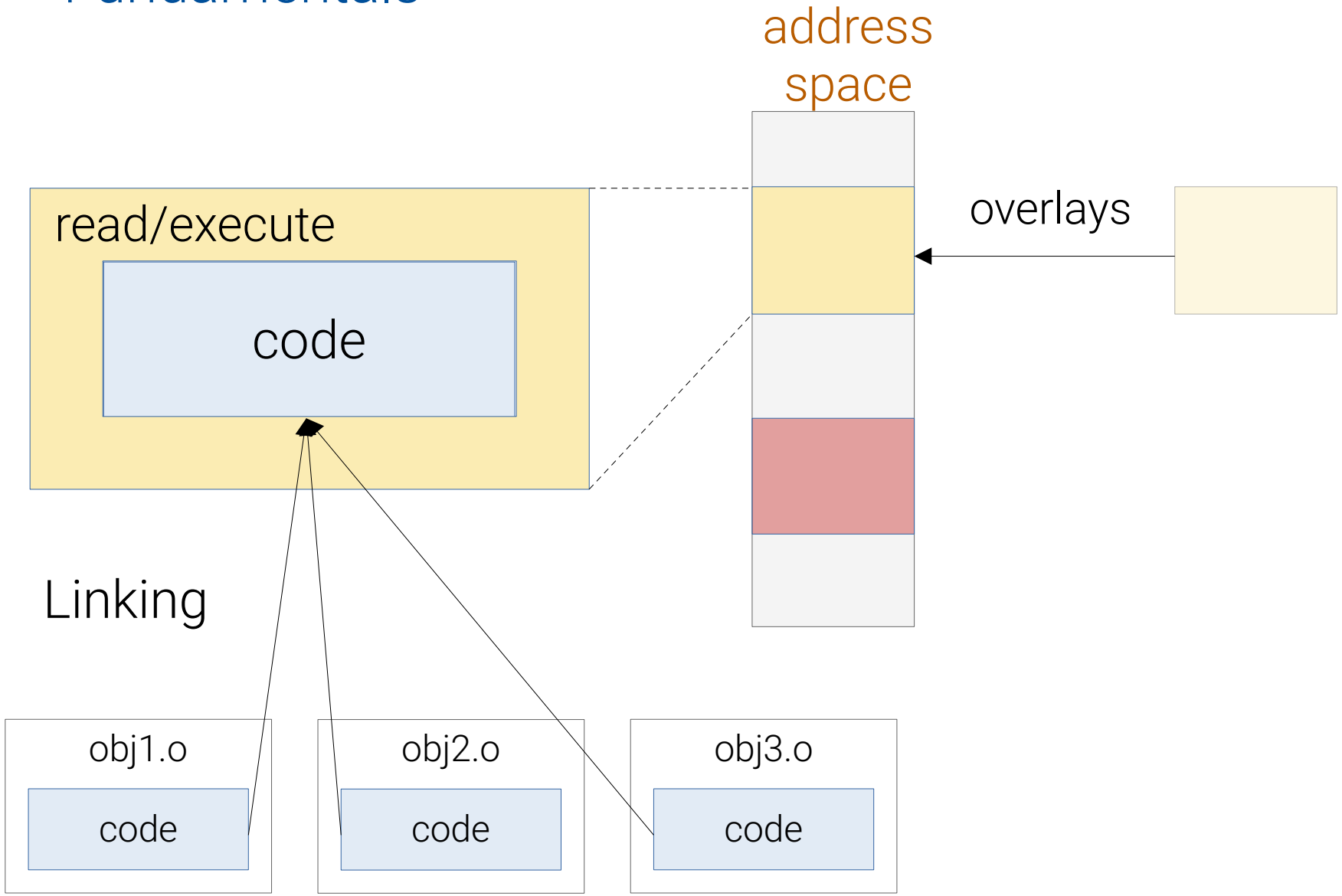
Fundamentals



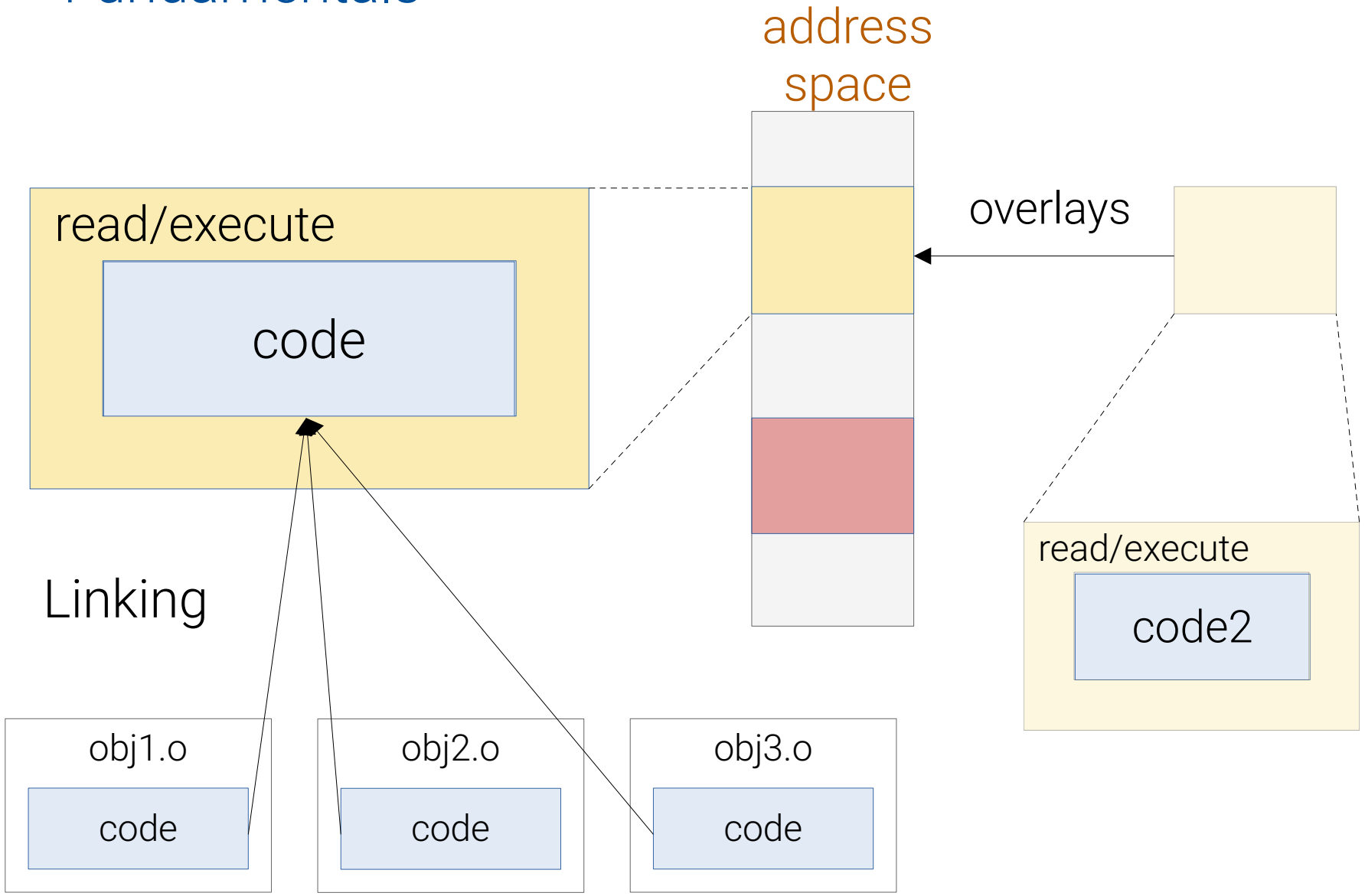
Fundamentals



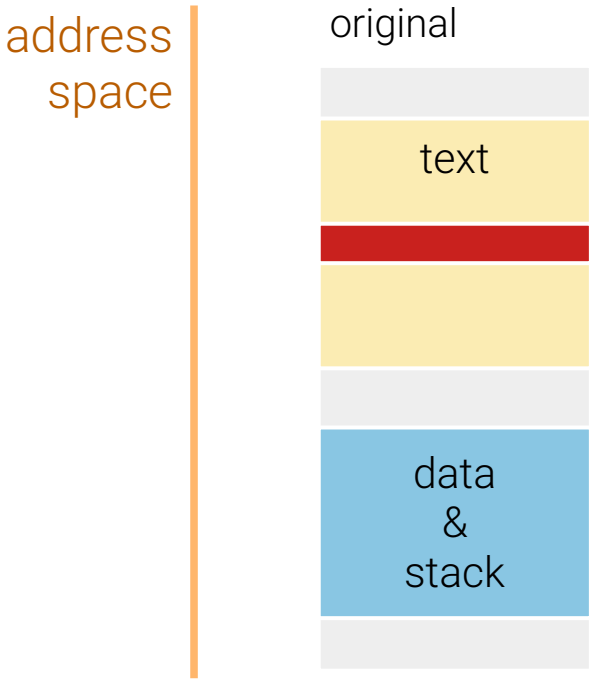
Fundamentals



Fundamentals

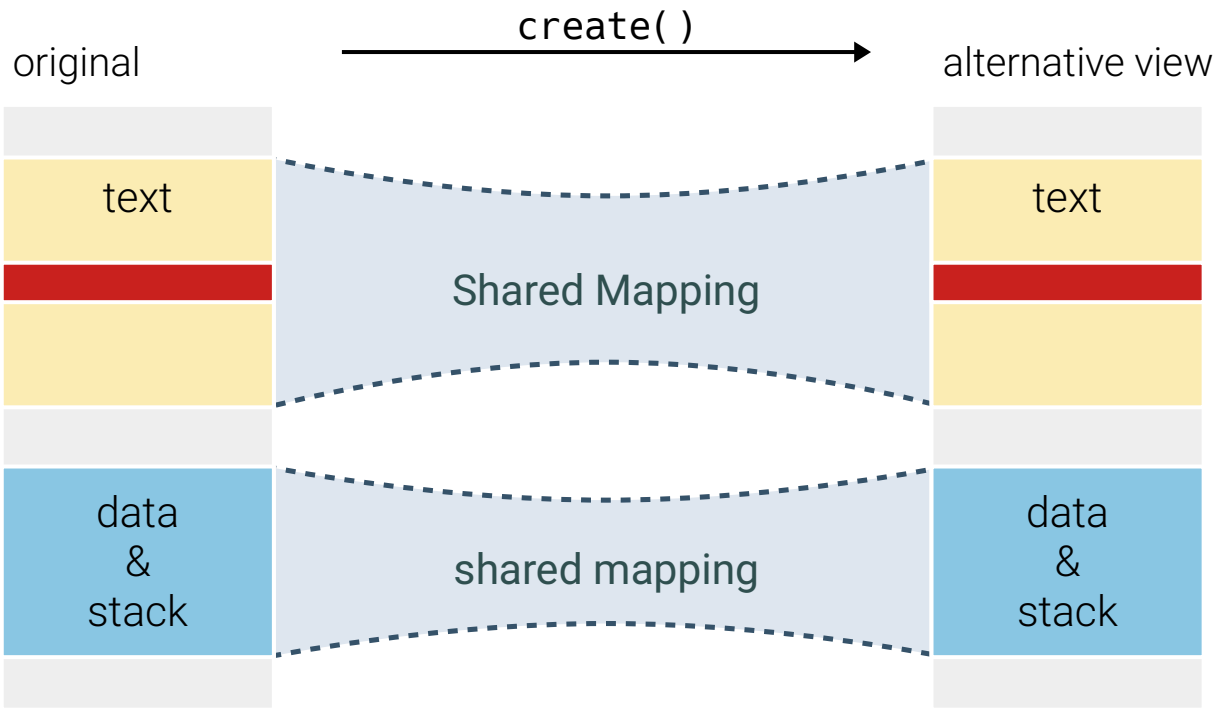


Fundamentals – Address-Space Views

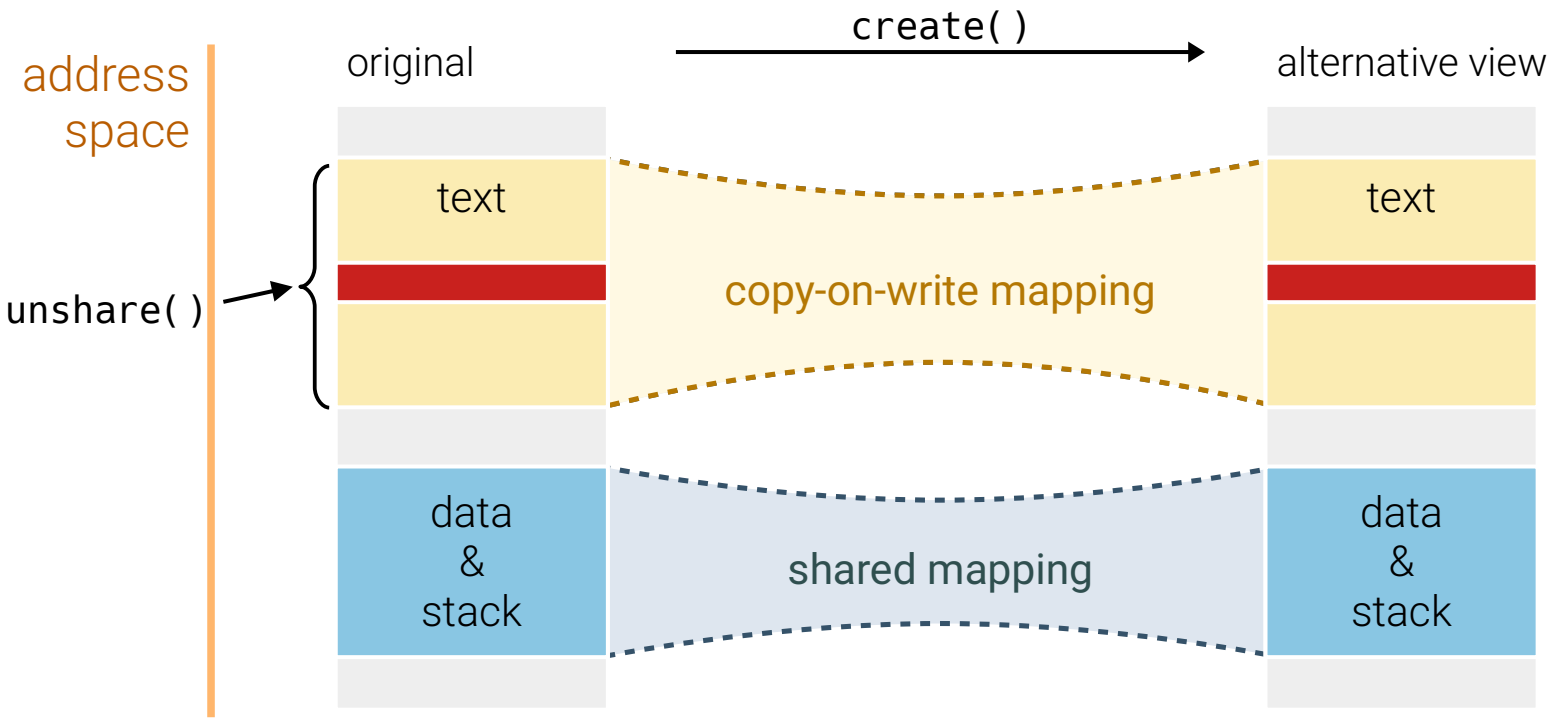


Fundamentals – Address-Space Views

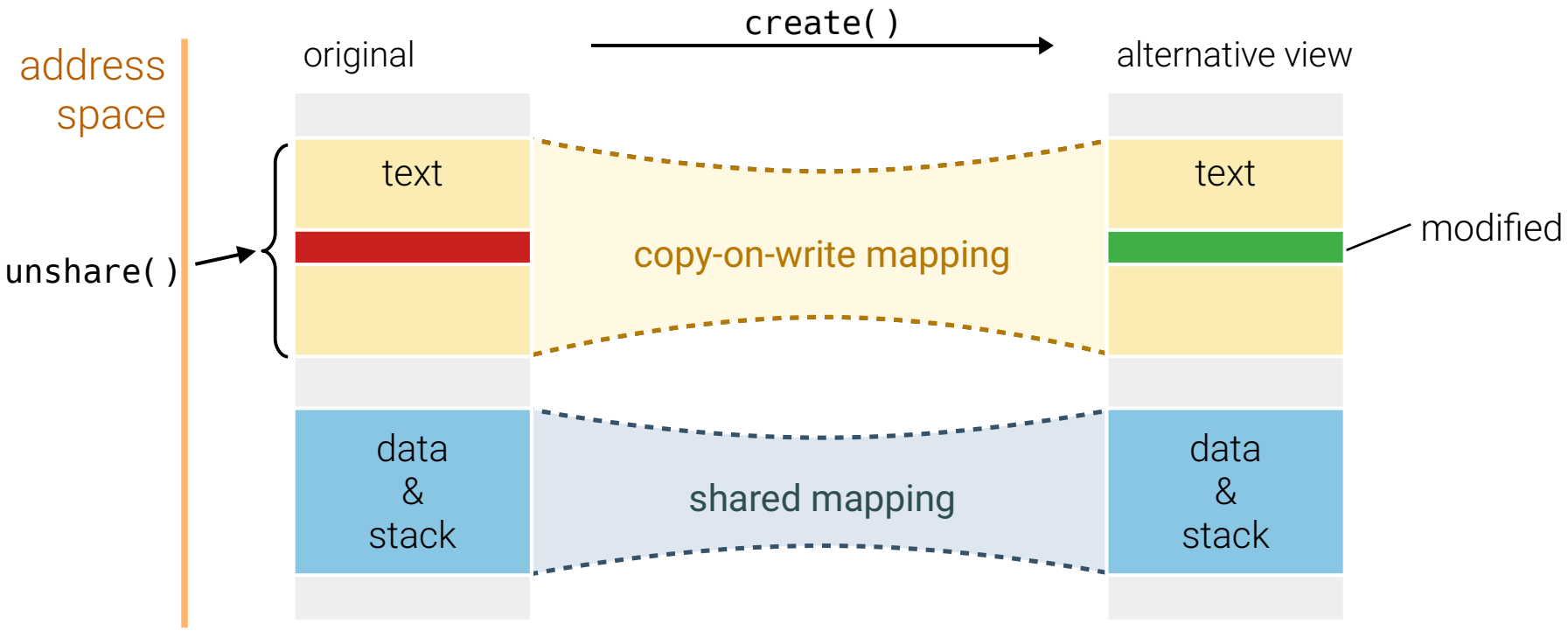
address space



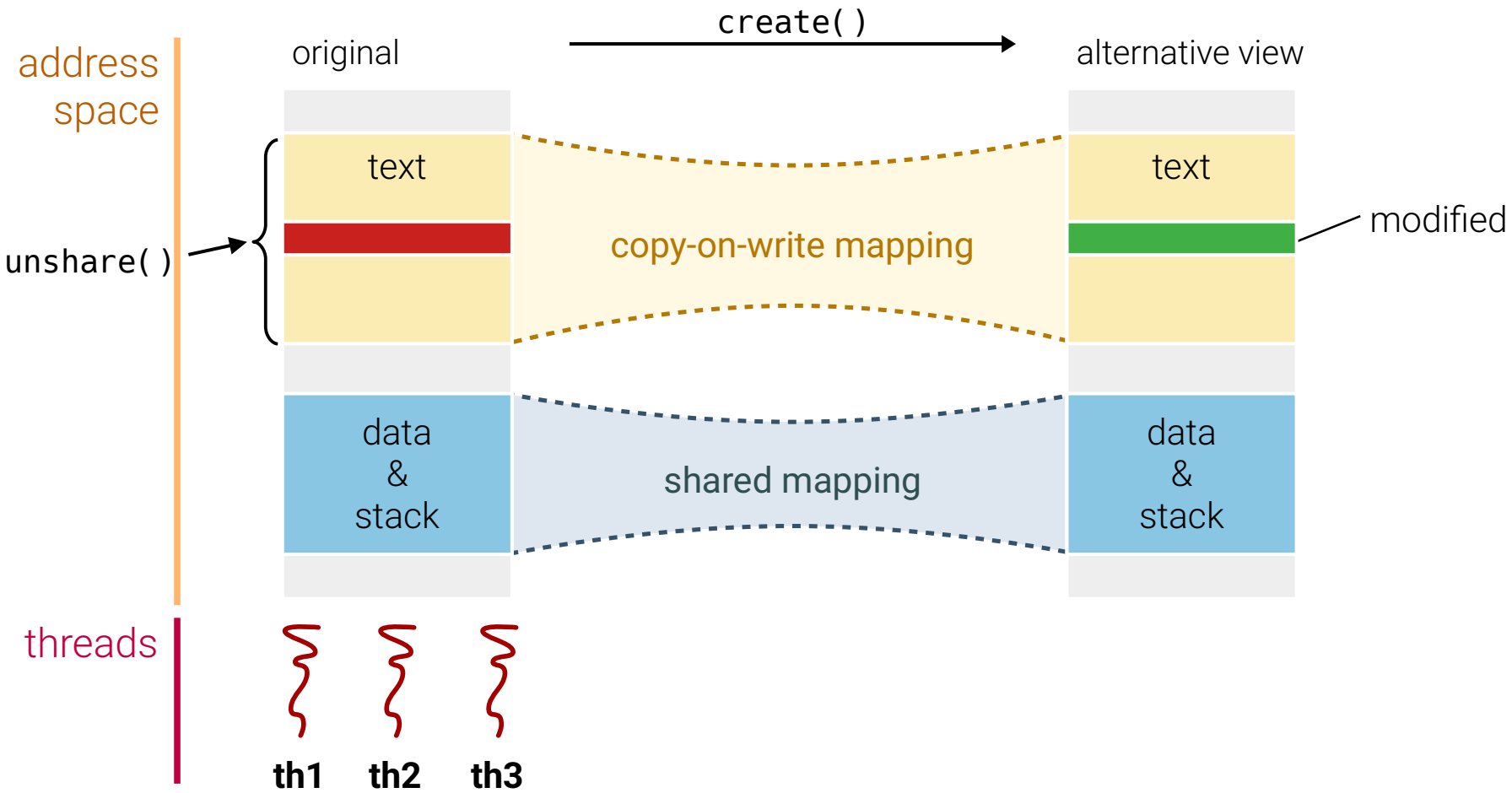
Fundamentals – Address-Space Views



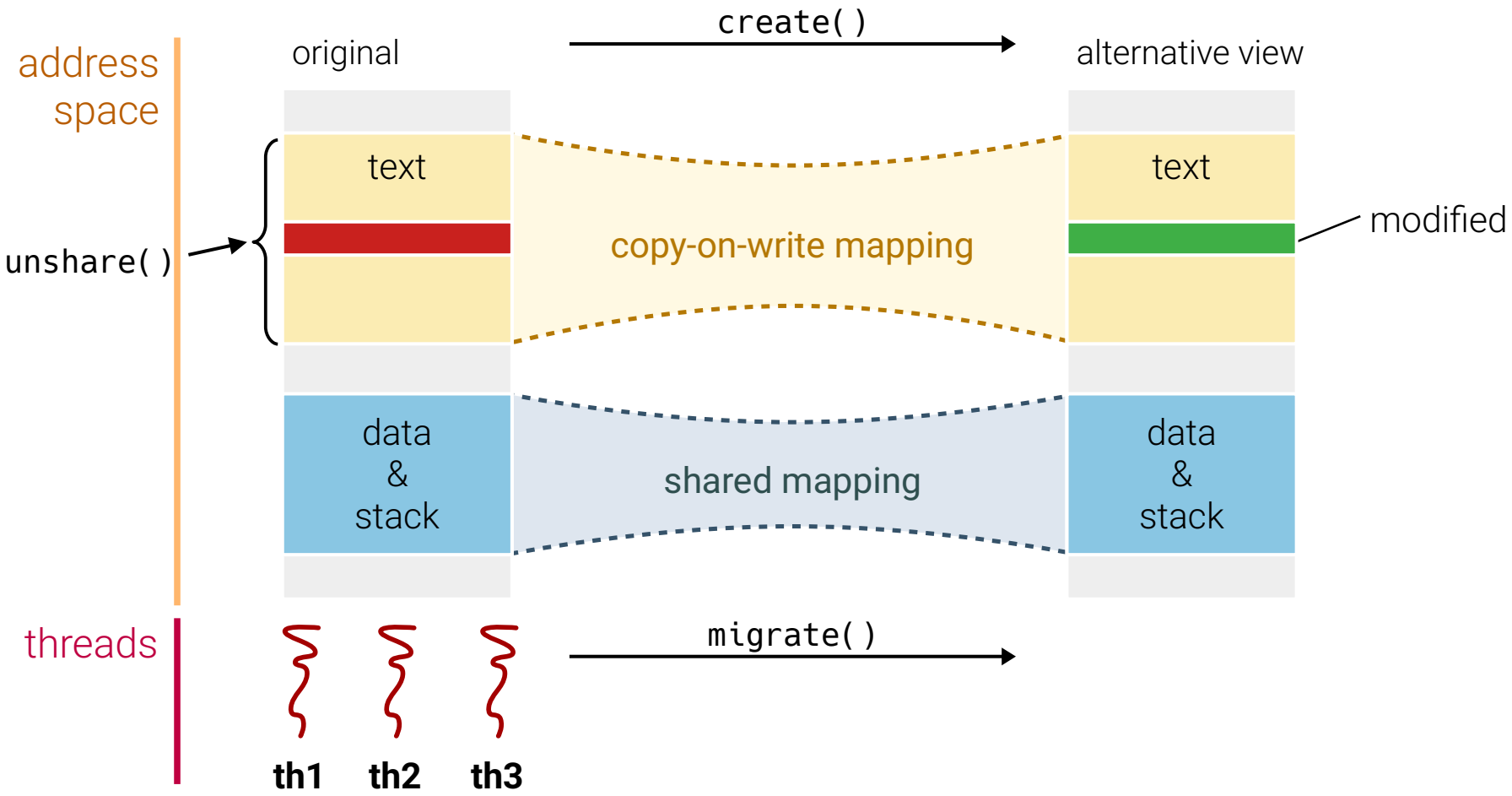
Fundamentals – Address-Space Views



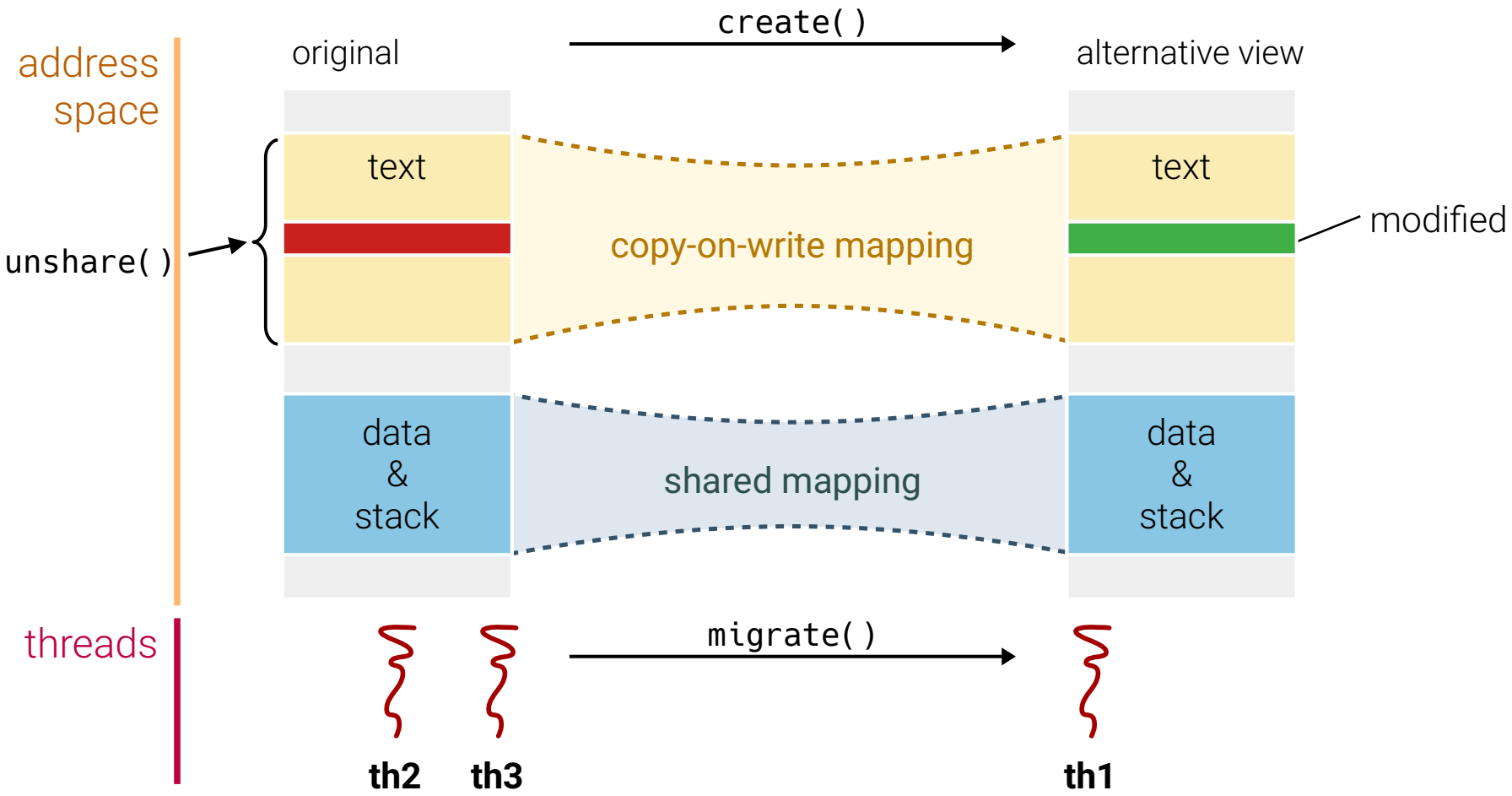
Fundamentals – Address-Space Views



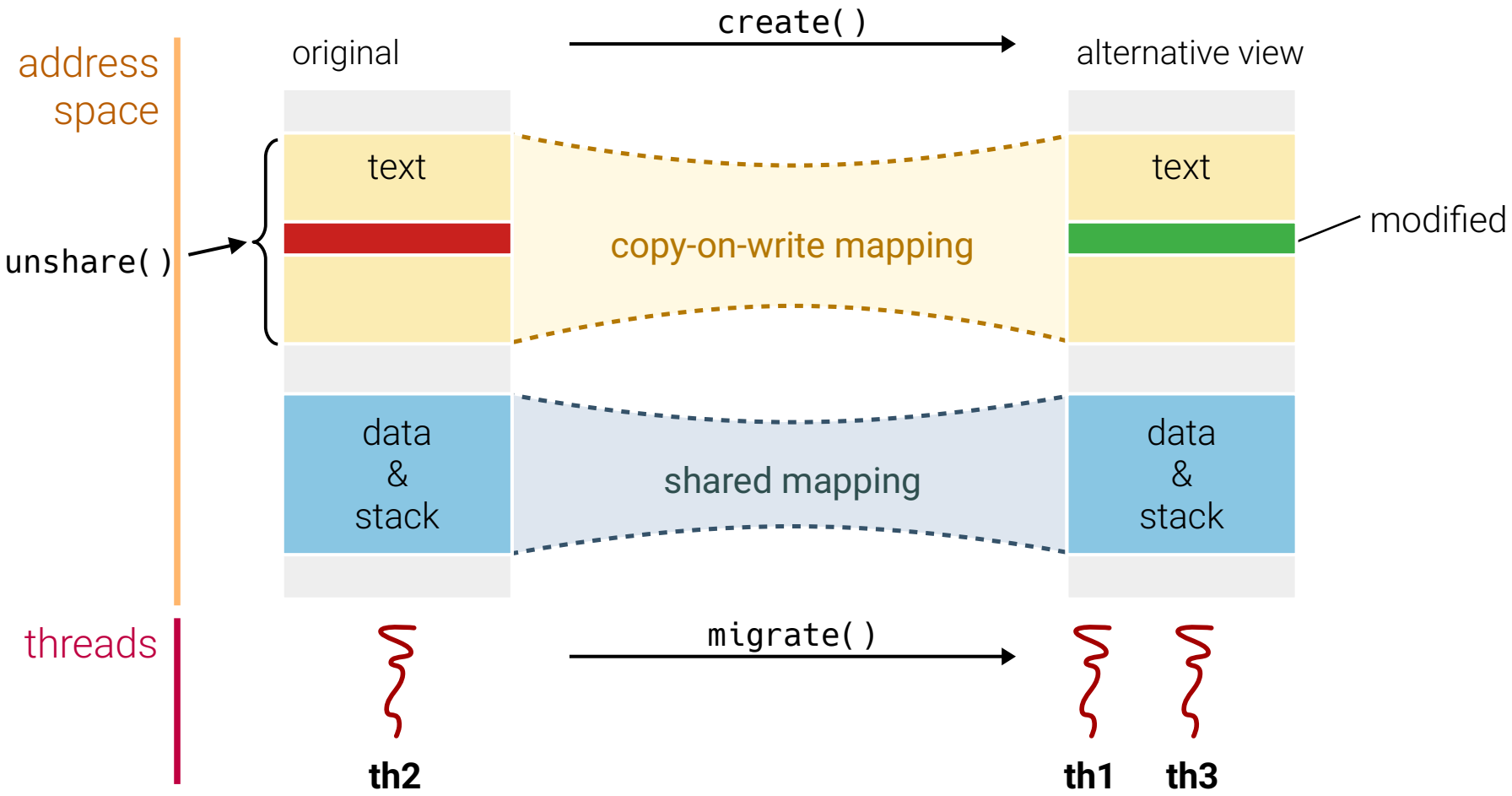
Fundamentals – Address-Space Views



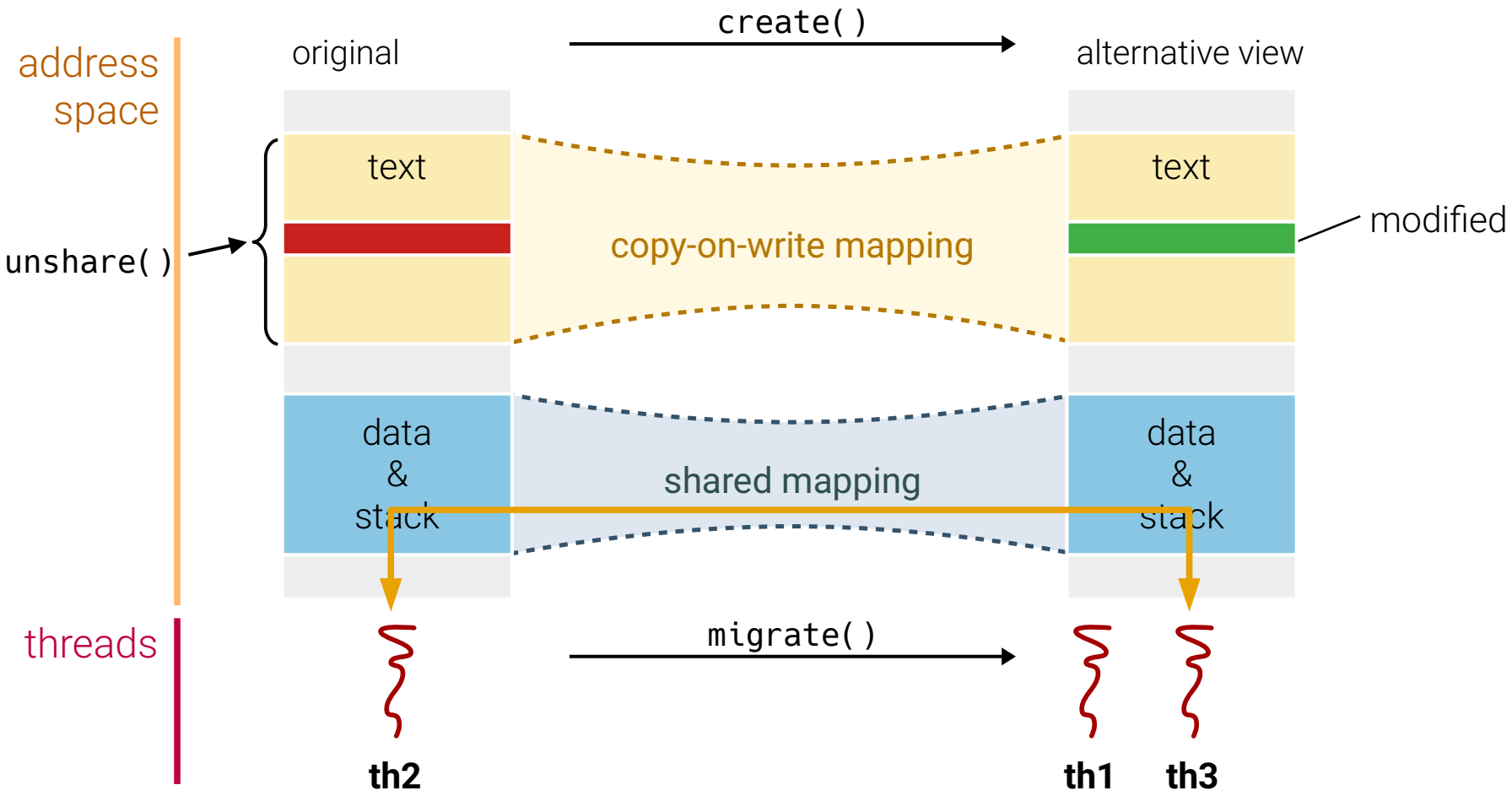
Fundamentals – Address-Space Views



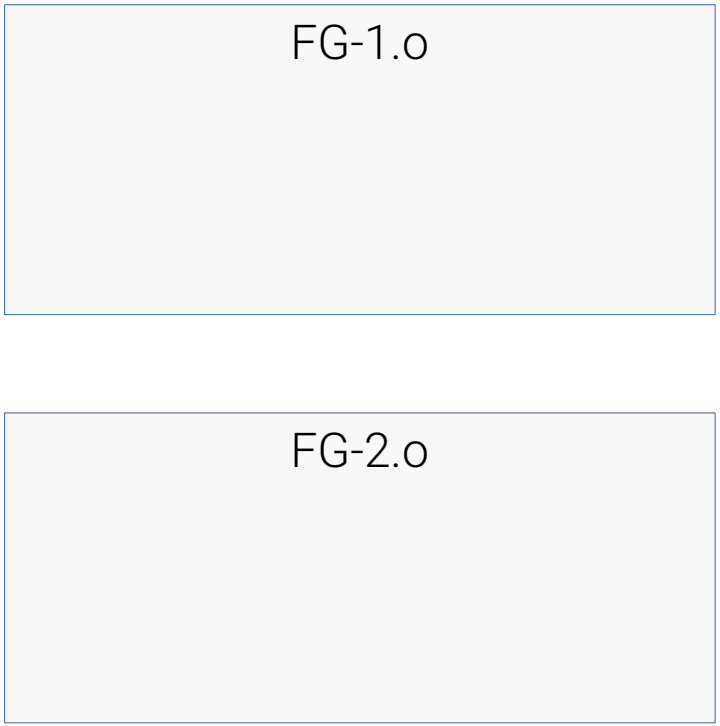
Fundamentals – Address-Space Views



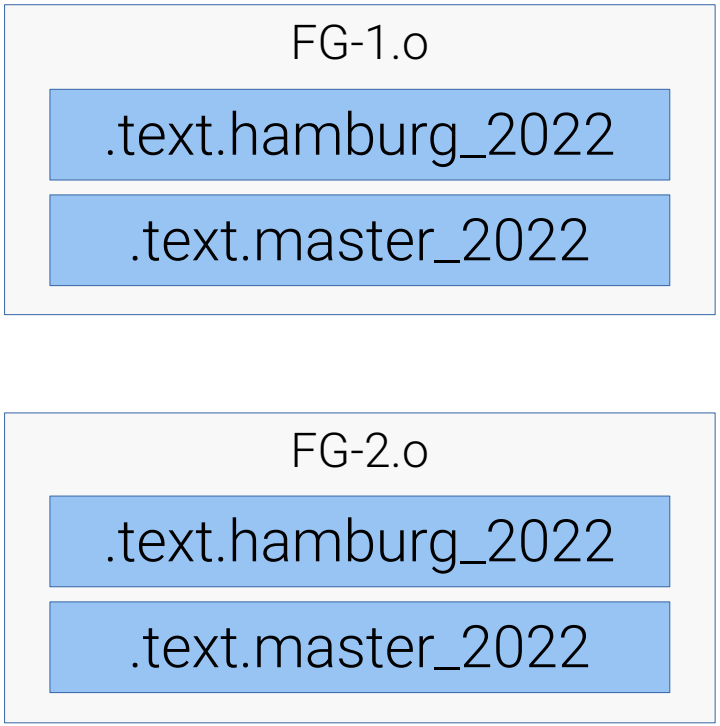
Fundamentals – Address-Space Views



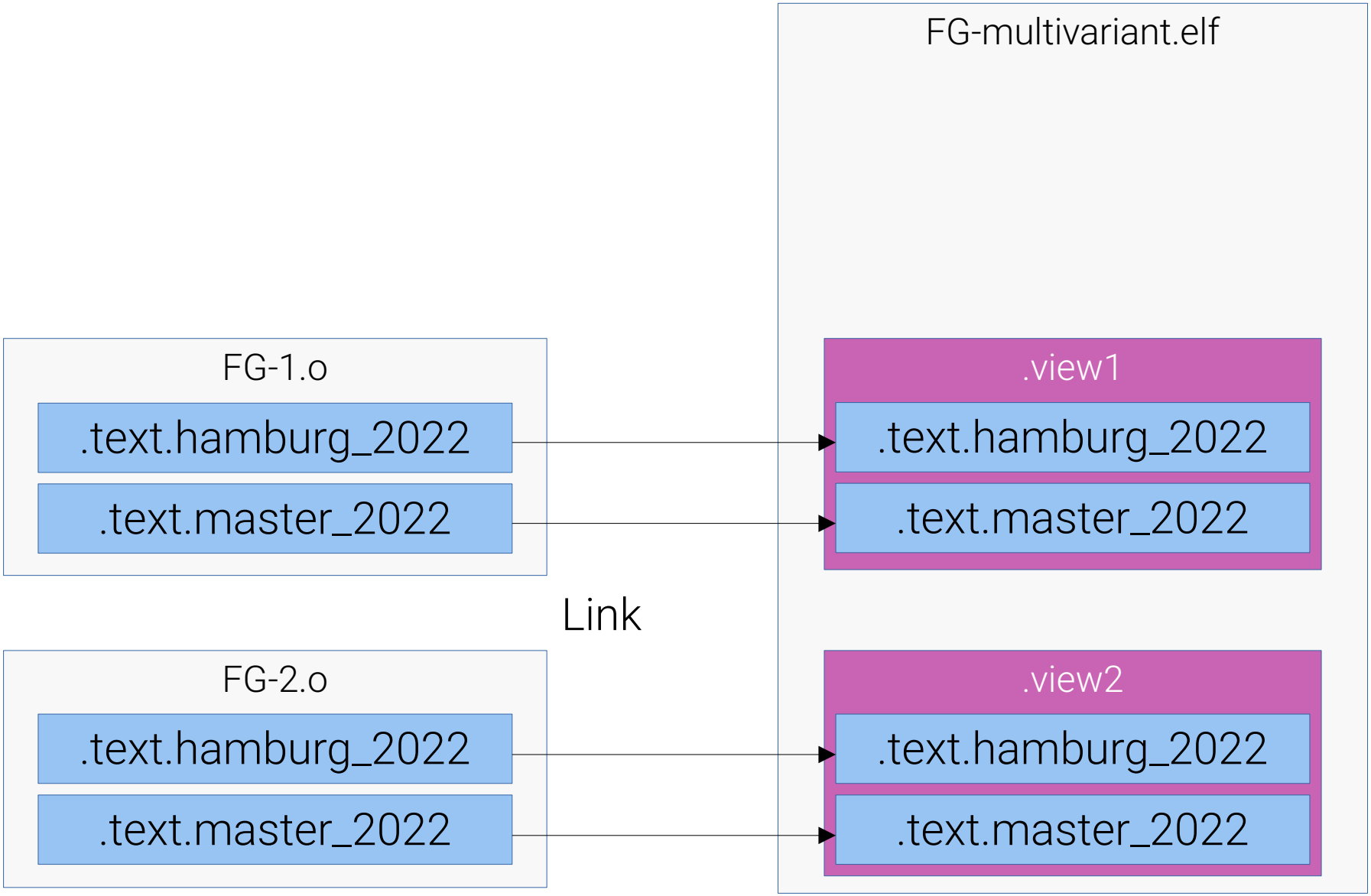
Implementation – LLVM lld



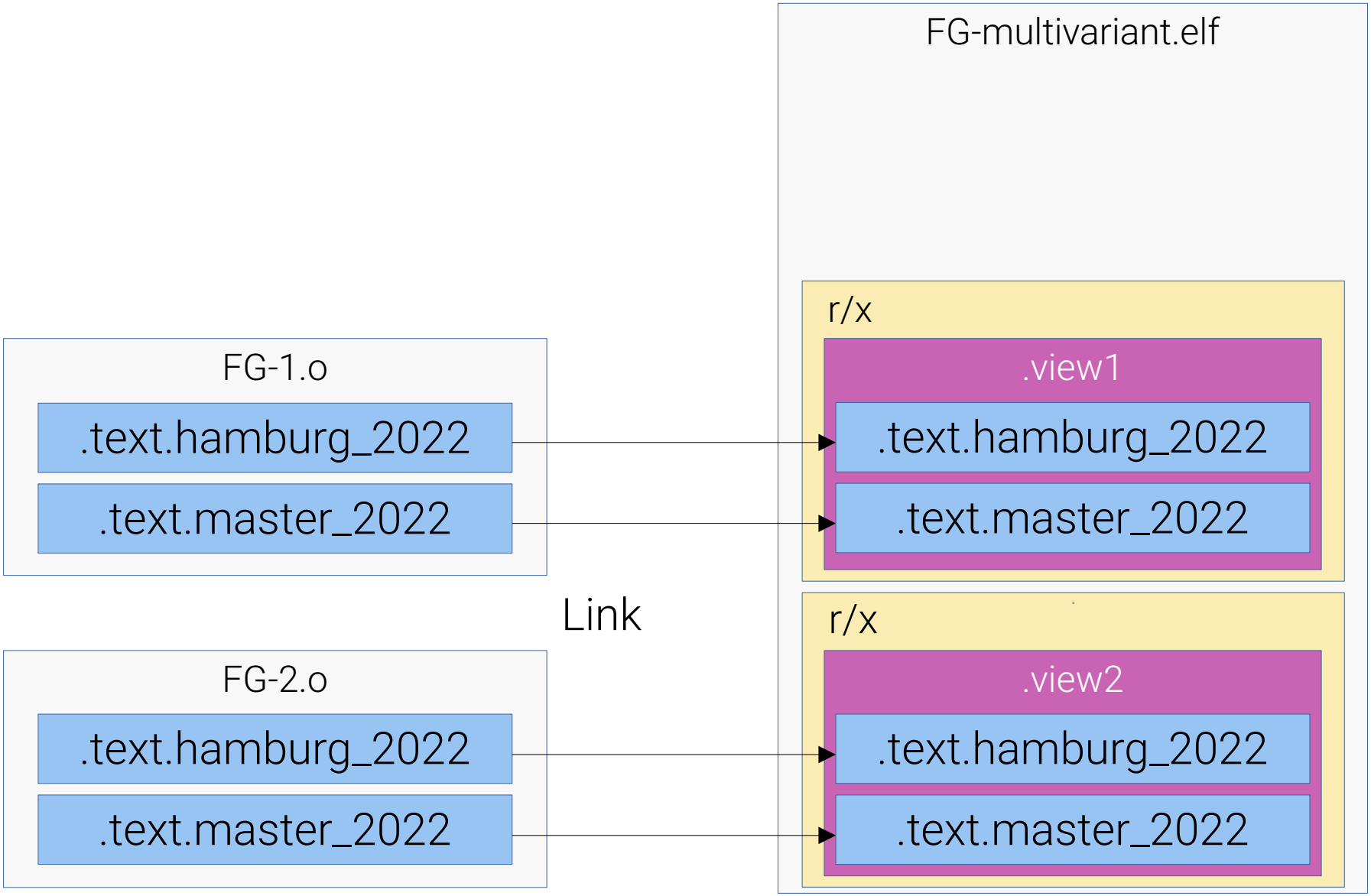
Implementation – LLVM lld



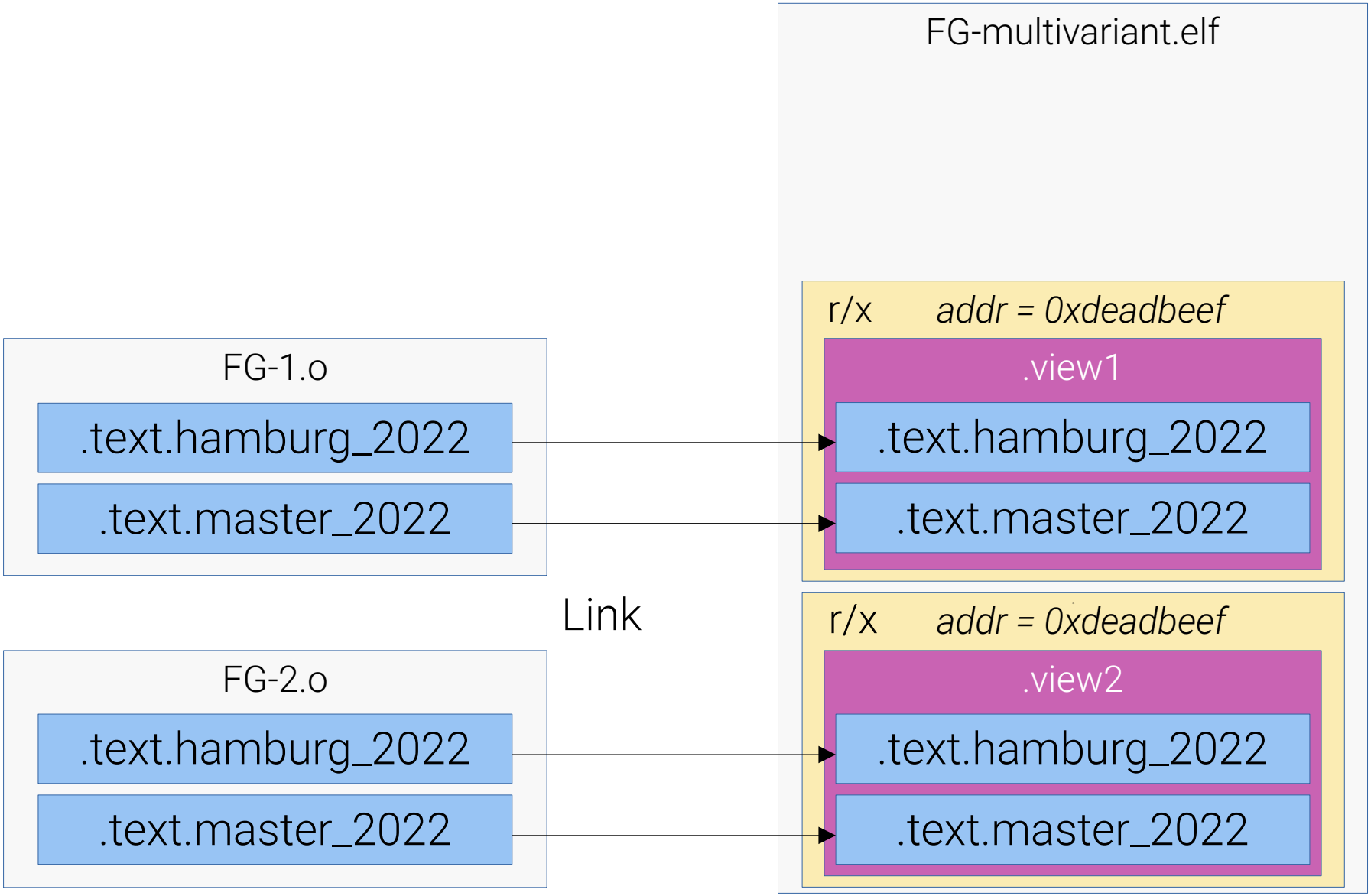
Implementation – LLVM lld



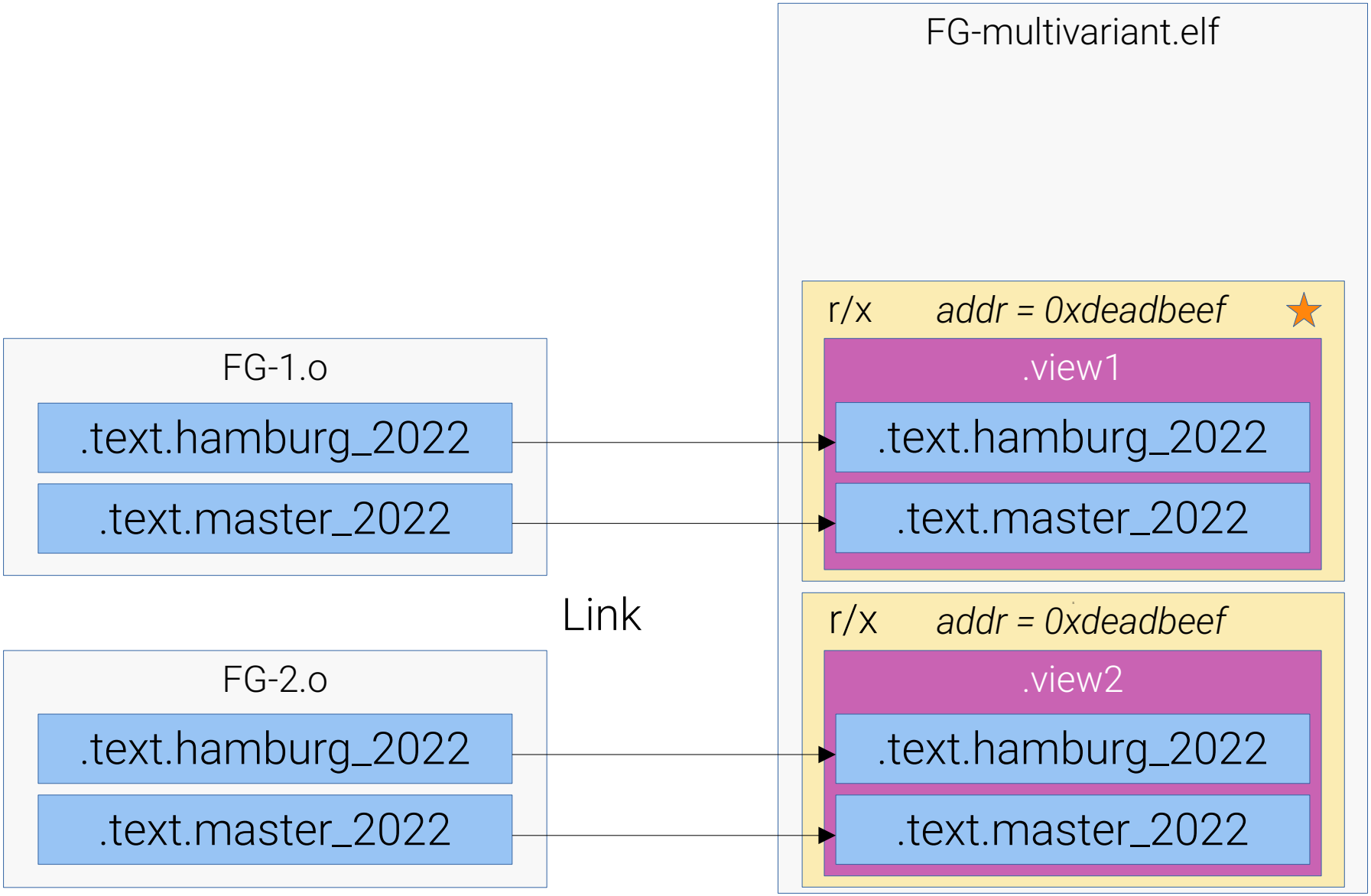
Implementation – LLVM lld



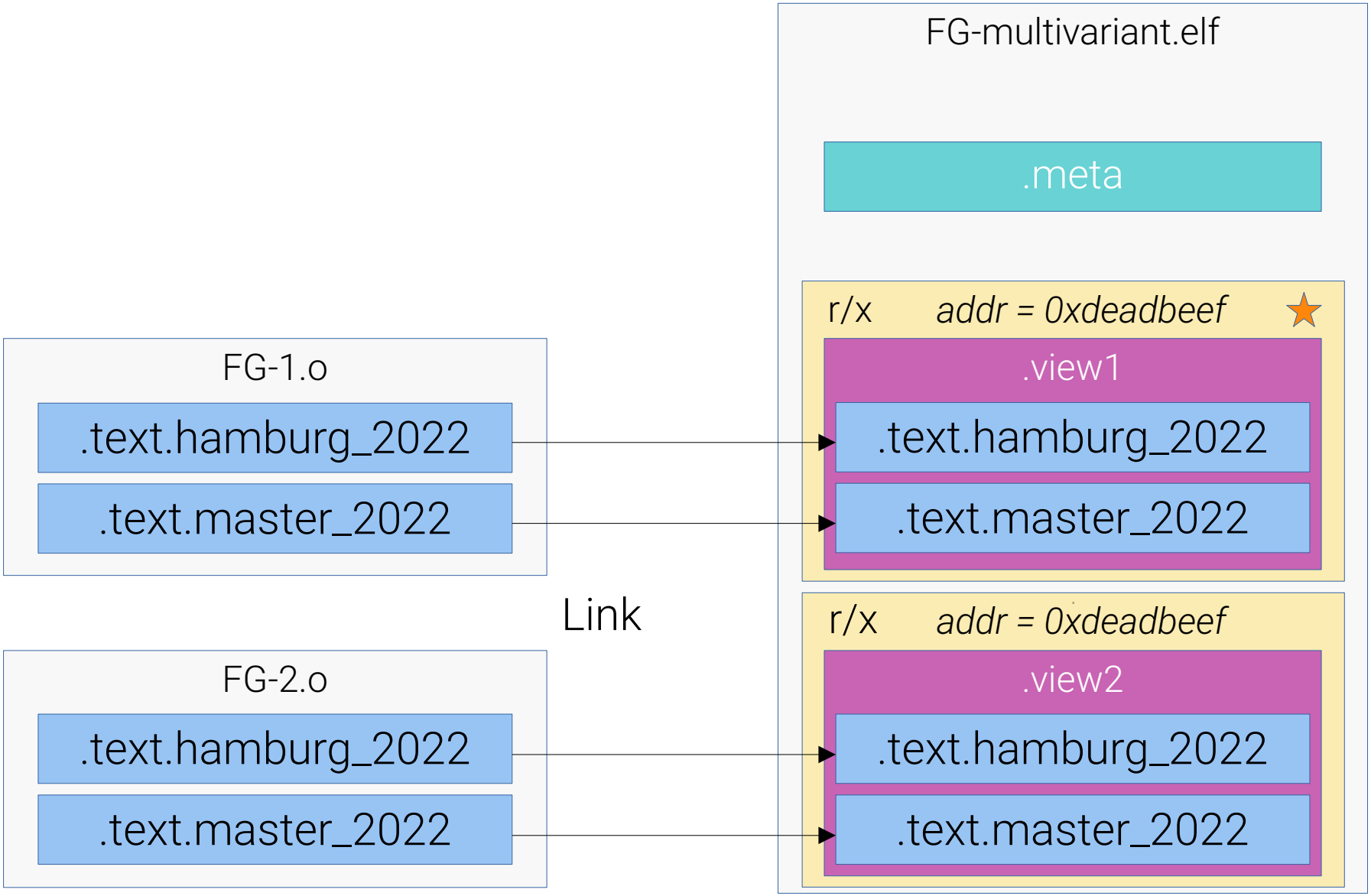
Implementation – LLVM lld



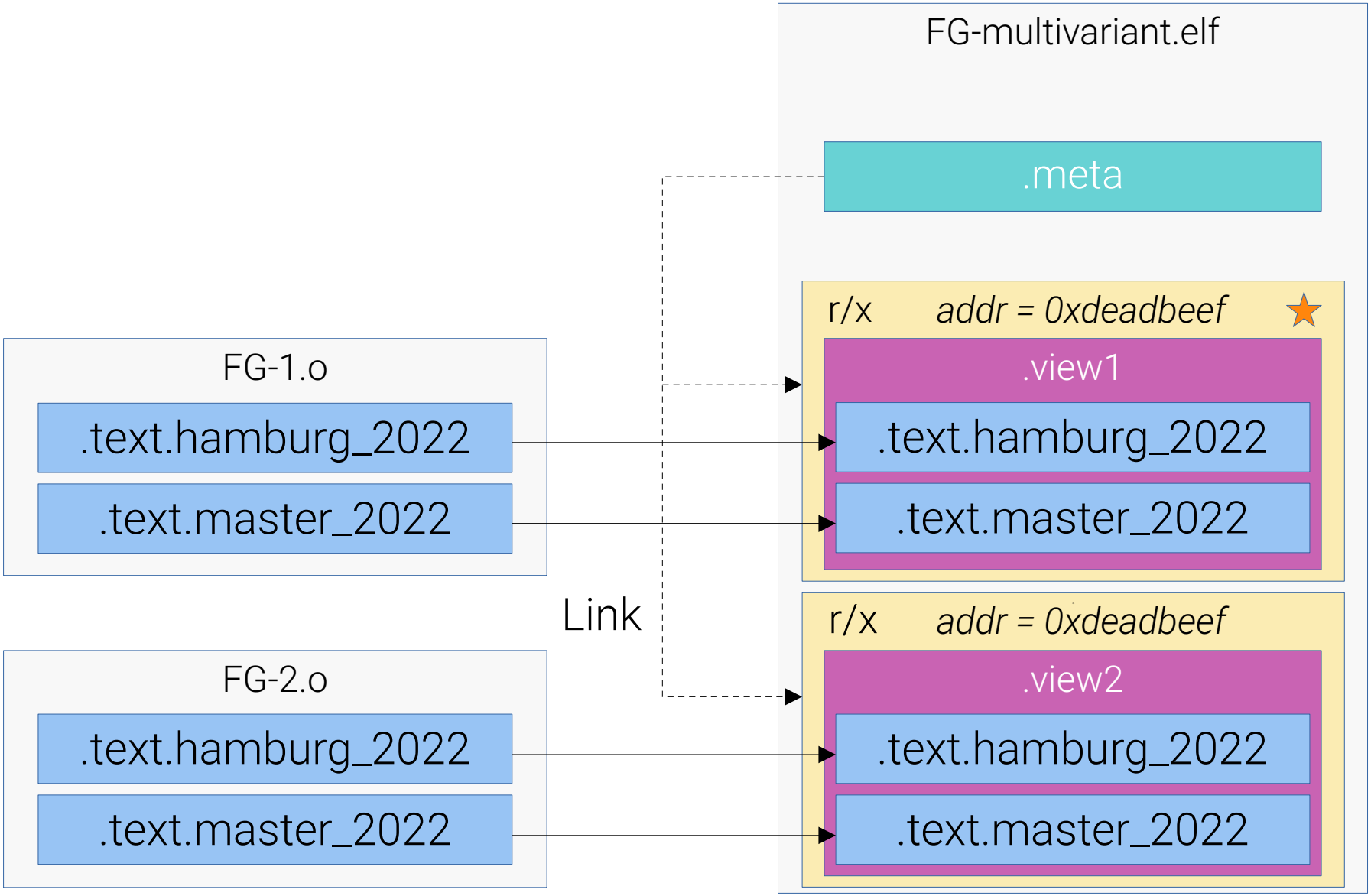
Implementation – LLVM lld



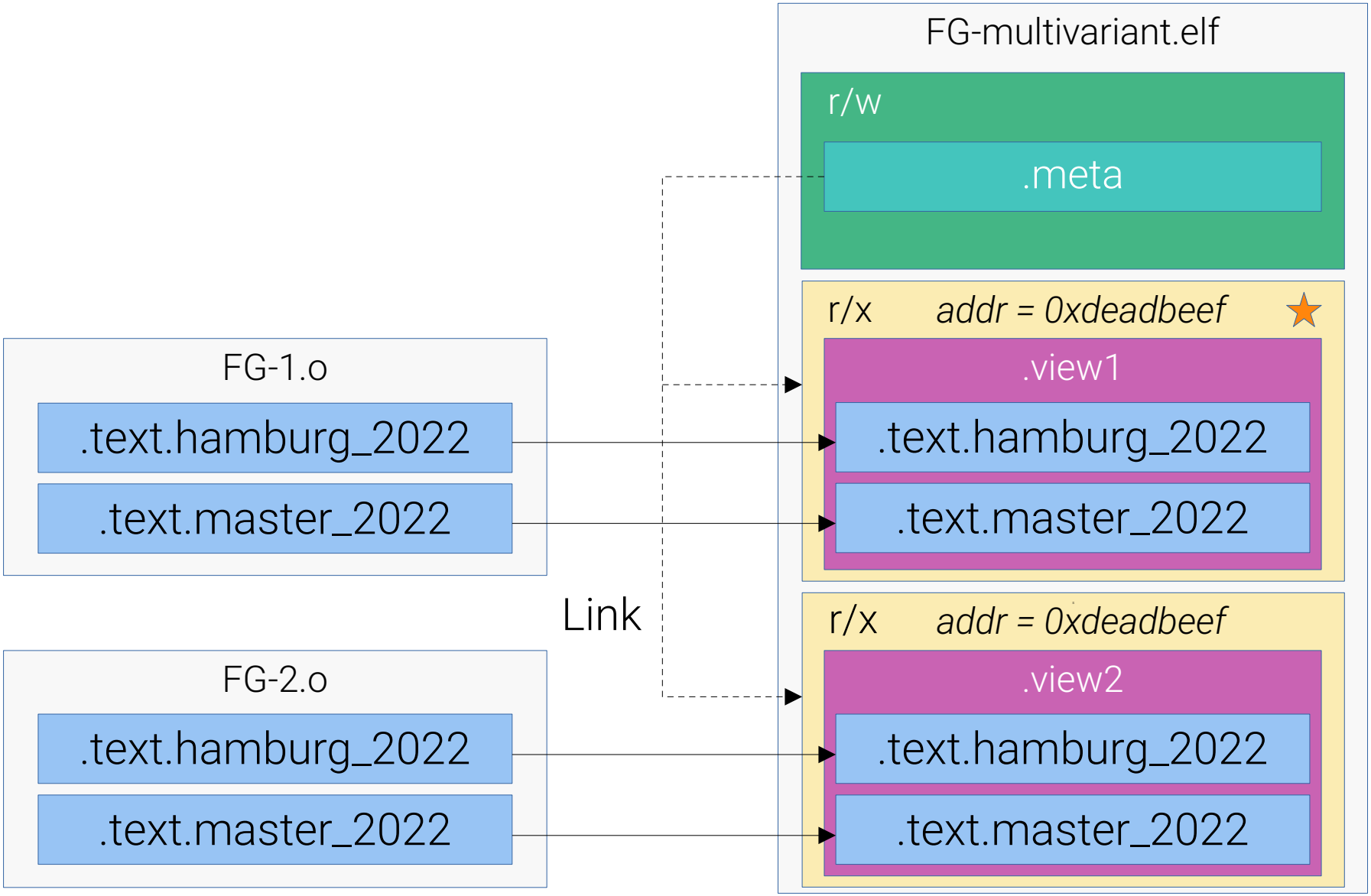
Implementation – LLVM lld



Implementation – LLVM lld

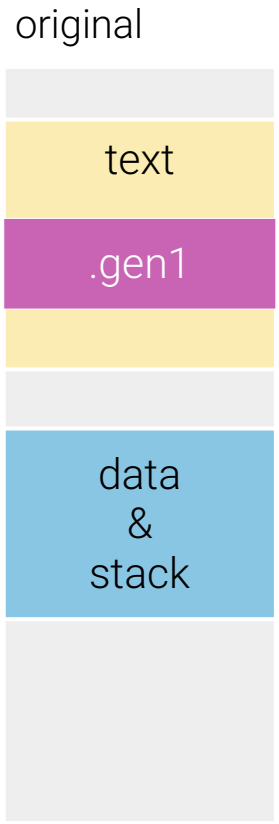


Implementation – LLVM lld

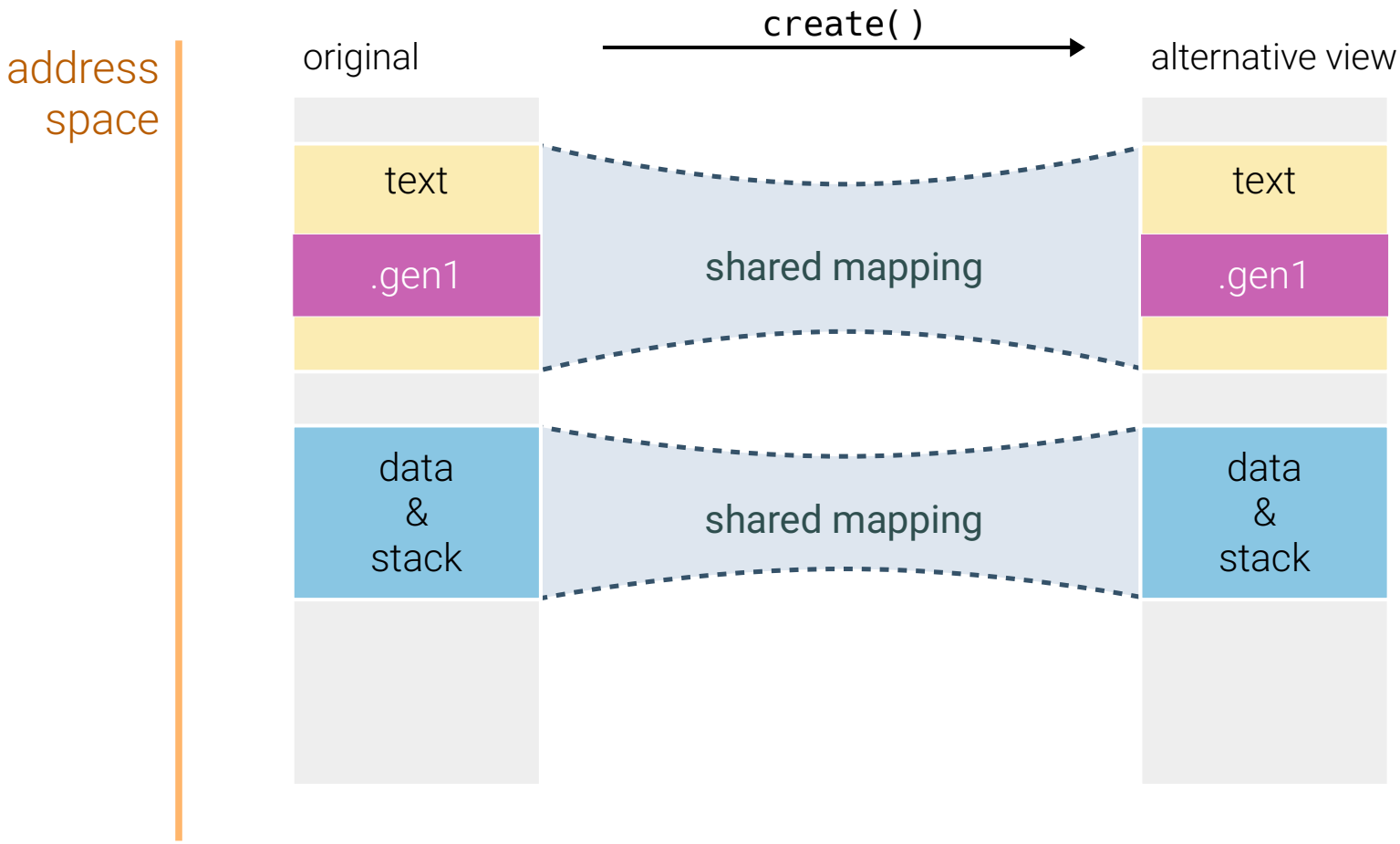


Implementation – Runtime

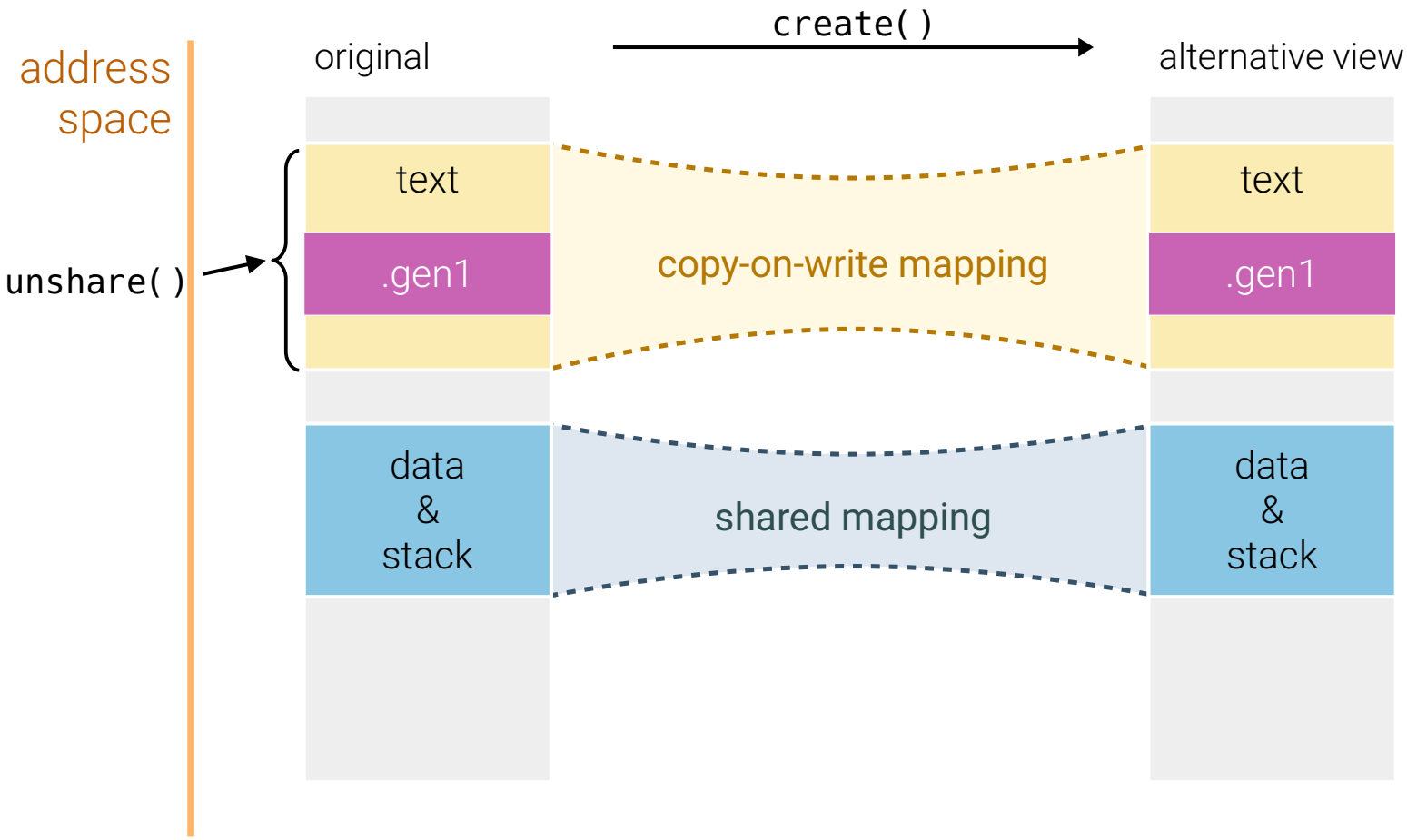
address space



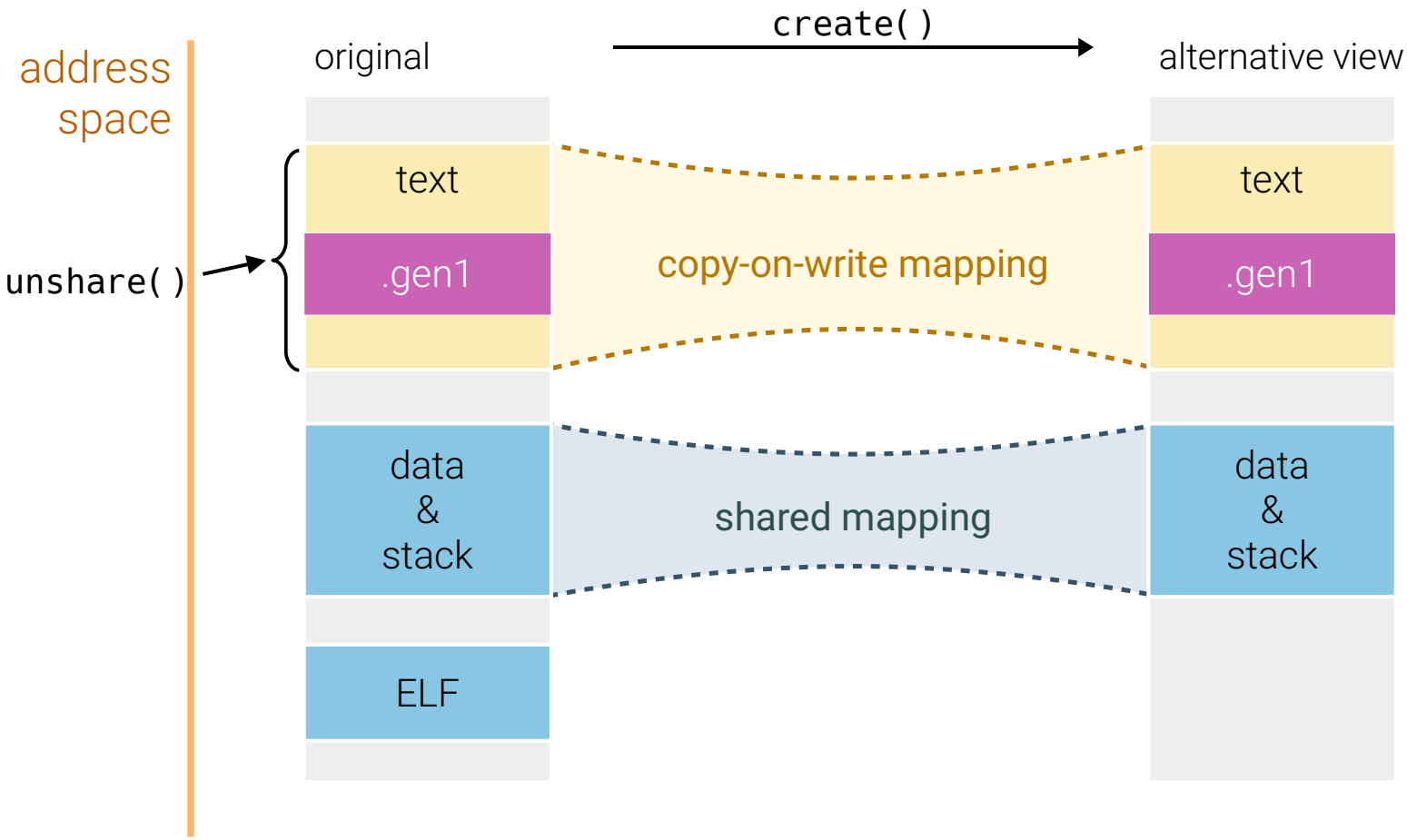
Implementation – Runtime



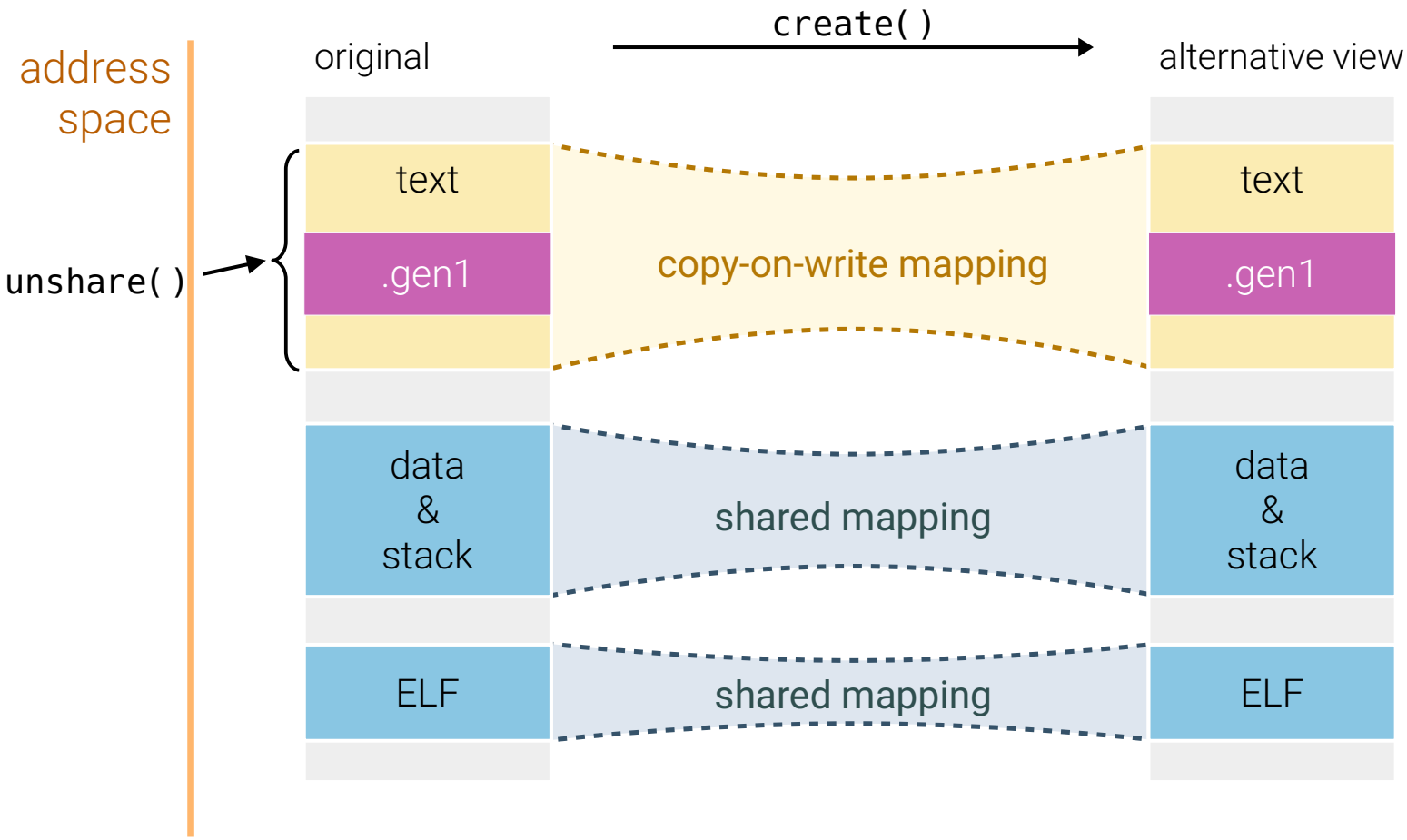
Implementation – Runtime



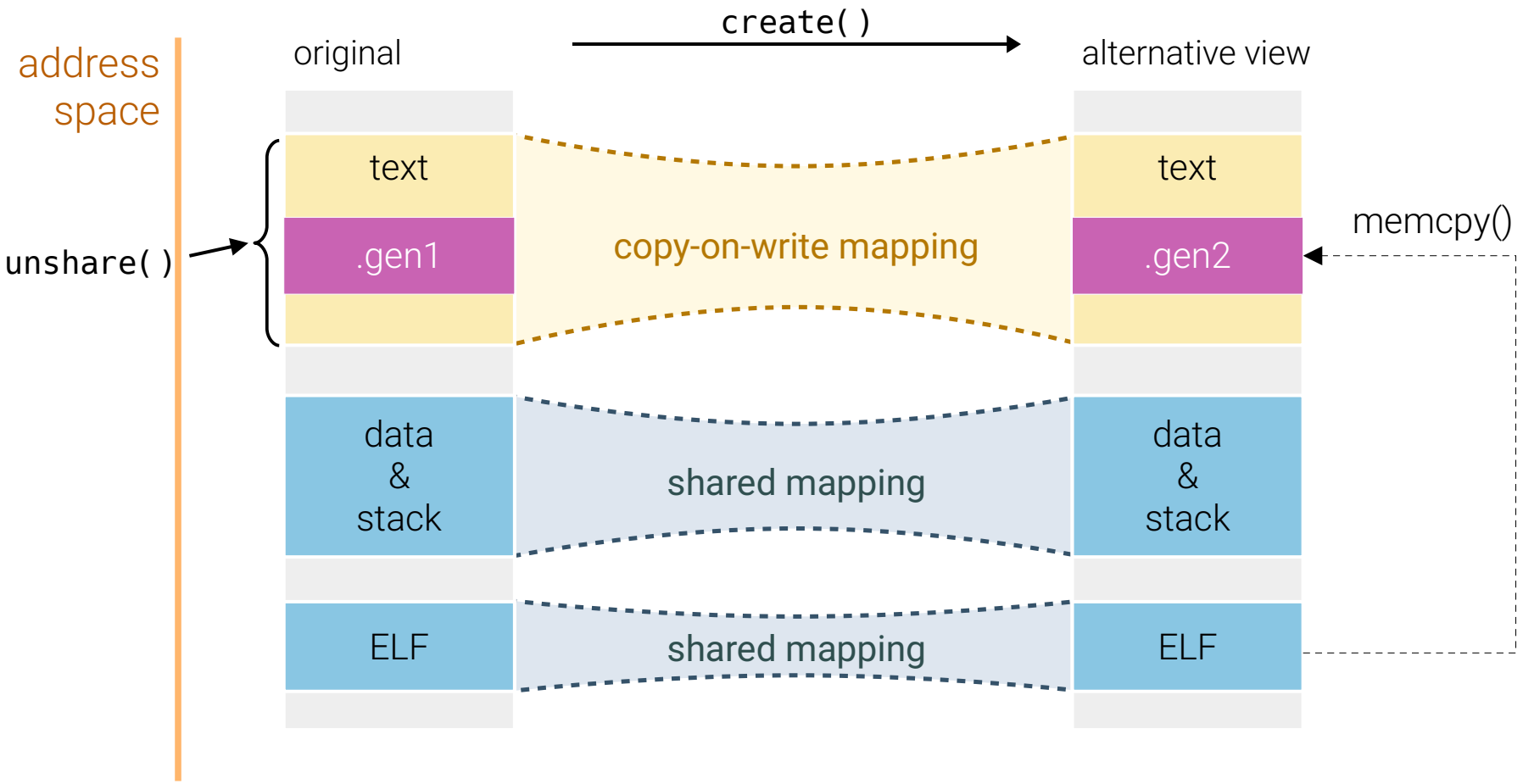
Implementation – Runtime



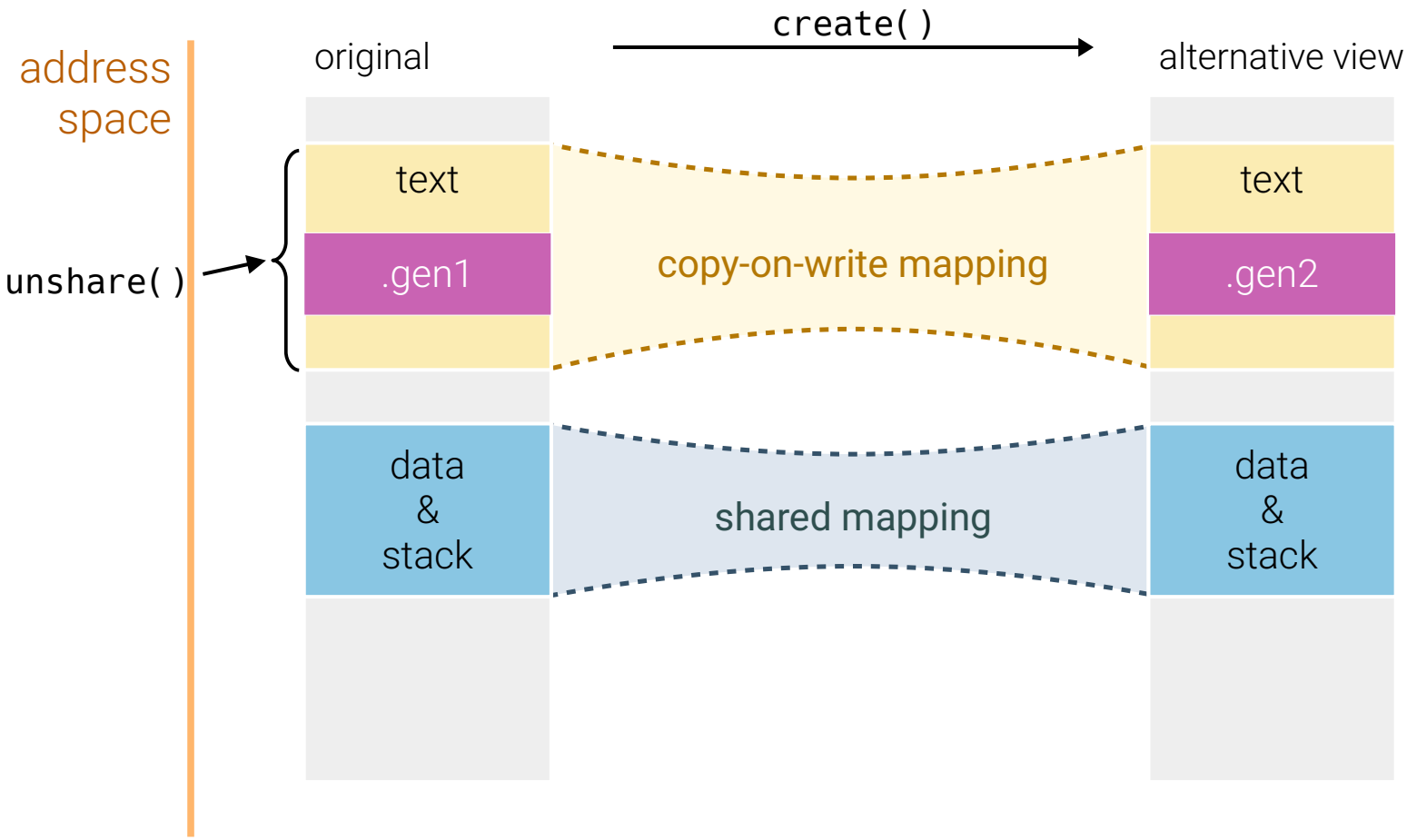
Implementation – Runtime



Implementation – Runtime



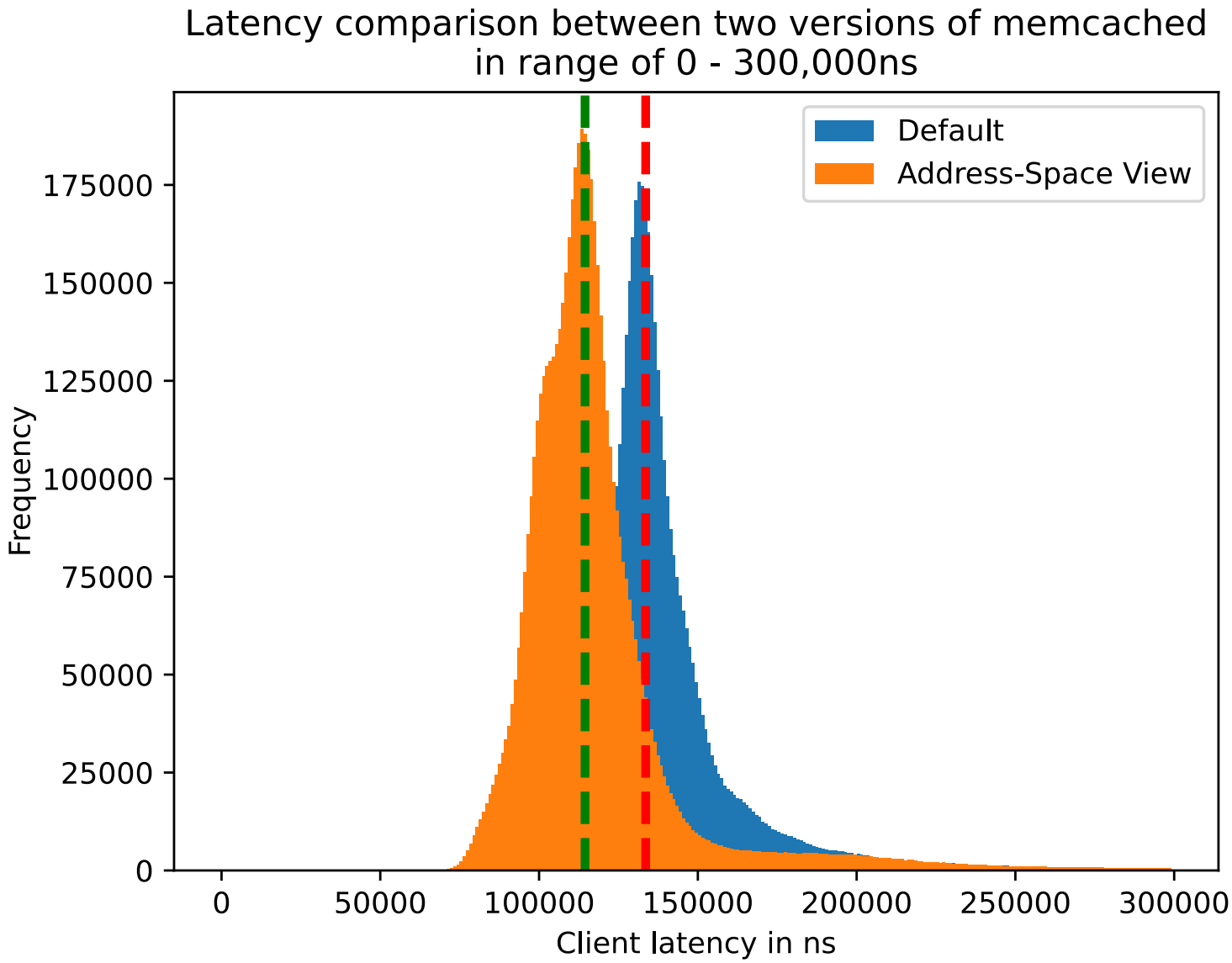
Implementation – Runtime



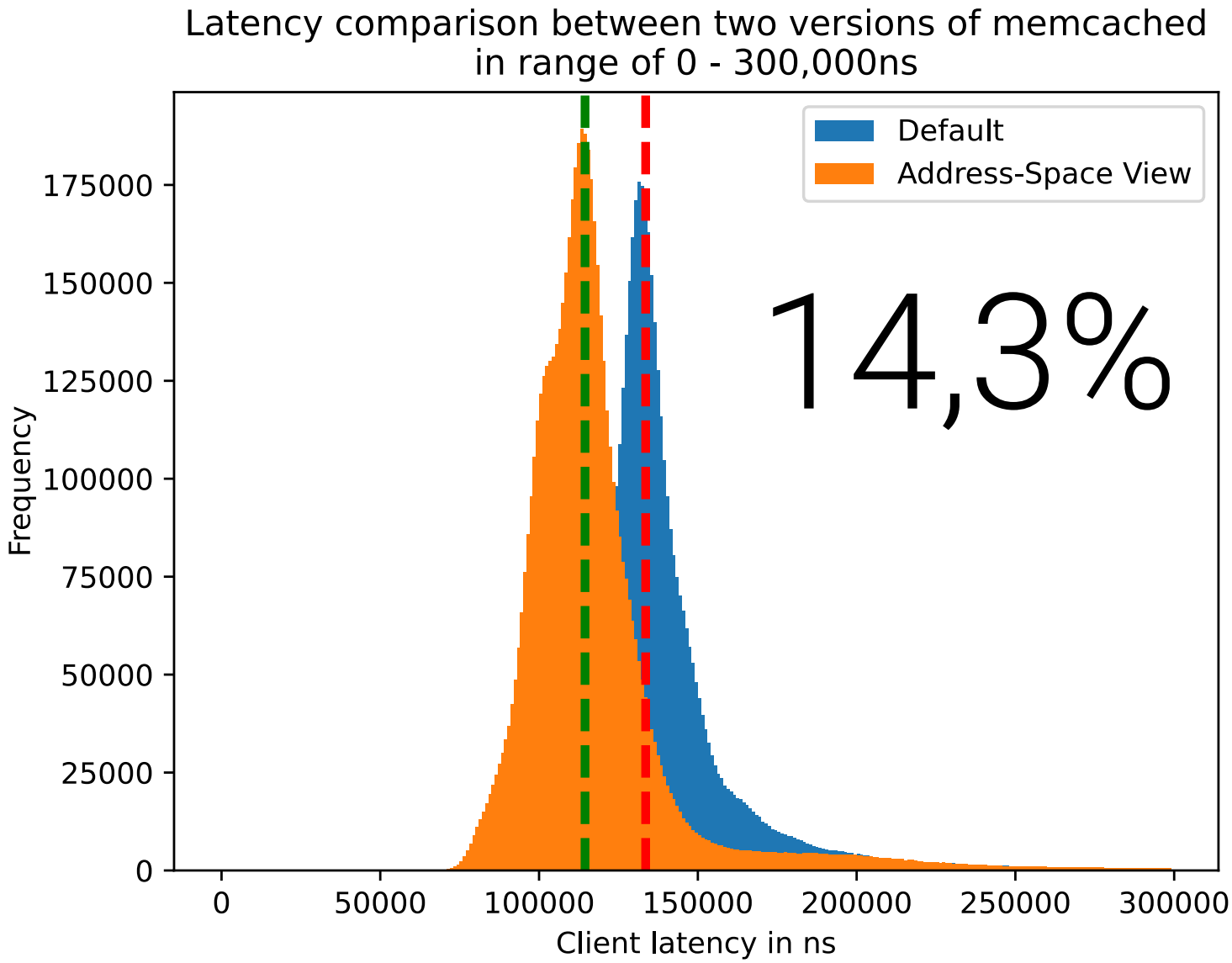
Evaluation

- Synthetic test cases
- Evaluation target *memcached*
  - Distributed memory caching system
  - Macro-benchmark address sanitizer impact
    - Default version with ASan globally enabled
    - Multivariant version with ASan partially enabled
  - 32 client threads measuring *memcached_get* latency

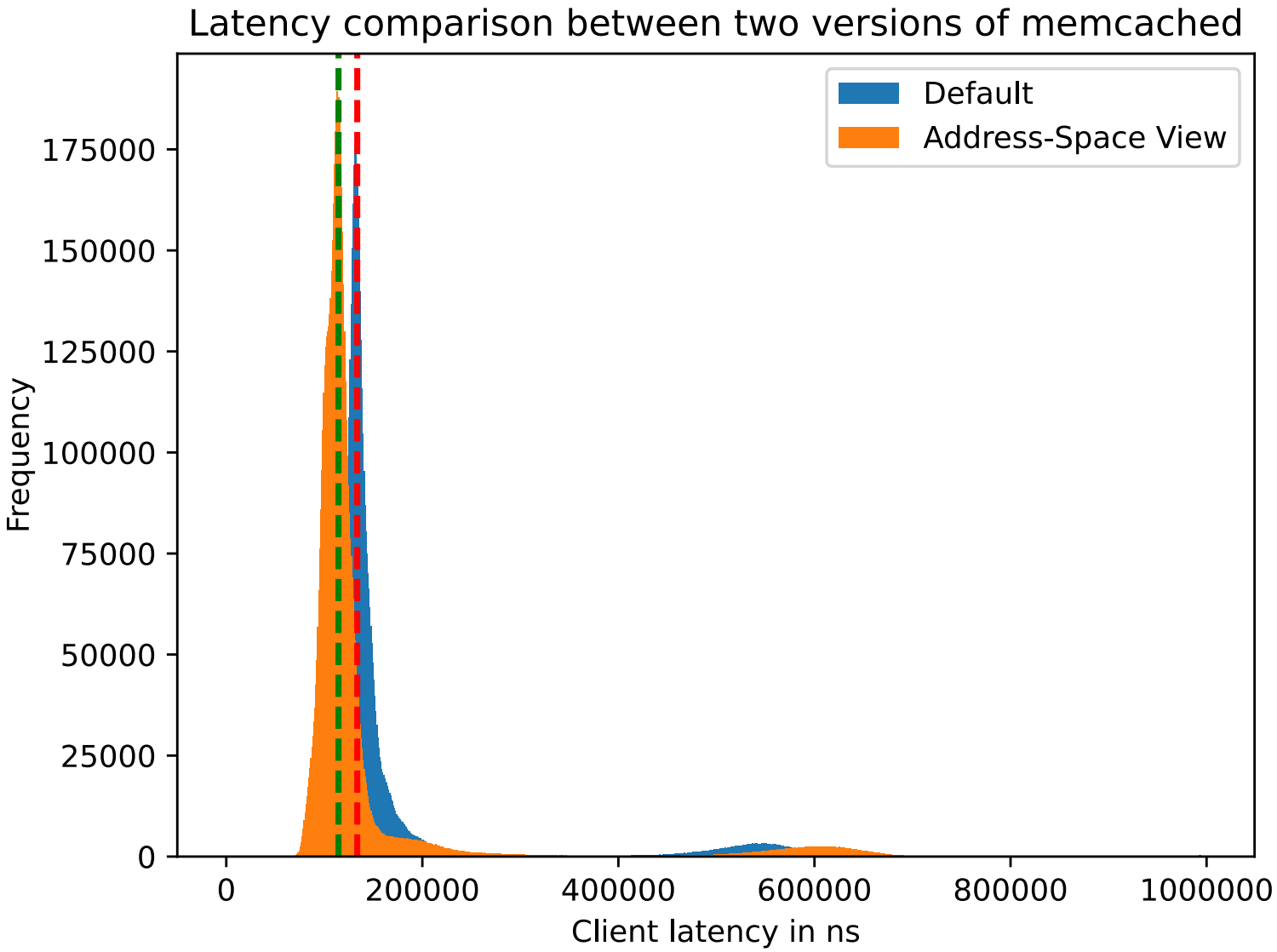
Evaluation


Latency comparison between two versions of memcached
in range of 0 - 300,000ns
Default
Address-Space View
Frequency
175000
150000
125000
100000
75000
50000
25000
0
0
50000
100000
150000
200000
250000
300000
Client latency in ns

Evaluation


Latency comparison between two versions of memcached
in range of 0 - 300,000ns
Default
Address-Space View
14,3%
Frequency
175000
150000
125000
100000
75000
50000
25000
0
0
50000
100000
150000
200000
250000
300000
Client latency in ns

Evaluation


Latency comparison between two versions of memcached
Default
Address-Space View
Frequency
175000
150000
125000
100000
75000
50000
25000
0
0
200000
400000
600000
800000
1000000
Client latency in ns

Conclusion

- Extension of the LLVM lld linker to build multivariant ELFs
  - Sections/Segments for all views
  - Meta data to find views during runtime
- Runtime to switch between views on demand
- Performance benefit for tailored ASan view
  - 14,3% median client latency reduction
- What's next?
  - View-local data
  - Reduce view granularity from *object-file* to *function*