MMB$_1$

O_1^0 $\cdots$ O_1^s

Input data

Iteration

State

M_1

PMB$_1$

MAC_1 Input
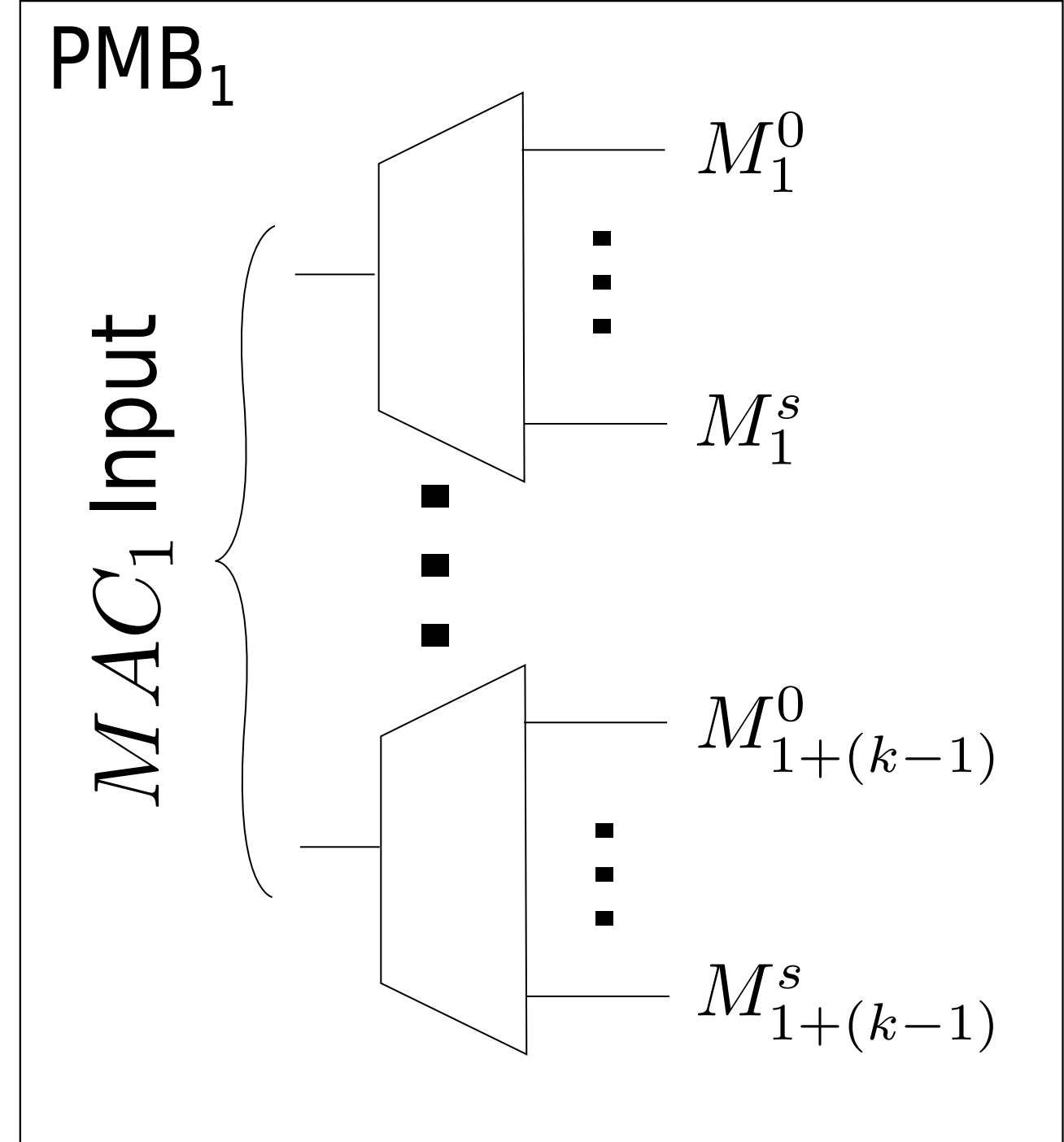
M_1^0

M_1^s

$M_{1+(k-1)}^0$

$M_{1+(k-1)}^s$

$$O_j^i = O_{[(k-1)i+j]\%N}$$

$$M_j^i = M_{(iN+j)\%(N+k-1)}$$