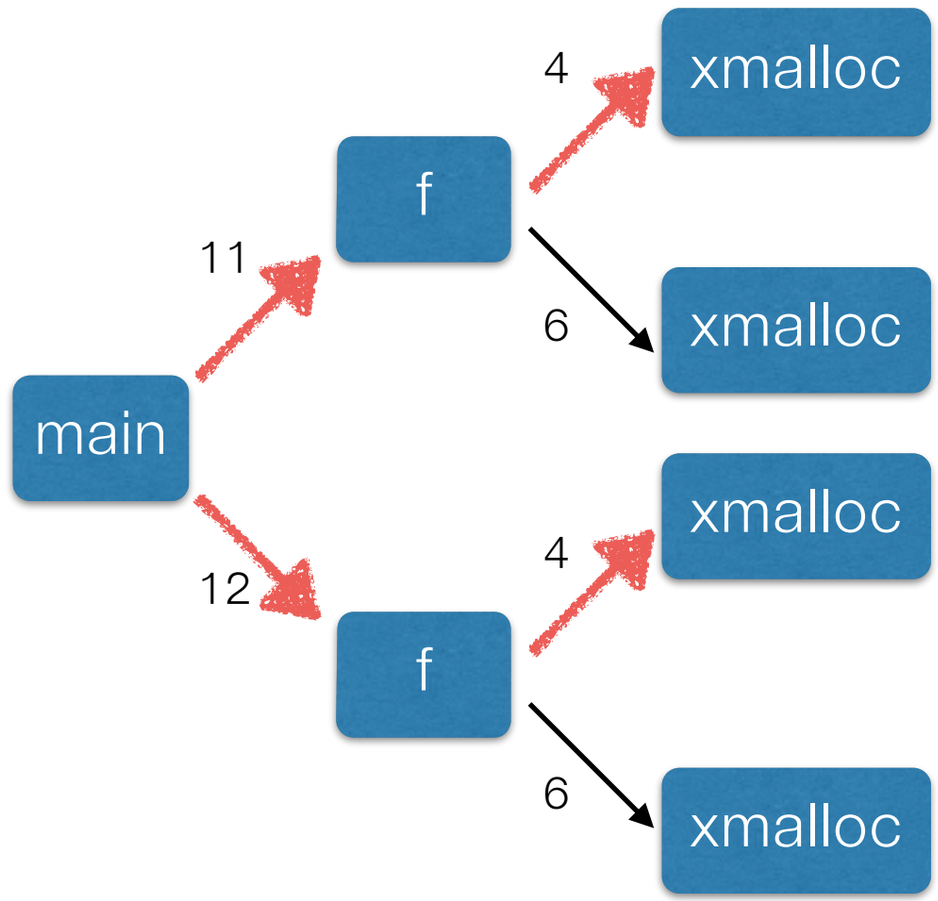
선별적으로
문맥을 구분하고 변수를 관계 짓는
프로그램 분석

허기홍 오학주
서울대학교 프로그래밍 연구실
ROSAEC 워크샵
2014.1.14

선별적 문맥 구분

- 문맥 구분의 효과를 가늠하는 전분석으로

```
1  char* xmalloc (int n) { return malloc(n); }
2
3  void f (int size) {
4    p = xmalloc (size);
5    assert (sizeof(p) > 1);      // Query 1
6    q = xmalloc (input());
7    assert (sizeof(q) > 1);      // Query 2
8  }
9
10 int main() {
11   f (8);
12   f (16);
13 }
```



4·11 4·12 ϵ

선별적 관계 분석

- 관계 분석의 효과를 가늠하는 전분석으로

```
1 int a = b;
2 int c = input();              // User input
3 for (i = 0; i < b; i++) {
4   assert (i < a);             // Query 1
5   assert (i < c);             // Query 2
6 }
```

b - a <= ★

i - b <= ★

i - a <= ★

c - b <= T

i - c <= T

...

{a, b, i} {c}

문제

- 관계과 문맥이 동시에 필요한 경우

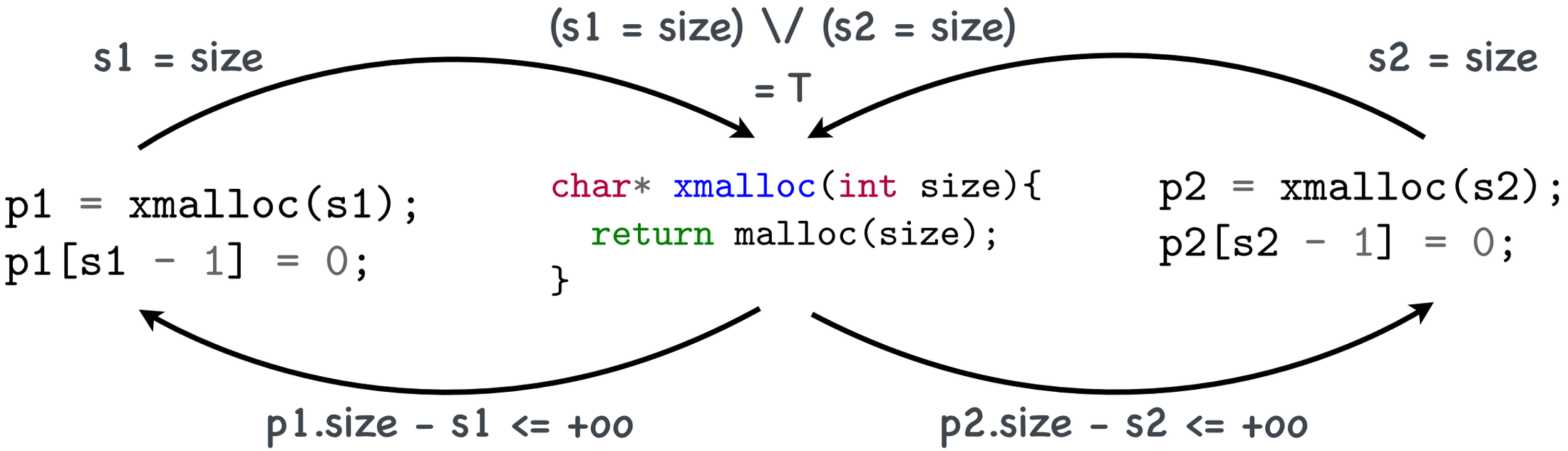
```
p1 = xmalloc(s1);
p1[s1 - 1] = 0;
```

```
char* xmalloc(int size){
  return malloc(size);
}
```

```
p2 = xmalloc(s2);
p2[s2 - 1] = 0;
```

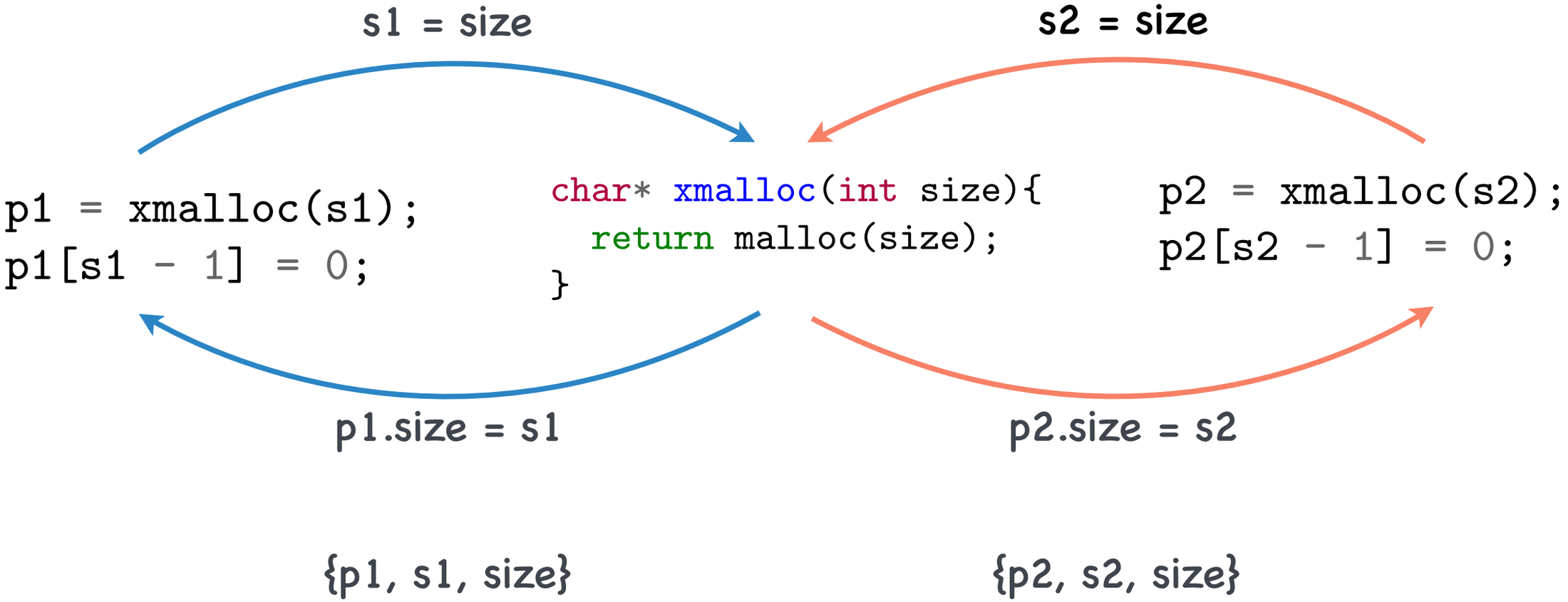
문제

- 관계과 문맥이 동시에 필요한 경우



해결책

- 선별적으로 문맥을 구분하고 변수를 관계 짓는 분석
  - 관계와 문맥 구분의 효과를 같이 가능하는 전분석



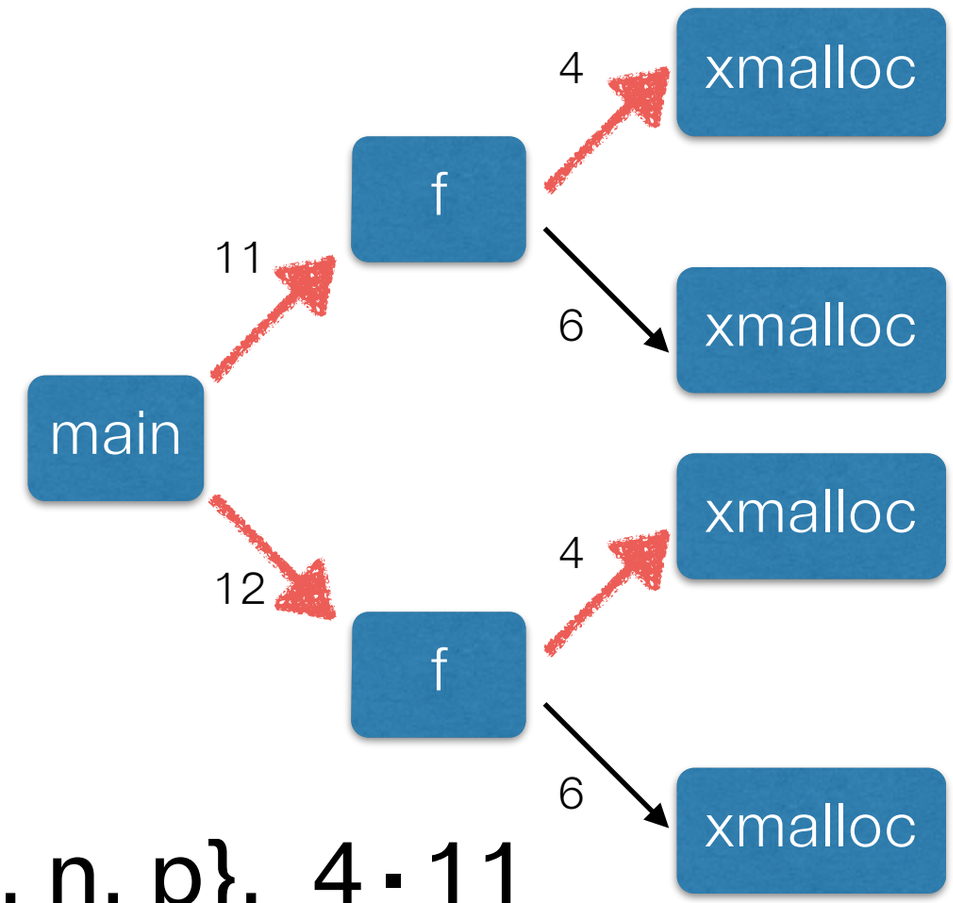
해결책

- 전체 변수의 관계와 모든 문맥을 구분하는 전분석
  - 값 도메인은 본분석보다 훨씬 요약
- 전분석 결과를 토대로 정확도 향상이 있을 부분 선정
- 정확도 향상을 위해 필요한 문맥과 변수 관계 추출

전분석

- 관계와 문맥 구분의 효과를 같이 가능

```
1   char* xmalloc (int n) { return malloc(n); }
2
3   void f (int size) {
4     p = xmalloc (size);
5     p[size - 1] = 0;      // Query 1
6     q = xmalloc (input());
7     q[size - 1] = 0;      // Query 2
8   }
9
10  int main() {
11    f (s1);
12    f (s2);
13  }
```



Query1 : {s1, size, n, p}, 4·11

Query2 : {s2, size, n, p}, 4·12

실험 결과

Pgm	LOC	Q	구문 기반 패킹 방식		선별적 문맥&관계 분석				비교	
			증명	시간	증명	전분석	본분석	합계	정확도↑	시간↓
spell-1.0	2,213	16	1	4.8	16	1.5	1.6	3.1	15	35.4%
httptunnel-3.3	6,174	28	16	26.0	26	12.3	5.5	17.8	10	31.5%
bc-1.06	13,093	10	2	247.1	10	69.2	34.8	104	8	57.9%
tar-1.17	20,258	17	7	1043.2	17	69.3	191.1	260.4	10	75.0%
종합		71	26	1321.1	69	152.3	233	385.3	43	70.8%

상향식 분석

- 각 함수별로 입출력 관계를 기록, 함수 호출시 사용

```
char* xmalloc(int size){
  return malloc(size);
}
```

Summary of xmalloc:

size - xmalloc.ret <= ★

```
1: p1 = xmalloc(s1);
   p1[s1 - 1] = 0;
```

s1 - size <= ★

size - xmalloc1.ret <= ★

xmalloc1.ret - p1 <= ★

s1 - p1 <= ★

```
2: p2 = xmalloc(s2);
   p2[s2 - 1] = 0;
```

s2 - size <= ★

size - xmalloc2.ret <= ★

xmalloc2.ret - p2 <= ★

s2 - p2 <= ★

정리

- 문맥 구분과 변수 관계를 모두 추적하기 위한 전분석 설계
  - 효율적인 상향식 전분석 (전, 후방) 고안
- 포스터 : 선별적으로 정확도를 높이는 분석
  - 문맥, 관계, 문맥&관계 등

고맙습니다