MUNI
FI

# Mornfall’s Divine tool and me

Abstract representation in interval domain

Pavol Mišenko

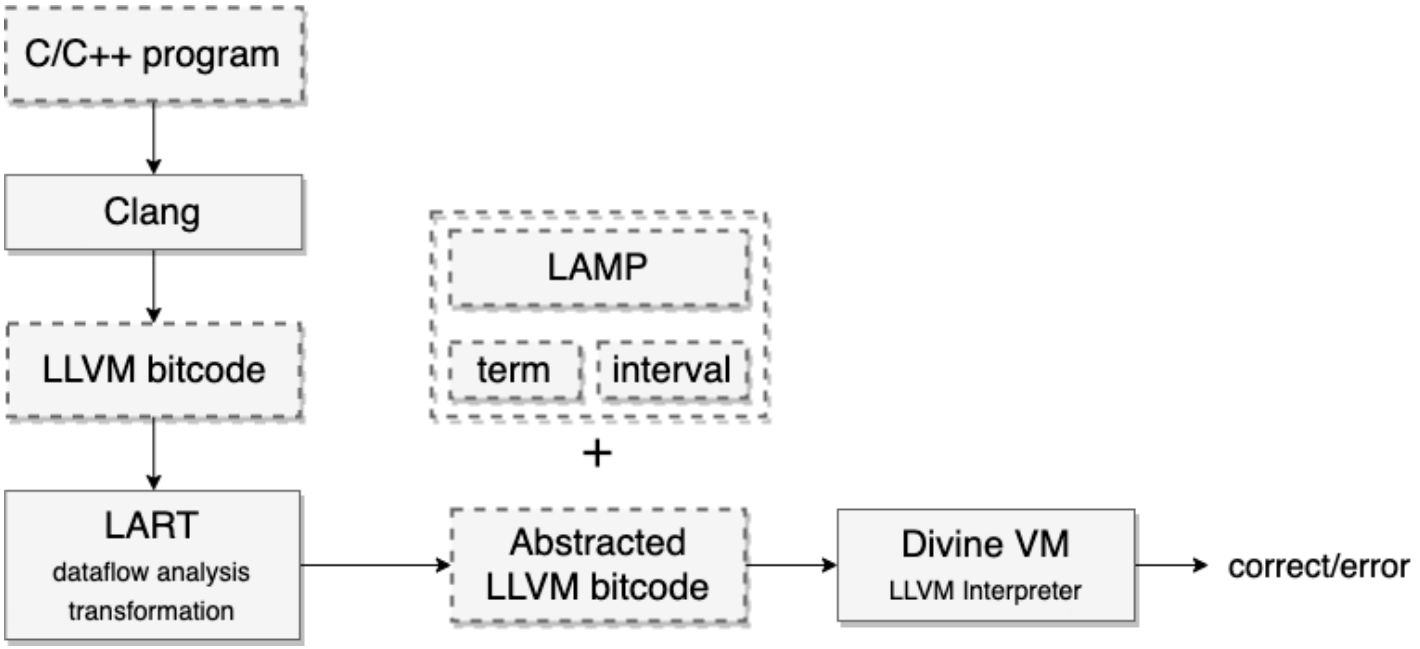
# Quick recap

How to deal with nondeterminism?

- Consider all possible options
- Symbolic representation
- Abstract domain representation
  - Unit domain
  - Zero domain
  - Sign domain
  - Interval domain

MUNI
FI

# Analysis workflow




MUNI
FI

# Problems to solve with interval domain

1. Domain representation
   - Value representation `[3, 5] ∽ {3,4,5}`
   - Operations `[3, 5] + [1, 2] = [4, 7] ∽ {4, 5, 6, 7}`
2. Nondeterministic control flow
3. Branch constraint propagation

```
i = [ 4, 8 ]
if i < 6:
    ...      i = [ 4, 5 ]
else
    ...      i = [ 6, 8 ]
```

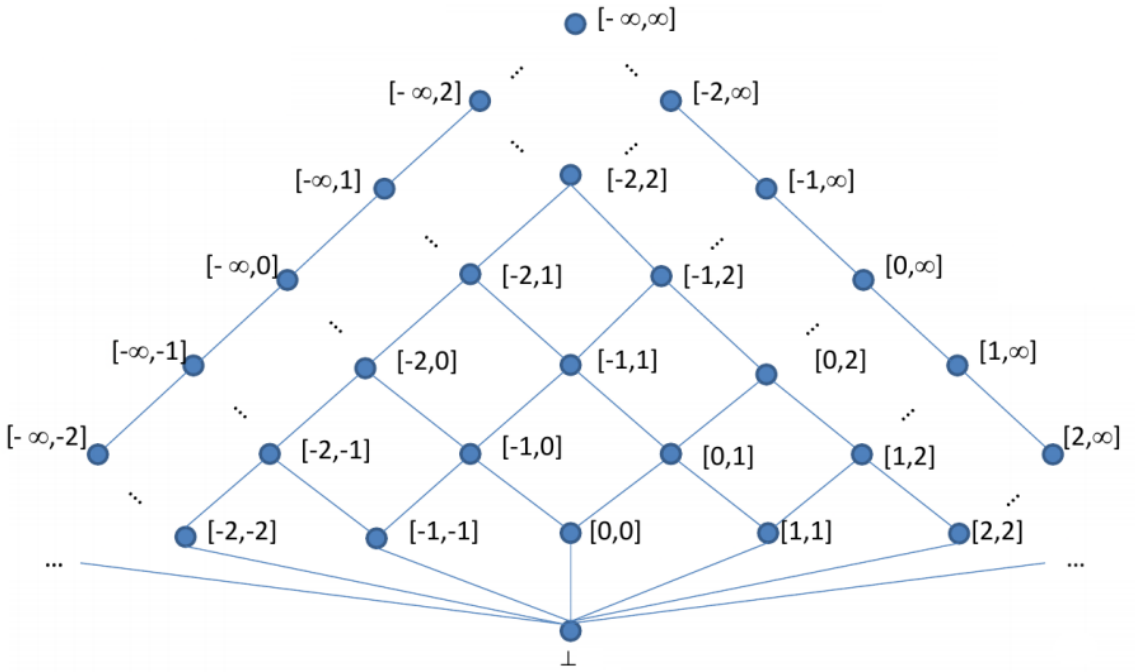
MUNI
FI

# Domain representation

- Interval domain lattice
  - Meet - ∩
  - Join - ∪
- Nondeterminism

```
int x = input()
        ↓
  x = [-∞, ∞]


 int y = 5
       ↓
  y = [5, 5]
```

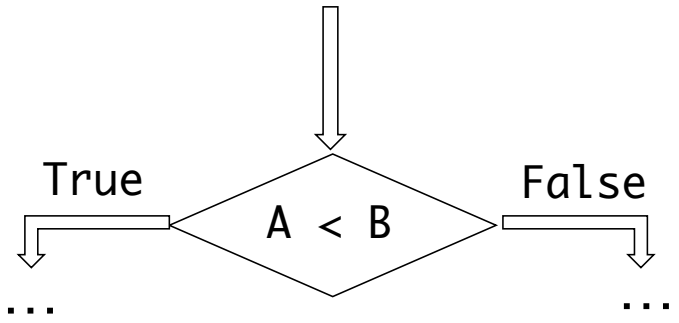



MUNI
FI

# Relational operations - LT

```
A = [1, 4]        B = [2, 7]        C = [5, 7]
```

```
A < C     -> True
C < A     -> False
A < B     -> Maybe
```




MUNI
FI

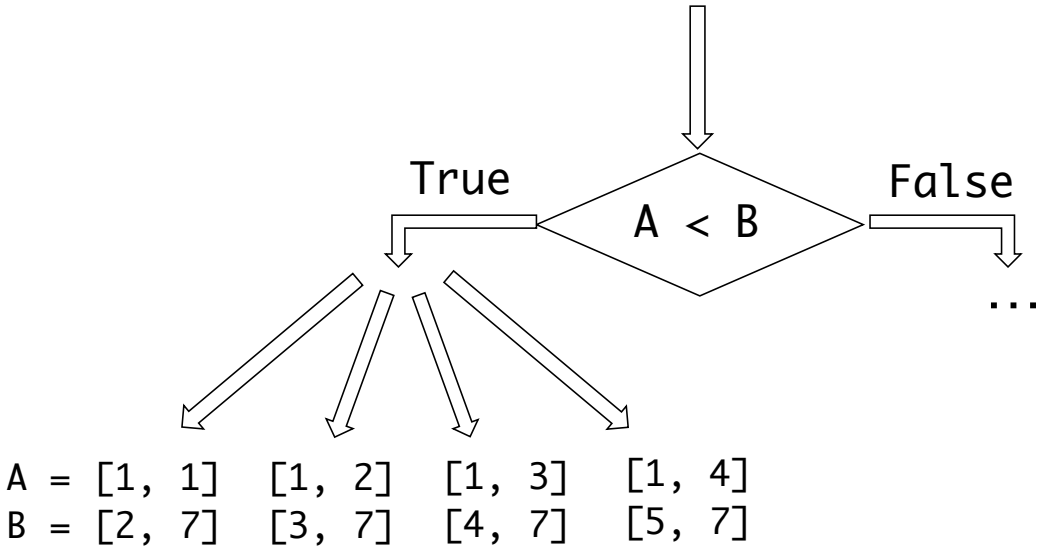
# Relational operations – BOP_LT

A = [1, 4]

B = [2, 7]

[1, 2, 3, 4]

[2, 3, 4, 5, 6, 7]

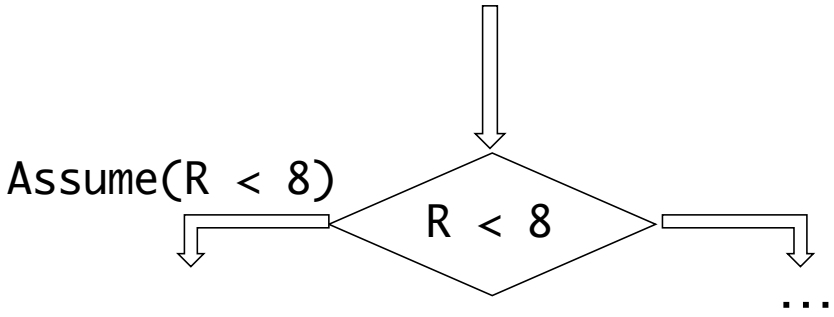



MUNI
FI

# Arithmetic operations – BOP_ADD

A = [2, 5]  B = [3, 5]

R = A + B = [5, 10]




R' = [5, 7]

Trivial approach:

$A_T = A \cap (R' - B) = [2, 5] \cap [0, 4] = [2, 4]$

$B_T = B \cap (R' - A) = [3, 5] \cap [0, 5] = [3, 5]$

$A_T + B_T = R_T = [5, 9]$

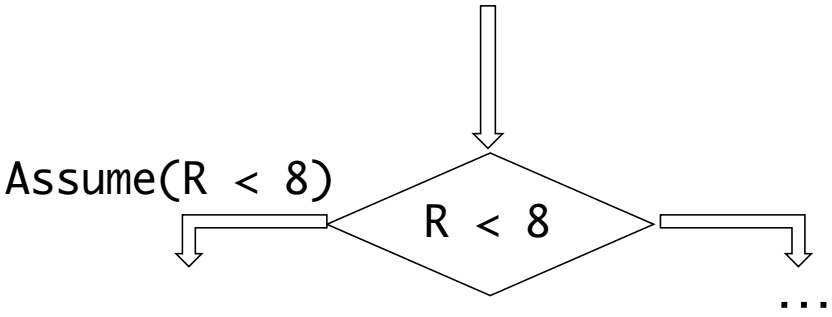
MUNI
FI

# Arithmetic operations – BOP_ADD

$A = [2, 5]$ $\quad B = [3, 5]$

$A_T = [2, 4]$ $\quad B_T = [3, 5]$

$R' = [5, 7]$ $\quad R_T = [5, 9]$




'Choose' approach:

$\Delta_H = RH_T - RH' = 9 - 7 = 2$ $\quad \Delta_L = RL' - RL_T = 5 - 5 = 0$

$i = choose( \Delta_H + 1 )$

$A = [AL_T, AH_T - i]$

$B = [BL_T, BH_T - \Delta_H + i]$

MUNI
FI

# Arithmetic operations – BOP_ADD

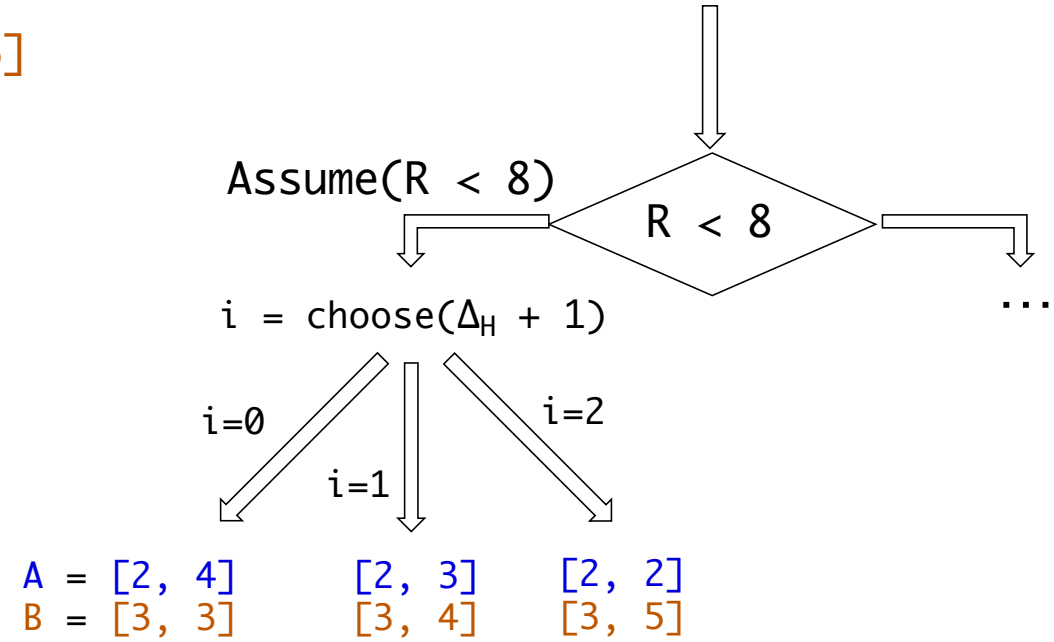
$A_T = [2, 4]$ $B_T = [3, 5]$

$\Delta_H = 2$ $\Delta_L = 0$

$R' = [5, 7]$

$A = [AL_T, AH_T - i]$

$B = [BL_T, BH_T - \Delta_H + i]$




MUNI
FI

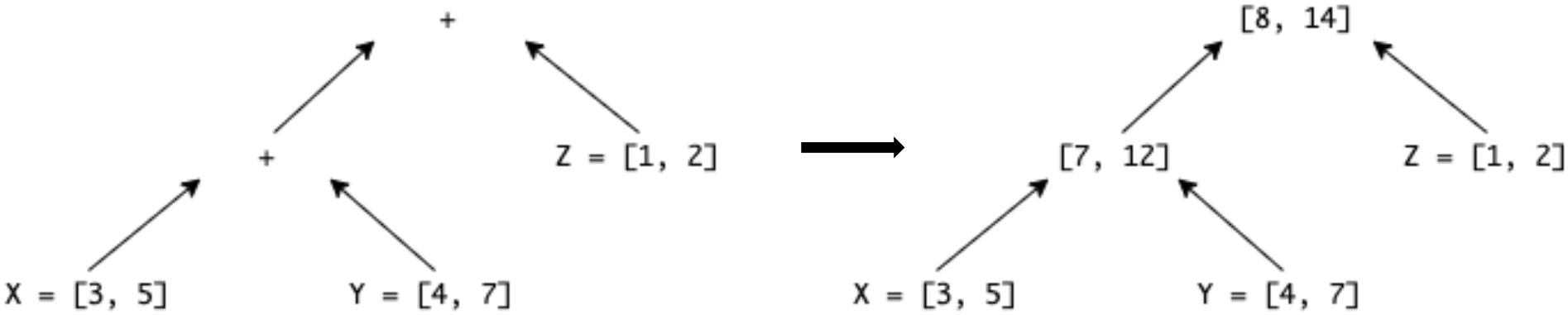
# Arithmetic operations – BOP_ADD

Invariants:

- Sum of intervals A and B after choose is equivalent to expected R’
- Unity of all intervals A across branches after choose is equivalent to $A_T$ before choose. (Same for B)

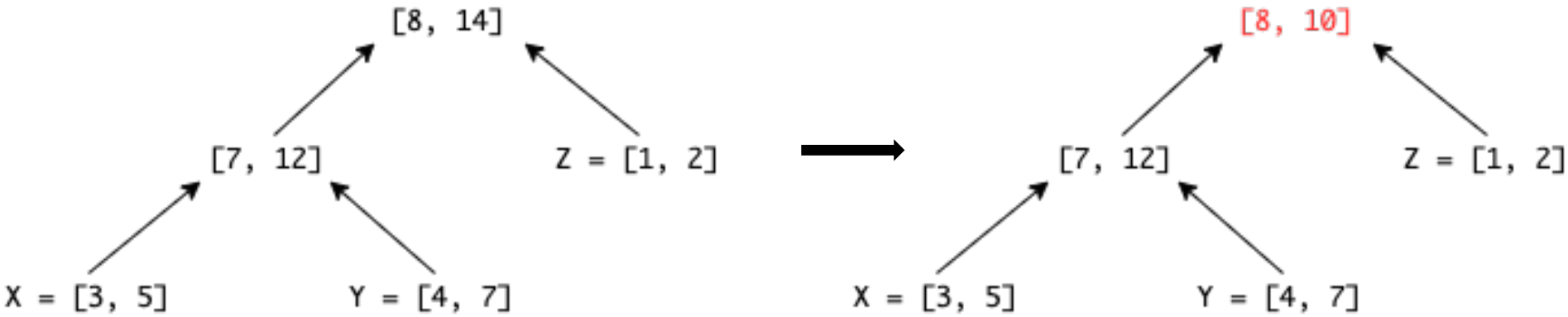
MUNI
FI

# Multiple level propagation



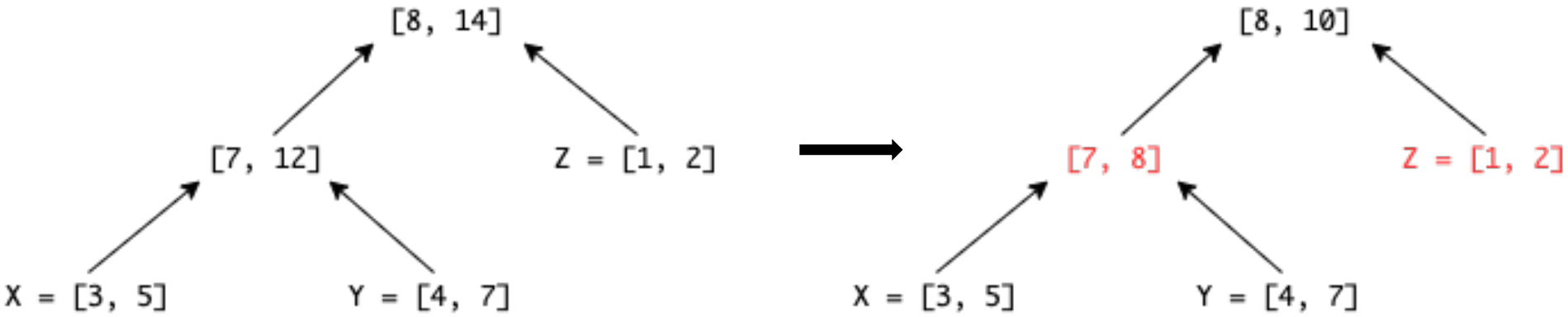

MUNI
FI

# Multiple level propagation



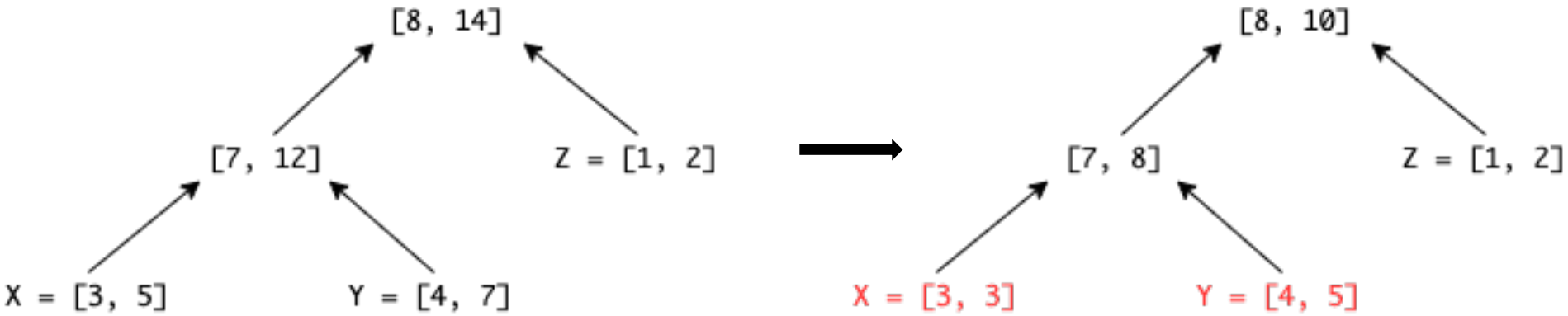

MUNI
FI

# Multiple level propagation




MUNI
FI

# Multiple level propagation

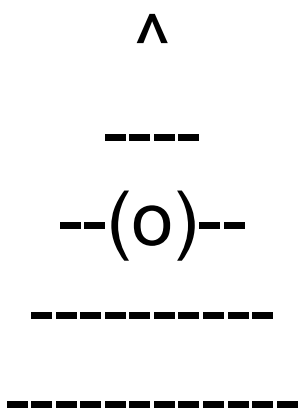



MUNI
FI

# What's Next

- Bitwise operation refinement
- Domain refinement
  - BOP splitting
- BOP propagation constraints

MUNI
FI



**Thank you for attention**

MUNI
FI