1 Lezione del 17-10-24

1.1 Rappresentazione dei numeri naturali

Noi rappresentiamo i numeri naturali attraverso una notazione posizionale, ovvero come:

- Un numero $\beta \geq 2$, detto **base di rappresentazione**. Nel caso del sistema decimale, $\beta = 10$.
- Un'insieme di β simboli, detti **cifre**, a ciascuno dei quali è associato un numero naturale $\in [0, \beta - 1]$.
- Una **legge di rappresentazione** che fa corrispondere ad ogni sequenza di cifre un numero naturale.

1.1.1 Notazione posizionale

Dato un numero $A \in \mathbb{N}$, lo posso rappresentare in base β attraverso una sequenza di cifre:

$$A \equiv (a_{n-1}a_{n-2}...a_1a_0)_\beta, \quad 0 \leq a_i \leq \beta - 1, \quad 0 \leq i \leq n - 1$$

dove la legge di rappresentazione è:

$$A = \sum_{i=0}^{n-1} a_i \cdot \beta^i$$

Nella rappresentazione di un numero naturale, una cifra contribuisce a determinare il numero in modo differente a seconda della propria posizione nella sequenza.

Normalmente usiamo il sistema decimale, con $\beta = 10$. Nell'informatica, ci interessiamo al sistema binario, con $\beta = 2$.

1.2 Teorema della divisione con resto

Vediamo come trovare la rappresentazione di un naturale A in una base β, noto che questo è sempre possibile:

Teorema 1.1: della divisone con resto

Dato $x \in \mathbb{N}, \beta \in \mathbb{N}, \beta > 0$, esiste ed è unica la coppia di numeri q, r:

- $q \in \mathbb{N}$;
- $r \in \mathbb{N}, \quad 0 \leq r < \beta$;

tale che $x = q \cdot \beta + r$.

questo vale anche per gli interi $\in \mathbb{Z}$, scambiando i simboli $\mathbb{N}$ con $\mathbb{Z}$.

Dimostrazione

Pensiamo di dividere $\mathbb{Z}$ in intervalli:

$$[n \cdot \beta, (n+1) \cdot \beta[, \quad n \in \mathbb{Z}$$

Si avrà che

$$\bigcup_{n\in\mathbb{Z}} [n\cdot\beta,(n+1)\cdot\beta[\equiv\mathbb{Z}$$

ergo x farà parte del q-esimo intervallo di questa lista. Possiamo definire allora $r = x - q\cdot\beta$, e da come abbiamo preso gli intervalli, $0\leq r<\beta$.

Resta da dimostrare l'unicità dei q,r trovati. Possiamo sostenere per assurdo che esistano due coppie (q_1,r_1) e (q_2,r_2) diverse tali che $x = q_1\cdot\beta + r_1 = q_2\beta + r_2$, con le ipotesi $q_i\in\mathbb{Z}$ e $0\leq r_i<\beta$.

Varrà allora:

$$(q_1-q_2)\cdot\beta = r_2 - r_1$$

e dall'ipotesi:

$$-\beta<(r_2-r_1)<\beta\rightarrow -\beta<(q_1-q_2)\cdot\beta<\beta$$

Cioè:

$$-1<(q_1-q_2)<1$$

che in Z significa $q_1-q_2=0$, che è contro l'ipotesi.

L'unicità del risultato è garantita da $0\leq r\leq\beta-1$.

1.2.1 Divisioni

Si ha che una divisione restituisce quoziente e resto:

$$q=\left\lfloor\frac{x}{\beta}\right\rfloor,\quad r=|x|_\beta,\quad x=q\cdot\beta+r=\left\lfloor\frac{x}{\beta}\right\rfloor\cdot\beta+|x|_\beta$$

Se la divisione è tra naturali, anche q è naturale, cioè $x\in\mathbb{N}\Rightarrow q\in\mathbb{N}$.

1.2.2 Proprietà dell'operatore modulo

Abbiamo usato l'operatore modulo ($|x|_\beta$). Vediamone alcune proprietà, dato $\alpha\in\mathbb{N}^+$:

1. $|x+k\cdot\alpha|_\alpha = |x|_\alpha,\quad k\in\mathbb{Z}$
   Questo da:

   $$x=\left\lfloor\frac{x}{\alpha}\right\rfloor\cdot\alpha+|x|_\alpha,\quad x+k\cdot\alpha=\left(\left\lfloor\frac{x}{\alpha}\right\rfloor+k\right)\cdot\alpha+|x|_\alpha$$

   chiamiamo $x'=x+k\cdot\alpha$:

   $$x'=\left\lfloor\frac{x'}{\alpha}\right\rfloor\cdot\alpha+|x'|_\alpha=\left\lfloor\frac{x}{\alpha}+k\right\rfloor\cdot\alpha+|x'|_\alpha=\left(\left\lfloor\frac{x}{\alpha}\right\rfloor+k\right)\cdot\alpha+|x'|_\alpha$$

   Dove il passaggio $\lfloor\frac{x}{\alpha}+k\rfloor=\lfloor\frac{x}{\alpha}\rfloor+k$ è concesso da $k\in\mathbb{Z}$. Notiamo che le ultime due espresioni ricavate si equivalgono, ergo dev'essere vero che $|x'|_\alpha=|x|_\alpha$, da cui la tesi.

2. $|x+y|_\alpha = ||x|_\alpha+|y|_\alpha|_\alpha$
   Questo da:

   $$|x+y|_\alpha=\left|\left\lfloor\frac{x}{\alpha}\right\rfloor\cdot\alpha+|x|_\alpha+\left\lfloor\frac{y}{\alpha}\right\rfloor\cdot\alpha+|y|_\alpha\right|_\alpha=\left|\left(\left\lfloor\frac{x}{\alpha}\right\rfloor+\left\lfloor\frac{y}{\alpha}\right\rfloor\right)\cdot\alpha+|x|_\alpha+|y|_\alpha\right|_\alpha$$

   e l'applicazione della proprietà (1), da cui la tesi.

3. $|x \cdot y|_\alpha = ||x|_\alpha \cdot |y|_\alpha|_\alpha$
   Questo da:
$$|x \cdot y|_\alpha = \left| \left(\left\lfloor \frac{x}{\beta} \right\rfloor \cdot \beta + |x|_\beta \right) \left(\left\lfloor \frac{y}{\beta} \right\rfloor \cdot \beta + |y|_\beta \right) \right|$$
$$= \left| \left\lfloor \frac{x}{\alpha} \right\rfloor \left\lfloor \frac{y}{\alpha} \right\rfloor \alpha^2 + \left(\left\lfloor \frac{x}{\alpha} \right\rfloor |y|_\alpha + \left\lfloor \frac{y}{\alpha} \right\rfloor |y|_\alpha \right) \alpha + |x|_\alpha \cdot |y|_\alpha \right|$$
   Chiamiamo allora:
$$\left\lfloor \frac{x}{\alpha} \right\rfloor \left\lfloor \frac{y}{\alpha} \right\rfloor \alpha + \left(\left\lfloor \frac{x}{\alpha} \right\rfloor |y|_\alpha + \left\lfloor \frac{y}{\alpha} \right\rfloor |y|_\alpha \right) = k$$
   da cui:
$$|x \cdot y|_\alpha = |k \cdot \alpha + |x|_\alpha \cdot |y|_\alpha|_\alpha$$
   che ancora applicando la proprietà (1) dà la tesi.

1.2.3 Algoritmo delle divisioni successive

Possiamo usare il teorema della divisione con resto iterativamente per trovare la sequenza di cifre che rappresentano A in base β:

Algoritmo 1 delle divisioni successive

Input: un naturale A e una base β
Output: la rappresentazione di A in base β
$i \leftarrow 1$
while $q_i \neq 0$ **do**
  $A = q_i \cdot \beta + \alpha_{i-1}$
  $i \leftarrow i + 1$
end while

Dimostriamo la correttezza dell'algoritmo: si ha che eseguendo i passaggi ricaviamo una forma:
$$A = a_0 + \beta \cdot q_1 = a_0 + \beta \cdot (a_1 + \beta(a_2 + \beta \cdot (...)))$$
e quindi:
$$A = \sum_{i=0}^{n-1} a_i \cdot \beta^i$$
che è per definizione la rappresentazione di A in base β. Inoltre, il teorema della divisione con resto garantisce che la n-upla di cifre trovata è **unica**.

1.2.4 Rappresentazione su un numero finito di cifre

Con n cifre in base β, sappiamo che potremo formulare β^n sequenze differenti quindi rappresentare al massimo il numero $\beta^n - 1$, cioè quello dove tutte le cifre hanno valore massimo, $\beta - 1$.

Ciò si dimostra da:
$$A = \sum_{i=0}^{n-1} (\beta - 1) \cdot \beta^i = \sum_{i=0}^{n-1} \beta^{i+1} - \sum_{i=0}^{n-1} \beta^i = \sum_{i=1}^{n} \beta^i - \sum_{i=0}^{n-1} \beta^i = \beta^n - 1$$

Il numero di cifre necessario per rappresentare A è il numero minimo n per cui $\beta^n - 1 \geq A$, ergo:
$$n = \log_\beta(\beta^n) \geq \log_\beta(A + 1) \rightarrow n = \lceil \log_\beta(A + 1) \rceil$$

1.3 Reti combinatorie per i numeri naturali

Vogliamo cosotruire reti logiche che elaborino numeri naturali rappresentati in una data base β, generalmente $\beta = 2$. Si useranno **reti combinatorie**, dove lo *stato di uscita* è il **risultato** e lo *stato di ingresso* sono gli **operandi**.

Per ogni operazione aritmetica di base daremo una descrizione **indipendente dalla base**, usando le proprietà della notazione posizionale per scomporre l'operazione in blocchi elementari. In seguito, dettaglieremo le reti logiche che implementano questi blocchi elementari in base 2, attraverso le porte logiche già studiate.

Notiamo che spesso ci concentreremo più sulle **cifre** che sulle codifiche, indipendentemente dalla base.

1.3.1 Complemento

Dato $A = (a_{n-1}a_{n-2}...a_1a_0)_\beta$, in base β su n cifre, $0 \leq A \leq \beta^n$, definisco complemento di a in base β il numero:

$$\overline{A} = \beta^n - 1 - A$$

Si ha che il complemento di un numero a n cifre sta su n cifre, e che:

$$\overline{A} = \beta^n - 1 - A = \sum_{i=0}^{n-1}(\beta - 1)\beta^i - \sum_{i=0}^{n-1}\alpha_i\beta^i = \sum_{i=0}^{n-1}(\beta - 1 - a_i)\beta^i$$

$\beta - 1 - \alpha_i$ è una cifra in base β in quanto compresa fra 0 e $\beta - 1$. Quindi, $\overline{A} = (\overline{a_{n-1}a_{n-2}}...\overline{a_1a_0})_\beta$.

Questo significa che basta saper fare il complemento di una singola cifra per fare il complemento di un numero. In base 2, questo significa usare una porta not. In altre basi diventà più complicato, ad esempio in base 10 con codifica BCD avrò un circuito con 4 ingressi e 4 uscite, con tabella di verità:

x_3	x_2	x_1	x_0	z_3	z_2	z_1	z_0
0	0	0	0	1	0	0	1
0	0	0	1	1	0	0	0
0	0	1	0	0	1	1	1
0	0	1	1	0	1	1	0
0	1	0	0	0	1	0	1
0	1	0	1	0	1	0	0
0	1	1	0	0	0	1	1
0	1	1	1	0	0	1	0
1	0	0	0	0	0	0	1
1	0	0	1	0	0	0	0
1	0	1	0	–	–	–	–
1	0	1	1	–	–	–	–
1	1	0	0	–	–	–	–
1	1	0	1	–	–	–	–
1	1	1	0	–	–	–	–
1	1	1	1	–	–	–	–

che dopo una sintesi dà:

$$\begin{cases} z_3 = \overline{x_3 x_2 x_1} \\ z_2 = \overline{x_3 x_2} x_1 + x_2 \overline{x_1} \\ z_1 = x_1 \\ z_0 = \overline{x_0} \end{cases}$$