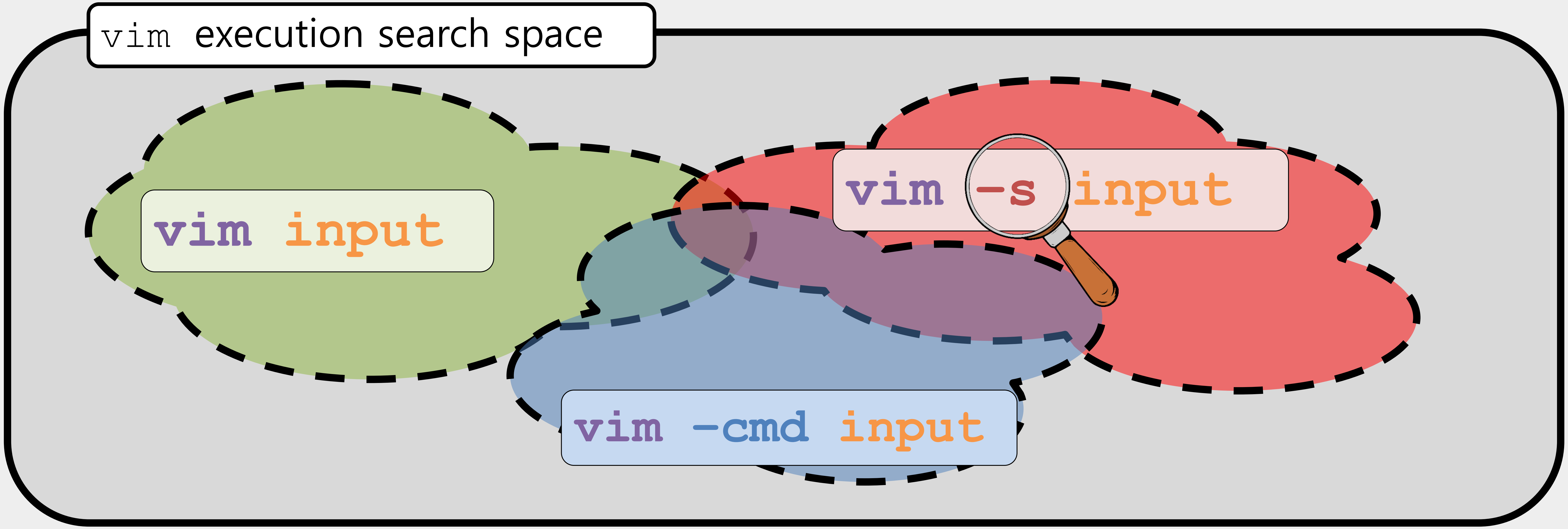
ICST 2022

POWER : Program Option-Aware Fuzzer for High Bug Detection Ability

Ahcheong Lee (KAIST, South Korea)
Irfan Ariq (KAIST , South Korea)
Yunho Kim (Hanyang Univ. , South Korea)
Moonzoo Kim (KAIST , South Korea)

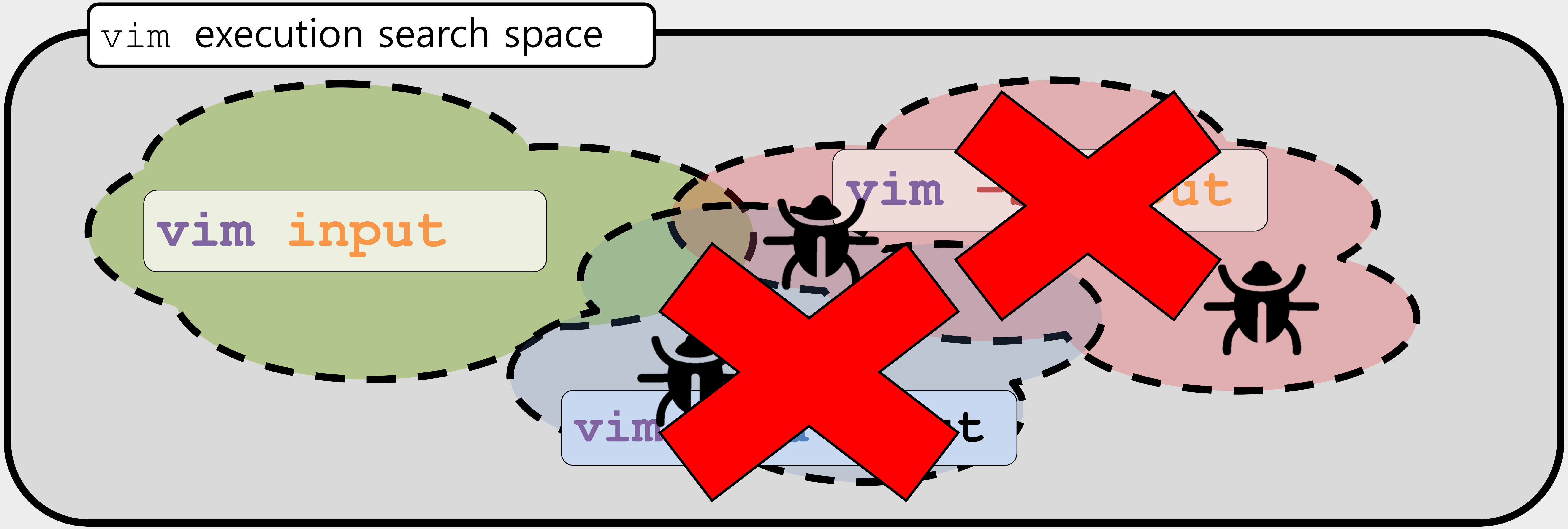
In Short - Mutate Command Lines Options!

CLI (Command Line Interface) programs use **command line options** to determine which features (functions) to execute



Command Line Options Are Not Used by Current Fuzzing Techniques.

3/4 of 100 recent fuzzing papers provide NO command line information.

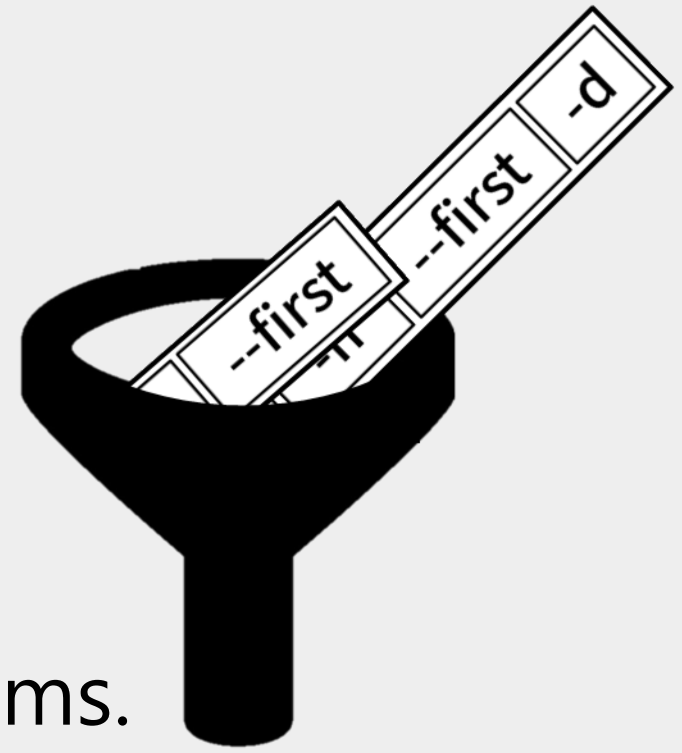


Contributions

Contribution 1.
POWER carefully mutate and select CLI options.

Contribution 2.
POWER detected 88 crashes in 19 subjects.
(which is significant more than other state-of-the-art fuzzers)

Contribution 3.
We reported the crashes to improve the quality of the open-source programs.



Careful Mutation/Selection of Command Line Options

Careful Mutation

✗

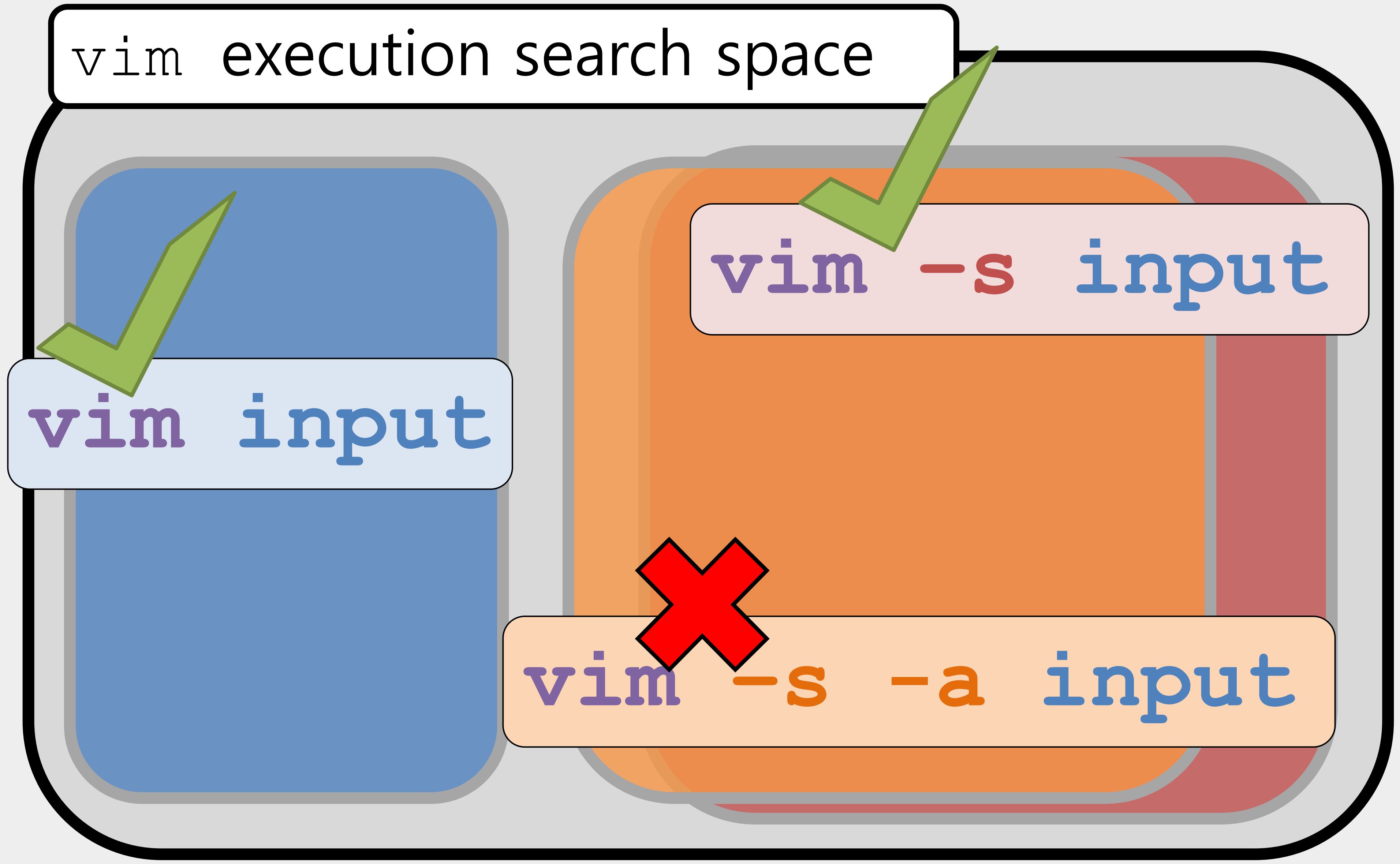
```
vim %s@!d0sd@!
vim %20132A3!#*$
vim #^^$%(@as092
```

○

```
vim -e -s -clean -cmd
vim -e -s 'g '
vim -q -first
```

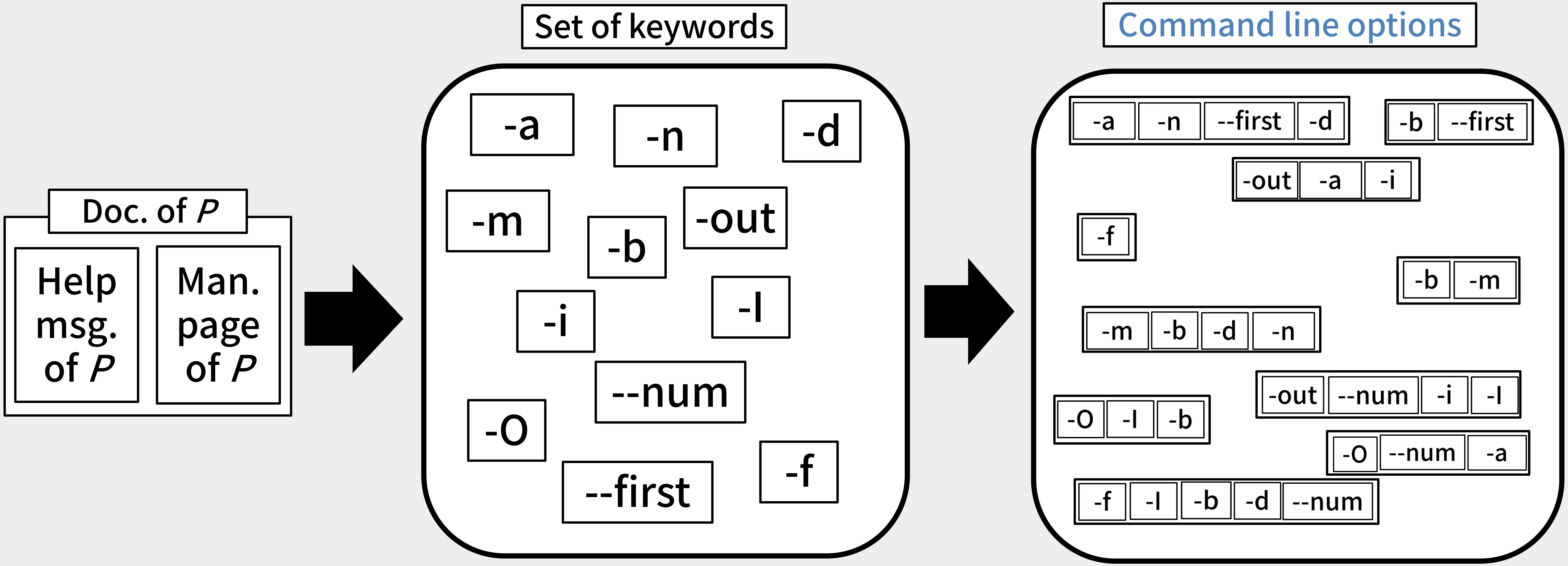
Careful Selection

Focus on Distinct CLI options.

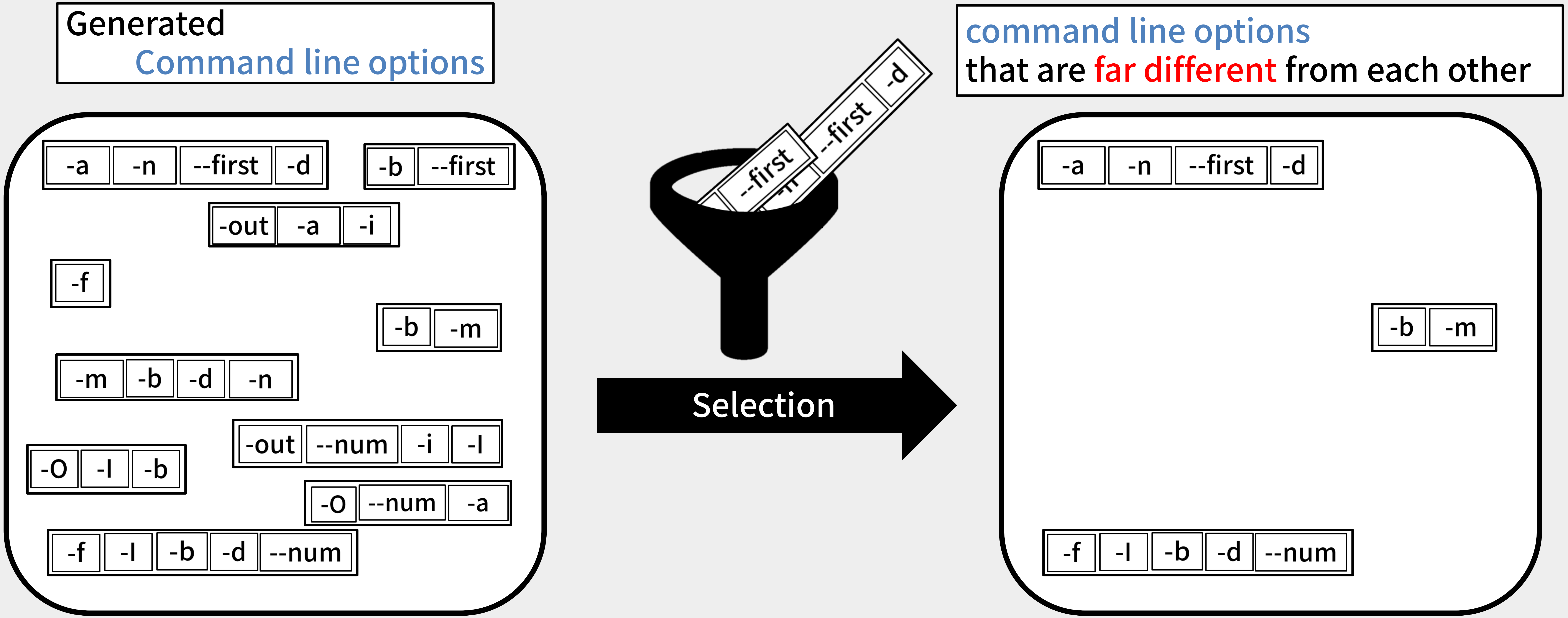


Careful Generation of Command Line Options

Dictionary-based mutation to generate valid command line options



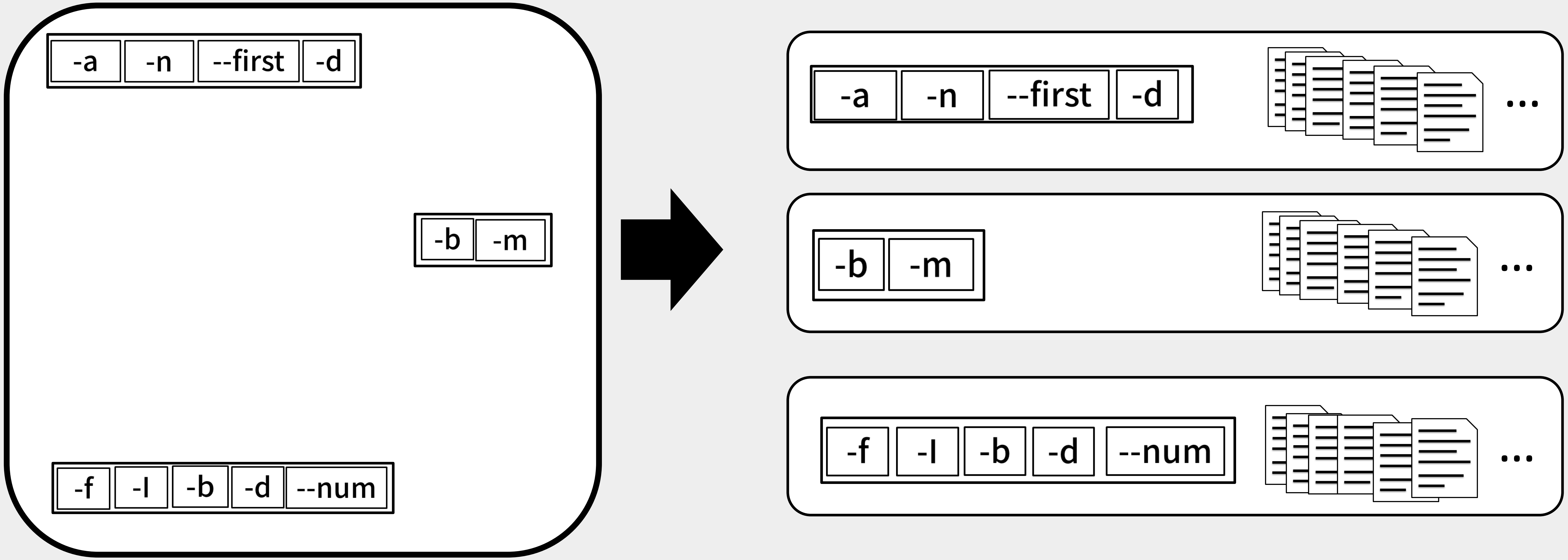
Careful Selection of Distinct Command Line Options



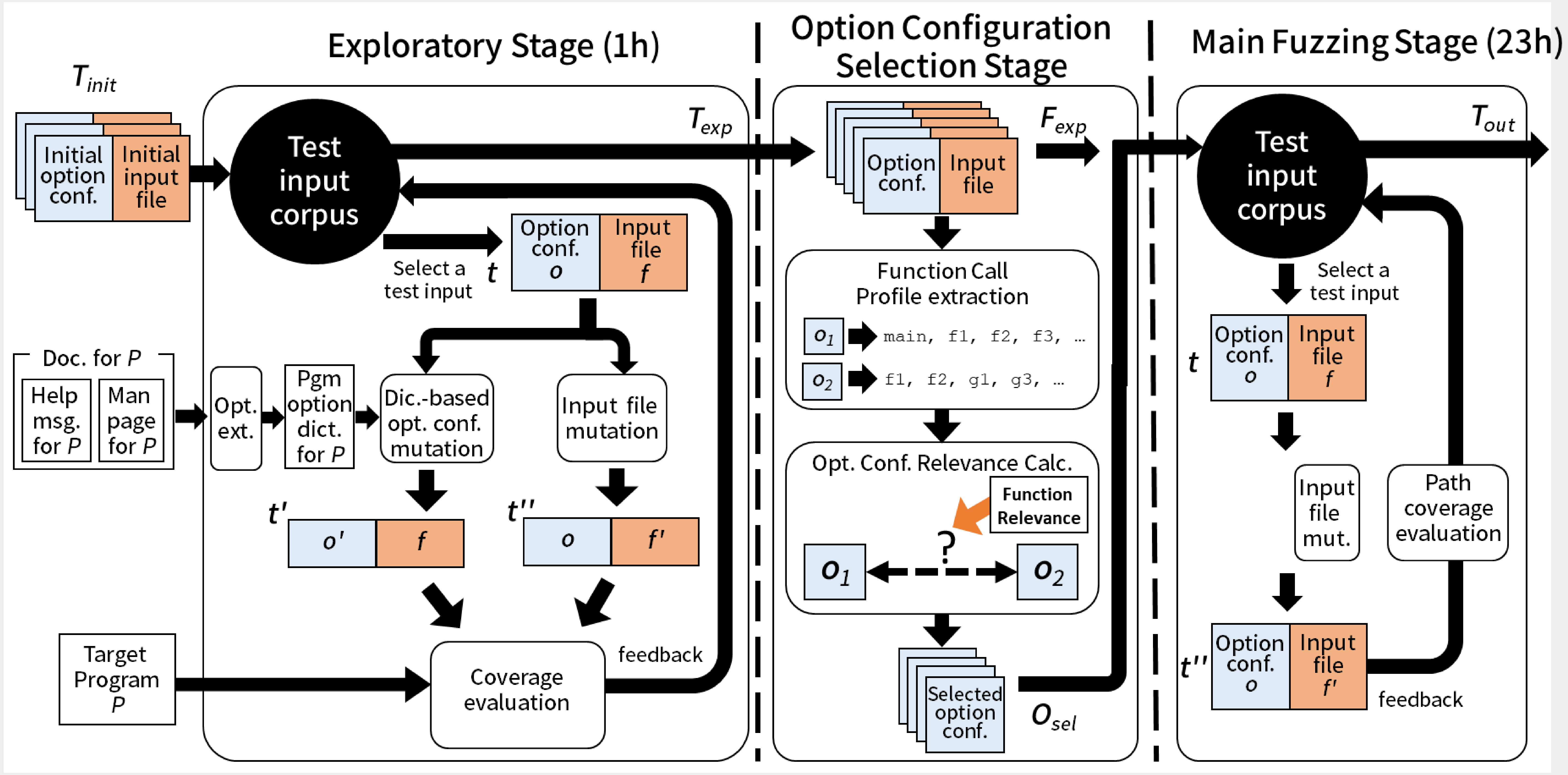
Careful Selection of Distinct Command Line Options

command line options that are far different from each other

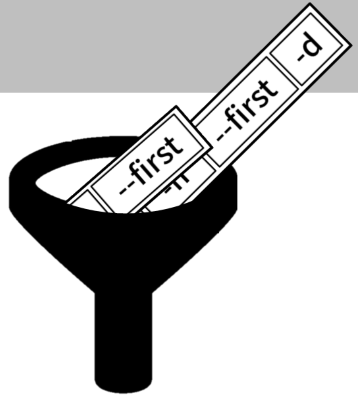
Mutate input file with selected command line options

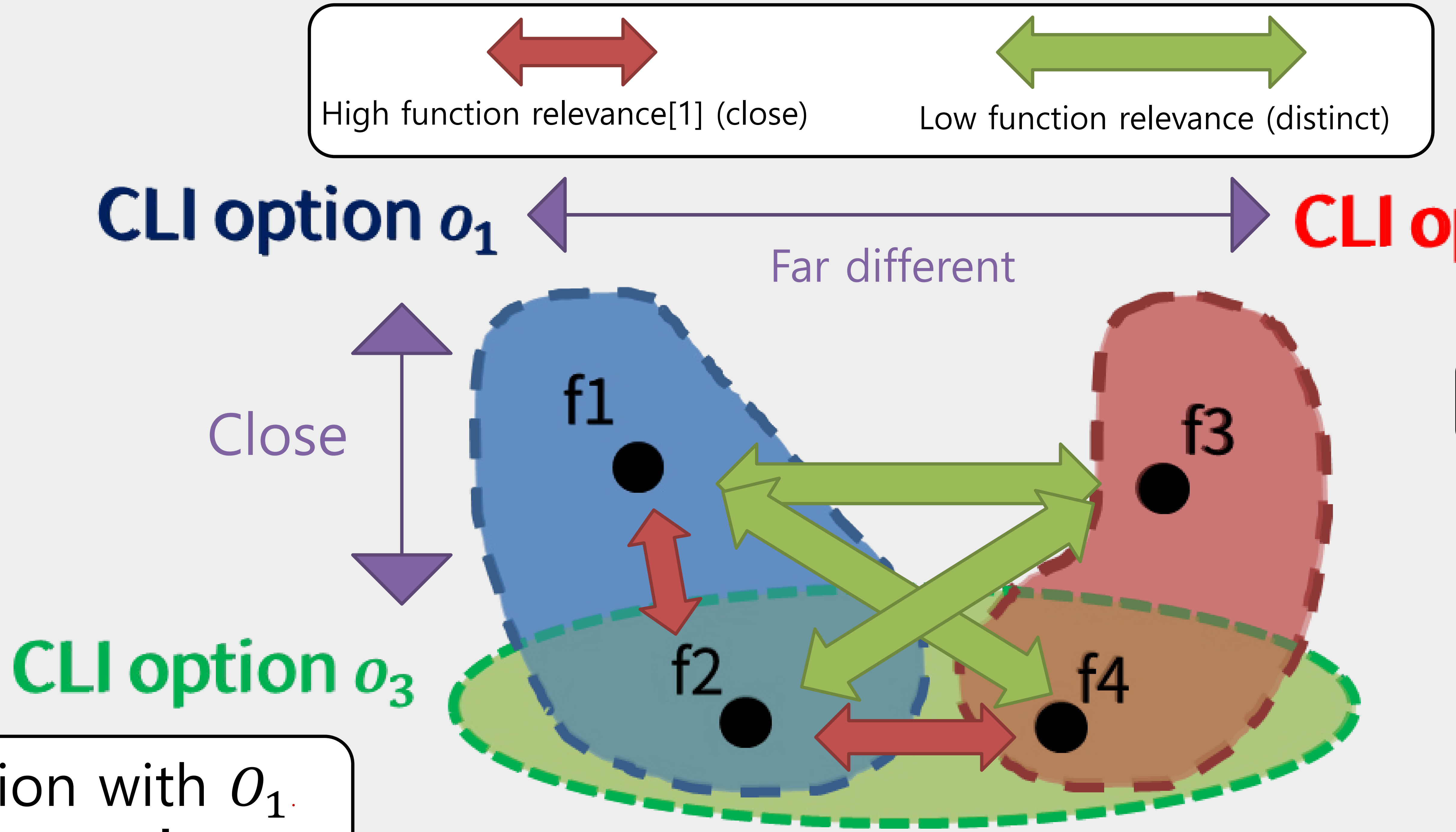


POWER Framework



How to select "distinct/different" command line options





Selected CLI option

O_1, O_2

Execution with O_1 cover $f1$ and $f2$.

[1] Kim et al. Precise concolic unit testing of C programs using extended units and symbolic alarm filtering.(ICSE '18)

Evaluation

RQ1. Is POWER better than the state-of-the-art fuzzer?

RQ2. Did relevance-based option selection contribute to POWER's performance?

RQ3. Did option selection strategy contribute to POWER's performance?

Measurement: the number of detected crashes

Setup : 24 hours run, repeated 10 times.

Test subjects

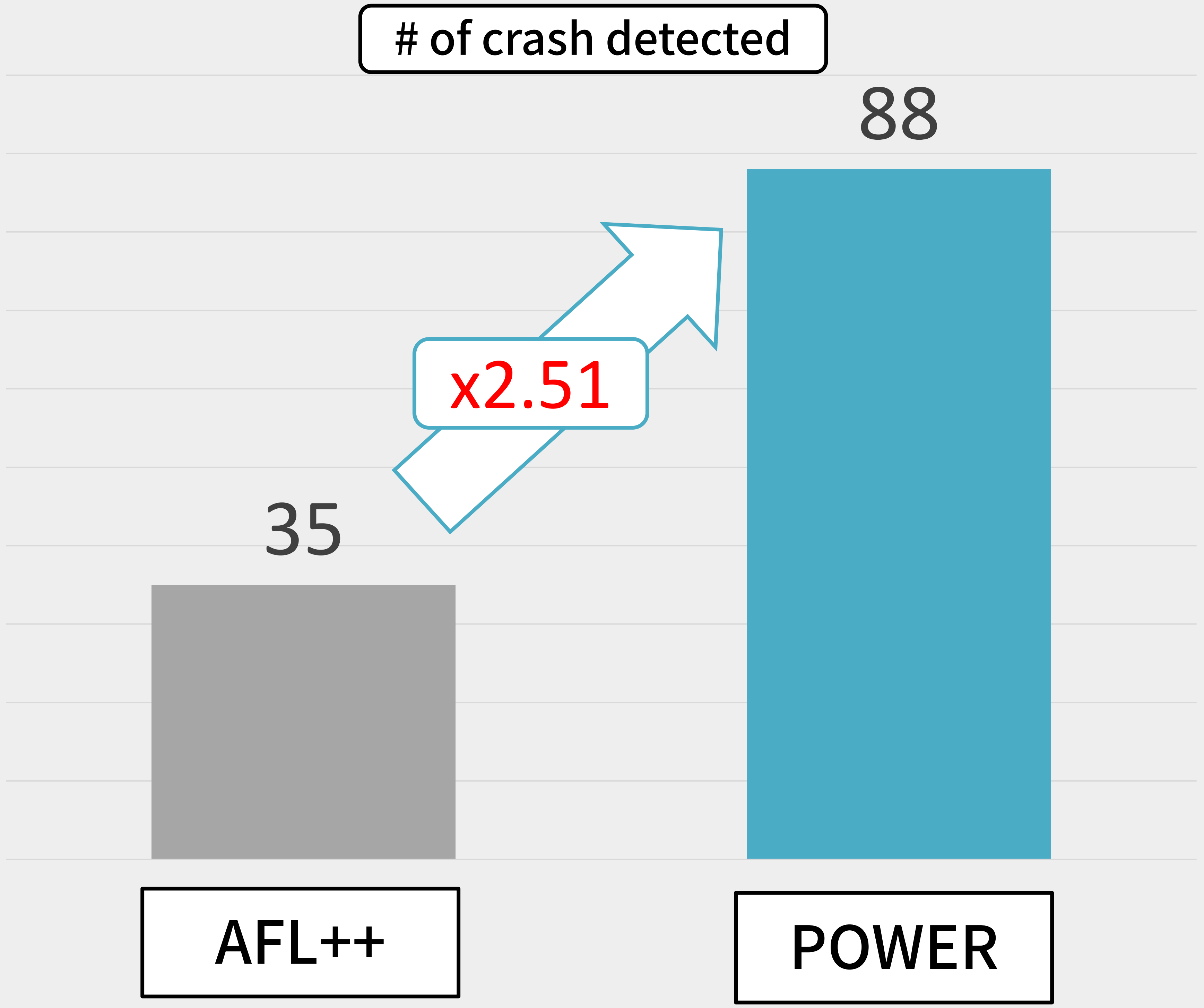
30 subjects that are used by other fuzzing papers

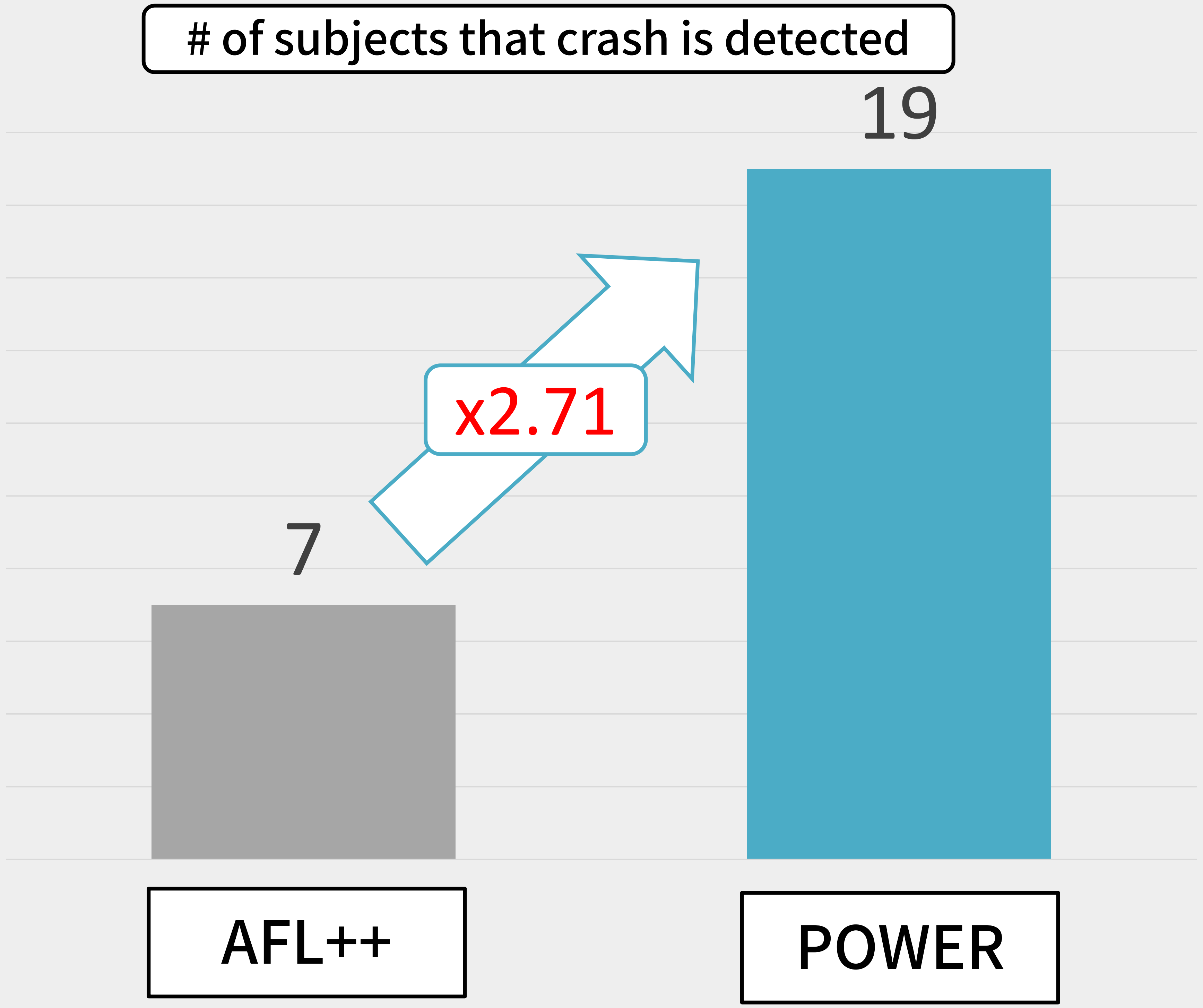
Avg. Loc : 137,570
Avg. # of keywords : 87

Subjects	Size (Loc)	# of CLI keywords	Subjects	Size (Loc)	# of CLI keywords	Subjects	Size (Loc)	# of CLI keywords
avconv	454,936	80	jasper	2,920	16	readelf	74,789	169
bison	54,423	54	mpg123	11,298	123	size	436,055	19
cflow	18,197	45	mutool	364,318	224	tiff2pdf	8,234	35
cjpeg	6,308	37	nasm	70,903	33	tiff2ps	5,646	41
djpeg	5,792	37	objdump	877,165	145	tiffinfo	3,752	10
dwarfdump	83,545	48	pdftohtml	38,111	32	vim	296,916	54
exiv2	33,417	79	pdftopng	97,890	33	xmlcatalog	2,609	27
ffmpeg	774,186	230	pdftops	103,077	46	xmllint	11,285	94
gm	197,891	760	pngfix	7,020	15	xmlwf	4,147	19
gs	1,174,673	53	pspp	4,901	25	yara	5,862	37

Result – RQ 1 : Is POWER better than the state-of-the-art fuzzer?

AFL++ with 10 popular CLI options used by other fuzzing papers





Result – Crash example

One crash found in `mpg123` contains 13 command line keywords:

```
./mpg123 -smooth -listentry -z -w 1 --quiet --index - -4to1
-2 -q -fifo --outfile
```

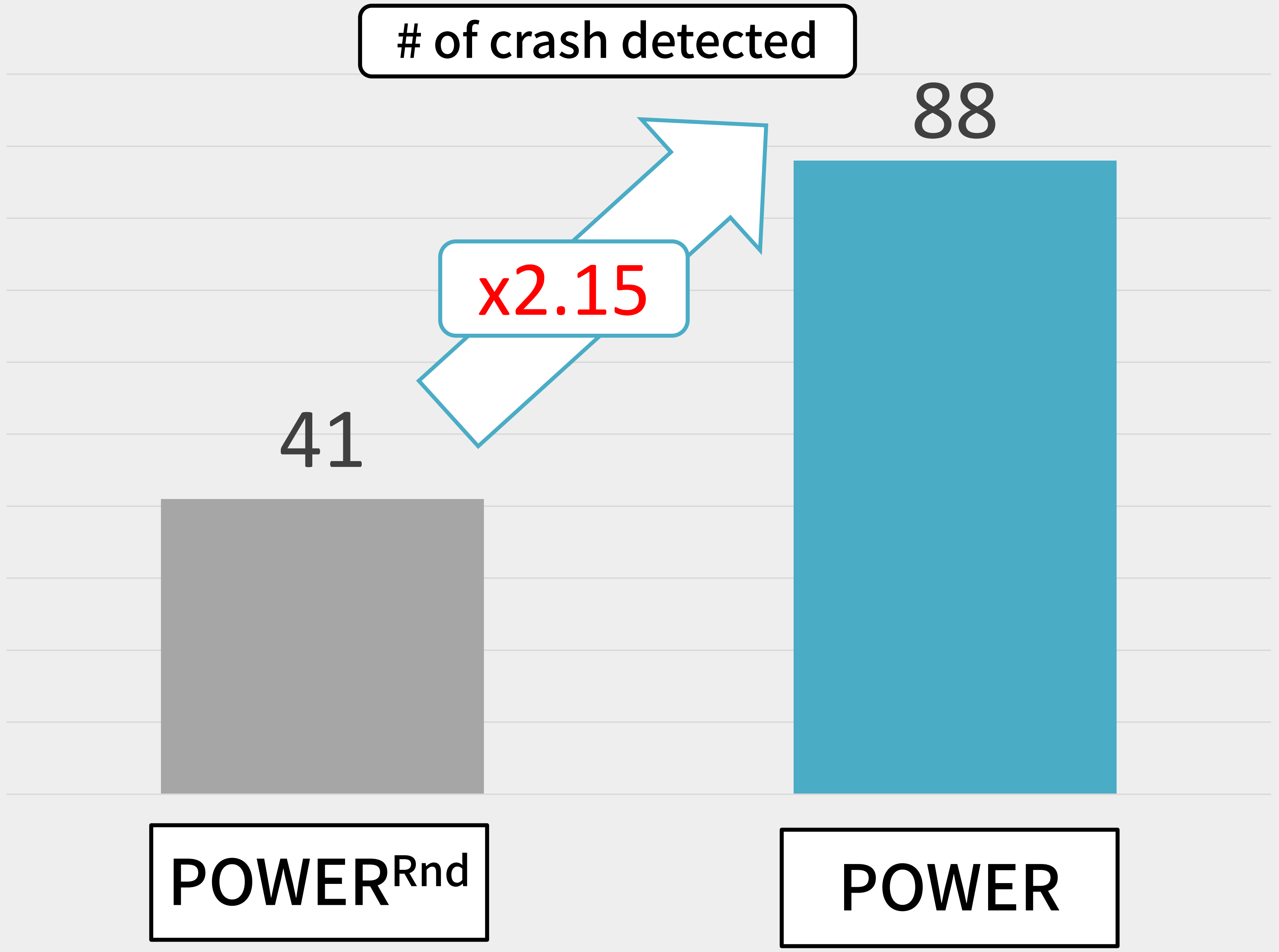
The developer of `mpg123` commented that:

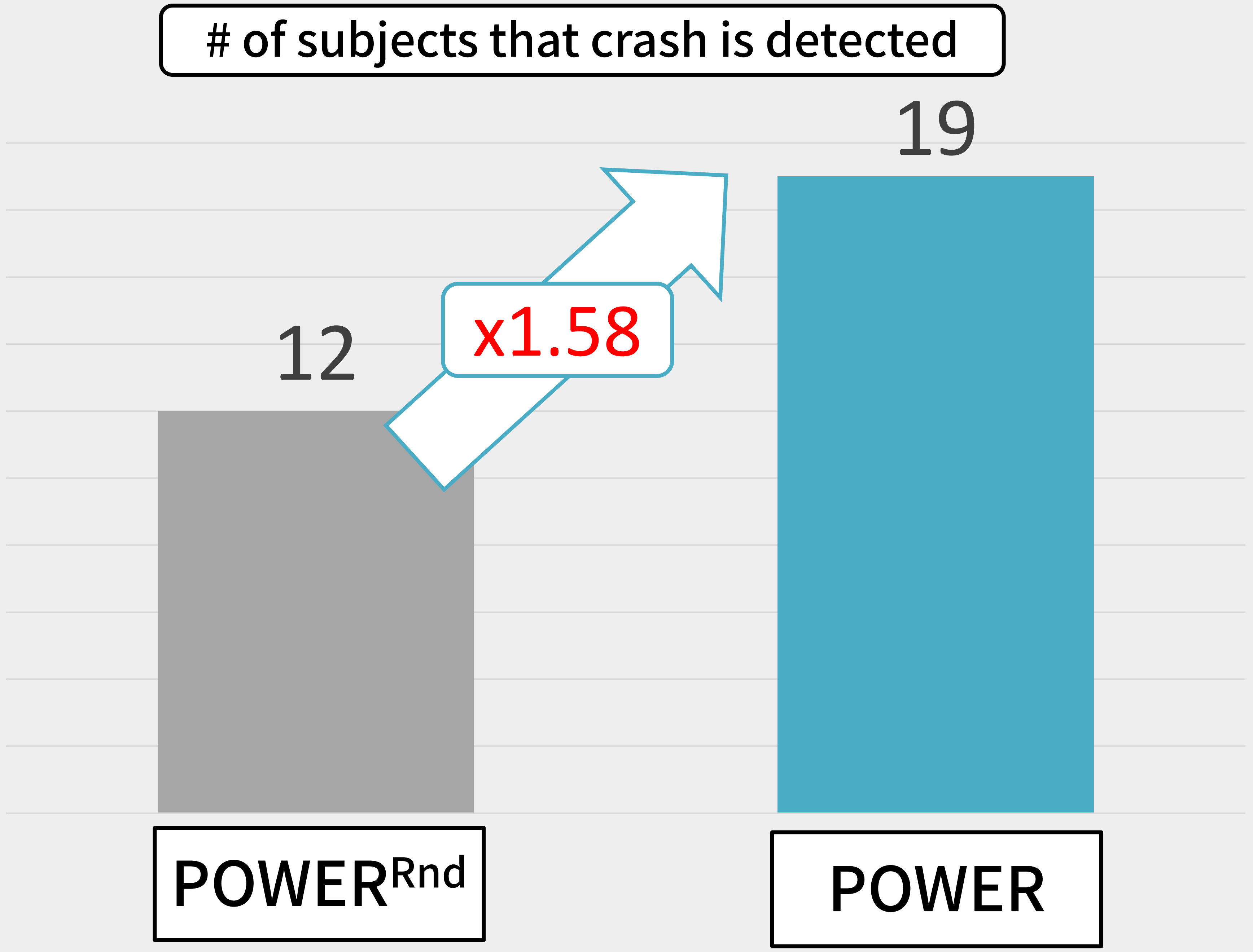
“Interesting approach you find stuff where oss-fuzz didn’t anymore.”

Evaluation – RQ2

RQ2: Did relevance-based option selection contribute to POWER's performance?

- POWER^{Rnd}
  - Apply random function relevance value

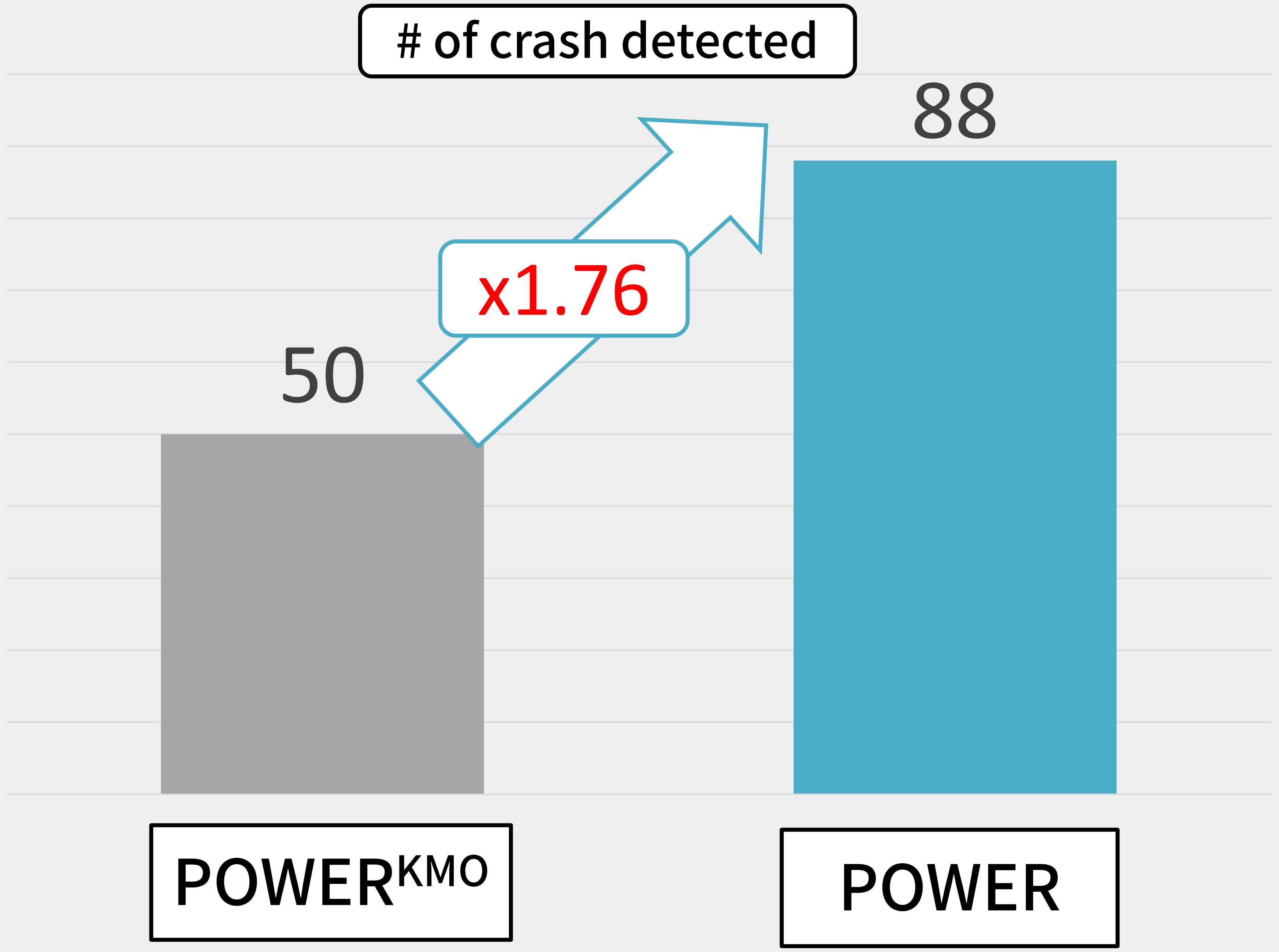


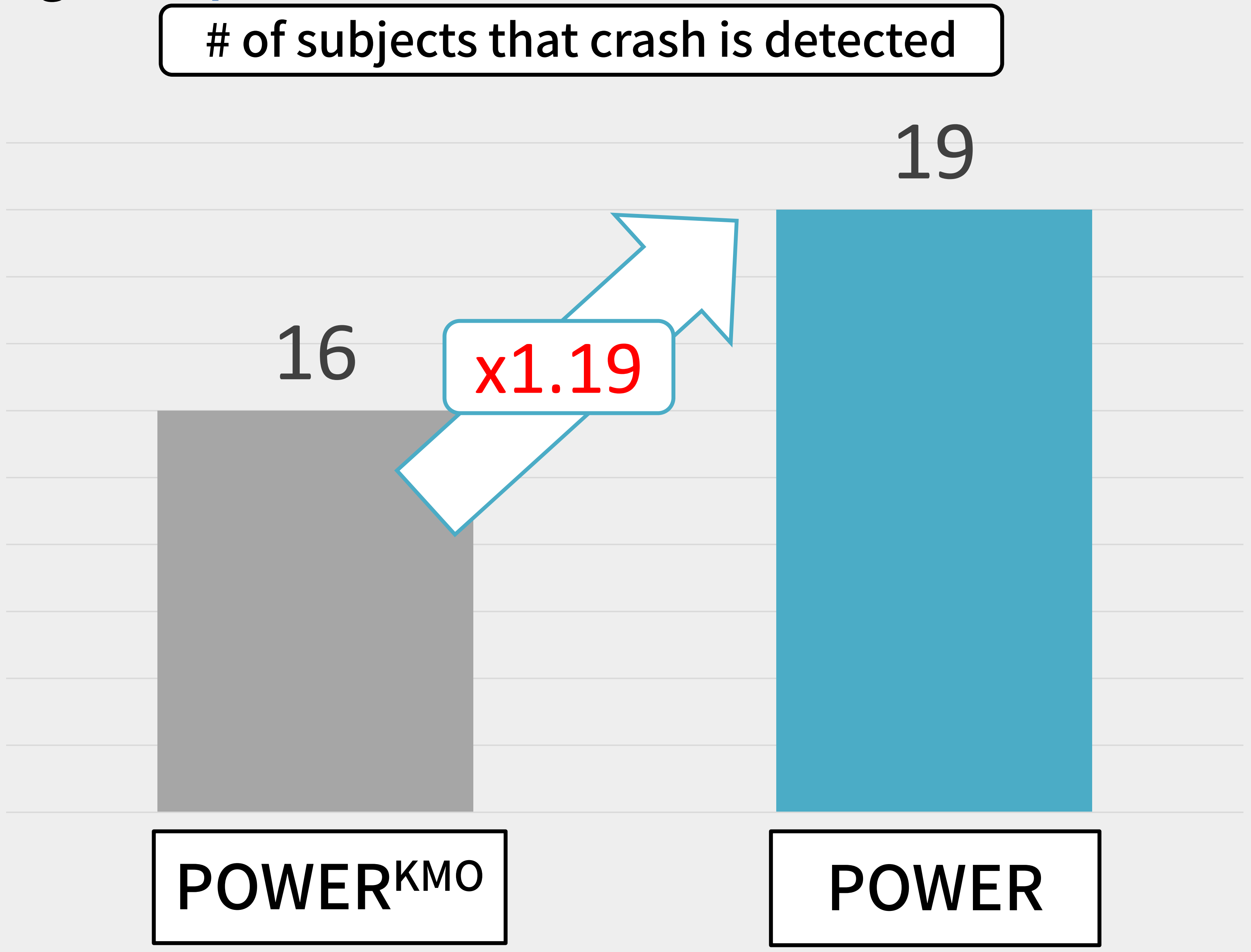


Result – RQ3

RQ3. Did option selection strategy contribute to POWER's performance?

- POWER^{KMO}
  - Keep Mutating CLI Options instead of selecting CLI options





Conclusion

Contribution 1.
POWER is the first fuzzing thechnique that actively and carefully mutate and select CLI options based on dynamic function relevance metric.

Contribution 2.
On the latest version of 30 open source C/C++ programs,
POWER detected significantly more crashes (88 crashes in 19 subjects)
than other state-of-the-art fuzzers.

Contribution 3.
We reported the crashes to improve the quality of the open source subject programs.