迎新报告

刘力铭

研究内容

C 代码风格检查器——Crulet

```c
void static_p(int a){
    if(a == 1)
        a++;
}
```

GJB_8_1_2.c

```
GJB_8_1_2.c:1:6: warning: [GJB-9.1.1] 函数必须有返回语句
void static_p(int a){
     ^
GJB_8_1_2.c:1:19: remark: [GJB-1.2.1] 推荐在同一文件中对基本类型进行typedef
void static_p(int a){
                  ^
GJB_8_1_2.c:3:9: warning: [GJB-2.1.3] then/else中的语句必须用大括号括起来
        a++;
        ^
2 warnings generated.
```

C 代码符号执行工具——Canalyze

```
1 int main()
2 {
3     int *p = 0;
4     return *p;
5 }
```

test.c

```
1. int main()
   1. Start Analysis.
2. {
3.     int *p = 0;
4.     return *p;
   2. The pointer is NULL.    *p
5. }
6.
```

C++ 代码符号执行工具——Canalyze++

```
1 int main()
2 {
3     int *p = 0;
4     return *p;
5 }
```

test.c

```
1.  int main()
    1. Start Analysis.
2.  {
3.      int *p = 0;
4.      return *p;
    2. The pointer is NULL.    *p
5.  }
6.
```

关键字指导的灰盒模糊测试

- 第三作者
  - 参与设计关键字提取算法
  - 实现候选关键字提取工具

异常处理可达性分析

- 进行中
  - 针对 C++ 异常处理机制
  - 分析异常处理的基本块可达性

自我感悟

感悟

科研不易

勉励告诫

告诫

- 从入学时就应开始寻找毕业课题
- 做工具和发论文是两条不同的路