2017156019 염민휘

과제를 진행한 인원 : 1명(Alone)

function increment (y)

comment Return y+1, where y ∈ N

1. x:=0, c:=1, d:=1; → y와 c 모두 0이 될 때까지 반복
2. while (y>0) V (c>0) do → y를 2로 나눈 나머지 (y가 홀수면 1, 짝수면 0)
3. a:= y mod 2 → a는 y를 2로 나눈 나머지
4. if a ⊕ c then x:=x+d; → a XOR c 즉, a, c 중 1이 하나만 있으면 x 값에 x+d 대입
5. c:= a ∧ c; → a와 c 모두 1이면 c=1, 아니면 0
6. d:=2d; y:=⌊y/2⌋; → d의 값(자리값)을 2배, y는 2로 나누면 0,,
7. return(x) → x값 리턴

• 알고리즘 이해.

011(2)가 있다고 가정하겠음. 첫 루프를 돌게 되면…

i) 1. x:=0, c:=1, d:=1, y=1 (2^n=d=1 즉, 2^0 자리의 y값 =1)
   2. y=1, c=1 이기에 3줄 실행 → do,,
   3. a:=1 mod 2 = 1,,
   4. if a⊕c but, a와 c 모두 1임 ⇒ x=0 유지,,
   5. c:= a∧c → a와 c 모두 1이기에 c=1,, <Carry>
   6. d의 값(자리값) ×2 = 2, y ⌊1/2⌋ = 0,,
   7. return : 0,,

⇒ 011(2)

두번째 루프를 돌게 되면…

ii) 1. x=0, c=1, d=2, y=1 (2^n=d=2 즉, 2^1 자리의 y값 =1)
   2. y=1, c=1 이기에 3줄 실행 → do,,
   3. a:=1 mod 2 = 1,,
   4. if a⊕c but, a와 c 모두 1임 ⇒ x=0 유지,
   5. c:= a∧c → a와 c 모두 1이기에 c=1,, <Carry>
   6. d의 값(자리값) ×2 = 4, y=⌊1/2⌋ = 0,,
   7. return : 0,,

⇒ 011(2)

세 번째 루프를 돌게 되면..

iii) 1. x=0, c=1, d=4, y=0 (2^n=d=4 즉, 2^2 자리의 y값 = 0)
   2. y=0, c=1 이기에 3줄 실행 → do,,
   3. a:= 0 mod 2 = 0,,
   4. if a⊕c → c만 1이기에 x:= x+d = 0+4 = 4(2^2)
   5. c:=a∧c but, c만 1이기에 c=0,, <Carry 없음>
   6. d의 값 ×2 = 8, y=⌊0/2⌋=0,,
   7. return : 0,,

⇒ 011(2)

네 번째 루프를 돌게 되면…

iv) 1. x=4, c=0, d=8, y=0
   2. y=0, c=0 이기에 반복문 종료!,,

⇒ 011(2) + 1(2) = 100(2) = 4 (y값 + c값)

이는 최종 리턴값인 x 값(2^2)과 동일하다.,,

⇒ 이는 초기값에 c 즉, 캐리값 1을 넣어줌으로써, "1을 이진수에 더하는 알고리즘"임을 알 수 있다.

· 변수 정의

최초값 : y_0 , 종료 시 리턴값 x_t ($= y_0$에 1을 더한 값) $= y_0+1$

$a := y \bmod 2 \Rightarrow a_{j+1} = y_j \bmod 2$

$c := a \wedge c$: 둘 다 1-bit라 $c=1 \Rightarrow c_{j+1} = \lfloor (a_{j+1} + c_j)/2 \rfloor$

$d := 2d \Rightarrow d_{j+1} = 2d_j$

$y := \lfloor y/2 \rfloor \Rightarrow y_{j+1} = \lfloor y_j/2 \rfloor$

x는 $a+c$가 1인 때, x에 d를 더한 값임 $\Rightarrow x_{j+1} = x_j + d_j\{(a_{j+1}+c_j) \bmod 2\}$

$= (a+c) \bmod 2 = 1$

루프가 j번 돌았을 때, x_t(전자) 값은 $x_j + (y_j + c_j)d_j$ 이고 이는 y_0+1과 같다.

$\therefore x_j + (y_j + c_j)d_j = y_0+1 \ (j \geq 0) \Rightarrow$ loop invariant

이를 귀납법을 통해 참임을 증명해보자

· 귀납법

i) $j=0$, $(y_0 + c_0)\cdot d_0 + x_0 = (y_0+1)\cdot 1 + 0 = y_0+1$ → 성립

ii) $j = j+1$ ($j+1$번 루프가 돌았을 때)

$(y_{j+1} + c_{j+1})d_{j+1} + x_{j+1} = y_0+1$ 이 성립한다고 가정하자.

위 식은 $(\lfloor y_j/2 \rfloor + \lfloor (a_{j+1}+c_j)/2 \rfloor)\cdot 2d_j + x_j + d_j\{(a_{j+1}+c_j) \bmod 2\}$

$= 2d_j(\lfloor y_j/2 \rfloor) + (\lfloor (y_j \bmod 2 + c_j)/2 \rfloor)\cdot 2d_j + x_j + d_j\{(y_j \bmod 2 + c_j) \bmod 2\}$

[※ $(y_j \bmod 2 + c_j) = N$으로 치환하면, $d_j(2\lfloor N/2 \rfloor + N \bmod 2)$ 이다.
이는 몫과 나머지 정리이므로, $d_j \cdot N$으로 치환된다 ($2\lfloor N/2 \rfloor + N \bmod 2 = N$)
여기서 N은 원래 값으로 다시 치환해주면 $d_j(y_j \bmod 2 + c_j)$]

$= 2d_j(\lfloor y_j/2 \rfloor) + x_j + d_j(y_j \bmod 2 + c_j)$

$= d_j(2\lfloor y_j/2 \rfloor + y_j \bmod 2) + x_j + d_j \cdot c_j$

※ 몫과 나머지 정리로 인해 이는 y_j와 같다

$= d_j \cdot y_j + x_j + d_j \cdot c_j$

$= d_j(y_j + c_j) + x_j$ 로 정리 가능하며

$d_j(y_j+c_j) + x_j = y_0+1$ 이 성립한다

y는 루프가 돌 때마다 계속 2로 나누어지고, 결국 0이 될 것이다.
C또한 0이거나, 다음 루프에 0이 될 것이다. ∴ y와 C는 마지막 루프 때, 0이 된다는 뜻

iii) j = t (마지막 루프)

$(y_t + C_t)\, d_t + x_t = y_{n+1}$ 이 성립하는가?

$y_t, C_t = 0$ $\therefore x_t = y_{n+1}$ (while 반복문이 종료되고, x_t를 리턴)

∴ Loop Invariant 가 성립함이 증명되었다