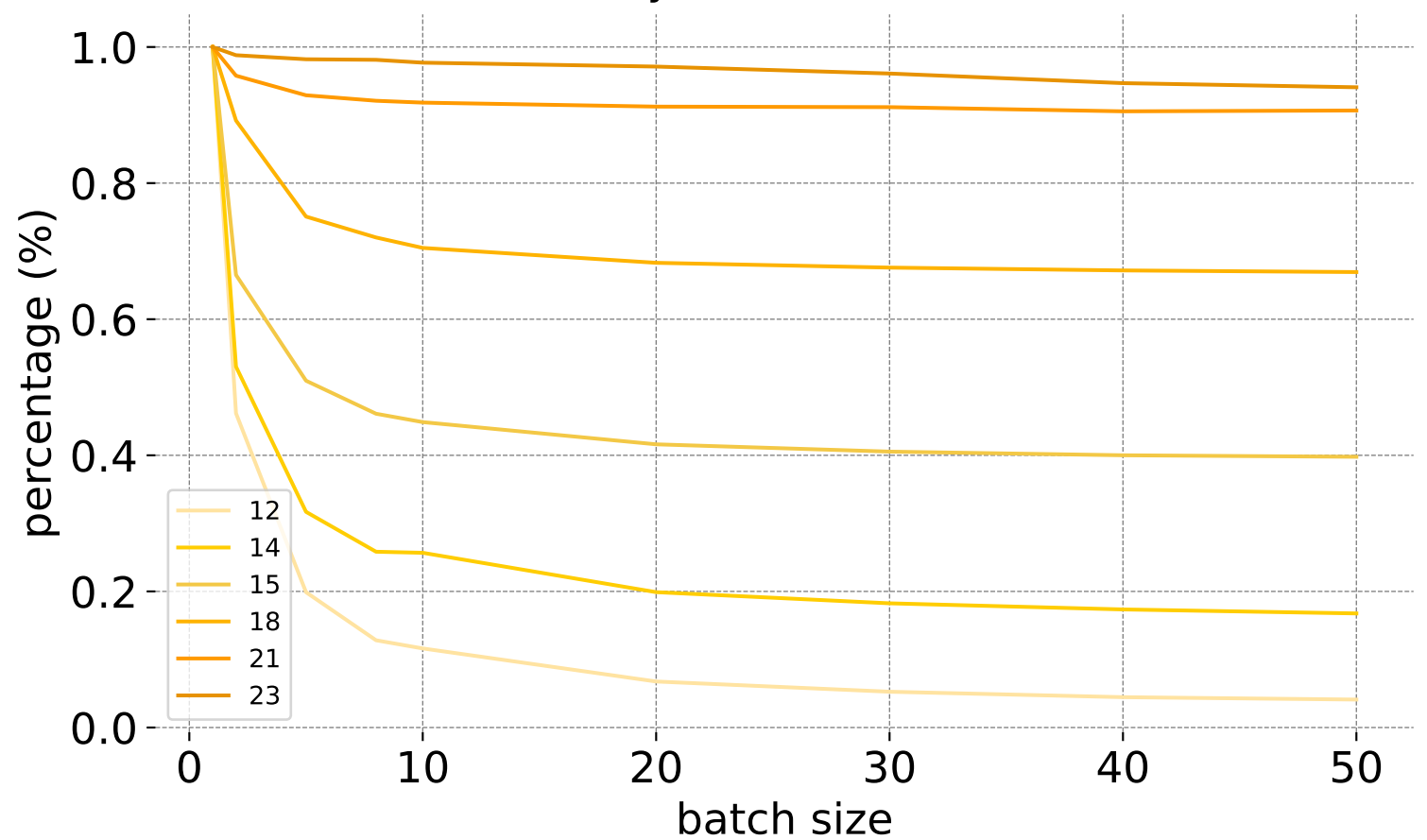


(a) cyclic forward NTT



(b) negative cyclic forward NTT