Systemization of DNS Self-Amplification

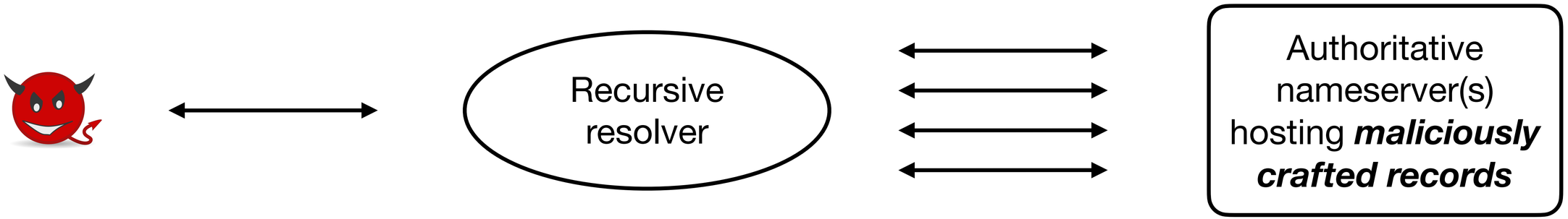
Huayi Duan
Senior Researcher, ETH Zürich

Joint work with:
Marco Bearzi, Jodok Vieli, Cagin Tanir, Liwen Xu,
David Basin, Adrian Perrig, Si Liu, and Bernhard Tellenbach

ETH zürich armasuisse ZISC Zurich Information Security & Privacy Center Swiss National Science Foundation HASLERSTIFTUNG

Emergence of DNS Self-Amplification

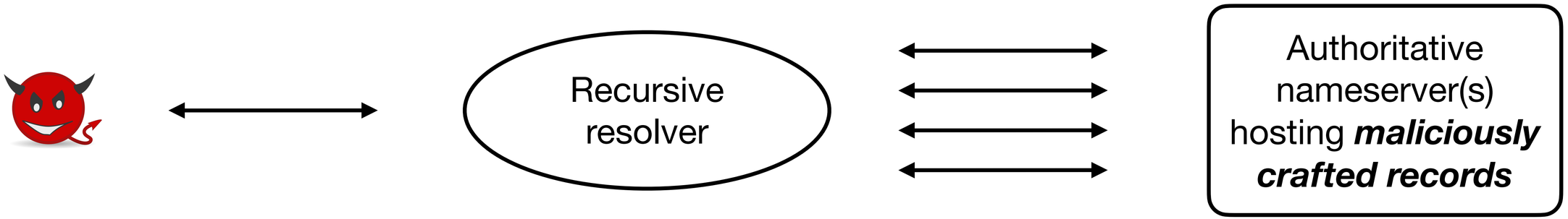
Message Amplification Factor (MAF) ≫1



Primary target: DNS servers

Emergence of DNS Self-Amplification

Message Amplification Factor (MAF) ≫1



> The recommended priorities for the resolver designer are:
>
> 1. Bound the amount of work (packets sent, parallel processes started) so that a request can't get into an infinite loop or start off a chain reaction of requests or queries with other implementations EVEN IF SOMEONE HAS INCORRECTLY CONFIGURED SOME DATA.
>
> — RFC1034

Can we enumerate all such vulnerabilities?

What is the maximum achievable MAF?

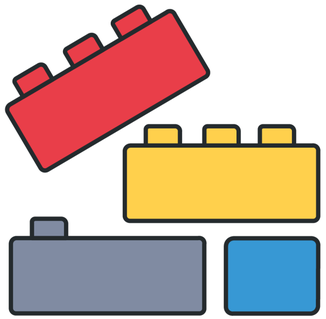
> The recommended priorities for the resolver designer are:
>
> 1. Bound the amount of work (packets sent, parallel processes started) so that a request can't get into an infinite loop or start off a chain reaction of requests or queries with other implementations EVEN IF SOMEONE HAS INCORRECTLY CONFIGURED SOME DATA.
>
> — RFC1034

Systematization of DNS Self-Amplification

Can we enumerate all such vulnerabilities?

What is the maximum achievable MAF?

Identify ***amplification primitives***



Analyze their ***composability***

↓

CAMP
(Compositional Amplification)

Taxonomy of Amplification Primitives

Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

Taxonomy of Amplification Primitives

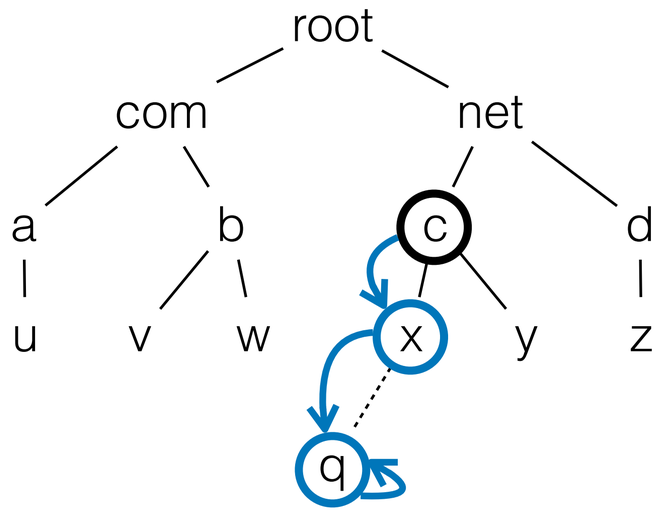
Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

Names on the same path?

All

Self-probing



Taxonomy of Amplification Primitives

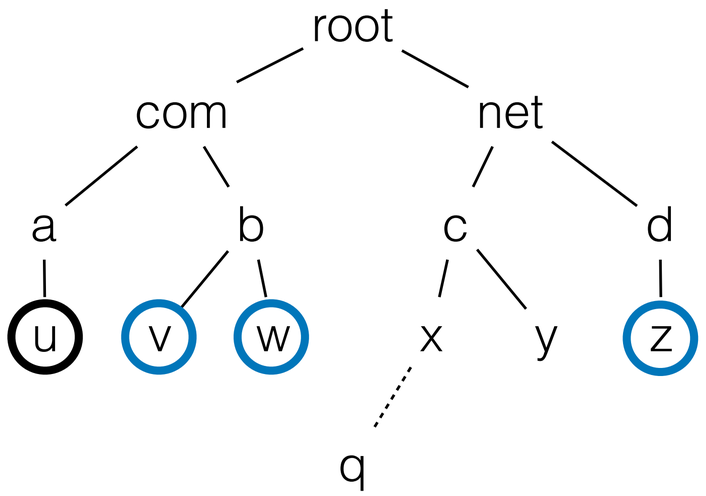
Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

Names on the same path?

All None

Self-probing



Taxonomy of Amplification Primitives

Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

Names on the same path?

All

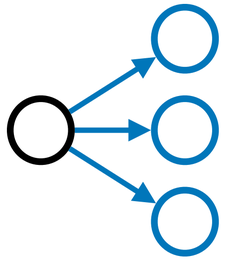
Self-probing

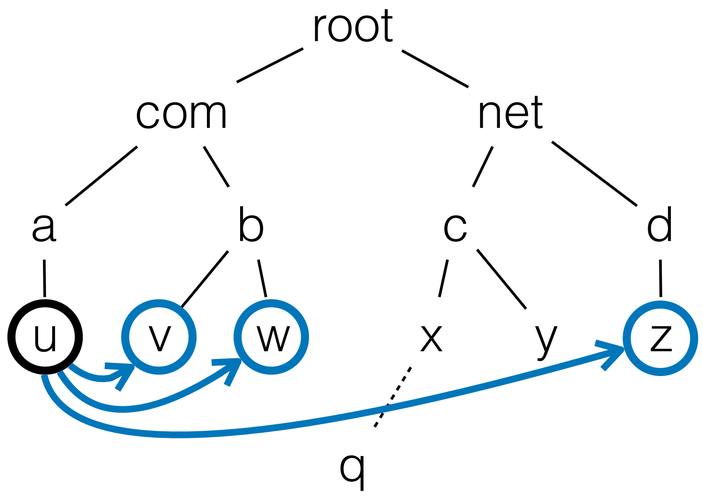
None

Independent derivatives?

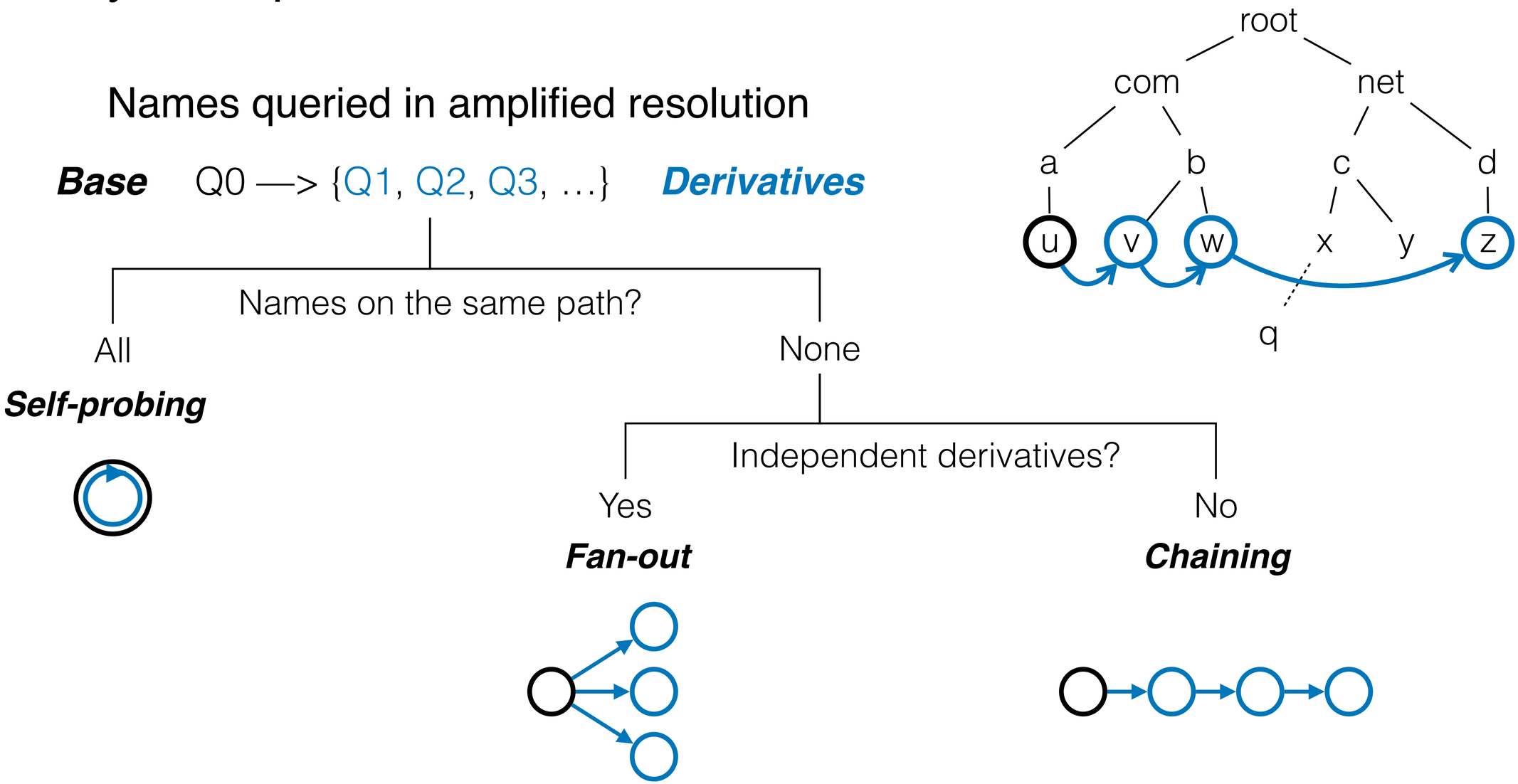
Yes

Fan-out

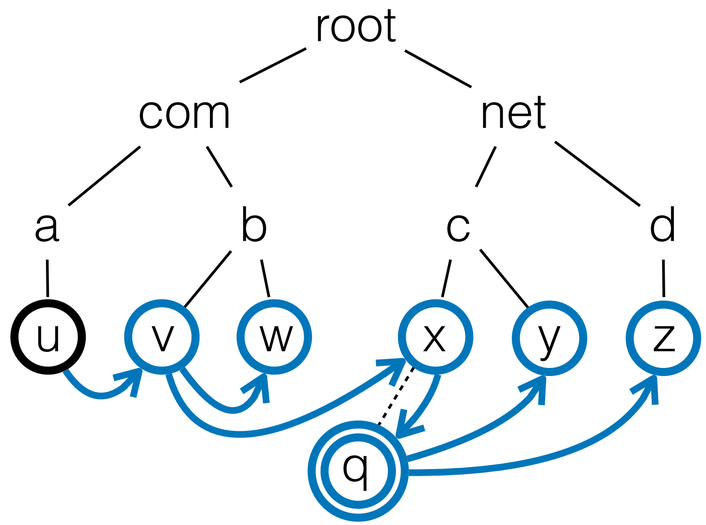




Taxonomy of Amplification Primitives



Taxonomy of Amplification Primitives



Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

Names on the same path?

All

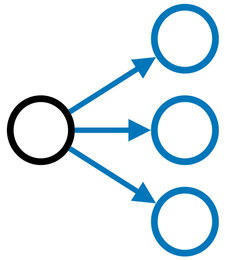
Self-probing

None

Independent derivatives?

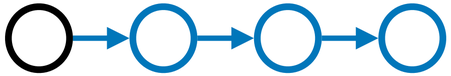
Yes

Fan-out



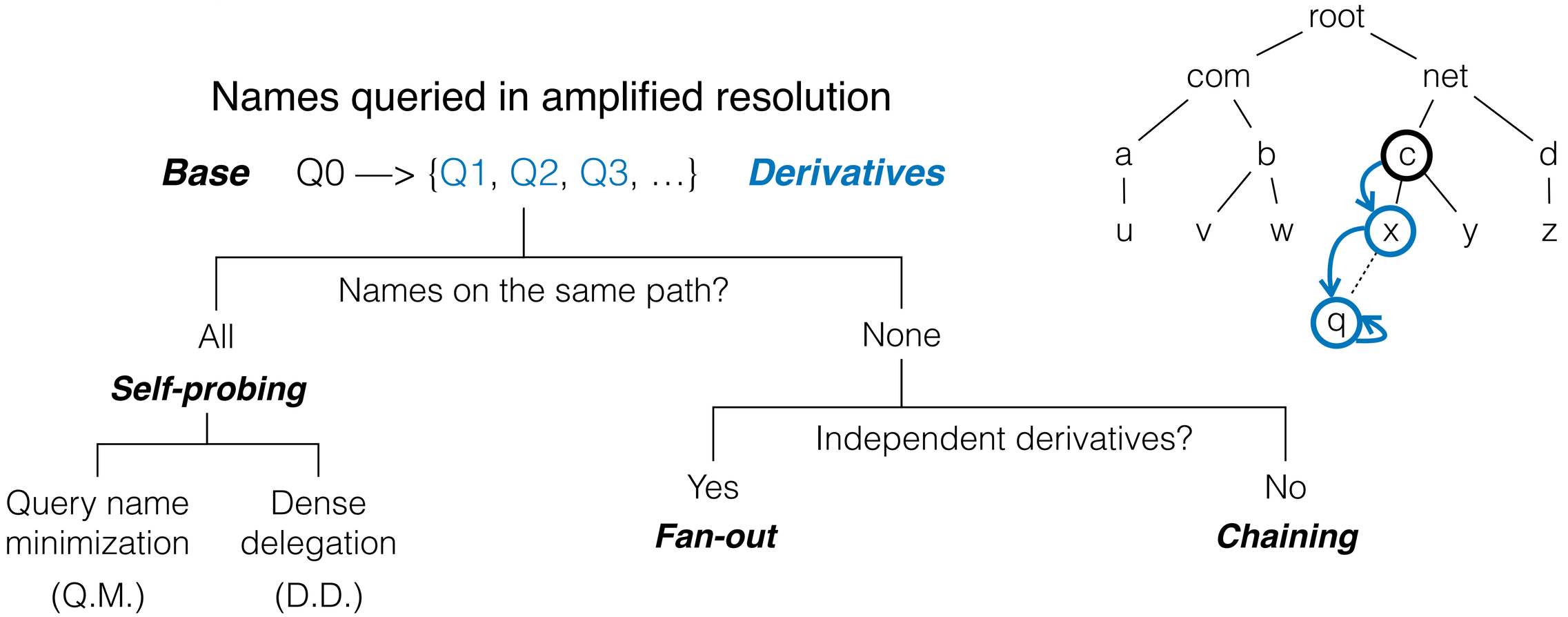
No

Chaining



Allow breakdown of complex resolution

Taxonomy of Amplification Primitives



Taxonomy of Amplification Primitives

Names queried in amplified resolution

Base Q0 —> {Q1, Q2, Q3, …} ***Derivatives***

Names on the same path?

All

Self-probing

Query name minimization (Q.M.)

Dense delegation (D.D.)

None

Independent derivatives?

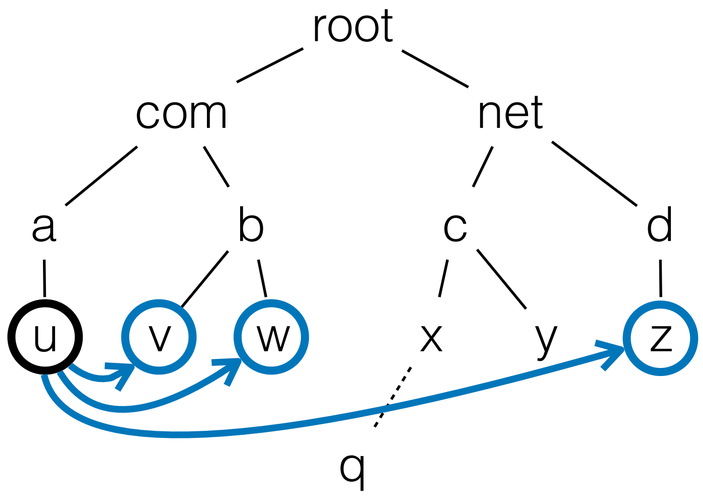
Yes

Fan-out

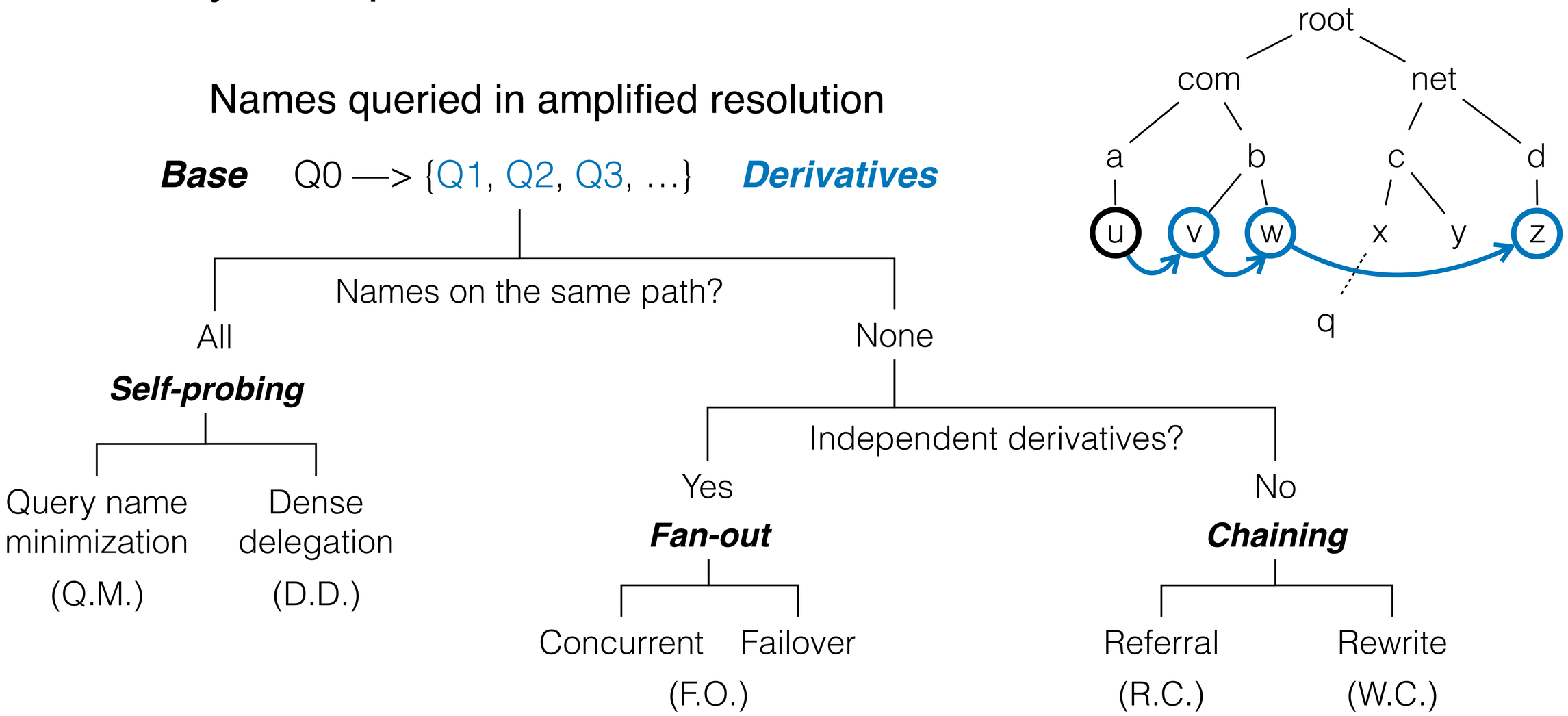
Concurrent Failover (F.O.)

No

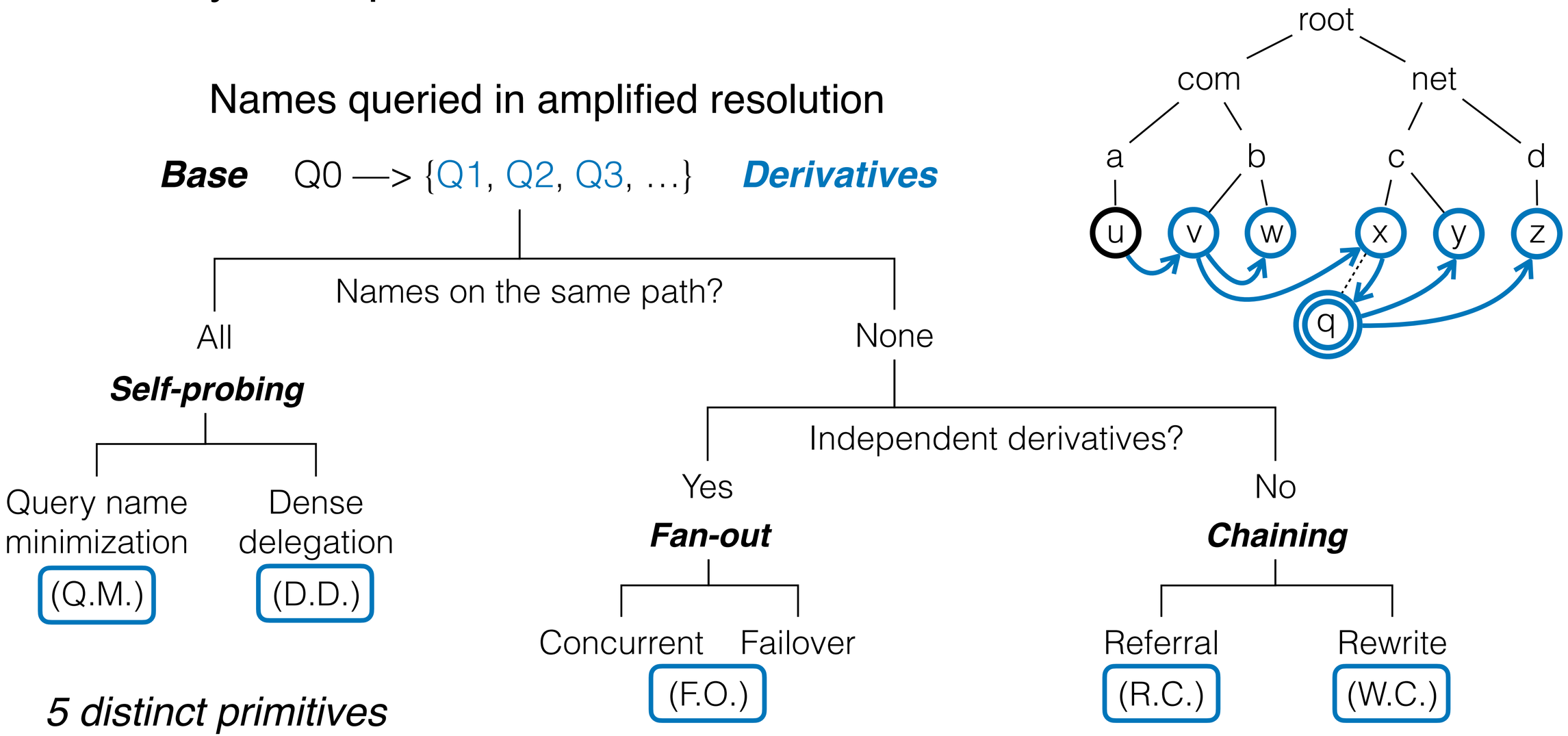
Chaining



Taxonomy of Amplification Primitives



Taxonomy of Amplification Primitives



5 distinct primitives

Composability Analysis

Observation: one primitive's derivative can be another primitive's base

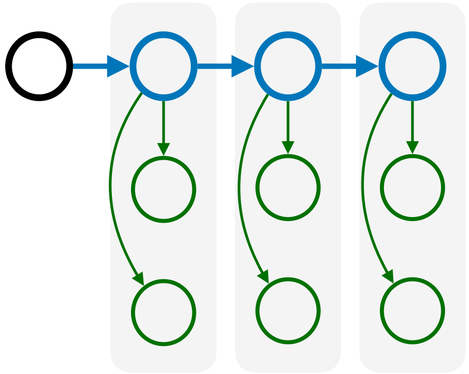
primary ***secondary***

Composability Analysis

Observation: one primitive's derivative can be another primitive's base

primary ***secondary***

Focus on ***regular multiplicative*** compositions

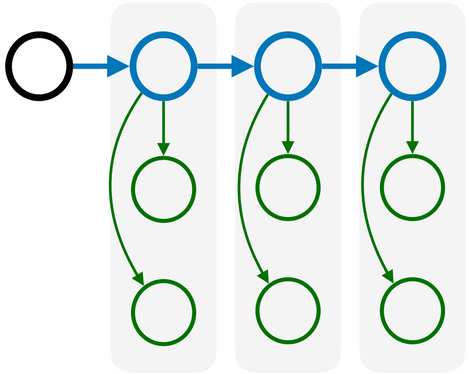


Composability Analysis

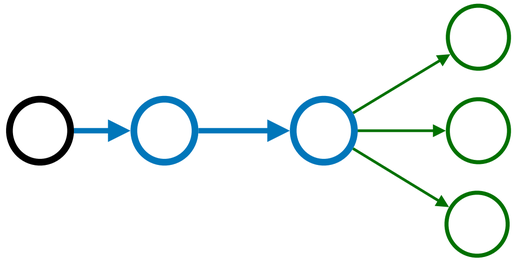
Observation: one primitive's derivative can be another primitive's base

primary ***secondary***

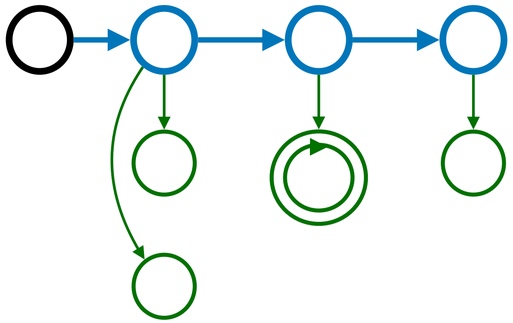
Focus on ***regular multiplicative*** compositions



additive



irregular



Composability Analysis

Results: 16/25 regular multiplicative compositions

Compo-sability		Secondary				
		F.O.	R.C.	W.C.	Q.M.	D.D.
Primary	F.O.	✔	✔	✔	✔	✔
	R.C.	✘	✘	✘	✔	✔
	W.C.	✔	✔	✘	✔	✔
	Q.M.	✘	✘	✘	✘	✘
	D.D.	✔	✔	✔	✔	✔

Composability Analysis

Results: 16/25 regular multiplicative compositions

Compo-sability		Secondary				
		F.O.	R.C.	W.C.	Q.M.	D.D.
Primary	F.O.	✔	✔	✔	✔	✔
	R.C.	✘	✘	✘	✔	✔
	W.C.	✔	✔	✘	✔	✔
	Q.M.	✘	✘	✘	✘	✘
	D.D.	✔	✔	✔	✔	✔

All permitted (implicitly) by RFCs, except two

> “The domain name used as the value of an NS record, or part of the value of an MX record **must not be an alias.**”
>
> – RFC2181

Composability Analysis

Results: construction with carefully crafted zones (on min #nameservers)

Compo-sability		Secondary				
		F.O.	R.C.	W.C.	Q.M.	D.D.
Primary	F.O.	✔	✔	✔	✔	✔
	R.C.	✘	✘	✘	✔	✔
	W.C.	✔	✔	✘	✔	✔
	Q.M.	✘	✘	✘	✘	✘
	D.D.	✔	✔	✔	✔	✔

Example: Rewrite Chain X Fan-out

nameserver@**0.0.0.1**

zone r0.a

```
q.r0.a   CNAME   q.r1.a
```

zone r1.a

```
q.r1.a   CNAME   q.r2.a
```

zone r2.a

```
q.r2.a   CNAME   q.r3.a
```

nameserver@**0.0.0.2**

zone a

```
r1.a   NS   n11.b
r1.a   NS   n12.b
r1.a   NS   n13.b

r2.a   NS   n21.b
r2.a   NS   n22.b
r2.a   NS   n23.b

r3.a   NS   n31.b
r3.a   NS   n32.b
r3.a   NS   n33.b
```

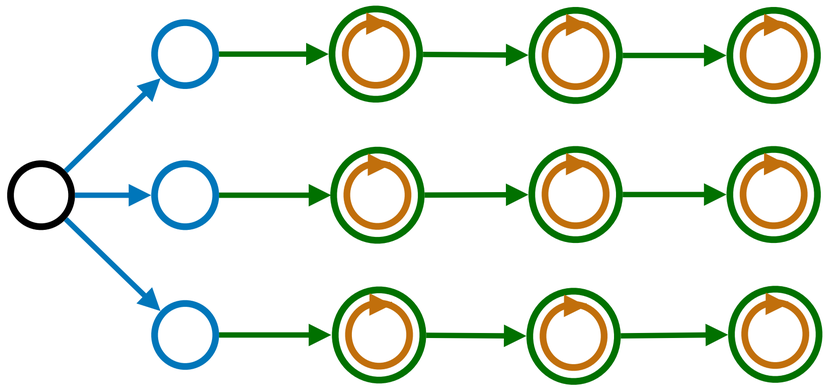
zone b

```
n11.b   A   0.0.0.1
n12.b   A   0.0.0.1
n13.b   A   0.0.0.1

n21.b   A   0.0.0.1
n22.b   A   0.0.0.1
n23.b   A   0.0.0.1

n33.b   A   0.0.0.1
n33.b   A   0.0.0.1
n33.b   A   0.0.0.1
```

Composability Analysis

Exponentially many ***multi-dimensional*** (regular or irregular) compositions!

Example: **Fan-out** X **Chain** X **Self-probing**



Evaluation of MAF on resolvers (before patching)

BIND 9.18.28

W.C. = 17 F.O. = 20 R.C. = 7

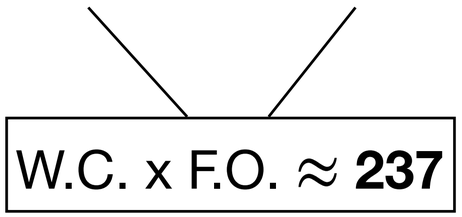
Unbound 1.20.0

D.D. ≈ 82 W.C. = 12 Q.M. = 8

Evaluation of MAF on resolvers (before patching)

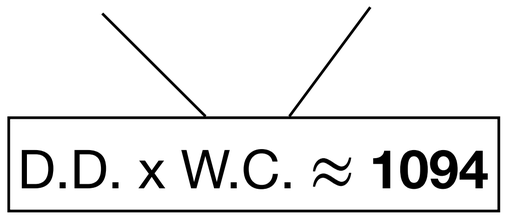
BIND 9.18.28

W.C. = 17 F.O. = 20 R.C. = 7



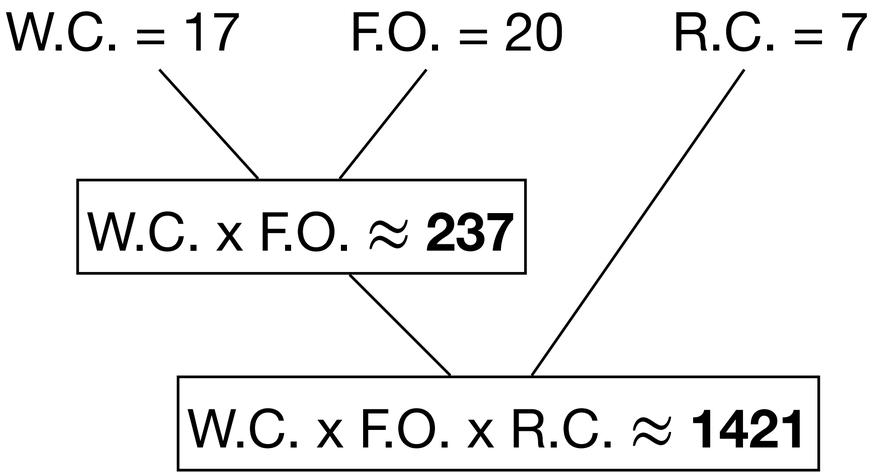
Unbound 1.20.0

D.D. ≈ 82 W.C. = 12 Q.M. = 8

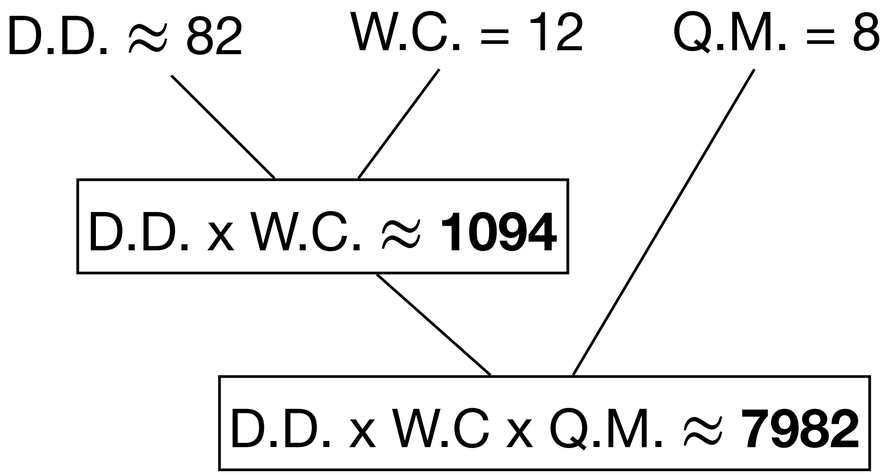


Evaluation of MAF on resolvers (before patching)

BIND 9.18.28



Unbound 1.20.0



Concluding remarks

Self-amplification is inherent to DNS

Systematic analysis & mitigation is necessary

Concluding remarks

Self-amplification is inherent to DNS

Systematic analysis & mitigation is necessary

```
The recommended priorities for the resolver designer are:
     1. Bound the amount of work (packets sent, parallel processes) ...
                                                                - RFC1034
```

Concluding remarks

Self-amplification is inherent to DNS

Systematic analysis & mitigation is necessary

```
The recommended priorities for the resolver designer are:
     1. Bound the amount of work (packets sent, parallel processes) ...
                                                                - RFC1034
```

RFC disambiguation and compliance

- Prohibit aliasing for NS names
- Restrict scope of QMIN
- Explicit guidelines on setting resolution bounds
- …

Thank you!

Contact: huayi.duan@inf.ethz.ch

Find more in our paper