Homework 6.1

Casey Bates

12 May 2020

1 Diffusion in the θ Step

(a)

If a bit $a_{in}[i][j][k]$ is changed, the bits $a_{in}[i+1][0...4][k]$ (Blue in Figure 1) and $a_{in}[i-1][0...4][k+1]$ (Purple in Figure 1) could potentially be changed.

Therefore, if the bit in $a_{in}[2][1][24]$ is changed, 10 bits will be affected: $a_{in}[3][0...4][24]$, and $a_{in}[1][0...4][25]$

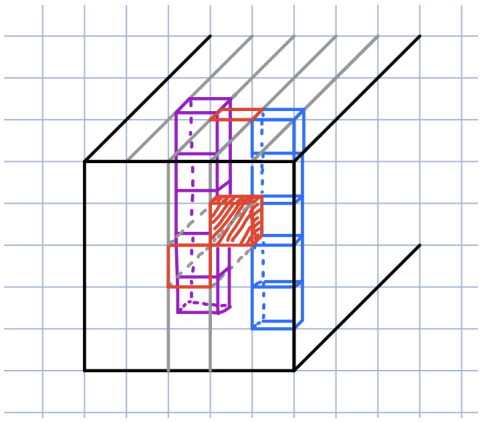

Figure 1: Sketch of 3D Array a_{in}

(b)

For the second application of the θ function, we will apply the same principal as part (a) on the newly affected bits. A change of the bits in column $a_{in}[3][0...4][24]$ will affect the bits $a_{in}[4][0...4][24]$ and $a_{in}[2][0...4][25]$. Similarly, a change of the bits in column $a_{in}[1][0...4][25]$ will affect the bits $a_{in}[2][0...4][25]$ and $a_{in}[0][0...4][26]$. Since both columns will affect $a_{in}[2][0...4][25]$, we need only count it once.

Therefore, 15 additional bits will be affected in the second consecutive round of θ. After two rounds, we will have a total of 25 bits affected by the change of one bit at the start.

2 Find RC[2] in the ι Step

For round $\iota_r = 2$, with $0 \leq l \leq 6$ and x^t reduced in $F_2[x]/(x^8+x^6+x^5+x^4+1)$, we have:

l	$2^l - 1$	$t = l + 7\iota_r$	x^t	$rc[t] = bit[0][0][2^l - 1]$
0	0	14	$x^{14} = x^7 + x^6 + x^4 + x^3$	0
1	1	15	$x^{15} = x^7 + x^6 + 1$	1
2	3	16	$x^{16} = x^7 + x^6 + x^5 + x^4 + x + 1$	1
3	7	17	$x^{17} = x^7 + x^4 + x^2 + x + 1$	1
4	15	18	$x^{18} = x^6 + x^4 + x^3 + x^2 + 1$	1
5	31	19	$x^{19} = x^7 + x^5 + x^4 + x^3 + x^2 + x$	0
6	63	20	$x^{20} = x^3 + x^2 + x + 1$	1

RC[2] =	1	...	0	...	1	...	1	0	0	0	1	0	1	0
	63		31		15		7	6	5	4	3	2	1	0

RC[2] = 0x8000000000000808A