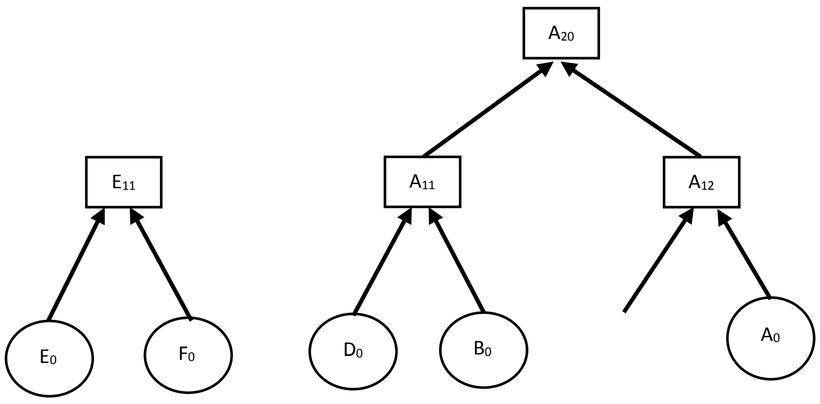
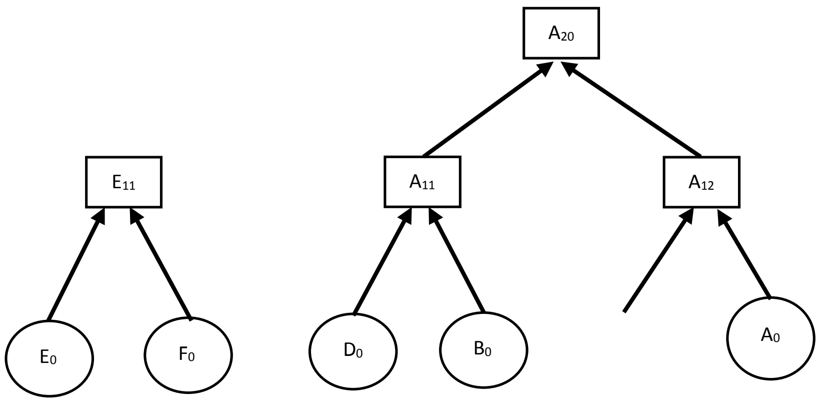


Root commitment = $A_{20} \oplus E_{11}$

$A_{20} = A_{11} \oplus A_{12}$

$A_{12} = A_0 \oplus C_0$

$A_0 = MAC_{KA}(N \,||\, ACK)$



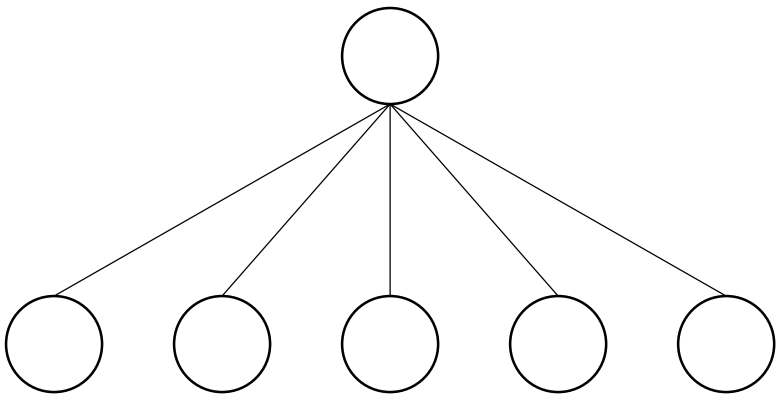
Root commitment = $A_{20} \oplus E_{11}$

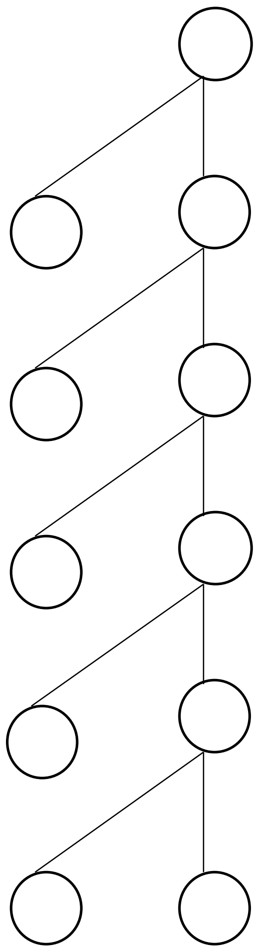
$A_{20} = A_{11} \oplus A_{12}$

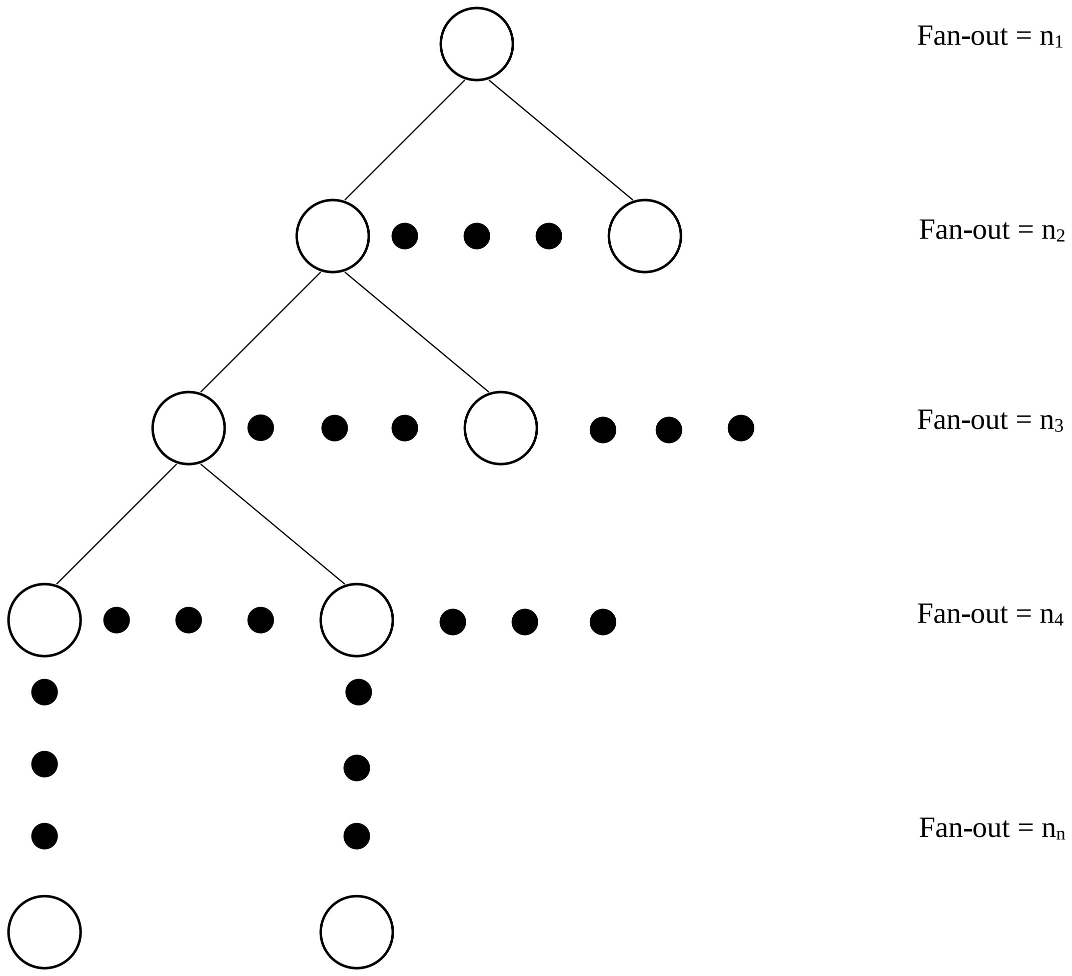
$A_{12} = A_0 \oplus C_0$

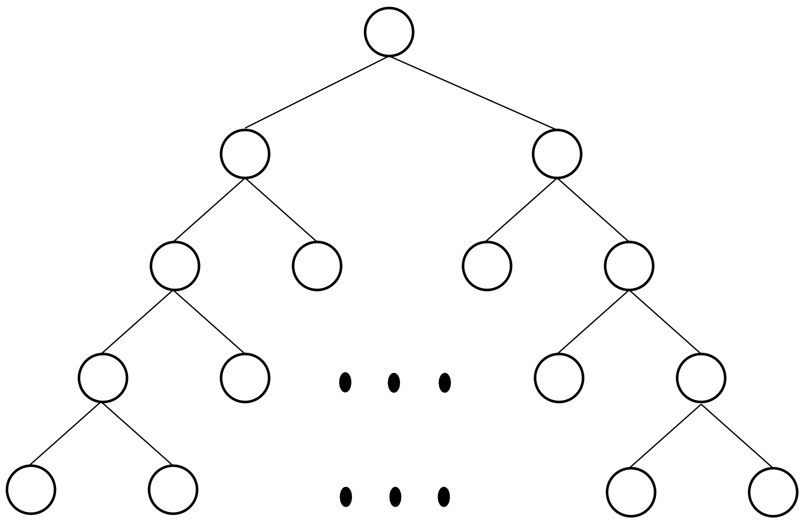
$A_0 = MAC_{KA}(N \,||\, NACK)$

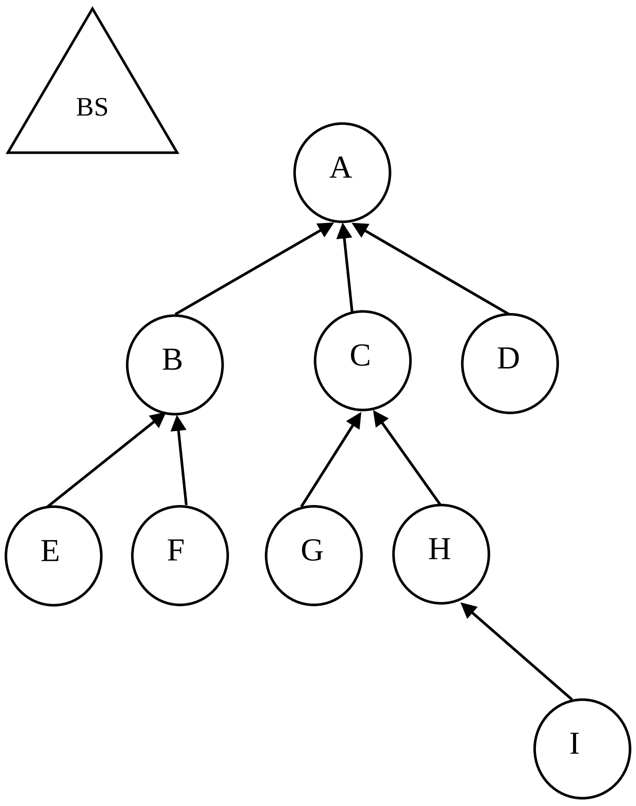
Aggregation tree

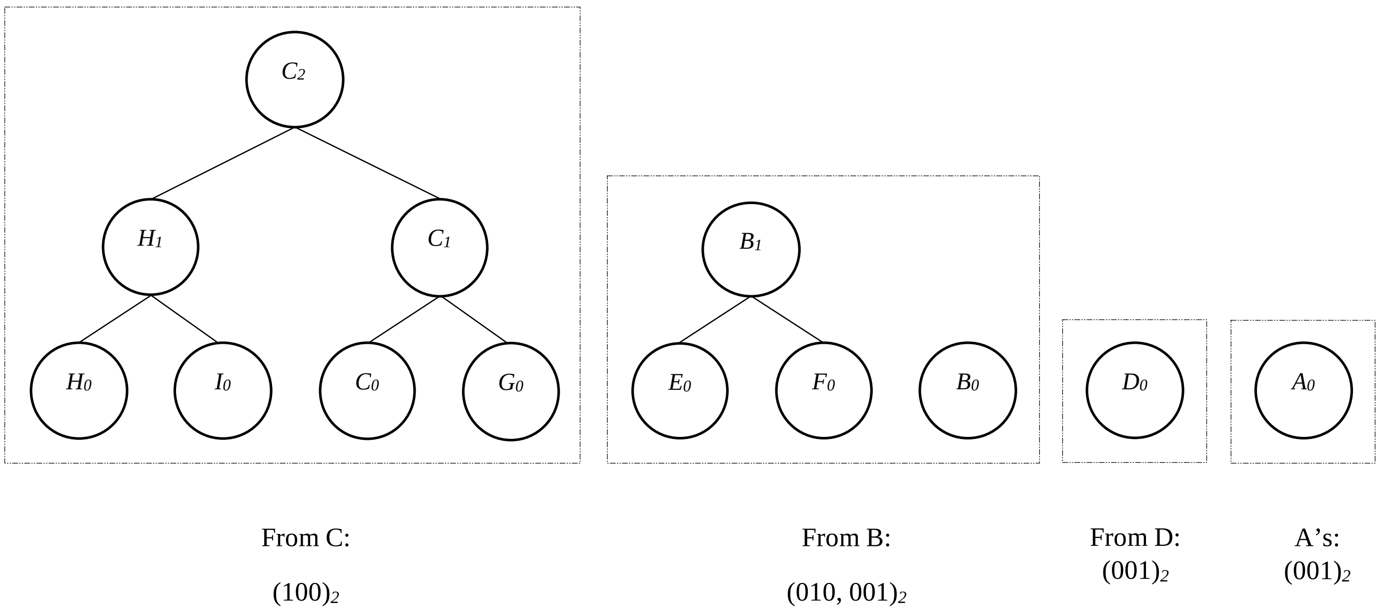





Fan-out = n_1
Fan-out = n_2
Fan-out = n_3
Fan-out = n_4
Fan-out = n_n




BS
A
B
C
D
E
F
G
H
I



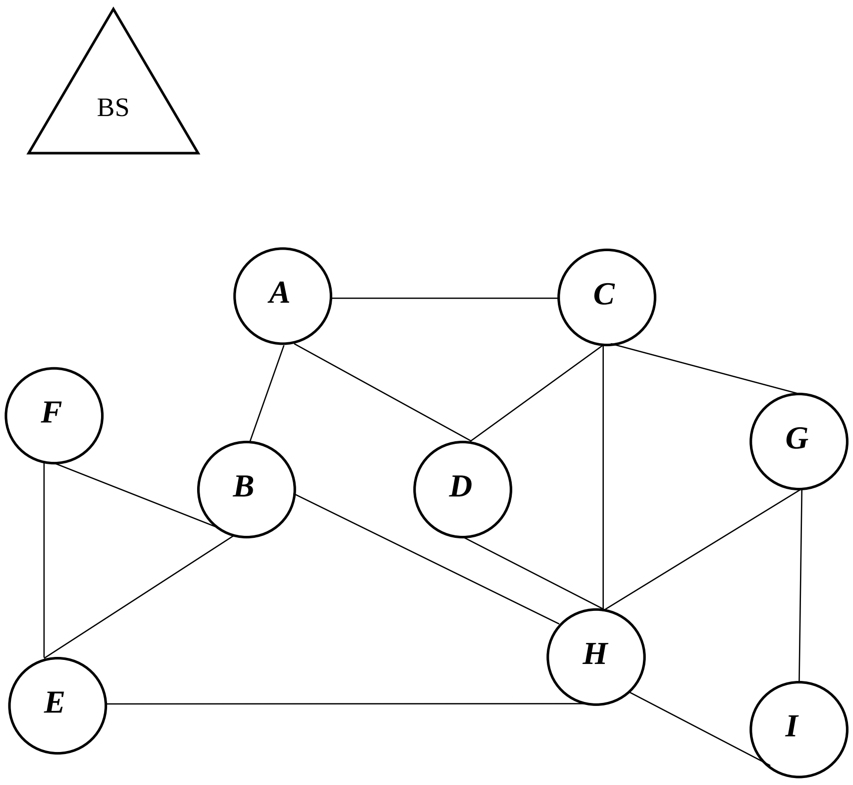
$\mathbf{C_2 = < C.id, 4, C_2.value, H\ [\ N \,||\, C.id \,||\, 4 \,||\, C_2.value\ ] >}$

$\mathbf{B_1 = < B.id, 2, B_1.value, H\ [\ N \,||\, B.id \,||\, 2 \,||\, B_1.value\ ] >}$

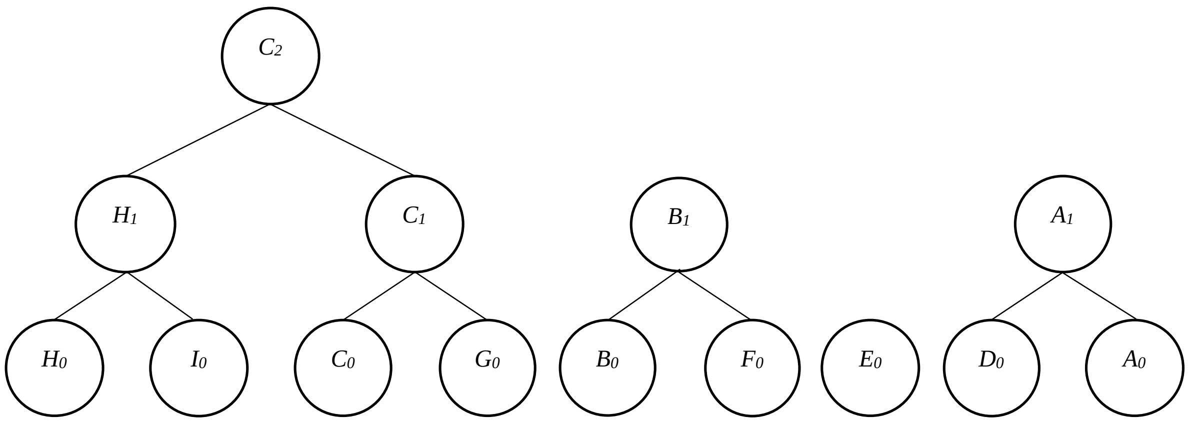
$\mathbf{H_0 = < H.id, 1, H.value, H\ [\ N \,||\, H.id \,||\, 1 \,||\, H.value\ ] >}$

$\mathbf{D_0 = < D.id, 1, D.value, H\ [\ N \,||\, D.id \,||\, 1 \,||\, D.value\ ] >}$

$\mathbf{A_0 = < A.id, 1, A.value, H\ [\ N \,||\, A.id \,||\, 1 \,||\, A.value\ ] >}$

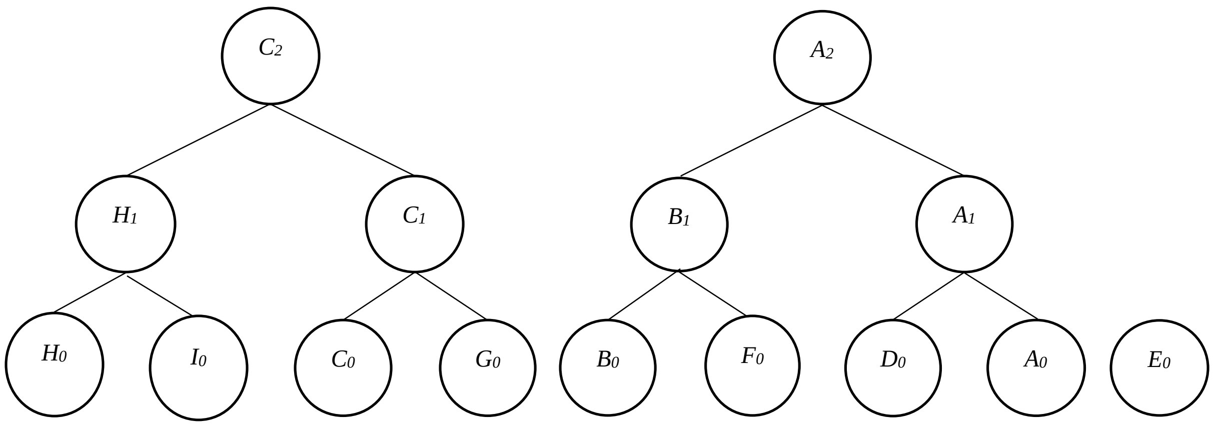

BS
A
C
F
G
B
D
H
E
I

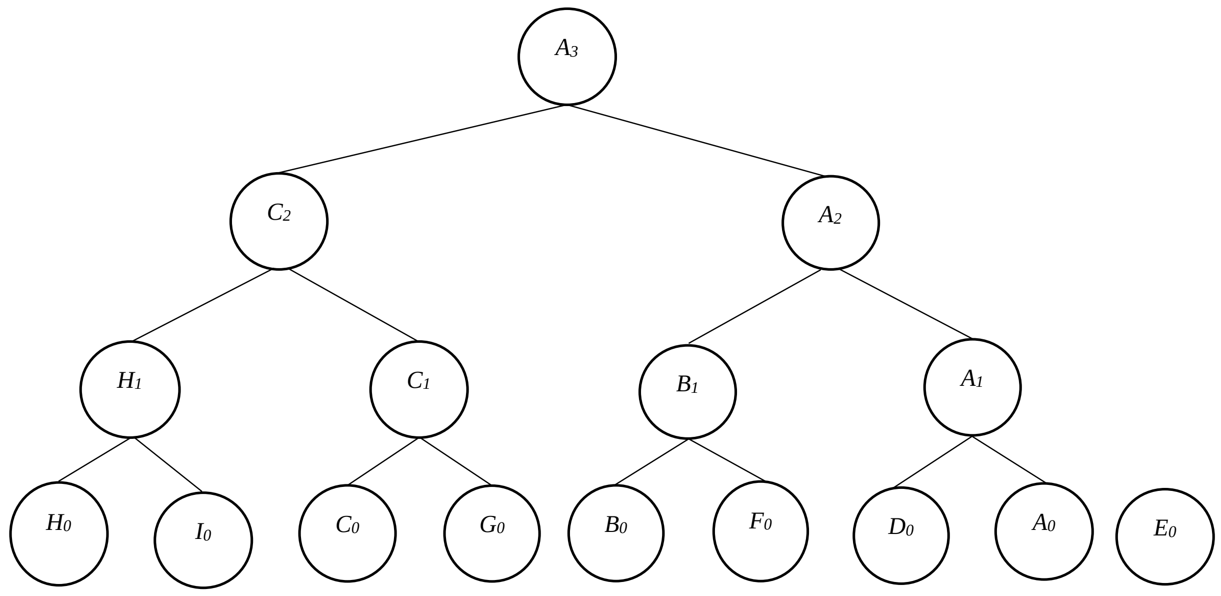
D

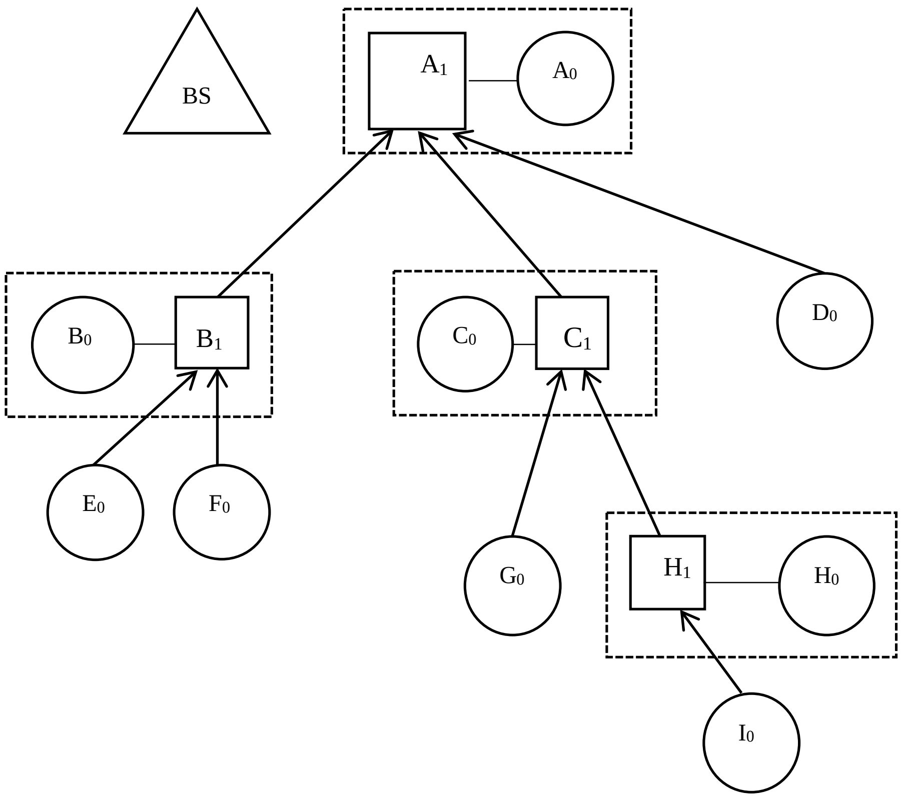


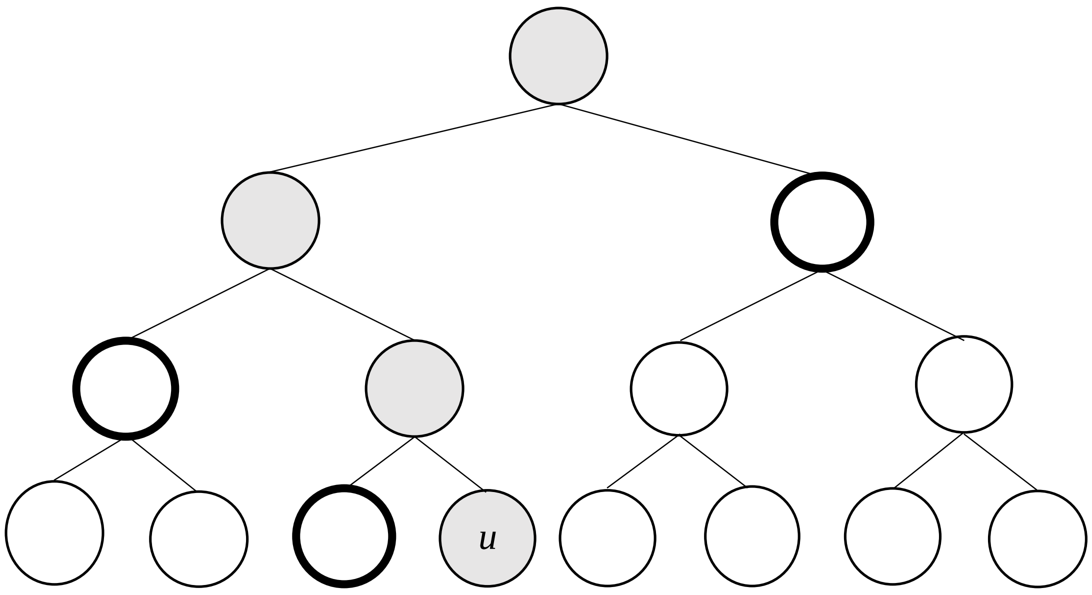
$$\mathbf{A_1.value = A_0.value + D_0.value}$$

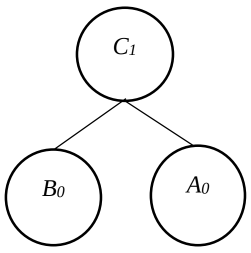
$$\mathbf{A_1 = < A.id,\ 2,\ A_1.value,\ H\ [\ N\ ||\ A.id\ ||\ 2\ ||\ A_1.value\ ||\ A_0\ ||\ D_0]\ >}$$

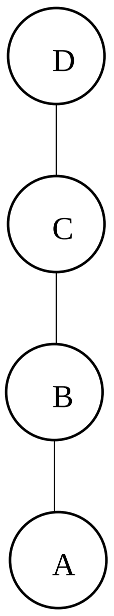

C_2
H_1
C_1
H_0
I_0
C_0
G_0
A_2
B_1
A_1
B_0
F_0
D_0
A_0
E_0

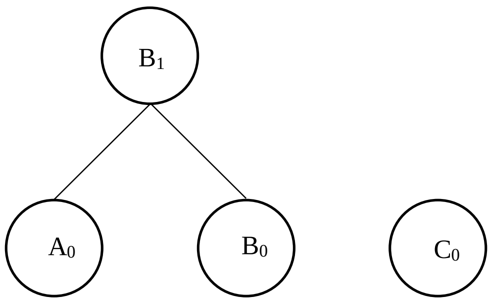

A3
C2
A2
H1
C1
B1
A1
H0
I0
C0
G0
B0
F0
D0
A0
E0

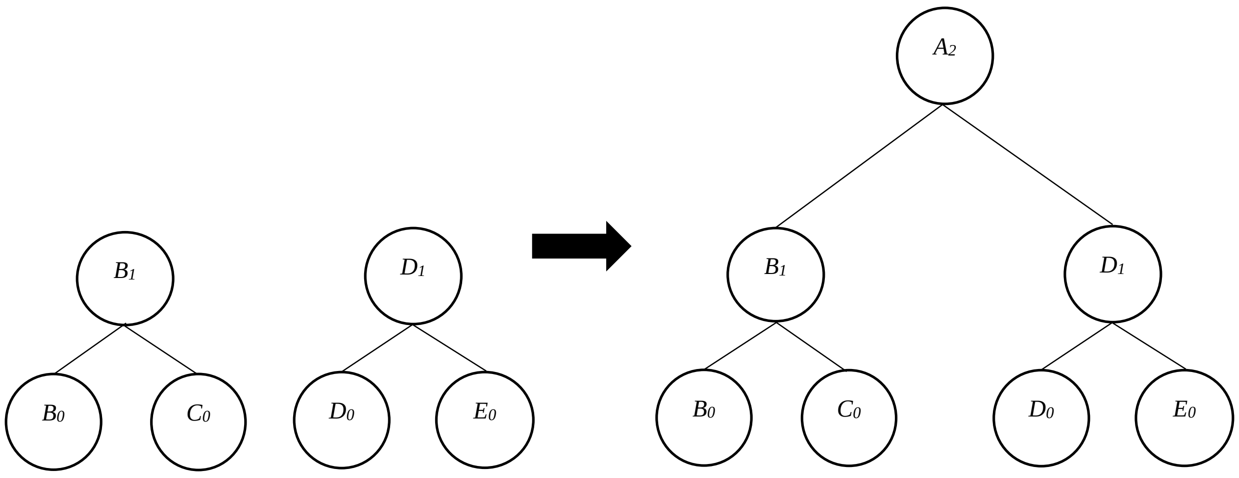

BS
A_1
A_0
B_0
B_1
C_0
C_1
D_0
E_0
F_0
G_0
H_1
H_0
I_0

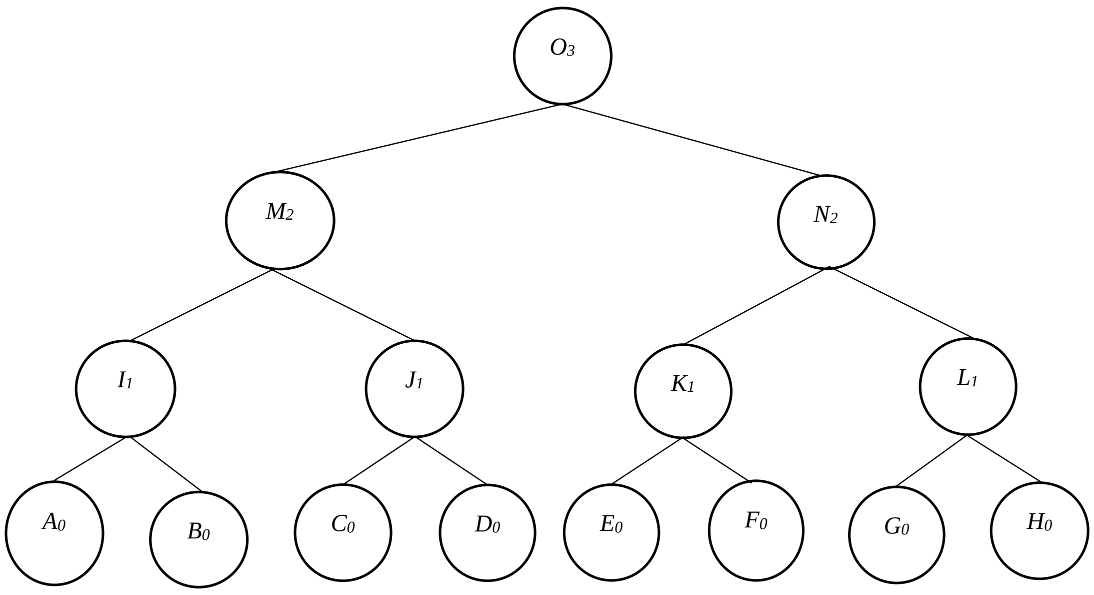

u


C_1
B_0
A_0


D
C
B
A


B_1
A_0
B_0
C_0


B_1
B_0
C_0
D_1
D_0
E_0
A_2
B_1
D_1
B_0
C_0
D_0
E_0


O_3
M_2
N_2
I_1
J_1
K_1
L_1
A_0
B_0
C_0
D_0
E_0
F_0
G_0
H_0