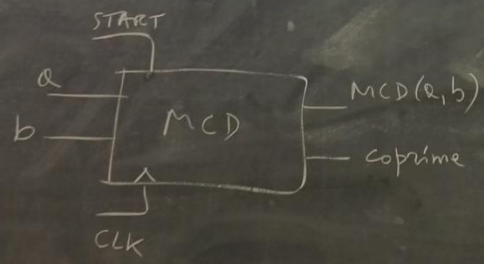
MCD(a,b)

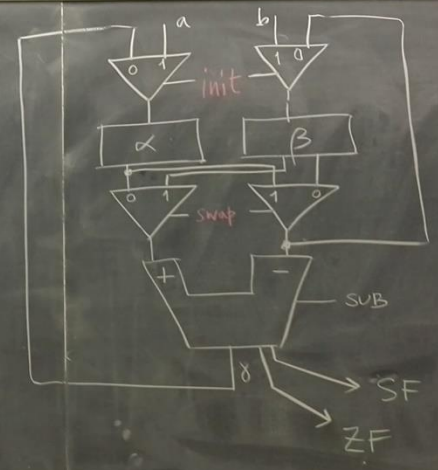
19/11/12

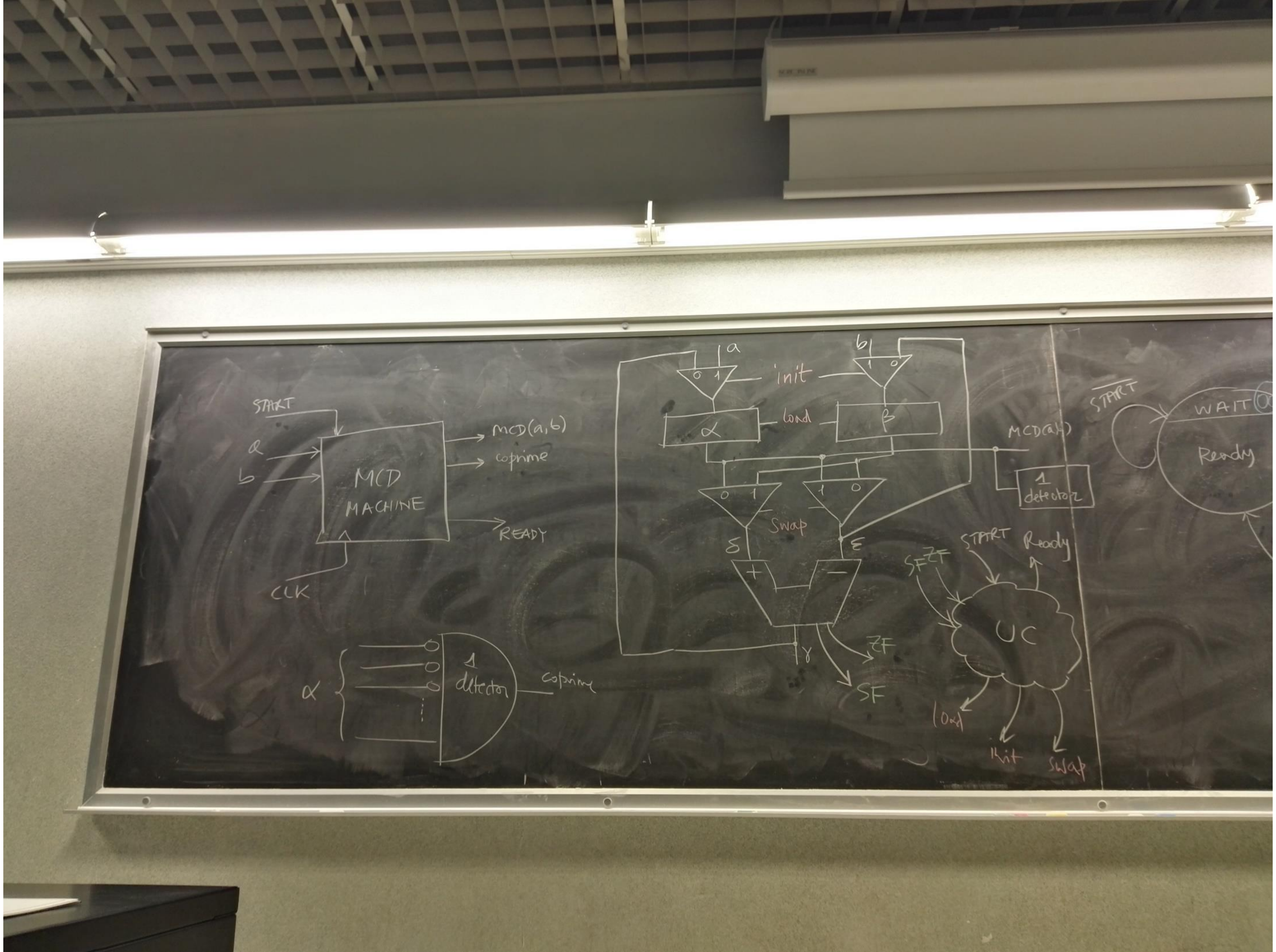


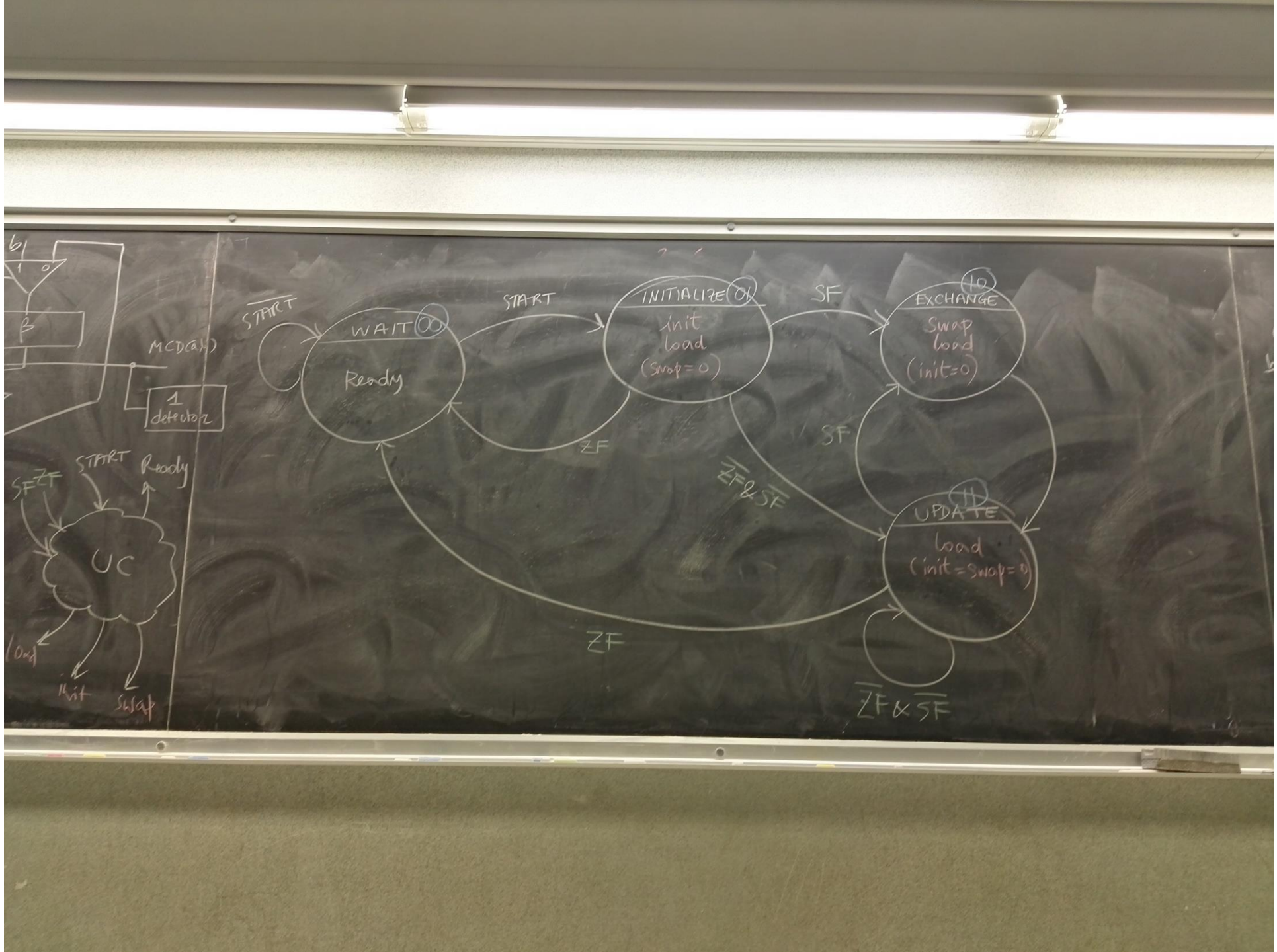
0. $\alpha \leftarrow a$, $\beta \leftarrow b$
1. $\alpha = \beta \Rightarrow MCD(a,b) = \alpha$: STOP
2. $\alpha < \beta \Rightarrow \alpha \leftrightarrow \beta$
3. $\gamma \leftarrow (\alpha - \beta)$, $\alpha \leftarrow \beta$, $\beta \leftarrow \gamma$; vai a 1

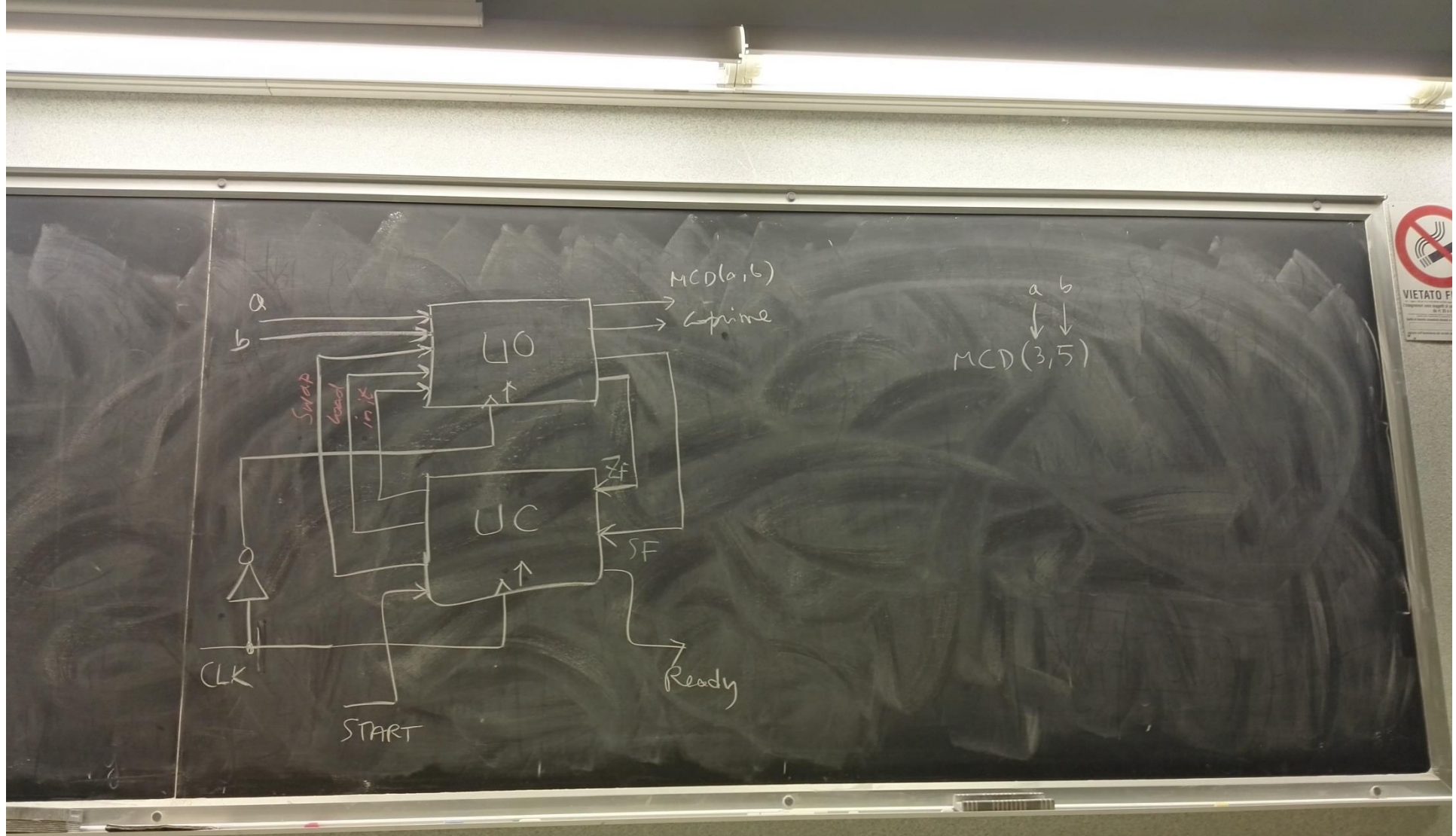
a = 153, b = 68

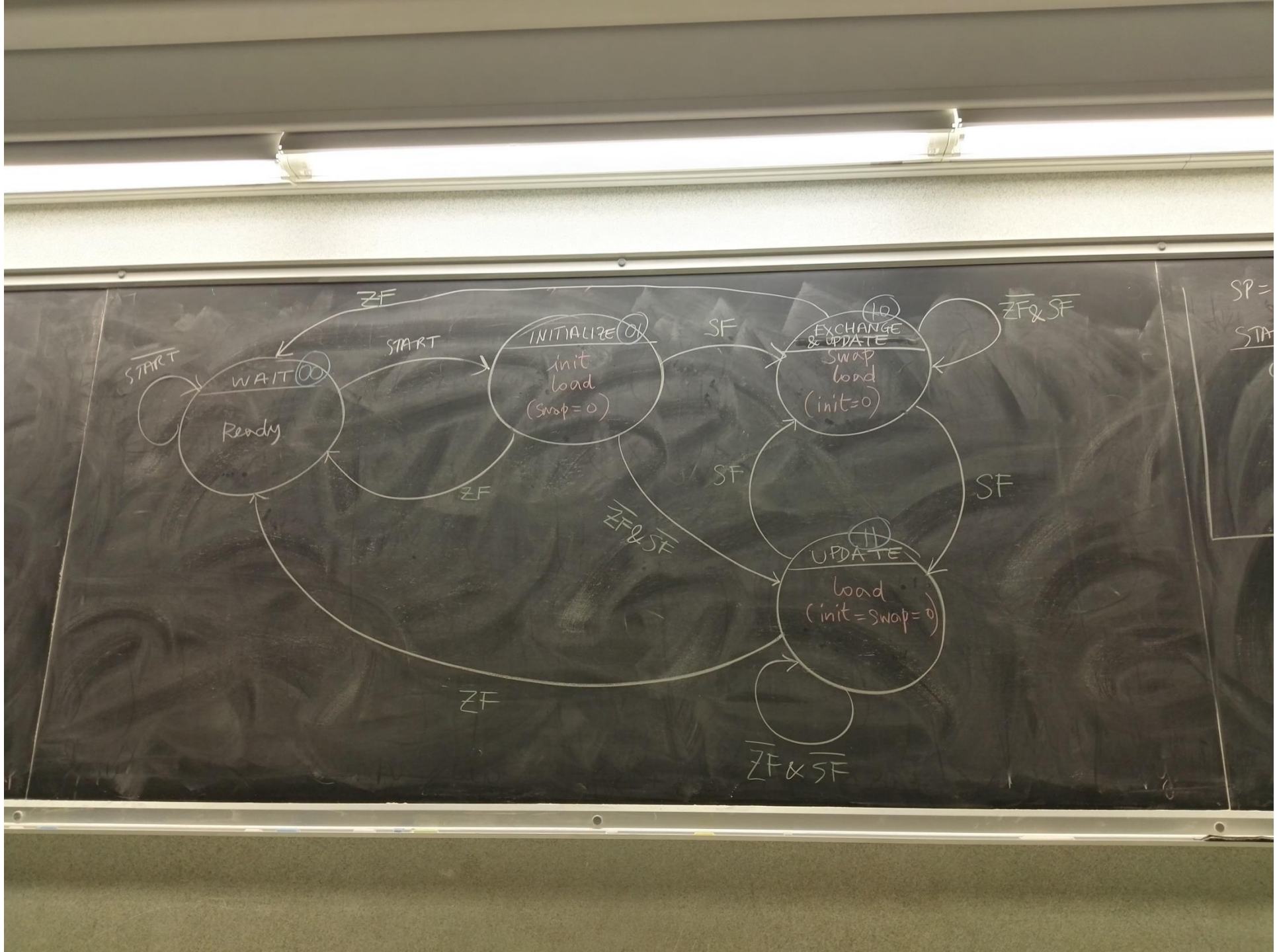
α	β	γ = α − β
153	68	85
85	68	17
17	68	−51
68	17	51
51	17	34
34	17	17
(17)	17	0

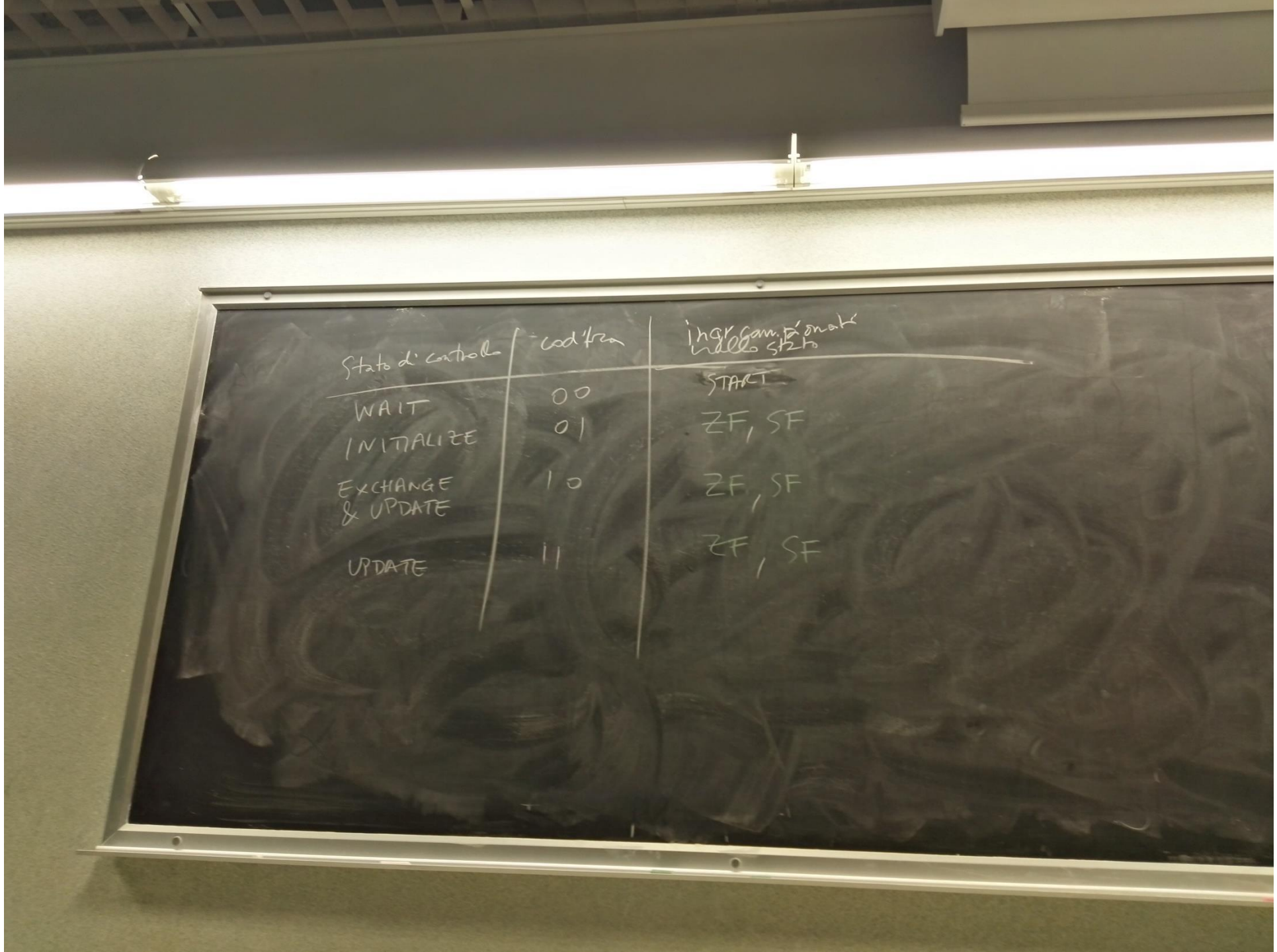


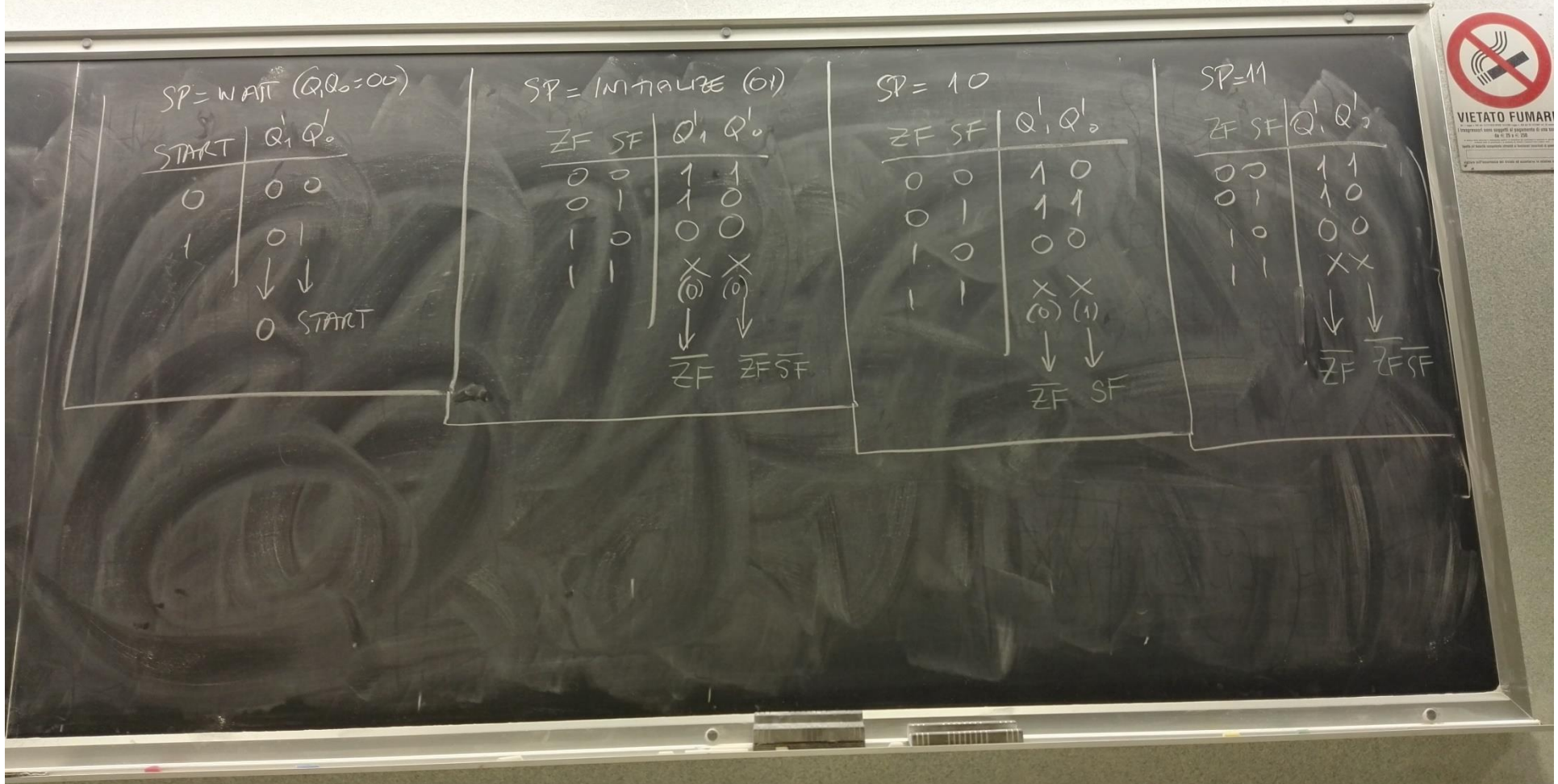

START
a
b
MCD MACHINE
CLK
MCD(a,b)
coprime
READY
α
1 detector
coprime
a
b
init
load
α
β
swap
δ
ε
+
−
γ
ZF
SF
MCD(a,b)
1 detector
START
Ready
SF ZF
UC
load
init
swap
START
WAIT
Ready

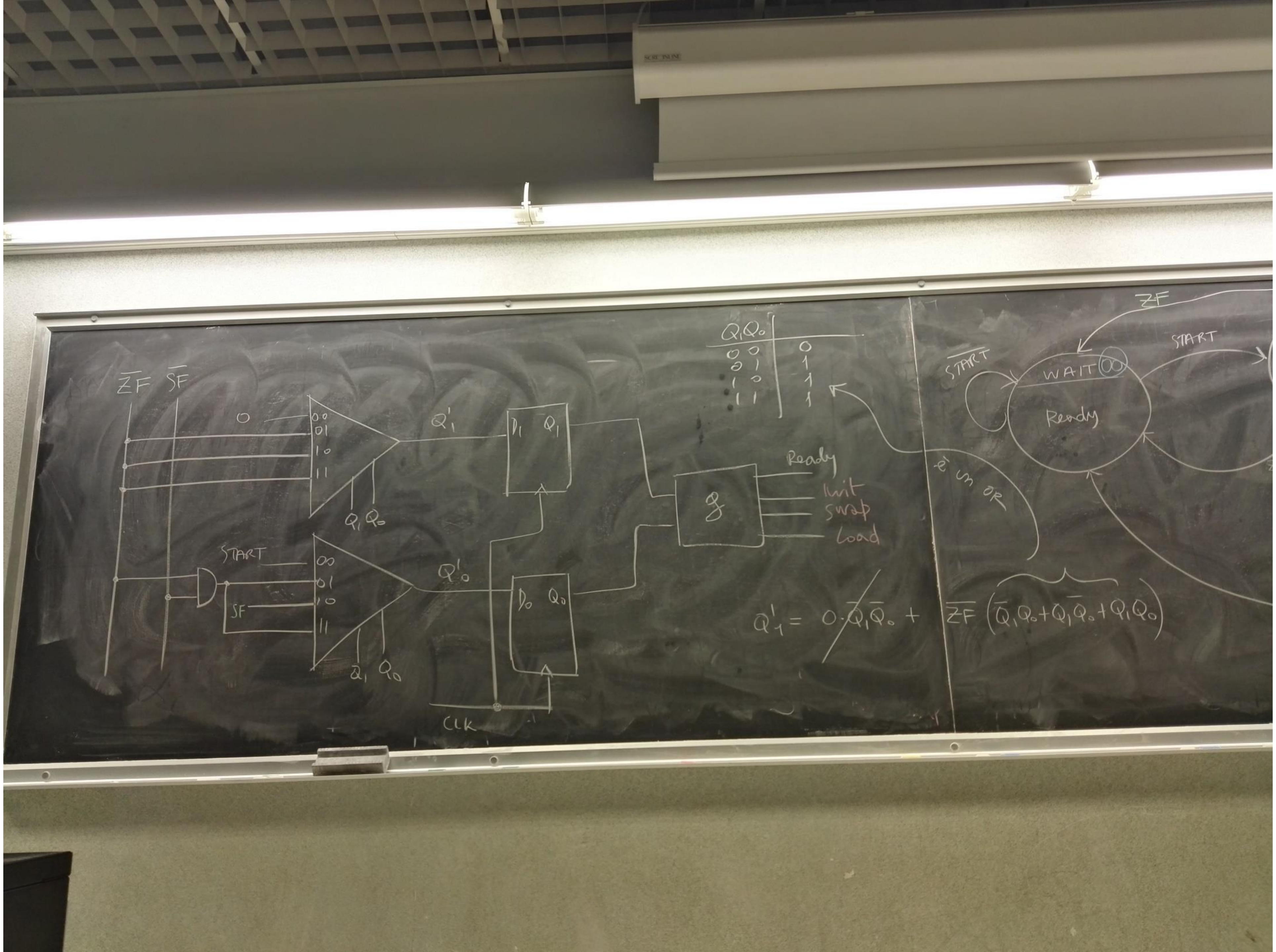

b
1
0
B
MCD(a,b)
1
detector Z
START
SF ZF
Ready
UC
Load
Init
Swap
START
WAIT
00
Ready
START
INITIALIZE
01
init
load
(Swap = 0)
ZF
SF
EXCHANGE
10
Swap
load
(init=0)
SF
ZF & SF
UPDATE
11
load
(init = Swap = 0)
ZF
ZF & SF


a
b
UO
MCD(a,b)
a prime
swap
load
init
Zf
UC
SF
CLK
START
Ready
a b
MCD(3,5)


ZF
START
START
WAIT 00
Ready
INITIALIZE 01
init
load
(swap=0)
SF
10
EXCHANGE & UPDATE
swap
load
(init=0)
ZF & SF
SF
SF
ZF
ZF & SF
11
UPDATE
load
(init=swap=0)
ZF
ZF & SF


Stato di controllo
codifica
ingressi condizionati
START
WAIT
00
INITIALIZE
01
ZF, SF
EXCHANGE & UPDATE
10
ZF, SF
UPDATE
11
ZF, SF


SP = WAIT (Q1Q0 = 00)
START | Q'1 Q'0
0 | 0 0
1 | 0 1
0 START
SP = INITIALIZE (01)
ZF SF | Q'1 Q'0
0 0 | 1 1
0 1 | 1 0
1 0 | 0 0
1 1 | X X
(0) (0)
ZF ZF SF
SP = 10
ZF SF | Q'1 Q'0
0 0 | 1 0
0 1 | 1 1
1 0 | 0 0
1 1 | X X
(0) (1)
ZF SF
SP = 11
ZF SF | Q'1 Q'0
0 0 | 1 1
0 1 | 1 0
1 0 | 0 0
1 1 | X X
ZF ZF SF
VIETATO FUMARE


Q1Q0
0 0 | 0
0 1 | 1
1 0 | 1
1 1 | 1
ZF SF
0
00
01
10
11
Q'1
D1 Q1
Q1 Q0
START
SF
Q'0
D0 Q0
Q1 Q0
CLK
g
Ready
Init
Swap
Load
Q'1 = 0·Q1Q0 + ZF(Q1Q0+Q1Q0+Q1Q0)
ZF
START
START
WAIT 00
Ready
e' un OR