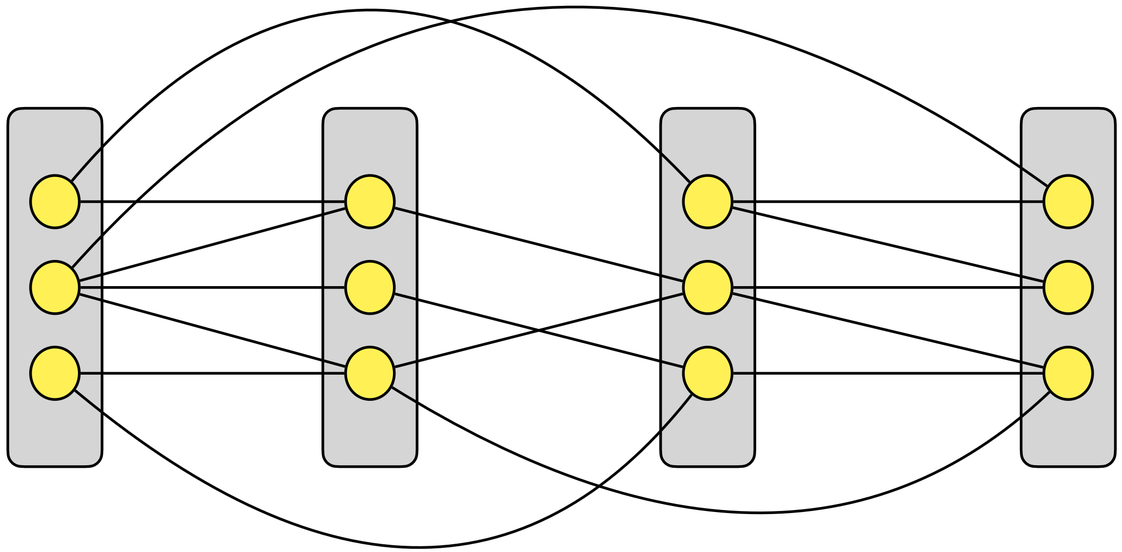
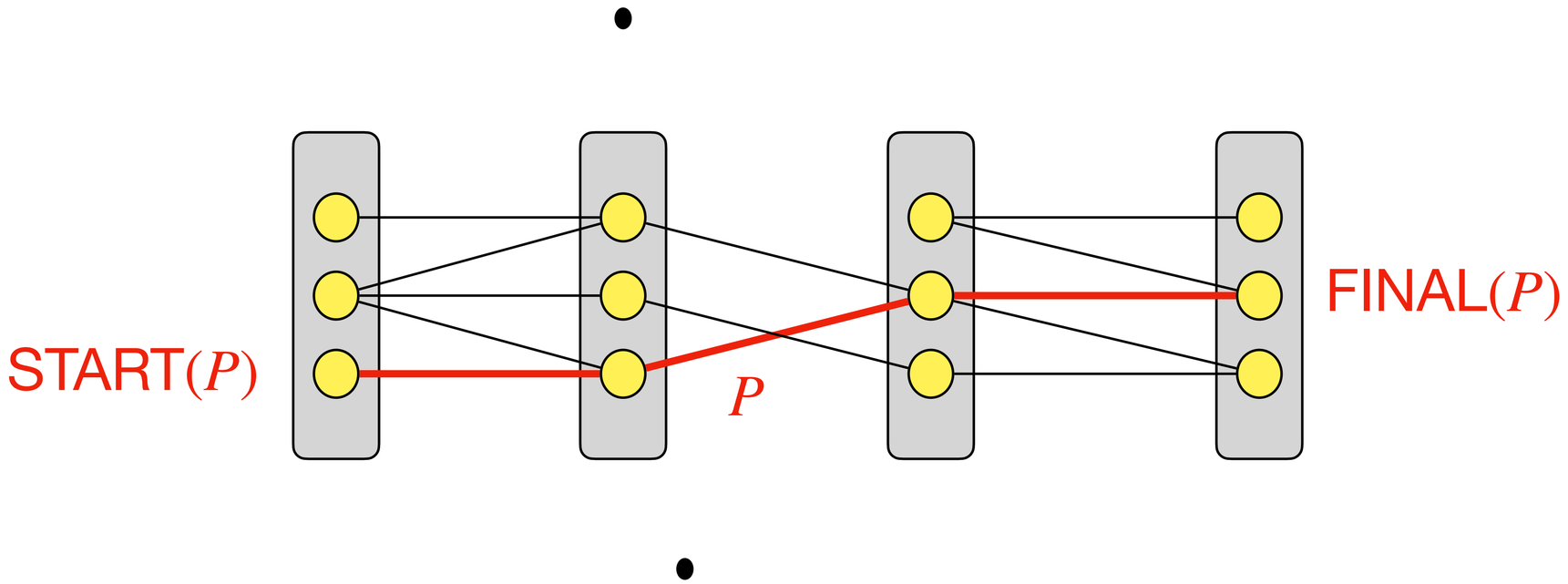
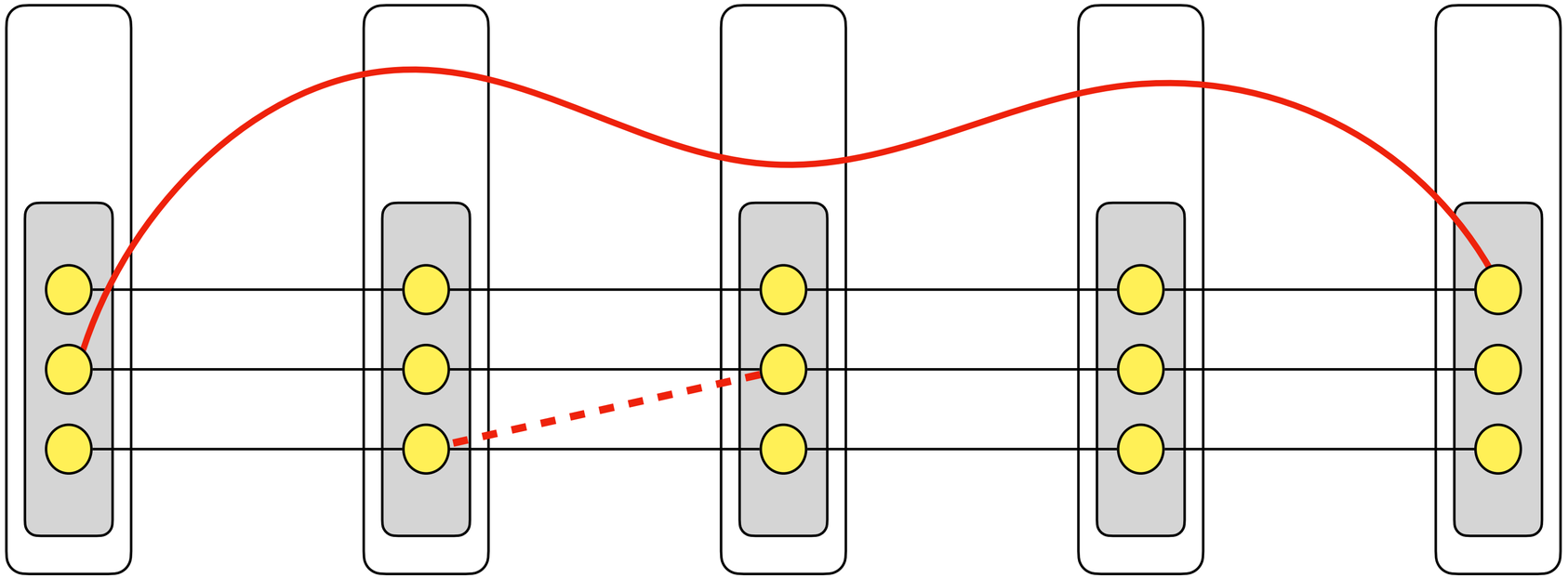
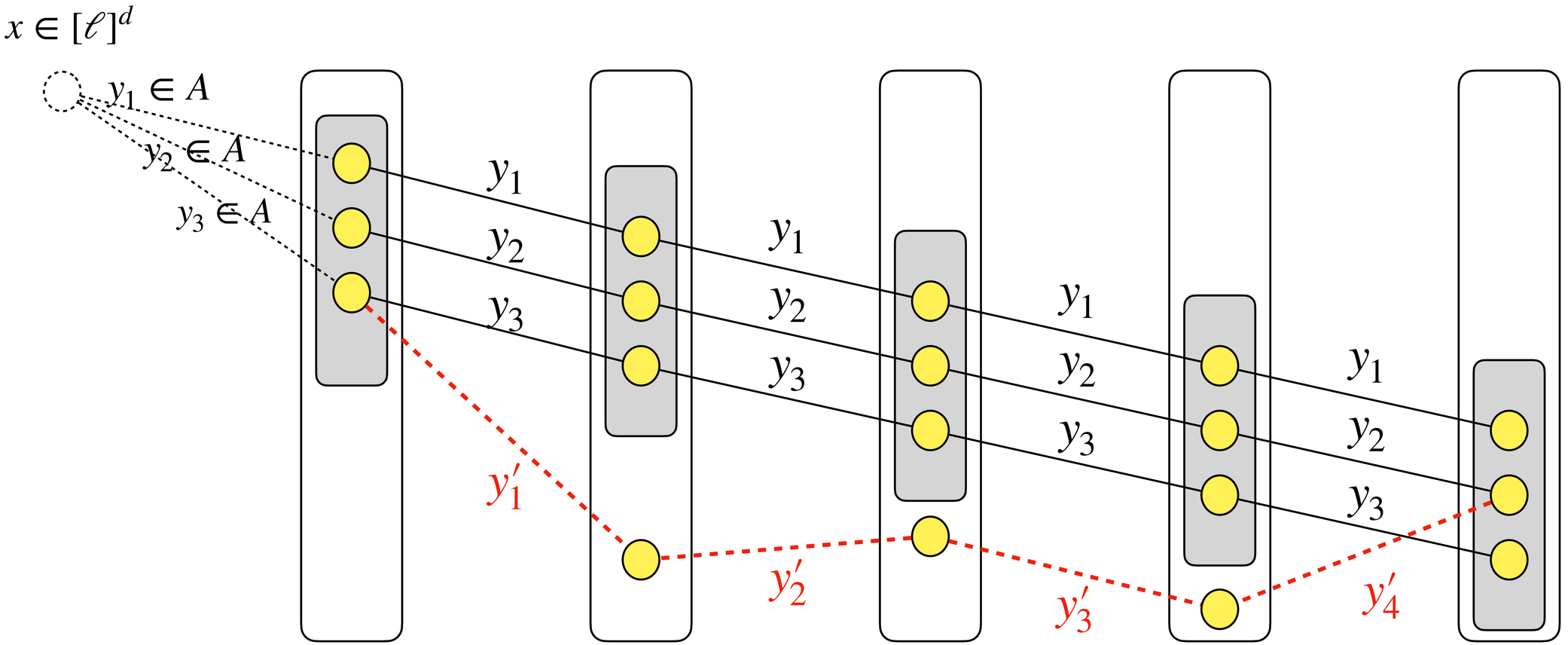
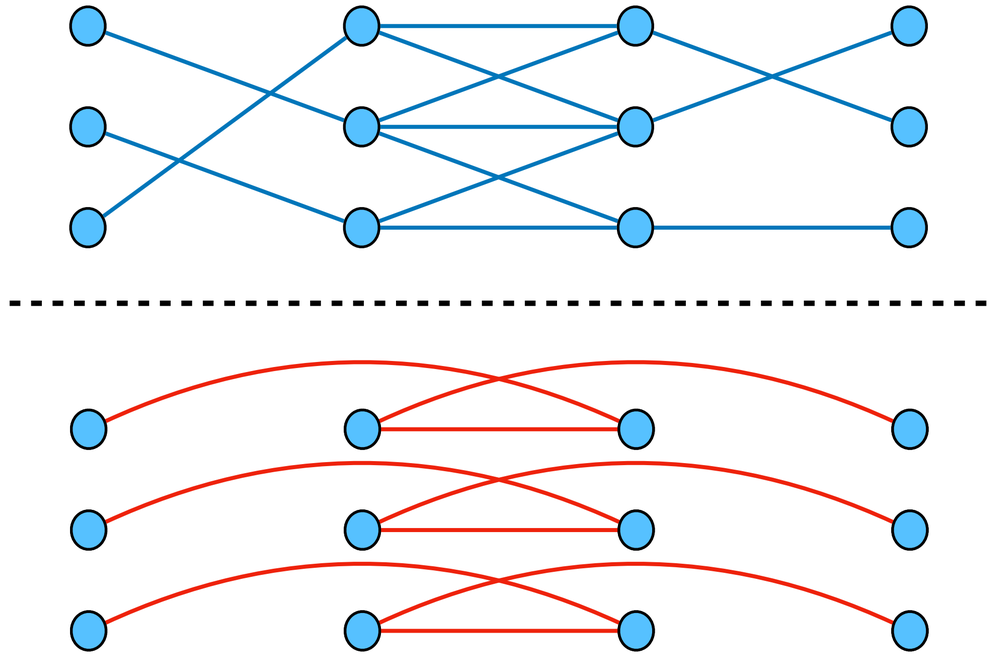
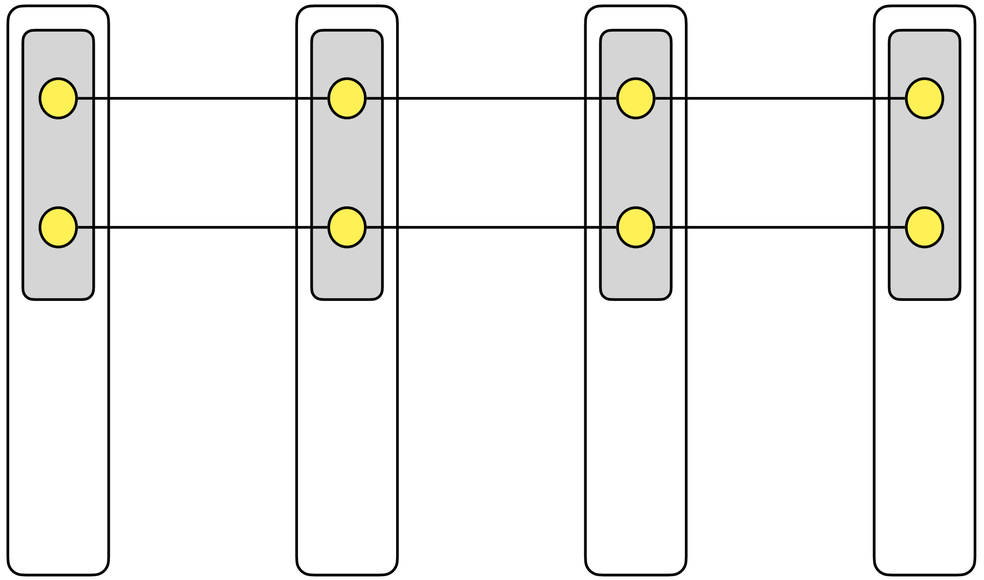


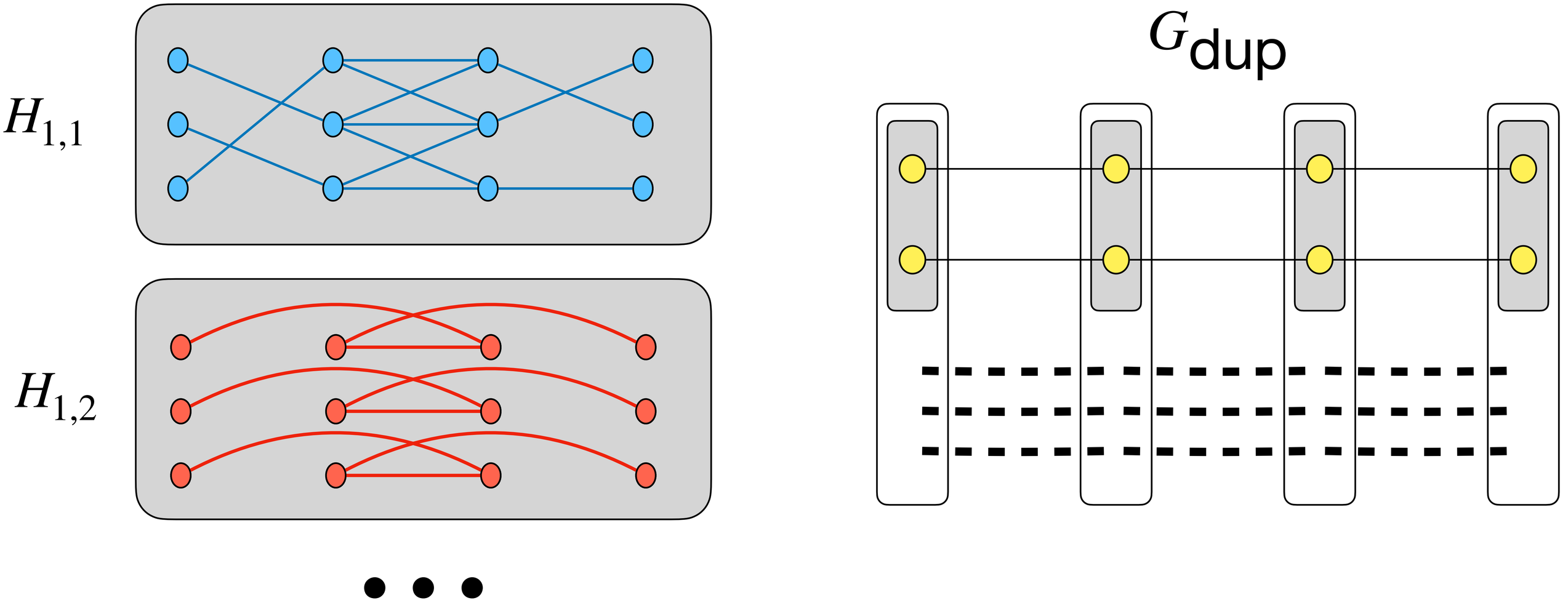

START($P$)
$P$
FINAL($P$)



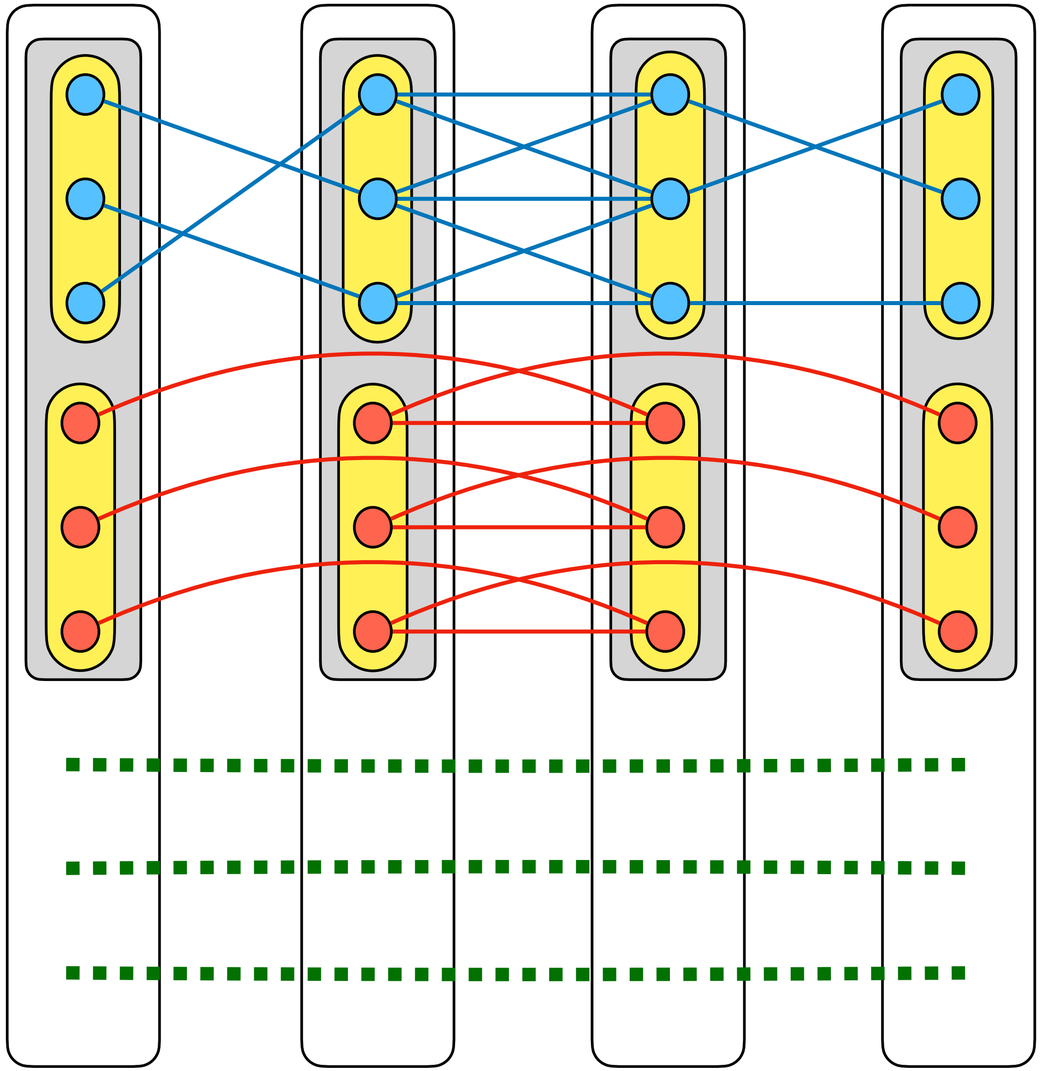

$x \in [\ell]^d$
$y_1 \in A$
$y_2 \in A$
$y_3 \in A$
$y_1$
$y_2$
$y_3$
$y_1$
$y_2$
$y_3$
$y_1$
$y_2$
$y_3$
$y_1$
$y_2$
$y_3$
$y'_1$
$y'_2$
$y'_3$
$y'_4$

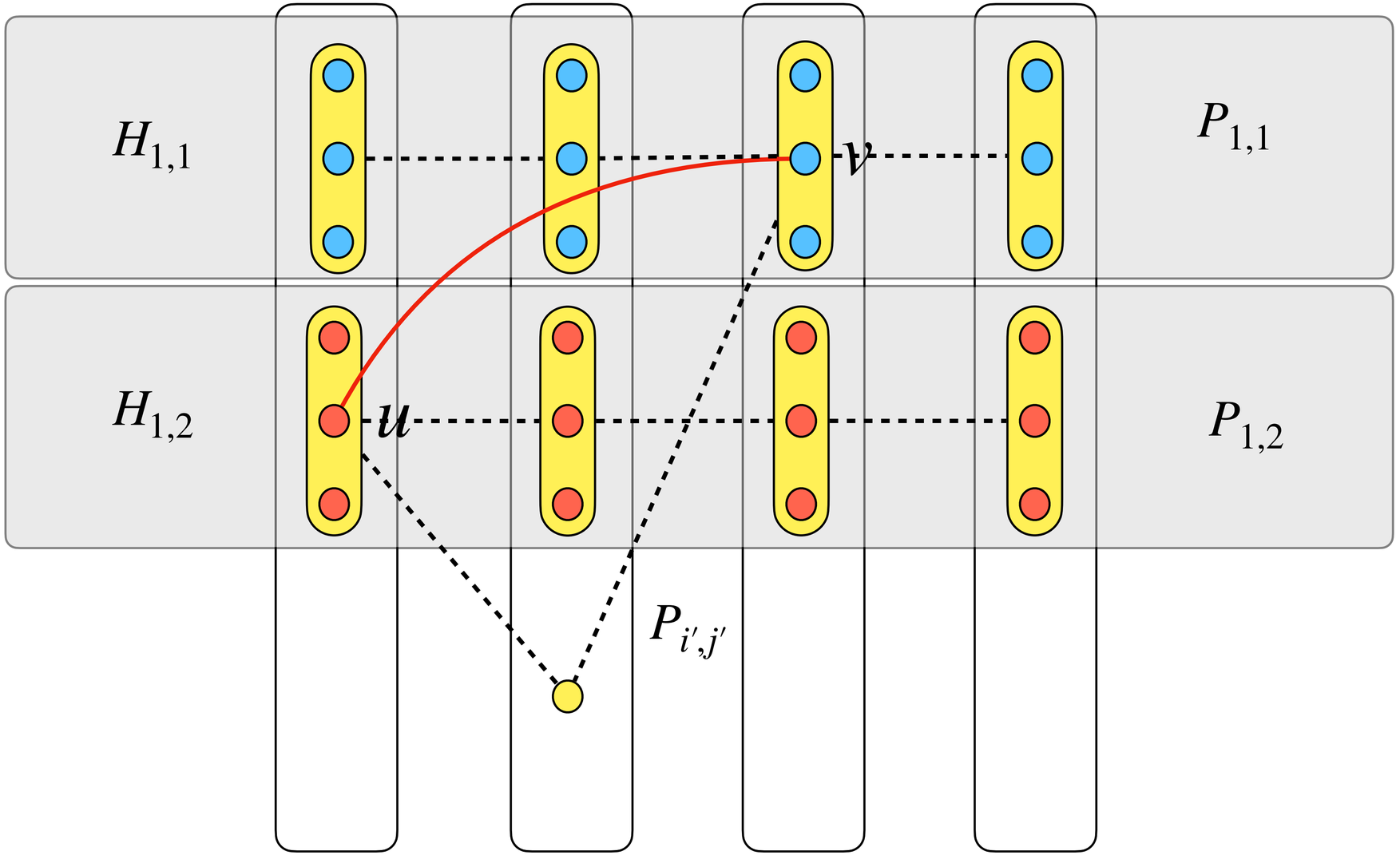


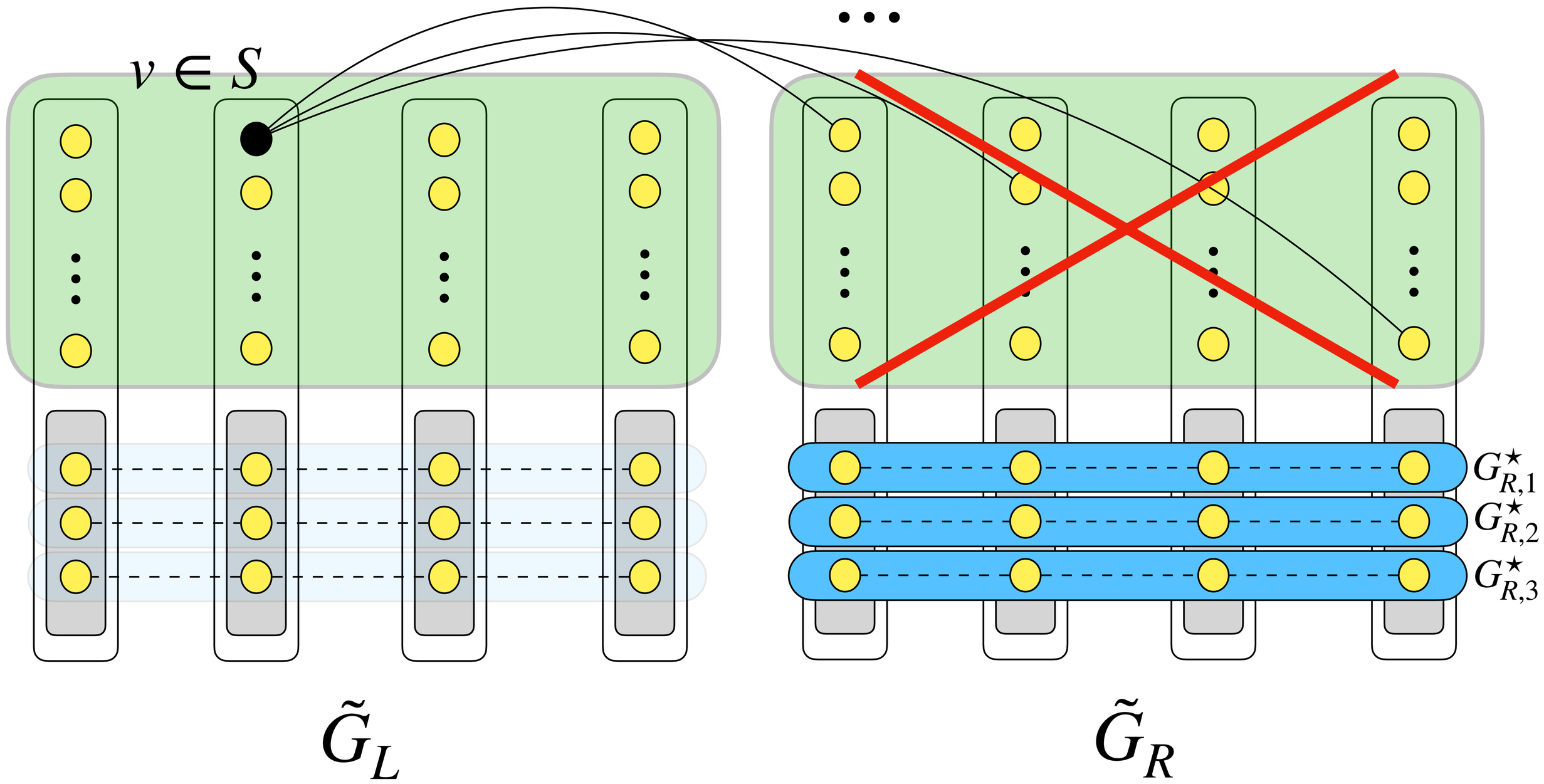


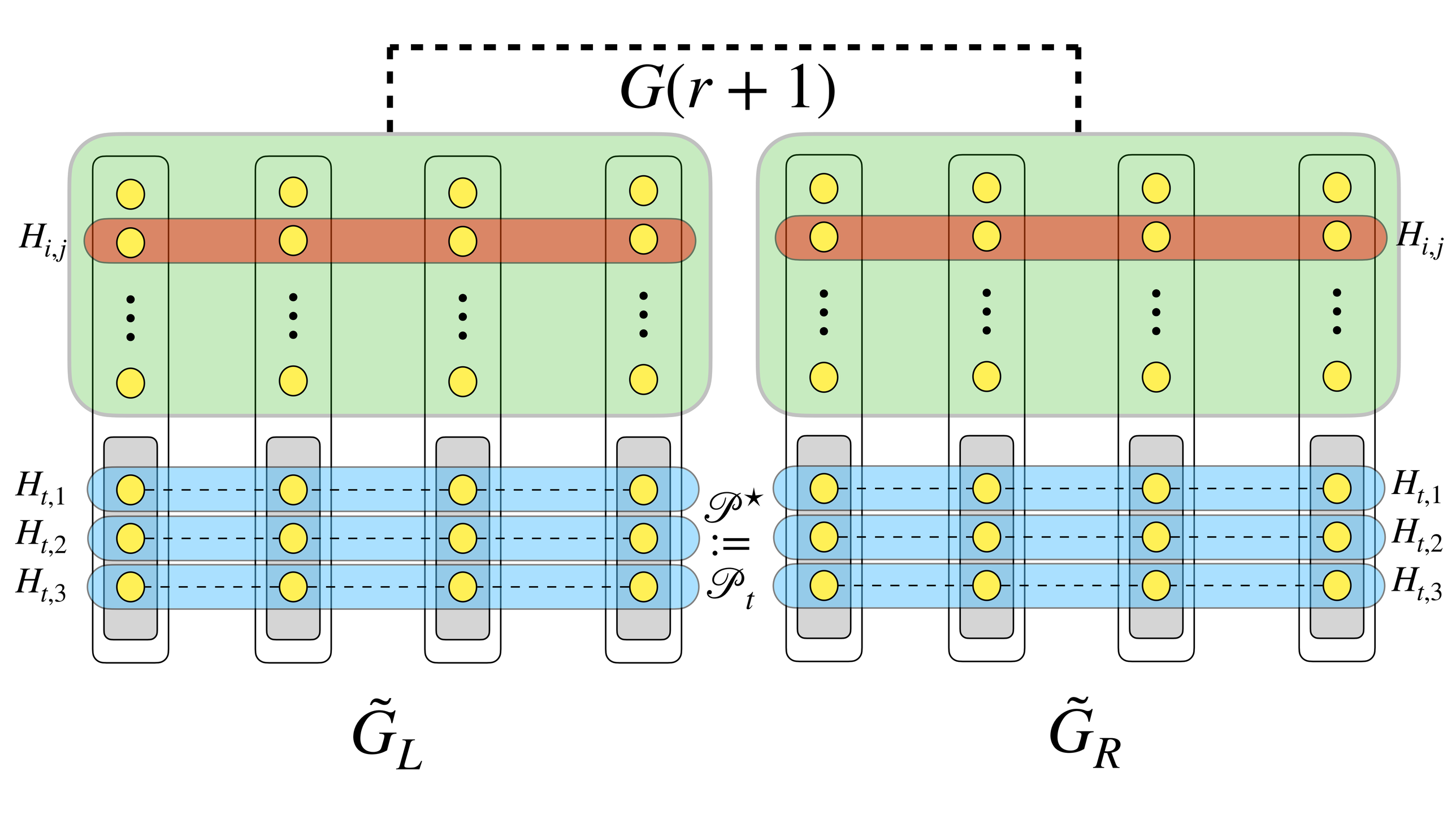

$H_{1,1}$
$H_{1,2}$
$G_{\mathrm{dup}}$

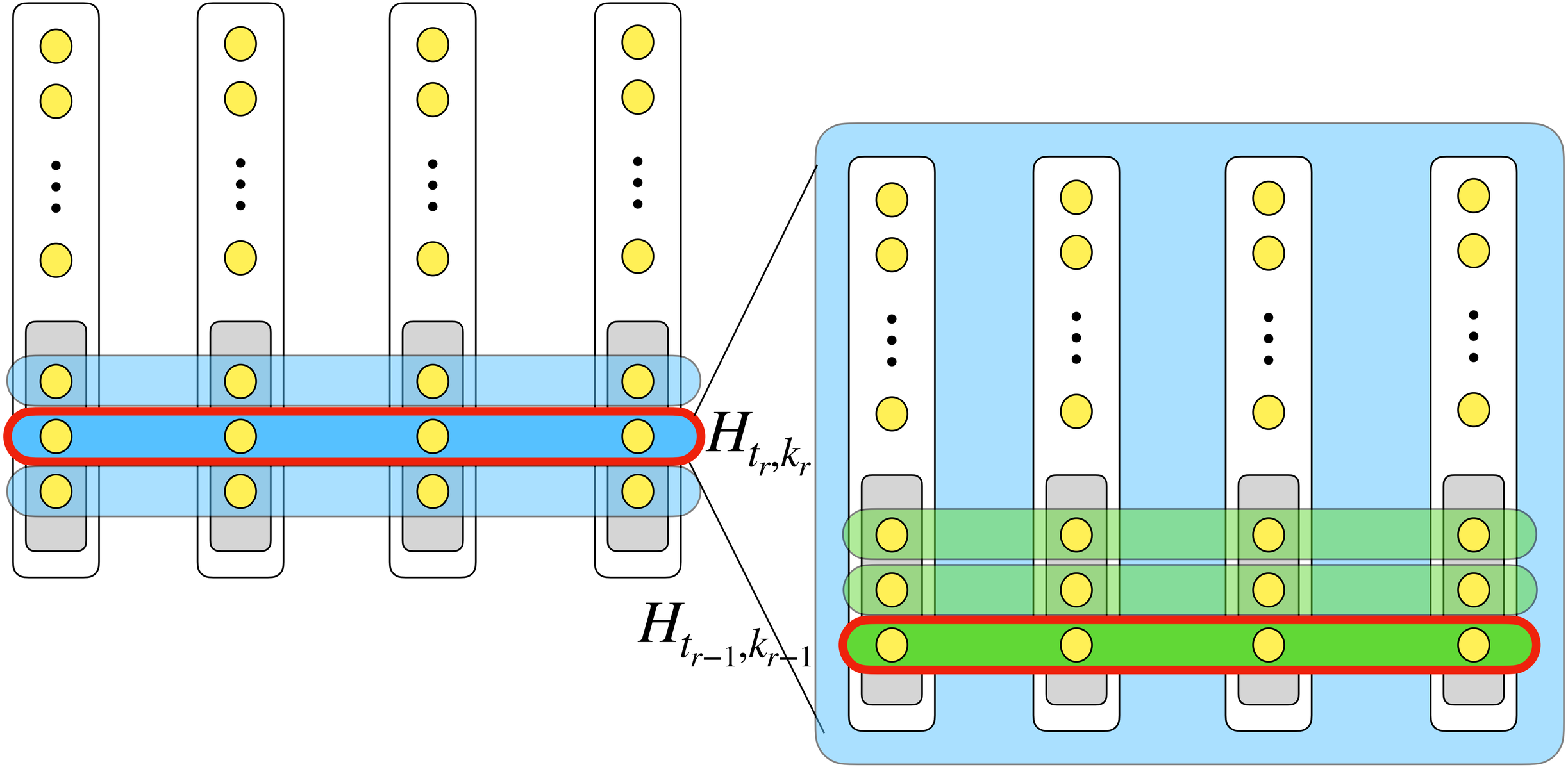
embed($\mathscr{H} \to G_{\text{dup}}$)




$H_{1,1}$
$H_{1,2}$
$P_{1,1}$
$P_{1,2}$
$u$
$v$
$P_{i',j'}$


$v \in S$
$\cdots$
$G^{\star}_{R,1}$
$G^{\star}_{R,2}$
$G^{\star}_{R,3}$
$\tilde{G}_L$
$\tilde{G}_R$


$G(r+1)$
$H_{i,j}$
$H_{i,j}$
$H_{t,1}$
$H_{t,2}$
$H_{t,3}$
$\mathscr{P}^\star$
$:=$
$\mathscr{P}_t$
$H_{t,1}$
$H_{t,2}$
$H_{t,3}$
$\tilde{G}_L$
$\tilde{G}_R$


$H_{t_r,k_r}$
$H_{t_{r-1},k_{r-1}}$

(1)

$\pi_r \quad \mathbb{F}_r$

$r$-round

$(r+1)$-party

$\mathrm{cc}(\pi_r) = s$

success probability:

$\delta$

(2)

$\sigma \quad \mathbb{F}_{r-1}$

$r$-round

$r$-party

$\mathrm{ic}(\sigma, \mathcal{G}_{r-1}) \leqslant \frac{s}{p_r}$

success probability:

$\delta$

(3)

$\pi' \quad \mathbb{F}_{r-1}$

$r$-round

$r$-party

$\mathrm{cc}(\pi') \lesssim \frac{s}{p_r \cdot \varepsilon}$

success probability:

$\delta - \varepsilon$

(4)

$\pi_{r-1}$ $\mathbb{F}_{r-1}$

---

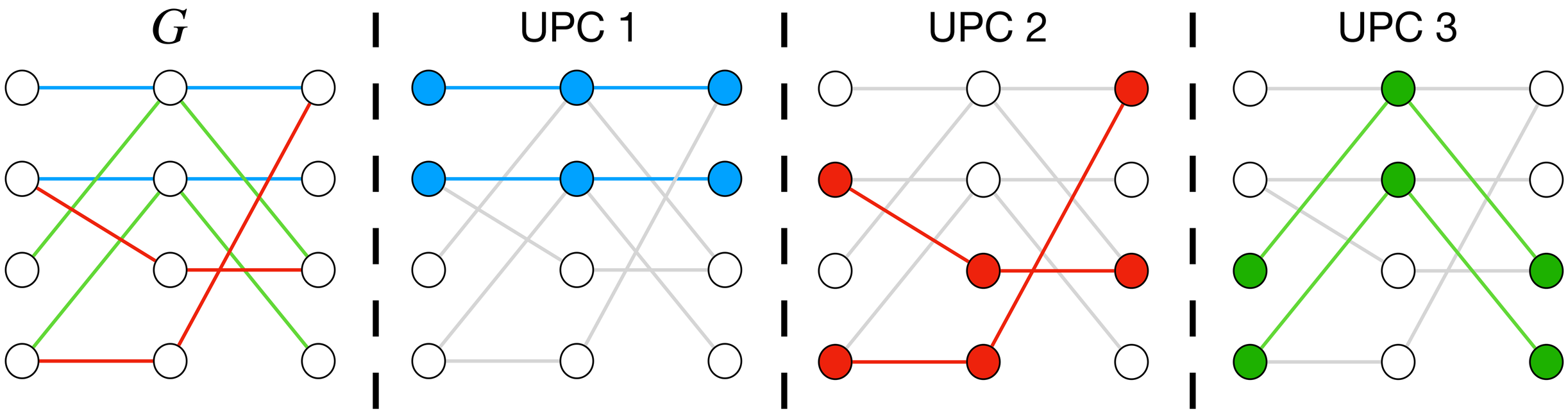
$(r-1)$-round

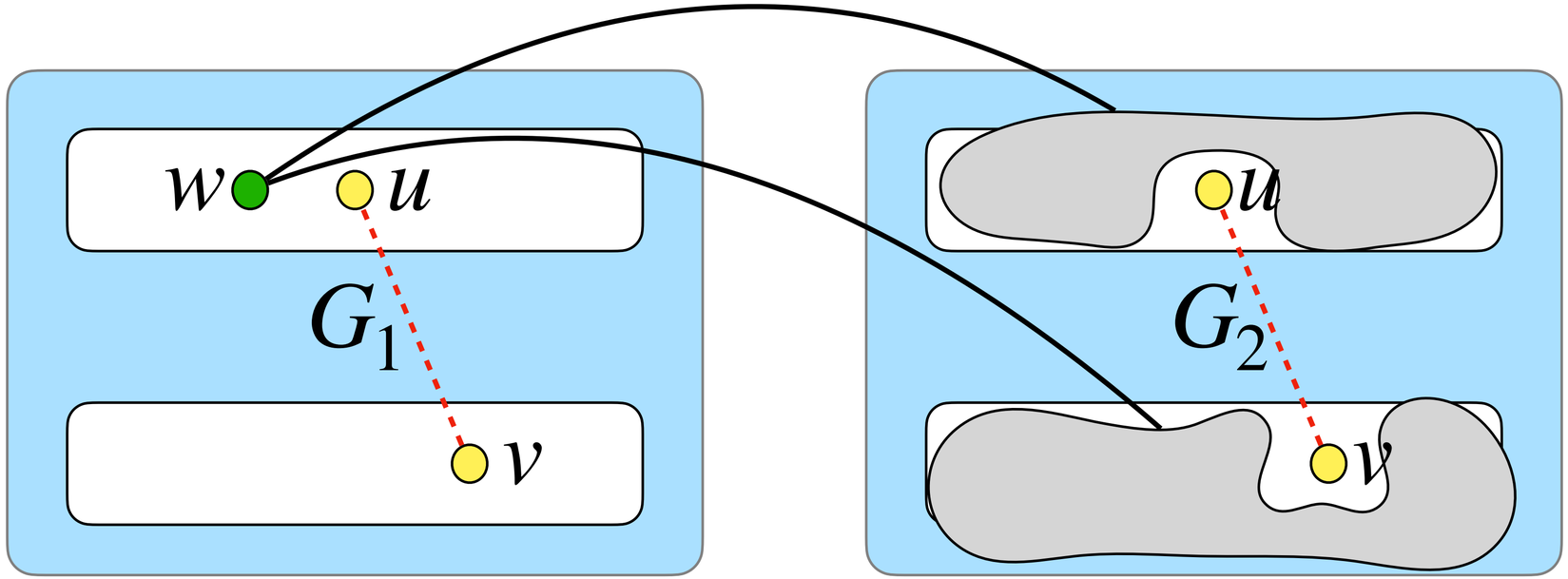
$r$-party

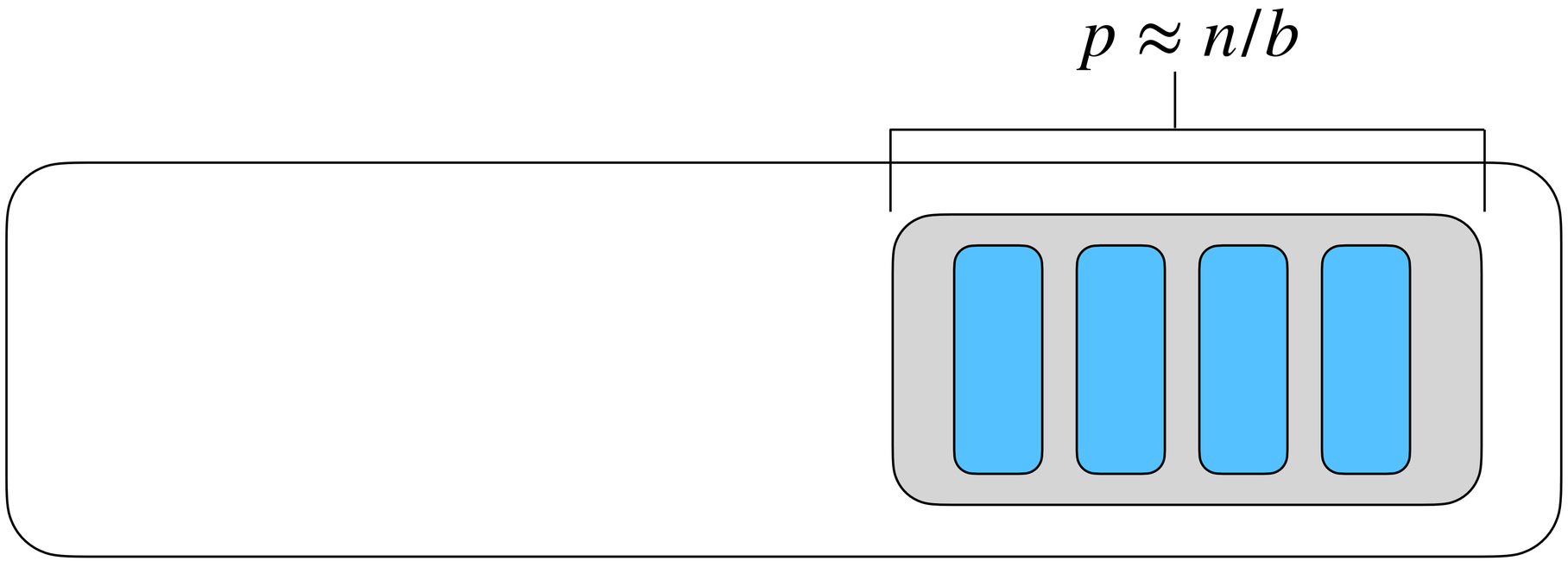
$$\mathrm{cc}(\pi') \lesssim \frac{s}{p_r \cdot \varepsilon}$$

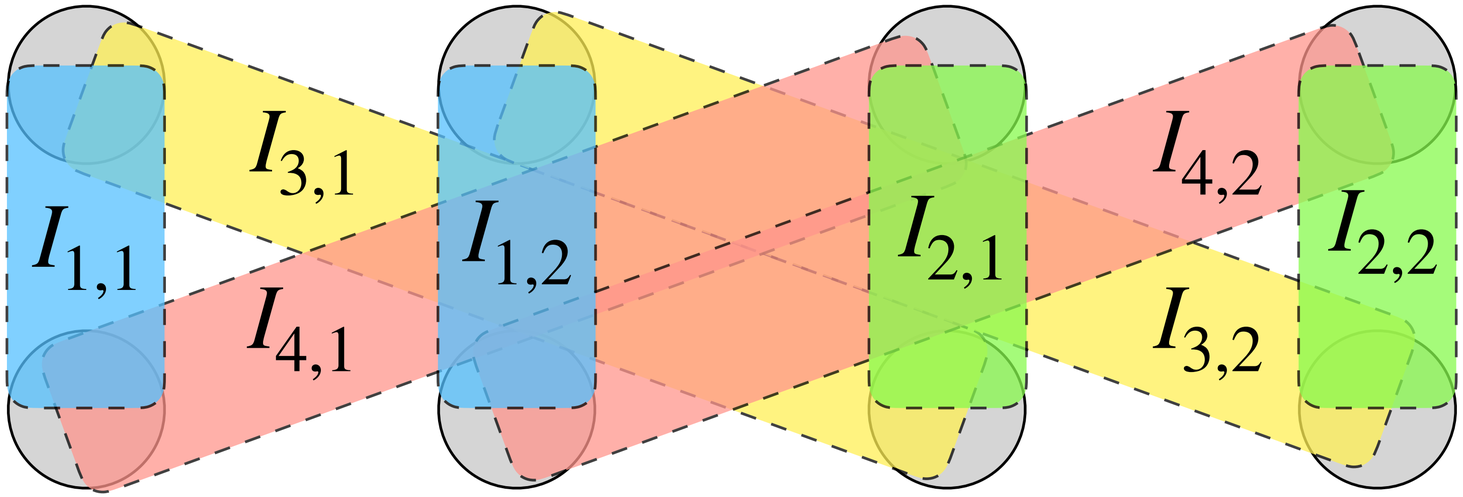
success probability:

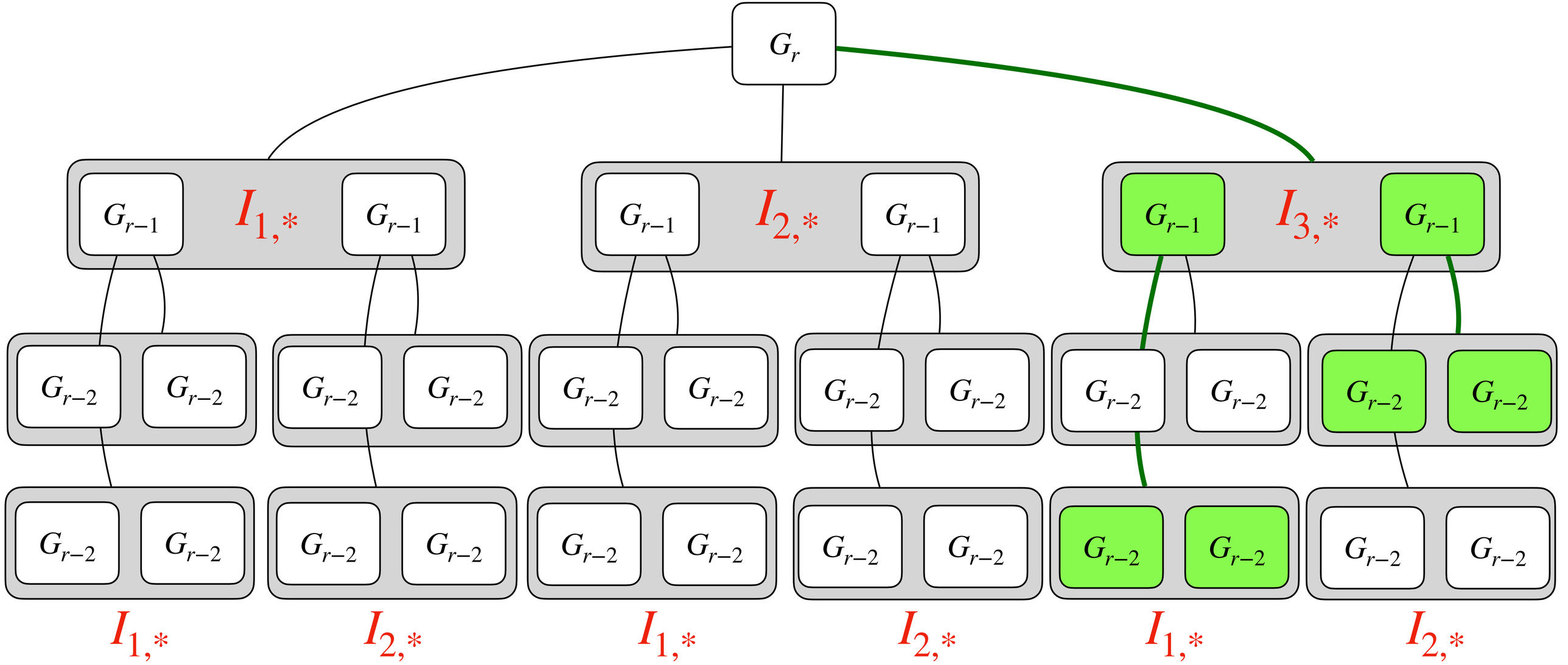
$$\delta - \varepsilon - \sqrt{\frac{s}{p_r \cdot q_r}}$$

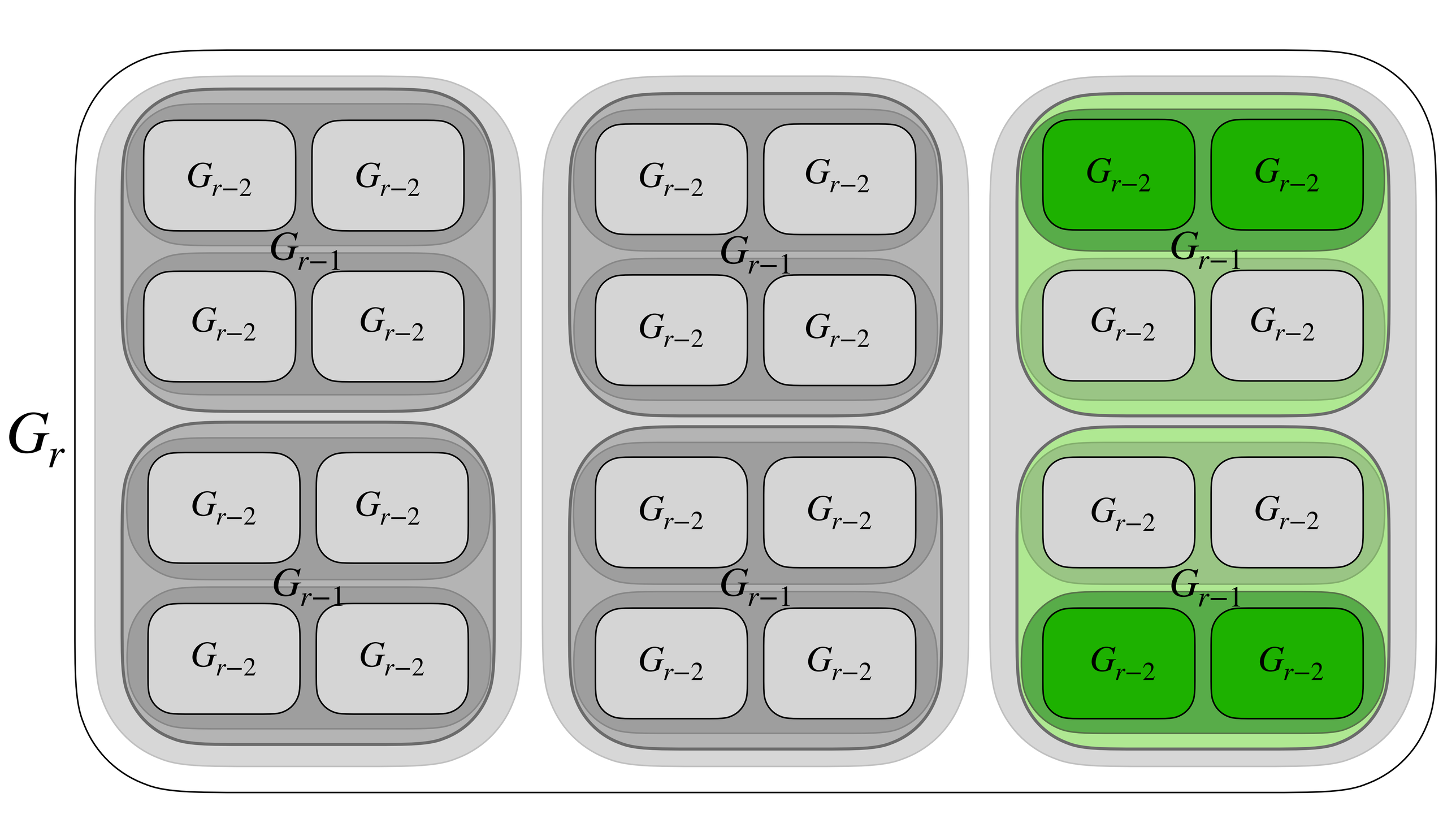

$G$
UPC 1
UPC 2
UPC 3

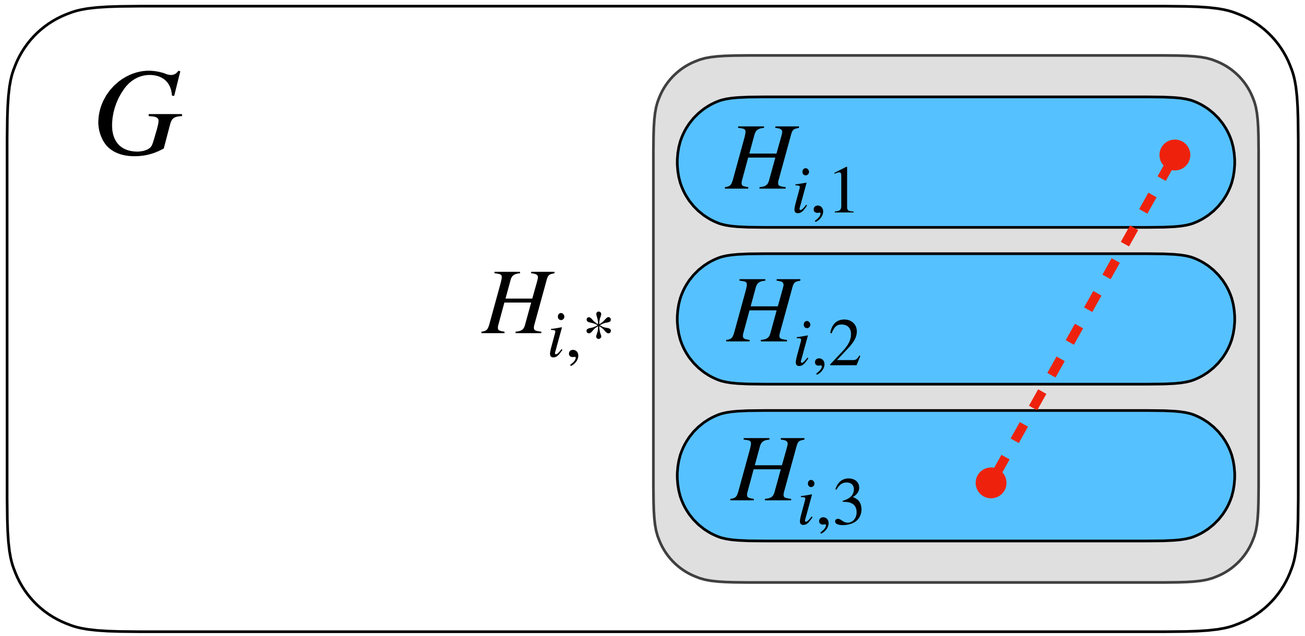

w
u
$G_1$
v
u
$G_2$
v


$p \approx n/b$


$I_{1,1}$
$I_{3,1}$
$I_{4,1}$
$I_{1,2}$
$I_{2,1}$
$I_{4,2}$
$I_{3,2}$
$I_{2,2}$


$G_r$
$G_{r-1}$ $I_{1,*}$ $G_{r-1}$
$G_{r-1}$ $I_{2,*}$ $G_{r-1}$
$G_{r-1}$ $I_{3,*}$ $G_{r-1}$
$G_{r-2}$ $G_{r-2}$
$G_{r-2}$ $G_{r-2}$
$G_{r-2}$ $G_{r-2}$
$G_{r-2}$ $G_{r-2}$
$G_{r-2}$ $G_{r-2}$
$G_{r-2}$ $G_{r-2}$
$G_{r-2}$ $G_{r-2}$
$G_{r-2}$ $G_{r-2}$
$G_{r-2}$ $G_{r-2}$
$G_{r-2}$ $G_{r-2}$
$I_{1,*}$
$I_{2,*}$
$I_{1,*}$
$I_{2,*}$
$I_{1,*}$
$I_{2,*}$


$G_r$
$G_{r-1}$
$G_{r-2}$


$G$
$H_{i,*}$
$H_{i,1}$
$H_{i,2}$
$H_{i,3}$