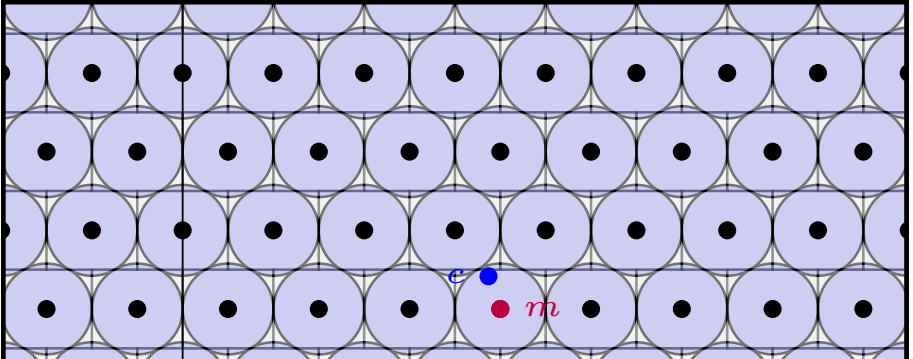

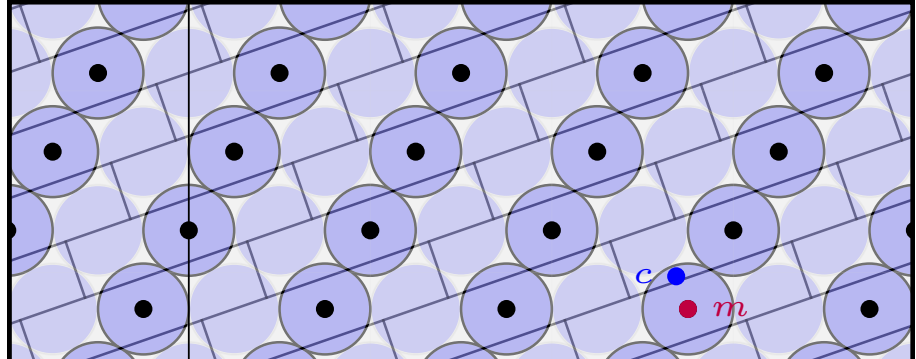

$\text{sk} = \boldsymbol{B}$

$\text{pk} = \boldsymbol{H}$, s.t $\mathcal{L}(\boldsymbol{H}) \subset \mathcal{L}(\boldsymbol{B})$