

DFAの仕組み ～命題論理～

何らかの条件を命題としてとらえ、
ある命題Xと別の命題Yがある場合に
「命題Xが真ならば 命題Yが真である」
と言えるかを考えます。

例えば、n を整数として

命題X : $0 < n < 5$ 命題Y : $n \neq 0$

命題Xが真ならば命題Yも真である

命題X : $0 \leq n < 5$ 命題Y : $n \neq 0$

命題Xが真であっても命題Yが真である
とは限らない

C言語との関係

前スライドの例は、次のコードと関係します。

```
1: int func(int n) {  
2:     int a = 0;  
3:     if ( (0 < n) && (n < 5) ) {  
4:         a = 100 / n;  
5:     }  
6:     return a;  
7: }
```

n が取り得る値の範囲が決まる
= 命題X : $0 < n < 5$

nはゼロであってはならない
= 命題Y : $n \neq 0$

命題X \Rightarrow 命題Y が成り立つかどうかによって

4行目が不具合を引き起こす可能性があるかを判定

DFAのステップ

○ステップ1

プログラムを読み解きながら、プログラムを命題論理に変換する

```
if ( (0 < n) && (n < 5) ) {  
    a = 100 / n;  
}
```

命題X: $0 < n < 5$
命題Y: $n \neq 0$

○ステップ2

変換した命題論理を、命題論理の真偽を教えてくれるプログラム(Theorem Solver)に渡す

命題X \Rightarrow 命題Y ?

○ステップ3

Theorem Solverが教えてくれた答えに基づいて警告を出す