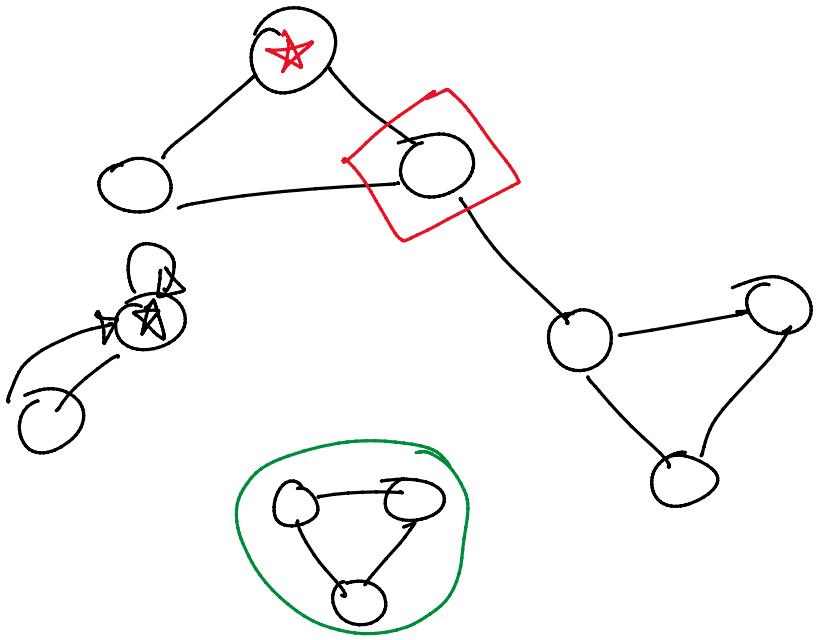
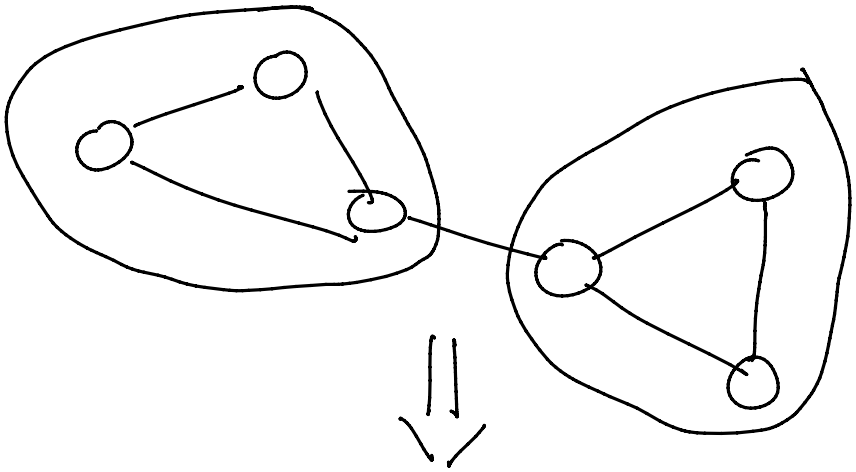
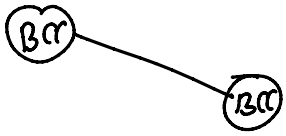
Class 27

Sunday, August 1, 2021 9:53 PM







$S_1 = AABEBCDD$

$S_2 = AABEBCDD$

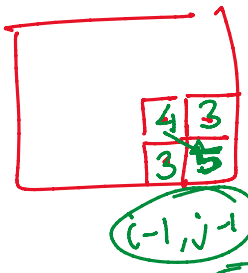
$S_1 = aX_1X_2X_3f \rightarrow$ $X_1\ X_2$ / $X_2\ X_3$

$S_2 = aX_1X_2X_3f \rightarrow$

$i=0$

$X_1\ X_2$

X_1 X_2 X_3 X_3



n ⊕ x = P

3 ⊕ 0	= 3
3 ⊕ 1	= 2
3 ⊕ 2	= 1
3 ⊕ 3	= 0
3 ⊕ 4	= 7
3 ⊕ 5	= 6

n = 3
m = 5

P

011 ⊕ 004 = 010

011 ⊕ 010 = 001

n ⊕ x = P
n ⊕ P = x

3 ⊕ 1 = (2)

100

011 ⊕ 100 = 111

(4)

011 ⊕ 001 = 010

011 ⊕ 101 = 110

m → 101
n → 011
100

00

000
001
010
011
100
101
~~110~~
~~4~~

EGCD:

$$ax + by = \gcd(a, b)$$

$$\begin{bmatrix} a & b \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \end{bmatrix}$$

$$\underset{1\times 2}{\begin{bmatrix} a & b \end{bmatrix}} \underset{2\times 1}{\begin{bmatrix} x \\ y \end{bmatrix}} = \begin{bmatrix} ax+by \end{bmatrix}$$

$$gcd(a,b) = gcd(b, a\%b)$$

s0 → $55x + 80y = 5$ → (3, -2)

s1 → $80x + 55y = 5$ → (-2, 3)

s2 → $55x + 25y = 5$ → (1, -2)

s3 → $25x + 5y = 5$ → (0, 1)

s4 → $5x + 0.y = 5$ → (1, 0)

$0 - 1\lfloor \frac{55}{25} \rfloor$

$0 - 1(2)$

-2

$1 + 2(1)$

$-2 + 3(0)$

$ax_0 + by_0 = g$ ——— ①

$bx_1 + (a\%b)y_1 = g$ ——— ②

$\Rightarrow bx_1 + (a - \lfloor a/b \rfloor b)y_1 = g$

$\Rightarrow bx_1 + ay_1 - by_1\lfloor a/b \rfloor = g$

$\Rightarrow ay_1 + b(x_1 - y_1\lfloor a/b \rfloor) = g$ ——— ③

$x_0 = y_1$

$y_0 = x_1 - y_1\lfloor a/b \rfloor$

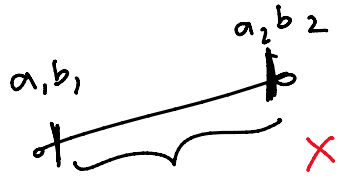
— o —

$55(3) + 80(-2) = 5$ → $ax + by = g$

$a\left(x + \frac{b}{g}\right) + b\left(y - \frac{a}{g}\right) = g$

$\Rightarrow ax + \frac{ab}{g} + by - \frac{ab}{g} = g$

$\Rightarrow ax + by = g$



$x \longrightarrow x + \frac{b}{g}$

$y \longrightarrow y - \frac{a}{g}$

$a_2 - a_1$

$\frac{a_2 - a_1}{b_2 - b_1}$ $y \rightarrow y - \frac{u}{q}$ $\Rightarrow ax + by = y$

$3 \rightarrow 3 + 16 \rightarrow 19$

$-2 \rightarrow -2 - 11 \rightarrow -13$