TESTING PROGRAMS WITH HIGHLY CONSTRAINED INPUTS

Valentin Huber

INPUT PROCESSING STEPS

Programs typically process inputs in **distinct steps**, with increasing constraints on **input correctness**.

```
(P1): VBq-"7.6arK w;zu%6$K>%OT                Lexical Error
(P2): && float += % " ( ; == [                Syntactic Error
(P3): int main() { return i; }                Semantic Error
(P4): int main() { return 0; }                Fully Valid
```

MEASURES

Input Correctness

Adherence to Format

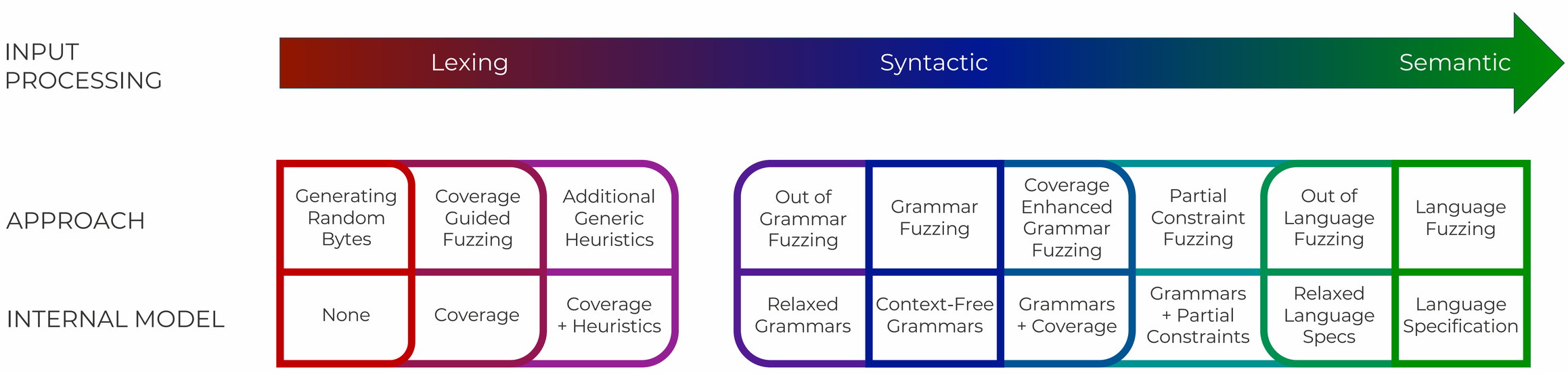
- Distance from **Specification**
- Failure Step in **Implementation**

Input Interestingness

Distance to Boundaries

- **Syntactically**: Structural Extremes
- **Semantically**: Equivalence Class Boundaries

APPROACH CATEGORIZATION



INITIAL EXPERIMENTS

Distribution of inputs across failure steps, as measured on the C compiler **clang** with different approaches.

Fuzzing Approach	Seeds	Other	Lexing	Syntactic	Semantic	Valid
Coverage Guided	❌	0.001	0.566	0.362	0.066	0.0048
	✅	0.000	0.357	0.317	0.316	0.0101
Out of Grammar	❌	0.054	0.293	0.164	0.489	0.0006
	✅	0.054	0.292	0.164	0.489	0.0007
Grammar	❌	0.008	0.397	0.231	0.364	0.0010
	✅	0.008	0.396	0.230	0.365	0.0012
Coverage Grammar	❌	0.000	0.000	0.571	0.429	0.0000
	✅	0.000	0.003	0.553	0.444	0.0000

None of the tested approaches reliably **produce valid inputs**.

FUTURE WORK

- Measure input correctness distribution on **more targets**
- **Combine** measures with other measures such as coverage
- **Out of language fuzzing**: Invalidate constraints
- Extend grammars for **partial constraint fuzzing**
- Generate inputs with high **input interestingness**

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Funded by the European Union

European Research Council
Established by the European Commission

This work is funded by the European Union (ERC S3, 101093186). Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them.

ICSE 2026 RIO DE JANEIRO | BRAZIL