Algebra Crittografia (Unimib)

24 gennaio 2022

wikitolearn
collaborative textbooks

This book is the result of a collaborative effort of a community of people like you, who believe that knowledge only grows if shared.
We are waiting for you!

Get in touch with the rest of the team by visiting http://join.wikitolearn.org

Capitolo 1

Crittografia

1.1 Teoremi ausiliari sugli interi

Teorema (388)

Esistono infiniti numeri primi.

Dimostrazione

Supponiamo che tutti e soli i primi siano $p_1, p_2, \ldots, p_r$. Costruisco allora il numero

$$p_1 * p_2 * \cdots * p_r + 1$$

Questo è un numero intero, che si potrà fattorizzare come prodotto di numeri primi. Questo numero non è divisibile per nessuno dei p_i , perché nella divisione per i p_i si ha resto 1. Questo contraddice il teorema fondamentale dell'aritmetica, e affinché il numero si possa fattorizzare, devono esistere altri numeri primi, e così via.

Teorema (389 Teorema di Eulero-Fermat)

Siano a, n interi positivi, con $M.C.D.(a, n) = 1$. Allora $a^{\phi(n)} \equiv 1 \mod n$.

Dimostrazione

Definisco l'insieme

$$I = \{[a_1], [a_2], \ldots, [a_l]\}$$

dove gli a_i sono tutti e soli gli elementi invertibili di $\mathbb{Z}_n$. Sappiamo che $l = \phi(n)$.

Considero poi l'insieme

$$I_a = \{[aa_1], [aa_2], \ldots, [aa_l]\}$$

ottenuto moltiplicando per a gli elementi di I . Allora $[aa_i]$ è ancora invertibile, infatti $M.C.D.(n, aa_1) = 1$ perché $M.C.D.(a, n) = 1$ per ipotesi e anche a, a_1 sono coprimi.

I però contiene tutti gli elementi invertibili in $\mathbb{Z}_n$, allora l'insieme costruito I_a è contenuto in I . Se $[aa_i] = [aa_j]$, allora $n \mid aa_i - aa_j = a(a_i - a_j)$, e siccome n è coprimo con a , allora $n \mid a_i - a_j$, cioè $[a_i] = [a_j]$, quindi due elementi di I_a sono esattamente l , cioè $I_a = I$.

Moltiplico tra loro gli elementi di I :

$$p_1 = [a_1] * [a_2] * \cdots * [a_l] = [a_1 a_2 \dots a_l]$$

e moltiplicando tra loro gli elementi di I_a , dovrei ottenere lo stesso risultato perché i due insiemi sono uguali:

$$p_2 = [aa_1][aa_2] \dots [aa_l] = [a^l a_1 a_2 \dots a_l].$$

Eguagliando p_1 e p_2 si deve avere

$$[a^l][a_1 a_2 \dots a_l] = [a_1 a_2 \dots a_l]$$

Pongo $x = [a_1 a_2 \dots a_l]$.

$$[a^l][x] = [x]$$

$[x]$ è invertibile, perché $M.C.D.(n, a^l) = 1$, allora semplificando per $[x]$:

$$[a^l] = [1]$$

cioè $a^l \equiv 1 \mod n$, e quindi $a^{\phi(n)} \equiv 1 \mod n$.

Osservazione (390)

L'ipotesi a, n coprimi è essenziale, infatti, se $M.C.D.(a, n) = d \neq 1$, allora a^k non è mai congruo a 1 modulo n quando $k \geq 1$, infatti se $d \mid a^k$, allora $d \nmid a^k - 1$. In generale, *l'equazione* $a^k \equiv 1 \mod n$ *con* n, a *non coprimi non ha mai soluzione.*

Esempio (391)

Per $n = 12$ e $a = 7$, il teorema dice che siccome $7, 12$ sono coprimi, allora $7^{\phi(12)} \equiv 1 \mod 12$. $\phi(12) = n * (1 - 1/2) * (1 - 1/3) = 12 * 1/2 * 2/3 = 4$, quindi $7^4 \equiv 1 \mod 12$. Questo si può verificare, infatti

$$7^4 - 1 = (7^2 - 1)(7^2 + 1) = 48 * 50$$

e $n = 12 \mid 48 * 50$ perché $6 \mid 48$ e $2 \mid 50$.

1.2 Metodo RSI

1.2.1 Introduzione

La crittografia consiste in tecniche che due persone stabiliscono per scriversi messaggi, in modo che non siano facilmente interpretabili da una terza persona.

La persona che riceve il messaggio criptato può decifrarlo solo se conosce la chiave utilizzata per decodificarlo.

In alcuni casi, la decifratura di un messaggio è molto più lunga della cifratura, anche se il codice crittografico è noto.

1.2.2 Descrizione del sistema RSA

Scelta della chiave Scegli un intero n abbastanza grande, e vogliamo trasmettere m dove $0 < m < n - 1$:

"abbastanza grande" significa che n deve permettere di rappresentare tutti i valori che potrebbero comparire nel messaggio.

Calcolo $\phi(n)$ e scelgo un intero e con $M.C.D.(e, \phi(n)) = 1$. Supponiamo che sia vera la seguente proprietà $*$:

$$t^{k\phi(n)+1} \equiv t \mod n \, \forall t \in [0, \ldots, n-1], \, \forall k \in \mathbb{Z}.$$

Prendo una soluzione b della congruenza

$$xe \equiv 1 \mod \phi(n)$$

tale soluzione esiste per come è stato scelto e , coprimo con $\phi(n)$.

Le informazioni pubbliche sono n e e . Tutto il resto (b) rimane privato in mano all'unica persona che può decifrare il messaggio.

Cifratura Preso m si calcola m^e e si prende l'unico numero $m^{\bar{e}}$ compreso tra 0 e $n - 1$ congruo a m^e modulo n . Trasmetto $m^{\bar{e}}$.

Decifratura Solo chi conosce b può decifrare il messaggio.

Calcolo $(m^{\bar{e}})^b$ e prendo l'unico intero compreso tra 0 e $n - 1$ a cui è congruo. Questo numero sarà m .

Esempio (392)

INFORMAZIONI PRELIMINARI: Prendo $n = 15$, $e = 3$, e calcolo $\phi(n) = \phi(3) * \phi(5) = 8$.

Prendo la soluzione b di $ex \equiv 1 \mod \phi(n)$, cioè di

$$3x \equiv 1 \mod 8,$$

in questo caso $b = 3$.

CIFRATURA: Supponiamo $m = 7$. Allora cerco $m^{\bar{e}}$ tale che $m^e \equiv m^{\bar{e}} \mod n$ e $0 < m^{\bar{e}} < n - 1$, cioè

$$7^3 \equiv \dots \mod 15,$$
$$7^2 \equiv 4 \mod 15, \longrightarrow 7^3 \equiv 28 \mod 15$$
$$28 \equiv 13 \mod 15, \longrightarrow 7^3 \equiv 13 \mod 15, \text{ per transitività delle congruenze.}$$

quindi $m^{\bar{e}} = 13$. Spedisco 13 , che diventa la parola cifrata.

DECIFRATURA: Cerco il numero m risolvendo $(m^{\bar{e}})^b \equiv m \mod n$, con $0 \leq m \leq n - 1$.

$$13^3 \equiv \dots \mod 15$$
$$13^2 \equiv 4 \mod 15$$
$$\longrightarrow 13^3 \equiv 13 * 4 \mod 15$$
$$52 \equiv 7 \mod 15$$
$$\longrightarrow 13^3 \equiv 7 \mod 15.$$

quindi $m = 7$, come deve.

1.2.3 Dimostrazione della decifratura

Devo mostrare che effettivamente $(m^{\bar{e}})^b \equiv m \mod n$, dove $m^{\bar{e}}$ è il messaggio cifrato.

Dimostrazione

Siccome $m^{\bar{e}} \equiv m^e \mod n$, si ha

$$(m^{\bar{e}})^b \equiv m^{eb} \mod n$$

b è stata costruita come soluzione della congruenza $be \equiv 1 \mod \phi(n)$, allora $be = 1 + \phi(n)k$ con k intero. Segue quindi che

$$m^{eb} \equiv m^{1+\phi(n)k} \mod n$$

e per la proprietà $* \ m^{1+\phi(n)k} \equiv m \mod n$, cioè, per transitività, $(m^{\bar{e}})^b \equiv m \mod n$.

Questo metodo crittografico funziona per il seguente motivo. Non conoscendo b , per trovarlo bisogna risolvere la congruenza $ex \equiv 1 \mod \phi(n)$ e quindi bisogna conoscere $\phi(n)$, quindi chi ha $\phi(n)$ riesce a trovare b . Per trovare $\phi(n)$ bisogna fattorizzare n in numeri primi, e la difficoltà sta proprio in questo, infatti non si conosce nessun algoritmo polinomiale che permetta di fattorizzare n in numeri primi. Quindi una persona che non conosce b , pur conoscendo e, n , non riesce a ricavare $\phi(n)$ con facilità e quindi ha difficoltà nel decifrare il messaggio.

Per fare in modo che $\phi(n)$ sia difficile da ottenere, n non può essere scelto primo. In genere n viene preso come prodotto di due numeri primi di 300 cifre.

1.2.4 Validità della proprietà ast

Proposizione (393 proprietà $\ast$)

Sia n un numero intero senza quadrati, cioè che non sia divisibile per il quadrato di un numero primo. Allora $t^{k\phi(n)+1} \equiv t \mod n$ per ogni t e per ogni k . (le ipotesi implicano anche un'ulteriore restrizione sulla scelta di n , che deve essere scelto senza quadrati)

Dimostrazione

Divido la dimostrazione in due casi:

- Caso 1: $M.C.D.(t, n) = 1$

Per il teorema di Eulero-Fermat, sappiamo che $t^{\phi(n)} \equiv 1 \mod n$, allora elevando alla k :

$$t^{k\phi(n)} \equiv 1 \mod n$$

moltiplicando per t :

$$t^{k\phi(n)+1} \equiv t \mod n.$$

- Caso 2: $n = p_1 * p_2 * \cdots * p_l$ dove i p_i sono primi distinti.

$$\phi(n) = (p_1 - 1) * (p_2 - 1) * \cdots * (p_l - 1)$$

Mostro prima che $t^{k\phi(n)+1} \equiv t \mod p_1$.

Se t è coprimo con p_1 , siccome $k\phi(n)$ è multiplo di $p_1 - 1$, applicando ancora Eulero-Fermat si ottiene:

$$t^{k\phi(n)} \equiv 1 \mod p_1$$
$$\longrightarrow t^{k\phi(n)+1} \equiv t \mod p_1$$

Quando invece $p_1 \mid t$, $t \equiv 0 \mod p_1$, perché è multiplo di p_1 , quindi l'equazione da dimostrare diventa $0 \equiv 0 \mod p_1$ che è vera.

Per ora abbiamo dimostrato che $t^{k\phi(n)+1} \equiv t \mod p_i$, per $i = 1, \ldots, l$. equivalentemente

$$p_i \mid t^{k\phi(n)+1} - t, \forall i$$

allora anche il prodotto dei primi divide il secondo membro, cioè

$$p_1 * p_2 * \cdots * p_l \mid t^{k\phi(n)+1} - t$$

cioè $n \mid t^{k\phi(n)+1} - t$, cioè vale la proprietà $*$. (solo in quest'ultimo passaggio si sfrutta il fatto che n è senza quadrati)

1.3 Test di primalità

Esistono dei test probabilistici per testare se n è primo.

Definizione (394 Pseudo-primo)

n si dice uno *pseudo-primo* rispetto alla base b se $b^{n-1} \equiv 1 \mod n$, dove $0 < b < n$, e se $M.C.D.(b, n) = 1$.

Passi del test di primalità:

1. Scegli b con $0 < b < n$ e calcola $d = M.C.D.(b, n)$.
2. Se d è diverso da 1, n non è primo (costo di $\log n$ operazioni).
3. Se $d = 1$, calcolo $b^{n-1} \mod n$.
4. Se $[b^{n-1}]_n \neq [1]_n$, restituisce " n non primo".
5. Se $[b^{n-1}]_n = [1]_n$, restituisci " n è pseudoprimo rispetto alla base b ".

Questo test funziona perché, se n fosse primo, si avrebbe $\phi(n) = n - 1$. Per Eulero-Fermat, con b, n coprimi, si avrebbe $b^{\phi(n)} \equiv 1 \mod n$, quindi $b^{n-1} \equiv 1 \mod n$. Quindi se questo non avviene il numero non è primo. Tuttavia se si ha $b^{n-1} \equiv 1 \mod n$, non è detto che il numero sia primo.

Ci sono numeri che risultano pseudoprimi per qualsiasi base b anche se non sono numeri primi.

Definizione (395 Primo di Carmichael)

Un numero n si dice *primo di Carmichael* se n è pseudoprimo rispetto a ogni b con $0 < b < n$.

1.3.1 Lemma sugli pseudoprimi

Lemma (396)

Sia n un numero naturale, allora

1. se n è pseudoprimo rispetto alle basi b_1, b_2 , allora è pseudoprimo rispetto alla base $b_2 b_1^{-1}$
2. se esiste una base b per cui n non è uno pseudoprimo, allora ce ne sono almeno $\phi(n)/2$ con tale proprietà.

Dimostrazione

Dimostro il punto 2 del lemma: Siano $b_1, \ldots, b_t$ tutte le basi per cui n è pseudoprimo, e sia c una base per cui n non è pseudoprimo. Allora

$$b_i^{n-1} \equiv 1 \mod n.$$

Considero i numeri $cb_1, cb_2, \ldots, cb_t$, allora n non è pseudoprimo per nessuno di queste basi, che sono almeno t .

Questo mostra che il numero di basi per cui n non è pseudoprimo è almeno quanto il numero di basi per cui n è pseudoprimo. Sia s il numero di basi per cui n non è pseudoprimo. Allora $s \geq t$, inoltre $s+t = \phi(n)$, perché $s+t$ è il numero totale di elementi coprimi con n . Unendo le due equazioni $s + t = \phi(n)$ e $s + t \leq 2s$, si ha $\phi(n) \leq 2s$, cioè $s \geq \phi(n)/2$.

Lemma (397)

1. Se n è primo di Carmichael, allora n è senza quadrati (come i numeri utilizzati nel protocollo RSA).
2. n è primo di Carmichael se e solo se $p-1 \mid n-1$ per ogni divisore primo di n ;
3. se n è primo di Carmichael, allora n è divisibile per almeno tre primi.

Esempio (398 applicazione del lemma)

$561 = 3 * 11 * 17$. $n-1 = 560$. I divisori primi di n sono $p_1 = 3, p_2 = 11, p_3 = 17$, e si ha che $2, 16, 10$ dividono 560 , cioè per ogni divisore $p-1 \mid n$, e quindi 561 è il più piccolo primo di Carmichael. Senza conoscere la fattorizzazione di 561 , basta estrarne la radice cubica e verificare se ha divisori.

1.4 Gioco

1.4.1 Domande

Penso ad un numero x tra 0 e 15. Facendomi le 7 domande che seguono, a cui posso rispondere sì o no, una persona è in grado non solo di indovinare il numero che ho pensato, ma anche di capire se a una delle sette domande ho detto una bugia. Le possibili risposte totali sono 2^7 . In base alle regole del gioco ho otto possibilità (o non dico bugie, oppure ne dico una ad una sola delle sette domande).

Le domande sono le seguenti:

1. $x > 8$?
2. x è uno tra i seguenti numeri: $4, 5, 6, 7, 12, 13, 14, 15$?
3. x è uno tra i seguenti numeri: $2, 3, 6, 7, 10, 11, 14, 15$?

4. x è dispari?
5. x è uno tra i seguenti numeri: $1, 2, 4, 7, 9, 10, 12, 15$?
6. x è uno tra i seguenti numeri: $1, 2, 5, 6, 8, 11, 12, 15$?
7. x è uno tra i seguenti numeri: $1, 3, 4, 6, 8, 10, 13, 15$?

Indico le risposte affermative con 1 e quelle negative con 0: se non ho detto bugie nelle prime 4 domande, si può risalire al numero che ho pensato perché la sua rappresentazione in base due si ottiene leggendo in ordine le cifre associate alle risposte alle prime quattro domande.

Prova: le risposte date dal concorrente alle domande sono n, s, n, s, s, n, n . Se il giocatore non ha detto bugie, il numero che ha pensato ha come rappresentazione binaria 0101 , e quindi è 5. Verifico se questo è consistente con le risposte date alle domande successive, e questo non avviene perché se il numero fosse 5, la risposta alla domanda 6 dovrebbe essere sì.

Si può scoprire che il giocatore ha detto una bugia alla terza domanda, e quindi, correggendo la risposta a questa domanda, la rappresentazione binaria associata al numero è 0111 e il numero pensato è 7.

1.4.2 Trucco

Considero la matrice seguente:

$$H = \begin{matrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{matrix}$$

(le righe sono i numeri da 1 a 7 in rappresentazione binaria)

Supponiamo di avere la seguente stringa di risposte: $B = (1, 0, 1, 0, 0, 1, 0)$

1. se non si sono dette bugie, il numero pensato è quello che in base 2 si scrive come 1010 , dove $1, 0, 1, 0$

sono i valori ottenuti nelle prime quattro domande

1. Osservo che $B \times H$ è un vettore con coefficienti in $\mathbb{Z}_2$ e tre componenti.

In questo caso

$$B \times H = (1, 0, 0)$$

Se il vettore ottenuto è nullo, non ho detto bugie. Altrimenti si cerca in quale riga della matrice compare il vettore, quindi la bugia è stata detta alla quarta riga.

1. In questo modo correggo l'errore e posso così risalire al numero guardandone la sua rappresentazione binaria.

Scelto il numero x , denotiamo con c_x il vettore che si ottiene rispondendo alle 7 domande senza dire nessuna bugia: questo vettore è tale che $c_x \times H = 0$. Infatti H è stata costruita in modo tale che moltiplicando uno dei vettori c_x per $x = 0, 1, \ldots, 15$ per H ottengo 0.

H ha rango 3, quindi l'insieme dei vettori v tali che $v \times H = 0$ è un sottospazio di $(\mathbb{Z}_2)^7$ di dimensione $7 - 3 = 4$, e ha cardinalità $2^4 = 16$ (corrispondenti appunto ai numeri da 0 a 15).

Se un giocatore dice una bugia all'i-esima domanda, il vettore che viene dato al posto di c_x è $c_x + e_i$ con e_i vettore della base canonica.

$$(c_x + e_i) \times H = c_i H + e_i H = e_i H$$

perché $c_x H = 0$. $e_i H$ è l'i-esima riga di H , e corrisponde quindi alla domanda in cui è stata detta la bugia.

Sia $C = \{c_0, c_1, \ldots, c_{15}\}$. Nota che:

1. la somma di elementi di C sta ancora in C , perché C è spazio delle soluzioni dell'equazione $v \times H = 0$.
2. Due elementi diversi di C hanno coordinate che differiscono in almeno tre posizioni.

Dimostrazione

Se suppongo che quest'affermazione sia falsa, e cioè che c_m, c_n differiscano in solo due coordinate, la i-esima e la j-esima, si avrebbe che $c_m + e_i = c_n + e_j$, ma questo non può avvenire (intuitivamente $c_m + e_i$ corrisponde alle risposte date da un giocatore che dice una bugia all'i-esima domanda).

1.5 Spazio di Hamming

1.5.1 Distanza sullo spazio di Hamming

Definizione (399 Spazio di Hamming)

Sia Q un insieme finito con q elementi, e sia n un numero naturale. Lo *spazio di Hamming*, $H(n, q)$ è l'insieme delle n-uple $(x_1, x_2, \ldots, x_n)$ con $x_i \in Q$.

Definisco una distanza $d \in H(n, q)$:

Definizione (400 Distanza di Hamming)

Dati $v = (v_1, \ldots, v_n)$ e $w = (w_1, \ldots, w_n)$, definisco la distanza

$$d(v, w) = |\{i \, t.c. \, v_i \neq w_i\}|.$$

d si chiama *distanza di Hamming*.

Proposizione (401)

d è una distanza.

Dimostrazione

1. $d(v,w) = 0$ se e solo se $v = w$;
2. $d(v,w) = d(w,v)$
3. $d(v,w) \leq d(v,z) + d(z,w)$

Infatti sia $a = d(v,z)$ e $b = d(z,w)$: questo significa che se cambio a coordinate di v trovo z , e se cambio b coordinate di z trovo w , quindi se cambio al più $a+b$ coordinate trovo w a partire da v .

1.5.2 Codici

Definizione (402 Codice e parole di un codice)

Un codice C di lunghezza n e sull'alfabeto Q è un sottoinsieme di $H(n,q)$ con almeno due elementi. Gli elementi di C si chiamano *parole* del codice.

Supponiamo che C abbia k elementi, cioè che $C = \{c_1, c_2, c_3, \ldots, c_k\}$. Sia M l'insieme dei messaggi che vogliamo spedire. Sia $f : M \to C$ biettiva (nell'esempio precedente, i messaggi sono i numeri tra 0 e 15, e f la funzione che a ogni numero associa le risposte alle sette domande che rappresentano i codici).

Decifratura: se si riceve un vettore $v \in H(n,q)$, lo si decodifica prendendo un elemento $c' \in C$ tale che $d(v,c')$ sia minima. Dato c' , risalgo al messaggio calcolando $f^{-1}(c')$. Se $v \in C$, si prende $c' = v$. (nell'esempio precedente, si correggeva la bugia per trovare c')

1.5.3 Correttore di errori

Definizione (403 Correttore di errori)

Dato un intero e , diremo che C è *correttore di e errori* se per ogni $w \in H(n,q)$ esiste al più un $c \in C$ tale che $d(w,c) \leq e$.

Definizione (404 Distanza del codice)

La *distanza del codice* C è denotata con d ed è per definizione $\min_{c,c' \in C,\, c \neq c'}\{d(c,c')\}$ (è la distanza tra due parole arbitrarie, nell'esempio precedente era 3).

Proposizione (405)

C di distanza minima d è correttore di e errori se e solo se $d \geq 2e+1$. (il codice nell'esempio precedente è correttore di 1 errore, perché $d = 3$ implica $e = 1$)

Dimostrazione

Supponiamo che $d \geq 2e+1$; sia $w \in H(n,q)$ e supponiamo per assurdo che esistano due vettori $c_1, c_2 \in C$ tali che $d(w,c_1) = d(w,c_2) \leq e$. Allora per definizione di distanza sul codice C e per l'ipotesi:

$$d = \min_{c,c' \in C} \{d(c,c')\} \leq d(c_1,c_2) \leq d(c_1,w) + d(w,c_2) \leq 2e$$

e questo è assurdo, quindi $c_1 = c_2$ e C è correttore di e errori.

Viceversa, supponiamo per assurdo che $d \leq 2e$, e supponiamo che $f = \lfloor d/2 \rfloor$, siano c_1, c_2 parole del codice a distanza d . Posso portare c_1 in c_2 alterando d coordinate: chiamo w la parola che ottengo alterando f coordinate di c_1 per portarlo in c_2 , allora $d(w,c_1) = f$ e $d(w,c_2) = d - f$. $f, d-f$ sono $\leq e$ ($*$), ma w dista al più e sia da c_1 che da c_2 , ma allora il codice non può correggere e errori.

$*$: se d è pari, la disuguaglianza $d - f \leq e$ è ovvia perché $f = d - f = d/2$. Invece se d è dispari, $d/2 \leq e$ implica $\lfloor d/2 \rfloor + 1 \leq e$ perché e è intero, quindi $d - f = d - \lfloor d/2 \rfloor < \lfloor d/2 \rfloor + 1 < e$)

In genere si cercano codici con $d \geq 2e+1$, ma questi due valori sono in conflitto; infatti se prendo d grande il codice potrà avere meno parole.

Denoto con

$$B_e(c) = \{w \in Q^n \, t.c. \, d(w,c) \leq e\}.$$

allora vale il seguente corollario:

Corollario (406)

C è correttore di e errori se e solo se le palle $B_{e,c}$ centrate negli elementi del codice di raggio e sono a due a due disgiunte.

1.5.4 Considerazioni probabilistiche

Per semplicità assumeremo che l'alfabeto sia $Q = \{0,1\} = \mathbb{Z}_2$. Facciamo le seguenti tre ipotesi sul canale di trasmissione:

1. la probabilità p che 0 venga cambiato in 1 è la stessa che 1 sia cambiato in 0.
2. p non dipende dalla coordinata, e inoltre $p < 1/2$

In realtà l'ipotesi che tutte le coordinate possono essere cambiate con la stessa probabilità non è realistica, perché nella pratica, quando si trasmette un segnale, è più probabile che ci siano rumori che portano a errori nella trasmissione all'inizio piuttosto che alla fine del processo. Per quanto riguarda l'altra ipotesi, se $p = 1/2$, non si spedisce nessuna informazione perché quello che sta succedendo è aleatorio.

1. la probabilità di errore è indipendente dalle coppie di coordinate.

Anche quest'ipotesi non è realistica perché nella realtà, se una coordinata è sbagliata, è più probabile che anche le seguenti siano sbagliate.

Definizione (407 Decodificazione con il metodo maximum likelyhood)

Data w , la decodificazione con il metodo maximum likelyhood è quella con c per cui la probabilità che " c trasmessa e w ricevuta" siano massime.

Proposizione (408)

In un canale che soddisfa le precedenti richieste, il metodo di decodifica maximum likelihood coincide con il metodo di decodifica dato dalla minima distanza.

Dimostrazione

Calcolo la probabilità condizionale dell'evento " c sia trasmessa dato che w sia ricevuta". Sia $d = d(w, c)$, allora la probabilità che w sia ricevuta dato che c sia trasmessa è data dalla formula $p^d * (1-p)^{n-d}$ (infatti esattamente d cordinate di c sono state cambiate per trovare w , e siccome la probabilità che una coordinata venga cambiata è p , la probabilità che ne vengano cambiate d è p^d , mentre il fattore $(1-p)^{n-d}$ rappresenta il fatto che $n-d$ coordinate non vengono cambiate). Inoltre la probabilità che c sia trasmessa è data da $1/|C|$, quindi per la formula di Bayes:

$$P(c\text{trasmessa}|\text{wricevuta}) = \frac{\text{P}(\text{wricevuta}|\text{ctrasmessa})}{\text{P}(\text{wricevuta})} * \text{P}(\text{ctrasmessa})$$
$$= \frac{p^d * (1-p)^{n-d} * 1/|C|}{P(w\text{ricevuta})}$$

La funzione che a d associa $p^d*(1-p)^{n-d}$ è decrescente in d , quindi $P(c\text{trasmessa}|\text{wricevuta})$ è massima quando d è minima.

1.5.5 Rate di un codice

Definizione (409 Rate)

Il *rate* di un codice C è $\frac{\log_q |C|}{n}$.

Esempio (410)

Supponiamo che $|C| = |Q|^k$, allora il rate è dato da $\frac{\log_{|Q|}(|Q|^k)}{n} = k/n$. Se $k/n \to 1$, allora il numero di parole che posso spedire è vicino al numero massimo di n-uple a disposizione, invece se $k/n \to 0$, il codice è rarefatto all'interno delle possibili n-uple.

Teorema (411 teorema di Shannon)

Dato un canale con le tre proprietà di prima, e tale che la probabilità che "0 trasmesso e 1 ricevuto" sia p , allora

a) sia r tale che $r < 1 + p * \log_2 p + (1-p) * \log_2(1-p)$ e $\varepsilon > 0$, allora esiste un codice C con rate r e per cui la probabilità

che venga commesso un errore usando il metodo di decodifica è minore di ε .

b) se $r > 1 + p \log_2 p + (1-p) \log_2(1-p)$ allora la probabilità di errore di una parola generica in

codice con rate r è limitata inferiormente da una costante maggiore di 0.

Definizione (412 Capacità del canale)

La quantità $1 + p * \log_2 p + (1-p) * \log_2(1-p)$ è detta *capacità del canale*.

Intuitivamente, se r è minore della capacità del canale, si può sempre trovare un codice che minimizza l'errore di trasmissione, altrimenti questo non è possibile.

La dimostrazione è di esistenza ma non costruttiva: non si ha idea di come realizzare il codice.

1.6 Codici lineari

1.6.1 Definizione di codice lineare

Supponiamo che l'alfabeto Q sia un campo, con q elementi. Nota che lo spazio di Hamming $H(n, Q)$ è uno spazio vettoriale di dimensione n su Q .

Definizione (413 Codice lineare)

Un codice C si dice *lineare* se C è un sottospazio vettoriale di $H(n, Q)$.

Osservazione (414)

Osservo che C ha come cardinalità una potenza di q , della forma q^k . Sia $\{c_1, c_2, \ldots, c_k\}$ una base di C . Ora un elemento generico di C si scrive come $\alpha_1 c_1 + \cdots + \alpha_k c_k$ per una scelta univoca di $\alpha_1, \ldots, \alpha_k$ nel campo Q . Per la scelta di ognuno dei coefficienti α_k ho q possibilità, quindi in totale ho q^k elementi.

1.6.2 Peso di un codice

Definizione (415 Peso di una parola)

Il *peso* di una parola w è per definizione $\mathrm{wt(w)} = \mathrm{d(w, 0)}$, ossia il numero di coordinate diverse da 0 (wt sta per "weight").

Definizione (416 Peso di un codice lineare)

Il *peso di un codice lineare* C è il minimo dei pesi delle parole non nulle del codice C , cioè

$$\mathrm{wt(C)} = \min_{\mathrm{c\in C, c\neq 0}} \{\mathrm{wt(c)}\}.$$

Da un punto di vista computazionale per calcolare il peso di un codice bisogna fare $|C| - 1$ controlli (uno per ogni parola del codice, escluso lo zero). Calcolare la distanza minima tra due elementi invece costa $|C|^2$ operazioni, ma con la proposizione seguente si ha che nel caso di codici lineari anche per calcolare la distanza minima bastano $|C| - 1$ operazioni, perché, in base alla proposizione che segue, il peso minimo coincide con la distanza minima.

Proposizione (417)

Detta d la distanza minima di uno spazio di Hamming, si ha:

1. $$d(v, w) = \mathrm{wt(v - w)},\ \forall \mathrm{v, w} \in \mathrm{H(n, q)}$$
2. Nel caso di un codice lineare d e wt(C) coincidono.

Dimostrazione

1. Per il punto 1, basta osservare che $d(v, w)$ è il numero di coordinate per cui v differisce da w , ma allora è uguale al numero di coordinate per cui $v - w$ differisce da 0, quindi è wt(v − w) .
2. Devo dimostrare le due disuguaglianze:

disuguaglianza 1: $d(C) \leq \mathrm{wt(C)}$. Infatti, il minimo che compare nella definizione di $d(C)$ viene fatto su tutte le coppie (c_1, c_2) con $c_1 \neq c_2$, mentre il minimo di wt(C) viene fatto solo sulle coppie $(0, c)$ con $c \neq 0$.

Disuguaglianza 2: $d(C) \geq \mathrm{wt(C)}$

$$d(C) = \min_{(c_1,c_2)\in C,\, c_1\neq c_2} d(c_1, c_2)$$

e per il punto 1:

$$= \min_{c_1,c_2\in C,\, c_1\neq c_2} \mathrm{wt(c_1 - c_2)}$$

ma C è lineare, allora $c_1, c_2 \in C \longrightarrow c_1 - c_2 \in C$, e $c_1 - c_2 \neq 0$. Allora

$$= \min_{c\neq 0, c\in C} \mathrm{wt(c)} = \mathrm{wt(C)}.$$

Quindi i codici lineari si usano perché con questi è più comodo calcolare la minima distanza.

1.6.3 Matrice generatrice

Definizione (418 Matrice generatrice)

Una *matrice generatrice* G di un codice lineare C è una matrice che ha per righe una base di C .

Osservazione (419)

Nota che data una matrice G , il codice lineare C è univocamente dato, perché i suoi elementi sono combinazioni lineari di elementi di G (e questo è il secondo vantaggio, oltre alla riduzione dei costi computazionali, di usare codici lineari).

Definizione (420 Matrice di parità)

Dato un codice lineare C , di dimensione k , una base di C ha k elementi e una matrice generatrice è della forma $k \times n$. La *matrice di parità* per C si denota con H , è una matrice $n-k \times n$ per cui

$$C := \{v \in H(n,Q)\, t.c.\, v \times H^t = 0\} = \ker H.$$

Esempio (421)

Se $n = 15$, e C ha dimensione $k = 10$, servono cinque equazioni lineari per descrivere C .

Esempio (422)

Sull'alfabeto $\mathbb{Z}_2$, considero la matrice H , data da un'unica riga con entrate uguali a 1. Allora

$$\begin{aligned} C &= \{v\, t.c.\, vH^t = 0\} \\ &= \{v\, t.c.\, \sum_{i=1}^{n} v_i = 0\} \\ &= \{v\, t.c.\, \text{v ha un numero pari di coordinate uguali a 1}\} \end{aligned}$$

(da qui viene il nome "matrice di parità")

Proposizione (423)

Siano G, H matrici con righe linearmente indipendenti, tali che G è una matrice $k \times n$ e H è una matrice $n-k \times n$, allora G, H sono rispettivamente la matrice generatrice e la matrice di parità di un codice C se e solo se $GH^t = 0$.

Dimostrazione

Questo è vero perché $GH^t = 0$ implica che le righe $g_1, \ldots, g_k$ di G stanno in $\ker H$, e quindi siccome $\ker H$ e $\text{span}(\text{g}_1, \ldots, \text{g}_\text{k})$ sono entrambi sottospazi vettoriali di dimensione k , allora essi coincidono.

1.6.4 Costruzione di H a partire da G e viceversa

Sia A una matrice $k \times n-k$, e sia $G = (I_k\, A)$ (G ha la matrice identica $k \times k$ nel blocco a sinistra e la matrice A nel blocco accanto). Allora la matrice di parità H è data da:

$$H = (-A^t\, I_{n-k})$$

Infatti in particolare osservo che

$$GH^t = -A + A = 0$$

questo significa che le righe di H sono linearmente indipendenti. Vale il viceversa: se C ha matrice di parità $H = (-A^t\, I_{n-k})$, allora $G = (I_k\, A)$.

Data una matrice che non è della forma descritta sopra, la si può portare in tale forma con l'eliminazione di Gauss.

1.6.5 Determinazione della distanza minima di un codice

Proposizione (424)

Un codice lineare C ha distanza minima $\geq d$ se e solo se comunque prese $d-1$ colonne di H , esse sono linearmente indipendenti.

Dimostrazione

Supponiamo che C ha distanza minima $\geq d$, e sia l il numero minimo di colonne di H linearmente dipendenti. Dobbiamo dimostrare che $l \geq d$. Supponiamo che le colonne linearmente dipendenti di H siano le prime l . Allora, se chiamo queste colonne $v_1, \ldots, v_l$, si ha che

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_l v_l = 0$$

dove $\alpha_1, \ldots, \alpha_l$ sono coefficienti scalari non nulli.

Prendo il vettore $c = (\alpha_1, \alpha_2, \ldots, \alpha_l, 0, 0, \ldots)$ di lunghezza n . Allora

$$cH^t = \alpha_1 v_1 + \cdots + \alpha_l v_l + 0 = 0.$$

e quindi c è una parola del codice C , perché risolve l'equazione $vH^t = 0$, e ha peso l (infatti l coordinate sono non nulle). Allora

$$l = \mathrm{wt(c)} \geq \mathrm{wt(C)} = \mathrm{d(C)}.$$

Ho quindi dimostrato che $l \geq \mathrm{wt(C)}$. Se prendo $d-1$ colonne di H queste sono linearmente indipendenti.

Esempio (425)

Sull'alfabeto $Q = \{0, 1\}$, se consideriamo un codice con dimensione $k = 4$ e parole di $n = 7$ lettere, si ha che il codice ha 2^4 elementi. Calcolare il peso minimo richiederebbe molte operazioni, e quindi si può usare la proposizione sulla distanza minima appena dimostrata, e verificare se $d - 1$ colonne della matrice generatrice sono indipendenti.

1.6.6 Codifica di un messaggio per codici lineari

Per la codifica serve la matrice generatrice. L'insieme dei messaggi sono k-uple di vettori a coefficienti nell'alfabeto Q . Data una tale k-upla v , associamo ad essa l'elemento $v * G$, che è una parola del codice perché è combinazione lineare delle righe di G .

La funzione che manda v in vG è una funzione da C in sé ed è iniettiva perché le righe di G sono linearmente indipendenti, e quindi è anche suriettiva perché sto lavorando su insiemi finiti.

Riassumendo, la k-upla v viene codificata in $v * G$. (come nel giochino, in cui i messaggi, cioè i numeri da 0 a 15 in rappresentazione binaria, venivano codificati nel vettore di 7 elementi corrispondente alle risposte alle 7 domande, attraverso il prodotto vG).

1.6.7 Decodifica e correzione degli errori

Per la decodifica serve la matrice di parità H . Per fissare le idee, supponiamo che C ha distanza minima d e che sia correttore di e errori, con $d \geq 2e + 1$.

Diciamo che sia stata spedita c e che sia stata ricevuta w , e che siano stati commessi al massimo e errori. Allora da w vogliamo ricostruire c . Si ha $w = c+u$, con u errore. Quindi

$$wH^t = (c + u)H^t = cH^t + uH^t = uH^t$$

infatti $c \in C$ e quindi $cH^t = 0$. Allora $wH^t = uH^t$

Definizione (426 Sindrome)

wH^t è detta sindrome.

Mostriamo ora che errori diversi hanno sindromi diverse. Questo permetterà di correggere l'errore u utilizzando una tavola precompilata con due colonne: la prima costituita da tutte le sindromi, e la seconda costituita dagli errori.

Proposizione (427)

Siano u_1, u_2 errori distinti, allora $u_1H^t \neq u_2H^t$ (anche le sindromi sono distinte)

Dimostrazione

Siano u_1, u_2 errori distinti ma con la stessa sindrome, cioè tali che $u_1H^t = u_2H^t$, allora $(u_1 - u_2)H^t = 0$. Questo implica che $u_1 - u_2$ è una parola del codice,

non nulla perché per ipotesi $u_1 \neq u_2$. Quindi $\mathrm{wt}(\mathrm{u}_1 - \mathrm{u}_2) \geq \mathrm{d}$ perché d è il peso minimo. Per la disuguaglianza triangolare

$$2e + 1 \leq \mathrm{wt}(\mathrm{u}_1 - \mathrm{u}_2) \leq \mathrm{wt}(\mathrm{u}_1) + \mathrm{wt}(\mathrm{u}_2).$$

u_1, u_2 hanno peso minore di e perché nel nostro canale avvengono al massimo e errori, e si ottiene $2e \geq 2e + 1$ e questo è assurdo.

Esempio (428)

Riprendendo l'esempio del giochino, sia $n = 7$, $k = 4$, $Q = \{0, 1\}$.

$$H = \begin{matrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{matrix}$$

$d = 3$ perché prese due colonne, una non può essere multiplo dell'altra però le prime tre colonne sono linearmente dipendenti e quindi la distanza minima non può essere 4. Il codice è correttore di 1 errore. Gli errori sono tutti i vettori con peso 1, e quindi sono $e_1, e_2, \ldots, e_7$ vettori della base canonica.

In questo caso la tavola delle sindromi è semplice, perché all'errore e_i basta associare l'i-esima colonna di H .

Supponiamo che

$$w = (1, 1, 1, 1, 0, 0, 0)$$

allora

$$w * H^t = (1, 0, 0)$$

La sindrome $(1, 0, 0)$ è alla quarta colonna di H , quindi l'errore associato è e_4 , e devo correggere la quarta coordinata di w , quindi la parola trasmessa è $C = (1, 1, 1, 0, 0, 0, 0)$.

Matrice generatrice: per calcolarla voglio portare H nella forma $(-A^t, I_3)$, e per farlo scambio la prima e la settima riga, la seconda e la sesta riga, la quarta e la quinta riga

$$H' = \begin{matrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{matrix}$$

Allora ottengo:

$$G' = (I_4, A)$$

$$= \begin{matrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{matrix}$$

e rifacendo gli scambi appena effettuati:

$$= \begin{matrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{matrix}$$

1.6.8 Codici di Hamming

I codici di Hamming sono i codici correttori di un errore più utilizzati.

- Fisso q , numero di elementi dell'alfabeto, e l , intero positivo.

Sull'insieme di tutti i vettori non nulli di lunghezza l , definisco una relazione di equivalenza: $v \sim w$ se v e w sono multipli l'uno dell'altro.

- Sia H una matrice che ha per colonne rappresentanti di ciascuna classe di equivalenza.

H ha l righe perché le colonne sono vettori di lunghezza l . Le colonne sono tante quante le classi di equivalenza. Il numero totale di vettori non nulli è $q^l - 1$, allora il numero di classi di equivalenza è

$$\frac{q^l - 1}{q - 1}$$

($q - 1$ è il numero di elementi in una classe di equivalenza, perché gli scalari per cui posso moltiplicare un vettore per ottenere i suoi multipli è proprio $q - 1$).

- Il codice di Hamming con parametri q, l è un codice lineare con matrice di parità H .

Per essere correttore di 1 errore, la distanza minima dev'essere 3, quindi due colonne di H non nulle non devono essere l'una multiplo dell'altra.

Nota che C ha distanza minima $d \geq 3$ per costruzione, perché le colonne non sono l'una multiplo dell'altra.

Esempio (429)

Sia $q = 3$, $Q = \{0, 1, 2\}$ e $l = 3$. Allora H ha tre righe e $\frac{3^3-1}{3-1} = 13$ colonne. Le colonne sono vettori di lunghezza 3 non nulli, e colonne diverse devono essere una multiplo dell'altra, ad esempio, se $(0, 0, 1)$ è una colonna, $(0, 0, 2)$ non lo sarà.

Le colonne di H sono:

$(0,0,1)$, $(0,1,0)$, $(0,1,1)$, $(0,1,2)$, $(1,0,0)$, $(1,0,1)$, $(1,0,2)$, $(1,1,0)$, $(1,1,1)$, $(1,1,2)$, $(1,2,0)$, $(1,2,1$

Capitolo 2

Fonti per testo e immagini; autori; licenze

2.1 Testo

- **Corso:Algebra Crittografia (Unimib)/Crittografia/Teoremi ausiliari sugli interi** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Crittografia_(Unimib)/Crittografia/Teoremi_ausiliari_sugli_interi?oldid=48110 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Crittografia (Unimib)/Crittografia/Metodo RSI** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Crittografia_(Unimib)/Crittografia/Metodo_RSI?oldid=48225 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Crittografia (Unimib)/Crittografia/Test di primalità** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Crittografia_(Unimib)/Crittografia/Test_di_primalit%C3%A0?oldid=48127 *Contributori:* Riccardo Iaconelli, Toma.luca95 e Mmontrasio
- **Corso:Algebra Crittografia (Unimib)/Crittografia/Gioco** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Crittografia_(Unimib)/Crittografia/Gioco?oldid=38023 *Contributori:* Mmontrasio
- **Corso:Algebra Crittografia (Unimib)/Crittografia/Spazio di Hamming** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Crittografia_(Unimib)/Crittografia/Spazio_di_Hamming?oldid=48148 *Contributori:* Toma.luca95 e Mmontrasio
- **Corso:Algebra Crittografia (Unimib)/Crittografia/Codici lineari** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_Crittografia_(Unimib)/Crittografia/Codici_lineari?oldid=48141 *Contributori:* Toma.luca95 e Mmontrasio

2.2 Immagini

2.3 Licenza dell'opera