Alessandro D'Angelo 18.2.4054

BCC203

Tutoria

1. Shift-And Exato

	a	b	r	a	b	r	a
M[a]	1	0	0	1	0	0	1
M[b]	0	1	0	0	1	0	0
M[c]	0	0	0	0	0	0	0
M[r]	0	0	1	0	0	1	0

R' = ((R >> 1) | 10m−1) & M[T[i]]

R	0	0	0	0	0	0	0

Passo a passo:

abracabcabc abrabrabra abababrabrb

{a} R' = (0000000 | 1000000) & 1001001 = 1000000 & 1001001 = 1000000

{b} R' = (0100000 | 1000000) & 0100100 = 1100000 & 0100100 = 0100000

{r} R' = (0010000 | 1000000) & 0010010 = 1010000 & 0010010 = 0010000

{a} R' = (0001000 | 1000000) & 1001001 = 1001000 & 1001001 = 1001000

{c} R' = (1001000 | 1000000) & 0000000 = 1001000 & 0000000 = 0000000

{a} R' = (0000000 | 1000000) & 1001001 = 1000000 & 1001001 = 1000000

{b} R' = (0100000 | 1000000) & 0100100 = 1100000 & 0100100 = 0100000

{c} R' = (0010000 | 1000000) & 0000000 = 1010000 & 0000000 = 0000000

{a} R' = (0000000 | 1000000) & 1001001 = 1000000 & 1001001 = 1000000

{b} R' = (0100000 | 1000000) & 0100100 = 1100000 & 0100100 = 0100000

{c} R' = (0010000 | 1000000) & 0000000 = 1010000 & 0000000 = 0000000

{ } R' = (0000000 | 1000000) & 0000000 = 0000000 & 0000000 = 0000000

{a} R' = (0000000 | 1000000) & 1001001 = 1000000 & 1001001 = 1000000

{b} R' = (0100000 | 1000000) & 0100100 = 1100000 & 0100100 = 0100000

{r} R' = (0010000 | 1000000) & 0010010 = 1010000 & 0010010 = 0010000

{a} R' = (0001000 | 1000000) & 1001001 = 1001000 & 1001001 = 1001000

{b} R' = (0100100 | 1000000) & 0100100 = 1100100 & 0100100 = 0100100

{r} R' = (0010010 | 1000000) & 0010010 = 1010010 & 0010010 = 0010010

{a} R' = (0001001 | 1000000) & 1001001 = 1001001 & 1001001 = 1001001

Como o número 1 se encontra na última posição então achamos o padrão.

2. Shift-And Aproximado

	a	b	r	a	b	r	a
M[a]	1	0	0	1	0	0	1
M[b]	0	1	0	0	1	0	0
M[c]	0	0	0	0	0	0	0
M[r]	0	0	1	0	0	1	0

R0 = ((R >> 1) | 10m−1) & M[T[i]]

R1 = ((R1 >> 1) & M[T[i]]) | R0 | 10m−1

Passo a passo:

abracabcabc abrabrabra abababrabrb

R0 = (0000000 | 1000000) & 1001001 = 1000000 & 1001001 = 1000000

R1 = (0000000 & 1000000) | 1000000 | 1000000 = 1000000

{a}

R0 = (0000000 | 1000000) & 1001001 = 1000000 & 1001001 = 1000000

R1 = (0000000 & 1000000) | 1000000 | 1000000 = 1000000

{b}

R0 = (0100000 | 1000000) & 0100100 = 1100000 & 0100100 = 0100000

R1 = (0100000 & 0100100) | 1000000 | 1000000 = 1100000

{r}

R0 = (0010000 | 1000000) & 0010010 = 1010000 & 0010010 = 0010000

R1 = (0110000 & 0010010) | 0100000 | 1000000 = 1110000

{a}

R0 = (0001000 | 1000000) & 1001001 = 1001000 & 1001001 = 1001000

R1 = (0111000 & 1001001) | 0010000 | 1000000 = 1011000

{c}

R0 = (1001000 | 1000000) & 0000000 = 1001000 & 0000000 = 0000000

R1 = (0101100 & 0000000) | 1001000 | 1000000 = 1001000

{a}

R0 = (0000000 | 1000000) & 1001001 = 1000000 & 1001001 = 1000000

R1 = (0100100 & 1001001) | 0000000 | 1000000 = 1000000

{b}

R0 = (0100000 | 1000000) & 0100100 = 1100000 & 0100100 = 0100000

R1 = (0100000 & 0100100) | 1000000 | 1000000 = 1100000

{c}

R0 = (0010000 | 1000000) & 0000000 = 1010000 & 0000000 = 0000000

R1 = (0110000 & 0000000) | 0100000 | 1000000 = 1100000

{a}

R0 = (0000000 | 1000000) & 1001001 = 1000000 & 1001001 = 1000000

R1 = (0110000 & 1001001) | 0000000 | 1000000 = 1000000

{b}

R0 = (0100000 | 1000000) & 0100100 = 1100000 & 0100100 = 0100000

R1 = (0100000 & 0100100) | 1000000 | 1000000 = 1100000

{c}

R0 = (0010000 | 1000000) & 0000000 = 1010000 & 0000000 = 0000000

R1 = (0110000 & 0000000) | 0100000 | 1000000 = 1100000

{ }

R0 = (0000000 | 1000000) & 0000000 = 1000000 & 0000000 = 0000000

R1 = (0110000 & 0000000) | 0000000 | 1000000 = 1000000

{a}

R0 = (0000000 | 1000000) & 1001001 = 1000000 & 1001001 = 1000000

R1 = (0100000 & 1001001) | 0000000 | 1000000 = 1000000

{b}

R0 = (0100000 | 1000000) & 0100100 = 1100000 & 0100100 = 0100000

R1 = (0100000 & 0100100) | 1000000 | 1000000 = 1100000

{r}

R0 = (0010000 | 1000000) & 0010010 = 1010000 & 0010010 = 0010000

R1 = (0110000 & 0010010) | 0100000 | 1000000 = 1110000

{a}

R0 = (0001000 | 1000000) & 1001001 = 1001000 & 1001001 = 1001000

R1 = (0111000 & 1001001) | 0010000 | 1000000 = 1011000

{b}

R0 = (0100100 | 1000000) & 0100100 = 1100100 & 0100100 = 0100100

R1 = (0101100 & 0100100) | 1001000 | 1000000 = 1101100

{r}

R0 = (0010010 | 1000000) & 0010010 = 1010010 & 0010010 = 0010010

R1 = (0110110 & 0010010) | 0100100 | 1000000 = 1110110

{a}

R0 = (0001001 | 1000000) & 1001001 = 1001001 & 1001001 = 1001001

R1 = (0111011 & 1001001) | 0010010 | 1000000 = 1011011