M8 - Mutation Fuzzing

Guillermo Polito

guillermo.polito@inria.fr
@guillep

Goals

- Ideas from mutation analysis can be applied to fuzzing
- Structured inputs can be mutated to obtain new structured inputs
- Semantic-preserving vs Semantic-non-preserving mutations

What if we want slightly different inputs?

- Same conditions:
  - same parents
  - same birthplace
  - …

2 years old

León
Panthera leo
TOP TRUMPS File

Peso (lbs/kg):	496/155
Velocidad (mph/kph):	50/80
Sigilo:	37
Riesgo de encuentro:	2
Puntuación de asesino Top Trumps:	79

Los leones nacen con los ojos cerrados y no los abren hasta las dos semanas de vida.

Los leones viven en grupos, llamados manadas, y las hembras son las que cazan la mayor parte del tiempo. Las leonas más grandes suelen emboscar a las presas y las hembras situadas a los costados las persiguen. Los machos suelen hacer guardia y defender a la manada de los intrusos. Entre sus presas se incluyen mamíferos como los antílopes, las cebras y los facóqueros.

80 km/h

2 years 8 month old

Peso (lbs/kg):	496/155
Velocidad (mph/kph):	50/80
Sigilo:	37
Riesgo de encuentro:	2
Puntuación de asesino Top Trumps:	79

Los leones nacen con los ojos cerrados y no los abren hasta las dos semanas de vida.

Los leones viven en grupos, llamados manadas, y las hembras son las que cazan la mayor parte del tiempo. Las leonas más grandes suelen emboscar a las presas y las hembras situadas a los costados las persiguen. Los machos suelen hacer guardia y defender a la manada de los intrusos. Entre sus presas se incluyen mamíferos como los antílopes, las cebras y los facóqueros.

77 km/h

What if we want slightly different inputs?

- Same conditions:
  - same parents
  - same birthplace
  - …

- Why not study siblings?

2 years old

León
Panthera leo
TOP TRUMPS File

Peso (lbs/kg):	496/155
Velocidad (mph/kph):	50/80
Sigilo:	37
Riesgo de encuentro:	2
Puntuación de asesino Top Trumps:	79

Los leones nacen con los ojos cerrados y no los abren hasta las dos semanas de vida.

Los leones viven en grupos, llamados manadas, y las hembras son las que cazan la mayor parte del tiempo. Las leonas más grandes suelen emboscar a las presas y las hembras situadas a los costados las persiguen. Los machos suelen hacer guardia y defender a la manada de los intrusos. Entre sus presas se incluyen mamíferos como los antílopes, las cebras y los facóqueros.

80 km/h

2 years 8 month old

León
Panthera leo
TOP TRUMPS File

Peso (lbs/kg):	496/155
Velocidad (mph/kph):	50/80
Sigilo:	37
Riesgo de encuentro:	2
Puntuación de asesino Top Trumps:	79

Los leones nacen con los ojos cerrados y no los abren hasta las dos semanas de vida.

Los leones viven en grupos, llamados manadas, y las hembras son las que cazan la mayor parte del tiempo. Las leonas más grandes suelen emboscar a las presas y las hembras situadas a los costados las persiguen. Los machos suelen hacer guardia y defender a la manada de los intrusos. Entre sus presas se incluyen mamíferos como los antílopes, las cebras y los facóqueros.

77 km/h

What if we want slightly different inputs?

- Same conditions:
  - same parents
  - same birthplace
  - …

- Why not study siblings?

  slight genetical mutations

2 years old

León

Panthera leo

TOP TRUMPS File

Peso (lbs/kg):	496/155
Velocidad (mph/kph):	50/80
Sigilo:	37
Riesgo de encuentro:	2
Puntuación de asesino Top Trumps:	79

Los leones nacen con los ojos cerrados y no los abren hasta las dos semanas de vida.

Los leones viven en grupos, llamados manadas, y las hembras son las que cazan la mayor parte del tiempo. Las leonas más grandes suelen emboscar a las presas y las hembras situadas a los costados las persiguen. Los machos suelen hacer guardia y defender a la manada de los intrusos. Entre sus presas se incluyen mamíferos como los antílopes, las cebras y los facóqueros.

80 km/h

2 years 8 month old

León

Panthera leo

TOP TRUMPS File

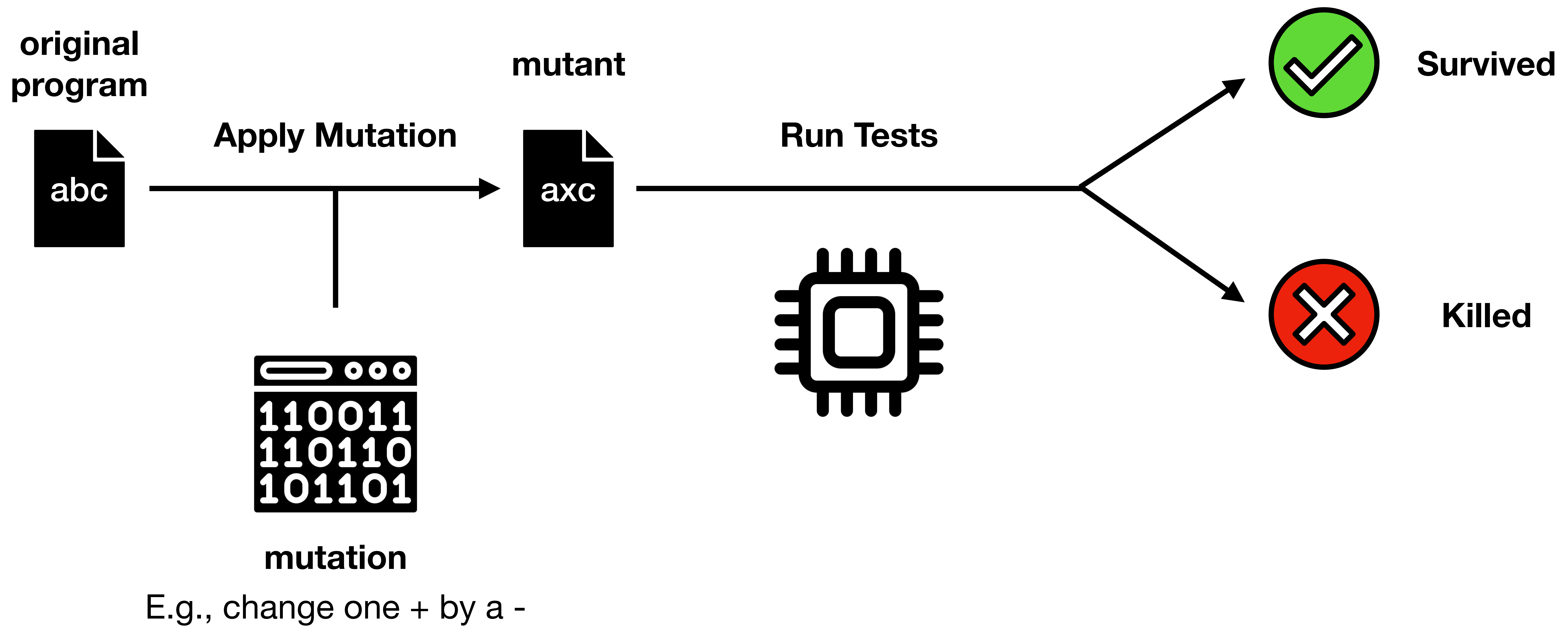
Peso (lbs/kg):	496/155
Velocidad (mph/kph):	50/80
Sigilo:	37
Riesgo de encuentro:	2
Puntuación de asesino Top Trumps:	79

Los leones nacen con los ojos cerrados y no los abren hasta las dos semanas de vida.

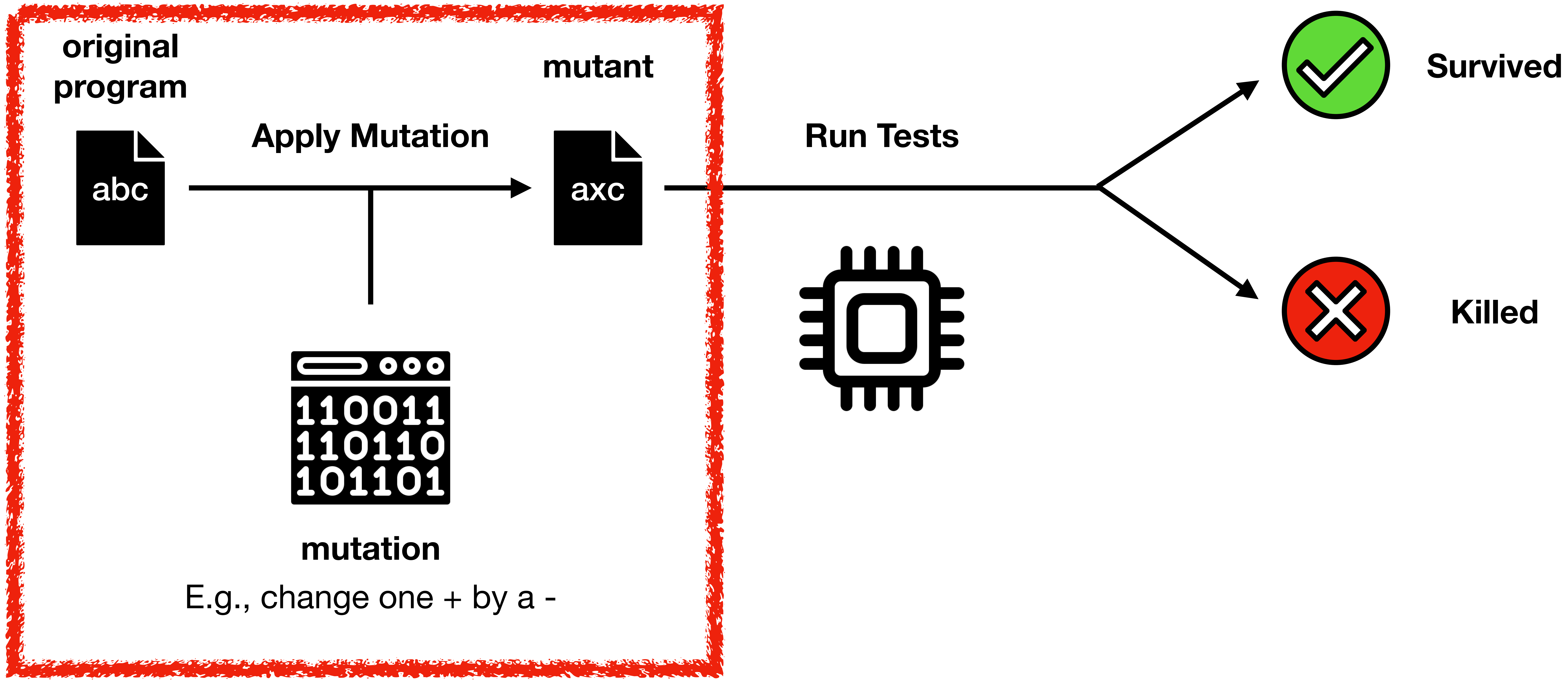
Los leones viven en grupos, llamados manadas, y las hembras son las que cazan la mayor parte del tiempo. Las leonas más grandes suelen emboscar a las presas y las hembras situadas a los costados las persiguen. Los machos suelen hacer guardia y defender a la manada de los intrusos. Entre sus presas se incluyen mamíferos como los antílopes, las cebras y los facóqueros.

77 km/h

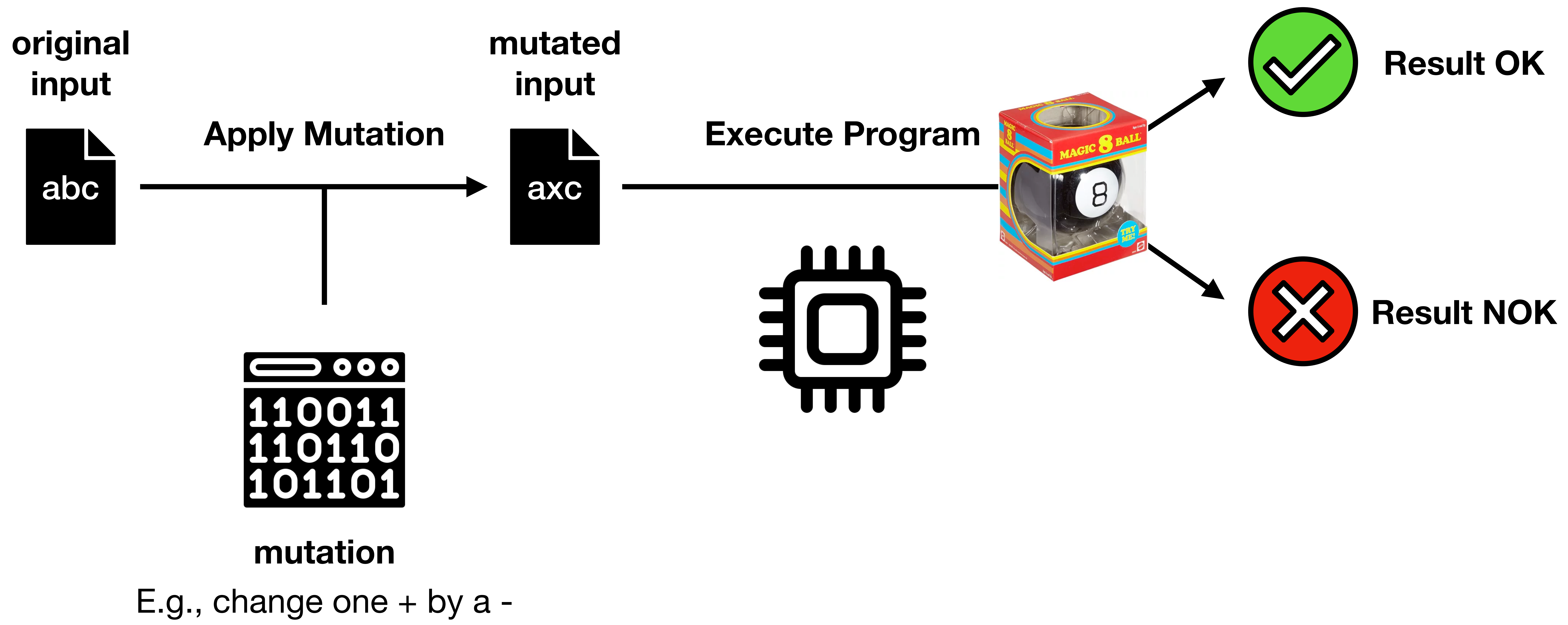
Remember Mutation Analysis



Remember Mutation Analysis



Mutations as Fuzzers



Mutation Analysis vs Mutation Fuzzing

- **Mutation analysis** evaluates test suite *quality*
  - High Mutation Score => good tests
  - Surviving mutants => show missing tests, or are equivalent

- **Mutation fuzzing** creates small variants
  - There is no notion of score
  - Equivalent mutants could be valuable!

Random String Mutator

```
f := PzMutationFuzzer new
  seed: { ‘abcd’ };
  yourself.

(1 to: 10) collect: [ :e | f fuzz ]
```

```
3ou
AbC|dM
aEbcN`
bc
a`c$#
bcc
abc$
aabcd
!cbb~d
;
```

String Mutations

- Insert a *random* character in a *random position* of the string
- Delete a character in a *random position* of the string
- Replace a character by a *random* character in a *random position* of the string

Building a String Mutation Fuzzer

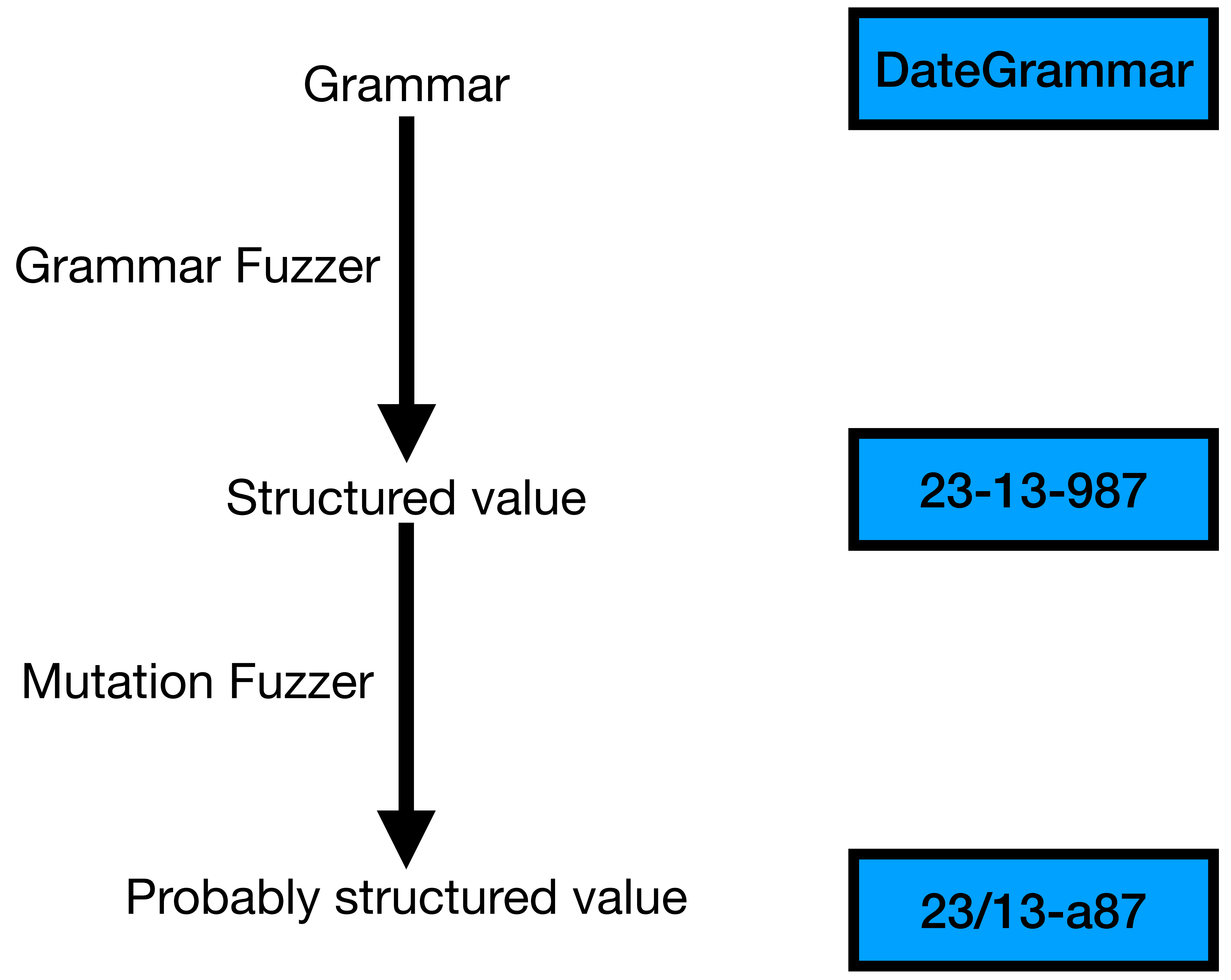
```
PzMutationFuzzer>>fuzz

  | mutationCandidate trials |
  mutationCandidate := seed at: (random nextInteger: seed size).
  trials := random nextIntegerBetween: minMutations and: maxMutations.
  trials timesRepeat: [
     mutationCandidate := self mutate: mutationCandidate ].
  ^ mutationCandidate
```

```
PzMutationFuzzer>>mutate: mutationCandidate
  | mutationIndex mutation |
  mutationIndex := random nextInteger: mutations size.
  mutation := mutations at: mutationIndex.
  ^ mutation mutate: mutationCandidate
```

Chaining Fuzzers

- Mutating a correct value
    - pre-existent or grammar-fuzzed
    - produces *probably* correct values
    - and *probably incorrect* too



How can we get more out of mutations?

Domain-specific mutations

- E.g., swap day and month

```
f := PzMutationFuzzer new
  seed: { '00-11-22' };
  mutations: { PzDayMonthSwapMutation new }
  yourself.
```

- E.g., change the schema of a URL (http by ftp)
- E.g., change the a smic operator by another (+ by -)

Implementing a Mutation

```
PzDeleteCharacterMutation>>mutate: aString
  | index |
  index := aString size atRandom.
  ^ (aString copyFrom: 1 to: index - 1),
     (aString copyFrom: index + 1 to: aString size)
```

Possible Extensions and Next Steps

- Do not mutate strings: mutate ASTs or data structures
  - E.g., look for interesting nodes in the tree and modify/replace them

- Mutate grammars. E.g., modify rule weights
- Semantic-preserving and non-semantic-preserving mutations

- Guide mutations with profiling. E.g., only mutate covered code

Takeaways

- Mutations generate variations of pre-existing inputs
- Simple string-based mutations simulate typos
- We can design domain-specific mutations
  - for simple text formats e.g., dates
  - for complex languages e.g., operators
    - and these can work on top of ASTs

Material

- The Fuzzing Book. Mutation Chapter. A. Zeller et al
  https://www.fuzzingbook.org/html/MutationFuzzer.html

- Binary Fuzzing Strategies in AFL — Blog
  https://lcamtuf.blogspot.com/2014/08/binary-fuzzing-strategies-what-works.html