```
1
```

```
int main(int argc, char *argv[]){
  if(argc != 2) | B0
                    B1
     return -1; B11
  int a:
                                      B2
  int b;
  FILE *fp = fopen(argv[1], "r");
  if (fp == NULL) {
     printf("Failed to open file\n");
     return 1; B11
  }
  if (fscanf(fp, "%d %d", &a, &b) != 2) {
    printTimeAndStr(88, 88, true, "two ints!");
    return -2; B11
  }else{
     fclose(fp);
  printTimeAndInt("aaaa", a);
                                               В7
  printTimeAndInt("bbbbb", b);
  printf("Two input ints: %d 和 %d\n", a, b);
  printTimeAndStr(a, b, true, "main start");
  if(a==5){
     printTimeAndStr(a, b, true, "a==5\n\n"); | B8
     redundant(a,b,a);
      printTimeAndStr(a, b, true, "a!=5\n\n"); | B9
     testswitch(a,b,b);
     printTimeAndStr(a, b, true, "enda!=5\n");
  printAfterTestSwitch(a);
  return 0;
```

```
B12
void testswitch(int a, int b, int bb){
  printTimeAndStr(a, b, true, "func switch begin\n");
  switch(bb){
     case 1:
                                                                 B14
       assert(0);
       func_target_one(a);
       printTimeAndStr(a, b, true, "switch b1\n\n");
       break;
     case 5:
                                                                 B15
        printTimeAndStr(a, b, true, "switch b5\n\n");
       func_target(a);
       break;
     case 7:
       func_target_seven(a);
                                                                 B16
       printTimeAndStr(a, b, true, "switch b7\n\n");
       break;
     default:
       func_target_default(a);
                                                                 B13
       printTimeAndStr(a, b, true, "sw default\n");
       break;
  func_target_end(a);
                                     B17
```

Fig. 1. An example for illustrating the differences between our proposal of redundant basic block termination (rbbt for short), BEACON and SIEVEFUZZ. It contains the source codes with annotations of basic blocks and optimization results of two functions with the above three proposa. Bi (i=0, 1, 2, ..., 17) denotes a basic block. The function main is the entry of the program and the function testswitch contains the basic block as a target location. \times denotes the termination of the execution of a redundant basic block.

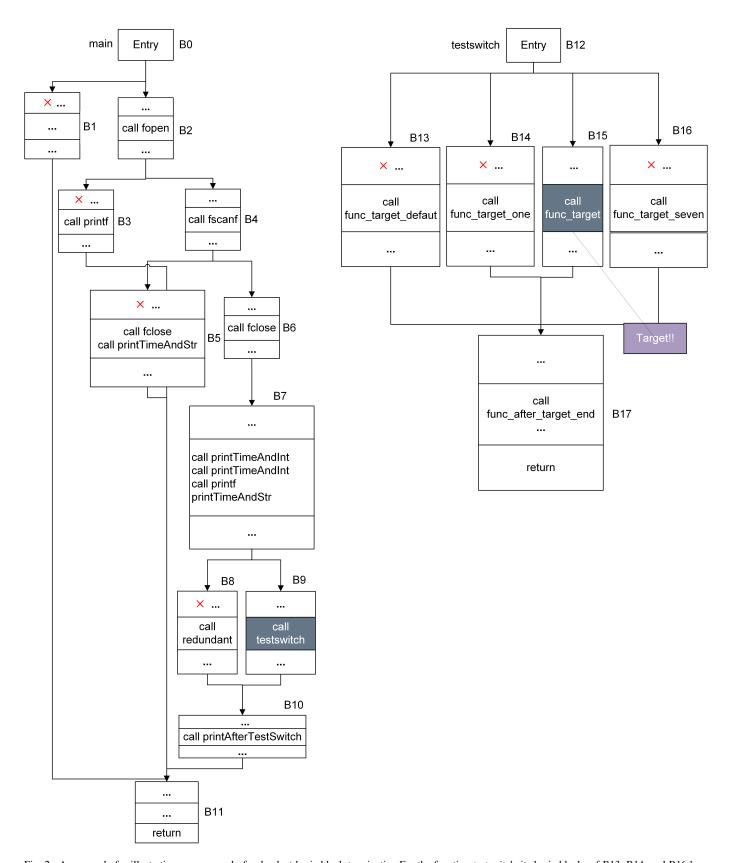
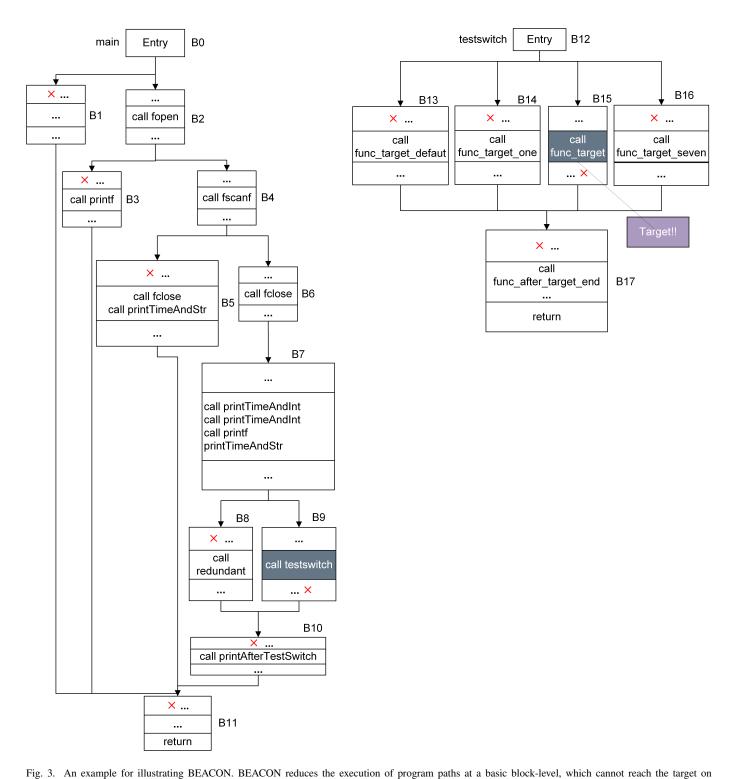


Fig. 2. An example for illustrating our proposal of redundant basic block termination. For the function *testswitch*, its basic blocks of B13, B14, and B16 have no connects to B15 where the target function *func_target* is called. Therefore, these basic blocks would be identified as redundant basic blocks of *testswitch* and would be instrumented with exit instructions to terminate its execution. Similarly, the basic blocks of B1, B3, B5, and B8 would be identified as redundant for *main*. × denotes the termination of the execution of a redundant basic block.



the control flow or satisfy the conditional constraints. However, with closed source code, BEACON is provided as an executable binary adapting only for Clang with the version of 4.0, which limits its **generality and availability** for future research. Another difference from our proposal of redundant basic block termination is to **terminate all of the paths after the basic blocks where its parent function calls the target-related functions**. This over-pruning strategy will hindering triggering bugs around the targets. × denotes the termination of the execution of a redundant basic block.

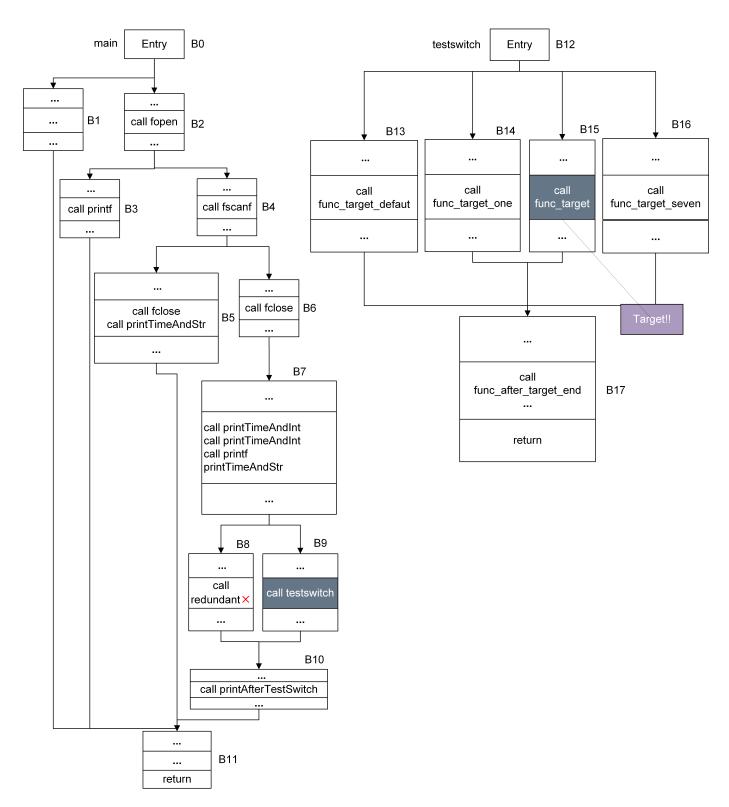


Fig. 4. An example for illustrating SIEVEFUZZ. SIEVEFUZZ preemptively terminates the execution of the functions unrelated to target functions. Because it works at a function level, it terminates much less basic blocks than our proposal of rbbt. × denotes the termination of the execution of a target-unrelated function. Actually it only terminates the execution of the function named redundant in our example.