TEAM PRESENTATION #2

-CONTROL FLOW GRAPH

TEAM [T2]

200811415 김영현

200811455 정용겸

200811457 조성우

발표자 → 200811465 허준행

팀 프로젝트 내용

- **SASD**를 이용하여, 다음의 프로그램을 개발한다.

- 개발할 프로그램
  - 입력 : C 프로그램
  - 출력 : CFG (Control Flow Graph)
  - 내용 : 입력 받은 C 프로그램을 CFG 로 변환하여 효과적으로 출력한다.

KU KONKUK UNIVERSITY

CFG에 대한 소개

KU KONKUK UNIVERSITY

CFG를 그리는 알고리즘

Statement of purpose

and now, What to do

프리젠테이션 목표

1. CFG가 무엇인지 이해하고
2. CFG를 그리는 방법을 습득한 뒤
3. SASD기법을 적용하여 프로그램을 개발한다

CFG에 대한 소개

KU KONKUK UNIVERSITY

Control Flow Analysis

- 프로그램의 제어 흐름(일련의 명령의 실행)을 이용하는 정적 코드 분석 기술 중 하나이다.

- CFA는 프로그램을 실행시키지 않고 소프트웨어의 성능을 평가할 수 있으며, 이를 시각적으로 표현하기 위해서 CFG를 사용하게 된다.

Control Flow Graph – 1. 정의

- 소프트웨어 모듈의 논리구조를 그래프로 표기
- Block과 Edge로 이루어져 있음
- 프로그램 실행 동안 가능한 모든 경로를 포함
- 개별 함수에 대한 내부적인 제어 흐름을 표현
- 컴파일러 최적화와 정적 분석에 사용

Control Flow Graph – 2. 목적

- 프로그램 중에 불필요한 부분이 있는지 없는지 발견할 수 있음
- 단일 block으로부터 프로그램 실행이 빠져나가지 않는 일종의 무한 루프와 같은 문제들을 해결하는 데 도움이 됨
- 프로그램의 어떤 영역이 다른 부분과 의존 관계를 보여주는 종속 그래프 생성에 도움이 됨

Control Flow Graph – 3. 용어

- ***Entry block*** : 모든 제어 흐름이 그래프로 진입하기 위해 통과하는 block
- ***Exit block*** : 모든 제어 흐름이 그래프를 떠나기 위해 통과하는 block
- ***Reachability*** : block 또는 subgraph와 entry block을 포함하는 다른 subgraph와의 연결 관계

Control Flow Graph – 3. 용어

- ***Dominator*** : entry로부터의 모든 경로가 block N에 도달하기 위해 block M을 통과해야 하는 경우, block M은 block N의 dominator이다

- ***Post-dominator*** : block N으로부터의 모든 경로가 그래프를 떠나기 위해 block M을 통과해야 하는 경우, block M은 block N의 post-dominator이다

- ***Loop header*** : loop body내의 모든 block을 dominate하는 entry point

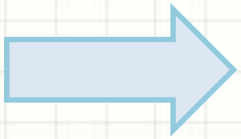
Control Flow Graph – 3. 용어

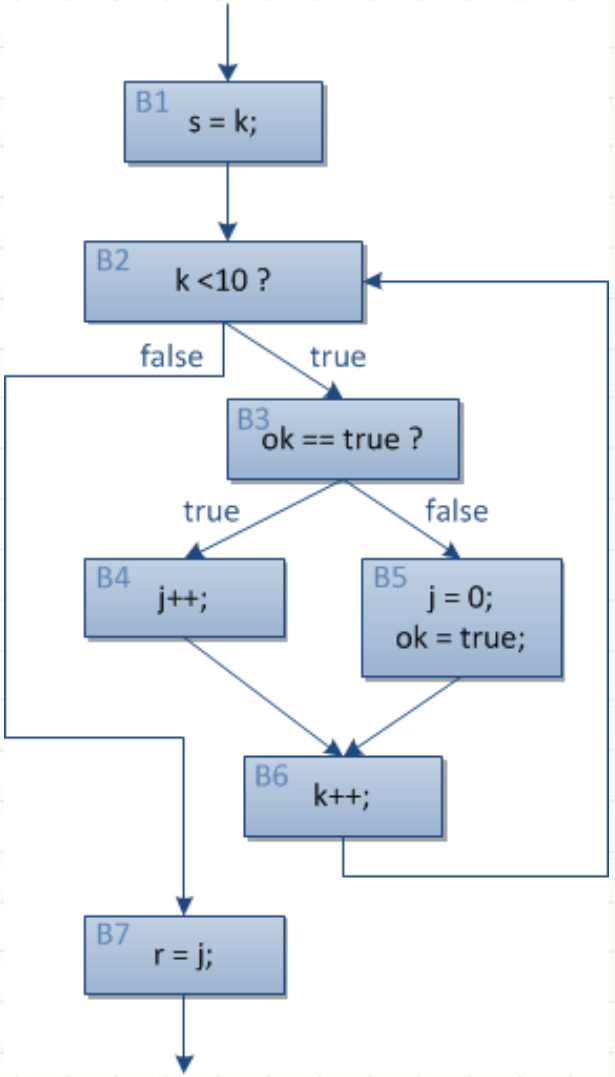
- ***Back Edge*** : loop를 구성하는 edge
- ***Abnormal Edge*** : 프로그램의 예외처리(Exception handling)를 위한 edge
- ***Impossible Edge*** : exit block의 post-dominating property를 유지하기 위한 edge
- ***Critical Edge*** : 단독으로 source block 또는 destination block에 연결되지 않는 edge

Control Flow Graph – 4. 예제

```
s = k ;

while(k < 10) {
        if(ok)
                j++ ;
        else {
                j = 0 ;
                ok = true ;
        }
        k++ ;
}
r = j ;
```





CFG를 그리는 알고리즘

KU KONKUK UNIVERSITY

기본 아이디어

- 입력 프로그램의 leader를 찾는다.

- 명령어를 읽어서 parsing할 때,
  - 프로그램 제어문(분기, 함수 호출, 함수 리턴)이 아니면 basic block으로 node를 형성한다.

  - 프로그램 제어문이면 연결리스트를 사용함으로써 각 node간의 연결성을 알 수 있도록 edge를 사용한다.

알고리즘의 종류

- Positioning Algorithms
  - BFS(Breath First Search) Positioning
  - Loop Positioning
  - Hierarchical Positioning

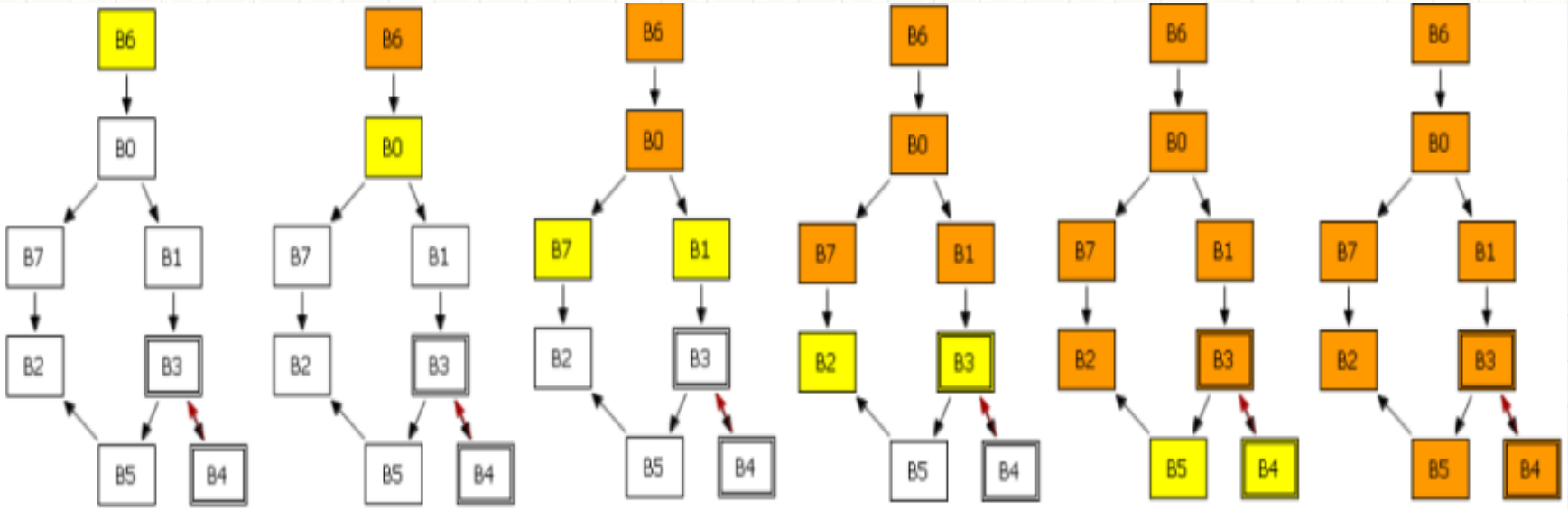
모든 block의 배치를 결정하는 알고리즘

- Routing Algorithms
  - Bezier Routing
  - Manhatten Routing

block들을 연결하는 edge를 그리는 알고리즘

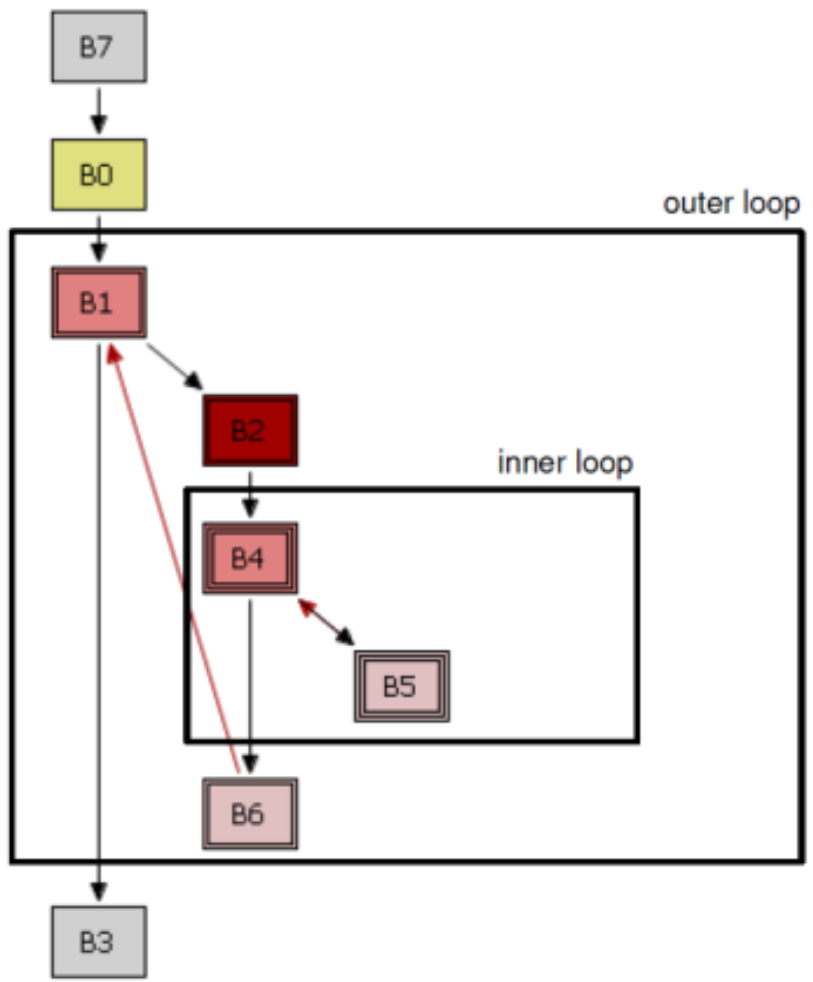
알고리즘의 종류 (cont.)

- Breath First Search Positioning
  - 특정한 edge는 고려하지 않고 block들을 트리 구조로 배치한 알고리즘
  - 가독성은 좋지만, 복잡한 프로그램엔 부적합



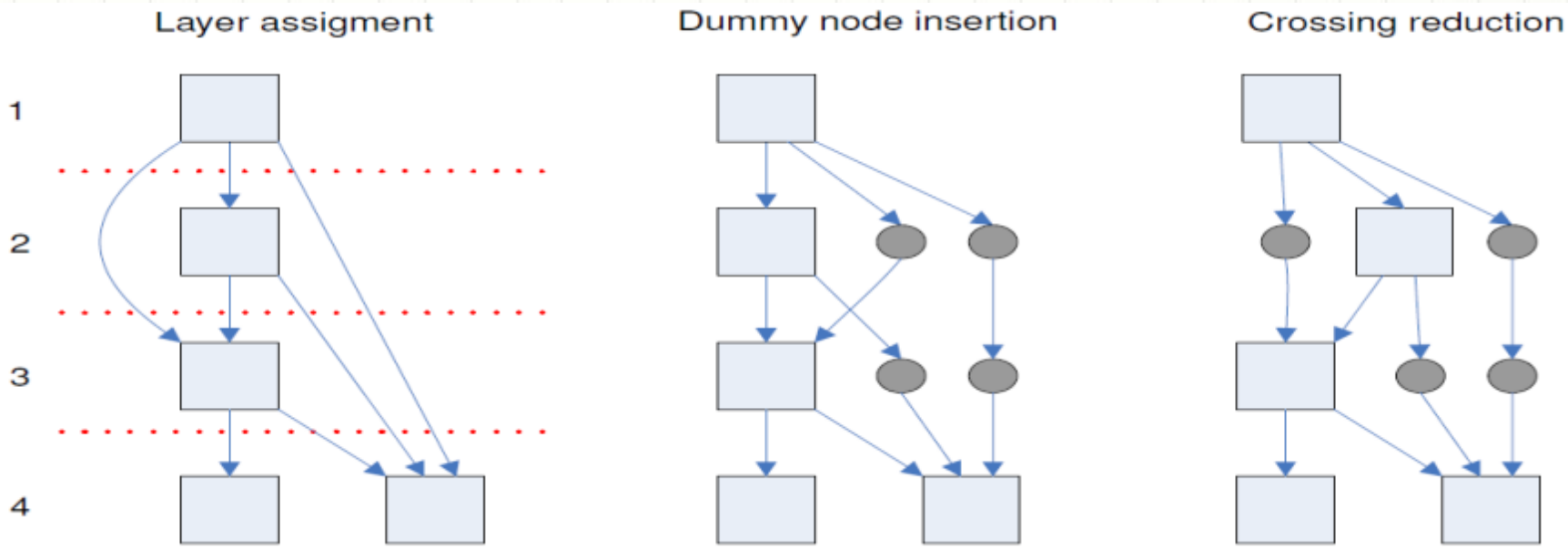
알고리즘의 종류 (cont.)

- Loop Positioning
  - loop를 조금 더 분리되도록 만드는 알고리즘
  - loop들을 그룹 지어 inner loop 부분과 outer loop 부분으로 나누어 생각
  - 그래프를 실제 코드와 유사하게 보이도록 만들 수 있다



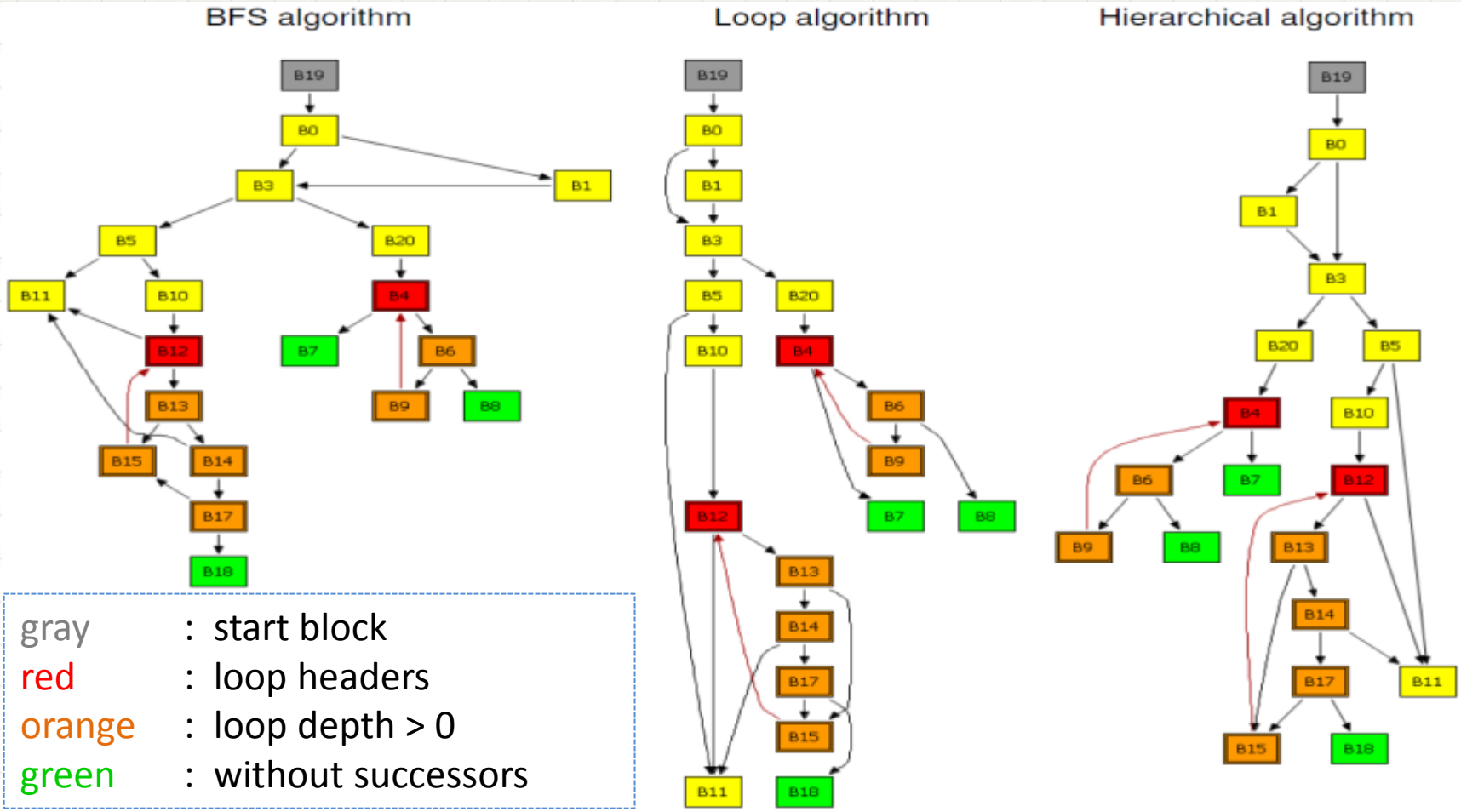
알고리즘의 종류 (cont.)

- Hierarchical Positioning
  - 특별한 control flow에 대한 정보 없이도 구체적인 CFG를 그릴 수 있는 알고리즘
  - 관련성 있는 loop들이 분산되기 때문에 loop 구조를 분석하는데 부적합



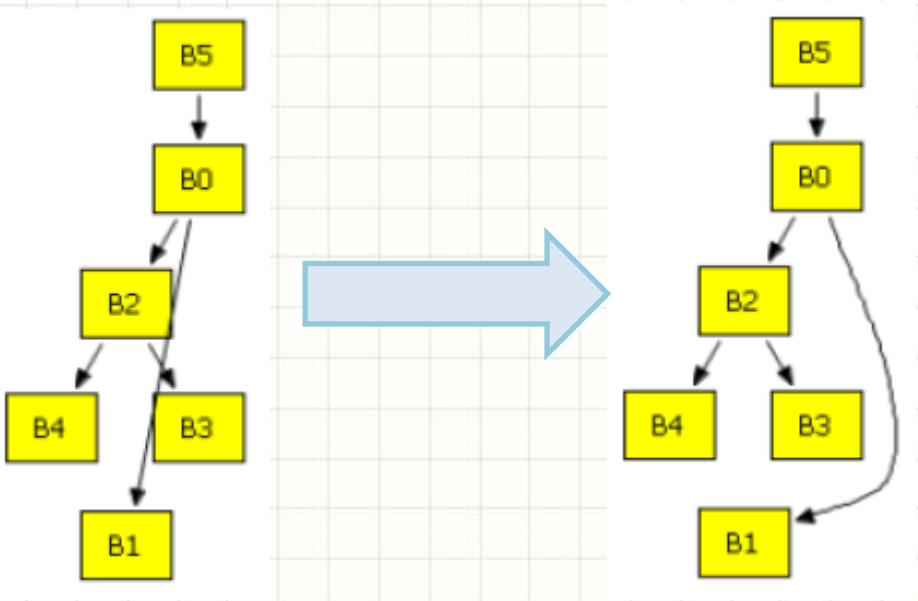
알고리즘의 종류 (cont.)

- Comparison of three Positioning algorithms



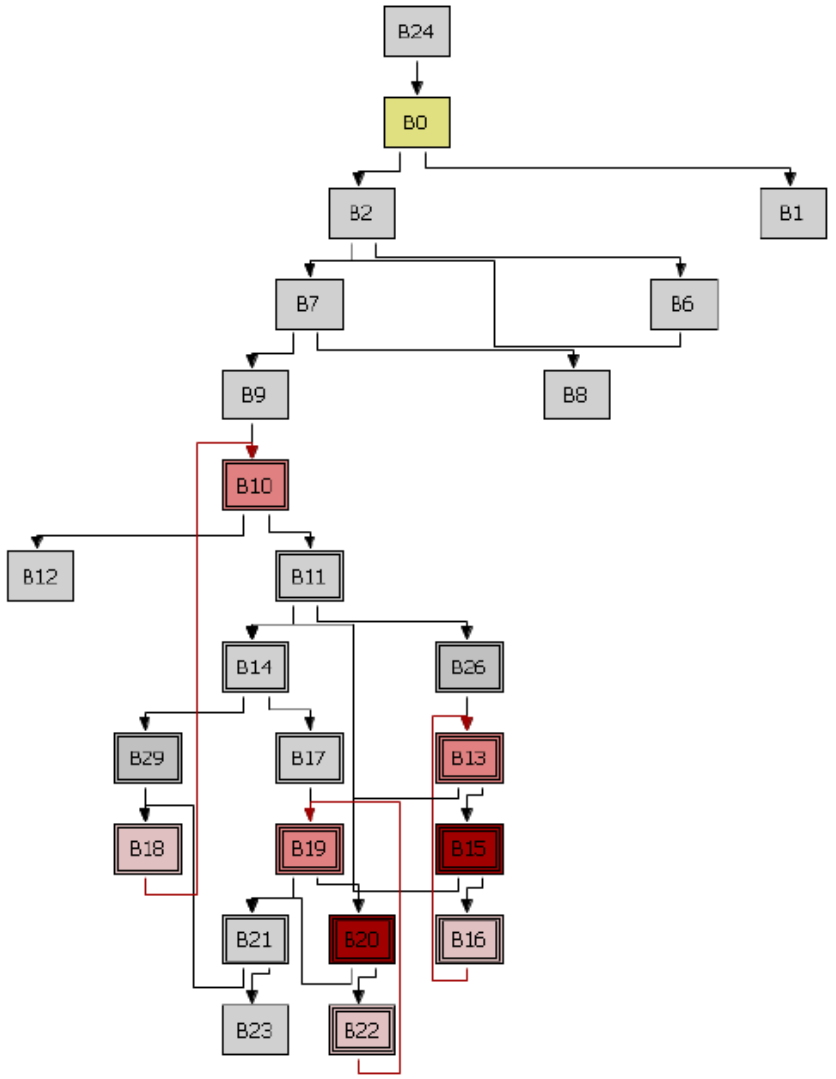
알고리즘의 종류 (cont.)

- Bezier Routing
  - 종이 위에 사람이 직접 그리듯이 연결을 그리는 기법
  - Block 사이를 최단 경로로 연결한 뒤, 조건에 맞게 수정하여 최종 곡선 경로를 표현



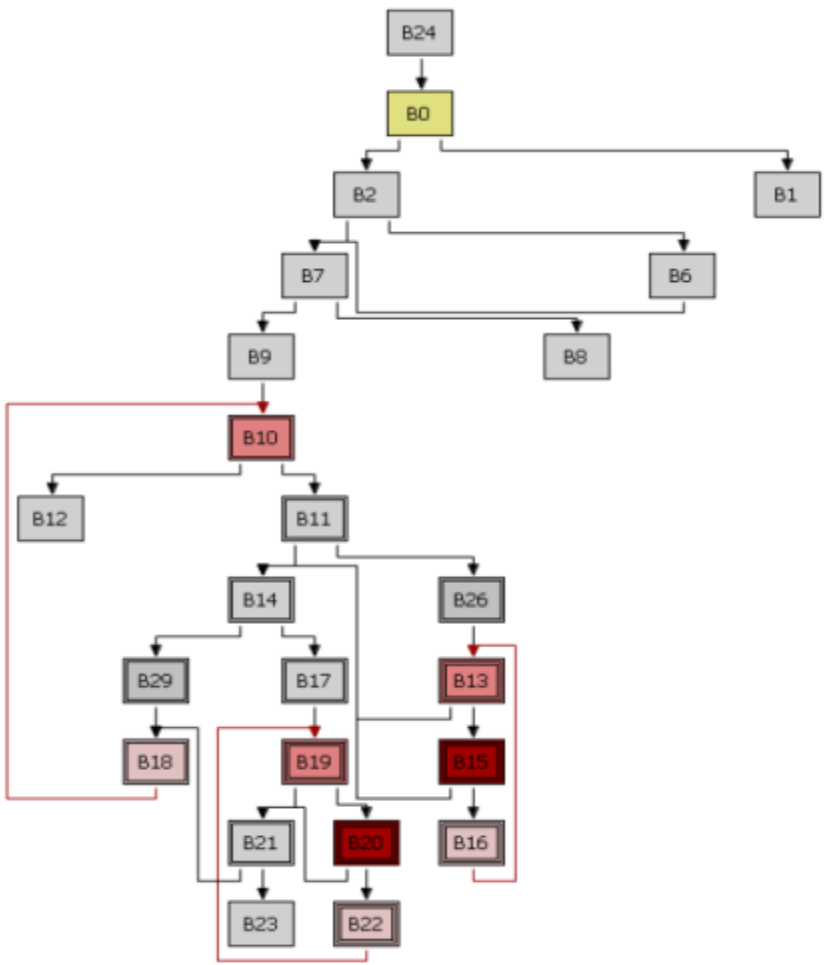
알고리즘의 종류 (cont.)

- Manhatten Routing
  - CFG를 그리는 화면을 좌표계로 생각
  - 모든 경로를 좌표로 구성하여 직각으로 표현하는 기법
  - 경로는 block의 아래에서 출발하여 block의 위에 도착

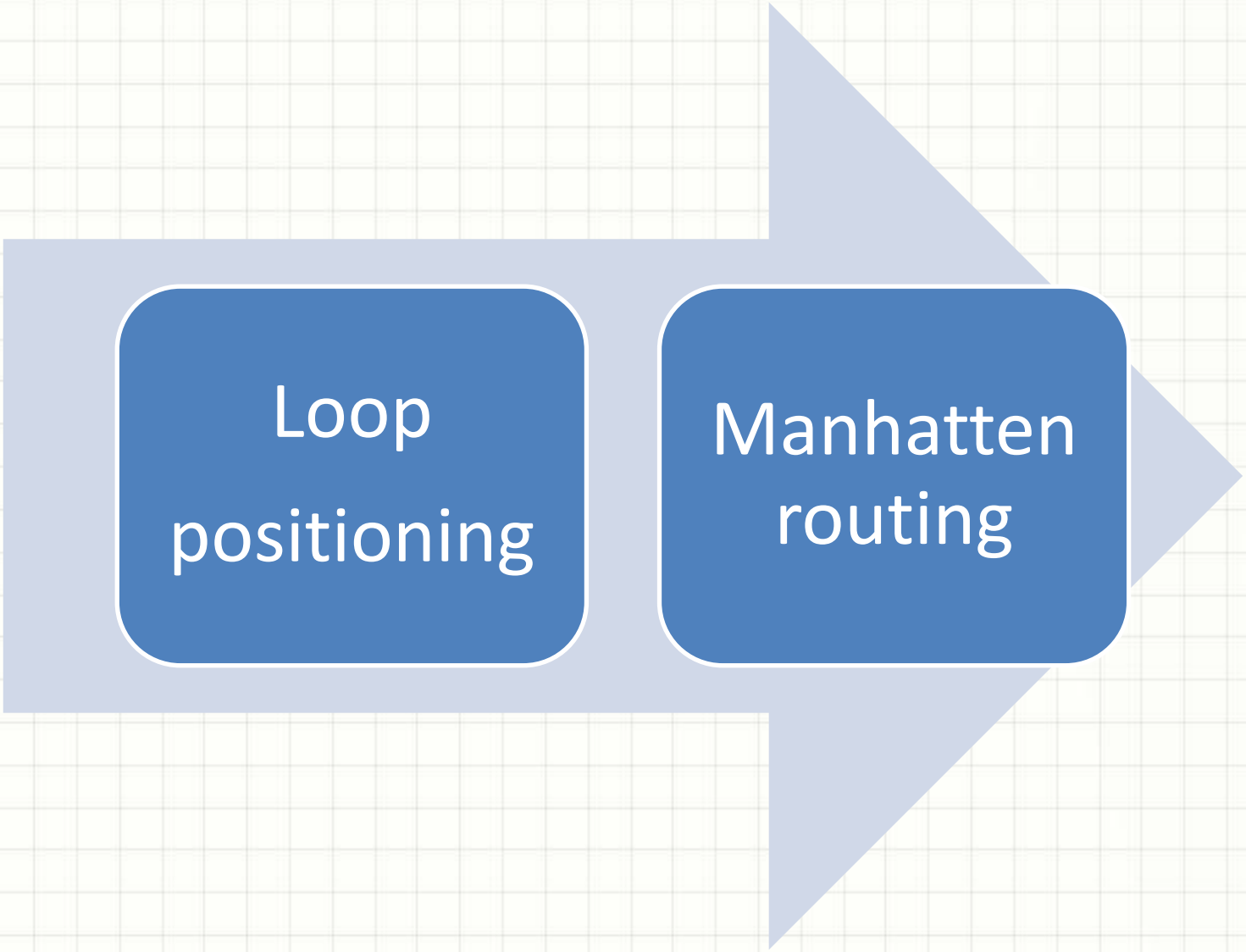


알고리즘의 종류 (cont.)

- Comparison of two Routing algorithms



선택한 알고리즘



선택한 알고리즘 (Cont.)

- 프로그램의 오류 중 상당 부분은 잘못된 loop구조로 인해 발생
- 프로그램 분석에서 loop구조의 분석은 다른 프로그램 구성요소의 분석보다 우선시 되어야 함
- 따라서, loop 분석에 용이한 ***loop positioning*** algorithm을 사용하여 CFG의 block을 배치

선택한 알고리즘 (Cont.)

- block사이의 edge를 좌표를 이용해 표현할 경우, 다른 기법보다 기계적 연산에 유리
- 한 개의 block으로 들어오는 edge들의 end point를 동일하게 설정하여 모호성을 최소화
- 따라서, ***manhatten routing*** algorithm을 사용하여 block사이의 edge를 표현하기로 결정

STATEMENT OF PURPOSE

KU KONKUK UNIVERSITY

Statement of Purpose

- C 프로그램의 소스코드를 입력 받아 콘솔 창에 CFG를 출력한다.
- 제어문을 제외한 소스코드를 line 단위의 basic block으로 parsing한다.
- parsing된 block들을 loop positioning algorithm으로 배치한다.
- 제어문을 block사이의 관계를 표현하는 edge로 parsing한다.
- parsing된 edge들을 manhatten routing 기법으로 출력한다.

QUESTIONS ?

KU KONKUK UNIVERSITY