1 Lezione del 23-10-24

1.1 Divisione

Siano dati X, un naturale in base β su $n+m$ cifre, detto **dividendo**, con $0 \leq X \leq \beta^{n+m}-1$, e Y, un naturale in base β su m cifre, detto **divisore**, con $0 \leq Y \leq \beta^m - 1$. Vogliamo calcolare i due numeri Q ed R tali che:

$$X = Q \cdot Y + R$$

Abbiamo che, con $|Y = 0|$, la divisione non è fattibile, quindi avremo bisogno di un uscita di **non fattibilità** `no_div`.

1.1.1 Dimensioni di resti e quozienti

Assumendo $Y > 0$, si ha che Q sta su $n + m$ cifre (caso peggiore $Y = 1$), mentre R sta su m cifre, in quanto $0 \leq R \leq Y$ dalle proprietà della divisione. Scelgo, per ragioni tecniche, che il quoziente dovrà stare su n cifre, quindi impongo $Q \leq \beta^n - 1$. Nel caso non si possa rappresentare Q, quindi, userò sempre la stessa uscita `no_div` di prima.

La decisione fatta riguardo a Q implica che:

$$X = Q \cdot Y + R \leq (\beta^n - 1) \cdot Y + (Y - 1) = \beta^n \cdot Y - 1 \Rightarrow X < \beta^n \cdot Y$$

L'ipotesi potrebbe sembrare limitante, ma visto che si può ricavare n che soddisfi la disuguaglianza, possiamo eseguire qualsiasi divisione poste **estensioni** del dividendo e **riserve** di cifre (cioè più delle strettamente necessarie) per il quoziente.

Nel caso il numero di cifre n, m sia dato dal problema, cioè quando si lavora su **campi finiti**, l'ipotesi è restrittiva.

1.1.2 Modulo divisore

Vogliamo quindi realizzare un circuito che:

1. Verifichi la **fattibilità** della divisione nelle ipotesi date;
2. Se il quoziente sta su n cifre, lo restituisca, altrimenti restituisca `no_div`.

La divisione viene svolta, tradizionalmente, prendendo un sottoinsieme delle n cifre più significative del dividendo, tali per cui possiamo trovare quante volta il divisore sta nel sottoinsieme. Formalmente, quindi, prendo il minimo numero di cifre più significative di X per ottenere un $X' \in [Y, \beta \cdot Y[$ Si nota che m cifre possono non bastare, mentre $m + 1$ bastano sempre (purchè X non abbia zeri in testa).

Calcolo quindi dei quozienti e resti **parziali**, q e R', dalla divisione di X' e Y. Si ha che q sta su una sola cifra, perchè $X' < \beta \cdot Y$ dall'ipotesi.

Calcolo quindi il nuovo dividendo X' concatenando R' con la cifra più significativa non ancora utilizzata di X. Il nuovo dividendo, date le ipotesi, è ancora $< \beta \cdot Y$:

$$R' \leq Y - 1, \quad \beta \cdot R' + (\beta - 1) \leq \beta \cdot Y - \beta + \beta + 1 = \beta \cdot Y$$

Si itera fino ad esaurimento delle cifre del dividendo. A questo punto il **quoziente** è ottenuto dal concatenamento dei quozienti parziali, e il resto è l'ultimo resto parziale.

Abbiamo che l'unica divisione effettiva è quella di $m + 1$ per m cifre, mentre tutte le altre sono effettivamente scomposizioni, quindi circuiti di logica a costo nullo.

1.1.3 Divisione nei processori Intel x86

Abbiamo visto come nei processori Intel x86, abbiamo a disposizione tre versioni della divisione:

Dim. sorgente (divisore)	Dim. dividendo	Dividendo	Quoziente	Resto
8 bit	16 bit	AX	AL	AH
16 bit	32 bit	DX_AX	AX	DX
32 bit	64 bit	EDX_EAX	EAX	EDX

Si ha che la `DIV` ammette dividendo su $2n$ bit e divisore su n bit, con $n = 8, 16, 32$, e richiede che il quoziente stia su n bit (altrimenti genera un'eccezione). Questo è quello che si otterrebbe ponendo $n = m$.

1.1.4 Divisione elementare in base 2

Resta quindi da capire come effettuare la divisione elementare fra un numero a $m + 1$ cifre e un altro a m cifre, sotto l'ipotesi $X \leq 2Y = 2^1 \cdot Y$ (siamo in $\beta = 2$).

Abbiamo che Q può valere 0 o 1. Vale 0 se il divisore Y è maggiore del dividendo X, 1 altrimenti. R, invece, è uguale al dividendo X se questo è minore del divisore Y, altrimenti è uguale a $X - Y$:

$$Q = \begin{cases} 0, & X < Y \\ 1, & X \geq Y \end{cases}, \quad R = \begin{cases} X, & X < Y \\ X - Y, & X \geq Y \end{cases}$$

Per rappresentare questo sistema ci serve un comparatore fra X e Y. Lo realizziamo con un sottrattore (di cui bisognavamo comunque per il calcolo di $X - Y$), quindi mandando Y complementato (ed opportunamente esteso) al secondo input di un sommatore, ed X al primo. Il sommatore ha $C_{in} = 0$.

Fuori dal sommatore, avremo $X - Y$ come risultato, e b_{out} come discrimnante per $X < Y$. Mandiamo quindi X e $X - Y$ agli ingressi di un multiplexer con variabile di controllo C_{out} dal sommatore, cioè discriminiamo fra X e $X - Y$ sulla base di quanto restituito dal comparatore.

A questo punto si ha che b_{out} rappresenta Q, mentre l'uscita del multiplexer è R.