프로그램 옵션을 고려하는 퍼징

POWERUP: Program Option-Aware Interleaving Fuzzing Platform for High Bug Detection

---

이아청 (KAIST 김문주 교수님 연구실)
최영석 (KAIST)
김윤호 (한양대)
홍신 (한동대)
김문주 (KAIST)

2023 SW재난센터 여름워크샵

퍼징 - 무작위 변이 기반 입력 생성 기법

cjpeg – 이미지 변환 프로그램

```
./cjpeg -gray input.jpg
```

퍼징 - 무작위 변이 기반 입력 생성 기법

cjpeg – 이미지 변환 프로그램

```
./cjpeg -gray input.jpg
```

입력 파일= 단순 바이트 값의 나열

ff	d8	ff	e0	00	…

변이

새로운 테스트 입력값

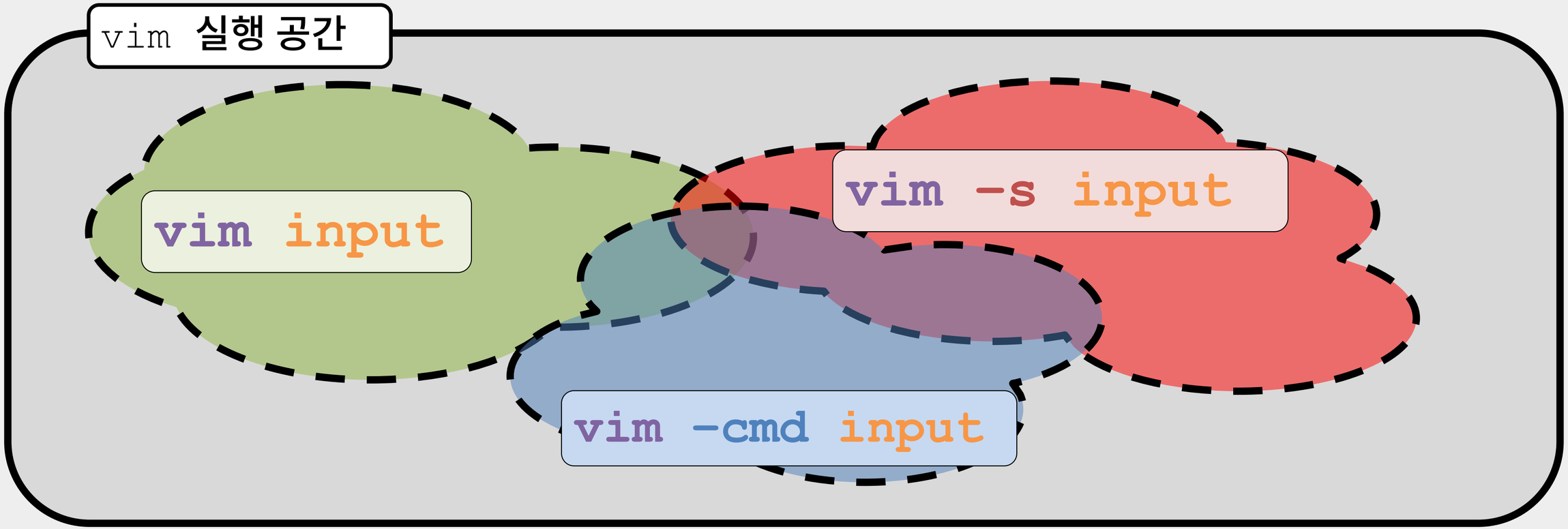
ff	d8	3a	e0	00	…

목표 : 프로그램 옵션 (커맨드 라인)도 같이 다양하게 만들자!

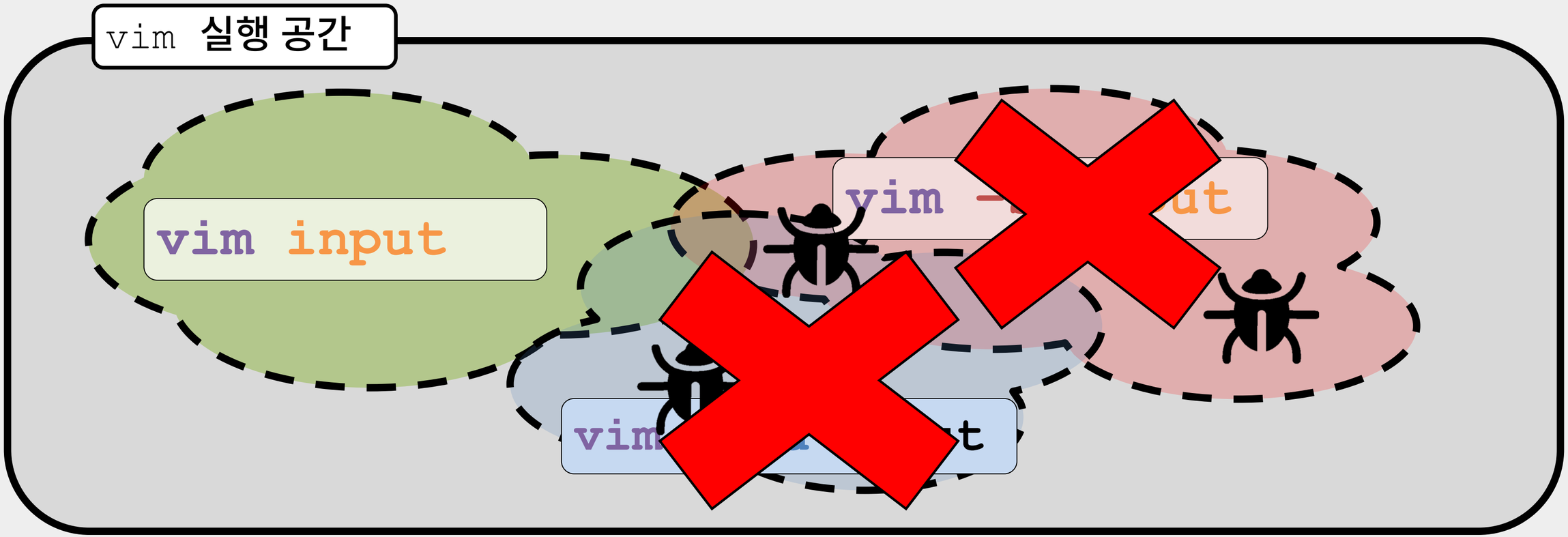
CLI (Command Line Interface) 프로그램은 커맨드 라인이
어떤 기능을 실행할지를 결정

목표 : 프로그램 옵션 (커맨드 라인)도 같이 다양하게 만들자!

CLI (Command Line Interface) 프로그램은 커맨드 라인이
어떤 기능을 실행할지를 결정



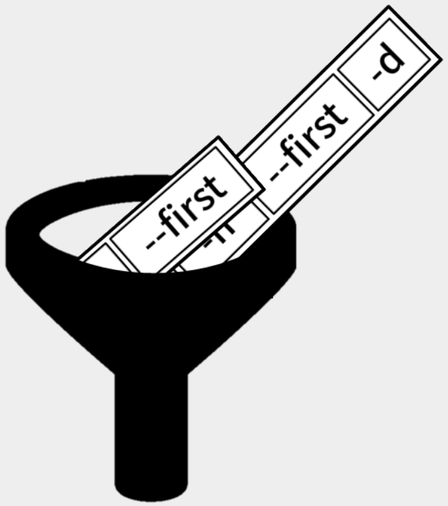
기존 연구는 커맨드 라인을 고려하지 않았음



Contributions

Contribution 1.
다른 특성을 가지는 프로그램 옵션과 파일을
분리하여 다르게 변이하는 기법 제시

Contribution 2.
POWERUP을 사용하여 15개의 실제 오픈 소스
프로그램에서 85개의 크래시 오류 발견

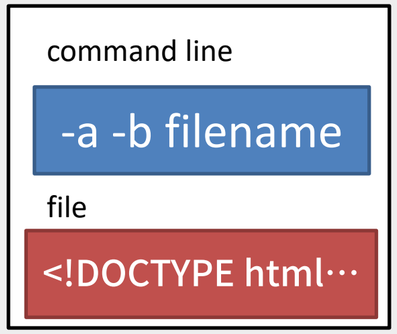


2 Key features

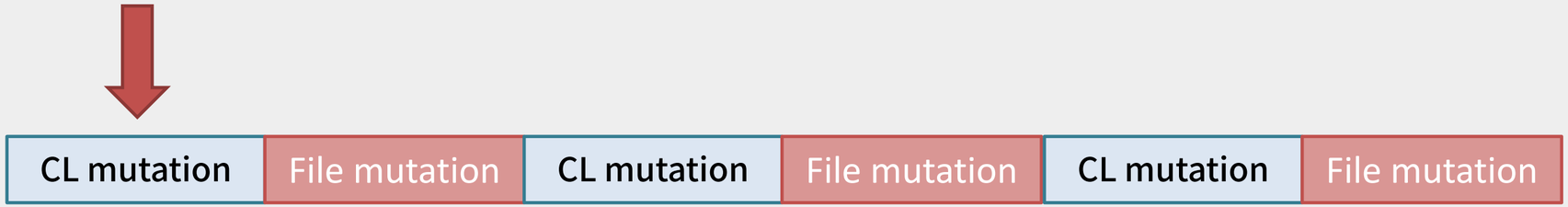
1. 분리하여 번갈아가며 변이하는 전략
   프로그램 옵션과 파일을 독립적으로 변이

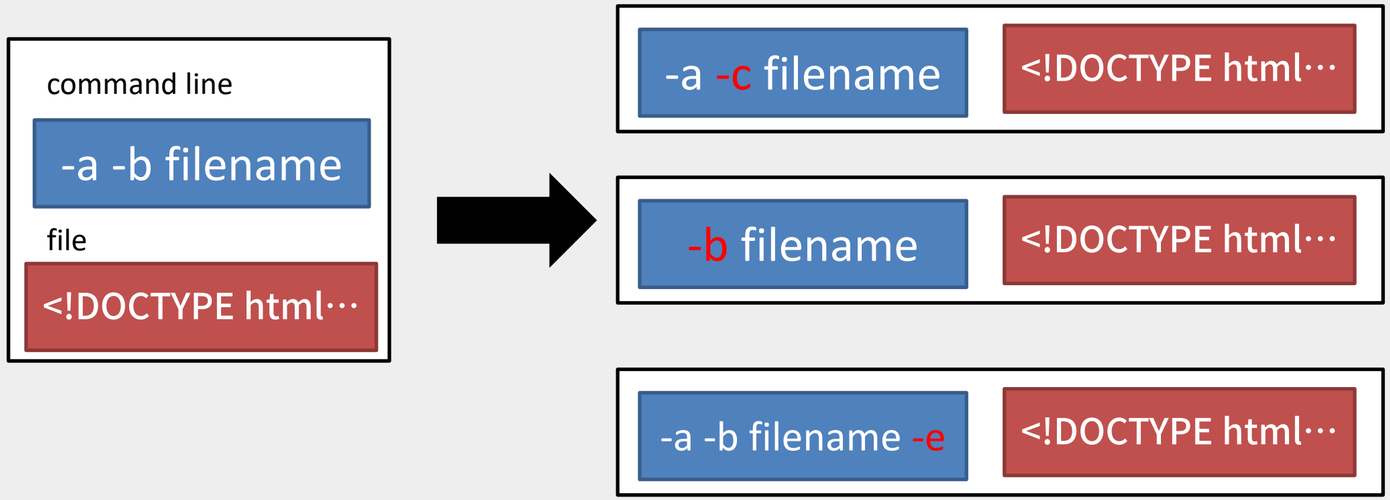
2. 서로 다른 프로그램 옵션 선별
   비슷한 프로그램 옵션에 시간 낭비를 줄이고 효율적으로 변이

전체 프로세스 1 - 커맨드 라인 변이

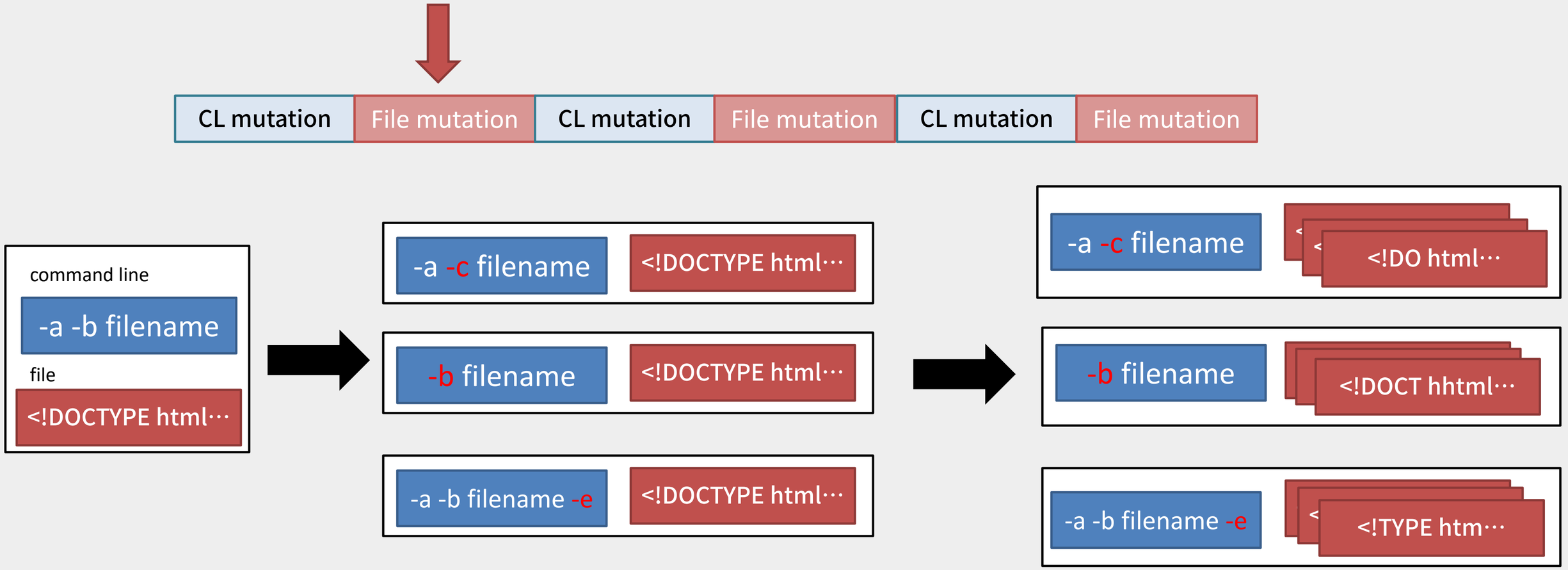


전체 프로세스 1 - 커맨드 라인 변이

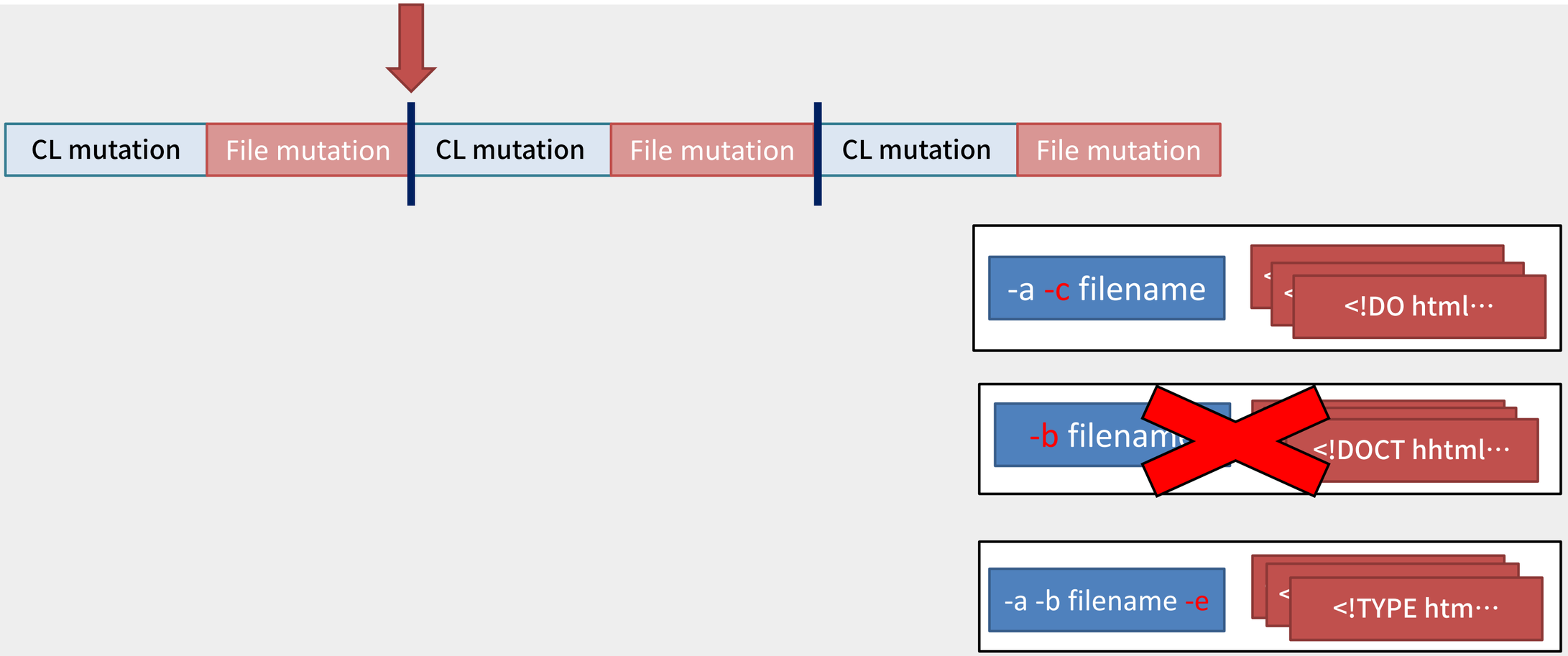




전체 프로세스 2 - 파일 변이



전체 프로세스 3 - 비슷한 프로그램 옵션 선별/제외



같이 변이하지 않고 따로 변이하는 이유 - 1

기존 프로그램 옵션/파일 변이 방식

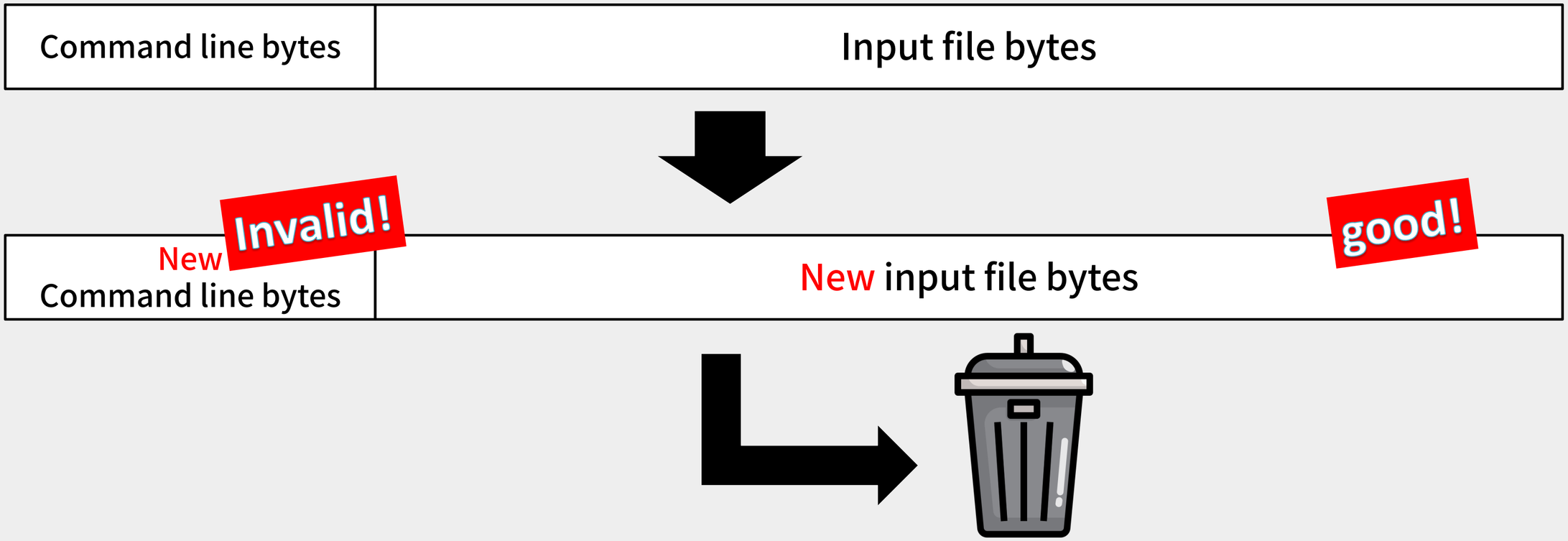
command line	input file
-a -b -c -opt -s	<!DOCTYPE html><!-- saved from url=https://www. / --><html

동시에, 같이 변이

-a -e -format -opt -s	<!DOCTYPE html><!-- saved asasdfsdfsdfs://www. / --><html

같이 변이하지 않고 따로 변이하는 이유 - 1

옵션/파일 둘 중 하나를 잘못 건드리는 경우, 둘 다 버려진다.



같이 변이하지 않고 따로 변이하는 이유 - 2

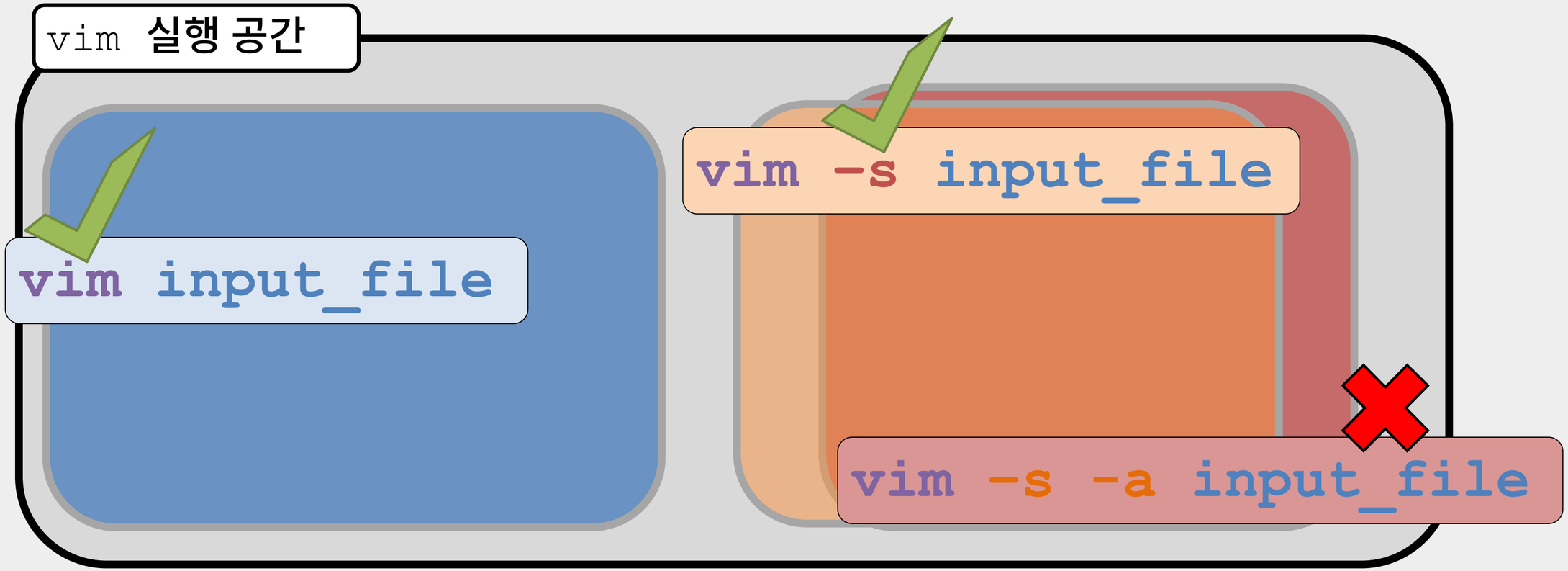
옵션/파일을 동시에 변이하면, 보다 깊게 도달하는 입력 생성이 어려움.

```
02: if(process_args(argc,argv,&glflags)==SUCCESS){ P
03:  if(open_detect_dwarf_obj(fname,&ftype)==SUCCESS){ F
      ...
04:   if(ftype == DW_FTYPE_ELF) { F
05:    if(!(glflags.gf_1 || glflags.gf_2)) { P
        ...
06:     /* function: process_one_file */
07:     if(dwarf_init_path_dl(fname, &dobj)==SUCCESS){ F
         ...
08:      /* function: print_frames */
09:      if(glflags.gf_eh_frame_flag) { P
10:       if(dwarf_get_frame(dobj, ...) == SUCCESS){ F
```

P 프로그램 옵션에 따라 결정되는 분기

F 파일 내용에 따라 결정되는 분기

서로 다른 옵션 선별 및 선택



서로 다른 옵션 선별 및 선택 - 1

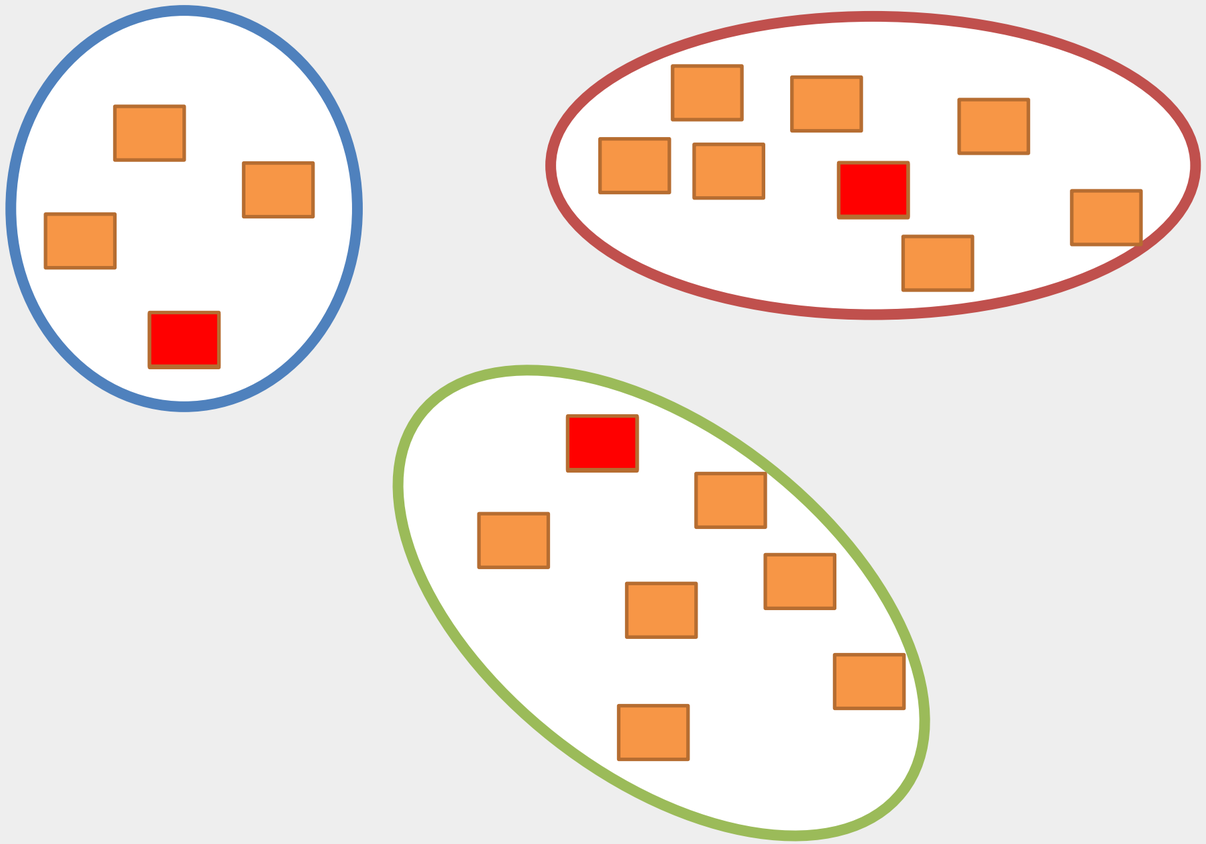
1. 함수 호출 정보 추출

CL1 → main, f1, f2, g1, g2

CL2 → main, g1, h1, h2

서로 다른 옵션 선별 및 선택 - 2

2. Clustering (K-means)



$$\text{Distance} = 1 - \frac{|A \cap B|}{|A \cup B|}$$

평가

⭐ 다른 최신 기법들에 비해
더 높은 분기 커버리지를 달성하고,
더 많은 크래시 오류를 탐지했는가?

12시간 동안 테스트 생성 수행 후, 커버리지 및 오류 개수를 산출

테스트 대상 프로그램

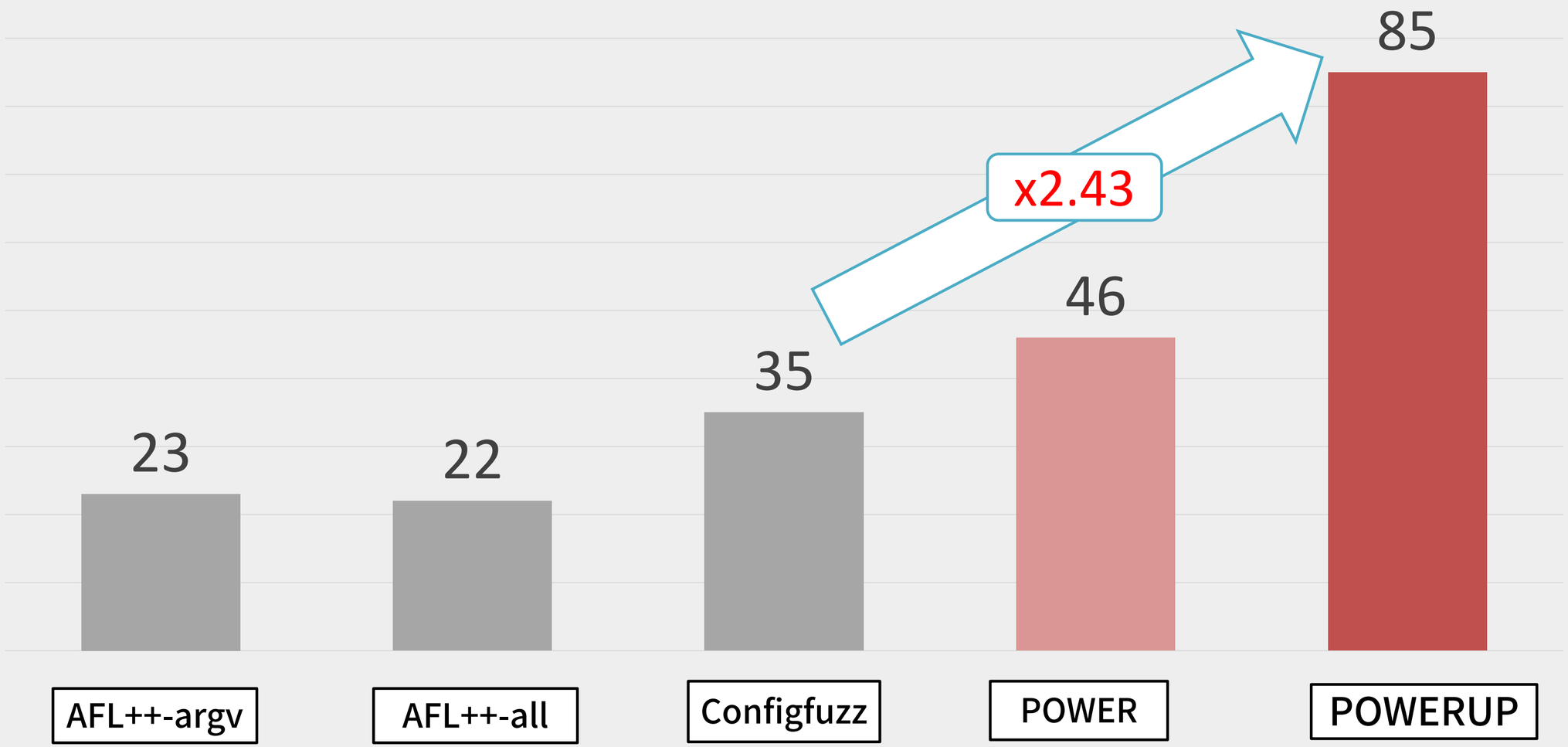
20 C/C++ 실제 오픈 소스 프로그램 (최신 버전)을 대상으로 테스트 생성 수행

프로그램	크기 (Loc)	CLI 키워드 개수	프로그램	크기 (Loc)	CLI 키워드 개수
avconv	454,936	761	nasm	70,903	218
bison	54,423	51	objdump	877,165	84
cjpeg	6,308	33	pdftohtml	38,111	26
dwarfdump	83,545	103	pdftopng	97,890	18
exiv2	33,417	76	pspp	4,901	20
ffmpeg	774,186	1817	readelf	74,789	98
gm	197,891	757	tiff2pdf	8,234	30
gs	1,174,673	350	tiff2ps	5,646	34
jasper	2,920	20	xmllint	11,285	66
mpg123	11,298	122	xmlwf	4,147	15

평균 LoC : 199,333

키워드 개수 평균 : 235
키워드 개수 중간값 : 71

⭐ 결과 - 탐지한 크래시 오류 개수



⭐ 결과 - 달성한 분기 커버리지