RILEVAZIONE E LOCALIZZAZIONE DI ERRORI NEI SISTEMI NUMERICI DELLE CLASSI RESIDUE

F. BARSI* P. MAESTRINI*

Nota Interna n°4 - Serie Speciale
Convenzione CNR - ENI
Ottobre 1971

* Istituto di Elaborazione della Informazione
Via S. Maria, 46. 56100 PISA

INTRODUZIONE

E' ben noto come la sicurezza della trasmissione digitale di dati possa essere aumentata impiegando codici per la rappresentazione dell'informazione.

Individuate particolari classi di errore, la cui probabilità di occorrenza è ritenuta massima, è in generale possibile determinare dei codici per rilevare o eventualmente rilevare e correggere gli errori di tali classi.

L'incremento di sicurezza che ne consegue ha come contropartita una ridondanza nella rappresentazione dell'informazione. Esempi tipici di tali codici, che chiameremo codici di trasmissione, sono i codici di Hamming.

Data la evidente affinità dei problemi connessi, codici di questo tipo trovano applicazione anche per la rilevazione e la correzione di errori su dati memorizzati in memorie digitali di vario tipo.

Nel caso in cui si richieda di rilevare o correggere anche errori introdotti durante l'esecuzione di operazioni aritmetiche, oltre che nella trasmissione e nella memorizzazione dei dati, la classe dei codici utilizzabili si riduce notevolmente.

E' stato dimostrato [1] che il codice si conserva attraverso le operazioni aritmetiche se e soltanto se:

a) la parte ridondante del codice si riduce ad una replica dell'informazione di partenza
b) la parte ridondante del codice e l'informazione di partenza sono riconducibili a numeri appartenenti ad una stessa classe di congruenza, rispetto ad un opportuno modulo.

Il caso a) corrisponde ovviamente all'impiego di tecniche di ridondanza. La duplicazione dell'informazione permette la rilevazio

ne di un qualunque errore che non interessi contemporaneamente la parte non ridondante e la parte ridondante del codice.

Con la triplicazione diventa possibile la correzione di errori.

Il caso b) comprende i codici conosciuti complessivamente come *codici residui*. L'importanza dei codici residui risiede nel fatto che essi permettono di rilevare o rilevare e correggere particolari classi di errori con una ridondanza minore di quella che consegue rispettivamente alla duplicazione e alla triplicazione.

Ovviamente la minore ridondanza corrisponde ad una minore ampiezza della classe degli errori rilevati e corretti. Questa classe, d'altronde, può essere fatta coincidere con quella degli errori la cui probabilità di occorrenza è massima.

Per una discussione di tale problema e dei possibili compromessi tra ridondanza in hardware e ridondanza in tempo si rimanda al riferimento [2] .

Fra i codici residui, i più noti sono quelli in cui i numeri sono rappresentati in un sistema posizionale, mentre la ridondanza è introdotta aggiungendo una cifra residua (codici residui sistematici) oppure introducendo un fattore moltiplicativo (codici residui non sistematici).

Codici di questo tipo, adatti sia alla rilevazione che alla correzione di errori, sono ampiamente trattati nella letteratura [3, 4, 5, 6] .

Non altrettanto noti sono i codici in cui anche la rappresentazione del numero è fatta in un sistema numerico residuo, mentre la parte ridondante del codice consiste in una o più cifre residue aggiuntive. Più propriamente in tal caso si può parlare di rappresentazione dei numeri in un sistema residuo ridondante [7].

Questa ultima classe di codici ha particolari motivi di interesse in quanto le diverse cifre residue in larga misura non sono gerarchicamente ordinate, lasciando intravedere interessan-

ti sviluppi per quanto riguarda gli studi di riconfigurabilità dei sistemi.

I sistemi numerici ridondanti sono stati studiati principalmente nei lavori di Watson [2] e Akuŝskiĭ e Yudickiĭ [8].

Nel primo lavoro vengono determinate in particolare delle condizioni e delle procedure per la rilevazione e la correzione di errori interessanti singole cifre residue utilizzando un metodo tabulare.

Nel secondo lavoro lo stesso problema viene affrontato da un diverso punto di vista, mirando principalmente alla determinazione di condizioni sufficienti o necessarie e sufficienti per la rilevazione e la correzione di errori su una o più cifre residue.

Questa nota contiene una prima raccolta dei risultati di un ampio studio tendente ad estendere i lavori citati.

In particolare viene precisata la ridondanza necessaria e sufficiente per la correzione di errori su una singola cifra residua (Teoremi 6 e 7) correggendo un risultato di Watson che risulta legato al particolare metodo da questi proposto per la correzione di errori.

Inoltre viene messa in evidenza la possibilità di correggere, con una ridondanza ovviamente minore di quella necessaria nel caso sopra accennato, particolari classi di errore, che costituiscono una sottoclasse di quelli interessanti una singola cifra residua e che sono caratterizzati da assegnati valori di un "parametro di errore".

Tali sottoclassi possono risultare particolarmente significative potendo coincidere, ad esempio, con gli errori che interessano un solo bit del codice binario impiegato per codificare i simboli di una cifra residua.

Vengono determinate delle condizioni necessarie e sufficienti per la correzione di sottoclassi di errori caratterizzate da assegnati valori del "parametro di errore".

PARTE PRIMA

TEORIA DELLE CONGRUENZE

1) Generalità

A ciascun intero a corrisponde un unico resto r, positivo, risultante dalla sua divisione per un intero m (modulo), con $m > 0$.*

Definizione 1.1. Due interi a e b, aventi lo stesso resto r, con lo stesso divisore intero positivo m, sono detti "congruenti modulo m" e si indica:

$$a \equiv b \pmod{m}$$

(a congruente a b modulo m) .

I resti o residui r_a ed r_b vengono anche indicati con la notazione:

$$|a|_m, \ |b|_m$$

e si legge:
a modulo m, b modulo m .

In generale sono quindi equivalenti le notazioni:

$$f \equiv g \pmod{m} \quad \text{e:}$$

$$|f|_m = |g|_m$$

Teorema 1.1. La congruenza $a \equiv b \pmod{m}$ è equivalente alla uguaglianza:

(*) Esempio:

a = 13	m = 5	resto = 3
a = -13	m = 5	resto = 2

Teorema 1.2. La congruenza $a \equiv b \pmod{m}$ è equivalente alla divisibilità di $(a - b)$ per m.

Segue dal Teorema 1.1.

2) Alcune proprietà delle congruenze

Teorema 2.1. Le congruenze possono essere sommate membro a membro.

Infatti, siano date le congruenze:

$$a_1 \equiv b_1 \pmod{m}$$
$$a_2 \equiv b_2 \pmod{m}$$
.....
.....
.....
$$a_k \equiv b_k \pmod{m}$$

Dal Teorema 1.1:

$$a_1 = b_1 + m\, t_1$$
$$a_2 = b_2 + m\, t_2$$
.....
.....
$$a_k = b_k + m\, t_k$$

Sommando membro a membro:

$$a_1 + a_2 + \ldots\ldots + a_k = b_1 + b_2 + \ldots\ldots + b_k + m\,(t_1 + t_2 + \ldots + t_k)$$

e ancora dal Teorema 1.1:

$$a_1 + a_2 + \ldots\ldots + a_k \equiv b_1 + b_2 + \ldots\ldots + b_k \pmod{m}$$

Teorema 2.2. Si può trasportare un termine di una congruenza da un membro all'altro cambiandone il segno.

Infatti, sia data la congruenza:

re divisi per un loro divisore comune, purchè questo sia primo rispetto al modulo.

Infatti, sia:

$a \equiv b \pmod{m}$

$a = a_1 d$

$b = b_1 d$

$(d, m) = 1$

La differenza:

$a - b = (a_1 - b_1) d$

è divisibile per m.

Poichè d è primo rispetto ad m, $a_1 - b_1$ sarà divisibile per m, cioè:

$a_1 \equiv b_1 \pmod{m}$

Teorema 2.7. Si possono moltiplicare per uno stesso intero entrambi i membri di una congruenza ed il modulo.

Sia:

$a \equiv b \pmod{m}$

cioè:

$a = b + m t$

Moltiplicando ambo i membri per k:

$a k = b k + m k t$

cioè:

$a k \equiv b k \pmod{m k}$

Teorema 2.8. Si possono dividere entrambi i membri di una congruenza ed il modulo per un loro divisore comune.

Sia:

$a \equiv b \pmod{m}$

$a = a_1 d$

$b = b_1 d$

$m = m_1 d$

Si ha:

$a = b + m t$

ovvero:

$a_1 d = b_1 d + m_1 d t$

$a_1 = b_1 + m_1$

cioè:

$a_1 \equiv b_1 \pmod{m_1}$

Teorema 2.9. Se la congruenza:

$a \equiv b$

vale per più moduli $m_1, m_2, \ldots, m_k$, vale anche per il modulo uguale al loro minimo comune multiplo.

Da:

$a \equiv b \pmod{m_1}$

$a \equiv b \pmod{m_2}$

.....

.....

$a \equiv b \pmod{m_k}$

segue che la differenza $a - b$ è divisibile per tutti i moduli $m_1, m_2, \ldots, m_k$. Cioè $(a - b)$ è multiplo di ciascuno degli m_i, cioè è un loro multiplo comune.
$(a - b)$ deve quindi essere divisibile per il minimo comune multiplo dei moduli, m, ovvero:

$a \equiv b \pmod{m}$

3) Rappresentazione dei numeri nel sistema delle classi residue

Definizione 3.1. Dato un insieme di interi positivi $p_1, p_2, \ldots, p_n$ (moduli del sistema) si dirà sistema numerico delle classi residue quel sistema in cui un intero N si rappresenta nella forma:

$$N = (\alpha_1, \alpha_2, \ldots\ldots, \alpha_n)$$

dove:

$$\alpha_i = N - \left\lfloor \frac{N}{p_i} \right\rfloor \cdot p_i$$

per $i = 1, 2, \ldots\ldots, n$ (*)

α_i rappresenta il minimo resto (residuo) non negativo della divisione di N per p_i.

Si ha evidentemente:

$$0 \leqslant \alpha_i < p_i$$

Sia ora a un intero. Rappresentare a nel sistema delle classi residue di moduli $p_1, p_2, \ldots\ldots, p_n$ significa considerare il sistema di congruenze:

$$a \equiv \alpha_1 \pmod{p_1}$$

$$a \equiv \alpha_2 \pmod{p_2}$$

.....

.....

$$a \equiv \alpha_n \pmod{p_n}$$

con $0 \leqslant \alpha_i < p_i$.

Si può dimostrare che tale sistema ammette una ed una sola soluzione:

(*) D'ora in poi con la notazione:

$\lfloor x \rfloor$

si indicherà il più grande intero che non supera x.

$a \equiv \alpha \pmod{P}$

dove P è il minimo comune multiplo dei moduli.

In particolare, se a è compreso nell'intervallo, aperto a destra, [0, P) si avrà:

$a = \alpha$

In altri termini, se si conviene di operare solo con numeri dell'intervallo [0, P) si avrà una corrispondenza biunivoca tra numeri e loro rappresentazione nel sistema delle classi residue.

E' inoltre evidente la convenienza di impiegare sistemi di moduli mutuamente primi. In questo caso, infatti, il campo del sistema diviene:

$P = p_1 \, p_2 \, \cdots\cdots \, p_n$

E' importante notare che, a differenza di quanto avviene nei sistemi numerici posizionali, in cui le singole cifre sono tra loro dipendenti a causa della propagazione dei riporti, nel sistema numerico delle classi residue ogni cifre è indipendente dalle altre.

Ogni "digit" residuo, infatti, si elabora indipendentemente dagli altri "digit" e contiene una informazione globale, anche se incompleta, sul numero rappresentato nell'intero sistema.

Così, tutte le operazioni aritmetiche vengono svolte separatamente per ciascun modulo. Facciamo un esempio per la somma:

Siano $p_1 = 5$, $p_2 = 7$ i moduli di un sistema residuo. Rappresentiamo in questo sistema i numeri 12 e 18:

$12 = (2, 5)$

$18 = (3, 4)$

La somma:

$12 + 18 = 30 = (0, 2)$

si ottiene, espressa nel sistema residuo, sommando separatamente,

modulo 5 e modulo 7, le coppie di cifre relative a ciascun modulo:

$12 + 18 = (|2 + 3|_5, \ |5 + 4|_7) = (0, 2)$.

PARTE SECONDA

1) *RILEVAZIONE E LOCALIZZAZIONE DI ERRORI NEI SISTEMI NUMERICI RIDONDANTI DELLE CLASSI RESIDUE*

Nel sistema numerico delle classi residue, sia dato l'insieme di moduli $p_1, p_2, \ldots\ldots, p_n$, mutuamente primi.

Definizione. Chiameremo *campo di lavoro* del sistema la quantità:

$$P = p_1 \cdot p_2 \cdot \ldots\ldots \cdot p_n$$

Sia p_{n+1} un altro modulo (modulo ridondante o modulo di controllo), primo rispetto a $p_1, p_2, \ldots\ldots, p_n$.

Definizione. Chiameremo *campo completo* del sistema la quantità:

$$P = p_{n+1} \cdot P.$$

Definizione. Chiameremo numeri regolari i numeri compresi nell'intervallo $[0, P)$, irregolari i numeri compresi nell'intervallo $[P, P)$.

Se conveniamo di operare con numeri dell'intervallo $[0, P)$ espressi nel più ampio intervallo $[0, P)$, durante l'elaborazione e trasmissione dei numeri sarà condizione sufficiente per la rilevazione di errore la presenza di un numero $A \geqslant P$.(*)

Enunciamo alcuni teoremi fondamentali:

(*) Si noti che la parte di controllo partecipa alle stesse proprietà aritmetiche della parte di lavoro del codice. La parte di controllo, cioè, fornisce una informazione ridondante della stessa natura di quella fornita dai moduli di lavoro.

Teorema 1. Sia $p_1, p_2, \ldots\ldots, p_n, p_{n+1}$ (*) un sistema di moduli che soddisfa la condizione:

$$p_i \leqslant p_{n+1} \text{ per } i = 1, 2, \ldots\ldots, n+1$$

e sia $A\ (\alpha_1, \alpha_2, \ldots\ldots, \alpha_i, \ldots\ldots, \alpha_n, \alpha_{n+1})$ un numero regolare.
Allora il numero $\overline{A}\ (\alpha_1, \alpha_2, \ldots\ldots, \overline{\alpha}_i, \ldots\ldots, \alpha_n, \alpha_{n+1})$ con $i = 1, \ldots\ldots, n+1$ ottenuto da A cambiando *una* cifra è irregolare.

Dimostrazione. Dalla teoria delle congruenze si ha che:

$$\overline{A} \equiv A \pmod{\frac{P}{p_i}}$$

dove:

$$\frac{P}{p_i} \geqslant \frac{P}{p_{n+1}} = P$$

Si ha cioè che A ed $\overline{A}$ differiscono fra loro di multipli di

$$\frac{P}{p_i} .$$

Dalla regolarità di A segue quindi l'irregolarità di $\overline{A}$, cioè $\overline{A}$ non può essere contenuto nell'intervallo $[0, P)$.
E' inoltre evidente che esiste una sola cifra $\overline{\alpha}_i$ (cioè $\overline{\alpha}_i = \alpha_i$) che può ritrasformare $\overline{A}$ in un numero regolare, e precisamente in A .

Corollario 1.1. Sotto le stesse ipotesi del teorema 1 sia ora $\overline{A}$ un numero generato da A per variazione di più cifre re-

(*) Parlando di moduli, sottintenderemo sempre, in ciò che segue, che essi sono mutuamente primi.

lative a moduli il cui prodotto ξ sia tale che $\xi < p_{n+1}$. Allora $\bar{A}$ è irregolare.

La dimostrazione è analoga a quella del teorema considerando come unico modulo il prodotto dei moduli ξ .

Definizione. Il numero A_i; compreso nell'intervallo $[0, P/p_i)$, ottenuto da A eliminando la cifra α_i è detto "proiezione" di A rispetto al modulo p_i .

Definizione. Un sistema di moduli $p_1, p_2, \ldots\ldots, p_n, p_{n+1}$ per cui:

$$p_1 < p_2 < \ldots\ldots < p_n < p_{n+1}$$

è detto sistema ordinato di moduli.

Teorema 2. Sia $p_1, p_2, \ldots\ldots, p_n, p_{n+1}$ un sistema di moduli che soddisfa alla condizione:

$p_i \leqslant p_{n+1}$ per $i = 1, 2, \ldots\ldots, n+1$.

Allora condizione necessaria e sufficiente affinchè un numero A sia regolare è che:

$$A_1 = A_2 \ldots\ldots = A_{n+1}$$

Dimostrazione. Necessità. Se il numero è regolare, poichè $p_i \leqslant p_{n+1}$ $(i = 1, \ldots\ldots, n+1)$:

$$A_1 = A_2 = \ldots\ldots = A_{n+1}$$

Sufficienza. Si abbia:

$$A_1 = A_2 = \ldots\ldots = A_{n+1} = \xi < \frac{P}{p_{n+1}}$$

Ciò equivale a scrivere, per $i = 1, \ldots\ldots, n+1$:

$$A \equiv A_i \pmod{\frac{P}{p_i}}$$

$$A \equiv \xi \pmod{\frac{P}{p_i}}$$

Dalla teoria delle congruenze è noto che se una stessa congruenza vale per più moduli, vale anche per il modulo m.c.m. dei moduli. Cioè:

$$A \equiv \xi \pmod{P}$$

Per essere A compreso nell'intervallo $[0, P)$, segue:

$$A = \xi < \frac{P}{p_{n+1}}$$

cioè A è regolare.

Teorema 3. Sia $p_1, p_2, \ldots\ldots, p_n, p_{n+1}$ un sistema di moduli che soddisfa alla condizione:

$$p_i \leqslant p_{n+1} \quad \text{per} \quad i = 1, 2, \ldots\ldots, n+1$$

Allora se le proiezioni A_i ed A_j $(i \neq j \quad 1 \leqslant i, \ j \leqslant n+1)$ di un numero A coincidono, segue:

$$A < \frac{P}{\max (p_i, p_j)}$$

Dimostrazione. Si ha:

$$A_i \equiv A \pmod{\frac{P}{p_i}} \qquad A_i < P/p_i$$

$$A_j \equiv A \pmod{\frac{P}{p_j}} \qquad A_j < P/p_j$$

ma, per ipotesi:

$$A_i = A_j = \xi$$

per cui:

$$A \equiv \xi \pmod{P}$$

ovvero

$$A = \xi < \frac{P}{\max\,(p_i,\ p_j)}$$

Corollario 3.1. Nel sistema di moduli del Teorema 3, condizione necessaria e sufficiente affinchè un numero A sia regolare è che

$A_i = A_{n+1}$ $(1 \leqslant i \leqslant n)$.

Corollario 3.2. Nel sistema di moduli del Teorema 3, condizione necessaria e sufficiente affinchè un numero A sia regolare è che:

$$A_i = A_j < \frac{P}{p_{n+1}} \quad \text{per} \quad 1 \leqslant i,\ j \leqslant n,\ i \neq j\ .$$

Teorema 4. Sia $p_1, p_2, \ldots\ldots, p_n, p_{n+1}$ un sistema di moduli che soddisfa alla condizione:

$$p_i \leqslant p_{n+1} \quad \text{per} \quad i = 1, 2, \ldots\ldots, n+1\ .$$

Allora, se la proiezione A_i di un numero *irregolare* A soddisfa la condizione:

$$A_i > \frac{P}{p_{n+1}} \tag{1}$$

il numero A non può pensarsi generato da numero regolare per variazione della cifra i.ma.

Dimostrazione. Infatti, se A fosse generato da un numero regolare per variazione della cifra i.ma, tutte le altre cifre sarebbero quelle del numero regolare e, poichè A_i trascura proprio α_i, A_i dovrebbe essere regolare.

Corollario 4.1. Se la (1) è verificata per ogni i = 1, 2, ..., n allora il numero irregolare A può pensarsi generato da un numero regolare per variazione sulla cifra (n+1)-ma.

Teorema 5. Sia $p_1, p_2, \ldots\ldots, p_n, p_{n+1}$ un sistema ordinato di moduli.

Allora, se un numero irregolare A soddisfa la condizione:

$$\frac{P}{p_{n+1}} \leqslant A < \frac{P}{p_j}$$

il numero A non può pensarsi generato da un numero regolare per variazione di *una* cifra relativa ai moduli $p_1, p_2, \ldots\ldots, p_j$.

Dimostrazione. Ammettendo, per assurdo, che il numero A sia generato da un numero regolare $\overline{A}$ per variazione della cifra α_i $(1 \leqslant i \leqslant j)$, si avrà:

$$A \equiv \overline{A} \pmod{\frac{P}{p_i}}$$

con:

$$\frac{P}{p_i} \geqslant \frac{P}{p_j} \quad \text{per} \quad 1 \leqslant i \leqslant j$$

Quindi, essendo A compreso nell'intervallo $[\frac{P}{p_{n+1}}, \frac{P}{p_j})$

il numero $\overline{A}$ non potrà essere compreso nell'intervallo:

$[0, \frac{P}{p_{n+1}})$, dovendo A ed $\overline{A}$ differire di multipli di $\frac{P}{p_i}$.

Definizione. Diremo che un numero irregolare $\overline{A}$ è un numero avente k alternative di correzione (o semplicemente k-alternativo) se esistono k numeri regolari $A_1, A_2, \ldots\ldots, A_k$ ognuno dei qua-

li differisce da $\overline{A}$ per la cifra relativa ad uno dei moduli. L'insieme dei moduli sui quali $A_1, A_2, \ldots, A_k$ differiscono da $\overline{A}$ sarà chiamato insieme alternativo di $\overline{A}$.

E' evidente che le proiezioni di un numero irregolare $\overline{A}$ relative ai moduli dell'insieme alternativo sono regolari e, viceversa, che se una proiezione di $\overline{A}$ relativa ad un certo modulo è regolare, questo modulo appartiene all'insieme alternativo.

Teorema 6. In un insieme ordinato di moduli $p_1, p_2, \ldots, p_n, p_{n+1}$, condizione necessaria e sufficiente affinchè l'insieme alternativo di un qualunque numero irregolare $\overline{A}$ sia composto al più di due moduli è che: $p_{n+1} > p_n \cdot p_{n-1}$

Dimostrazione. E' evidente che p_{n+1} appartiene *sempre* all'insieme alternativo.

Necessità. Sia $\overline{A}$ un qualunque numero irregolare avente la proiezione $\overline{A}_k$ $(1 \leqslant k \leqslant n)$ regolare. Si avrà:

$$\overline{A} = \overline{A}_k + \alpha_k \frac{P}{p_k} \tag{1}$$

con:

$$0 \leqslant \overline{A}_k \leqslant \frac{P}{p_{n+1}} - 1 \tag{2}$$

$$1 \leqslant \alpha_k \leqslant p_k - 1 \tag{3}$$

Sia poi $\overline{A}_i$ una qualunque altra proiezione di $\overline{A}$ $(i \neq k, 1 \leqslant i \leqslant n)$. Si avrà:

$$\overline{A} = \overline{A}_i + \alpha_i^* \frac{P}{p_i} \tag{4}$$

dove α_i^* è un opportuno intero dell'intervallo $[0, p_i)$.

Ma $\overline{A}_i$ sarà irregolare:

$$\frac{P}{p_{n+1}} \leqslant \overline{A}_i \leqslant \frac{P}{p_i} - 1 \qquad (5)$$

Combinando la (1) con la (4):

$$\overline{A}_i = \overline{A}_k + \alpha_k \frac{P}{p_k} - \alpha_i^* \frac{P}{p_i} \qquad (6)$$

Sostituendo $\overline{A}_i$ nella (5):

$$\frac{P}{p_{n+1}} \leqslant \overline{A}_k + \alpha_k \frac{P}{p_k} - \alpha_i^* \frac{P}{p_i} \leqslant \frac{P}{p_i} - 1 \qquad (7)$$

Le (2), (3), (7) riassumono le ipotesi della condizione necessaria:

$$0 \leqslant \overline{A}_k \leqslant \frac{P}{p_{n+1}} - 1 \qquad (2)$$

$$1 \leqslant \alpha_k \leqslant p_k - 1 \qquad (3)$$

$$\frac{P}{p_{n+1}} \leqslant \overline{A}_k + \alpha_k \frac{P}{p_k} - \alpha_i^* \frac{P}{p_i} \leqslant \frac{P}{p_i} - 1 \qquad (7)$$

Determiniamo il valore di α_i^* . La (7) può scriversi:

$$-\frac{P}{p_{n+1}} + \alpha_k \frac{P}{p_k} - \alpha_i^* \frac{P}{p_i} \geqslant -\overline{A}_k$$

$$\frac{P}{p_{n+1}} - \frac{P}{p_i p_k}(\alpha_k p_i - \alpha_i^* p_k) \leqslant \overline{A}_k \qquad (7')$$

$$\frac{P}{p_i} - 1 - \frac{P}{p_i p_k}(\alpha_k p_i - \alpha_i^* p_k) \geqslant \overline{A}_k \qquad (7'')$$

La (7'), tenendo conto della parte destra della (2):

$$\frac{P}{p_{n+1}} - \frac{P}{p_i p_k}(\alpha_k p_i - \alpha_i^* p_k) \leqslant \frac{P}{p_{n+1}} - 1$$

$$\frac{P}{p_{n+1}} - \frac{P}{p_i p_k}(\alpha_k p_i - \alpha_i^* p_k) < \frac{P}{p_{n+1}}$$

$$\alpha_k p_i - \alpha_i^* p_k > 0 \qquad (8')$$

La (7''), tenendo conto della parte sinistra della (2):

$$\frac{P}{p_i} - 1 - \frac{P}{p_i p_k}(\alpha_k p_i - \alpha_i^* p_k) \geqslant 0$$

$$\frac{P}{p_i} - \frac{P}{p_i p_k}(\alpha_k p_i - \alpha_i^* p_k) > 0$$

$$\frac{1}{p_k}(\alpha_k p_i - \alpha_i^* p_k) < 1$$

$$\alpha_k p_i - \alpha_i^* p_k < p_k \qquad (8'')$$

Cioè, riassumendo:

$$0 < \alpha_k p_i - \alpha_i^* p_k < p_k \qquad (8)$$

Da cui si deduce:

$$\alpha_i^* = \left[\frac{\alpha_k p_i}{p_k}\right]$$

ed inoltre:

$$\alpha_k p_i - \alpha_i^* p_k = |\alpha_k p_i| p_k \qquad (9)$$

Sostituendo la (9) nella (7):

$$\frac{P}{p_{n+1}} \leqslant \bar{A}_k + \frac{P}{p_i p_k} \cdot |\alpha_k p_i|_{p_k} \leqslant \frac{P}{p_i} - 1 \qquad (10)$$

che dovrà valere per qualsiasi valore di $\overline{A}_k$ compreso nell'intervallo $[0, \frac{P}{p_{n+1}})$.

Dalla (10):

$$-\overline{A}_k \leqslant -\frac{P}{p_{n+1}} + \frac{P}{p_i p_k} \cdot |\alpha_k p_i|_{p_k}$$

$$\frac{P}{p_{n+1}} - \frac{P}{p_i p_k} \cdot |\alpha_k p_i|_{p_k} \leqslant \overline{A}_k \leqslant \frac{P}{p_{n+1}} - 1 - \frac{P}{p_i p_k} |\alpha_k p_i|_{p_k} \qquad (11)$$

Tenendo conto della (2) si ha che la (11) sarà verificata se:

$$\frac{P}{p_{n+1}} - \frac{P}{p_i p_k} \cdot |\alpha_k p_i|_{p_k} \leqslant 0$$

$$\frac{1}{p_{n+1}} \leqslant \frac{|\alpha_k p_i|_{p_k}}{p_i p_k}$$

$$p_{n+1} \geqslant \frac{p_i p_k}{|\alpha_k p_i|_{p_k}} \qquad (12)$$

e se:

$$\frac{P}{p_i} - 1 - \frac{P}{p_i p_k} |\alpha_k p_i|_{p_k} \geqslant \frac{P}{p_{n+1}} - 1$$

$$\frac{p_k}{p_i p_k} - \frac{|\alpha_k p_i|_{p_k}}{p_i p_k} \geqslant \frac{1}{p_{n+1}}$$

$$p_{n+1} \geqslant \frac{p_i p_k}{p_k - |\alpha_k p_i|_{p_k}} \qquad (13)$$

Le (12) e (13) dovranno essere verificate per ogni α_k $(1 \leqslant \alpha_k \leqslant p_k - 1)$. D'altra parte, poichè $(p_i, p_k) = 1$, se α_k varia in un sistema completo di residui anche:

$$|\alpha\, p_i|_{p_k} \quad \text{e} \quad p_k - |\alpha_k p_i|_{p_k}$$

variano in un sistema completo di residui e, poichè ad $\alpha_k = 0$ corrisponde $|\alpha_k p_i|_{p_k} = 0$ il minimo dei restanti valori è 1.

Quindi, per il variare di α_k le (12) e (13) si riscrivono:

$$p_{n+1} \geqslant p_i p_k \tag{14}$$

Dovendo la (14) valere per ogni possibile coppia p_i, p_k $(i \neq k, \quad 1 \leqslant i, \quad k \leqslant n)$:

$$p_{n+1} > p_n p_{n-1} \tag{15}$$

il che dimostra la condizione necessaria.

Sufficienza. Ammettiamo che valga la (15) e che, per assurdo, esistano due proiezioni $\overline{A}_i$ ed $\overline{A}_k$ regolari:
$(i \neq k, \quad 1 \leqslant i, \quad k \leqslant n)$

$$\overline{A}_k = \overline{A} - \alpha_k \frac{P}{p_i}$$

$$\overline{A}_i = A - \alpha_i \frac{P}{p_i}$$

$$\overline{A}_i = \overline{A}_k + \alpha_k \frac{P}{p_k} - \alpha_i \frac{P}{p_i}$$

Se $\overline{A}_i > \overline{A}_k$ ciò che può supporsi senza ledere la generalità, necessariamente:

$$0 < \alpha_k \frac{P}{p_k} - \alpha_i \frac{P}{p_i} < \frac{P}{p_{n+1}}$$

ovvero:

$$p_{n+1} < \frac{p_i p_k}{\alpha_k p_i - \alpha_i p_k}$$

$$\alpha_k p_i - \alpha_i p_k > 0$$

contrariamente alla (15).

Il teorema 6 dà la condizione necessaria e sufficiente affinchè l'insieme alternativo di un qualunque numero irregolare sia composto al più da due moduli. Sotto tale condizione un numero irregolare potrà pensarsi generato al più da due numeri regolari per variazione di una cifra.

Per eliminare l'ambiguità rimanente, supponiamo di sostituire l'unico modulo di controllo finora considerato con più moduli $p_{n+1}, p_{n+2}, \ldots\ldots, p_{n+r}$, primi fra loro e rispetto agli altri moduli del sistema.

Teorema 7. In un sistema di moduli $p_1, p_2, \ldots\ldots, p_n, p_{n+1}, \ldots\ldots, p_{n+r}$ per cui:

$p_{n+1} \cdot p_{n+2}, \ldots\ldots, p_{n+r} > p_i$ per $i = 1, 2, \ldots\ldots, n + r$

condizione necessaria e sufficiente affinchè l'insieme alternativo di un qualunque numero irregolare sia composto al più da un modulo è che:

$$p_{n+1} \cdot p_{n+2} \cdot \ldots\ldots \cdot p_{n+r} \geqslant p_i \cdot p_j$$

con $i \neq j$, $1 \leqslant i, j \leqslant n + r$

Dimostrazione. Necessità. Sia $\overline{A}$ un qualunque numero irregolare avente la proiezione $\overline{A}_j$ $(1 \leqslant j \leqslant n + r)$ regolare. Si avrà:

$$\overline{A} = \overline{A}_j + \alpha_j \frac{P}{p_j} \tag{1}$$

con:

$$0 \leqslant \overline{A}_j \leqslant \frac{P}{p_{n+1} \cdot p_{n+2} \cdots p_{n+r}} - 1 \tag{2}$$

$$1 \leqslant \alpha_j \leqslant p_j - 1 \tag{3}$$

Sia poi $\overline{A}_i$ una qualunque altra proiezione di $\overline{A}$ $(i \neq j,$ $1 \leqslant i \leqslant n + r)$. Si avrà:

$$\overline{A} = \overline{A}_i + \alpha_i^* \frac{P}{p_i} \tag{4}$$

dove α_i^* è un opportuno intero dell'intervallo $[0, p_i)$.
Ma $\overline{A}_i$ sarà irregolare:

$$\frac{P}{p_{n+1} \cdot p_{n+2} \ldots p_{n+r}} \leqslant \overline{A}_i \leqslant \frac{P}{p_i} - 1 \tag{5}$$

In maniera del tutto analoga al Teorema 6 si ottiene, dopo vari passaggi:

$$p_{n+1} \cdot p_{n+2} \cdots \cdots \cdots p_{n+r} \geqslant p_i \, p_j \tag{6}$$

e, dovendo la (6) valere per ogni possibile coppia p_i, p_j $(i \neq j,\ 1 \leqslant i,\ j \leqslant n + r)$ segue la condizione necessaria.

Sufficienza. La dimostrazione è assolutamente analoga a quella data per il Teorema 6.

Osservazioni

Volutamente, nel corso di questo paragrafo, ci si è astenuti da precisi riferimenti agli errori.

E' evidente, infatti, che le proprietà messe in luce saranno sfruttate diversamente al variare della classe di errori considerata.

Esamineremo ora con maggior dettaglio la classe di errori che si presenta con maggior frequenza, cioè gli errori su singola cifra residua, che chiameremo semplicemente, in seguito, *errori singoli*.

Dal Teorema 1 discende che un numero A, esente da errore e quindi regolare, per effetto di errore singolo genera un numero irregolare $\overline{A}$, purchè il modulo di controllo soddisfi alla condizione di essere maggiore di ciascuno dei moduli di lavoro.

Se quindi ci si limita a considerare gli errori singoli, sarà condizione necessaria e sufficiente perchè sia presente un errore il fatto che un numero sia irregolare.

Sui possibili metodi per rilevare l'irregolarità di un numero appare inutile dilungarsi. Ci limiteremo a rinviare al Teorema 2 ed ai Corollari 3.1 e 3.2 che possono dare utili suggerimenti.

Più difficile appare il discorso quando si passa alla localizzazione dell'errore. I Teoremi 4 e 5 danno infatti solo delle condizioni sufficienti a garantire l'*esattezza* di una o più cifre.

Tuttavia, impiegando moduli di controllo che soddisfino la condizione imposta dal Teorema 6, le cose migliorano notevolmente. In tal caso infatti un numero irregolare $\overline{A}$ possiede al massimo due proiezioni regolari, cioè $\overline{A}_{n+1}$ ed al più una proiezione su un modulo di lavoro.

Se nella trasmissione o elaborazione di dati si rileva un numero $\overline{A}$ irregolare saremo in grado, quindi, di dire che la cifra errata è α_{n+1} se la sola proriezione regolare è quella relativa al modulo ridondante.

Nel caso in cui esistano due proiezioni regolari, ci sarà am

biguità, cioè non si saprà dire se l'errore si sia prodotto sul modulo di controllo o sul modulo di lavoro che presenta proiezione regolare.

Per eliminare questa ambiguità occorreranno almeno due moduli ridondanti, come risulta dal Teorema 7, che dà le condizioni necessarie e sufficienti a garantire la presenza di una sola proiezione regolare. In questo caso, per localizzare il guasto sarà sufficiente analizzare le proiezioni del numero irregolare: la cifra errata sarà quella relativa al modulo che presenta proiezione regolare ed il numero esatto sarà la proiezione regolare stessa.

2) RILEVAZIONE E LOCALIZZAZIONE DI PARTICOLARI SOTTOCLASSI DI ERRORE SINGOLO CON UN SOLO MODULO DI CONTROLLO

Parlando di errore singolo si è ammesso che questo potesse essere qualsiasi, cioè che una cifra potesse cambiare in qualsiasi altra cifra, all'interno di un singolo modulo.

Occorre tuttavia tener presente che, per una data unità aritmetica operante su un dato sistema numerico residuo, potranno essere individuate diverse classi di guasti con diverse probabilità di occorrenza. E', per esempio, plausibile, pensare che i guasti più probabili siano quelli che interessano un singolo bit di una singola cifra residua.

Ci proponiamo allora di vedere se sia possibile ridurre la ridondanza del modulo di controllo limitando le classi di errore singolo possibili. Per far questo è necessario tornare ad analizzare da vicino il Teorema 6, mettendo il luce alcune interessanti proprietà. Il modo in cui tali proprietà possono essere utilizzate per la correzione di errori interessanti un solo bit sarà discusso nel paragrafo successivo.

Riscriviamo la (12) e la (13) del Teorema 6:

$$p_{n+1} \geqslant \frac{p_i p_k}{|\alpha_k p_i|_{p_k}} \qquad (A)$$

$$p_{n+1} \geqslant \frac{p_i p_k}{p_k - |\alpha_k p_i|_{p_k}} \qquad (B)$$

Sotto le ipotesi del Teorema 6, la (A) e la (B) dovevano essere valide per ogni possibile coppia p_i, p_k ($i \neq k$, $1 \leqslant i$, $k \leqslant n$) e per

qualsiasi α_k $(1 \leqslant \alpha_k \leqslant p_k - 1)$.

Ma se α_k varia in $[1, p_k - 1]$, i denominatori delle (A) e (B) assumono sempre il valore 1, come minimo valore.

Imponiamo allora che i parametri α_k (che chiameremo "*parametri di errore*") non possano assumere tutti i valori dell'intervallo $[1, p_k - 1]$, ma solo quei valori per cui:

$$|\alpha_k p_i|_{p_k},\ p_k - |\alpha_k p_i|_{p_k} \geqslant n_k \tag{1}$$

dove:

$$n_k = \varphi(p_k) \tag{2}$$

Le (A) e (B) si riscrivono:

$$p_{n+1} \geqslant \frac{p_i p_k}{n_k} \tag{3}$$

Esaminiamo attentamente la (1) e (2).

Teorema 8. Se, per un certo α_k^* :

$$|\alpha_k^*\ p_i|_{p_k},\ p_k - |\alpha_k^*\ p_i|_{p_k} \geqslant n_k \tag{4}$$

allora, per $\bar{\alpha}_k^* = p_k - \alpha_k^*$:

$$|\bar{\alpha}_k^*\ p_i|_{p_k},\qquad p_k - |\bar{\alpha}_k^*\ p_i|_{p_k} \geqslant n_k \tag{5}$$

Dimostrazione

$$|\bar{\alpha}_k^* p_i|_{p_k} = |(p_k - \alpha_k^*) p_i|_{p_k} = |p_k - \alpha_k^*\ p_i|_{p_k} = p_k - |\alpha_k^*\ p_i|_{p_k}$$

$$p_k - |\bar{\alpha}_k^*\ p_i|_{p_k} = |\alpha_k^*\ p_i|_{p_k}$$

cioè le (5) equivalgono alle (4).

Teorema 9. Il numero di α_k che soddisfano alla (1) è:

$$N_k = 2\left\{\left[\frac{p_k}{2}\right] - n_k\right\} + 1 \qquad (6)$$

se p_k è pari.

$$N_k = 2\left\{\left[\frac{p_k}{2}\right] - n_k + 1\right\} \qquad (7)$$

se p_k è dispari.

Dimostrazione

Poichè α_k varia in un sistema completo di residui (escluso lo 0, nel qual caso $|\alpha_k\ p_i|_{p_k} = 0$) il massimo valore raggiunto dal 1° membro della (1) sarà:

$$\left[\frac{p_k}{2}\right]$$

Se p_k è pari, questo valore sarà raggiunto da un determinato α_{ko} che coincide con il suo complemento al modulo p_k. Infatti:

$$|\alpha_{ko}\ p_i|_{p_k} = \left[\frac{p_k}{2}\right]$$

$$p_k - |\alpha_{ko}\ p_i|_{p_k} = \left[\frac{p_k}{2}\right]$$

$$|\alpha_{ko}\ p_i|_{p_k} = p_k - |\alpha_{ko}\ p_i|_{p_k} = |p_k - |\alpha_{ko} p_i|_{p_k}|_{p_k} = |(p_k - \alpha_{ko}) p_i|_{p_k}$$

da cui, per essere $1 \leqslant \alpha_{ko}$, $p_k - \alpha_{ko} \leqslant p_k - 1$:

$$\alpha_{ko} = p_k - \alpha_{ko}$$

Se p_k è dispari il valore $\left[\frac{p_k}{2}\right]$ sarà invece raggiunto da due distinti α_k.

Per entrambi i casi (p_k pari o dispari) esisteranno poi due valori α_k per cui il membro sinistro della (1) vale:

$$\left[\frac{p_k}{2}\right] - 1$$

e, proseguendo, esisteranno altri due valori di α_k per cui il membro sinistro della (1) vale:

$$\left[\frac{p_k}{2}\right] - 2$$

e così via, diminuendo di una unità.
Gli α_k che soddisfano la (1) saranno quindi:

$$2\left\{\left[\frac{p_k}{2}\right] - n_k\right\}$$

oltre ad uno o due valori iniziali a seconda che p_k sia pari o dispari.

Corollario 9.1. Affinchè la (1) possegga soluzioni per α_k deve essere:

$$n_k \leqslant \left[\frac{p_k}{2}\right]$$

Riscriviamo la (1) nella forma:

$$|\pm\alpha_k p_i|_{p_k} \geqslant n_k \qquad (1')$$

se, per ogni $p_i \neq p_k$ $(1 \leqslant i, \quad k \leqslant n)$:

$$|\pm p_i|_{p_k} = \text{costante} = C\,(p_k) \qquad (8)$$

allora la (1') assume la forma:

$$|\pm\alpha_k C\,(p_k)|_{p_k} \geqslant n_k \qquad (1'')$$

cioè i valori di α_k che soddisfano la (1) non variano al variare di p_i.

Il valore di n_k resta determinato dalla particolare

classe di errori che si vogliono localizzare sul modulo p_k, cioè dal numero di parametri di errore α_k che si rendono necessari.

Limitazione inferiore del modulo di controllo

Riprendiamo in esame la (3):

$$p_{n+1} \geqslant \frac{p_i p_k}{n_k} \tag{3}$$

Assunto, ad esempio, p_k dispari, sostituendo la (7) nella (3):

$$p_{n+1} \geqslant \frac{p_i p_k}{\left[\frac{p_k}{2}\right] + 1 - \frac{N_k}{2}} \tag{9}$$

dove N_k è il numero di parametri di errore α_k che si rendono necessari. Con buona approssimazione:

$$p_{n+1} \geqslant \frac{p_i p_k}{\frac{p_k}{2} + 1 - \frac{N_k}{2}} \tag{10}$$

Assumendo che il numero di α_k occorrenti per la localizzazione di una data classe di errori cresca linearmente con il numero di bits della parola, cioè che:

$$n_k = \sigma \cdot \log_2 p_k \tag{11}$$

otteniamo:

$$p_{n+1} \geqslant \frac{p_i p_k}{\frac{p_k}{2} + 1 - \frac{\sigma}{2} \cdot \lg_2 p_k} \tag{10'}$$

e, sviluppando $\lg_2 p_k$ in serie di Taylor, arrestandosi al secondo termine:

$$p_{n+1} \geqslant \frac{p_i p_k}{\frac{p_k}{2} + 1 - \frac{\sigma}{2}\left\{\frac{1}{lg_e 2} \cdot (p_k - 1) - \frac{1}{lg_e 2} \cdot \frac{(p_k - 1)^2}{2}\right\}}$$

(12)

$$p_{n+1} \geqslant \frac{p_i p_k}{p_k\left(\frac{1}{2} - \frac{\sigma}{lg_e 2}\right) + \frac{\sigma}{4 \cdot lg_e 2} \cdot p_k^2 + \frac{3\sigma}{4 \cdot lg_e 2} + 1}$$

Trascurando il termine $\frac{3\sigma}{4 \cdot lg_e 2} + 1$ e dividendo numeratore e denominatore per p_k:

$$p_{n+1} \geqslant \frac{p_i}{\frac{\sigma}{4 \cdot lg_e 2} \cdot p_k + \left(\frac{1}{2} - \frac{\sigma}{lg_e 2}\right)} \tag{13}$$

da cui risulta che il limite inferiore di p_{n+1} è con buona approssimazione inversamente proporzionale alla grandezza del modulo in errore. Supponendo il sistema di moduli ordinato si avrà quindi:

$$p_{n+1} \geqslant \frac{p_1 \cdot p_i}{n_1} \tag{14}$$

e, dovendo la (14) valere per ogni p_i ($i \neq k$, $1 \leqslant i$, $k \leqslant n$):

$$p_{n+1} \geqslant \frac{p_1 \cdot p_n}{n_1} \tag{15}$$

cioè, ricapitolando, sotto l'ipotesi (8) e (11) il limite inferiore di p_{n+1} sara determinato dai valori estremi (massimo e minimo) dei moduli di lavoro e dal numero di α_k necessari per la localizzazione della prescelta classe di errori sul modulo più piccolo.

Localizzazione di errori sul modulo di controllo

Analizziamo ora se sia possibile localizzare senza ambiguità particolari classi di errore (cioè errori caratterizzati da particolari α_{n+1}) sul modulo di controllo.

Se un numero irregolare $\overline{A}$ risulta generato da un numero regolare A per errore sulla cifra (n + 1) - ma, sarà della forma:

$$\overline{A} = A + \alpha_{n+1} \frac{P}{p_{n+1}} \tag{16}$$

Ricerchiamo, se esistono, dei valori di α_{n+1} tali che, per ogni A regolare, le proiezioni di $\overline{A}$ rispetto a tutti i moduli non ridondanti siano irregolari. La proiezione generica sarà della forma:

$$\overline{A}_i = \overline{A} - \alpha_i \frac{P}{p_i} \tag{17}$$

dove α_i è un opportuno valore compreso fra 0 e $p_i - 1$.

Combinando la (17) con la (16):

$$\overline{A}_i = A + \alpha_{n+1} \frac{P}{p_{n+1}} - \alpha_i \frac{P}{p_i}$$

Seguendo gli stessi ragionamenti del Teorema 6, la condizione necessaria e sufficiente per cui $\overline{A}_i$ è irregolare si scrive:

$$|\alpha_{n+1} \cdot p_i|_{p_{n+1}} \geqslant p_i \tag{18'}$$

$$p_{n+1} - |\alpha_{n+1} \cdot p_i|_{p_{n+1}} \geqslant p_i \tag{18''}$$

ovvero, con unica notazione:

$$|\pm \alpha_{n+1} \cdot p_i|_{p_{n+1}} \geqslant p_i \qquad (18)$$

La (18) dovrà essere valida per tutti i p_i $(1 \leqslant i \leqslant n)$.

Riassumendo, se esistono valori di α_{n+1} tali che la (18) sia soddisfatta per ogni p_i, gli errori caratterizzati da tali parametri saranno localizzabili senza ambiguità, cioè daranno luogo a proiezioni non ridondanti tutte irregolari.

Teorema 10. Se un valore α^*_{n+1} soddisfa la (18), allora anche il valore:

$$\bar{\alpha}_{n+1} = p_{n+1} - \alpha^*_{n+1}$$

soddisfa la (18).

La dimostrazione è del tutto analoga a quella del Teorema 8.

Se, per un determinato sistema di moduli, vale la relazione:

$$|\pm p_i|_{p_{n+1}} = \text{costante} = C\,(p_{n+1})$$

per ogni p_i $(1 \leqslant i \leqslant n)$, allora la (18) si scrive:

$$|\pm \alpha_{n+1} \cdot C\,(p_{n+1})|_{p_{n+1}} \geqslant p_i$$

ed, ammettendo il sistema ordinato:

$$|\pm \alpha_{n+1} \cdot C\,(p_{n+1})|_{p_{n+1}} \geqslant p_n \qquad (19)$$

Inoltre, se vale la (19) il numero di α_{n+1} che soddisfano sarà:

$$N_{n+1} = 2 \left\{ \left[\frac{p_{n+1}}{2} \right] \quad p_n \right\} + 1 \qquad (20')$$

se p_{n+1} è pari

$$N_{n+1} = 2 \left\{ \left[\frac{p_{n+1}}{2} \right] - p_n + 1 \right\} \qquad (20'')$$

se p_{n+1} è dispari.

Considerazioni sugli errori

Sia A un numero regolare. Per errore sulla cifra di ordine k ($1 \leqslant k \leqslant n + 1$) si otterrà il numero irregolare:

$$\overline{A} = A + \alpha_k \frac{P}{p_k} \qquad (21)$$

$$A = \overline{A}_k \qquad (22)$$

dove:

$$1 \leqslant \alpha_k \leqslant p_k - 1 \qquad (23)$$

Mettiamo in relazione il residuo esatto con il residuo errato. Prendendo la (21) modulo p_k:

$$\overline{r}_k = \left| r_k + \alpha_k \frac{P}{p_k} \right| p_k \qquad (24)$$

dove:

$\overline{r}_k$ è la cifra errata
r_k è la cifra esatta
$\overline{r}_k$, $r_k = 0, 1, \ldots\ldots, p_k - 1$
Per essere i moduli primi fra loro, inoltre:

$\overline{r}_k \neq r_k$
cioè:

$$k \frac{P}{p_k} \not\equiv 0 \pmod{p_k}$$

Teorema 11. Fissato α_k, esiste fra $\overline{r}_k$ ed r_k una corri-

spondenza biunivoca.

Dimostrazione. Evidentemente, ad ogni r_k della (24) corrisponde solo $\bar{r}_k$.
Viceversa, fissato un $\bar{r}_k$, questo corrisponderà ad un solo r_k.
Ammettiamo infatti, per assurdo, che, per $r'_k \neq r''_k$, sia:

$$\bar{r}_k = |r'_k + \alpha_k \frac{P}{p_k}|_{p_k}$$

$$\bar{r}_k = |r''_k + \alpha_k \frac{P}{p_k}|_{p_k}$$

si avrà:

$$|r'_k + \alpha_k \frac{P}{p_k}|_{p_k} = |r''_k + \alpha_k \frac{P}{p_k}|_{p_k}$$

ovvero:

$$|r'_k|_{p_k} = |r''_k|_{p_k}$$

$$r'_k = r''_k$$

contrariamente all'ipotesi.

Per un certo α_k, chiameremo r_k ed $\bar{r}_k$ rispettivamente (residuo) predecessore e successore.

Fissato ora un valore r_{k1}, formiamo, a partire da esso, una lista in cui ciascun elemento sia il successore dell'elemento che lo precede. Si avrà:

$$r_{k2} = \bar{r}_{k1} = |r_{k1} + \alpha_k \frac{P}{p_k}|_{p_k}$$

$$r_{k3} = \bar{r}_{k2} = |r_{k2} + \alpha_k \frac{P}{p_k}|_{p_k} = |r_{k1} + 2\alpha_k \frac{P}{p_k}|_{p_k}$$

.....

$$r_{ki} = \bar{r}_{k,i-1} = \left| r_{k1} + (i - 1)\ \alpha_k \frac{P}{p_k} \right|_{p_k} \qquad (25)$$

Noti quindi k, α_k e la lista dei successori, si determina il residuo esatto prendendo l'elemento che precede il residuo errato.

Caratteristiche della lista dei successori

Considerati due qualsiasi elementi della lista dei successori, $r_{k,i}, r_{k,i+1}$ con:

$$r_{k,i+1} = \left| r_{k,i} + \alpha_k \frac{P}{p_k} \right|_{p_k}$$

la differenza fra il successore e il predecessore:

$$r_{k,i+1} - r_{k,i} = \left| r_{k,i} + \alpha_k \frac{P}{p_k} \right|_{p_k} - r_{k,i}$$

considerata modulo p_k, dà:

$$\left| r_{k,i+1} - r_{k,i} \right|_{p_k} = \left| \alpha_k \frac{P}{p_k} \right|_{p_k} = E\ (\alpha_k) \qquad (26)$$

Dalla (26) risulta che:

a) La differenza, mod p_k, fra elementi consecutivi dalla lista dei successori, è una costante che dipende solo da α_k e da k, che chiameremo *passo* della lista relativa a k, α_k e che si identifica con l'errore.

b) Per un certo k, ad α_k distinti corrispondono distinti $E(\alpha_k)$.

Teorema 12. Fissati k, α_k il numero di elementi che compongono le liste dei successori è uguale per tutte le liste. Ciascuna

lista si richiude sul primo elemento (liste circolari). Inoltre il numero delle liste di successori è (α_k, p_k).

Dimostrazione. Scriviamo la (25) nella forma:

$$r_{k,n+1} = |r_{k1} + n \cdot \alpha_k \cdot \frac{P}{p_k}|_{p_k}$$

Sia $n_o \neq 0$ il più piccolo valore di n per cui:

$$n_o \, \alpha_k \frac{P}{p_k} \equiv 0 \pmod{p_k}$$

ovvero:

$$(n_o \, \alpha_k \frac{P}{p_k}, p_k) = p_k \tag{27}$$

Ciò significa che esisterà una lista, di lunghezza n_o, che si richiuderà sul primo elemento r_{k1}.
Ma n_o non dipende dal particolare valore di r_{k1}, cioè tutte le liste avranno lo stesso numero di successori.
Dimostriamo ora l'ultima parte del teorema.
Sia n_o il numero di elementi di ciascuna lista, l il numero di liste. Evidentemente:

$$n_o \cdot l = p_k$$

La (27), per essere:

$$(\frac{P}{p_k}, p_k) = 1$$

può scriversi:

$$(n_o \, \alpha_k \cdot \frac{P}{p_k}, p_k) = (n_o \cdot \alpha_k, p_k) = p_k \tag{28}$$

Sia ora:

$(\alpha_k, p_k) = d$

$\alpha_k = a_k \cdot d$

$p_k = \pi_k \cdot d$

$(a_k, \pi_k) = 1$

La (27) diviene:

$$(n_o \cdot \alpha_k \frac{P}{p_k}, p_k) = n_o \alpha_k, p_k) = (n_o \cdot d \cdot a_k, d \cdot \pi_k) =$$

$$= d \cdot (n_o \cdot a_k, \pi_k) = d \cdot (n_o, \pi_k) = p_k =$$

$$= \pi_k \cdot d \qquad (29)$$

$$(n_o, \pi_k) = \pi_k \qquad (30)$$

Il più piccolo n_o per cui, vale la (29) sarà:

$n_o = \pi_k$

cioè le liste saranno composte da π_k elementi e, poichè:

$n_o \cdot l = \pi_k \cdot l = p_k = \pi_k \cdot d$

segue:

$l = d$

ciò che dimostra il Teorema.

3) RILEVAZIONE E LOCALIZZAZIONE DI ERRORI SU SINGOLO BIT DI UNA SINGOLA CIFRA RESIDUA CON UN SOLO MODULO DI CONTROLLO

Si consideri ora una sottoclasse di errori singoli particolarmente significativa: gli errori su singolo bit di una singola cifra residua. Nella generalità dei casi, sono questi gli errori più probabili di una data unità aritmetica.

Fissato un insieme di moduli di lavoro, soddisfacenti, per quanto possibile, alla condizione (8) del paragrafo precedente, restano determinati, per ogni modulo di controllo, quei valori del parametro di errore che soddisfano le (A), (B) e (18) del pr. 2.

Sarà possibile rilevare e localizzare errori su singolo bit di cifra residua se e solo se il codice binario delle cifre relative ad ogni modulo soddisfa la *condizione* seguente:

Tutte le parole del codice binario che sono a distanza unitaria (cioè che differiscono per un bit) hanno come corrispondenti delle cifre residue che differiscono di quantità $E(\alpha_k)$ (pr. 2 (26)) determinate dai valori disponibili dei parametri di errore.

Se, ad esempio, si considerano le parole del codice binario di tre bits:

0 0 1
1 0 1

evidentemente a distanza unitaria, cui corrispondono, modulo p_i, rispettivamente le cifre residue 3 e 7, sarà possibile localizzare l'errore singolo 0 0 1 → 1 0 1 sul modulo p_i se risulterà disponibile un parametro α_i tale che $E(\alpha_i) = 7 - 3 = 4$.

Esempio

Siano $p_1 = 12$ e $p_2 = 13$ due moduli di lavoro e $p_3 = 47$

un modulo di controllo. I parametri di errore che soddisfano le (A), (B) e (18) del paragrafo 2 sono:
per il *primo* modulo:

α_1	$E(\alpha_1)$
4	8
5	7
6	6
7	5
8	4

per il *secondo* modulo:

α_2	$E(\alpha_2)$
4	7
5	12
6	4
7	9
8	1
9	6

per il *modulo di controllo:*

α_c	$E(\alpha_c)$
1	15
2	30
5	28
6	43
9	41
13	7
17	20
30	27
34	40

38	6
41	4
42	19
45	17
46	32

Codici binari che soddisfano la condizione richiesta sono:

a) per il *primo* modulo (tra parentesi il corrispondente valore residuo):

(0)	0000
(1)	1001
(2)	1010
(3)	1100
(4)	1111
(5)	0001
(6)	0010
(7)	0100
(8)	1000
(9)	1101
(10)	1110
(11)	0011

b) per il *secondo* modulo:

(0)	0000
(1)	0001
(2)	1101
(3)	1010
(4)	0010
(5)	0011
(6)	1100
(7)	0100

(8) 0101
(9) 1011
(10) 1110
(11) 0110
(12) 1000

c) per il *modulo di controllo:*

(0)	000000	(24)	001010
(1)	011001	(25)	110110
(2)	101000	(26)	011111
(3)	011100	(27)	010000
(4)	000001	(28)	001011
(5)	110111	(29)	111000
(6)	000100	(30)	001110
(7)	000010	(31)	010001
(8)	101100	(32)	100000
(9)	101010	(33)	010100
(10)	000101	(34)	010010
(11)	000011	(35)	111100
(12)	110000	(36)	100001
(13)	000110	(37)	010101
(14)	101101	(38)	100100
(15)	101110	(39)	100010
(16)	110001	(40)	010110
(17)	001000	(41)	111101
(18)	110100	(42)	100101
(19)	110010	(43)	100011
(20)	010111	(44)	011000
(21)	001001	(45)	100110
(22)	110101	(46)	111011
(23)	001100		

Si noti, ad esempio, che gli elementi del codice di sei bits

relativo al modulo di controllo:

101010 (9)

101110 (15)

a distanza unitaria, hanno come corrispondenti due numeri, 9 e 15 tali che:

$$|15 - 9|_{47} = 6$$

dove 6 è una degli $E(\alpha_c)$ disponibili sul modulo di controllo.

E' di particolare interesse notare che, ove si fosse voluto localizzare tutti gli errori singoli, per il Teorema 6 si sarebbe dovuto impiegare un modulo di controllo:

$$p_3 > 12 \times 13 = 156$$

ed inoltre vi sarebbe stata l'ambiguità di cui si è parlato al paragrafo 2.

4) RILEVAZIONE E LOCALIZZAZIONE DI PARTICOLARI SOTTOCLASSI DI ERRORE SINGOLO CON L'USO DI DUE MODULI DI CONTROLLO

Riprendiamo in esame il Teorema 7, analogamente a quanto è stato fatto nel paragrafo 2 per il Teorema 6. Dovrà essere:

$$p_{n+1}\ p_{n+2} > p_i \qquad (1)$$

per $i = 1, 2, \ldots\ldots, n$

ed inoltre:

$$p_{n+1}\ p_{n+2} \geqslant \frac{p_i p_k}{|\pm \alpha_k p_i|_{p_k}} \qquad (2)$$

per $i \neq k, \quad 1 \leqslant i, \quad k \leqslant n+2$

Se si considerano tutti i possibili errori singoli, la (2) dovrà essere verificata per ogni coppia p_i, p_k ($i \neq k, \quad 1 \leqslant i, \quad k \leqslant n+2$) e per ogni possibile α_k ($1 \leqslant \alpha_k \leqslant p_k - 1$), per cui segue la condizione necessaria e sufficiente del Teorema.

Se, al contrario, si impone che i parametri di errore possano assumere solo quei valori per cui:

$$|\pm \alpha_k\ p_i|_{p_k} \geqslant n_k \qquad (3)$$

dove:

$$n_k = \varphi\ (p_k) \qquad (4)$$

la (2) assume la forma:

$$p_{n+1}\ p_{n+2} \geqslant \frac{p_i p_k}{n_k} \qquad (5)$$

del tutto analoga alla (3) del paragrafo 2;

Valgono immutati i Teoremi 8, 9 ed il Corollario 9.1.
Sotto l'ipotesi che:

$$|\pm p_i|_{p_k} = \text{costante} = C\ (p_k) \tag{6}$$

per ogni $p_i \neq p_k$, $1 \leqslant i \leqslant n + 2$

si ha che i valori di α_k che soddisfano la (3) non variano al variare di p_i . Inoltre si ha, sotto l'ipotesi (6), per il limite inferiore sui moduli di controllo:

$$p_{n+1}\ p_{n+2} \geqslant \frac{p_m\ p_M}{n_m} \tag{7}$$

dove:

p_m è il modulo più piccolo

p_M è il modulo più grande

n_m è un parametro dipendente dalla particolare classe di errori che si vogliono localizzare sul modulo p_m .

5) *RILEVAZIONE E LOCALIZZAZIONE DI ERRORI SU SINGOLO BIT DI UNA SINGOLA CIFRA RESIDUA CON L'USO DI DUE MODULI DI CONTROLLO*

Valgono considerazioni analoghe a quelle del paragrafo 3. Fissato un insieme di moduli di lavoro, restano determinati, per ogni coppia di moduli di controllo, quei valori del parametro di errore che soddisfano la (2) del paragrafo 4.

Si conserva ovviamente immutato quanto detto a proposito della codifica in binario delle cifre residue.

Esempio

Siano $p_1 = 15$, $p_2 = 17$, $p_3 = 31$ tre moduli di lavoro e $p_4 = 8$, $p_5 = 23$ due moduli di controllo. I parametri di errore che soddisfano le (2) del paragrafo 4 sono:
per il *primo* modulo:

α_1	$E(\alpha_1)$
3	9
4	2
5	10
6	3
9	12
10	5
11	13
12	6

per il *secondo* modulo:

α_2	$E(\alpha_2)$
1	16
2	15
4	13
7	10
10	7
13	4
15	2
16	1

per il *terzo* modulo:

α_3	$E(\alpha_3)$
1	17
3	20
5	23
6	9
7	26
10	15
13	4
14	21
15	7
16	24
17	10
18	27
21	16
24	5
25	22
26	8
28	11
30	14

per il *primo modulo di controllo:*

α_{c1}	$E(\alpha_{c1})$
2	6
3	5
4	4
5	3
6	2

per il *secondo modulo di controllo:*

α_{c2}	$E(\alpha_{c2})$
1	13
2	3
5	19
7	22
10	15
11	5
12	18
13	8
16	1
18	4
21	20
22	10

Codici binari che soddisfano la condizione vista al paragrafo 3 sono:

a) per il *primo* modulo (tra parentesi il corrispondente valore residuo):

(0) 0000
(1) 0011
(2) 1000
(3) 0100
(4) 0111

d) per il *primo modulo di controllo:*

(0) 000
(1) 111
(2) 001
(3) 010
(4) 100
(5) 011
(6) 101
(7) 110

e) per il *secondo modulo di controllo:*

(0) 00000
(1) 00001
(2) 11100
(3) 00010
(4) 00100
(5) 00101
(6) 11111
(7) 00110
(8) 01000
(9) 01001
(10) 01111
(11) 01010
(12) 01100
(13) 10000
(14) 10001
(15) 01110
(16) 10010
(17) 10100
(18) 10101
(19) 10111
(20) 10110
(21) 11000
(22) 11001

BIBLIOGRAFIA

[1] Peterson, W.W. — *Error Correcting Codes*, John Wiley and Sons, Inc., N. Y., 1961.

[2] Watson, R.W. — *Error Detection and Correction and Other Residue Interacting Operations in a Redundant Residue Number System*, Ph. D. Dissertation, University of California, Berkeley, 1965.

[3] Szabo; Tanaka. — *Residue Aritmmetic and its Applications to Computer Technology*, Mc Graw, 1967.

[4] Avizienis, A. — *Arithmetic Error Codes: Cost and Effectiveness Studies for Application in Digital System Design*, 1971 International Symposium on Fault-Tolerant Computing Digest. Pasadena, 1971.

[5] Massey, J.L. — *Survey of Residue Coding for Arithmetic Errors*, ICC Bulletin, Vol. 3, 1964.

[6] Garner. — *Error Codes for Arithmetic Operations*, IEEE Trans. EC, 1966, pag. 763.

[7] Garner. — *The Classification of finite number numbers*, IFIP Congress 68, Edinburgh, Aug. 1968.

[8] Akuŝskiĭ, I.Ya; Yudickiĭ, D.I. — *Maŝinnaya Arifmetika v ostatočnyh Klassah*, Sovetskoe Radio, Moskva, 1960.

[9] Vinogravod, I.M. — *Elements of number Theory*, Dover Publications, Inc., New York. 1954.

I N D I C E

Introduzione ..... Pag. 1

PARTE PRIMA

Teoria delle congruenze ..... " 6

1. Generalità ..... " 6

2. Alcune proprietà delle congruenze ..... " 8

3. Rappresentazione dei numeri nel sistema delle classi residue ..... " 12

PARTE SECONDA

1. Rilevazione e localizzazione di errori nei sistemi numerici ridondanti delle classi residue ..... " 16

Osservazioni ..... " 29

2. Rilevazione e localizzazione di particolari sottoclassi di errore singolo con un solo modulo di controllo .... " 31

Limitazione inferiore del modulo di controllo ..... " 35

Localizzazione di errori sul modulo di controllo ..... " 37

Considerazioni sugli errori ..... " 39

Caratteristiche della lista dei successori ..... " 41

3. Rilevazione e localizzazione di errori su singolo BIT di una singola cifra residua con un solo modulo di controllo ..... " 44

4. Rilevazione e localizzazione di particolari sottoclassi di errore singolo con l'uso di due moduli di controllo. " 49

5. Rilevazione e localizzazione di errori su singolo BIT di una singola cifra residua con l'uso di due moduli di controllo ..... " 51

Bibliografia ..... " 56