Fondamenti di Algoritmi, Complessità e Problem Solving

Corso tenuto dal Professor Ferdinando Cicalese

Università di Verona

Alessio Gjergji

Indice

Capitolo 1

Introduzione

1.1 Cos'è la complessità computazionale?

La Teoria della Complessità pone domande fondamentali sullo studio dei problemi computazionali, cercando di comprendere la natura e le sfide che questi rappresentano. Le questioni centrali che guida la ricerca in questo campo includono:

- Come le risorse necessarie per risolvere un problema si scalano con una misura della dimensione del problema?
- Perché alcuni problemi sono difficili e altri facili?
- Cosa rende i problemi difficili, "difficili"?
- Perché tutto ciò è importante per noi?

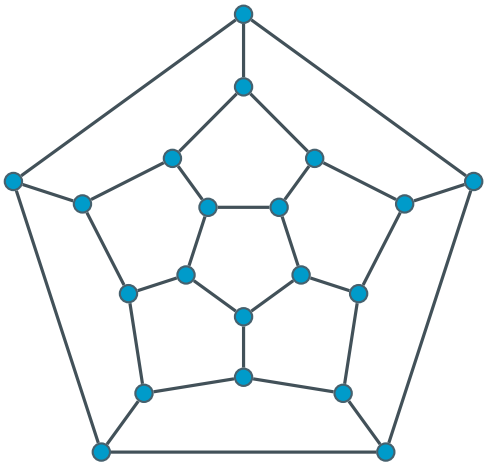
Queste domande ci aiutano a capire non solo la natura dei problemi computazionali ma anche come e perché alcune questioni sono intrinsecamente più complesse di altre. Esplorando queste domande, la Teoria della Complessità ci fornisce strumenti e metriche per valutare e confrontare problemi computazionali, gettando luce sui limiti del calcolo e sull'efficacia degli algoritmi.

Definizione di Complessità Computazionale

La Complessità Computazionale è lo studio delle risorse necessarie per risolvere problemi computazionali.

1.1.1 Primi problemi computazionali

Supponiamo di di avere il seguente grafo:



Supponiamo di voler risolvere questi due problemi:

- C'è un cammino del grafo $\mathcal{G}$ che tocca tutti gli archi esattamente una volta?
- C'è un cammino del grafo $\mathcal{G}$ che tocca tutti i nodi esattamente una volta?

Il primo problema è noto come **Problema del Ciclo Euleriano**, mentre il secondo è noto come **Problema del Cammino Hamiltoniano**.

1.1.2 Il Ciclo Euleriano

Il problema del Ciclo Euleriano è stato formulato da Leonhard Euler nel 1736, quando risolse il problema dei ponti di Königsberg. Il problema consisteva nel trovare un percorso che attraversasse ogni ponte della città esattamente una volta senza ripercorrere lo stesso ponte.

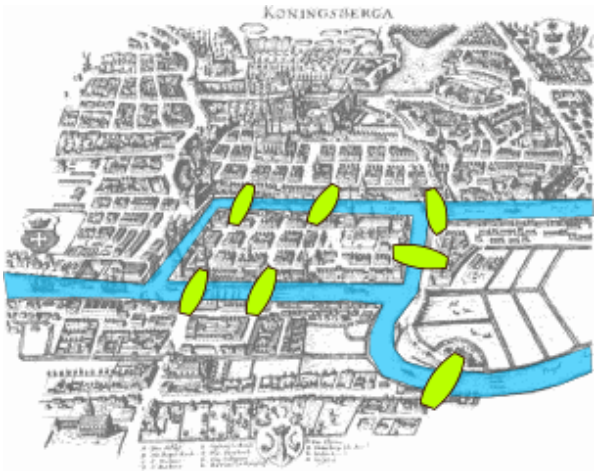


Figura 1.1.1: I ponti di Königsberg

Euler riuscì a trasformare questo problema pratico in un quesito astratto di teoria dei grafi. Sostanzialmente, il problema chiede se esiste un ciclo in un grafo che attraversi tutti gli archi

esattamente una volta. Euler formulò un teorema, che descrive le condizioni necessarie affinché esista tale ciclo.

Teorema di Euler

Un grafo connesso e non orientato possiede un ciclo che inizia e termina sullo stesso vertice e attraversa ogni arco esattamente una volta se e solo se ogni vertice ha grado pari. Se ci sono esattamente due vertici di grado dispari, allora esiste un percorso che inizia in un vertice, attraversa ogni arco esattamente una volta, e termina nell'altro vertice.

Euler dimostrò che un grafo ha un ciclo euleriano se e solo se è connesso e ogni nodo ha un grado pari. Se il grafo non è connesso, o se ha più di due nodi con un grado dispari, allora non può avere un ciclo euleriano. Questo risultato non solo ha risolto il problema dei ponti di Königsberg ma ha anche gettato le basi per il campo della teoria dei grafi.

Il costo computazionale per **decidere** se un grafo ha un ciclo euleriano è $O(|V| + |E|)$, dove $|V|$ è il numero di nodi e $|E|$ è il numero di archi.

Algorithm 1: Determinazione di un ciclo euleriano in un grafo $\mathcal{G}$

Input : Un grafo connesso e non orientato $\mathcal{G}$
Output: Booleano che indica se il grafo $\mathcal{G}$ ha un ciclo euleriano

```
1  odd-vertex-num ← 0
2  foreach v ∈ G.V do
3  |  if degree(v) mod 2 ≠ 0 then
4  |  |  odd-vertex-num ← odd-vertex-num + 1
5  |  end
6  end
7  if odd-vertex-num = 0 ∨ odd-vertex-num = 2 then
8  |  return true
9  end
10 return false
```

Ci chiediamo ora quanto costa **certificare** che il grafo $\mathcal{G}$ ha un ciclo euleriano. La complessità computazionale per certificare che un grafo ha un ciclo euleriano è $O(|V| + |E|)$, dove $|V|$ è il numero di nodi e $|E|$ è il numero di archi. Questo perché ci basterebbe scorrere il grafo e contare il grado di ogni nodo.

1.1.3 Il Cammino Hamiltoniano e il Ciclo Hamiltoniano

Proprio come il problema dei ponti di Königsberg ha portato alla definizione del ciclo euleriano, la ricerca di un ciclo che visiti ogni vertice di un grafo esattamente una volta ha portato alla definizione di un ciclo hamiltoniano. Questo problema prende il nome dal matematico William Rowan Hamilton che lo studiò nel XIX secolo.

A differenza dei cicli euleriani, dove un ciclo deve attraversare tutti gli archi esattamente una volta, un ciclo hamiltoniano deve passare per tutti i vertici una sola volta e tornare al vertice di partenza. Il problema del ciclo hamiltoniano chiede se tale ciclo esista in un dato grafo.

Problema del Ciclo Hamiltoniano

Un ciclo hamiltoniano esiste in un grafo $\mathcal{G}$ se e solo se esiste una sequenza chiusa che visita ogni vertice una volta prima di ritornare al vertice iniziale. Tuttavia, a differenza del problema euleriano, non esiste un criterio semplice per verificare l'esistenza di un ciclo hamiltoniano in un grafo generale.

Il problema del ciclo hamiltoniano è `NP-completo`, il che significa che non è noto alcun algoritmo efficiente che lo risolva per ogni grafo in tempo polinomiale. È interessante notare che, mentre per i cicli euleriani è relativamente semplice determinarne l'esistenza e costruirli, per i cicli hamiltoniani anche solo la verifica della loro esistenza può essere computazionalmente impegnativa.

Quanto costa **decidere** se un grafo $\mathcal{G}$ è hamiltoniano? Non lo sappiamo con certezza! Forse richiede tempo esponenziale? Quanto costa **verificare** che un grafo G sia o non sia hamiltoniano? Per mostrare che lo è, basta fornire un cammino hamiltoniano.

1.1.4 Il Problema della partizione massima

Consideriamo i seguenti 38 numeri. La loro somma è 2 000 000:

```
14175 15055 16616 17495 18072 19390 19731 22161 23320 23717
26343 28725 29127 32257 40020 41867 43155 46298 56734 57176
58306 61848 65825 66042 68634 69189 72936 74287 74537 81942
82027 82623 82802 82988 90467 97042 97507 99564
```

Per verificare una potenziale soluzione a questo problema, si potrebbe pensare di provare tutte le possibili combinazioni dei 38 numeri presi 19 alla volta. Questo approccio, tuttavia, comporterebbe l'esplorazione di circa 35×10^9 configurazioni diverse, un compito computazionalmente oneroso.

Se, invece, vi fosse data una specifica partizione dei numeri, il costo per verificarne la validità sarebbe notevolmente inferiore. Per confermare che una partizione proposta è una soluzione valida, sarebbe sufficiente:

1. Assicurarsi che ciascun gruppo sia composto esattamente da 19 numeri.
2. Sommare i numeri in uno dei gruppi per verificare che la loro somma sia pari a 1000000.

Questa metodologia di verifica fornisce un modo efficiente per confermare la correttezza di una soluzione proposta senza la necessità di esaminare tutte le possibili combinazioni.

1.1.5 La Primalità di un Numero e la Ricerca di Fattori Piccoli

Un problema fondamentale nell'aritmetica e nella crittografia è determinare se un numero intero N sia primo o meno. Inoltre, si può voler sapere se N ha un fattore piccolo, inferiore a un certo limite q.

Un esempio storico notevole fu presentato da Frank Cole nel 1903, quando dimostrò che:

$$N = 193707721 \times 761838257287$$

scomponendo così il numero in due fattori primi, senza l'ausilio di computer o calcolatrici elettroniche, ma probabilmente mediante metodi sistematici e molta pazienza.

Algoritmi per la Primalità

L'algoritmo più efficiente conosciuto per decidere se un numero intero N sia primo ha una complessità temporale di $O((\log N)^{6+\epsilon})$, dove ϵ è un piccolo numero positivo. Questo dimostra che, sebbene non sia immediato, il problema della primalità può essere risolto in tempo polinomiale.

Fattorizzazione:

D'altra parte, non conosciamo una procedura efficiente per fattorizzare un grande intero nei suoi divisori, al di là del tentativo di tutte le possibilità. Questo rende la fattorizzazione di grandi numeri una sfida significativa, specialmente per i numeri che hanno solo fattori grandi.

Costo della Certificazione di un Fattore Piccolo

La certificazione o verifica di un fattore piccolo di N può essere relativamente semplice e rapida. Se ci viene dato un fattore $f < q$, possiamo semplicemente dividere N per f e verificare se il risultato è un numero intero senza resto. Questo processo ha un costo computazionale di $O(\log N)$, rendendolo efficiente anche per numeri molto grandi.

Questa discussione evidenzia il contrasto tra la relativa facilità di verificare la primalità o la presenza di fattori piccoli e la difficoltà significativa di fattorizzare numeri grandi. Questo contrasto è al cuore di molti sistemi di crittografia moderni, che si affidano alla difficoltà di fattorizzare come garanzia di sicurezza.

1.1.6 Il problema degli scacchi

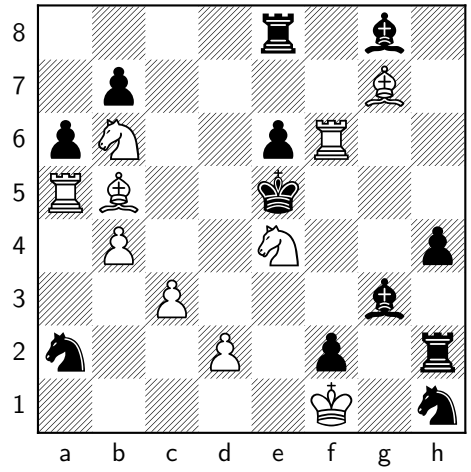


Figura 1.1.2: Scacco Matto in 3 mosse

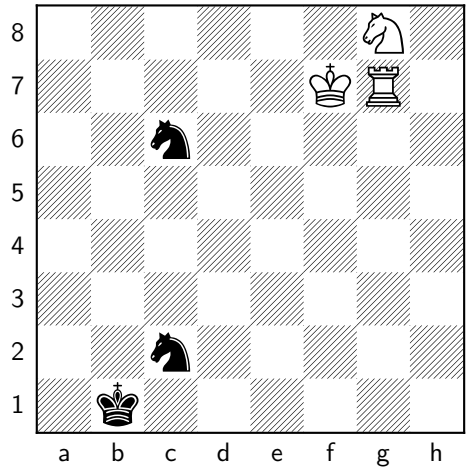


Figura 1.1.3: Scacco Matto in 262 mosse

Un aspetto interessante degli scacchi è la verifica della presenza di uno scacco matto in una data posizione. La complessità di tale verifica aumenta con il numero di mosse necessarie per raggiungere lo scacco matto dallo stato attuale della scacchiera. Consideriamo il seguente ragionamento logico per dimostrare uno scacco matto in n mosse:

"Esiste una mossa w_1 tale che, per qualsiasi risposta b_1, esiste una mossa w_2 tale che, per qualsiasi risposta b_2, ..., fino a che per qualsiasi risposta b_{n-1}, esiste una mossa w_n che produce uno scacco matto."

Questo implica una sequenza di mosse forzate in cui il Bianco, indipendentemente dalle mosse del Nero, può garantire uno scacco matto. Tale sequenza di mosse è spesso indicata come "matto in n mosse". Il processo di verifica di questa affermazione richiede una conoscenza approfondita delle strategie di scacchi e, per posizioni complesse, può richiedere molto tempo.

1.2 Problema computazionale

Problema computazionale

Un problema computazionale descrive un infinito insieme di possibili input, chiamati *istanze*, e rappresenta una relazione che mappa ogni istanza a un insieme non vuoto di possibili output.

Questa definizione sottolinea due componenti fondamentali di un problema computazionale:

- **Insieme di Istanze**: Ogni problema computazionale ammette un'infinità di possibili istanze di input. Queste istanze rappresentano le diverse configurazioni o scenari su cui il problema può operare.

- **Relazione Input-Output**: Per ogni istanza di input, esiste una relazione ben definita che determina l'insieme dei possibili output. Questa relazione è cruciale per definire correttamente il problema e per comprendere la natura delle soluzioni possibili.

Un problema computazionale non è una singola domanda, ma una famiglia di domande, ognuna delle quali corrisponde a una diversa istanza di input.

1.2.1 Misurazione dell'efficienza algoritmica

L'efficienza di un algoritmo nel risolvere un problema computazionale è fondamentale per comprendere sia la sua praticità sia la sua applicabilità a insiemi di dati di grandi dimensioni. La misurazione dell'efficienza algoritmica si basa su diversi fattori chiave:

- **Dimensione dell'istanza (n)**: Rappresenta la quantità di dati in input all'algoritmo. La dimensione dell'istanza è spesso il fattore più diretto che influenza la complessità di un problema.
- **Crescita delle risorse utilizzate ($T(n)$)**: Indica come le risorse necessarie per eseguire l'algoritmo crescono con l'aumentare della dimensione dell'input. $T(n)$ è spesso espressa in termini di tempo (*ad esempio, il numero di operazioni richieste*) o spazio (*ad esempio, la quantità di memoria necessaria*).
- **Caso peggiore**: Analizza la complessità dell'algoritmo nella situazione più sfavorevole possibile. Questo scenario fornisce un limite superiore sulle risorse necessarie per qualsiasi input di dimensione n.

Anche se non trattato qui, è importante notare che, oltre al caso peggiore, si può considerare anche il caso medio, che fornisce un'indicazione delle risorse necessarie in media, dato un insieme rappresentativo di istanze di input.

Questa analisi permette di valutare e confrontare algoritmi in base alla loro efficienza, guidando la scelta dell'algoritmo più adatto per un determinato problema e insieme di dati.

1.2.2 Complessità computazionale

La **complessità computazionale** si riferisce alla quantità di risorse computazionali necessarie per risolvere il problema in questione. La complessità può essere esplorata sotto due principali prospettive: i limiti superiori e i limiti inferiori.

Limiti Superiori

I *limiti superiori* indicano quanto bene possiamo risolvere il problema, cioè la complessità dell'algoritmo più efficiente conosciuto che risolve il problema. Dimostrare un limite superiore significa mostrare che esiste almeno un algoritmo con la complessità affermata per risolvere il problema.

Limiti Inferiori

I *limiti inferiori*, d'altra parte, indicano quanto sia difficile il problema, ossia la quantità minima di risorse che ogni algoritmo deve utilizzare per risolverlo. Per stabilire un limite inferiore, dobbiamo mostrare che tutti gli algoritmi hanno una complessità almeno pari al limite inferiore affermato.

Esempio

Consideriamo il problema della moltiplicazione di due numeri interi di n cifre.

- **Limiti Superiori:** La procedura elementare insegnata nelle scuole richiede $O(n^2)$ moltiplicazioni ed addizioni elementari. Tuttavia, questo non è necessariamente la complessità del problema della moltiplicazione, poiché esistono algoritmi più efficienti.
- **Limiti Inferiori:** Al minimo, dobbiamo leggere tutto l'input, il che implica una complessità di almeno $\Omega(n)$.
- L'*algoritmo di Karatsuba* riduce la complessità a $O(n^{\log_2 3}) = O(n^{1.585})$, dimostrando che la moltiplicazione può essere effettuata più velocemente rispetto alla procedura elementare.
- L'*algoritmo migliore conosciuto* per la moltiplicazione ha una complessità inferiore a $o(n^{1+\epsilon})$ per ogni $\epsilon > 0$, dove la notazione $o(\cdot)$ indica una crescita asintotica più lenta rispetto alla funzione dentro le parentesi.

Questo esempio illustra come l'analisi della complessità fornisca una comprensione profonda sia delle potenzialità sia dei limiti degli algoritmi nel risolvere problemi computazionali.

1.2.3 Trattabilità di un problema

La comprensione della differenza tra **crescita polinomiale** e **crescita esponenziale** delle risorse necessarie da un algoritmo è fondamentale per valutare la sua efficienza e praticabilità. Jack Edmonds, nel 1965, ha sottolineato l'importanza di questa distinzione, che rimane centrale nell'analisi degli algoritmi.

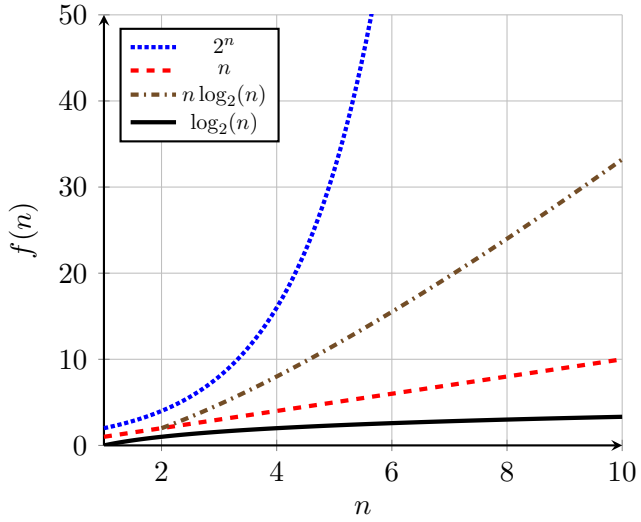
Crescita Polinomiale

La crescita polinomiale si verifica quando il requisito di risorse di un algoritmo è limitato da n^k per qualche costante k. In questo contesto, se l'input raddoppia da n a $2n$, il requisito di risorse aumenta di un fattore costante, da n^k a $2^k n^k$. Questo indica che la crescita delle risorse necessarie è gestibile e prevedibile al crescere delle dimensioni dell'input.

Crescita Esponenziale

Al contrario, la crescita esponenziale descrive una situazione in cui il requisito di risorse cresce proporzionalmente a c^n per qualche costante $c > 1$. Quando l'input raddoppia, il requisito di risorse si quadruplica, passando da c^n a $c^{2n} = (c^n)^2$. Questa rapida escalation rende gli algoritmi con crescita esponenziale impraticabili per input di grandi dimensioni.

Confronto tra crescita polinomiale ed esponenziale



Legge di Moore

La legge di Moore, formulata da Gordon Moore nel 1965, afferma che il numero di transistor in un microprocessore raddoppia approssimativamente ogni 18 mesi.

Ogni due anni la velocità dei computer raddoppia, ma questo non è sempre decisivo. Consideriamo due scenari:

Algoritmi Polinomiali: $O(n^k)$

Con un algoritmo polinomiale, il tempo di esecuzione cresce polinomialmente con la dimensione dell'input n. In un tempo T:

- Se oggi risolviamo istanze di dimensione n_T,
- tra due anni possiamo risolvere istanze di dimensione $n' = n_T 2^{1/k}$.

Questo dimostra che l'aumento di potenza computazionale ci permette di gestire istanze significativamente più grandi in modo più efficiente.

Algoritmi Esponenziali: $\Omega(2^n)$

Con un algoritmo esponenziale, il tempo di esecuzione cresce esponenzialmente con la dimensione dell'input n. In un tempo T:

- Se oggi risolviamo istanze di dimensione n_T,
- tra due anni possiamo risolvere istanze di dimensione $n' = n_T + 1$.

In questo caso, l'aumento di potenza computazionale ci consente di affrontare solo istanze leggermente più grandi, evidenziando i limiti degli algoritmi con crescita esponenziale.

Capitolo 2

NP completezza e co-NP

2.1 Classi di complessità

L'idea fondamentale per dimostrare che determinati problemi sono più difficili dei problemi risolvibili in tempo polinomiale è quella di "ritagliare" una classe di problemi che abbiano una determinata caratteristica, e dimostrare che un problema specifico è almeno tanto difficile quanto i problemi di quella classe, **riducendo** il problema specifico ad un problema della classe.

2.1.1 Tipologie di problemi

- **Problemi decisionali**: problemi che ammettono risposta sì/no. Un problema di decisione è quindi un insieme di istanze, e la risposta è sì se l'istanza appartiene all'insieme, no altrimenti.

  Un problema di decisione è il seguente: dato un grafo $\mathcal{G}$ dire se esiste un cammino euleriano in $\mathcal{G}$.

- **Problemi di ricerca**: problemi di ricerca ammettono una soluzione che può essere trovata in tempo polinomiale.

  Un problema di ricerca è il seguente: dato un grafo $\mathcal{G}$ trovare un cammino euleriano in $\mathcal{G}$.

- **Problemi di ottimizzazione**: problemi di ottimizzazione ammettono una soluzione che può essere trovata in tempo polinomiale.

  Un problema di ottimizzazione è il seguente: dato un grafo $\mathcal{G}$ trovare il cammino euleriano più lungo in $\mathcal{G}$.

Nello studio della complessità considereremo solo problemi decisionali, in quanto tutti i problemi di ricerca e di ottimizzazione possono essere ricondotti a problemi di decisione. Ciò significa che se siamo in grado di dire che un determinato problema di decisione è difficile, allora possiamo dire che anche il problema di ricerca e quello di ottimizzazione sono difficili,

perché se fossimo in grado di risolvere un problema di ricerca o di ottimizzazione, potremmo risolvere anche il problema di decisione in tempo polinomiale.

2.1.2 Formalizzazione di un problema computazionale

In relazione a ciò che è stato detto nella sezione 1.2, un problema computazionale è un insieme infinito di istanze e la loro relazione con la soluzione associata. Matematicamente, possiamo definire un problema computazionale attraverso:

- $\mathbb{A}$ denota il problema computazionale sotto esame.
- $\mathscr{I}(\mathbb{A})$ rappresenta lo spazio delle istanze, ovvero il dominio dei possibili quesiti.
- $\texttt{sol}(\mathbb{A})$ esprime la relazione che associa a ciascuna istanza la sua soluzione o insieme di soluzioni.

Esempio 2.1.1 Consideriamo, ad esempio, il problema del ciclo hamiltoniano. In questo contesto:

- $\mathbb{A}$ corrisponde alla questione di determinare l'esistenza di un ciclo hamiltoniano.
- $\mathscr{I}(\mathbb{A})$ comprende tutti i possibili grafi $\mathcal{G}$ sui quali indaghiamo.
- $\texttt{sol}(\mathbb{A})$ identifica i percorsi che visitano ogni nodo del grafo esattamente una volta, se esistenti.

Pertanto, la relazione $\mathbb{A}$ si configura come una **connessione** fra lo spazio delle istanze e le corrispondenti soluzioni. Matematicamente, ciò si traduce nella seguente inclusione:

$$\mathbb{A} \subseteq \mathscr{I}(\mathbb{A}) \times \texttt{sol}(\mathbb{A})$$

indicando con $(\mathcal{G}, \mathcal{P})$ l'insieme delle coppie dove $\mathcal{P}$ rappresenta un valido ciclo hamiltoniano nel grafo $\mathcal{G}$.

Per ciascuna istanza x appartenente allo spazio dei problemi computazionali, $\texttt{sol}(x)$ denota l'insieme delle soluzioni y tali che $(x, y) \in \mathbb{A}$, ovvero:

$$\texttt{sol}(x) = \{y \mid (x, y) \in \mathbb{A}\}$$

Problemi di Decisione

Nei problemi di decisione, lo spazio delle soluzioni è binario, $\texttt{sol}(\mathbb{A}) = \{\texttt{yes}, \texttt{no}\}$. Pertanto, A associa a ciascuna istanza x una delle due possibili risposte, determinando se l'istanza soddisfa la proprietà esaminata:

$$A : \mathscr{I}(\mathbb{A}) \to \{\texttt{yes}, \texttt{no}\}$$

Problemi di Ricerca

Per i problemi di ricerca $\mathbb{A}^S$, il problema di decisione associato $\mathbb{A}^D$ verifica l'esistenza di almeno una soluzione per l'istanza x:

$$\mathbb{A}^D(x) = \begin{cases} \texttt{yes} & \text{se esiste almeno una soluzione,} \\ \texttt{no} & \text{altrimenti} \end{cases}$$

2.1.3 La Classe P

Nella teoria della complessità computazionale, la capacità di risolvere un problema computazionale va oltre la semplice identificazione di una soluzione per un'istanza specifica. Ciò richiede l'impiego di un algoritmo deterministico A che, per ogni istanza x nell'insieme $\mathscr{I}(\mathbb{A})$, produce una soluzione y valida, ovvero $y \in \texttt{sol}(x)$:

$$A(x) = y \quad \text{con} \quad y \in \texttt{sol}(x)$$

Il *tempo di esecuzione* $T_A(x)$ dell'algoritmo A su un'istanza x è fondamentale, poiché riflette l'efficienza con cui l'algoritmo raggiunge la soluzione.

Classe P

Un algoritmo A è definito *polinomiale* (poly-time) quando il suo tempo di esecuzione, per ogni istanza $x \in \mathscr{I}(\mathbb{A})$, è limitato superiormente da un polinomio nella dimensione di x:

$$T_A(x) = O(|x|^c) \quad \text{per una certa costante } c \in \mathbb{N}.$$

Un problema computazionale viene considerato *fuori dalla classe P* qualora non esista, per nessuna costante c, un algoritmo capace di risolvere tutte le sue istanze in tempo polinomiale $O(n^c)$.

2.1.4 La Classe EXP

Classe EXP

La classe EXP raggruppa i problemi di decisione risolvibili da un algoritmo deterministico in tempo esponenziale rispetto alla dimensione dell'input. Un problema $\mathbb{A}$ appartiene a EXP se esiste un algoritmo A per cui, data una costante c_A, per ogni istanza $x \in \mathscr{I}(\mathbb{A})$ si ha che:

$$T_A(x) = O(2^{|x|^{c_A}})$$

In altre parole, il tempo di esecuzione di A è limitato superiormente da una funzione esponenziale della dimensione dell'input elevata a una costante. Questa classe include quindi problemi per i quali la risoluzione richiede una quantità di tempo che cresce esponenzialmente con l'aumentare della dimensione dell'input.

Da qui segue che la classe EXP è una generalizzazione della classe P, poiché ogni problema risolvibile in tempo polinomiale è anche risolvibile in tempo esponenziale. In altre parole, P è un sottoinsieme di EXP.

$$\texttt{P} \subseteq \texttt{EXP}$$

Perché se un problema $\mathcal{A} \in \texttt{P}$, allora esiste un algoritmo A, per cui, data una costante c_A, per ogni istanza $x \in \mathscr{I}(\mathbb{A})$ si ha che:

$$T_A(x) = O(|x|^{c_A})$$

Poiché, ogni polinomio è anche una funzione esponenziale, si ha che:

$$T_A(x) = O(2^{|x|^{c_A}})$$

Quindi $\mathbb{A} \in \texttt{EXP}$.

È importante notare che un problema è nella classe EXP, non se gli unici algoritmi conosciuti per risolverlo sono esponenziali, ma se esiste almeno un algoritmo deterministico che lo risolve in tempo esponenziale.

Esempio 2.1.2 Consideriamo il problema del cammino euleriano. Un cammino euleriano è un cammino che attraversa ogni arco del grafo esattamente una volta. In input si ha un grafo $\mathcal{G}$ e si vuole sapere se esiste un cammino euleriano in $\mathcal{G}$, quindi l'output è `yes` se esiste un cammino euleriano e `no` altrimenti. Questo problema è nella classe P, infatti esiste un algoritmo polinomiale per risolverlo, controllando se il grafo è connesso e se ogni nodo ha grado pari.

Esempio 2.1.3 Consideriamo il problema del commesso viaggiatore. In input si ha un grafo completo pesato $\mathcal{G}$ e si vuole sapere se esiste un ciclo hamiltoniano di peso minimo in $\mathcal{G}$, quindi l'output è `yes` se esiste un ciclo hamiltoniano e `no` altrimenti. Non sappiamo se esiste un algoritmo polinomiale per risolvere questo problema, quindi non sappiamo se è nella classe P. Sappiamo che per ogni istanza, se la soluzione è `yes` possiamo certificarla in tempo polinomiale.

Prova Semplice

Una **prova semplice** è un certificato di lunghezza polinomiale che può essere verificato in tempo polinomiale.

Cerchiamo di caratterizzare i problemi che hanno una prova semplice.

2.1.5 La Classe NP

Classe NP

Un problema $\mathbb{A}$ appartiene alla classe NP se esiste un algoritmo deterministico A (*verificatore*) e una funzione polinomiale p tale che, per ogni istanza $x \in \mathscr{I}(\mathbb{A})$, esiste un certificato y di lunghezza polinomiale rispetto alla dimensione di x tale che:

$$B(x,y) = \begin{cases} \texttt{yes} & \text{se } x \in \texttt{sol}(\mathbb{A}), \\ \texttt{no} & \text{altrimenti} \end{cases}$$

Inoltre, esiste una costante c_A tale che il tempo di esecuzione di A è limitato superiormente da una funzione polinomiale della dimensione di x:

$$T_A(x,y) = O(p(|x|^{c_A}))$$

In notazione formale, si ha che:

$$\begin{aligned} \texttt{NP} = \{\mathbb{A} \mid \exists A, c_A, \forall x \in \mathscr{I}(\mathbb{A}) : \mathbb{A}(x) = \texttt{yes} \Rightarrow \\ \exists y, |y| = O((|x|^{c_A})), \text{ t.c. } A(x,y) = \texttt{yes} \wedge T_A(x,y) = O((|x|^{c_A}))\} \end{aligned}$$

È importante notare che il tempo di esecuzione del verificatore A è polinomiale rispetto alla dimensione dell'input x e del certificato y. Ciò significa che, se esiste un certificato y tale che

$A(x, y) = \texttt{yes}$, allora esiste un algoritmo che può verificare la soluzione in tempo polinomiale. Da questo segue che il certificato deve essere di lunghezza polinomiale rispetto alla dimensione dell'input x.

$$|y| = O((|x|^{c_A}))$$

Teorema 2.1.1 La classe P è un sottoinsieme della classe NP.

$$\texttt{P} \subseteq \texttt{NP}.$$

Dimostrazione. Consideriamo il problema $\mathbb{A} \in \texttt{P}$. Allora esiste un algoritmo deterministico A che risolve per ogni istanza $x \in \mathscr{I}(\mathbb{A})$ in tempo polinomiale:

$$T_A(x) = O(|x|^{c_A}).$$

Definiamo un verificatore B per $\mathbb{A}$. Per ogni istanza $x \in \mathscr{I}(\mathbb{A})$ e y, $B(x, y) = A(x)$. Quindi se $\mathbb{A}(x) = \texttt{yes}$, allora per ogni $y \in \{0,1\}^*$, $B(x, y) = \texttt{yes}$ e se $\mathbb{A}(x) = \texttt{no}$, allora per ogni $y \in \{0,1\}^*$, $B(x, y) = \texttt{no}$. □

Teorema 2.1.2 La classe NP è sottoinsieme della classe EXP.

$$\texttt{NP} \subseteq \texttt{EXP}.$$

Dimostrazione. Consideriamo un problema $\mathbb{A} \in \texttt{NP}$. Allora esiste un algoritmo deterministico B e una costante c_B tale che per ogni istanza $x \in \mathscr{I}(\mathbb{A})$, esiste un certificato y di lunghezza polinomiale rispetto alla dimensione di x tale che:

$$B(x, y) = \begin{cases} \texttt{yes} & \text{se } x \in \texttt{sol}(\mathbb{A}), \\ \texttt{no} & \text{altrimenti.} \end{cases}$$

Quindi il tempo di esecuzione di B è limitato superiormente da una funzione polinomiale della dimensione di x:

$$T_B(x, y) = O((|x|^{c_B}))$$

Definiamo un algoritmo deterministico $A^{\texttt{EXP}}$ che per ogni $x \in \mathscr{I}(\mathbb{A})$ cicla su tutti i possibili certificati y della taglia ammissibile per i certificati e usa $B(x, y)$ per verificare se x è una soluzione di $\mathbb{A}$:

Algorithm 2: Algoritmo $A^{\texttt{EXP}}$

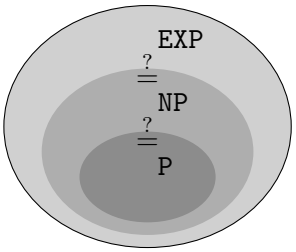
Input: Un'istanza $x \in \mathscr{I}(\mathbb{A})$
Output: yes se $x \in \texttt{sol}(\mathbb{A})$, no altrimenti

```
1 foreach y ∈ {0,1}^{|x|^{c_B}} do
2     if B(x, y) = yes then
3         return yes
4     return no
```

Sappiamo che $A^{\texttt{EXP}}(x) = \texttt{yes}$ se e solo se esiste un certificato $y \in \{0,1\}^{|x|^{c_B}}$ tale che $B(x,y) = \texttt{yes}$, ovvero se $\mathbb{A} = \texttt{yes}$. Il tempo di esecuzione di $A^{\texttt{EXP}}$ è limitato superiormente da una funzione esponenziale della dimensione di x:

$$T_{A^{\texttt{EXP}}}(x) = O(2^{|x|^{c_B}})$$

Quindi $\mathbb{A} \in \texttt{EXP}$, ovvero $\texttt{NP} \subseteq \texttt{EXP}$. □



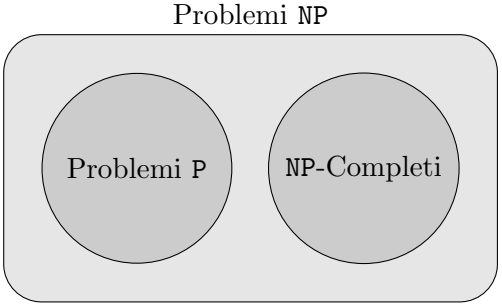
Non sappiamo se le inclusioni sono strette, ma sappiamo che P è incluso strettamente in EXP.

Congettura P ≠ NP

Se $\texttt{P} \neq \texttt{NP}$, quindi $\texttt{P} \subset \texttt{NP}$, allora esistono problemi che possono essere verificati in tempo polinomiale, ma non possono essere risolti in tempo polinomiale.

$$\texttt{P} \subset \texttt{NP}$$
$$\texttt{P} \neq \texttt{NP}$$

Il problema è che non esiste una dimostrazione formale che $\texttt{P} \neq \texttt{NP}$. Siamo convinti di ciò perché crediamo che alcuni problemi NP siano più difficili di altri e se siamo in grado di risolvere tali problemi allora siamo in grado di risolvere tutti i problemi NP. Questa situazione porta alla distinzione tra i problemi NP cosiddetti "difficili" o NP-hard e i problemi NP-completi, per i quali una soluzione efficiente implicherebbe la possibilità di risolvere efficientemente ogni problema nell'insieme NP.



2.2 Riduzione polinomiale tra problemi

La riduzione polinomiale ci permette di mettere in relazione i problemi tra loro, permettendoci di dimostrare che un problema è almeno tanto difficile quanto un altro problema.

Riduzione polinomiale (Karp)

Siano $\mathbb{A}$ e $\mathbb{B}$ due problemi decisionali. Diciamo che $\mathbb{A}$ si riduce polinomialmente a $\mathbb{B}$, e scriviamo $\mathbb{A} \leq_p \mathbb{B}$, se esiste una funzione calcolabile in tempo polinomiale $f : \{0,1\}^* \to \{0,1\}^*$ tale che per ogni $x \in \{0,1\}^*$:

$$\forall x \in \mathbb{A} \qquad \mathbb{A}(x) = \texttt{yes} \iff \mathbb{B}(f(x)) = \texttt{yes}$$

2.2.1 Colorazione di un grafo

Consideriamo il problema della colorazione di un grafo. Dato un grafo $\mathcal{G} = (V, E)$, dove V è l'insieme dei vertici e E è l'insieme degli archi, il problema consiste nel determinare se è possibile colorare i vertici di $\mathcal{G}$ con k colori in modo che due vertici adiacenti non abbiano lo stesso colore. Solitamente tale problema si associa al problema di allocazione di risorse, dove i vertici rappresentano le risorse e gli archi rappresentano le relazioni di dipendenza tra le risorse.

La coloriazione è **propria** se per ogni arco $(u, v) \in E$ si ha che $c(u) \neq c(v)$, ovvero due vertici adiacenti non possono avere lo stesso colore.

Il problema della `k-colorazione` è un problema `NP` perché possiamo verificare in tempo polinomiale se una colorazione è propria. Quindi una **prova semplice** che dimostra che il problema della `k-colorazione` è `NP` è la seguente:

- Dato un grafo $\mathcal{G}$ e una colorazione $c : V \to \{1, \ldots, k\}$, possiamo verificare in tempo polinomiale se c è una colorazione propria, e tale colorazione si verifica in tempo polinomiale $O(|V|+|E|)$. Immaginiamo che la colorazione sia una funzione che associa ad ogni vertice un numero intero che rappresenta il colore del vertice. Se c è una colorazione propria, allora per ogni arco $(u, v) \in E$ si ha che $c(u) \neq c(v)$.

Ci chiediamo ora se esiste un algoritmo polinomiale per la colorazione di un grafo. La risposta è legata al parametro k che rappresenta la diversa tipologia di problemi che possiamo avere. Proviamo a vedere per i diversi valori di k se esiste un algoritmo polinomiale per la colorazione di un grafo:

- $\mathbf{k = 1}$: se $k = 1$ allora il problema è banale, perché tutti i vertici devono avere lo stesso colore, per farlo basta che il grafo sia massimamente disconnesso, ovvero non ci siano archi tra i vertici. Questo problema è risolvibile in tempo polinomiale.
- $\mathbf{k = 2}$: se $k = 2$ allora il problema è equivalente al problema della `bipartizione` di un grafo, ovvero se è possibile dividere i vertici di un grafo in due insiemi V_1 e V_2 tali che non esistano archi tra vertici dello stesso insieme. Per verificare che un grafo è bipartito

possiamo verificare che non esistano cicli dispari nel grafo. Questo problema è risolvibile in tempo polinomiale, infatti possiamo utilizzare l'algoritmo di BFS, che ha complessità $O(|V| + |E|)$.

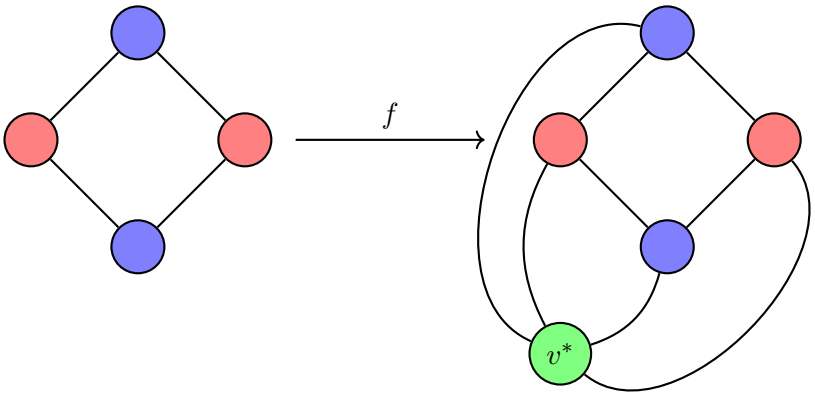
Per $k \geq 3$ non sappiamo se esiste un algoritmo polinomiale per la colorazione di un grafo.

k-colorazione $\leq_p$ (k + 1)-colorazione

Se (k+1)-colorazione è P, allora k-colorazione è P, ovvero (k+1)-colorazione non è più facile di k-colorazione.

$$\texttt{(k+1)-col} \in \texttt{P} \implies \texttt{k-col} \in \texttt{P} \equiv \texttt{k-col} \notin \texttt{P} \implies \texttt{(k+1)-col} \notin \texttt{P}$$

Forniamo la funzione calcolabile in tempo polinomiale f, tale che per ogni grafo $\mathcal{G}$, se $\mathcal{G}$ è un grafo k-colorabile, se e solo se $f(\mathcal{G})$ è un grafo (k+1)-colorabile.



L'idea è quella di aggiungere un vertice v^* al grafo $\mathcal{G}$, e collegare v^* a tutti i vertici di $\mathcal{G}$, in modo tale che v^* abbia un colore diverso da tutti gli altri vertici. Per costruire la funzione f possiamo procedere come segue:

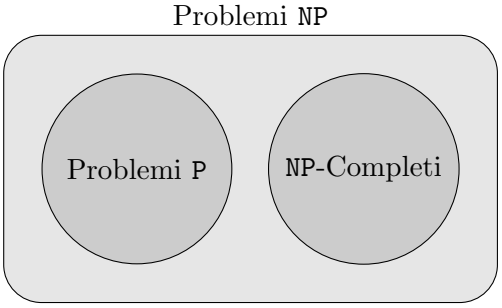
- Dato un grafo $\mathcal{G}$, aggiungiamo un vertice v^* al grafo $\mathcal{G}$.
- Colleghiamo v^* a tutti i vertici di $\mathcal{G}$.
- Assegnamo a v^* un colore diverso da tutti gli altri vertici, ovvero il colore $k + 1$.

Se $\mathcal{G}$ è k-colorabile, allora esiste una colorazione c tale che per ogni arco $(u, v) \in E$ si ha $c(u) \neq c(v)$. Se aggiungiamo un vertice v^* al grafo $\mathcal{G}$, e lo colleghiamo a tutti i vertici di $\mathcal{G}$, allora v^* deve avere un colore diverso da tutti gli altri vertici, ovvero il colore $k + 1$. Quindi, se $\mathcal{G}$ è k-colorabile, allora $\mathcal{G}'$ è (k+1)-colorabile.

Se $\mathcal{G}'$ è (k+1)-colorabile senza perdita di generalità diciamo che il colore di v^* è $k + 1$. Poiché per ogni v, $c(v) \neq k+1$, $c(v) \in \{1, \ldots, k\}$ e quindi $c(v) \neq c(v^*)$, ovvero tutti i vertici v hanno un colore diverso da v^*. Quindi, se $\mathcal{G}'$ è (k+1)-colorabile, allora $\mathcal{G}$ è k-colorabile.

2.3 Problemi NP-completi

I problemi NP-completi sono una classe di problemi che sono problemi in NP e se uno di questi problemi è in P, allora tutti i problemi in NP sono in P, ovvero P = NP. Se P ≠ NP, allora nessun problema NP-completo è in P.



Supponiamo che esista un problema $\mathbb{B} \in$ NP tale che per ogni problema $\mathbb{A}$ in NP, esiste una riduzione polinomiale da $\mathbb{A}$ a $\mathbb{B}$. Quindi se $\mathbb{B}$ è in P, allora $\mathbb{A}$ è in P allora per ogni problema $\mathbb{A}$ in NP esiste una riduzione polinomiale da $\mathbb{A}$ a $\mathbb{B}$ e quindi $\mathbb{A}$ è in P. Per contrapposizione, se P ≠ NP, allora $\mathbb{B}$ non è in P e quindi $\mathbb{A}$ non è in P.

Diciamo che $\mathbb{B}$ è NP-completo se $\mathbb{B}$ è in NP e per ogni problema $\mathbb{A}$ in NP, $\mathbb{A}$ è riducibile a $\mathbb{B}$ in tempo polinomiale, ovvero $\mathbb{A} \leq_p \mathbb{B}$.

> Un problema $\mathbb{B}$ è NP-completo se $\mathbb{B}$ è in NP e $\mathbb{B}$ è NP-hard.

Un problema NP-completo deve essere un problema rappresentativo di tutti i problemi in NP, deve essere quindi codificabile in modo tale che tutti i problemi in NP siano riducibili a esso.

2.3.1 Soddisfacibilità booleana

Il problema della soddisfacibilità booleana è il problema di determinare se una formula booleana è soddisfacibile, ovvero se esiste un assegnamento di valori di verità alle variabili della formula che rende la formula vera. L'input al problema è una formula booleana in forma normale congiuntiva (CNF) ϕ e l'output è yes se e solo se esiste un assegnamento di valori di verità alle variabili della formula che rende la formula vera.

Una **formula booleana in forma normale congiuntiva (CNF)** è definita come una congiunzione di clausole. Formalmente, sia $\phi(x_1, \ldots, x_n)$ una formula booleana che dipende dalle variabili booleane $x_1, \ldots, x_n$. Questa formula può essere espressa come segue:

$$\phi(x_1, \ldots, x_n) = C^{(1)} \wedge C^{(2)} \wedge \cdots \wedge C^{(m)}$$

dove m è il numero totale di clausole nella formula, e ogni clausola $C^{(i)}$ è definita come una disgiunzione di uno o più letterali:

$$C^{(i)} = l_1^{(i)} \vee l_2^{(i)} \vee \cdots \vee l_{k_i}^{(i)}$$

In questa definizione, k_i rappresenta il numero di letterali nella i-esima clausola $C^{(i)}$, e ogni letterale $l_j^{(i)}$ può essere una variabile booleana x_t o la sua negazione $\overline{x_t}$, per qualche $t \in \{1, \ldots, n\}$. In altre parole, ogni letterale è definito come:

$$l_j^{(i)} \in \{x_1, \overline{x_1}, x_2, \overline{x_2}, \ldots, x_n, \overline{x_n}\}$$

Questa struttura garantisce che la formula ϕ sia una congiunzione di clausole, dove ogni clausola è una disgiunzione di letterali, e ogni letterale è una variabile booleana o la sua negazione.

Una formula `CNF` è quindi una funzione di n variabili booleane che restituisce un valore booleano. Un assegnamento a di valori di verità alle variabili della formula è una funzione $a : \{a_1, \ldots, a_n\} \to \{0, 1\}$ che assegna un valore di verità a ciascuna variabile della formula. Un assegnamento a è detto **soddisfacente** per la formula ϕ se e solo se $\phi(a_1, a_2, \ldots, a_n) = \texttt{true}$.

Esempio

Consideriamo la seguente formula booleana in forma normale congiuntiva:

$$\phi(x_1, x_2, x_3, x_4) = (x_1 \vee x_2 \vee x_3 \vee \overline{x_4}) \wedge (\overline{x_1} \vee \overline{x_2}) \wedge (x_1 \vee x_2 \vee x_3 \vee \overline{x_4})$$

Un assegnamento $a : \{a_1, a_2, a_3, a_4\} \to \{0, 1\}$ può essere il seguente:

$$a = \{\texttt{true}, \texttt{false}, \texttt{true}, \texttt{true}\}$$

Risolvendo la formula con l'assegnamento a otteniamo:

$$\phi(a_1, a_2, a_3, a_4) = \texttt{true} \wedge \texttt{true} \wedge \texttt{true} = \texttt{true}$$

Quindi l'assegnamento a soddisfa la formula ϕ.

Riduzione di `SAT` a `k-col`

Prima di dimostrare che `SAT` è un problema `NP`-completo, dimostriamo che `SAT` si riduce a `k-col`. L'obiettivo è mostrare che problemi molto diversi, come il problema di decisione su grafi, hanno una codifica in un problema di tipo logico come `SAT`.

> Dato un grafo $\mathcal{G}$, istanza di `k-col`, possiamo costruire in tempo polinomiale una formula booleana $\phi_{\mathcal{G}}$ in forma normale congiuntiva tale che $\mathcal{G}$ è `k-col` se e solo se $\phi_{\mathcal{G}}$ è soddisfacibile.

La misura del grafo $\mathcal{G}$ è definita come il numero di archi e nodi del grafo.

$$|\mathcal{G} = (V, E)| = |V| + |E|$$

Per una formula $\phi_{\mathcal{G}}$ in forma normale congiuntiva, la misura è il numero di letterali.

Le variabili in $\phi_{\mathcal{G}}$ sono:

$$x_1^{v_1}, x_2^{v_1}, \ldots, x_k^{v_1}, x_1^{v_2}, x_2^{v_2}, \ldots, x_k^{v_2}, \ldots, x_1^{v_n}, x_2^{v_n}, \ldots, x_k^{v_n}$$

Ovvero sia, per ogni vertice $v \in V$ abbiamo k variabili $x_1^v, x_2^v, \ldots, x_k^v$.

Per ogni vertice $v \in V$ e per ogni colore $i \in \{1, \ldots, k\}$, definiamo la seguente clausola:

$$C^{(v)} = x_1^v \vee x_2^v \vee \cdots \vee x_k^v$$

Ovvero, l'OR di tutte le variabili associate al vertice v, per ogni colore i, codificando il fatto che ad ogni vertice deve essere associato un colore. Con questa prospettiva almeno una delle variabili $x_1^v, x_2^v, \ldots, x_k^v$ deve essere vera, e quindi almeno un colore deve essere associato al vertice v. Non basta però dire che un colore deve essere associato ad ogni vertice, ma bisogna anche garantire che un vertice non possa avere due colori diversi. Per fare ciò, uno una nuova clausola associata al vertice, ovvero su tutte le coppie possibili di colori distinti, non vogliamo che al vertice v siano associati entrambi i colori.

$$D^{(v)} = \bigwedge_{1 \leq i < j \leq k} (\overline{x_i^v} \vee \overline{x_j^v})$$

Se fosse vero, per esempio, che x_1^v e x_2^v sono entrambi veri, allora la clausola $D^{(v)}$ sarebbe falsa, e quindi la formula $\phi_{\mathcal{G}}$ sarebbe falsa. Questo garantisce che ad ogni vertice sia associato un solo colore.

Questo non garantisce una colorazione propria, ovvero che vertici adiacenti abbiano colori diversi. Per fare ciò, per ogni arco $e = (u, v) \in E$, aggiungiamo la seguente clausola:

$$E^{(e)} = \bigwedge_{1 \leq i \leq k} (\overline{x_i^u} \vee \overline{x_i^v})$$

Se fosse vero che x_i^u e x_i^v sono entrambi veri, allora la clausola $E^{(e)}$ sarebbe falsa, e quindi la formula $\phi_{\mathcal{G}}$ sarebbe falsa. Questo garantisce che vertici adiacenti abbiano colori diversi.

Definiamo ora la formula $\phi_{\mathcal{G}}$ come:

$$\phi_{\mathcal{G}} = \bigwedge_{v \in V} \left(C^{(v)} \wedge D^{(v)} \right) \wedge \bigwedge_{e \in E} E^{(e)} \tag{2.1}$$

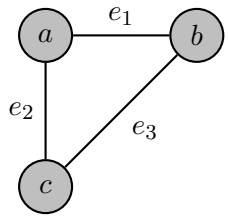
La dimensione della formula è:

$$|\phi_{\mathcal{G}}| = |V| \cdot \left(k + \left(\frac{k}{2} \right) \cdot 2 \right) + |E| \cdot k \cdot 2 = O(|V| \cdot k + |E| \cdot k) = O(k \cdot (|V| + |E|))$$

Quindi polinomiale nella taglia del grafo.

Esempio

Consideriamo il seguente grafo $\mathcal{G}$ e una 2-col:



$$V = \{a, b, c\}$$
$$E = \{(a, b), (a, c), (b, c)\}$$

Quindi definiamo le clausole:

$$C^{(a)} = x_1^a \vee x_2^a \qquad D^{(a)} = (\overline{x_1^a} \vee \overline{x_2^a})$$
$$C^{(b)} = x_1^b \vee x_2^b \qquad D^{(b)} = (\overline{x_1^b} \vee \overline{x_2^b})$$
$$C^{(c)} = x_1^c \vee x_2^c \qquad D^{(c)} = (\overline{x_1^c} \vee \overline{x_2^c})$$
$$E^{(e_1)} = (\overline{x_1^a} \vee \overline{x_1^b}) \wedge (\overline{x_2^a} \vee \overline{x_2^b})$$
$$E^{(e_2)} = (\overline{x_1^a} \vee \overline{x_1^c}) \wedge (\overline{x_2^a} \vee \overline{x_2^c})$$
$$E^{(e_3)} = (\overline{x_1^b} \vee \overline{x_1^c}) \wedge (\overline{x_2^b} \vee \overline{x_2^c})$$

Quindi la formula $\phi_{\mathcal{G}}$ è:

$$\phi_{\mathcal{G}} = C^{(a)} \wedge D^{(a)} \wedge C^{(b)} \wedge D^{(b)} \wedge C^{(c)} \wedge D^{(c)} \wedge E^{(e_1)} \wedge E^{(e_2)} \wedge E^{(e_3)}$$

Dimostriamo che k-col si riduce polinomialmente a SAT.

Teorema 2.3.1 $\texttt{k-col} \leq_p \texttt{SAT}$

Dimostrazione. Dimostriamo entrambi i versi dell'implicazione.

($\Rightarrow$)

Dimostriamo prima che se $\mathcal{G}$ è k-colorabile, allora $\phi_{\mathcal{G}}$ è soddisfacibile.

Sia $\{c(v) \mid v \in V\}$ una colorazione propria di $\mathcal{G}$, ossia, per ogni arco $e = (u, v) \in E$, vale che $c(u) \neq c(v)$ e $c(v) \in \{1, \ldots, k\}$. Definiamo l'assegnamento $a_j^{v_i}$ come segue:

$$a_j^{v_i} = \begin{cases} \texttt{true} & \text{se } c(v_i) = j, \\ \texttt{false} & \text{altrimenti.} \end{cases}$$

Dimostriamo ora che questo assegnamento soddisfa tutte le clausole di $\phi_{\mathcal{G}}$.

1. Per la clausola $C^{(v)}$, che assicura che ogni vertice v riceva almeno un colore:

$$\exists c(v_i) = j \implies a_j^{v_i} = \texttt{true}$$
$$\implies C^{(v)}(a) = \texttt{true}.$$

2. Per la clausola $D^{(v)}$, che previene che un vertice v abbia più di un colore:

$$\forall i \neq j,\, a_i^v = \texttt{false} \vee a_j^v = \texttt{false} \implies D^{(v)}(a) = \texttt{true}.$$

3. Per la clausola $E^{(e)}$, che assicura che due vertici adiacenti u e v non abbiano lo stesso colore:

$$\begin{aligned} c(u) \neq c(v) &\implies \forall i,\, a_i^u = \texttt{false} \vee a_i^v = \texttt{false} \\ &\implies E^{(e)}(a) = \texttt{true}. \end{aligned}$$

Questo dimostra che se $\mathcal{G}$ è k-colorabile, allora esiste un assegnamento di verità che soddisfa $\phi_{\mathcal{G}}$, ovvero la formula $\phi_{\mathcal{G}}$ è soddisfacibile.

($\Leftarrow$)

Ora dimostriamo che se $\phi_{\mathcal{G}}$ è soddisfacibile, allora $\mathcal{G}$ è k-colorabile.

Assumiamo che esista un assegnamento di verità a che soddisfa $\phi_{\mathcal{G}}$ e mostriamo che $\mathcal{G}$ è k-colorabile. Questa parte di dimostrazione serve ad evitare che la formula $\phi_{\mathcal{G}}$ possa essere soddisfatta da un assegnamento che non rappresenti una colorazione propria di $\mathcal{G}$.

Esiste l'assegnamento $a = (a_1^{v_1}, \ldots, a_k^{v_1}, \ldots, a_1^{v_n}, \ldots, a_k^{v_n})$ tale che $\phi_{\mathcal{G}}(a) = \texttt{true}$. Mostriamo che da questo assegnamento possiamo costruire una colorazione propria di $\mathcal{G}$. Per farlo, definiamo una colorazione per $\mathcal{G}$ basata su a come segue:

$$\forall v \in V, \quad c(v) = i \iff a_i^v = \texttt{true}.$$

1. Ogni vertice v è colorato con un solo colore. Possiamo esprimere questa condizione come segue:

$$\begin{aligned} \phi(a) = \texttt{true} &\implies C^{(v)}(a) = \texttt{true} \\ &\implies \exists i \in \{1, \ldots, k\} \text{ tale che } a_i^v = \texttt{vero} \\ &\implies c(v) = i. \end{aligned}$$

2. Ogni vertice v è colorato con un solo colore. Possiamo esprimere questa condizione come segue:

$$\begin{aligned} \phi(a) = \texttt{true} &\implies D^{(v)}(a) = \texttt{true} \\ &\implies \nexists i, j \in \{1, \ldots, k\} \text{ tali che } a_i^v = a_j^v = \texttt{true} \\ &\implies \exists i \in \{1, \ldots, k\} \text{ tale che } c(v) = i. \end{aligned}$$

perché se esistessero due colori i, j tali che $a_i^v = a_j^v = \texttt{true}$, allora $C^{(v)}(a) = \texttt{false}$, che è assurdo.

3. Dimostriamo che la colorazione è propria, ossia che ogni arco non è monocromatico, ossia che per ogni arco $e = (u, v) \in E$, $c(u) \neq c(v)$. Possiamo esprimere questa condizione come segue:

$$\begin{aligned} \phi(a) = \texttt{true} &\implies E^{(e)}(a) = \texttt{true} \\ &\implies \nexists i \in \{1, \ldots, k\} \text{ tale che } a_i^u = a_i^v = \texttt{true} \\ &\implies \nexists i \in \{1, \ldots, k\} \text{ tale che } c(u) = c(v) \\ &\implies c(u) \neq c(v). \end{aligned}$$

Questo dimostra che se $\phi_{\mathcal{G}}$ è soddisfacibile, allora $\mathcal{G}$ è k-colorabile.

Abbiamo dimostrato che $\mathcal{G}$ è k-colorabile se e solo se $\phi_{\mathcal{G}}$ è soddisfacibile. □

Questo teorema dimostra che la difficoltà di risolvere il problema della colorazione di un grafo è equivalente alla difficoltà di risolvere il problema della soddisfacibilità di una formula booleana.

2.3.2 Circuit-SAT

Il problema Circuit-SAT è un problema di soddisfacibilità di una formula booleana particolare, in cui la formula è rappresentata da un circuito logico. Un circuito logico è una rappresentazione di una formula booleana in cui le porte logiche sono connesse tra loro da cavi. Ogni porta logica è rappresentata da un nodo del circuito, mentre i cavi sono rappresentati dagli archi del circuito.

L'input del problema Circuit-SAT è un circuito logico $\mathcal{C}$ e l'output è yes se e solo se il circuito $\mathcal{C}$ è soddisfacibile.

Si tratta di un grafo aciclico diretto (DAG) in cui i nodi interni sono porte logiche e i nodi di input sono costituiti da variabili booleane.

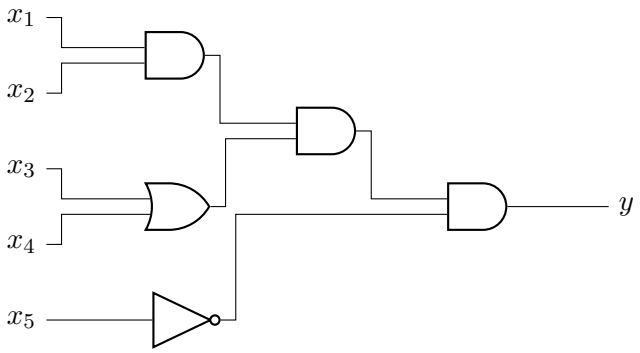


Figura 2.3.1: Esempio di circuito logico

Ogni vertice del circuito logico ha associato l'operatore booleano AND, OR o NOT. In particolare l'operatore NOT è associato a nodi con *in-degree* 1, mentre gli operatori AND e OR sono associati

a nodi con *in-degree* 2. I vertici con *in-degree* 0 sono detti *input*, mentre i vertici con *out-degree* 0 sono detti *output*.

Dato un assegnamento booleano a delle variabili di input, possiamo valutare il circuito logico $\mathcal{C}$ assegnando ad ogni nodo il valore booleano corrispondente all'operatore associato al nodo e ai valori booleani dei nodi di input. In questo modo possiamo valutare il circuito logico come una formula booleana.

2.3.3 NP-completezza di SAT

Teorema 2.3.2 di Cook-Levin Il problema SAT è NP-completo.

Per dimostrare il seguente teorema utilizziamo il seguente lemma.

Lemma 2.3.1 *Per ogni problema in $\mathbb{B} \in P$ e per ogni $n \in \mathbb{N}$, esiste un circuito booleano $\mathcal{C}_n$ tale che per ogni $x \in \mathcal{I}(\mathbb{B})$ tale che $|x| = n$, $\mathbb{B}(x) = 1$ se e solo se $\mathcal{C}_n(x) = 1$, ovvero*

$$\mathcal{C}_n(x) = \mathbb{B}(x)$$

Inoltre $\mathcal{C}_n$ ha dimensione polinomiale rispetto a n.

Dimostrazione. Per dimostrare che SAT è NP-completo, dobbiamo dimostrare che

1. SAT è in NP.

   Sappiamo che SAT è in NP in quanto possiamo verificare in tempo polinomiale una soluzione proposta per il problema.

2. Circuit-SAT è NP-completo.

   Dimostrare che Circuit-SAT è NP-completo equivale a dimostrare che Circuit-SAT appartiene a NP e per ogni problema in NP esiste una riduzione polinomiale da esso a Circuit-SAT.

   - Dimostriamo che Circuit-SAT appartiene a NP. Dato un circuito logico $\mathcal{C}$ e un assegnamento booleano a delle variabili di input, possiamo valutare il circuito logico $\mathcal{C}$ assegnando ad ogni nodo il valore booleano corrispondente all'operatore associato al nodo e ai valori booleani dei nodi di input. In questo modo possiamo valutare il circuito logico come una formula booleana. Se la formula booleana è soddisfacibile, allora il circuito logico $\mathcal{C}$ è soddisfacibile.

   - Sfruttiamo il lemma 2.3.1 per dimostrare che Circuit-SAT è NP-completo.

     Per ogni problema $\mathbb{A}$ appartenente alla classe NP, possiamo affermare che $\mathbb{A}$ è riducibile a Circuit-SAT. Questa riduzione comporta la definizione di una trasformazione che, fissato un input x appartenente all'insieme delle istanze $\mathcal{I}(\mathbb{A})$ di $\mathbb{A}$, genera un circuito booleano $\mathcal{C}_x^{\mathbb{A}}$ tale che $\mathbb{A}(x) = 1$ se e solo se $\mathcal{C}_x^{\mathbb{A}}$ è soddisfacibile.

     Essendo $\mathbb{A}$ un problema in NP, esiste un verificatore polinomiale $B(x, y)$ che determina se y è una soluzione corretta per l'input x fissato, per ogni x in $\mathcal{I}(\mathbb{A})$. In altre parole:

$$\mathbb{A}(x) = \texttt{yes} \iff \exists y \in \{0,1\}^{|x|^c} : B(x,y) = \texttt{yes}$$

dove y è una stringa di lunghezza polinomiale in $|x|$ e c è una costante.

Il calcolo di $B(x,y)$ appartiene alla classe P, il che implica che, fissato l'input x, esiste un circuito booleano $\mathcal{C}_x^{\mathbb{A}}$ di dimensione polinomiale che, per ogni assegnazione di y di lunghezza n, soddisfa la relazione $\mathcal{C}_x^{\mathbb{A}}(y) = B(x,y)$.

Quindi, $\mathcal{C}_x^{\mathbb{A}}$ rappresenta un circuito booleano che può essere costruito in tempo polinomiale e che codifica il problema $\mathbb{A}$ per un'istanza specifica x fissata.

$$x \in \mathcal{I}(\mathbb{A}) \qquad \mathbb{A}(x) = 1 \iff \exists y \quad t.c. \quad B(x,y) = 1 \iff \exists y \quad t.c. \quad \mathcal{C}_x^{\mathbb{A}}(y) = 1$$

Abbiamo così dimostrato che, per ogni problema in NP, esiste una riduzione polinomiale a Circuit-SAT, con l'input x fissato durante la trasformazione.

3. Circuit-SAT $\leq_p$ SAT.

   Dato il seguente circuito booleano $\mathcal{C}$:

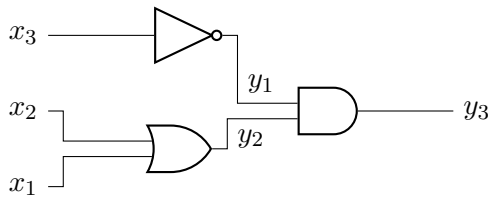


Figura 2.3.2: Circuito booleano $\mathcal{C}$

Vogliamo trasformare il circuito booleano $\mathcal{C}$ in una formula booleana ϕ in forma normale congiuntiva, in una riduzione polinomiale tale che:

$$\mathcal{C}(x) = 1 \iff \exists x' \quad t.c. \quad \phi(x') = 1$$

Per farlo prendiamo tutti gli output del circuito e gli assegnamo una variabile, in questo caso y_i con $i \in \{1,2,3\}$ e le fissiamo rispetto alle variabili di input. In questo caso abbiamo che:

$$y_1 = \overline{x_3} \quad y_2 = x_1 \vee x_2 \quad y_3 = y_1 \wedge y_2$$

Non sono quindi libere nella formula ϕ le variabili y_i ma sono fissate rispetto alle variabili di input. Inoltre y_3 è dovrà essere a 1 per far si che il circuito sia soddisfacibile.

La formula ϕ sarà quindi:

$$\phi(x_1,x_2,x_3,y_1,y_2,y_3) = \big[(x_1 \vee x_2) = y_1\big] \wedge \big[\overline{x_3} = y_2\big] \wedge \big[y_1 \wedge y_2 = y_3\big] \wedge y_3$$

Quindi abbiamo che:

$$\exists x \quad t.c. \quad \mathcal{C}(x) = 1 \iff \exists x, y \quad t.c. \quad \phi(x, y) = 1$$

Per trasformare la formula ϕ in una formula in forma normale congiuntiva possiamo utilizzare le equivalenze logiche.

Passiamo quindi da un circuito che ha un numero di input n ad una formula che ha un numero di variabili polinomiale in n, da qui otteniamo una formula in forma normale congiuntiva (*applicando le equivalenze logiche*) che ha un numero di clausole polinomiale in n che è soddisfacibile se e solo se il circuito è soddisfacibile.

Sappiamo che per ogni $\mathbb{A} \in$ NP, $\mathbb{A} \leq_p$ Circuit-SAT $\leq_p$ SAT, quindi abbiamo SAT $\in$ NP − *completo.* □

2.3.4 Formule K-CNF

Una formula K-CNF è una formula in forma normale congiuntiva dove ogni clausola ha al più k letterali.

Per esempio la formula:

$$\phi = (x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_4) \wedge (\overline{x_1} \vee x_2 \vee x_3 \vee x_4 \vee x_5)$$

è una formula 5-CNF.

Teorema 2.3.3 3-SAT è NP-completo.

Dimostrazione. Per dimostrare che 3-SAT è NP-completo dobbiamo dimostrare che:

1. 3-SAT è in NP.
2. 3-SAT è NP-hard.

Banalmente, 3-SAT è in NP in quanto possiamo verificare in tempo polinomiale se un'assegnazione di valori alle variabili soddisfa la formula.

Dimostriamo ora che 3-SAT è NP-hard dimostrando che SAT si riduce in tempo polinomiale a 3-SAT. Questo possiamo farlo, in quanto conosciamo che SAT è NP-completo e quindi possiamo ridurre SAT a 3-SAT. Per farlo, sfruttiamo una trasformazione clausola per clausola, trasformando una clausola con k letterali in una serie di clausole in 3-CNF che possono essere soddisfatte se e solo se la clausola originale è soddisfacibile. Questa trasformazione garantisce che la formula risultante sia in 3-CNF e abbia una lunghezza polinomiale rispetto alla formula originale.

Supponiamo che C sia una clausola:

$$C = (l_1 \vee l_2 \vee l_3 \vee \ldots \vee l_k)$$

dove $k > 3$ e l_i sono letterali che possono essere variabili booleane o le loro negazioni. Possiamo trasformare C in una formula in forma normale congiuntiva a tre termini (3-CNF) introducendo

una serie di variabili ausiliarie z_i. La trasformazione procede come segue:

$$C' = (l_1 \vee l_2 \vee z_1) \wedge (\overline{z_1} \vee l_3 \vee z_2) \wedge \ldots \wedge (\overline{z_{k-3}} \vee l_{k-1} \vee l_k)$$

In questa trasformazione, ogni nuova clausola contiene esattamente tre letterali, aderendo alla definizione di 3-CNF. La formula risultante C' consiste di $k-2$ clausole, poiché per ogni letterale in C oltre ai primi tre, inseriamo una nuova clausola che utilizza una variabile ausiliaria introdotta. Ciò mantiene la struttura richiesta per una formula 3-CNF, assicurando che ogni clausola abbia al massimo tre letterali.

La trasformazione aggiunge un totale di $k-3$ variabili ausiliarie, poiché ogni nuova variabile ausiliaria z_i è utilizzata per collegare le clausole tra loro in modo che la formula complessiva sia equivalente alla clausola originale C in termini di soddisfacibilità.

Perciò, la taglia della formula risultante è polinomiale rispetto alla taglia della formula originale, e la trasformazione può essere eseguita in tempo polinomiale.

Mostriamo ora che se C è soddisfacibile, allora C' è soddisfacibile. Supponiamo che esista un assegnamento di valori alle variabili che soddisfa C. Dato che almeno uno dei letterali in C è vero, possiamo assegnare valori alle variabili ausiliarie in modo da garantire che ogni clausola in C' sia soddisfatta. Ad esempio, se l_1 è vero, allora la prima clausola di C' è soddisfatta. Possiamo poi assegnare a ciascuna variabile ausiliaria z_i un valore che assicuri la soddisfazione delle clausole successive, tenendo conto che ogni clausola contiene o una variabile ausiliaria o la sua negazione insieme a letterali di C. Pertanto, se C è soddisfacibile, possiamo costruire un assegnamento che soddisfa anche C'.

Mostriamo che se C' è soddisfacibile, allora C è soddisfacibile. Supponiamo che esista un assegnamento di valori alle variabili che soddisfa C'. Dato che C' è soddisfacibile, almeno uno dei letterali in ogni clausola di C' deve essere vero.

Quindi esiste un assegnamento a_x e a_z tale che a_x e a_z soddisfano C'. Supponiamo per assurdo che a_x non soddisfi C. Quindi tutti i letterali l_i in C' sono falsi.

Avendo una clausola del tipo:

$$C' = (\texttt{false} \vee \texttt{false} \vee z_1) \wedge (\overline{z_1} \vee \texttt{false} \vee z_2) \wedge \ldots \wedge (\overline{z_{k-3}} \vee \texttt{false} \vee \texttt{false})$$

La clausola non può essere soddisfatta, in quanto per soddisfare la prima sottoclausola, z_1 deve essere vero, ma per soddisfare la seconda sottoclausola, z_2 deve essere vero e così via. Ma per soddisfare l'ultima sottoclausola, z_{k-3} deve essere falso, il che è una contraddizione, poiché z_{k-3} deve essere vero per soddisfare la penultima sottoclausola. Quindi a_x deve soddisfare C per soddisfare C'.

Consideriamo il caso in cui $k < 3$.

Data una formula in forma normale congiuntiva con clausole minori o uguali a tre letterali ϕ, possiamo trasformarla in una formula in forma normale congiuntiva φ con clausole esattamente di tre letterali tale che ϕ sia soddisfacibile se e solo se φ è soddisfacibile.

Supponiamo che ϕ contenga una clausola C con k letterali, dove $k < 3$ e dimostriamo che C è soddisfacibile se e solo se C' è soddisfacibile.

Supponiamo che C sia una clausola con un solo letterale:

$$C = (l_1)$$

La trasformazione procede come segue:

$$C' = (l_1 \vee z_1 \vee z_2) \wedge (l_1 \vee \overline{z_1} \vee z_2) \wedge (l_1 \vee z_1 \vee \overline{z_2}) \wedge (l_1 \vee \overline{z_1} \vee \overline{z_2})$$

In questa trasformazione, ogni nuova clausola contiene esattamente tre letterali, aderendo alla definizione di `3-CNF`. Se l_1 è vero, allora tutte le clausole in C' sono soddisfatte. Se l_1 è falso, allora almeno una delle clausole in C' non è soddisfatta, garantendo che C' sia soddisfacibile se e solo se C è soddisfacibile.

Supponiamo ora che C contenga due letterali:

$$C = (l_1 \vee l_2)$$

La trasformazione procede come segue:

$$C' = (l_1 \vee l_2 \vee z_1) \wedge (l_1 \vee l_2 \vee \overline{z_1})$$

Se la formula originale è soddisfacibile, allora o l_1 o l_2 è vero, e quindi la clausola C' è soddisfatta. Se C non è soddisfacibile, allora l_1 e l_2 sono entrambi falsi, e quindi C' non è soddisfacibile, poiché non esiste alcun valore di verità per z_1 che possa rendere soddisfatta la clausola.

Dimostriamo ora che se C' è soddisfacibile, allora C è soddisfacibile. Se C' è soddisfacibile, allora esiste un assegnamento a_x e a_z tale che a_x e a_z soddisfano C'. Supponiamo per assurdo che a_x non soddisfi C.

Quindi nel caso in cui C contenga un solo letterale, avrei:

$$C' = (\texttt{false} \vee z_1 \vee z_2) \wedge (\texttt{false} \vee \overline{z_1} \vee z_2) \wedge (\texttt{false} \vee z_1 \vee \overline{z_2}) \wedge (\texttt{false} \vee \overline{z_1} \vee \overline{z_2})$$

Disponendo di tutte le configurazioni possibili, non esiste un assegnamento che possa soddisfare C', poiché almeno uno dei letterali deve essere vero per soddisfare la clausola. Quindi a_x deve soddisfare C per soddisfare C'. Il ragionamento può essere esteso a tutte le clausole con due letterali di ϕ, dimostrando che se C' è soddisfacibile, allora C è soddisfacibile. Quindi abbiamo dimostrato che se C' è soddisfacibile, allora C è soddisfacibile.

Nel caso in cui la clausola contenga tre letterali, allora C è già in forma normale congiuntiva, e quindi C è soddisfacibile se e solo se C' è soddisfacibile.

Perciò abbiamo dimostrato che `3-SAT` è `NP`-completo. □

2.3.5 NP-completezza di NAE-K-SAT

Introduciamo ora il problema `NAE-K-SAT` (*Not-All-Equal K-SAT*). L'istanza di un problema `NAE-K-SAT` è una formula in forma normale congiuntiva e l'output è `yes` se e solo se esiste un assegnamento di valori alle variabili che soddisfa la formula e in cui ogni clausola contiene almeno un letterale vero e almeno un letterale falso.

Esiste quindi un assegnamento a tale che per ogni clausola C della formula, l'assegnamento a pone almeno un letterale di C a `true` e almeno un letterale di C a `false`.

Esempio

Supponiamo di avere la seguente formula in forma normale congiuntiva:

$$\phi(x_1, x_2, x_3) = (x_1 \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3)$$

Un assegnamento del tipo $a = (x_1 = \texttt{true}, x_2 = \texttt{false}, x_3 = \texttt{true})$ non soddisfa la formula, in quanto la prima clausola è soddisfatta, ma la seconda clausola non è soddisfatta. Un assegnamento del tipo $a = (x_1 = \texttt{false}, x_2 = \texttt{false}, x_3 = \texttt{true})$ soddisfa la formula, in quanto entrambe le clausole sono soddisfatte.

Lemma 2.3.2 *Data una formula in forma normale congiuntiva ϕ, se $a = (a_1, \ldots, a_n)$ NAE soddisfa ϕ, allora anche l'assegnamento $a' = (\overline{a_1}, \ldots, \overline{a_n})$ NAE soddisfa ϕ.*

Dimostriamo ora che NAE-K-SAT è NP-completo, partendo dalla dimostrazione che NAE-3-SAT è in NP-completo.

Teorema 2.3.4 NAE-3-SAT è NP-completo.

Dimostrazione. Per dimostrare che NAE-3-SAT è NP-completo, dobbiamo mostrare che:

1. NAE-3-SAT è in NP.
2. NAE-3-SAT è NP-hard.

1. NAE-3-SAT è in NP: È possibile verificare in tempo polinomiale un dato assegnamento di verità per tutte le clausole, assicurando che ogni clausola abbia almeno un letterale vero e uno falso.

2. NAE-3-SAT è NP-hard: Dimostriamo che 3-SAT si riduce in tempo polinomiale a NAE-4-SAT, che a sua volta si riduce a NAE-3-SAT:

$$\texttt{3-SAT} \leq_p \texttt{NAE-4-SAT} \leq_p \texttt{NAE-3-SAT}$$

- **Riduzione da 3-SAT a NAE-4-SAT:** Per ogni clausola C in una formula 3-SAT, aggiungiamo una variabile ausiliaria z per formare la clausola $D = (C \vee z)$ nella formula NAE-4-SAT.

  La nuova formula NAE-4-SAT è soddisfacibile se e solo se la formula 3-SAT originale è soddisfacibile.

  ($\Rightarrow$) Se φ in 3-SAT è soddisfacibile con un assegnamento $a = (a_1, \ldots, a_n)$, allora l'assegnamento $b = (a_1, \ldots, a_n, \texttt{false})$ soddisfa ψ in NAE-4-SAT poiché l'aggiunta di $z = \texttt{false}$ non altera la soddisfacibilità di ogni clausola $D^{(i)}$.

  ($\Leftarrow$) Se ψ in NAE-4-SAT è soddisfacibile con un assegnamento $b = (b_1, \ldots, b_n, b_{n+1})$, possiamo ottenere un assegnamento per φ in 3-SAT ponendo $a = (b_1, \ldots, b_n)$. Se $b_{n+1} = \texttt{true}$, invertiamo ogni valore di $b_1, \ldots, b_n$ per soddisfare ϕ.

- **Riduzione da NAE-4-SAT a NAE-3-SAT:** L'obiettivo è mostrare che se una clausola ψ di NAE-4-SAT è soddisfacibile, allora esiste un assegnamento che soddisfa anche una clausola φ di NAE-3-SAT.

Supponiamo che la clausola ψ in `NAE-4-SAT` sia nella forma:

$$\psi = C^{(1)} \wedge C^{(2)} \wedge C^{(3)} \wedge C^{(4)}$$

dove $C^{(i)}$ è una clausola con al più quattro letterali

$$C^{(i)} = l_1^{(i)} \vee l_2^{(i)} \vee l_3^{(i)} \vee l_4^{(i)}$$

Vogliamo trasformare ψ in una formula ϕ in `NAE-3-SAT`. Per farlo spezziamo ogni clausola $C^{(i)}$ in due clausole $C_1^{(i)}$ e $C_2^{(i)}$:

$$C_1^{(i)} = l_1^{(i)} \vee l_2^{(i)} \vee z_i \qquad C_2^{(i)} = l_3^{(i)} \vee l_4^{(i)} \vee \overline{z_i}$$

La formula ϕ sarà quindi:

$$\varphi = \bigwedge_{i=1}^{m} (C_1^{(i)} \wedge C_2^{(i)})$$

Considerando la formula ψ:

$$\psi = (x_1 \vee x_2 \vee x_3 \vee \overline{x_4}) \wedge (x_1 \vee \overline{x_2} \vee \overline{x_3} \vee x_4)$$

Abbiamo che:

$$\varphi = (x_1 \vee x_2 \vee z_1) \wedge (x_3 \vee x_4 \vee \overline{z_1}) \wedge (\overline{x_1} \vee x_2 \vee z_2) \wedge (\overline{x_3} \vee x_4 \vee \overline{z_2})$$

($\Rightarrow$) Se ψ è soddisfacibile con un assegnamento $a = (a_1, \ldots, a_n)$, e tale assegnamento rende vera una delle due coppie di letterali in ogni clausola $C^{(i)}$, allora la z_i corrispondente è impostata a `false` e tale clausola sarà soddisfatta indipendentemente dall'assegnamento di z_i. L'impostazione di $\overline{z_i}$ a `true` garantisce che la seconda clausola sia soddisfatta. Quindi l'assegnamento $b = (a_1, \ldots, a_n, \texttt{false})$ soddisfa φ.

Se ψ è soddisfacibile con un assegnamento $a = (a_1, \ldots, a_n)$, e tale assegnamento rende vera entrambe le coppie di letterali in ogni clausola $C^{(i)}$, allora l'assegnamento $b = (a_1, \ldots, a_n, \texttt{true})$ soddisfa φ.

($\Leftarrow$) Supponiamo che esista un assegnamento $b = (b_1, \ldots, b_n, b_{n+1})$ che soddisfa φ. Per definizione di `NAE-3-SAT`, questo assegnamento soddisfa φ se e solo se in ogni clausola $C^{(i)}$ almeno un letterale è vero e almeno un letterale è falso.

Consideriamo due tipi di clausole in φ:

1. Clausole che includono la variabile aggiuntiva z o la sua negazione $\overline{z}$: Se $b_{n+1} = \texttt{true}$, allora $\overline{z}$ è falso, e viceversa. In queste clausole, l'assegnamento soddisfacente richiede che le altre variabili in $C^{(i)}$ (che fanno parte anche di ψ) debbano essere tali da non avere tutti i letterali dello stesso valore booleano, assicurando che ψ sia soddisfatta indipendentemente dal valore di b_{n+1}.

2. Clausole originali di ψ: Ogni clausola di ψ, che compare in φ senza z o $\overline{z}$, deve avere almeno un letterale vero e uno falso per soddisfare la condizione `NAE`. Quindi, l'assegnamento $a = (b_1, \ldots, b_n)$ deve soddisfare ψ, perché le clausole di ψ sono sottoclausole delle corrispondenti in φ.

Di conseguenza, se φ è soddisfacibile tramite b, allora ψ è soddisfacibile tramite $a = (b_1, \ldots, b_n)$, poiché ogni clausola in ψ è soddisfatta dall'assegnamento corrispondente di letterali in b escludendo b_{n+1}.

□

2.3.6 NP-completezza di 3-COL

Per dimostrare che 3-COL è NP-completo, dimostriamo che NAE-3-SAT si riduce in tempo polinomiale a 3-COL.

Teorema 2.3.5 3-COL è NP-completo.

Dimostrazione. Per dimostrare che 3-COL è NP-completo, dobbiamo mostrare che:

1. 3-COL è in NP.
2. 3-COL è NP-hard.

1. 3-COL è in NP: È possibile verificare in tempo polinomiale un dato assegnamento di colori per i vertici di un grafo, assicurando che vertici adiacenti abbiano colori diversi.

2. 3-COL è NP-hard: Dimostriamo che NAE-3-SAT si riduce in tempo polinomiale a 3-COL.

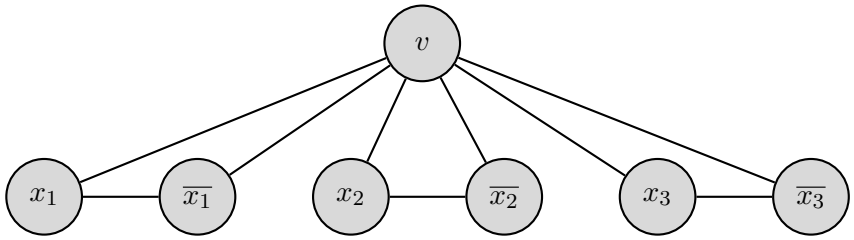
Per farlo trasformiamo una formula ϕ in NAE-3-SAT in un grafo $\mathcal{G}_\phi(V, E)$ in 3-COL. Consideriamo una formula ϕ in NAE-3-SAT con 3 variabili e m clausole.

$$\phi = C_1 \wedge C_2 \wedge \ldots \wedge C_m$$

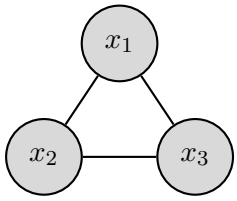
Ogni clausola C_i è nella forma:

$$C^{(i)} = (l_1^{(i)} \vee l_2^{(i)} \vee l_3^{(i)})$$

Costruiamo un grafo $\mathcal{G}_\phi(V, E)$ in 3-COL:

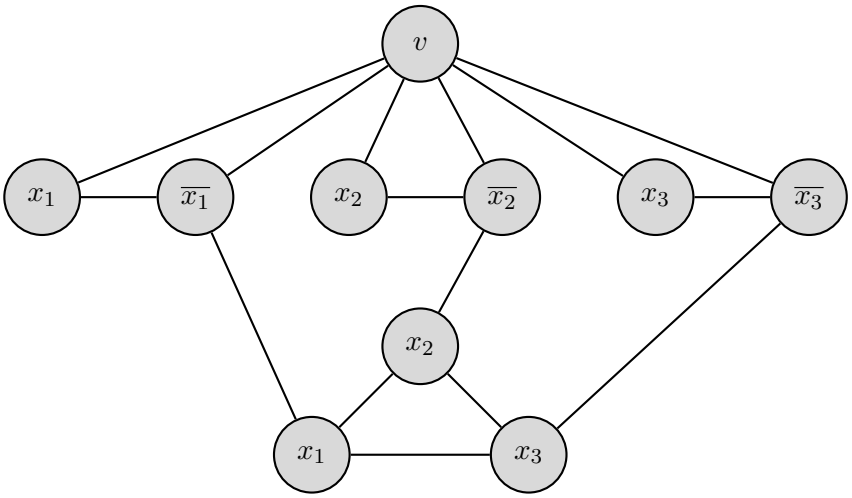


Due nodi adiacenti in $\mathcal{G}_\phi$ devono avere colori diversi, altrimenti la colorazione non sarebbe propria. Per ogni clausola $C^{(i)}$ in ϕ, aggiungiamo un triangolo in $\mathcal{G}_\phi$, dove ogni vertice è etichettato con un letterale di $C^{(i)}$.



A questo punto colleghiamo ogni vertice v del triangolo con il vertice $\overline{v}$ del grafo originale $\mathcal{G}_\phi$.

Supponendo che $C^{(i)} = (x_1 \vee \overline{x_2} \vee x_3)$, il risultato sarà:



Tale riduzione è polinomiale, poiché considerando una formula con $3m$ letterali, il grafo risultante avrà $3m + 2n + 1$ vertici e $6m + 3n$ archi, dove n è il numero di clausole e m è il numero di letterali.

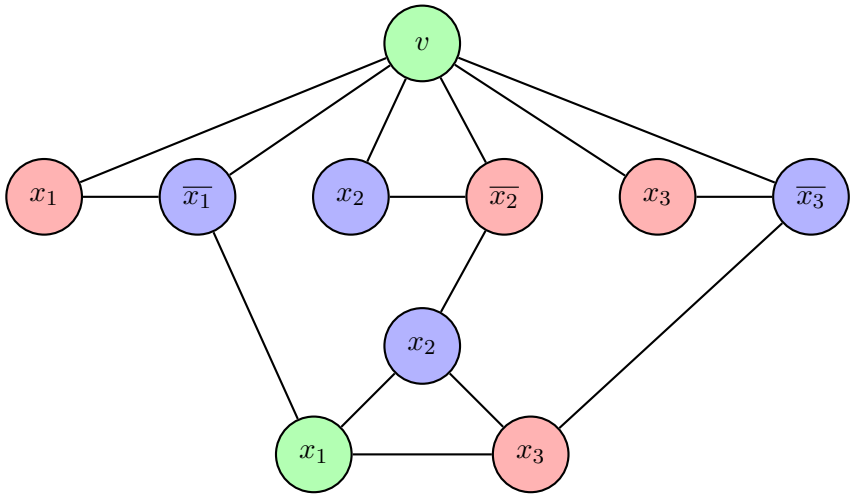
($\Rightarrow$) Se la formula ϕ in `NAE-3-SAT` è soddisfacibile, allora esiste un assegnamento $a_n \in \{true, false\}^n$ tale che per ogni i, $C^{(i)}(a_n)$ è soddisfatta. Esistono j, k tale che $l_j^{(i)}(a_n) =$ `true` e $l_k^{(i)}(a_n) =$ `false`. Assegneremo quindi la seguente colorazione al grafo $\mathcal{G}_\phi$:

$$C(w) = \begin{cases} \texttt{blu} & \text{se } w \text{ è etichettato con } l_i \text{ e } l_i(a_n) = \texttt{true} \\ \texttt{rosso} & \text{se } w \text{ è etichettato con } l_i \text{ e } l_i(a_n) = \texttt{false} \end{cases}$$

e fissiamo $C(v) =$ `verde`.

Poiché l'assegnamento era `NAE-3-SAT`, due di questi letterali di un triangolo avranno colori diversi. Mantengo la colorazione dei due vertici con colorazione opposta e modifico la colorazione del terzo vertice per garantire che non ci siano due vertici adiacenti con lo stesso colore.

Il risultato sarà il seguente:



($\Leftarrow$) Supponiamo ora che esista un assegnamento di colori che soddisfa $\mathcal{G}_\phi$ nel problema 3-COL. Questo significa che per ogni vertice nel grafo, incluso nel triangolo che rappresenta una clausola, i colori devono essere assegnati in modo che nessun vertice adiacente abbia lo stesso colore. In particolare, ciò implica che in ogni triangolo rappresentante una clausola $C^{(i)}$, i tre vertici (*che rappresentano i tre letterali della clausola*) devono avere almeno due colori diversi. Possiamo mappare questo assegnamento di colori indietro a un assegnamento di verità in NAE-3-SAT nel seguente modo:

- Assegniamo `true` ai letterali che sono colorati con il colore, diciamo, blu, e `false` ai letterali che sono colorati con il colore, diciamo, rosso.

Poiché in $\mathcal{G}_\phi$ ogni triangolo (*che rappresenta una clausola di* ϕ) ha vertici di almeno due colori diversi, nessuna clausola di ϕ sarà insoddisfatta. Questo perché la condizione di NAE-3-SAT richiede che in ogni clausola, non tutti i letterali siano uguali, e l'assegnamento derivato dall'assegnamento di colori garantisce esattamente questo. Dunque, ϕ è soddisfacibile in NAE-3-SAT.

□

2.3.7 Riduzione di Cook-Levin

Per dimostrare che 3-SAT è NP-completo, abbiamo mostrato che 3-SAT si riduce in tempo polinomiale a 4-SAT. Per farlo abbiamo trasformato ogni clausola C in una clausola $D = (C \vee z)$, dove z è una variabile ausiliaria. Abbiamo poi trasformato 4-SAT in 3-SAT.

$$(l_1 \vee l_2 \vee l_3 \vee l_4) \to (l_1 \vee l_2 \vee z) \wedge (\overline{z} \vee l_3 \vee l_4)$$

Abbiamo poi dimostrato che 3-SAT è NP-completo.

La stessa tecnica non ci darebbe informazioni utili per dimostrare che 2-SAT è NP-completo.

Teorema 2.3.6 2-SAT è in P.

Dimostrazione. Per procedere con la dimostrazione consideriamo il problema 2-SAT come un problema di ricerca, ovvero cerchiamo un assegnamento di verità che soddisfi la formula ϕ, mostrando quindi che esiste un algoritmo che in tempo polinomiale risolve il problema.

Data ϕ, costruiamo un grafo orientato $\mathcal{G}_\phi$ nel seguente modo:

- Per ogni letterale l_i possibile in ϕ, abbiamo un vertice in V.
- Per ogni clausola C in ϕ, aggiungiamo una coppia di archi $(\overline{l_i}, l_j)$ e $(\overline{l_j}, l_i)$.

Quello che osserviamo è che:

- Se abbiamo il cammino $x_1 \to x_2 \to x_3, \ldots, x_k \to y$ in $\mathcal{G}_\phi$, un assegnamento che soddisfa la formula ϕ e rende x vero, deve mettere a `true` tutti i vertici del cammino.
- Se in $\mathcal{G}_\phi$ esiste per una qualche variabile x un cammino $x \to \overline{x}$ allora nessun assegnamento che soddisfa la formula ϕ può rendere x vero.
- Se per qualche variabile x esistono in $\mathcal{G}_\phi$ sia il cammino $x \to \overline{x}$ che il cammino $\overline{x} \to x$, allora non esiste un assegnamento che soddisfa la formula ϕ.

Possiamo quindi utilizzare l'algoritmo di *componenti fortemente connesse* per verificare se esiste un assegnamento che soddisfa la formula ϕ.

Algorithm 3: 2SAT

Input: Una formula booleana ϕ rappresentata come un insieme di implicazioni in $\mathcal{G}_\phi$
Output: `true` se ϕ è soddisfacibile, `false` altrimenti

```
1 Costruisci il grafo di implicazione G_φ per φ
2 foreach variabile x in G_φ do
3     if x → x̄ e x̄ → x then
4         return false /* Esiste una contraddizione                    */
5 return true /* Nessuna contraddizione trovata, φ è soddisfacibile    */
```

Creare il grafo richiede tempo polinomiale, e l'algoritmo di componenti fortemente connesse ha complessità $O(V + E)$, dove n è il numero di vertici e m il numero di archi. Quindi 2-SAT è in P.

Mostriamo ora che se non troviamo un cammino $x \to \overline{x}$ o $\overline{x} \to x$ allora esiste un assegnamento che soddisfa la formula ϕ.

Algorithm 4: 2SAT

Input: Una formula booleana ϕ rappresentata come un insieme di implicazioni in $\mathcal{G}_\phi$
Output: Un assegnamento che soddisfa ϕ

```
1  Costruisci il grafo di implicazione G_φ per φ
2  foreach variabile x in G_φ non ancora assegnata do
3      if x → x̄ in G_φ then
4          a_x ← false
5          foreach percorso x̄ → y nel G_φ do
6              a_y ← true
7      else
8          a_x ← true
9          foreach percorso x → y nel G_φ do
10             a_y ← false
```

In termini computazionali l'algoritmo richiede tempo $O(2(2V + 2E) \cdot n)$, ovvero due BFS potenzialmente eseguiti su tutti i vertici del grafo, quindi è polinomiale. □

In termini di riduzione, quello che abbiamo dimostrato è che 2-SAT $\leq_T$ BFS, dove con il simbolo $\leq_T$ indichiamo una riduzione in tempo polinomiale di Cook-Turing.

$\mathbb{A} \leq_T \mathbb{B}$

Dati due problemi di decisione $\mathbb{A}$ e $\mathbb{B}$, diciamo che $\mathbb{A} \leq_T \mathbb{B}$ se esiste un algoritmo in tempo polinomiale per risolvere $\mathbb{A}$ che utilizza chiamate a un oracolo per risolvere $\mathbb{B}$.

Oracolo

Un oracolo è un'entità che può rispondere a domande in un solo passo di calcolo, $O(1)$.

Notiamo quindi che se un algoritmo risolve $\mathbb{B}$ in tempo polinomiale, allora risolverà anche $\mathbb{A}$ in tempo polinomiale.

Teorema 2.3.7 Se $\mathbb{A} \leq_T \mathbb{B}$ e $\mathbb{B} \in$ P, allora $\mathbb{A} \in$ P.

Ne consegue che:

Teorema 2.3.8 Se $\mathbb{A} \leq_T \mathbb{B}$ e $\mathbb{A} \notin$ P, allora $\mathbb{B} \notin$ P.

Inoltre abbiamo che:

Teorema 2.3.9 Se $\mathbb{A} \leq \mathbb{B} \implies \mathbb{A} \leq_T \mathbb{B}$.

Dimostrazione. Consideriamo x istanza del problema $\mathbb{A}$, la trasformiamo nell'istanza y, ovvero la riduzione applicata a x. Applichiamo l'algoritmo per $\mathbb{B}$ all'istanza y e otteniamo la risposta.

$$x \in \mathcal{I}(x) \implies y = R(x) \implies \mathbb{B}(R(x))$$

□

Si tratta di un caso particolare della riduzione di Cook-Turing, in cui si effettua un'unica chiamata al risolutore, ma non la si elabora.

2.4 Problemi co-NP

I problemi in co-NP sono i complementari dei problemi in NP. Un problema $\mathbb{A}$ è in co-NP se il complemento di $\mathbb{A}$ è in NP. In altre parole, un problema $\mathbb{A}$ è in co-NP se esiste un algoritmo in tempo polinomiale che verifica che una soluzione non appartiene a $\mathbb{A}$.

Se consideriamo un problema $\mathbb{A}$ appartenente a NP come un predicato A sulle istanze di $\mathbb{A}$, tale che $A(x) = \texttt{true}$ se e solo se $\mathbb{A}(x) = \texttt{yes}$, allora:

$$A(x) = \exists w \ t.c. \ B(x, y) = \texttt{true}$$

Dove il predicato B è un predicato in P.

Definiamo il predicato di un problema $\mathbb{A}$ in co-NP come:

$$\overline{A(x)} = \forall w \ t.c. \ B(x, y) = \texttt{false}$$

Problema co-NP

Data una classe di problemi di decisione $\mathcal{C}$, definiamo la classe co-NP come:

$$\texttt{co-NP} = \{\mathbb{A} \mid \overline{\mathbb{A}} \in \mathcal{C}\}$$

Dove $\mathcal{I}(\overline{\mathbb{A}}) = \mathcal{I}(\mathbb{A})$ e $\overline{\mathbb{A}(x)} = \texttt{yes} \iff \mathbb{A}(x) = \texttt{no}$.
Quindi:

$$\begin{aligned}\texttt{co-NP} &= \{\mathbb{A} \mid \overline{\mathbb{A}} \in \texttt{NP}\} \\ &= \{\mathbb{A} \mid \exists B(x, y) \text{ t.c. } \forall x, (\mathbb{A}(x) = \texttt{no}) \iff \exists w, B(x, w) = \texttt{no}\}\end{aligned}$$

Da questa definizione possiamo aggiungere che:

Teorema 2.4.1 $\mathbb{A} \leq \mathbb{B} \iff \overline{\mathbb{A}} \leq \overline{\mathbb{B}}$

2.4.1 Il problema small factor

Small factor è un problema che prende in input un intero n e un intero q e restituisce se esiste un fattore primo di n minore di q. Abbiamo osservato che il problema del *small factor* è in NP, in quanto possiamo verificare in tempo polinomiale se un dato fattore è primo e se è minore di q.

La taglia dell'input è il numero ci cifre di q e n, quindi $O(\log n + \log q)$, e non il valore numerico di n e q. Essenzialmente un algoritmo è polinomiale se usa un numero proporzionale al logaritmo dell'input.

Teorema 2.4.2 Il problema del *small factor* è in co-NP.

Dimostrazione. Consideriamo un'istanza del problema data da n e q, dove il compito è dimostrare che non esiste un fattore $r < q$ tale che $r \mid n$. Supponiamo di fare la fattorizzazione in numeri primi di n:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_i^{e_i}$$

dove $p_1 < p_2 < \ldots < p_i$. Se $p_1 \geq q$, allora non esiste un fattore primo minore di q, e quindi sappiamo che l'istanza non appartiene al problema, confermando che l'affermazione è falsa.

Per garantire che il certificato sia verificabile in tempo polinomiale, osserviamo che ogni p_i è rappresentabile con un numero di bit che è $O(\log n)$, il che implica che l'intero prodotto $p_1^{e_1} \cdot \ldots \cdot p_i^{e_i}$ sia anch'esso polinomiale rispetto alla taglia dell'input, ossia $O(\log n)$.

L'algoritmo quindi prende questo certificato e verifica:

1. che ogni p_i sia un fattore primo di n,
2. che la moltiplicazione $p_1^{e_1} \cdot \ldots \cdot p_i^{e_i}$ sia esattamente uguale a n.

Dopo aver confermato questi punti, verifica se $p_1 < q$. Se $p_1 \geq q$, allora n non ha fattori minori di q, e l'istanza è quindi nel complemento del problema "small factor".

Non possiamo affermare di più riguardo al problema del *small factor*, poiché è intrinsecamente legato alla difficoltà di fattorizzare numeri grandi, un problema alla base della sicurezza del crittosistema RSA. La fattorizzazione efficiente dei numeri interi, in particolare la scoperta di fattori piccoli, comprometterebbe direttamente la sicurezza di RSA.

Il problema del *small factor* non è sicuramente NP-completo, poiché è sia in NP che in co-NP, e non esiste un problema NP-completo in co-NP. □