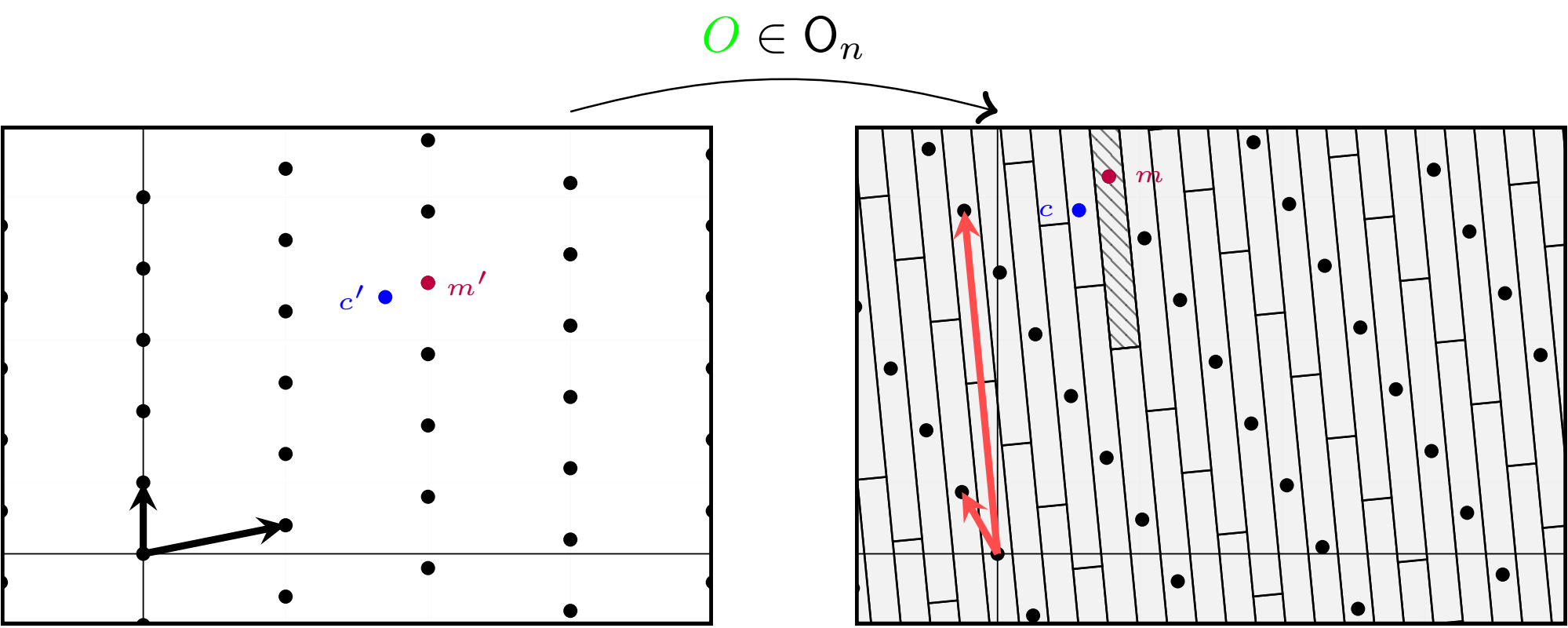

$\mathrm{sk} = O \in \mathsf{O}_n$

$\mathrm{pk} = \boldsymbol{B'}$, s.t $\mathcal{L}(\boldsymbol{B'}) = O \cdot \mathcal{L}(\boldsymbol{B})$