

COLT: Exercise 13

Ramon Xuriguera

Code available at:

<https://github.com/rxuriguera/colt/tree/master/exercises/013/>

Notation: $1 \leftarrow 0 \ 2 \ 4$ is the same as $x_1 x_3 x_5 \rightarrow x_2$

Step 1	Step 2	Step 3	Step 4	Step 5
EQ: 01011 S: 01011	EQ: 11100 S: 01011 11100	EQ: 00001 S: 00001 11100	EQ: 00011 S: 00001 11100	EQ: 01011 S: 00001 11100 01011
h: F \leftarrow 1,3,4 0 \leftarrow 1,3,4 2 \leftarrow 1,3,4	h: F \leftarrow 0,1,2 3 \leftarrow 0,1,2 4 \leftarrow 0,1,2 F \leftarrow 1,3,4 0 \leftarrow 1,3,4 2 \leftarrow 1,3,4	h: F \leftarrow 0,1,2 3 \leftarrow 0,1,2 4 \leftarrow 0,1,2 F \leftarrow 4 0 \leftarrow 4 1 \leftarrow 4 2 \leftarrow 4 3 \leftarrow 4	h: F \leftarrow 0,1,2 3 \leftarrow 0,1,2 4 \leftarrow 0,1,2 3 \leftarrow 4	h: F \leftarrow 0,1,2 3 \leftarrow 0,1,2 4 \leftarrow 0,1,2 F \leftarrow 1,3,4 0 \leftarrow 1,3,4 2 \leftarrow 1,3,4 F \leftarrow 4 0 \leftarrow 4 1 \leftarrow 4 2 \leftarrow 4 3 \leftarrow 4
Step 6	Step 7	Step 8	Step 9	Step 10
EQ: 00011 S: 00001 11100 01011	EQ: 00110 S: 00001 11100 01011 00110	EQ: 00011 S: 00001 11100 01011 00110	EQ: 01110 S: 00001 11100 01011 00110	EQ: 10010 S: 00001 11100 01011 00110 10010
h: F \leftarrow 0,1,2 3 \leftarrow 0,1,2 4 \leftarrow 0,1,2 F \leftarrow 1,3,4 0 \leftarrow 1,3,4 2 \leftarrow 1,3,4 3 \leftarrow 4	h: F \leftarrow 0,1,2 3 \leftarrow 0,1,2 4 \leftarrow 0,1,2 F \leftarrow 1,3,4 0 \leftarrow 1,3,4 2 \leftarrow 1,3,4 F \leftarrow 2,3 0 \leftarrow 2,3 1 \leftarrow 2,3 4 \leftarrow 2,3 F \leftarrow 4 0 \leftarrow 4 1 \leftarrow 4 2 \leftarrow 4 3 \leftarrow 4	h: F \leftarrow 0,1,2 3 \leftarrow 0,1,2 4 \leftarrow 0,1,2 F \leftarrow 1,3,4 0 \leftarrow 1,3,4 2 \leftarrow 1,3,4 F \leftarrow 2,3 0 \leftarrow 2,3 1 \leftarrow 2,3 4 \leftarrow 2,3 3 \leftarrow 4	h: F \leftarrow 0,1,2 3 \leftarrow 0,1,2 4 \leftarrow 0,1,2 F \leftarrow 1,3,4 0 \leftarrow 1,3,4 2 \leftarrow 1,3,4 1 \leftarrow 2,3 3 \leftarrow 4	h: F \leftarrow 0,1,2 3 \leftarrow 0,1,2 4 \leftarrow 0,1,2 F \leftarrow 0,3 1 \leftarrow 0,3 2 \leftarrow 0,3 4 \leftarrow 0,3 F \leftarrow 1,3,4 0 \leftarrow 1,3,4 2 \leftarrow 1,3,4 F \leftarrow 2,3 0 \leftarrow 2,3 1 \leftarrow 2,3 4 \leftarrow 2,3 F \leftarrow 4 0 \leftarrow 4 1 \leftarrow 4 2 \leftarrow 4 3 \leftarrow 4

Step 11EQ: 00011
S:00001
11100
01011
00110
10010

h:

F <- 0,1,2
3 <- 0,1,2
4 <- 0,1,2
F <- 0,3
1 <- 0,3
2 <- 0,3
4 <- 0,3
F <- 1,3,4
0 <- 1,3,4
2 <- 1,3,4
F <- 2,3
0 <- 2,3
1 <- 2,3
4 <- 2,3
3 <- 4**Step 12**EQ: 01110
S:00001
11100
01011
00110
10010

h:

F <- 0,1,2
3 <- 0,1,2
4 <- 0,1,2
F <- 0,3
1 <- 0,3
2 <- 0,3
4 <- 0,3
F <- 1,3,4
0 <- 1,3,4
2 <- 1,3,4
1 <- 2,3
3 <- 4**Step 13**EQ: 01010
S:00001
11100
01010
00110
10010

h:

F <- 0,1,2
3 <- 0,1,2
4 <- 0,1,2
F <- 0,3
1 <- 0,3
2 <- 0,3
4 <- 0,3
F <- 1,3
0 <- 1,3
2 <- 1,3
4 <- 1,3
F <- 2,3
0 <- 2,3
1 <- 2,3
4 <- 2,3
F <- 4
0 <- 4
1 <- 4
2 <- 4
3 <- 4**Step 14**EQ: 00011
S:00001
11100
01010
00110
10010

h:

F <- 0,1,2
3 <- 0,1,2
4 <- 0,1,2
F <- 0,3
1 <- 0,3
2 <- 0,3
4 <- 0,3
F <- 1,3
0 <- 1,3
2 <- 1,3
4 <- 1,3
F <- 2,3
0 <- 2,3
1 <- 2,3
4 <- 2,3
3 <- 4**Step 15**EQ: 01110
S:00001
11100
01010
00110
10010

h:

F <- 0,1,2
3 <- 0,1,2
4 <- 0,1,2
F <- 0,3
1 <- 0,3
2 <- 0,3
4 <- 0,3
2 <- 1,3
1 <- 2,3
3 <- 4**Step 16**EQ: 01111
S:00001
01100
01010
00110
10010

h:

F <- 0,3
1 <- 0,3
2 <- 0,3
4 <- 0,3
F <- 1,2
0 <- 1,2
3 <- 1,2
4 <- 1,2
F <- 1,3
0 <- 1,3
2 <- 1,3
4 <- 1,3
F <- 2,3
0 <- 2,3
1 <- 2,3
4 <- 2,3
F <- 4
0 <- 4
1 <- 4
2 <- 4
3 <- 4**Step 17**EQ: 00011
S:00001
01100
01010
00110
10010

h:

F <- 0,3
1 <- 0,3
2 <- 0,3
4 <- 0,3
F <- 1,2
0 <- 1,2
3 <- 1,2
4 <- 1,2
F <- 1,3
0 <- 1,3
2 <- 1,3
4 <- 1,3
F <- 2,3
0 <- 2,3
1 <- 2,3
4 <- 2,3
3 <- 4**Step 18**EQ: 01110
S:00001
01100
01010
00110
10010

h:

F <- 0,3
1 <- 0,3
2 <- 0,3
4 <- 0,3
3 <- 1,2
2 <- 1,3
1 <- 2,3
3 <- 4**Step 19**EQ: 01111
S:00001
01100
01010
00110
10010
01111

h:

F <- 0,3
1 <- 0,3
2 <- 0,3
4 <- 0,3
F <- 1,2,3,4
0 <- 1,2,3,4
F <- 1,2
0 <- 1,2
3 <- 1,2
4 <- 1,2
F <- 1,3
0 <- 1,3
2 <- 1,3
4 <- 1,3
F <- 2,3
0 <- 2,3
1 <- 2,3
4 <- 2,3
F <- 4
0 <- 4
1 <- 4
2 <- 4
3 <- 4**Step 20**EQ: 00011
S:00001
01100
01010
00110
10010
01111

h:

F <- 0,3
1 <- 0,3
2 <- 0,3
4 <- 0,3
F <- 1,2,3,4
0 <- 1,2,3,4
F <- 1,2
0 <- 1,2
3 <- 1,2
4 <- 1,2
F <- 1,3
0 <- 1,3
2 <- 1,3
4 <- 1,3
F <- 2,3
0 <- 2,3
1 <- 2,3
4 <- 2,3
3 <- 4

Step 21

EQ: 01110

S:

00001
 01100
 01010
 00110
 10010
 01111

h:

F \leftarrow 0,3
 1 \leftarrow 0,3
 2 \leftarrow 0,3
 4 \leftarrow 0,3
 F \leftarrow 1,2,3,4
 0 \leftarrow 1,2,3,4
 3 \leftarrow 1,2
 2 \leftarrow 1,3
 1 \leftarrow 2,3
 3 \leftarrow 4

Step 22

EQ: 11111

S:

00001
 01100
 01010
 00110
 10010
 01111

h:

1 \leftarrow 0,3
 2 \leftarrow 0,3
 4 \leftarrow 0,3
 0 \leftarrow 1,2,3,4
 3 \leftarrow 1,2
 2 \leftarrow 1,3
 1 \leftarrow 2,3
 3 \leftarrow 4

After the 22nd iteration, the EQ oracle returns a **Yes**
 and we are done.

Final hypothesis returned:

$$\begin{aligned}
 x_1x_4 &\rightarrow x_2 \quad \wedge \\
 x_1x_4 &\rightarrow x_3 \quad \wedge \\
 x_1x_4 &\rightarrow x_4 \quad \wedge \\
 x_2x_3x_4x_5 &\rightarrow x_1 \quad \wedge \\
 x_2x_3 &\rightarrow x_4 \quad \wedge \\
 x_2x_4 &\rightarrow x_3 \quad \wedge \\
 x_3x_4 &\rightarrow x_2 \quad \wedge \\
 x_5 &\rightarrow x_4
 \end{aligned}$$