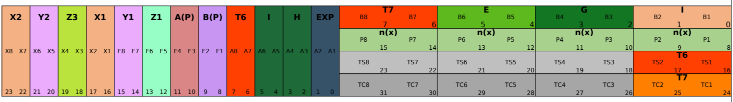
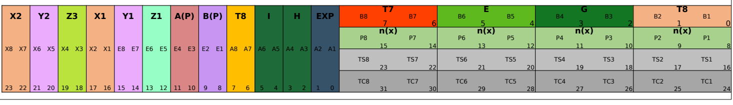
CopyV2H(A7,TS1)
CopyH2H(B7,TC1)

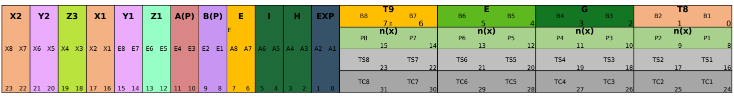


ModAdd(TS1,TC1)

CopyH2V(B1,A7)

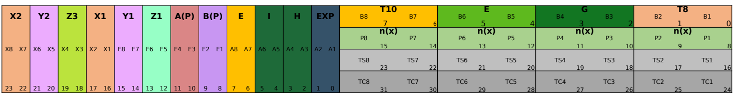


T9 = E*E*rinvpoly
CopyH2V(B5,A7)
CopyH2H(B5,B7)
MontMult(A7,B7,P1)

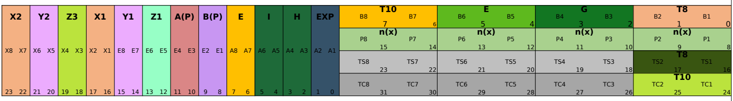


T10 = T9*E*rinvpoly

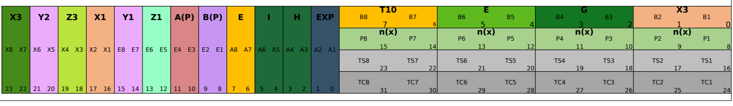
MontMult(A7,B7,P1)



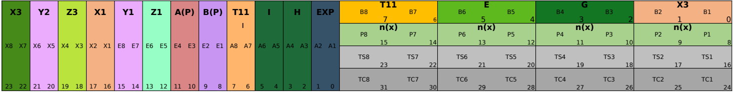
X3 = T8+T10
CopyH2H(B1,TS1)
CopyH2H(B7,TC1)



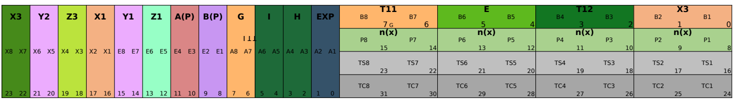
ModAdd(TS1,TC1)
CopyH2V(B1,X7)



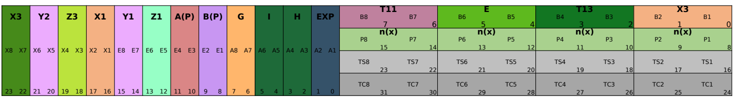
T11 = I*X3*rinvpoly
CopyV2H(A5,B1)
MontMult(X7,B1,P1)
CopyH2V(B1,A7)
CopyH2H(B1,B7)



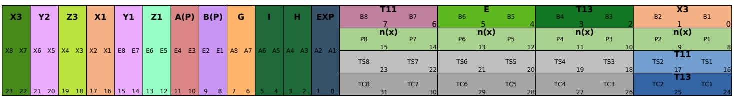
T12 = G*G*rinvpoly
CopyH2V(B3,A7)
MontMult(A7,B3,P1)



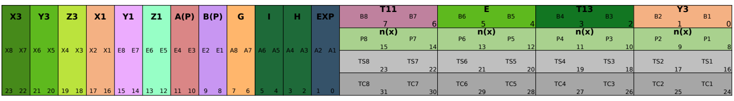
T13 = T12*H*rinvpoly
MontMult(A3,B3,P1)



Y3 = T11+T13
CopyH2H(B7,TS1)
CopyH2H(B3,TC1)



ModAdd(TS1,TC1)
CopyH2V(B1,X5)



All Steps are: