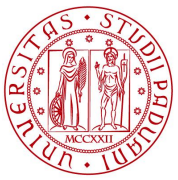

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Triennale in Matematica

Inapprossimabilità dello Shortest Vector Problem

per mezzo di Codici Reed-Solomon

Relatore:
Prof. Marco Di Summa

Laureando: Giacomo Fiorindo
Matricola: 2017594

Anno Accademico 2022/2023

22 Settembre 2023

Indice

Introduzione

Fin dall'antichità l'uomo si è posto il problema di comunicare informazioni in modo sicuro, soprattutto in ambito politico e militare. Nel corso della storia sono stati sviluppati sistemi di criptazione sempre più complessi per assicurarsi che questo avvenisse. Tra gli esempi più celebri abbiamo il cifrario di Cesare, che deve il nome a Giulio Cesare ed è uno dei più antichi algoritmi crittografici di cui siamo a conoscenza, ed Enigma, il sistema di criptazione tedesco la cui decifrazione ha stravolto gli sviluppi della seconda guerra mondiale.

Con l'avvento delle telecomunicazioni e in particolare di Internet la protezione di dati sensibili, come quelli bancari o medici, è diventata di interesse globale e di conseguenza la criptazione è diventata una materia di ricerca di grande importanza. Tra le diverse branche che si sono sviluppate negli anni, la crittografia basata sui reticoli, ovvero quella che sviluppa sistemi di criptazione la cui sicurezza deriva da proprietà e problemi computazionali intrinsechi ai reticoli, è una delle aree di ricerca di più successo.

Il problema computazionale centrale è il *Shortest Vector Problem* (SVP) ovvero quello di calcolare il vettore non nullo più corto in un reticolo dato. Il primo sistema di criptazione basato su questo problema fu presentato da M. Ajtai [1] nel 1996, seguito da un altro descritto lo stesso anno [3] in collaborazione con C. Dwork basato su una variante del problema nota come *unique* SVP. In pochi anni vi fu un proliferare di schemi di criptazione legati ad ulteriori varianti di SVP o problemi riconducibili ad esso come il sistema di criptazione asimmetrica NUTRU [9] e quello proposto da O. Regev nel 2005 [16] con il *Learning With Errors Problem*, al centro di molti sistemi moderni tra cui quelli di *criptazione omomorfica* iniziata dal lavoro innovativo di C. Gentry [8] o di *criptazione quantistica*.

Questi studi hanno in comune l'assunzione che SVP o una delle sue varianti siano computazionalmente difficili (si veda Appendice A). In questo lavoro ci concentriamo sulla variante decisionale e γ-approssimata rispetto alla norma ℓ_p del problema nota come γ-GapSVP$_p$ con $p \geq 1$ fisso e $\gamma = \gamma(n) \geq 1$ una funzione sul reticolo di rango n. Indichiamo con GapSVP$_p$ la versione esatta, ovvero con $\gamma = 1$.

Nel 1981 E. Boas riuscì a dimostrare che GapSVP$_\infty$ è *NP*-difficile [15]. Nel 1998 M. Ajtai [2] dimostro l'importante caso per $p = 2$ utilizzando riduzioni randomizzate. Negli anni successivi numerosi lavori [6, 13, 14, 12, 11] hanno provato che γ-GapSVP$_p$ è *NP*-difficile attraverso riduzioni randomizzate sotto condizioni su γ differenti.

Più recentemente H. Bennet e C. Peikert hanno mostrato [5] che γ-GapSVP$_p$ è *NP*-difficile per ogni $p \geq 1$ e $\gamma < 2^{\frac{1}{p}}$ attraverso riduzioni randomizzate a partire da reticoli ottenuti da *codici di Reed-Solomon*, una particolare tipologia di codici di correzione del-

l'errore. Più precisamente hanno dimostrato che γ-GapSVP$_p$ non è in RP a meno che $NP \subseteq RP$.

In questo lavoro presentiamo i loro traguardi. In particolare nel primo capitolo descriviamo formalmente i reticoli e dimostriamo che l'esistenza di algoritmi che producono *reticoli localmente densi* in tempo polinomiale ha implicazioni sulla complessità di γ-GapSVP$_p$. Nel secondo capitolo introduciamo i codici di correzione dell'errore lineari con le loro proprietà principali e loro sotto-categorie tra cui troviamo i codici Reed-Solomon. Infine, nel terzo capitolo dimostriamo che possiamo ottenere reticoli localmente densi per mezzo di codici Reed-Solomon in tempo polinomiale randomizzato e di conseguenza l'asserto iniziale del lavoro di Bennet e Peiker.

Capitolo 1

Reticoli Localmente Densi

Ricordiamo che un oggetto indicizzato da un insieme finito S di cardinalità n può sempre essere re-indicizzato da $\{0, ..., n-1\}$ enumerando $S = \{s_0, ..., s_{n-1}\}$ ed identificando s_i con i. In questo caso possiamo sostituire S ad esponente con n, ad esempio scriveremo $\mathbb{R}^n$ al posto di $\mathbb{R}^S$. Indicheremo con $[n]$ l'insieme $\{0, ..., n-1\}$.

Dato un insieme finito S ed un intero positivo $h \leq |S|$ denotiamo con $B_{S,h} = \left\{ \mathbf{v} \in \{0,1\}^S \;\middle|\; \|\mathbf{v}\|_1 = h \right\}$. Per l'osservazione sopra possiamo scrivere anche $B_{n,h}$. Inoltre, utilizziamo il simbolo $B_p^n(r) = \{\mathbf{x} \mid \|\mathbf{x}\|_p \leq r\} \subset \mathbb{R}^n$ per denotare la palla n-dimensionale di raggio r centrata nell'origine rispetto alla norma ℓ_p.

1.1 Reticoli

Definizione 1.1 (Reticolo)**.** Siano $\mathbf{b_1}, ..., \mathbf{b_n} \in \mathbb{R}^m$ vettori linearmente indipendenti. Detta $B = (\mathbf{b_1}, ..., \mathbf{b_n}) \in \mathbb{R}^{m \times n}$, il reticolo $\mathcal{L}$ generato da B è il dato

$$\mathcal{L} = \mathcal{L}(B) = \left\{ \sum_{i=1}^{n} \alpha_i \mathbf{b_i} \;\middle|\; \alpha_1, ..., \alpha_n \in \mathbb{Z} \right\}$$

I vettori $\mathbf{b_1}, .., \mathbf{b_n}$ sono detti *base* di $\mathcal{L}$, n è detto *rango* del reticolo ed m è la *dimensione* del reticolo. Se $m = n$ il reticolo è di *rango massimo*. Un reticolo si dice *intero* se $\mathbf{b_1}, ..., \mathbf{b_n} \in \mathbb{Z}^m$.

La base di un reticolo non è unica. Infatti sostituire a $\mathbf{b_j}$ il vettore $z\mathbf{b_i} + \mathbf{b_j}$ con $i \neq j$ e $z \in \mathbb{Z}$ genera lo stesso reticolo.

Definizione 1.2 (matrice unimodulare)**.** Una matrice quadrata U si dice *unimodulare* se $U \in \mathbb{Z}^{n \times n}$ per un opportuno $n \in \mathbb{N}$ e $\det(U) = \pm 1$.

Presentiamo qualche proprietà delle matrici unimodulari.

Lemma 1.1. *Sia U una matrice unimodulare. Allora U^{-1} è unimodulare.*

Dimostrazione. Poiché $\det(U^{-1}) = \frac{1}{\det(U)} = \pm 1$, basta mostrare che le entrate di U^{-1} sono intere. Sia $U^{ij} \in \mathbb{Z}^{n \times n}$ la matrice ottenuta sostituendo l'i-esima colonna il j-esimo versore e_j. Per la regola di Cramer $U^{-1}_{ij} = \frac{\det(U^{ij})}{\det(U)} \in \mathbb{Z}$ perché $\det(U^{ij}) \in \mathbb{Z}$. □

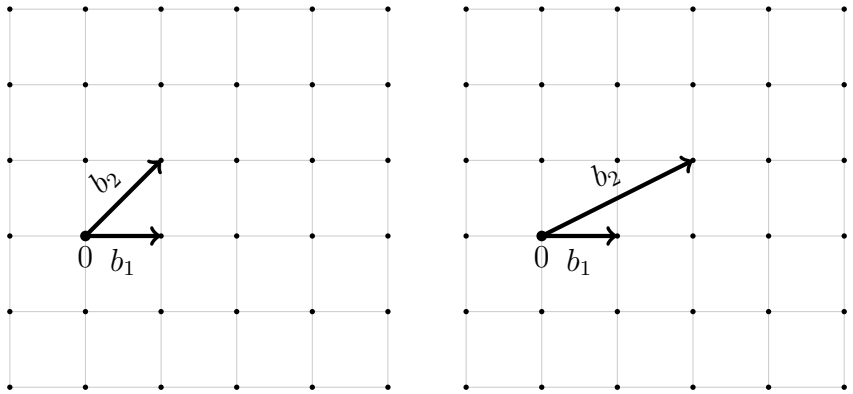

Figura 1.1: Esempio di reticolo di dimensione 2 con due basi diverse

Corollario 1.1.1. *Sia $f : \mathbb{Z}^n \to \mathbb{Z}^n$ tale che $f(\mathbf{x}) = U\mathbf{x}$ con U matrice unimodulare. Allora f è una biiezione.*

Dimostrazione. Basta osservare che $U\mathbf{x} \in \mathbb{Z}^n$ per $\mathbf{x} \in \mathbb{Z}^n$ e che per ogni elemento $\mathbf{y} \in \mathbb{Z}^n$ vale $U(U^{-1}\mathbf{y}) = \mathbf{y}$. □

Possiamo quindi riassumere l'osservazione precedente nella seguente proposizione:

Proposizione 1.2. *Siano $B_1 = (\mathbf{b_1}, ..., \mathbf{b_n}), B_2 = (\mathbf{b'_1}, ..., \mathbf{b'_n}) \in \mathbb{R}^{m\times n}$ due matrici di rango n. Allora $\mathcal{L}(B_1) = \mathcal{L}(B_2)$ se e solo se esiste una matrice unimodulare U tale che $B_2 = B_1U$.*

Dimostrazione. Supponiamo che $\mathcal{L}(B_1) = \mathcal{L}(B_2)$. Allora ogni colonna di B_1 si può vedere come una combinazione lineare a coefficienti interi delle colonne di B_2, ovvero $b_i = \sum_j v_{ij}\mathbf{b'_j}$ con $v_{ij} \in \mathbb{Z}$ per $j = 1, ..., n$. Detta $V = (v_{ij})$ abbiamo che $B_1 = B_2V$. Analogamente $B_2 = B_1U$ da cui segue che $B_2 = B_2VU$. Osservando che $B_2^TB_2$ è invertibile si ottiene che $VU = \mathbb{I}_n$. Si conclude osservando che U, V sono matrici a coefficienti interi.

Assumiamo ora che $B_2 = B_1U$. La matrice U definisce una biiezione di $\mathbb{Z}^n$ in sé stesso. Allora $\mathcal{L}(B_1) = \{B_1\mathbf{a} \mid \mathbf{a} \in \mathbb{Z}^n\} = \{B_1U\mathbf{a} \mid \mathbf{a} \in \mathbb{Z}^n\} = \mathcal{L}(B_2)$. □

Denotiamo la *minima distanza* di $\mathcal{L}$ rispetto alla norma ℓ_p come

$$\lambda_1^{(p)}(\mathcal{L}) = \min_{\mathbf{x}\in\mathcal{L}\setminus\{0\}} \|\mathbf{x}\|_p$$

che sarà oggetto del nostro studio nel Capitolo 3.

Definiamo infine il *determinante* di $\mathcal{L}$ come $\det(\mathcal{L}) = \sqrt{\det(B^TB)}$.

Osservazione. *Il determinante di un reticolo è ben definito come conseguenza della Proposizione 1.2.*

.

1.2 Reticoli Localmente Densi

Definizione 1.3 (Reticoli localmente densi)**.** Siano $p \in [1, \infty)$, $\alpha > 0$ reale e r, R interi positivi. Un (p, α, r, R)-*reticolo localmente denso* è il dato di un reticolo intero di rango R e dimensione n per qualche $n \in \mathbb{N}$ rappresentato da una matrice $A \in \mathbb{Z}^{n \times R}$, un intero positivo ℓ, un vettore di traslazione $\mathbf{x} \in \mathbb{Z}^n$ ed una matrice $T \in \mathbb{Z}^{r \times n}$ tali che

1. $\lambda_1^{(p)}(\mathcal{L}(A)) \geq \ell^{\frac{1}{p}}$.
2. $\{0,1\}^r \subseteq T(V) = \{T\mathbf{v} \mid \mathbf{v} \in V\}$ dove $V = (\mathbf{x} + \mathcal{L}(A)) \cap B_p^n(\alpha \ell^{\frac{1}{p}})$.

Nella sezione successiva utilizzeremo le proprietà di questi reticoli per analizzare la complessità dello *Shortest Vector Problem*.

Riportiamo senza dimostrazione la versione probabilistica del Lemma di Sauer ad opera di Micciancio [14] che riprenderemo nel Capitolo 3 per mostrare che la struttura ottenuta a partire dai codici Reed-Solomon soddisfi la seconda condizione della Definizione 1.3.

Teorema 1.3. *Siano r, n, h interi positivi, $W \subseteq B_{n.h}$ ed $\epsilon > 0$. Se $|W| \geq h! n^{\frac{24r\sqrt{h}}{\epsilon}}$ e $T \in \{0,1\}^{r \times n}$ è ottenuto campionando ogni entrata indipendentemente con probabilità $\frac{1}{4hr}$ che sia 1, allora $\{0,1\}^r \subseteq T(W)$ con probabilità almeno $1 - \epsilon$.*

1.3 Complessità di γ-GapSVP$_p$ attraverso Reticoli Localmente Densi

Diamo una definizione formale del problema al centro del nostro studio presentato nel capitolo introduttivo.

Definizione 1.4 (γ-GapSVP$_p$)**.** Siano $p \geq 1$ e $\gamma = \gamma(n) \geq 1$. Il γ-*approximate Shortest Vector Problem* in norma ℓ_p (γ-GapSVP$_p$) è il problema decisionale definito come segue. Data una base $B \in \mathbb{Z}^{m \times n}$ di una reticolo intero $\mathcal{L}$ e una distanza limite $s > 0$ determinare se soddisfino il caso-positivo oppure il caso-negativo, dove

- caso-positivo: $\lambda_1^{(p)}(\mathcal{L}) \leq s$.
- caso-negativo: $\lambda_1^{(p)}(\mathcal{L}) > \gamma s$.

Lo SVP è strettamente legato allo *Closest Vector Problem* (CVP) che dato $\mathbf{x} \in \mathcal{L}$ con $\mathcal{L}$ reticolo vuole determinare $\mathbf{y} \in \mathcal{L}, \mathbf{x} \neq \mathbf{y}$ tale che la distanza tra i due sia minima. In questo lavoro prendiamo in considerazione una sua variante γ-GapCVP'$_p$.

Definizione 1.5 (γ-GapCVP'$_p$)**.** Siano $p \geq 1$ e $\gamma = \gamma(n) \geq 1$. Il γ-*approximate Closest Vector Problem* in norma ℓ_p (γ-GapCVP'$_p$) è il problema decisionale definito come segue. Data una base $B \in \mathbb{Z}^{d \times r}$ di un reticolo intero $\mathcal{L}$ di rango r, un vettore $\mathbf{t} \in \mathbb{Z}^d$ fissato e una distanza limite $s > 0$ determinare se soddisfino il caso-positivo oppure il caso-negativo, dove

- caso-positivo: esiste un vettore $\mathbf{c} \in \{0,1\}^r$ tale che $\|B\mathbf{c} - \mathbf{t}\|_p \leq s$.
- caso-negativo: $\text{dist}_p(w\mathbf{t}, \mathcal{L}) > \gamma s \quad \forall w \in \mathbb{Z} \setminus \{0\}$.

Abbiamo introdotto questa versione per utilizzare il risultato ottenuto da S. Arora, L. Babai, J.Stern e Z. Sweedyk in [4] di cui riportiamo solo l'enunciato.

Teorema 1.4. *Per ogni $p \in [1, \infty)$ ed ogni costante $\gamma \geq 1$ γ-GapCVP'$_p$ è NP-difficile.*

Il motivo di tale interesse risiede nel teorema successivo in cui mostriamo che è possibile trovare una riduzione in tempo polinomiale da γ-GapCVP'$_p$ a γ'-GapSVP$_p$ con $\gamma > \gamma' \geq 1$ utilizzando i reticoli localmente densi.

Teorema 1.5. *Siano $p \geq 1$, r e n interi positivi, $\alpha > 0$ una costante e γ, γ' costanti tali che $\frac{1}{\alpha} > \gamma' \geq 1$ e $\gamma \geq \gamma' \left(\frac{1}{1-(\alpha\gamma')^p}\right)^{\frac{1}{p}}$. Allora esiste un algoritmo deterministico che in tempo polinomiale data un'occorrenza di γ-GapCVP'$_p$ $(B, \mathbf{t}, s)$ di rango r e un (p, α, r, R)-reticolo localmente denso $(A, \ell, \mathbf{x}, T)$ restituisce un'occorrenza di γ'-GapSVP$_p$ (B', s') di rango $R+1$ di caso-positivo (rispettivamente di caso-negativo) se $(B, \mathbf{t}, s)$ è di caso-positivo (rispettivamente di caso-negativo).*

Dimostrazione. Se $\mathbf{t} = \mathbf{0}$ $(B, \mathbf{t}, s)$ è banalmente di caso-positivo quindi basta porre una qualunque occorrenza di γ'-GapSVP$_p$ di caso-positivo come produzione della riduzione. Allora, senza perdita di generalità, possiamo assumere $\mathbf{t} \neq \mathbf{0}$.

Poniamo come valore ritornato dell'algoritmo (B', s') con

$$B' = \begin{pmatrix} BTA & BT\mathbf{x} - \mathbf{t} \\ \beta A & \beta\mathbf{x} \end{pmatrix} \text{ dove } \beta = \frac{\gamma' s}{\ell^{\frac{1}{p}}(1-(\alpha\gamma')^p)^{\frac{1}{p}}} \neq 0$$

$$s' = (s^p + \alpha^p \beta^p \ell)^{\frac{1}{p}}$$

Essendo tutte le quantità coinvolte calcolabili in tempo polinomiale segue immediatamente che l'algoritmo così definito viene eseguito in tempo polinomiale a sua volta.

Mostriamo ora la sua correttezza. Come prima cosa mostriamo che B' ha rango $R+1$. Sia $\mathbf{u} \in \mathbb{R}^{R+1} \setminus \{\mathbf{0}\}$. Se $(\beta A \mid \beta\mathbf{x})\mathbf{u} \neq \mathbf{0}$ allora $B'\mathbf{u} \neq \mathbf{0}$. Altrimenti se $(A \mid \mathbf{x})\mathbf{u} = 0$ si avrebbe che $u_{n+1} \neq \mathbf{0}$ per indipendenza delle colonne di A (è base di un reticolo). Allora $(BTA \mid BT\mathbf{x} - \mathbf{t})\mathbf{u} = BT(A \mid \mathbf{x})\mathbf{u} - u_{n+1}\mathbf{t} = -u_{n+1}\mathbf{t} \neq 0$ perché $\mathbf{t} \neq \mathbf{0}$. Di nuovo deduciamo che $B'\mathbf{u} \neq \mathbf{0}$ e quindi che le colonne di B' siano linearmente indipendenti.

Dimostriamo ora che $(B, \mathbf{t}, s)$ di caso-positivo implica (B', s') di caso positivo. Per la Definizione 1.5 esiste un vettore $\mathbf{c} \in \{0,1\}^r$ tale che $\|B\mathbf{c} - \mathbf{t}\|_p \leq s$ e per la Definizione 1.3 esiste un vettore $\mathbf{v} = \mathbf{x} + A\mathbf{z} \in \mathbf{x} + \mathcal{L}(A)$ per qualche $\mathbf{z} \in \mathbb{Z}^R$ tale che $\|\mathbf{v}\|_p^p \leq \alpha^p \ell$ e $T\mathbf{v} = \mathbf{c}$. Per tale $\mathbf{z}$ abbiamo che $T(\mathbf{x} + A\mathbf{z}) = T\mathbf{v} = \mathbf{c}$ e quindi

$$\begin{aligned} \lambda_1^{(p)}(\mathcal{L}(B'))^p &\leq \|B'(\mathbf{z}, 1)\|_p^p \\ &= \|BTA\mathbf{z} + BT\mathbf{x} - \mathbf{t}\|_p^p + \beta^p \|A\mathbf{z} + \mathbf{x}\|_p^p \\ &= \|B\mathbf{c} - \mathbf{t}\|_p^p + \beta^p \|A\mathbf{z} + \mathbf{x}\|_p^p \\ &\leq s^p + \alpha^p \beta^p \ell \\ &= (s')^p \end{aligned}$$

come volevamo.

Infine, consideriamo $(B, \mathbf{t}, s)$ di caso-negativo. Dobbiamo provare che $\lambda_1^{(p)}(\mathcal{L}(B'))^p > (\gamma' s')^p$. Essendo le colonne di B' linearmente indipendenti è equivalente mostrare che $\|B'(\mathbf{z}, w)\|_p^p > (\gamma' s')^p \quad \forall (\mathbf{z}, w) \in \mathbb{Z}^{R+1} \setminus \{\mathbf{0}\}$.

Se $w = 0$ necessariamente $\mathbf{z} \neq \mathbf{0}$. Allora per la Definizione 1.3 vale

$$\|B'(\mathbf{z}, w)\|_p^p \geq \beta^p \lambda_1^{(p)}(\mathcal{L}(A))^p > \beta^p \ell$$

Poiché $\beta^p \ell (1 - (\alpha\gamma')^p) = (\gamma' s)^p$ e per la definizione di s' vale

$$\beta^p \ell \geq (\gamma' s)^p + (\alpha\beta\gamma')^p \ell = (\gamma' s')^p$$

Se $w \neq 0$ per la Definizione 1.5 abbiamo che $\|B'(\mathbf{z}, w)\|_p^p \geq \mathrm{dist}_p(w\mathbf{t}, \mathcal{L}(B))^p > (\gamma s)^p$. Si conclude per definizione di γ, β e s' perché

$$(\gamma s)^p \geq (\gamma')^p \frac{s^p}{1 - (\alpha\gamma')^p} = (\gamma')^p \left(s^p + \frac{(\alpha\gamma' s)^p}{1 - (\alpha\gamma')^p} \right) = (\gamma')^p (s^p + \alpha^p \beta^p \ell) = (\gamma' s')^p$$

□

Ricordando che una riduzione in tempo polinomiale non cambia la classe di complessità, deduciamo il seguente corollario (si veda Appendice A per la notazione utilizzata).

Corollario 1.5.1. *Siano $p \geq 1$, r un intero positivo, $\alpha > 0$ una costante ed A un algoritmo che calcoli un $(p, \alpha, r, p(r))$-reticolo localmente denso in $p(r)$ tempo con $p(r)$ polinomio in r. Sia γ costante tale che $1 \leq \gamma < \frac{1}{\alpha}$, allora:*

1. *Se A è deterministico allora γ-GapSVP$_p$ è NP-difficile.*
2. *Se A è randomizzato e il valore ritornato soddisfa con probabilità 1 il primo punto della Definizione 1.3 e con almeno $\frac{2}{3}$ il secondo punto, allora γ-GapSVP$_p$ non è in RP a meno che $NP \subseteq RP$.*
3. *Se A è randomizzato e il valore ritornato soddisfa con probabilità almeno $\frac{2}{3}$ entrambi i punti della Definizione 1.3, allora non esiste un algoritmo randomizzato eseguibile in tempo polinomiale per γ-GapSVP$_p$ a meno che $NP \subseteq BPP$.*

Dimostrazione. Il primo e terzo punto seguono immediatamente dal Teorema 1.5 e dal Teorema 1.4. Osservando che nella parte della dimostrazione del Teorema 1.5 relativa al caso-negativo facciamo uso solamente del primo punto della Definizione 1.3, segue immediatamente anche il secondo punto del Corollario. □

Capitolo 2

Codici Reed-Solomon

L'avvento di sistemi di comunicazione elettronici ha posto il tema del corretto invio delle informazioni al centro dell'interesse dei ricercatori. Infatti questi sistemi non sono infallibili, basta pensare ad un disco graffiato o all'effetto del vento solare su trasmissioni fuori dall'atmosfera terrestre che potrebbero completamente alterare il messaggio iniziale rendendolo irriconoscibile. Una soluzione semplice e di successo prevede il ritorno dei dati ricevuti al mittente per un confronto. L'esempio principe è il protocollo *Transmission Control Protocol* (TCP) che governa un'ampia parte degli scambi via internet. Talvolta questo approccio non è praticabile come nel caso di invio di immagini da parte di satelliti. Nel 1948 C. Shannon [17] dimostra, in astratto, l'esistenza di un *canale di comunicazione* capace di inviare messaggi con un grado di correttezza prestabilito. Un *canale di comunicazione* è costituito dalle seguenti parti:

1. La **sorgente** presenta un messaggio $\mathbf{x} = x_1 \cdots x_k$ da inviare.
2. Il messaggio viene codificato da un **codificatore** aggiungendo ridondanza ottenendo la *parola codificata* o *messaggio codificato* $\mathbf{c} = c_1 \cdots c_n$. Questo passaggio è fondamentale perché gli errori dovuti alla trasmissione del messaggio lo renderebbero immediatamente irrecuperabile.
3. Il **canale di trasmissione** invia il messaggio codificato aggiungendo un *errore* (spesso chiamato *rumore*) $\mathbf{e} = e_1 \cdots e_n$. Il vettore ricevuto è quindi $\tilde{\mathbf{c}} = \mathbf{c} + \mathbf{e}$.
4. Un **decodificatore** rimuove l'errore e ritorna il messaggio $\tilde{\mathbf{x}}$.
5. Il **destinatario** riceve il messaggio.

Il comportamento desiderato prevede $\mathbf{x} = \tilde{\mathbf{x}}$. Poiché il passaggio da messaggio a messaggio codificato e viceversa è una corrispondenza biunivoca, il primo e ultimo pas-

Figura 2.1: Canale di comunicazione

saggio sono spesso ignorati. La *teoria dei codici* si occupa di trovare delle codifiche che garantiscano il corretto funzionamento del canale di comunicazione.

2.1 Codici Lineari

Tra le numerose topologie di codici, i più studiati sono i *codici lineari*.

Definizione 2.1 (codici lineari)**.** Sia $\mathbb{F}_q$ il campo finito con q elementi. Siano n ed m due interi positivi. Un (n, m)-codice $\mathcal{C}$ su $\mathbb{F}_q$ è un sottoinsieme di $\mathbb{F}_q^n$ di cardinalità m.
Se $\mathcal{C}$ è un sottospazio k-dimensionale di $\mathbb{F}_q^n$ con k intero positivo, chiamiamo $\mathcal{C}$ un $[n, k]$-codice lineare su $\mathbb{F}_q$ Un vettore (riga) $(a_1, a_2, ..., a_n)$ di $\mathcal{C}$ si dice *parola codificata* e solitamente si indica con $a_1 a_2 \cdots a_n$.

La natura di sottospazio di uno spazio vettoriale dei codici lineari ci permette di descriverli attraverso matrici. Una *matrice generante* di un $[n, k]$-codice lineare $\mathcal{C}$ è una matrice $k \times n$ G le cui righe formano una base per $\mathcal{C}$. In generale G non è unica. Diremo che G è in *forma standard* se $G = (\mathbb{I}_k \mid A)$. Un $[n, k]$-codice lineare $\mathcal{C}$ può essere visto come il nucleo di una trasformazione lineare. Chiamiamo *matrice di controllo* una matrice $(n - k) \times n$ H tale che $\mathcal{C} = \left\{ \mathbf{x} \in \mathbb{F}_q^n \;\middle|\; H\mathbf{x}^T = \mathbf{0} \right\}$ (ricordiamo che stiamo utilizzando i vettori in riga). Data una matrice di controllo, definiamo la *sindrome* di un vettore $\mathbf{x} \in \mathbb{F}_q^n$ rispetto ad H come il vettore in $\mathbb{F}_q^{n-k}$ definito da $H\mathbf{x}^T$. In particolare un codice lineare $\mathcal{C}$ si può vedere come l'insieme dei vettori di sindrome $\mathbf{0}$.

La matrice generante e la matrice di controllo sono legate tra loro dal seguente teorema.

Teorema 2.1. *Se $G = (\mathbb{I}_k \mid A)$ è la matrice generante in forma standard di un $[n, k]$-codice lineare $\mathcal{C}$, allora $H = (-A^T \mid \mathbb{I}_{m-k})$ è una matrice di controllo per $\mathcal{C}$.*

Dimostrazione. Per costruzione $HG^T = -A^T + A^T = O$. Allora $\mathcal{C}$ è contenuto nel nucleo della trasformazione lineare $\mathbf{x} \mapsto H\mathbf{x}^T$. Poiché H ha rango $n - k$, questa trasformazione ha nucleo di dimensione k come la dimensione di $\mathcal{C}$. □

Le righe di H sono indipendenti e quindi H è la matrice generante di un $[n, n-k]$-codice detto *codice duale* e indicato con $\mathcal{C}^\perp$. Dal teorema precedente segue immediatamente un risultato che lega ulteriormente un codice lineare con il suo duale.

Corollario 2.1.1. *Se G e H sono matrice generante e di controllo rispettivamente per un codice lineare $\mathcal{C}$, allora H e G sono matrice generante e di controllo rispettivamente per il duale $\mathcal{C}^\perp$.*

2.1.1 Distanza e Peso di Hamming

Dati due vettori $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ definiamo la *distanza (di Hamming)* $d(\mathbf{x}, \mathbf{y})$ come il numero di coordinate in cui i due vettori differiscono.

Lemma 2.2. *La distanza di Hamming definita sopra è una distanza su $\mathbb{F}_q^n$.*

Dimostrazione. La positività e la simmetria sono una diretta conseguenza della definizione. La disuguaglianza triangolare segue dall'osservazione che se due coordinate x_i, y_i sono diverse tra loro allora almeno una tra $x_i \neq z_i$ e $y_i \neq z_i$ deve essere vera per qualunque scelta di $\mathbf{z} \in \mathbb{F}_q^n$. □

Definiamo la *(minima) distanza* di un codice $\mathcal{C}$ come la minima distanza tra due parole codificate del codice.

Il *peso (di Hamming)* $wt(\mathbf{x})$ di un vettore $\mathbf{x} \in \mathbb{F}_q^n$ è il numero di coordinate non nulle di $\mathbf{x}$.

Lemma 2.3. *Se* $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ *allora* $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$.

Dimostrazione. Segue immediatamente dal fatto che $a \equiv b \mod q$ se e solo se $a - b \equiv 0 \mod q$ per ogni scelta di $a, b \in \mathbb{F}_q$. □

In particolare, in un codice lineare la distanza minima coincide con il peso minimo. Se la distanza minima d di un $[n, k]$-codice è nota, diremo che tale codice è un $[n, k, d]$-codice.

2.1.2 Reticoli di Controllo

Data una matrice di controllo H possiamo definire un *reticolo di controllo* $\mathcal{L}^\perp(H) = \left\{\mathbf{z} \in \mathbb{Z}^n \;\middle|\; H\mathbf{z}^T = \mathbf{0}\right\} = \ker(H) + q\mathbb{Z}^n = \mathcal{C} + q\mathbb{Z}^n$. Più in generale fissato $\mathbf{u} \in \mathbb{F}_q^r$ con $r = n - k$ definiamo $\mathcal{L}_{\mathbf{u}}^\perp(H) = \left\{\mathbf{z} \in \mathbb{Z}^n \;\middle|\; H\mathbf{z}^{\mathbf{T}} = \mathbf{u}\right\}$.

Osservazione. *Se esiste* $\mathbf{z} \in \mathbb{Z}^n$ *tale che* $H\mathbf{z}^T = \mathbf{u}$*, possiamo vedere* $\mathcal{L}_{\mathbf{u}}^\perp(H)$ *come la classe laterale* $\mathbf{z} + \mathcal{L}^\perp(H)$*. Possiamo quindi identificare le classi laterali di* $\mathcal{L}^\perp(H)$ *con le corrispondenti sindromi* $\mathbf{u}$*. Infatti se* $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ *appartengono alla stessa classe laterale di* $\mathcal{C}$ *abbiamo che* $\mathbf{x} - \mathbf{y} = \mathbf{c} \in \mathcal{C}$ *e quindi* $H\mathbf{x}^T = H(\mathbf{y} + \mathbf{c})^T = H\mathbf{y}^T$*. Viceversa se* $H\mathbf{x}^T = H\mathbf{y}^T$*, allora* $H(\mathbf{x} - \mathbf{y})^T = \mathbf{0}$ *e quindi* $\mathbf{x} - \mathbf{y} \in \mathcal{C}$*.*

Diamo ora un risultato che utilizzeremo nella costruzione di reticoli localmente densi tramite codici Reed-Solomon.

Lemma 2.4. *Siano* q *primo,* r *ed* n *interi positivi e* $H \in \mathbb{F}_q^{r \times n}$ *una matrice di controllo. Allora il reticolo di controllo* $\mathcal{L} = \mathcal{L}^\perp(H)$ *ha rango* n *e determinante* $\det(\mathcal{L}) \leq q^r$*. Vale l'uguaglianza se e solo se le colonne di* H *sono linearmente indipendenti.*

Dimostrazione. Dalla definizione di $\mathcal{L}$ si ha che $q\mathbb{Z}^n \subseteq \mathcal{L} \subseteq \mathbb{Z}^n$ da cui segue che il reticolo ha rango n. Consideriamo ora la mappa $\mathbf{z} \mapsto H\mathbf{z}^T$. Essa è un omomorfismo di gruppi additivi da $\mathbb{Z}^n$ a $\mathbb{F}_q^r$ che ha come nucleo proprio $\mathcal{L}$. Per il primo teorema di isomorfismo la mappa induce un isomorfismo dal gruppo quoziente $\mathbb{Z}^n/\mathcal{L} \to \mathrm{Im}(H) \subseteq \mathbb{F}_q^r$ dove vale l'uguaglianza se le colonne di H sono linearmente indipendenti. Si conclude osservando che $\det(\mathcal{L}) = \left|\mathbb{Z}^n/\mathcal{L}\right| = |\mathrm{Im}(H)| \leq \left|\mathbb{F}_q^r\right| = q^r$. □

2.1.3 Codifica, Decodifica ed Errore

La teoria dei codici si è sviluppata per assicurare il corretto trasferimento di dati attraverso un canale di comunicazione. Questa garanzia dipende dalle procedure di codifica e decodifica del codice utilizzate. In generale, la prima risulta semplice mentre la seconda molto complicata. Per questo motivo trovare nuovi codici con decodifica efficiente o trovare nuovi algoritmi più veloci per codici già studiati è un'attiva area di ricerca. In questa sezione discutiamo brevemente le due procedure nel contesto dei codici lineari, tuttavia le considerazioni presentate possono essere generalizzate anche per altre tipologie di codici.

Sia $\mathcal{C}$ un $[n, k]$-codice lineare su $\mathbb{F}_q$ con matrice generante G e sia $\mathbf{x} \in \mathbb{F}_q^k$ un messaggio. Il metodo più comune di codifica genera la parola codificata $\mathbf{c} = \mathbf{x}G$. Se G è in forma standard le prime k coordinate di $\mathbf{c}$ contengono il messaggio e le $n - k$ successive sono simboli di ridondanza usati per recuperare il messaggio in presenza di rumore nel canale di trasmissione. Per G qualsiasi è sempre possibile ricondursi, attraverso matrici elementari opportune, ad una matrice generante in cui esistono indici di colonne $i_1, ..., i_k$ tali che la matrice $k \times k$ formata da queste colonne sia la matrice identica. In questo caso il messaggio sarà contenuto nelle k coordinate $i_1, ..., i_k$.

Sia ora $\mathbf{y} = \mathbf{c} + \mathbf{e}$ la parola codificata arrivata a destinazione, con $\mathbf{e}$ l'errore dovuto alla trasmissione. L'obiettivo della procedura di decodifica è determinare l'errore. Solitamente, questo risultato viene ottenuto minimizzando la distanza $d(\mathbf{y}, \mathbf{k}) \, \forall \mathbf{k} \in \mathcal{C}$ o equivalentemente determinando un vettore $\mathbf{e}$ tale che $\mathbf{y} - \mathbf{e} \in \mathcal{C}$ che sia più piccolo possibile. In nessuno dei due casi abbiamo necessariamente l'unicità.

Per studiare i vettori vicini ad una data parola codificata è comodo introdurre il concetto di *sfera* di raggio r centrata ad un vettore $\mathbf{v} \in \mathbb{F}_q^k$:

$$S_r(\mathbf{v}) = \left\{ \mathbf{u} \in \mathbb{F}_q^k \;\middle|\; d(\mathbf{v}, \mathbf{u}) \leq r \right\}$$

Queste sfere sono disgiunte se il raggio scelto è sufficientemente piccolo.

Teorema 2.5. *Siano d la minima distanza di un codice $\mathcal{C}$ (non necessariamente lineare) e $t = \lfloor \frac{d-1}{2} \rfloor$. Allora le sfere di raggio t attorno a parole codificate distinte sono disgiunte.*

Dimostrazione. Siano $\mathbf{c_1}, \mathbf{c_2} \in \mathcal{C}$ e sa $\mathbf{z} \in S_t(\mathbf{c_1}) \cap S_t(\mathbf{c_2})$. Allora per la disuguaglianza triangolare (Lemma 2.2) vale $d(\mathbf{c_1}, \mathbf{c_2}) \leq d(\mathbf{c_1}, \mathbf{z}) + d(\mathbf{z}, \mathbf{c_2}) \leq 2t < d$. Quindi $\mathbf{c_1} = \mathbf{c_2}$. □

Da cui segue immediatamente il seguente risultato.

Corollario 2.5.1. *Usando la stessa notazione del teorema, se una parola codificata $\mathbf{c} \in \mathcal{C}$ è ricevuta come $\mathbf{y}$ in cui al più sono presenti t errori, allora $\mathbf{c}$ è l'unica parola codificata più vicina ad $\mathbf{y}$.*

Riportiamo senza dimostrazione (si veda [10]) un teorema che estende il corollario.

Teorema 2.6. *Sia $\mathcal{C}$ un $[n, k, d]$-codice. Se una parola codificata $\mathbf{c} \in \mathcal{C}$ è ricevuta come $\mathbf{y}$ in cui al più sono presenti ν errori e ϵ coordinate sono mancanti tali che $2\nu + \epsilon < d$, allora $\mathbf{c}$ è l'unica parola codificata più vicina ad $\mathbf{y}$.*

Da questi risultati è evidente che la minima distanza d di un codice sia una una buona indicazione della capacità di decodifica dello stesso. Infatti una distanza più grande permette un maggiore numero di errori. Di conseguenza, un ruolo centrale della teoria dei codici è produrre codici con distanze sempre maggiori. Uno di questi codici è il codice Reed-Solomon, un codice ciclico.

2.2 Codici Ciclici

Una famiglia molto importante di codici lineari sono i *codici ciclici*. Quando si studia questa topologia di codici è conveniente utilizzare gli indici $0, 1, ..., n-1$ pensarli come l'insieme degli interi modulo n. Un altra convenzione è $0^0 = 1$ in qualsiasi anello. Per il resto del lavoro assumeremo queste notazioni.

Un codice lineare $\mathcal{C}$ di lunghezza n su $\mathbb{F}_q$ si dice *ciclico* se per ogni elemento $\mathbf{c} = c_0 \cdots c_{n-2} c_{n-1}$ in $\mathcal{C}$ il vettore ottenuto applicando alle coordinate la mappa $i \mapsto i+1 \mod n$ ovvero $c_{n-1} c_0 \cdots c_{n-2}$ appartiene a $\mathcal{C}$ a sua volta.

Un altro modo di descrivere la parola codificata $\mathbf{c} = c_0 c_1 \cdots c_{n-1}$ è il polinomio $c(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1} \in \mathbb{F}_q[x]$ di grado al più $n-1$.

Osservazione. *Essendo la corrispondenza tra* $\mathbf{c}$ *e* $c(x)$ *biunivoca, il polinomio* $xc(x) = c^{n-1}x^n + c_0 x + ... + c_{n-2}x^{n-1}$ *rappresenta* $c_{n-1}c_0 \cdots c_{n-2}$.

La ciclicità di $\mathcal{C}$ ci dice che se $c(x) \in \mathcal{C}$ allora $xc(x) \in \mathcal{C}$ moltiplicando modulo $x^n - 1$. Questo ci suggerisce immediatamente che lo spazio appropriato in cui studiare i codici ciclici sia l'anello $\mathcal{R}_n = {}^{\mathbb{F}_q[x]}/_{x^n-1}$. In altri termini codici ciclici sono ideali di $\mathcal{R}_n$ e viceversa.

È chiaro che lo studio di questi codici è quindi legato allo studio dei fattori irriducibili e del campo di spezzamento di $x^n - 1$. A tale proposito è utile introdurre il concetto di *q-classe laterale ciclotomica* di s modulo n, ovvero l'insieme $C_s = \{s, sq, ..., sq^{r-1}\} \mod n$ dove r è il più piccolo intero positivo tale che $sq^r \equiv s \mod n$. Ovvero C_s è l'orbita della permutazione $i \mapsto iq \mod n$ che contiene s e quindi le distinte q-classi laterali ciclotomiche modulo n partizionano l'insieme $\{0, 1, ..., n-1\}$.

Le classi laterali ciclotomiche sono il cuore di due teoremi che riportiamo senza dimostrazione (si possono trovare in [10]) che ne illustrano i vantaggi.

Teorema 2.7. *Siano* n *un intero positivo coprimo con* q *e* $t = ord_n(q)$. *Sia poi* α *una radice primitiva* n*-esima dell'unità in* $\mathbb{F}_{q^t}$. *Allora:*

(i) Per ogni intero $0 \leq s < n$ *il polinomio minimo di* α^s *su* $\mathbb{F}_q$ *è*

$$m_{a^s}(x) = \prod_{i \in C_s} (x - \alpha^i)$$

dove C_s *e la q-classe laterale ciclotomica di* s *modulo* n.

(ii) I coniugati di α^s *sono gli elementi* α^i *con* $i \in C_s$.

(iii) La fattorizzazione di $x^n - 1$ in fattori irriducibili in $\mathbb{F}_q$ è data da

$$x^n - 1 = \prod_{s \in S} m_{\alpha^s}(x)$$

dove S è l'insieme dei rappresentanti delle q-classi laterali ciclotomiche modulo n.

Teorema 2.8. *Sia $\mathcal{C}$ un codice ciclico in $\mathcal{R}_n$ non nullo. Allora esiste un polinomio $g(x) \in \mathcal{C}$ con le seguenti proprietà:*

(i) $g(x)$ è l'unico polinomio monico di grado minimo in $\mathcal{C}$.

(ii) $\mathcal{C} = \langle g(x) \rangle$.

(iii) $g(x) \mid (x^n - 1)$.

Detto $k = n - \deg g(x)$

(iv) la dimensione di $\mathcal{C}$ è k e $\{g(x), xg(x), ..., x^{k-1}g(x)\}$ è una sua base.

(v) ogni elemento di $\mathcal{C}$ si può descrivere in modo unico come prodotto $g(x)f(x)$ dove $f(x) = 0$ o $\deg f(x) < k$.

(vi) La matrice generante di $\mathcal{C}$ è

$$G = \begin{pmatrix} g(x) & 0 & 0 & 0 \\ 0 & xg(x) & 0 & 0 \\ 0 & 0 & ... & 0 \\ 0 & 0 & 0 & x^{k-1}g(x) \end{pmatrix}$$

(vii) Se α è una radice primitiva n-esima dell'unità in qualche estensione di $\mathbb{F}_q$ allora

$$g(x) = \prod_{s \in S} m_{a^s}(x)$$

dove S è un sottoinsieme dell'insieme rappresentanti delle q-classi laterali ciclotomiche modulo n.

Sia $\mathcal{C}$ un codice ciclico in $\mathcal{R}_n$ con polinomio generante $g(x)$ e sia α una radice primitiva n-esima dell'unità in un'opportuna estensione di $\mathbb{F}_q$. Per i Teoremi 2.7 e 2.8 $g(x) = \prod_{s \in S} \prod_{i \in C_s} (x - \alpha^i)$ con S un sottoinsieme dell'insieme rappresentanti delle q-classi laterali ciclotomiche modulo n. L'insieme $T = T_\alpha = \bigcup_{s \in S} C_s$ è chiamato l'*insieme definente* di $\mathcal{C}$. Diciamo che T contiene un insieme di m consecutivi elementi M se esiste un insieme $\{b, b+1, ..., b+m-1\}$ di m interi consecutivi tale che $\{b, b+1, ..., b+m-1\}$ mod $n = M \subseteq T$. L'insieme $\mathcal{Z} = \{\alpha^i \mid i \in T\}$ è detto insieme degli zeri di $\mathcal{C}$, infatti $c(x)$ appartiene a $\mathcal{C}$ se e solo se $c(\alpha^i) = 0$ per ogni $i \in T$ per il Teorema 2.8. Ovvero T determina completamente il polinomio generante $g(x)$, il cui grado coincide con $|T|$ per lo stesso teorema.

2.3 Codici Reed-Solomon

Lo studio della distanza minima di un codice può essere facilitato da risultati che lo limitano inferiormente. Uno dei più storici è il limite Bose–Chaudhuri–Hocquenghem (limite BCH).

Teorema 2.9 (limite BCH)**.** *Sia $\mathcal{C}$ un codice ciclico di lunghezza n su $\mathbb{F}_q$ con insieme definente T e minimo peso d. Se T contiene $m-1$ elementi consecutivi per qualche intero m, allora $d \geq m$.*

Dimostrazione. Per ipotesi gli zeri di $\mathcal{C}$ contengono $\alpha^b, \alpha^{b+1}, ..., \alpha^{b+m-2}$. Sia ora $c(x) = \sum_{j=1}^{\omega} c_{i_j} x^{i_j} \in \mathcal{C}$ non nulla di peso ω.

Assumiamo per assurdo che $\omega < m$. Poiché $c(\alpha^i) = 0$ per $b \leq i \leq b+m-2$, abbiamo che $M\mathbf{u}^T = \mathbf{0}$ dove

$$M = \begin{pmatrix} \alpha^{i_1 b} & \alpha^{i_2 b} & ... & \alpha^{i_\omega b} \\ \alpha^{i_1 (b+1)} & \alpha^{i_2 (b+1)} & ... & \alpha^{i_\omega (b+1)} \\ \vdots & \vdots & ... & \vdots \\ \alpha^{i_1 (b+\omega-1)} & \alpha^{i_2 (b+\omega-1)} & ... & \alpha^{i_\omega (b+\omega-1)} \end{pmatrix}$$

e $\mathbf{u} = c_{i_1} c_{i_2} \cdots c_{i_\omega}$. Essendo $\mathbf{u} \neq \mathbf{0}$ deduciamo che M è degenere e quindi $\det M = 0$.

Tuttavia $\det M = \alpha^{(i_1+i_2+...+i_\omega)b} \det V$ dove V è la matrice di Vandermonde. Ricordando che $\det V = \prod_{1 \leq j < k \leq \omega} (\alpha^{i_k} - \alpha^{i_j})$ e osservando che gli α^{i_j} sono distinti, deduciamo che $\det V \neq 0$ e quindi che $\det M \neq 0$ trovando un assurdo. □

Sia m un intero tale che $2 \leq m \leq n$. Un *codice BCH* $\mathcal{C}$ su $\mathbb{F}_q$ di lunghezza n e distanza *pianificata* m è il codice ciclico con insieme definente $T = C_b \cup C_{b+1} \cup ... \cup C_{n+m-2}$ per qualche intero b dove C_i è la q-classe ciclotomica modulo n contenente i. L'insieme definente contiene $m-1$ elementi consecutivi e quindi per il limite BCH il codice ha distanza minima almeno m. Se $b = 1$ diciamo che $\mathcal{C}$ è un codice BCH *in senso stretto*.

Definizione 2.2 (Codice Reed-Solomon)**.** Un codice *Reed-Solomon* (RS) $\mathcal{C}$ su $\mathbb{F}_q$ è un codice BCH di lunghezza $n = q-1$.

Se $n = q-1$ allora $\mathrm{ord}_n(q) = 1$, ovvero tutti i fattori irriducibili di $x^n - 1$ hanno grado 1 e tutte le q-classi ciclotomiche modulo n hanno cardinalità 1. Più precisamente le radici di $x^n - 1$ sono gli elementi non nulli di $\mathbb{F}_q$. Quindi se $\mathcal{C}$ ha distanza pianificata m, il suo insieme definente ha cardinalità $m-1$ ed è $\{b, b+1, ..., b+m-2\}$ per qualche intero b.

Presentiamo ora una definizione equivalente dei codici Reed-Solomon in senso stretto che ci permette di definire una generalizzazione dei codici Reed-Solomon. Dato un intero $k \geq 0$, indichiamo con $\mathcal{P}_k$ l'insieme dei polinomi in $\mathbb{F}_q[x]$ di grado minore di k.

Teorema 2.10. *Sia α un elemento primitivo di $\mathbb{F}_q$ e sia k un intero tale che $0 \leq k \leq n = q-1$. Allora $\mathcal{C} = \{(f(1), f(\alpha), ..., f(\alpha^{q-2})) \mid f \in \mathcal{P}_k\}$ è il $[n, k, n-k+1]$-codice Reed-Solomon in senso stretto su $\mathbb{F}_q$.*

Dimostrazione. Poiché $\mathcal{P}_k$ è un sottospazio vettoriale su $\mathbb{F}_q$ di $\mathbb{F}_q[x]$, $\mathcal{C}$ è banalmente un codice lineare su $\mathbb{F}_q$. Mostriamo che $\mathcal{C}$ è k-dimensionale. Essendo $\mathcal{P}_k$ k-dimensionale basta mostrare che dati $f_1, f_2 \in \mathcal{P}_k$ distinti, i corrispondenti elementi in $\mathcal{C}$ lo sono a loro volta. Se così non fosse, la loro differenza sarebbe $\mathbf{0}$ implicando che $f_1 - f_2$, un polinomio non nullo di grado al più $k-1$, abbia $n \geq k$ radici. Assurdo.

Ora sia $\mathcal{D}$ il $[n, k, n-k+1]$-codice RS in senso stretto su $\mathbb{F}_q$. $\mathcal{D}$ ha insieme definente $\{1, ..., n-k\}$. Avendo mostrato che $\mathcal{C}$ è k-dimensionale è sufficiente provare che $\mathcal{C} \subseteq \mathcal{D}$ per avere l'uguaglianza. Sia $c(x) = \sum_{j=0}^{n-1} c_j x^j \in \mathcal{C}$. Per definizione esiste $f(x) = \sum_{m=0}^{k-1} f_m x^m \in \mathcal{P}_k$ tale che $c_j = f(\alpha^j)$ per $0 \leq j < n$. Sia $i \in T$, allora

$$c(\alpha^i) = \sum_{j=0}^{n-1} \left(\sum_{m=0}^{k-1} f_m \alpha^{jm} \right) \alpha^{ij} = \sum_{m=0}^{k-1} f_m \sum_{j=0}^{n-1} \alpha^{(i+m)j} = \sum_{m=0}^{k-1} f_m \frac{\alpha^{(i+m)n} - 1}{\alpha^{i+m} - 1}$$

Ricordando che α è una radice primitiva n-esima dell'unità, $\alpha^{i+m} \neq 1$ e $\alpha^{(i+m)n} = 1$ perché $1 \leq i + m \leq n - 1 = q - 2$. Quindi $c(\alpha^i) = 0 \quad \forall i \in T$, ovvero $c(x) \in \mathcal{D}$. □

Dal Teorema segue immediatamente la generalizzazione.

Definizione 2.3 (Codice Reed-Solomon generalizzato)**.** Siano $1 \leq k \leq n \leq q$ interi, $\gamma = (\gamma_0, ..., \gamma_{n-1}) \in \mathbb{F}_q^n$ tale che $\gamma_i \neq \gamma_j$ per $i \neq j$ e $\mathbf{v} = (v_0, ..., v_{n-1}) \in \mathbb{F}_q^n$ non nullo. I codici $\mathrm{GRS}_k(\gamma, \mathbf{v}) = \{(v_0 f(\gamma_0), ..., v_{n-1} f(\gamma_{n-1})) \mid f \in \mathcal{P}_k\}$ sono detti *codici Reed-Solomon generalizzati* (GRS).

Osserviamo che i codici RS in senso stretto sono codici GRS con $n = q - 1$, $\gamma_i = \alpha^i$ con α radice primitiva n-esima dell'unità e $v_i = 1$.

Si può dimostrare (Teorema 5.33 in [10]) che una matrice generante di $\mathrm{GRS}_k(\gamma, \mathbf{v})$ è data da

$$G = \begin{pmatrix} v_0 & v_1 & ... & v_{n-1} \\ v_0\gamma_0 & v_1\gamma_1 & ... & v_{n-1}\gamma_{n-1} \\ v_0\gamma_0^2 & v_1\gamma_1^2 & ... & v_{n-1}\gamma_{n-1}^2 \\ \vdots & \vdots & ... & \vdots \\ v_0\gamma_0^{k-1} & v_1\gamma_1^{k-1} & ... & v_{n-1}\gamma_{n-1}^{k-1} \end{pmatrix}$$

e una matrice di controllo da

$$H = \begin{pmatrix} w_0 & w_1 & ... & w_{n-1} \\ w_0\gamma_0 & w_1\gamma_1 & ... & w_{n-1}\gamma_{n-1} \\ w_0\gamma_0^2 & w_1\gamma_1^2 & ... & w_{n-1}\gamma_{n-1}^2 \\ \vdots & \vdots & ... & \vdots \\ w_0\gamma_0^{k-1} & w_1\gamma_1^{k-1} & ... & w_{n-1}\gamma_{n-1}^{k-1} \end{pmatrix}$$

dove $\mathbf{0} \neq (w) = (w_0, ..., w_{n-1}) \in \mathbb{F}_q^n$ e tale che $\sum_{i=0}^{n-1} w_i v_i h(\gamma_i) = 0$ per ogni polinomio $h \in \mathcal{P}_{n-1}$. In particolare per $v = (1, ..., 1)$ abbiamo che $w = (1, ..., 1)$. Essendo i γ_i due a due distinti, possiamo vedere γ come il sottoinsieme $S = \{\gamma_0, ...\gamma_{n-1}\} \subseteq \mathbb{F}_q$. Denoteremo con $H_q(n, S)$ la matrice di controllo del $GRS_k(\gamma, (1, ..., 1))$ su $\mathbb{F}_q$. Se $S = \mathbb{F}_q$, $H_q(n, S)$ sarà la matrice di controllo del codice RS (non generalizzato).

Capitolo 3

Reticoli Localmente Densi da Codici Reed-Solomon

In questo Capitolo mostriamo che è possibile costruire reticoli localmente densi per mezzo di codici Reed-Solomon. Più precisamente, detta $H = H_q(k, \mathbb{F}_q)$ la matrice di controllo del codice RS k-dimensionale, dimostriamo che $\mathcal{L} = \mathcal{L}^{\perp}(H)$ soddisfa la Definizione 1.3. Dedurremo dal legame tra somme di potenze e polinomi simmetrici il primo punto della definizione. Il secondo sarà una conseguenza del Teorema 1.3 con opportuni parametri.

3.1 Polinomi Simmetrici e Minima Distanza

Un polinomio $p(x_1, ..., x_n)$ si dice *simmetrico* se è invariante rispetto ad ogni permutazione dell'ordine delle variabili. Per questo motivo scriveremo un polinomio simmetrico come $p(X)$ con $X = \{x_1, ..., x_n\}$ insieme delle variabili e $p(T)$ per indicare la sua valutazione su un multiinsieme T di valori.

Per ogni intero non negativo i, denotiamo l'i-esima *somma di potenze* su un insieme X di variabili come

$$p_i(X) = \sum_{x \in X} x^i$$

e definiamo l'i-esimo polinomio simmetrico *elementare* come

$$e_i(X) = \begin{cases} 1 & \text{se} \quad i = 0 \\ \displaystyle\sum_{\substack{Z \subseteq X \\ |Z| = i}} \prod_{z \in Z} z & \text{se} \quad 1 \leq i \leq |Z| \\ 0 & \text{se} \quad i > |Z| \end{cases}$$

I due sono legati dalle *identitá di Newton* che affermano che per $1 \leq i \leq |X|$ vale

$$ie_i(X) = \sum_{j=1}^{i} (-1)^{j-1} e_{i-j}(X) p_j(X)$$

che ci permette di dimostrare il seguente lemma.

Lemma 3.1. *Siano T e U due multiinsiemi su $\mathbb{F}_q$ con q primo. Sia $k \leq q$ un intero positivo tale che $p_i(T) = p_i(U) \quad \forall i \in [k]$. Allora $e_i(T) = e_i(U) \quad \forall i \in [k]$.*

Dimostrazione. Per induzione.

Se $i = 0$ banalmente $e_0(T) = 1 = e_0(U)$ per definizione di $e_0(X)$.

Se $1 \leq i < k$, poiché $i \in \mathbb{F}_q$ vale

$$\begin{aligned} e_i(T) &= i^{-1} \sum_{j=1}^{i} (-1)^{j-1} e_{i-j}(T) p_j(T) \quad \text{per le identità di Newton} \\ &= i^{-1} \sum_{j=1}^{i} (-1)^{j-1} e_{i-j}(U) p_j(U) \quad \text{per ipotesi induttiva} \\ &= e_i(U) \quad \text{per le identità di Newton} \end{aligned}$$

□

Sia T un multiinsieme su $\mathbb{F}_q$ con q primo. Definiamo il *polinomio delle radici* $f_T(x) \in \mathbb{F}_q[x]$ come

$$f_T(x) = \prod_{t \in T} (x - t) = \sum i = 0^{|T|} (-1)^i e_i(T) x^{|T|-i}$$

Grazie al lemma precedente possiamo trovare una condizione sufficiente per l'uguaglianza di due multiinsiemi.

Proposizione 3.2. *Siano T e U due multiinsiemi su $\mathbb{F}_q$ con q primo. Sia $k \leq \frac{q}{2}$ un intero positivo tale che $|T| + |U| < 2k$ e che $p_i(T) = p_i(U) \quad \forall i \in [k]$. Allora $T = U$.*

Dimostrazione. Per definizione di $p_0(X)$ abbiamo che $|T| \equiv p_0(T) \mod q$ e $p_0(U) \equiv |U| \mod q$. Poiché $p_0(T) = p_0(U)$ e $0 \leq |T| + |U| < 2k \leq q$ abbiamo che $|T| = |U|$ e quindi in particolare che $f_T(x)$ e $f_U(x)$ hanno grado $|T| < k$. Allora per il Lemma 3.1 i due polinomi coincidono. Si conclude che $T = U$ ricordando che l'anello dei polinomi $\mathbb{F}_q[x]$ è un dominio a fattorizzazione unica e $f_T(x)$ spezza in $\mathbb{F}_q$. □

Questo risultato legato ai polinomi simmetrici ci permette di derivare un limite inferiore sulla distanza minima del reticolo $\mathcal{L}$ di un fattore tale da garantire il primo punto della Definizione 1.3.

Teorema 3.3. *Siano q un primo, $S \subseteq \mathbb{F}_q$ e $k \leq \frac{|S|}{2}$ un intero positivo. Indichiamo con $H = H_q(k, S) \in \mathbb{F}_q^{k \times S}$ e $\mathcal{L} = \mathcal{L}^{\perp}(H)$. Allora $\mathcal{L}$ ha distanza minima in ℓ^p tale che $\lambda_1^{(p)}(\mathcal{L}) \geq (2k)^{\frac{1}{p}} \ \forall p \in [1, \infty)$.*

Dimostrazione. Essendo $\mathcal{L} \subseteq \mathbb{Z}^S$ e $\|\mathbf{v}\|_p \geq \|\mathbf{v}\|_1^{\frac{1}{p}}$ per ogni $\mathbf{v} \in \mathbb{Z}^S$ basta provare il teorema per $p = 1$.

Sia ora $\mathbf{x} \in \mathcal{L}$ tale che $\|\mathbf{x}\|_1 < 2k$. Mostriamo che allora $\mathbf{x} = \mathbf{0}$. Siano $\mathbf{x}^+, \mathbf{x}^- \in \mathbb{Z}^S$ gli unici vettori non negativi tali che $\mathbf{x} = \mathbf{x}^+ - \mathbf{x}^-$. Definiamo il multiinsieme T^+: per ogni $s \in S$ con $x_s^+ > 0$, T^+ contiene s con molteplicità x_s^+. Analogamente, definiamo T^- dipendente da $\mathbf{x}^-$.

Osserviamo che $k \leq \frac{|S|}{2} \leq \frac{q}{2}$ per ipotesi, $|T^+| + |T^-| = \|\mathbf{x}\|_1 < 2k$ per costruzione e $p_i(T^+) = p_i(T^-)\ \forall i \in [k]$ essendo $H\mathbf{x}^T = H(\mathbf{x}^+ - \mathbf{x}^-)^T = \mathbf{0}$ e H matrice di controllo. Allora per la Proposizione 3.2 concludiamo che $T^+ = T^-$. Poiché T^+ e T^- erano disgiunti per costruzione deduciamo che $T^+ = T^- = \emptyset$, ovvero che $\mathbf{x} = \mathbf{0}$ come volevamo. □

3.2 Classi Laterali Dense

In questa sezione dimostriamo l'esistenza di classi laterali di $\mathcal{L}$ dense, ovvero con un numero elevato di vettori corti. Più precisamente, per il nostro studio richiediamo che esistano almeno $\binom{n}{h}q^{-k}$ vettori in $B_{n,h}$ per qualsiasi scelta di h. In seguito, mostriamo che una classe laterale campionata casualmente, e di conseguenza efficientemente, ha una buona probabilità di essere densa a sua volta. Utilizzeremo questo risultato per dimostrare che $\mathcal{L}$ soddisfa il secondo punto della Definizione 1.3.

Lemma 3.4. *Siano q un primo, k un intero positivo e $S \subseteq \mathbb{F}_q$ di cardinalità n. Inoltre, siano $H = H_q(k, S) \in \mathbb{F}_q^{k \times S}$ e $\mathcal{L} = \mathcal{L}^\perp(H)$. Allora esiste una classe laterale $\mathbf{x} + \mathcal{L}$ densa.*

Dimostrazione. Per il Lemma 2.4, $\mathcal{L}$ ha $\det(\mathcal{L}) \leq q^k$ classi laterali intere. Osserviamo anche che $B_{n,h}$ ha cardinalità $\binom{n}{h}$. Allora per il principio dei cassetti, il quale afferma che se j oggetti devono essere disposti in i contenitori distinti allora in uno di questi contenitore ci saranno almeno $\lceil \frac{j}{i} \rceil$ oggetti, deve esistere una classe laterale intera $\mathbf{x} + \mathcal{L}$ con $\mathbf{x} \in \mathbb{Z}^n$ opportuno tale che $|(\mathbf{x} + \mathcal{L}) \cap B_{n,h}| \geq \frac{\binom{n}{h}}{q^k}$ vettori binari di peso h. □

In particolare preso $\epsilon > 0$ opportunamente piccolo, abbiamo che per $n \approx q$, $h \approx \alpha^p 2k$ con $\alpha > \frac{1}{2^{\frac{1}{p}}}$ costante e $k = q^\epsilon$ esiste una classe laterale con approssimativamente $q^{(2\alpha^p - 1)k} = q^{\Omega(q^\epsilon)}$ vettori di questo tipo, un numero sub-esponenziale in q.

Lemma 3.5. *Siano q un primo, k un intero positivo e $S \subseteq \mathbb{F}_q$ di cardinalità n. Inoltre, siano $H = H_q(k, S) \in \mathbb{F}_q^{k \times S}$ e $\mathcal{L} = \mathcal{L}^\perp(H)$. Allora esiste un efficiente algoritmo randomizzato che presi $\delta \geq 0$, H e $h \in [n]$ restituisce $\mathbf{x} \in B_{n,h}$ tale che*

$$\mathbb{P}\left(|(\mathbf{x} + \mathcal{L}) \cap B_{n,h}| \geq \delta \binom{n}{h} q^{-k}\right) > 1 - \delta$$

Dimostrazione. L'algoritmo campiona in modo uniforme e randomizzato un vettore binario $\mathbf{x} \in B_{n,h}$ e lo ritorna. La procedura è quindi ovviamente efficiente.

Mostriamo la correttezza. Per ogni $\mathbf{u} \in \mathbb{F}_q^k$ sia $K_{\mathbf{u}} = \left|\left\{\mathbf{z} \in B_{n,h} \;\middle|\; H\mathbf{z}^T = \mathbf{u}\right\}\right|$ ed $s = H\mathbf{x}^T \in \mathbb{F}_q^k$ la sindrome di $\mathbf{x}$ rispetto alla matrice di controllo H. Allora:

$$\begin{aligned}
\mathbb{P}\left(|(\mathbf{x}+\mathcal{L}) \cap B_{n,h}| < \delta\binom{n}{h}q^{-k}\right) &= \mathbb{P}\left(K_{\mathbf{s}} < \delta\binom{n}{h}q^{-k}\right) \\
&= \sum_{\mathbf{u}\in\mathbb{F}_q^k : K_{\mathbf{u}} < \binom{n}{h}q^{-k}} \mathbb{P}\left(H\mathbf{X}^T = \mathbf{U}\right) \\
&= \sum_{\mathbf{u}\in\mathbb{F}_q^k : K_{\mathbf{u}} < \binom{n}{h}q^{-k}} \frac{K_{\mathbf{u}}}{\binom{n}{h}} \\
&< \sum_{\mathbf{u}\in\mathbb{F}_q^k : K_{\mathbf{u}} < \binom{n}{h}q^{-k}} \frac{\delta}{q^k} \\
&\leq \delta \quad \text{perché ci sono al più } q^k \text{ termini nella somma}
\end{aligned}$$

□

3.3 Reticoli Localmente Densi da Codici Reed-Solomon

Abbiamo ora tutti gli strumenti necessari a dimostrare che con opportuni parametri possiamo costruire un reticolo localmente denso a partire da matrici di controllo di codici Reed-Solomon e di conseguenza che SVP è *NP*-difficile.

Teorema 3.6. *Siano $p \in [1,\infty)$ e $\alpha > \frac{1}{2^{\frac{1}{p}}}$ una costante. Allora esiste un algoritmo randomizzato che in tempo polinomiale dato in sistema unario un intero positivo r sufficientemente grande restituisce un $(p,\alpha,r,p(r))$-reticolo localmente denso che soddisfa il primo punto della definizione con probabilità 1 ed il secondo con probabilità almeno $\frac{2}{3}$.*

Dimostrazione. L'algoritmo fissa

ϵ - una costante $\epsilon = 2\alpha^p - 1 > 0$.

k - un intero limitato polinomialmente in r e tale che $k \geq r^{\frac{1}{\frac{1}{2}-\delta}}$ per qualche costante arbitraria $\delta \in (0, \frac{1}{2})$.

q - un primo limitato polinomialmente in r e tale che $q \geq k^{\frac{3(1+\epsilon)}{\epsilon}}$, che esiste per il Postulato di Bertrand.

Successivamente, restituisce le componenti di un $(p,\alpha,r,p(r))$-reticolo localmente denso $(A,\ell,\mathbf{x},T)$ dove

A - $A \in \mathbb{Z}^{q\times q}$ è una base del reticolo $\mathcal{L} = \mathcal{L}^{\perp}(H)$ con $H = H_q(k,\mathbb{F}_q) \in \mathbb{F}_q^{k\times q}$.

ℓ - $\ell = 2k$.

x - $\mathbf{x} \in B_{q,h}$ è un vettore binario q-dimensionale di peso $h = \lfloor(1+\epsilon)k\rfloor$ campionato uniformemente.

T - $T \in \{0,1\}^{r \times q}$ campionando ogni entrata indipendentemente con probabilità $\frac{1}{4hr}$ che sia 1.

Studiamo la complessità dell'algoritmo. q può essere facilmente calcolabile in tempo $p(r)$ utilizzando l'algoritmo di divisione di Fibonacci. A è ottenuta in tempo polinomiale deterministico combinando le colonne della matrice generante in forma standard derivata dalla trasposizione di H (si vedano il Teorema 2.1 e le matrici dei codici GRS), che avviene in tempo polinomiale. l è banalmente calcolato in tempo polinomiale deterministico e sia $\mathbf{x}$ che T in tempo polinomiale randomizzato. Quindi, il tempo di esecuzione dell'algoritmo è polinomiale randomizzato come desiderato.

Dimostriamo ora la correttezza, ovvero mostriamo che $(A, \ell, \mathbf{x}, T)$ soddisfa la Definizione 1.3.

Punto 1 Il primo punto della definizione è sempre soddisfatto per il Teorema 3.3 poiché

$$\lambda_1^{(p)}(\mathcal{L}) \geq (2k)^{\frac{1}{p}} = \ell^{\frac{1}{p}}$$

Punto 2 Sia $W = (\mathbf{x} + \mathcal{L}) \cap B_{q,h}$. Per definizione dell'algoritmo abbiamo che

$$\|\mathbf{w}\|_q^q = h \leq (1+\epsilon)k = \alpha^p \ell \ \forall \mathbf{w} \in W$$

e di conseguenza che $W \subseteq V = (\mathbf{x} + \mathcal{L}) \cap B_p^q(\alpha \ell^{\frac{1}{p}})$.

Mostriamo ora che

$$\frac{\binom{q}{h}}{10q^k} \geq h!\ q^{240r\sqrt{h}} \tag{1}$$

Utilizzando la disuguaglianza $\binom{q}{h} \geq \left(\frac{q}{h}\right)^h$ e il fatto che $h \geq (1+\epsilon)k - 1$ abbiamo che

$$\frac{\binom{q}{h}}{10q^k} \geq \frac{q^{h-k}}{10h^h} = \Omega\left(\frac{q^{\epsilon k - 1}}{h^h}\right)$$

Inoltre per la scelta di k legata ad r e per il fatto che $h \leq (1+\epsilon)k$ vale

$$h!\ q^{240r\sqrt{h}} \leq h^h q^{240k^{\frac{1}{2}-\delta}\sqrt{(1+\epsilon)k}} \leq h^h q^{o(k)}$$

Dalla combinazione delle due equazioni deduciamo che è sufficiente provare che $q^{(1-o(1))\epsilon k} \geq h^{2h}$ per ottenere il risultato desiderato. Sfruttando che $k^{\frac{3(1+\epsilon)}{\epsilon}} \leq q \leq p(r)$, $h \leq (1+\epsilon)k$ e la monotonia del logaritmo basta dimostrare che vale

$$(1-o(1))\epsilon k \frac{3(1+\epsilon)}{\epsilon} \log k = (3-o(1))(1+\epsilon)k \log k \geq 2(1+\epsilon)k \log k + O(k)$$

che chiaramente vale per k sufficientemente grande e di conseguenza per r sufficientemente grande.

Per concludere osserviamo che per il Lemma 3.5

$$\mathbb{P}\left(|W| \geq \frac{\binom{q}{h}}{10q^k}\right) > 1 - \frac{1}{10} = \frac{9}{10}$$

Se questo evento si verifica e vale l'Equazione (1) abbiamo che $\{0,1\}^r \subseteq T(W) \subseteq T(V)$ on probabilità almeno $\frac{9}{10}$ per il Teorema 1.3. Allora, per la disuguaglianza di Boole, segue che l'algoritmo ha una probabilità di successo almeno $1 - \frac{2}{10} > \frac{2}{3}$ per r sufficientemente grande.

□

Come immediata conseguenza otteniamo il teorema riassuntivo di questo lavoro.

Teorema 3.7. *Per ogni $p \in [1, \infty)$ e costante $1 \leq \gamma < 2^{\frac{1}{p}}$ vale che γ-GapSVP$_p$ non è in RP a meno che $NP \subseteq RP$.*

Dimostrazione. Segue immediatamente dal Corollario 1.5.1 e il Teorema 3.6. □

Bibliografia

[1] M. Ajtai. «Generating hard instances of lattice problems (extended abstract)». en. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*. Philadelphia, Pennsylvania, United States: ACM Press, 1996, pp. 99–108.

[2] Miklós Ajtai. «The shortest vector problem in L_2 is NP -hard for randomized reductions (extended abstract)». en. In: *Proceedings of the thirtieth annual ACM symposium on Theory of computing - STOC '98*. Dallas, Texas, United States: ACM Press, 1998, pp. 10–19.

[3] Miklos Ajtai e Cynthia Dwork. *A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence Revision of: TR96-065*. Rapp. tecn. 065. 1996.

[4] Sanjeev Arora et al. «The Hardness of Approximate Optima in Lattices, Codes, and Systems of Linear Equations». en. In: *Journal of Computer and System Sciences* 54.2 (apr. 1997), pp. 317–331.

[5] Huck Bennett e Chris Peikert. *Hardness of the (Approximate) Shortest Vector Problem: A Simple Proof via Reed-Solomon Codes*. arXiv:2202.07736 [cs]. Feb. 2022.

[6] Jin-Yi Cai e A. Nerurkar. «Approximating the SVP to within a factor (1-1/dim/sup /spl epsiv//) is NP-hard under randomized conditions». In: *Proceedings. Thirteenth Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference) (Cat. No.98CB36247)*. 1998, pp. 46–55.

[7] Michael R. Garey e David S. Johnson. *Computers and Intractability; A Guide to the Theory of NP-Completeness*. USA: W. H. Freeman & Co., 1990.

[8] Craig Gentry. «Fully homomorphic encryption using ideal lattices». en. In: *Proceedings of the forty-first annual ACM symposium on Theory of computing*. Bethesda MD USA: ACM, mag. 2009, pp. 169–178.

[9] Jeffrey Hoffstein, Jill Pipher e Joseph H. Silverman. «NTRU: A ring-based public key cryptosystem». en. In: *Algorithmic Number Theory*. A cura di Joe P. Buhler. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1998, pp. 267–288.

[10] W. Cary Huffman e Vera Pless. *Fundamentals of Error-Correcting Codes*. en. Google-Books-ID: RAsjychHkLYC. Cambridge University Press, feb. 2010.

[11] Subhash Khot. «Hardness of approximating the Shortest Vector Problem in high ℓ_p norms». en. In: *Journal of Computer and System Sciences*. JCSS FOCS 2003 Special Issue 72.2 (mar. 2006), pp. 206–219.

[12] Subhash Khot. «Hardness of approximating the shortest vector problem in lattices». en. In: *Journal of the ACM* 52.5 (set. 2005), pp. 789–808.

[13] Daniele Micciancio. «Inapproximability of the Shortest Vector Problem: Toward a Deterministic Reduction». In: *Theory of Computing* 8 (set. 2012). Number: 22 Publisher: Theory of Computing, pp. 487–512.

[14] Daniele Micciancio. «The Shortest Vector in a Lattice is Hard to Approximate to within Some Constant». In: *SIAM Journal on Computing* 30.6 (gen. 2001). Publisher: Society for Industrial and Applied Mathematics, pp. 2008–2035.

[15] Van Emde Boas P. «Another NP-complete problem and the complexity of computing short vectors in a lattice». In: *Tecnical Report, Department of Mathmatics, University of Amsterdam* (1981). Publisher: Department of Mathmatics, University of Amsterdam.

[16] Oded Regev. «On lattices, learning with errors, random linear codes, and cryptography». en. In: *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*. Baltimore MD USA: ACM, mag. 2005, pp. 84–93.

[17] C. E. Shannon. «A mathematical theory of communication». In: *The Bell System Technical Journal* 27.3 (lug. 1948). Conference Name: The Bell System Technical Journal, pp. 379–423.

Appendice A

Complessità Temporale

In informatica, lo studio della complessità di un algoritmo è l'analisi dell'utilizzo delle risorse che questo impiega durante la sua esecuzione. Indichiamo con *complessità temporale* la quantità di tempo impiegata da un algoritmo a essere eseguito in funzione della lunghezza dei dati in input, che indicheremo con il parametro n.

Date due funzioni f e g definite su $\mathbb{N}$ a valori in $\mathbb{R}$ diciamo che

1. $f(n)$ è un $O(g(n))$ se $\exists c > 0, n_0 \in \mathbb{N}$ tale che $|f(n)| \leq c|g(n)|\ \forall n \geq n_0$.
2. $f(n)$ è un $\Omega(g(n))$ se $\exists c > 0, n_0 \in \mathbb{N}$ tale che $|f(n)| \geq c|g(n)|\ \forall n \geq n_0$.
3. $f(n)$ è un $\Theta(g(n))$ se $\exists c_1, c_2 > 0, n_0 \in \mathbb{N}$ tale che $c_1|g(n)| \leq |f(n)| \leq c_2|g(n)|\ \forall n \geq n_0$.

Nello studio dell'efficienza di un algoritmo solitamente si considera il caso peggiore ovvero l'istanza di un algoritmo che impiega il maggior tempo possibile. Definiamo la *funzione di complessità* di un algoritmo rispetto al tempo come la funzione che ad un input di grandezza n associa il tempo massimo che l'algoritmo impiega. Un algoritmo si dice *a tempo polinomiale* o semplicemente *polinomiale* se la sua funzione di complessità è un $O(p(n))$ con p polinomio. Un algoritmo che non è polinomiale si dice *esponenziale*.

Queste definizioni sono utilizzate per classificare i problemi computazionali in base all'efficienza del migliore algoritmo che risolve tale problema. La classe di problemi P contiene i problemi che possono essere risolti in tempo polinomiale tramite un algoritmo deterministico. Un problema appartiene alla classe NP se esiste un programma deterministico che verifica una soluzione in tempo polinomiale o alternativamente se esiste un algoritmo non deterministico che lo risolve in tempo polinomiale. Ricordiamo anche la classe RP contenente tutti i problemi decisionali risolvibili in tempo polinomiale da un algoritmo probabilistico che sbaglia solo da un lato, ovvero che nel caso negativo risulta sempre corretta e nel caso positivo ha una probabilità di successo superiore a $\frac{1}{2}$. La classe BPP contiene i problemi risolvibili in tempo polinomiale con una probabilità di errore al massimo di $\frac{1}{3}$. Dalle definizioni segue immediatamente che $P \subseteq RP \subseteq BPP \subseteq NP$. È un problema irrisolto mostrare le inclusioni inverse, in particolare $NP \subseteq P$ che la maggior parte della comunità scientifica considera falsa.

Uno strumento importante dell'analisi computazionale è la *riduzione algoritmica*. Diciamo che un problema è ridotto ad un altro problema se è possibile costruire un algoritmo

che trasformi un istanza del primo in un istanza del secondo. Un problema si dice *NP-completo* se ogni problema in *NP* è riducibile polinomialmente ad esso. Diciamo che un problema è *NP-difficile* se ogni problema *NP*-completo è riducibile polinomialmente ad esso.

Una trattazione più approfondita può essere trovata in [7].