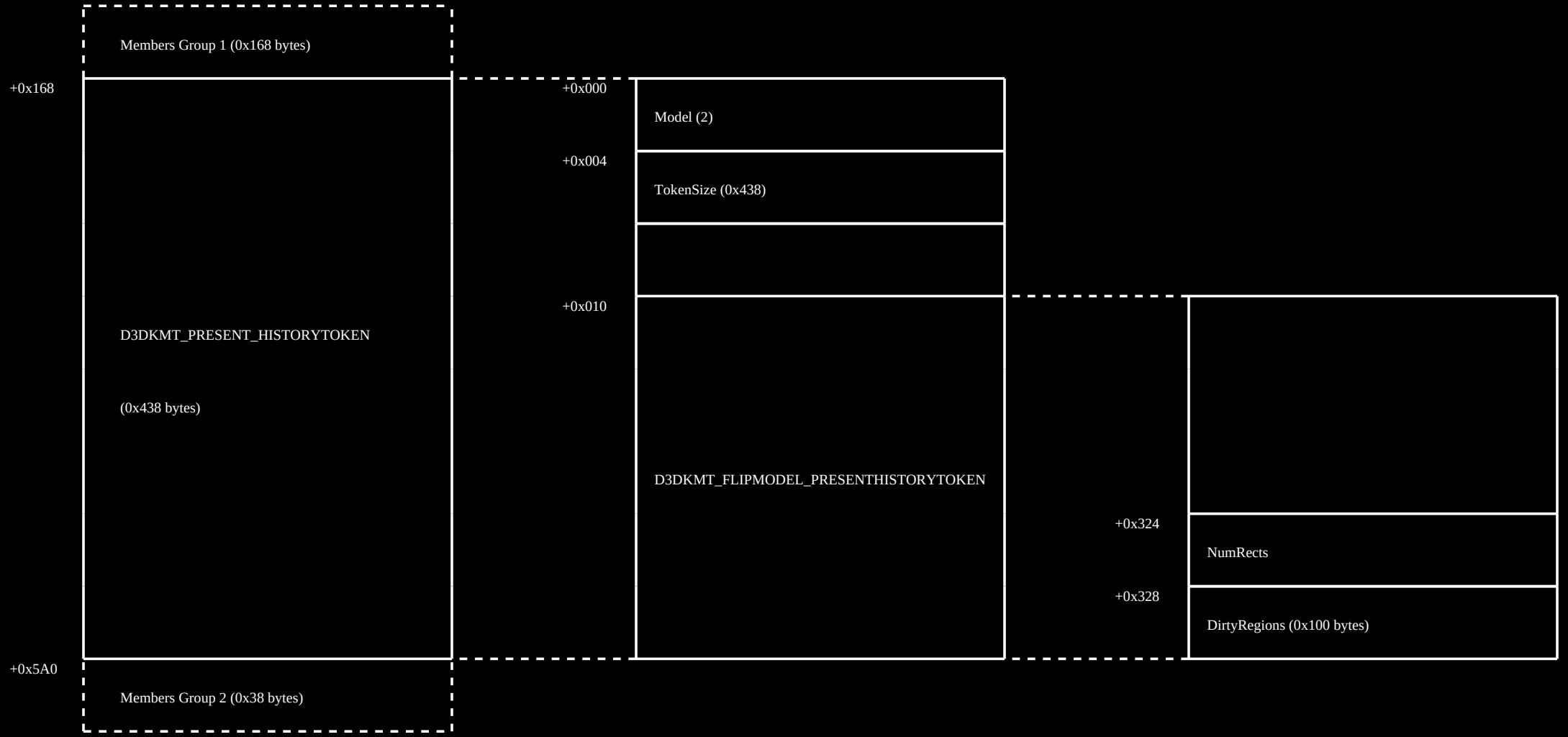
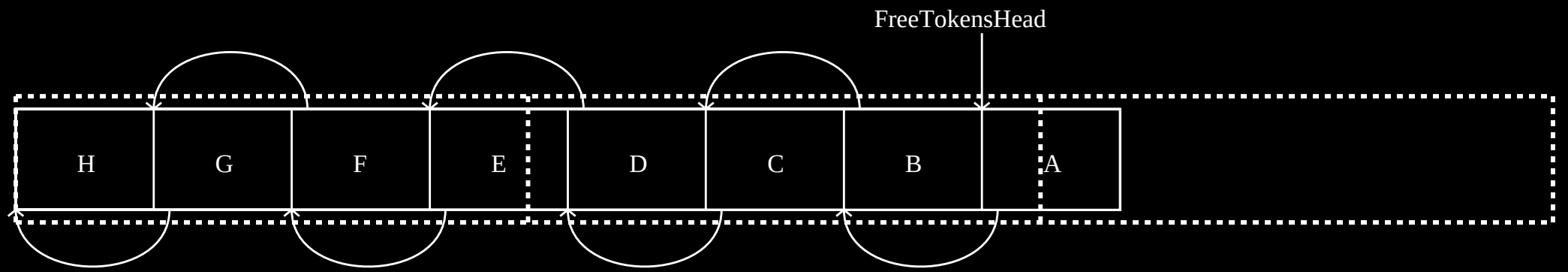
Layout

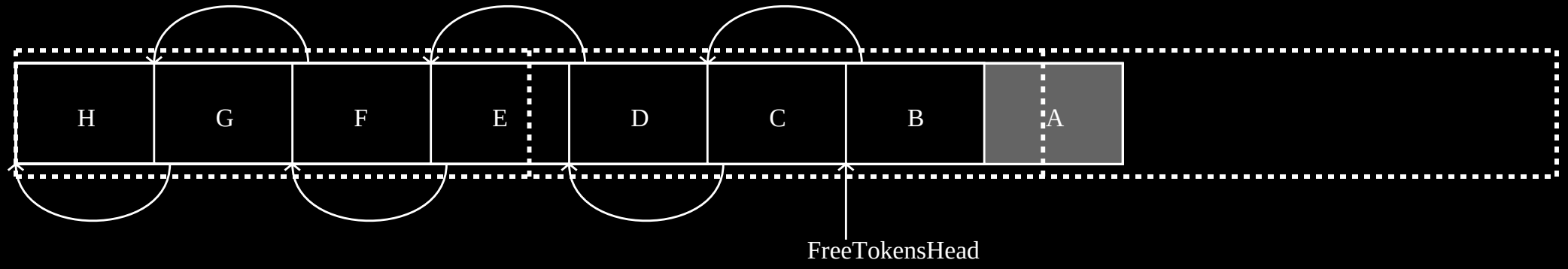

Members Group 1 (0x168 bytes)
+0x168
D3DKMT_PRESENT_HISTORYTOKEN
(0x438 bytes)
+0x5A0
Members Group 2 (0x38 bytes)
+0x000
Model (2)
+0x004
TokenSize (0x438)
+0x010
D3DKMT_FLIPMODEL_PRESENTHISTORYTOKEN
+0x324
NumRects
+0x328
DirtyRegions (0x100 bytes)

Lookaside-like Singly-Linked List of Hist Token



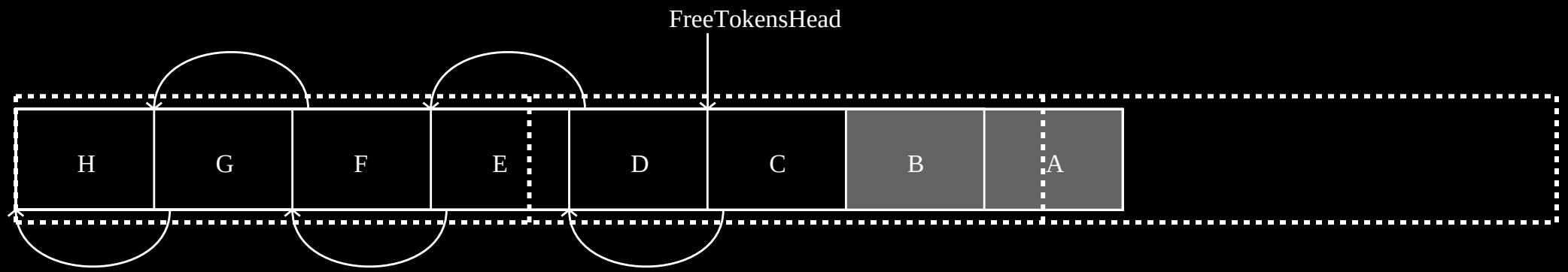
FreeSList: Head -> A -> B -> C -> D -> E -> F -> G -> H

Pop one node out for use (Pop A)



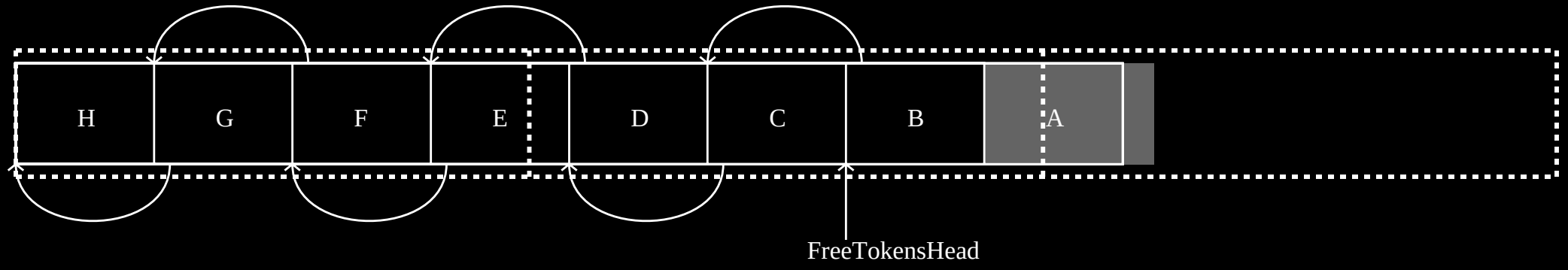
FreeSList: Head -> B -> C -> D -> E -> F -> G -> H

Pop another node out for use (Pop B)



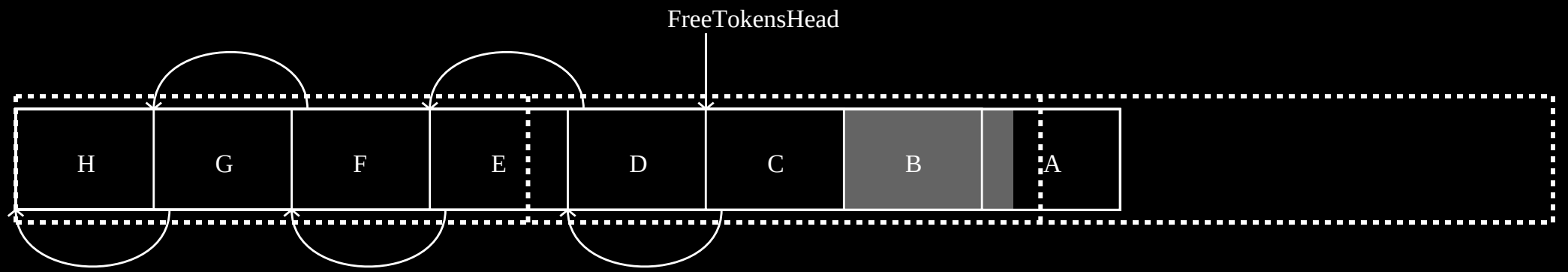
FreeSList: Head -> C -> D -> E -> F -> G -> H

Overflow Scenario 1



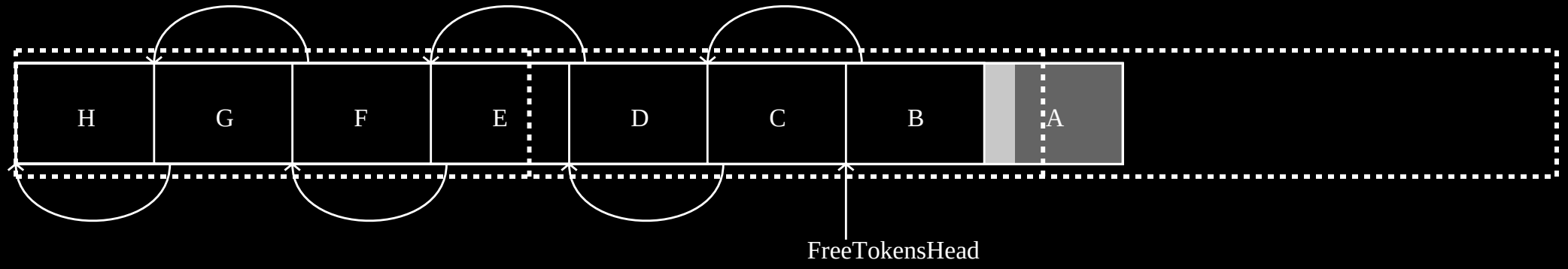
FreeSList: Head -> B -> C -> D -> E -> F -> G -> H

Overflow Scenario 2



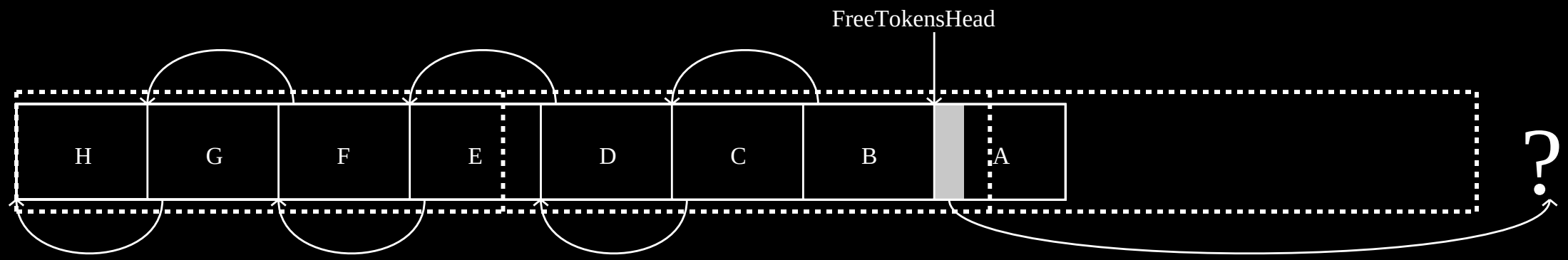
FreeSList: Head -> C -> D -> E -> F -> G -> H

Push node B back after overflow scenario 2



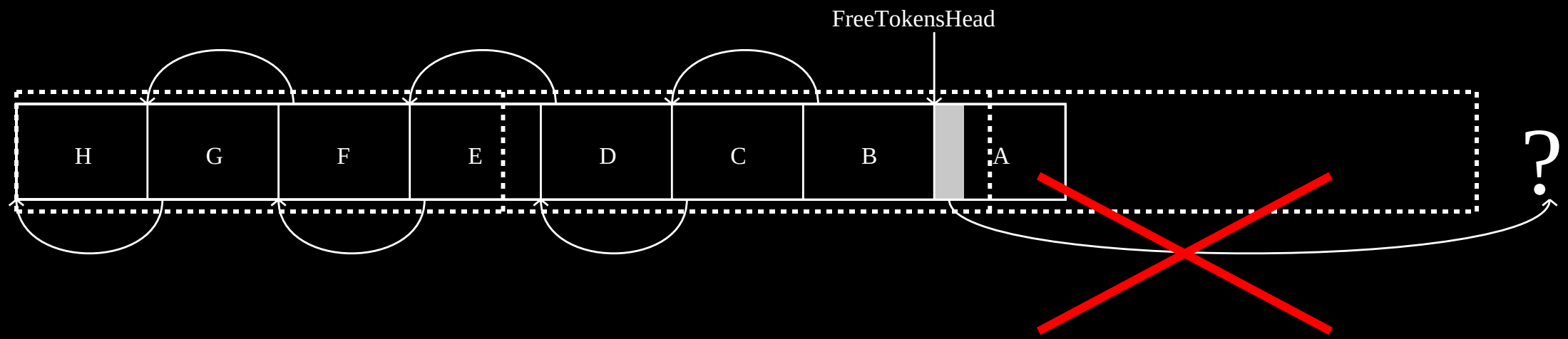
FreeSList: Head -> B -> C -> D -> E -> F -> G -> H

Will this overflow lead to arbitrary write?



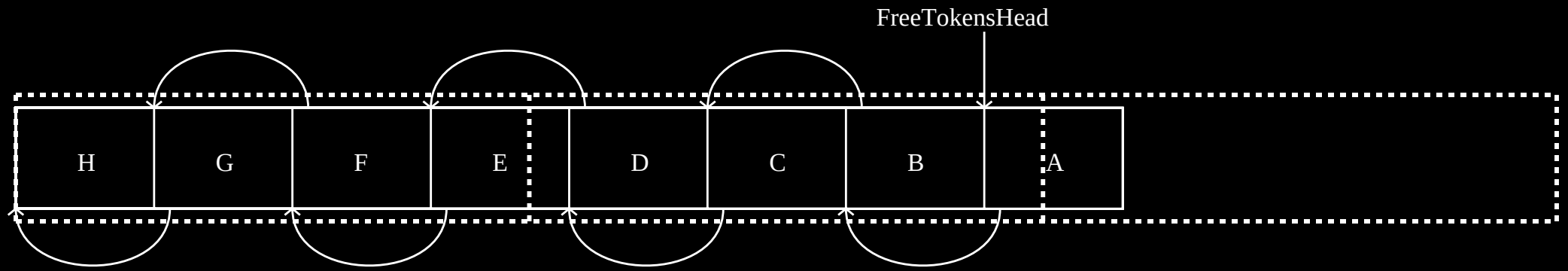
FreeSList: Head -> A -> B -> C -> D -> E -> F -> G -> H

Unfortunately!



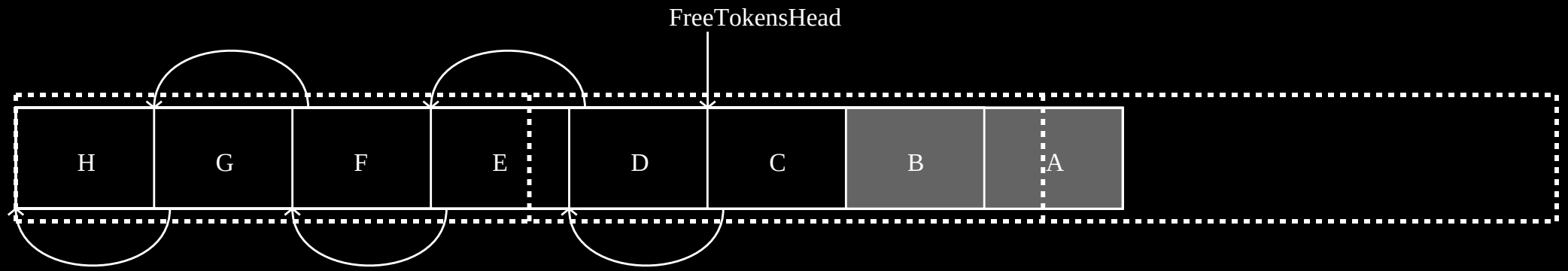
FreeSList: Head -> A -> B -> C -> D -> E -> F -> G -> H

The overwritten ‘Next’ field will be recovered



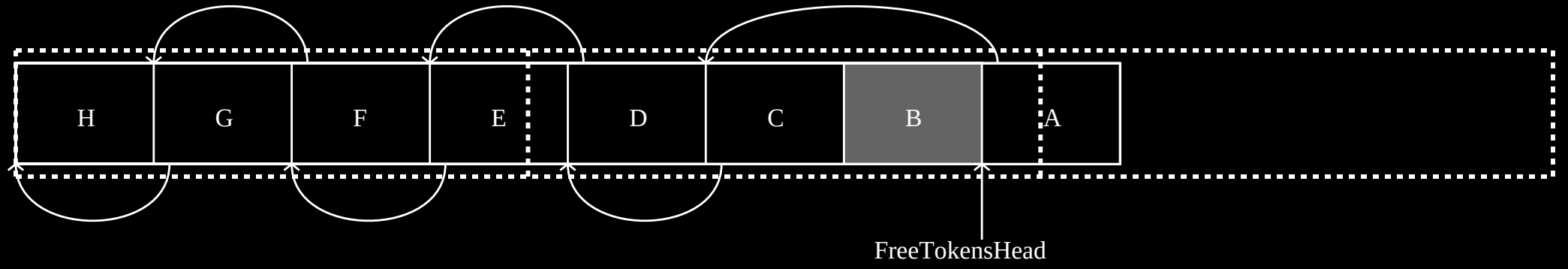
FreeSList: Head -> A -> B -> C -> D -> E -> F -> G -> H

Back to where after 2 pops



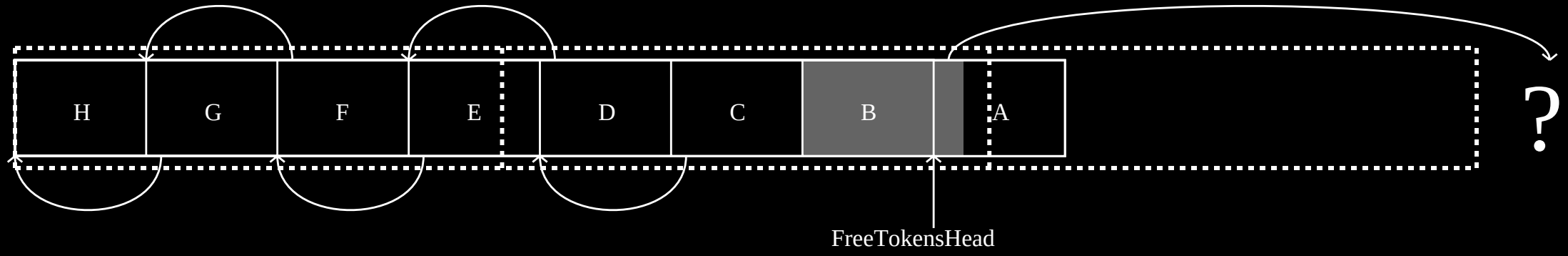
FreeSList: Head -> C -> D -> E -> F -> G -> H

Push in different orders with pop



FreeSList: Head -> A -> C -> D -> E -> F -> G -> H

Overflow Scenario 3



FreeSList: Head -> A -> ?