Fondamenti Logico Matematici dell'Informatica

UniShare

Davide Cozzi
@dlcgold

Indice

Capitolo 1

Introduzione

Questi appunti sono presi a lezione. Per quanto sia stata fatta una revisione è altamente probabile (praticamente certo) che possano contenere errori, sia di stampa che di vero e proprio contenuto. Per eventuali proposte di correzione effettuare una pull request. Link: `https://github.com/dlcgold/Appunti`.

Capitolo 2

Dimostrazioni = Algoritmi

Parliamo in primis del **paradigma dimostrazioni = algoritmi**.
Prendiamo come *linguaggio di specifica* un **linguaggio del prim'ordine con identità**.

Si riportano alcune definizioni utili in *logica matematica* tratte da Wikipedia:

Definizione 1. *Definiamo **linguaggio del primo ordine** come un linguaggio formale che serve per gestire meccanicamente enunciati e ragionamenti che coinvolgono i connettivi logici, le relazioni e i quantificatori $\forall$ e $\exists$.*
Si ha che "del primo ordine" ndica che c'è un insieme di riferimento e i quantificatori possano riguardare solo gli elementi di tale insieme e non i sottoinsiemi (posso dire "per tutti gli elementi" ma non "per tutti i sottoinsiemi").
Tale linguaggio è caratterizzato da:

- *un **alfabeto di simboli** per variabili, costanti, predicati, funzioni, connettivi, quantificatori o punteggiatura*
- *un **insieme di termini** per denotare gli elementi dell'insieme in analisi*
- *un **insieme di formule ben formate (FBF)** ovvero un insieme di stringhe composte di simboli dell'alfabeto che vengono considerate sintatticamente corrette*

Definizione 2. *Definiamo **sistema assiomatico** come un insieme di assiomi che possono essere usati per dimostrare teoremi. Una teoria matematica consiste quindi in una assiomatica e tutti i teoremi che ne derivano.*

Definizione 3. *Definiamo un sistema formale come una formalizzazione rigorosa e completa della nozione di sistema assiomatico costituito da:*

- *un alfabeto*
- *una grammatica che specifica quali sequenze finite dei simboli dell'alfabeto corrispondono ad una FBF. La grammatica deve essere ricorsiva, nel senso che deve esistere un algoritmo per decidere se una sequenza di simboli è o meno una formula ben formata*
- *un sottoinsieme delle FBF che sono gli assiomi. L'insieme degli assiomi è ricorsivo*
- *le regole di inferenze che associano formule ben formate ad n-uple di formule ben formate*

Definizione 4. *Definiamo gli* ***assiomi di Peano*** *come un gruppo di assiomi ideati al fine di definire assiomaticamente l'insieme dei numeri naturali:*

- *esiste un numero naturale: 0 (alternativamente 1 se si vuole escludere 0):*
$$0/1 \in \mathbb{N}$$
- *ogni naturale ha un naturale come successore. Ho quindi una funzione "successore" tale che:*
$$S : \mathbb{N} \to \mathbb{N}$$
- *numeri diversi hanno successori diversi, ovvero:*
$$x \neq y \to S(x) \neq S(y)$$
- *0 (o alternativamente 1) non è il successore di alcun naturale, ovvero:*
$$S(x) \neq 0, \forall x \in \mathbb{N}$$
- *ogni sottoinsieme di numeri naturali che contenga lo zero e il successore di ogni proprio elemento coincide con l'intero insieme dei numeri naturali. Ovvero dato $U \subseteq \mathbb{N}$ tale che:*
  - $0 \in U$
  - $x \in U \to S(x) \in U$

allora:

$$U = \mathbb{N}$$

Tale assioma è detto ***assioma dell'induzione*** *o* ***principio di induzione***

Definizione 5. *In una teoria del primo ordine si chiama* ***chiusura universale*** *di una formula ben formata $A(x_1, \ldots, x_n)$, con $x_1, \ldots, x_n$ variabili libere, la formula:*

$$\forall x_1 \forall x_2 \forall x_n \; A(x_1, \ldots, x_n)$$

ottenuta premettendo un quantificatore universale su ogni variabile libera.

Definizione 6. *Definiamo, in logica matematica,* ***aritmetica di Peano (PA)*** *come una teoria del primo ordine che ha come assiomi propri una versione degli* ***assiomi di Peano*** *espressi nel linguaggio del primo ordine. Si ha quindi che il linguaggio di PA è il linguaggio dell'aritmetica del primo ordine con i seguenti simboli:*

- *vari simboli per le variabili: x, y, z, x_1 etc...*
- *costanti individuali: 0 etc...*
- *simboli per funzioni unarie: S*
- *simboli per funzioni binarie $+$, $\times$ ($+(x, y)$ si indica anche con $x + y$ e analogamente si fa per $\times$)*
- *simboli per relazioni unarie: $=$*
- *simboli per connettivi logici, quantificatori e parentesi*

Gli assiomi di PA sono costituiti da:

- *gli assiomi logici*
- *gli assiomi per l'uguaglianza*
- *i seguenti assiomi propri (che "traducono" nella logica di Peano gli assiomi di Peano):*
  - $\forall x \neg(S(x) = 0)$
  - $\forall x \forall y(S(x) = S(y) \rightarrow x = y)$
  - $\forall x(x + 0 = x)$

- $\forall x \forall y(x + S(y) = S(x + y))$
- $\forall x(x \times 0 = 0)$
- $\forall x \forall y(x \times S(y) = (x \times y) + x)$

Agli assiomi propri si aggiunge anche il seguente assioma proprio:

$$(\phi(0, x_1, \ldots, x_n) \wedge (\forall x(\phi(x, x_1, \ldots, x_n) \rightarrow \phi(S(x), x_1, \ldots, x_n)) \rightarrow \forall x \phi(x, x_1, \ldots, x_n)$$

per ogni FBF $\phi(x, x_1, \ldots, x_n)$ di cui $x, x_1, \ldots, x_n$ sono variabili libere. Questo è uno schema di assiomi detto ***schema di induzione*** *e si ha un assioma per ogni FBF ϕ*

Definizione 7. *Definiamo, in logica classica, il* ***principio del terzo escluso*** *che stabilisce che una proposizione e la sua negazione hanno valore opposto, non avendo una "terza opzione". In logica classica è una* ***tautologia****.*

Definizione 8. *Un termine è un* ***termine chiuso*** *sse non contiene delle variabili individuali.*

Definizione 9. *Una* ***formula chiusa*** *è una formula costruita nel linguaggio dei predicati in cui o non compaiono variabili o tutte le variabili presenti sono vincolate a un quantificatore e sono dunque variabili legate.*

Esempio 1. *Vediamo qualche esempio:*

$$\forall x, y \in \mathbb{N},\ \exists z \in \mathbb{N}\ t.c.\ mcd(x, y, z)$$

ovvero z è l'mcd di x e y.
Un altro esempio:

$$\forall x \in \mathbb{N},\ \exists y \in \mathbb{N}\ t.c.\ fatt(x, y)$$

ovvero y è il fattoriale di z.

Formule come quelle dell'esempio possono essere lette come **specifiche del problema di trovare un algoritmo totalmente corretto** che calcoli il risultato di tale problema per ogni input valido. Questa lettura non è implicita nella logica classica, dove non è richiesto di stabilire come viene prodotto il risultato. Si ha quindi a che fare con una lettura di un problema algoritmico di interesse per un informatico.
Le **dimostrazioni** di questa tipologia di formule, nell'ambito dell'**aritmetica di Peano (*PA*)**, sono quindi interpretabili come gli algoritmi che calcolano le funzioni specificate.
Come *vantaggi* di questa "atteggiamento" si ha che:

- l'attenzione si concentra su costruire la dimostrazione, sui passi dimostrativi, e non sulla stesura del codice
- i passi elementari della dimostrazione sono automatici
- la correttezza della dimostrazione è verificabile in modo automatico
- l'estrazione/sintesi dell'algoritmo dalla dimostrazione è diretta. Una volta che si ha la dimostrazione corretta si può estrarre direttamente l'algoritmo. Tale algoritmo è totalmente corretto rispetto alla specifica

La difficoltà si trasferisce dall'ambito convenzionale della programmazione e codifica dell'algoritmo in se alla costruzione dimostrazione e dei passi dimostrativi.
Si hanno quindi anche degli *svantaggi*, abbastanza problematici:

- l'algoritmo ottenuto non è ottimale rispetto al problema. Rispetto a questo bisognerebbe capire come incorporare "più semantica" del problema da risolvere nella dimostrazione stessa
- il formalismo e il linguaggio delle dimostrazioni sono "lontani" da quelli usati usualmente nella pratica informatica

Non tutte le dimostrazioni sono direttamente interpretabili come algoritmi. Per vedere questa cosa prendiamo un esempio famoso di formula da dimostrare in analisi.

Esempio 2 (esempio di Troelstra)**.** *Esistono due numeri irrazionali n e m tali che n^m è razionale. In termini di formula del primo ordine si ha quindi:*

$$\exists n, m \in \{\mathbb{R}/\mathbb{Q}\} \ t.c. \ n^m \in \mathbb{Q}$$

Cerchiamo di capire se:

$$\sqrt{2}^{\sqrt{2}} \in \mathbb{Q} \ o \ \sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$$

Vediamo quindi i due casi (sono solo due per il principio del terzo escluso):

1. *assumo $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ e pongo $n = m = \sqrt{2}$ avendo trovato due numeri irrazionali n e m tali per cui $n^m \in \mathbb{Q}$*

2. assumo $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ *e pongo* $n = \sqrt{2}^{\sqrt{2}}$ *e* $m = \sqrt{2}$*. Ne segue che:*

$$n^m = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^2 = 2 \in \mathbb{Q}$$

e quindi ho due numeri irrazionali n *e* m *tali per cui* $n^m \in \mathbb{Q}$

Non possiamo essere soddisfatti di questa dimostrazione. Non veniamo a conoscenza, tramite la dimostrazione, che $\sqrt{2}^{\sqrt{2}}$ *sia o meno razionale. Non possiamo capirlo in quanto assumo il terzo escluso e quindi non so quale dei due casi sia valido, non abbiamo un "esiste" costruttivo (*$\exists n, m \in \{\mathbb{R}/\mathbb{Q}\}$*) in quanto non sappiamo se* $\sqrt{2}^{\sqrt{2}}$ *è razionale o meno. Nonostante ciò al dimostrazione sta perfettamente "in piedi" ma non esibisce* n *e* m *in quanto non determina se* $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$*.*

Quanto successo nell'esempio di Troelstra non può succedere in un **sistema costruttivo**.

Definizione 10. *Definiamo* ***sistema costruttivo*** *un sistema dove si hanno come requisiti minimali:*

- $S \vdash A \vee B \rightarrow S \vdash A$ *oppure* $S \vdash B$ *quindi se nel sistema dimostro* $A \vee B$ *allora nel sistema dimostro* A *o dimostro* B*, con* A *e* B *formule chiuse. Questa è la* ***disjunction property (DP)***
- $S \vdash \exists x A(x) \rightarrow S \vdash A(t)$ *quindi se ho dimostrato un esistenziale allora deve esistere un termine chiuso* t *per cui dimostro* $A(t)$ *nel sistema. Questa è la* ***explicitly definibility property (EDP)****, detta anche* ***existence/witness property***

La logica classica quindi **non è un sistema costruttivo** perché in logica classica riesco sempre a dimostrare $A \vee \neg A$ mentre nell'esempio di Troelstra si nota come non si possa dimostrare né A né $\neg A$. Quindi da una dimostrazione classica di $A \vee \neg A$ io non tiro fuori una dimostrazione classica di A oppure una dimostrazione classica di $\neg A$ quindi non vale la DP. Inoltre non vale nemmeno la EDP, ho dimostrato l'esistenza di n e m (che sono termini chiusi) ma non ho trovato se vale la proprietà che siano irrazionali. La logica classica quindi non è una logica costruttiva.

2.1 Interpretazione BHK

Passiamo quindi ad una semantica informale che per ogni costante logica associa una condizione per la sua *costruibilità*. Questa è **l'interpretazione Brouwer-Heyting-Kreisel (*BHK*)**.

Definizione 11. *Presa una costruzione π per questa semantica proposizionale si ha che:*

- $\pi(A \wedge B) = \pi'(A)$ *e* $\pi''(B)$ *ovvero una costruzione di* $A \wedge B$ *e uguale ad un'altra costruzione di* A ***e*** *un'altra ancora di* B
- $\pi(A \vee B) = \pi'(A)$ *o* $\pi''(B)$ *ovvero una costruzione di* $A \vee B$ *e uguale ad un'altra costruzione di* A ***o*** *un'altra ancora di* B
- $\pi(A \to B)$ *è una funzione (o un funzionale, ovvero un insieme di funzioni)* f *che associa ad ogni costruzione* $\pi'(A)$ *una costruzione* $\pi''(B)$ *tale che* $\pi'' = f(\pi')$*. Quindi* f *associa costruzioni di* A *a costruzioni di* B
- $\pi(\neg A)$ *è una costruzione* π' *di* $A \to \bot$

Lato semantica predicativa si ha che, dato un dominio D per la variabile x:

- $\pi(\exists x A(x)) = \langle c, \pi' \rangle |\, c \in D$ *e* $\pi'(A(c))$ *quindi è uguale ad una coppia* $= \langle c, \pi' \rangle$ *tale che c appartiene al dominio e* π' *è una costruzione effettiva di* $A(c)$
- $\pi(\forall x A(x)) =$ *è una funzione* f *che associa ad ogni elemento* $c \in D$ *una costruzione* $\pi'(A(c))$ *tale che* $\pi' = f(c)$

Questa semantica "naive" ha alcune problematiche/aporie:

- la BHK non specifica la costruzione di una formula atomica
- la BHK non dimostra il falso infatti nella costruzione di $\neg$ associamo la costruzione del $\neg A$ a quella dell'implicazione, che è una costruzione che associa costruzioni di A e costruzioni di B e quindi nessuna costruzione potrebbe avere il falso (???)

Bisognerà quindi chiarire alcune restrizioni dell'interpretazione BHK.
Si hanno varie semantiche per il costruttivismo che hanno "precisato" la BHK:

- la semantica della**realizzabilità ricorsiva** di Kleene
- la semantica dell'**interpretazione dialettica** di Gödel
- la semantica delle **prove possibili** di Prawitz
- la semantica dei **problemi finiti** di Medvedev

Queste 4 semantiche sono coerenti con la BHK e quindi sono **semantiche del costruttivismo**.
Passiamo ora ad una definizione formale.

Definizione 12. *Definiamo come* ***sistema costruttivo*** *un sistema S:*

$$S = T + L$$

dove:

- *T è una teoria con assiomi di forma particolare*
- *L è una logica intuizionistica, che prendiamo come punto di partenza per il costruttivismo, con le sue estensioni*

Non sempre comunque date T e L si ha che S è un sistema costruttivo.

Un esempio di sistema costruttivo è dato dall'**aritmetica intuizionistica**, ovvero la PA interpretata all'interno della logica intuizionistica. Altri esempi sono le **teorie con assiomi di Harrop**, teorie con assiomi $\forall\exists$ con matrice positiva priva di quantificatori e con minimo modello di Herbrandt etc...
Le clausole di Horn usate i Prolog hanno un modello minimo di Herbrandt e hanno assiomi $\forall\exists$ con matrice positiva priva di quantificatori dove $\exists$ viene eliminato attraverso skolemizzazione e il $\forall$ è implicito nelle regole del programma in quanto tutte le X, Y etc... si intendono quantificati universalmente.
Quindi la parte assiomatica di una teoria non basta a rendere costruttivo il sistema anche se la logica è costruttiva. Tuttavia se si restringono le assiomatizzazioni con formule del primo ordine di tipo particolare si possono ottenere sistemi costruttivi in cui vale come minimo la *DP* e la *EDP*.

2.2 Deduzione naturale

Vediamo un accenno della **deduzione naturale** ovvero di un **calcolo diretto** (quindi differente dal calcolo indiretto dei tableaux). Nella deduzione naturale si ha per ogni connettivo una **regola di introduzione** i e una **regola di eliminazione** e. Ad esempio se ho A e B come premesse posso introdurre l'and con la regola d:i introduzione dell'and:

$$\frac{A \quad B}{A \wedge B} i\wedge$$

Se invece ho $A \wedge B$ come premessa posso usare la regola di eliminazione dell'and, producendo:

$$\frac{A \wedge B}{A} e\wedge \text{ oppure } \frac{A \wedge B}{B} e\wedge$$

Avendo quindi due regole di eliminazione per l'and.
Passiamo all'or. Ho due regole di introduzione:

$$\frac{A}{A \vee B} i\vee \text{ oppure } \frac{B}{A \vee B} i\vee$$

L'eliminazione della or è complessa e verrà trattata più avanti ma è della forma:

$$\frac{A \vee B \quad C \quad C}{C} e\vee$$

Dove si ha che se se ho $A \vee B$ come premessa e assumendo A ho C ma anche assumendo B ho C posso eliminare l'or e ottenere C.
Passiamo all'implicazione. Se ho come assunzione A e da B riesco a dimostrare B allora posso introdurre l'implicazione:

$$\frac{\overset{[A]}{\overset{\cdots}{B}}}{A \to B} i\to$$

Per l'eliminazione ho che, tramite **modus ponens**:

$$\frac{A \to B \quad A}{B} e\to$$

Abbiamo poi la **regola del falso** che dice che dal falso segue qualsiasi cosa:

$$\frac{\bot}{B}\bot$$

e la regola dell'eliminazione della negazione che dice che se assumo $\neg A$ e ottengo il falso significa che si è ottenuta una contraddizione e quindi elimino il $\neg$:

$$\frac{\overset{[\neg A]}{\bot}}{A} e\neg$$

Passiamo al $\forall$. Se ho dedotto $A(p)$ per p generico posso introdurre il $\forall$:

$$\frac{A(p)}{\forall x A(x)} i\forall$$

Se ho come assunzione $\forall x A(x)$ posso dedurre un qualsiasi $A(t)$:

$$\frac{\forall x A(x)}{A(t)} e\forall$$

Possiamo fare l'equivalente per l'$\exists$, dove se esiste $A(t)$ posso dedurre l'esistenza di un certo x per cui vale $A(x)$:

$$\frac{A(t)}{\exists x A(x)} i\exists$$

L'eliminazione dell'esiste è complessa e verrà trattata più avanti ma è della forma:

$$\frac{\exists x A(x) \qquad \overset{[A(p)]}{C}}{C} e\exists$$

Dove assumendo $\exists x A(x)$, assumendo $A(p)$ con p generico e riuscendo ad ottenere C da quest'ultima assunzione con una serie di restrizioni posso ottenere C eliminando $\exists$.
Una dimostrazione in deduzione naturale è modulare alle logiche si vogliono usare:

- nelle dimostrazioni in logica classica utilizzo tutte le regole della deduzione naturale appena introdotte
- nelle dimostrazioni in logica intuizionistica non devo usare la regola di eliminazione della negazione
- nelle dimostrazioni in logica minimale non devo usare la regola di eliminazione della negazione e nemmeno la regola che dal falso segue qualsiasi cosa

Possiamo quindi caratterizzare queste tre logiche e nelle ultime due, quella intuizionistica e quella minimale, si può dimostrare che valgono DP e EDP mentre non posso dire lo stesso per la logica classica. Si ha inoltre che:

$$\text{logica minimale} \subseteq \text{logica intuizionistica} \subseteq \text{logica classica}$$

Discorso diverso vale per le teorie, ovvero per i sistemi, dove l'assiomatizzazione può fare la differenza portando anche fuori dalla costruttività (se ad esempio assumo come assioma che $\forall x A(x) \vee \neg A(x)$ e gli aggiungo la logica intuizionistica ottengo la logica classica che non è costruttiva).
Una teoria specifica è l'aritmetica di Peano dove si hanno i seguenti assiomi:

- $\forall x \neg(S(x) = 0)$

- $\forall x \forall y(S(x) = S(y) \to x = y)$
- $\forall x(x + 0 = x)$
- $\forall x \forall y(x + S(y) = S(x + y))$
- $\forall x(x \times 0 = 0)$
- $\forall x \forall y(x \times S(y) = (x \times y) + x)$

Dove si ha la regola d'identità che in realtà sono due, ovvero $id1$ e $id2$:

$$\frac{}{x = x} id1 \text{ e } \frac{x = y \quad A(x)}{A(y)} id2$$

Dove si ha anche il principio/regola d'induzione:

$$\frac{A(0) \quad \overset{[A(j)]}{\overset{\cdots}{A(S(j))}}}{A(t)} ind$$

Dove se dimostro $A(0)$ e assunto $A(j)$ dimostro il successore di $A(j)$ allora posso dedurre $A(t), \forall t$.

Esempio 3. *Vediamo ora un esempio con degli assiomi specifici, costruttivi:*

- $pari(0)$
- $\forall x(pari(x) \to \neg pari(S(x)))$
- $\forall x(\neg pari(x) \to pari(S(x)))$

Quindi si ha che se x è apri non lo è il successore e se x non è pari lo è il successore. Assumiamo inoltre che 0 sia pari.
Scritta così potrebbe essere riscritta "1:1" in Prolog.
Cerchiamo quindi din dimostrare che che:

$$\forall x(pari(x) \vee \neg pari(x))$$

che si può pensare si un terzo escluso e quindi valga sempre. Questa formula, a livello di specifica, va letta come una funzione "per ogni numero naturale costruisce $pari(x)$ o $\neg pari(x)$" quindi costruisce o la parte sinistra o la parte destra. Quindi la formula i può leggere come la specifica di algoritmo che per ogni naturale mi dice se vale la parte sinistra o la parte destra dell'or e quindi è un algoritmo di decisione effettivo che per ogni naturale ti dice se è pari o non è pari. Questa è un'interpretazione diversa da quella classica.

Posso quindi fare una dimostrazione per induzione.
Il ***caso base*** *è, chiamando pari p, assunto per assioma* $p(0)$ *e usando l'introduzione dell'or:*

$$\frac{p(0)}{p(0) \vee \neg p(0)} i\vee$$

Passo al ***caso passo****.*
Assumo per ipotesi induttiva $p(j) \vee \neg p(j)$ *e assumiamo* $\forall x(p(x) \vee \neg p(S(x)))$ *che è un altro degli assiomi. Procedo eliminando il* $\forall$*:*

$$\frac{\forall x(p(x) \vee \neg p(S(x)))}{p(j), p(j) \to \neg p(S(j))} e\forall$$

procedo quindi eliminando l'implicazione:

$$\frac{p(j), p(j) \to \neg p(S(j))}{\neg p(S(j))} e \to$$

e continuo inserendo l'or:

$$\frac{\neg p(S(j))}{p(S(j)) \vee \neg p(S(j))} i\vee$$

Analogamente faccio per l'altro assioma $\forall x(\neg p(x) \vee p(S(x)))$*:*

$$\frac{\forall x(\neg p(S(x)) \vee p(S(x)))}{\neg p(j), \neg p(j) \to p(S(j))} e\forall$$

$$\frac{\neg p(j), \neg p(j) \to p(S(j))}{p(S(j))} e \to$$

$$\frac{p(S(j))}{p(S(j)) \vee \neg p(S(j))} i\vee$$

Partendo quindi da $p(j) \vee \neg p(j)$ *posso fare l'eliminazione dell'or ottenendo il* ***caso passo****:*

$$\frac{p(j) \vee \neg p(j)}{p(S(j)) \vee \neg p(S(j))} e\vee$$

e quindi posso concludere il passo induttivo:

$$\frac{p(0) \vee \neg p(0) \quad p(S(j)) \vee \neg p(S(j))}{\forall x(p(x) \vee \neg p(x))} ind$$

concludendo al dimostrazione costruttiva.
Posso quindi dire che, essendo 0 pari, 1 è dispari e quindi 2 è pari, 3 dispari etc... in pratica è un ciclo che parte dal caso base e poi decide per qualsiasi numero naturale. Possiamo quindi estrarre un algoritmo iterativo (potrei anche estrarne uno ricorsivo) da questa dimostrazione. Tale algoritmo è visualizzabile nell'implementazione C nel listing 2.2.

Listing 1 Codice C dell'algoritmo di calcolo pari creato dalla dimostrazione

```c
#include <stdio.h>

void A1(int* fdv){
  *fdv = 0;
}
void A2(int* j, int* fdv){
  *fdv = 1;
  *j = *j + 1;
}
void A3(int* j, int* fdv){
  *fdv = 0;
  *j = *j + 1;
}
void base(int* f){
  A1(&*f);
}
void passo(int* j, int ff1, int* ff2){
  if (ff1 == 0){
    A2(&*j, &*ff2);
  }else{
    A3(&*j, &*ff2);
  }
}

int main(){
  int x, j, ff;
  scanf("%d", &x);
  j = 0;
  base(&ff);
  while(j <= x - 1){
    passo(&j, ff, &ff);
  }
  if (ff == 0){
    printf("%d è pari\n", x);
  }else{
    printf("%d è dispari\n", x);
  }
  return 0;
}
```

Come detto algoritmi così sintetizzati non sono algoritmi ottimali e l'esempio del pari o dispari è evidente. Normalmente si avrebbe infatti:

Listing 2 Codice C dell'algoritmo di calcolo pari ottimale

```c
#include <stdio.h>
int main(){
  int x;
  scanf("%d", &x);
  if ((x % 2) == 0){
    printf("%d è pari\n", x);
  }else{
    printf("%d è dispari\n", x);
  }
  return 0;
}
```

E quindi si ha un limite nella costruzione dell'algoritmo anche se il primo sappiamo essere corretto (avendo applicato la deduzione naturale e l'induzione, ho la garanzia che in quella assiomatizzazione il programma sia totalmente corretto) mentre di quest'ultimo dovremmo dimostrare la correttezza. Nel primo programma la componente funzionale della dimostrazione è data dalle varie funzioni che si richiamano. L'algoritmo per ogni istanza calcola se vale la parte sinistra o destra della disgiunzione in modo uniforme. Le funzioni si deducono automaticamente dalla prova costruttiva. Niente di tutto ciò è asseribile sull'algoritmo ottimo.
Parlando invece di Prolog avrei una situazione diversa. In Prolog ogni computazione è un'*istanza di dimostrazione* che varia di caso in caso e quindi non si ha una dimostrazione generale. Possiamo dire che un programma Prolog non rappresenta l'algoritmo che risolve il problema specificato per ogni dato di input. Si ha quindi un diverso modello di calcolo/computazione.

Capitolo 3

Logica Intuizionistica

La **logica proposizionale intuizionistica** è il primo paradigma che trattiamo di **logica costruttiva**, dove appunto valgono la **DP** e la **EDP**, che sono i due requisiti minimali per dire che una logica è costruttiva. L'intuizionismo proposizionale è il paradigma minimale di logica costruttiva.

3.1 Sintassi

Iniziamo a parlare dell'intuizionismo proposizionale e già a livello di linguaggio si ha una differenza tra la logica classica e quella intuizionistica.
Il linguaggio della logica proposizione intuizionistica comprende i seguenti *simboli*:

- variabili proposizionali A, B, C, etc...
- connettivi $\wedge$, $\vee$, $\neg$ e $\rightarrow$. Il $\neg$ è l'unico connettivo unario mentre gli altri sono connettici binari
- simboli ausiliari come "(" e ")" utili a stabilire precedenze tra connettivi

Una formula ben formata intuizionistica è definita così:

1. ogni variabile proposizionale appartiene alle FBF
2. se A e B sono FBF allora:
    - $\neg A$
    - $A \vee B$
    - $A \wedge B$

- $A \to B$

appartengono alle FBF

3. nient'altro appartiene alle FBF

E fin qui non si hanno differenze con la logica classica.
La differenza rispetto alla logica classica si riscontra nel fatto che i 4 connettivi intuizionistici sono tra loro **completamente indipendenti**. In logica classica invece potrei anche solo usare $\neg$ e $\vee$ in quanto gli altri due si possono ricavare da questi due (tramite leggi di De Morgan etc...). In logica classica $\neg$ e $\vee$ formano un insieme minimale di operatori. In logica intuizionistica non ho nulla del genere, non posso ridurre nessun connettivo ad un altro. D'altro canto anche Prolog riduceva pesantemente il linguaggio, basandosi sulla logica classica e sulle clausole di Horn anche se si può aprire una discussione in merito al fatto che comunque la riduzione del linguaggio delle clausole di Horn in Prolog comunque garantisce l'algoritmicità delle dimostrazioni e la loro costruttività. Le clausole di Horn sono infatti una restrizione del linguaggio classico e non tutte le formule di logica classifica sono esprimibili in termini di clausole di Horn e questa è la motivazione per cui il Prolog di fatto computa.
La logica classica pura non è costruttiva in quanto dimostro $A \vee \neg A$ anche se non è detto che poi siamo in grado di dimostrare A o di dimostrare $\neg A$. Il principio del terzo escluso fa "saltare" la costruttività della logica classica, "saltando" la proprietà della disgiunzione DP.
Da un punto di vista formale quindi la logica intuizionistica ha l'alfabeto della logica classica, la definizione di FBF della logica classica ma non si hanno le equivalenze classiche che permettevano la riduzione del numero di connettivi.
Le precedenze sui connettivi sono le stesse di quella logica classica e la modifica delle precedenze avviene con lo stesso uso delle parentesi della logica classica. Si ricorda che $\neg$ ha la precedenza su $\wedge$ che ha precedenza su $\vee$ che ha precedenza su $\to$.
Con il simbolo $\vdash$ indichiamo la **dimostrabilità**. Quindi la scrittura $\vdash A$, con $A \in FBF$, indica che la formula A è dimostrabile nella logica intuizionistica (in teoria bisognerebbe specificare la logica a pedice di $\vdash$ ma se omesso, salvo diversamente specificato, si parla di logica intuizionistica).
Passiamo quindi a presentare un **sistema deduttivo** per dimostrare formule nella logica intuizionistica.
Partiamo con un sistema deduttivo molto semplice.
L'apparato deduttivo maneggerà due tipi di formule, che indichiamo come **formule segnate** dai simboli T e F. Data una qualsiasi FBF A allora TA

e FA sono formule segnate con T e F.
Definiamo per ogni connettivo **T-regole** e **F-regole**. Suppongo che S sia un arbitrario insieme di formule segnate, con / che specifica che la regola si divide in due parti, con S_T specifico che tengo di S solo le formule segnate con T (sto facendo una *restrizione*):

connettivo	T-regola	F-regola
$\wedge$	$T\wedge = \frac{S,T(A\wedge B)}{S,TA,TB}$	$F\wedge = \frac{S,F(A\wedge B)}{S,FA/S,FB}$
$\vee$	$T\vee = \frac{S,T(A\vee B)}{S,TA/S,TB}$	$F\vee = \frac{S,F(A\vee B)}{S,FA,FB}$
$\rightarrow$	$T\rightarrow = \frac{S,T(A\rightarrow B)}{S,FA/S,TB}$	$F\rightarrow = \frac{S,F(A\rightarrow B)}{S_T,TA,FB}$
$\neg$	$T\neg = \frac{S,T(\neg A)}{S,FA}$	$F\neg = \frac{S,F(\neg A)}{S_T,TA}$

Senza le due restrizioni di S a $_T$ otterrei i tableaux della logica classica proposizionale. Quindi passare al questo apparato deduttivo della logica intuizionistica non è complesso.
Usando queste regole una **dimostrazione** è una sequenze di applicazione di queste regole che comincia sempre con FX dove X è la formula che voglio dimostrare e deve terminare con una configurazione, ovvero un insieme di sotto-dimostrazioni, che contiene una coppia complementare, ovvero una formula segnata T e la stessa formula segnata F. La logica intuizionistica (come quella classica) è **decidibile** quindi con un numero finito di passi riesco sempre a stabilire se una formula è dimostrabile o meno nella logica intuizionistica. Questo accade in quanto la lunghezza della formula è sempre finita, non si ha possibilità di generare formule infinite, e le regole vanno a destrutturare le formule ottenendo sempre formule di complessità minore ad ogni applicazione di regola e quindi prima o pi si arriva alle formule atomiche, finendo il processo in quanto non hanno ovviamente regole di destrutturazione.
Nella logica intuizionistica, a differenza di quella classica, non tutti gli ordini di applicazione delle regole portano ad una tavola chiusa, ovvero ad una dimostrazione della formula, anche se la formula è dimostrabile. Esistono strategia di soluzione che non vanno a buon fine e questo è dovuto all'ordine dell'applicazione delle regole e alla concorrenza tra l'applicazione di due regole. Le uniche regole che però hanno questo problema sono le due con restrizione. Non tutti (a priori rispetto all'ordine di applicazione delle regole) i tableaux quindi sono chiusi, a differenza della logica classica. Mi basta un tableaux chiuso (se ottengo più branch per una regola devono comunque

chiudere tutti) per dimostrare che una formula è dimostrabile mentre per dire che non lo è mi serve che tutti i possibili tableaux non siano chiusi. Si ricorda che non è necessaria una formula atomica con F e T per chiudere un tableaux ma una qualsiasi FBF con F e T.

Esempio 4. *Vediamo che il principio del terzo escluso nell'intuizionismo non è dimostrabile.*
Prendo:

$$A \vee \neg A$$

e chiediamoci se è dimostrabile nella logica intuizionistica.
So che non lo è quindi mi aspetto di non trovare un tableaux chiuso, ovvero che termina con tutti i rami che contengono una formula segnata T e la stessa segnata F. Tale formula può essere diversa ramo per ramo anche se non succederà in questo caso avendo solo A.
Parto segnando F la formula:

$$F(A \vee \neg A)$$

Applico la F di $\vee$:

$$\frac{F(A \vee \neg A)}{FA, F(\neg A)}$$

Applico ora l'unica regola che posso applicare, essendo A atomica, ovvero la F di $\neg$ (con praticamente $S = FA$ e quindi $S_T = \emptyset$):

$$\frac{FA, F(\neg A)}{TA}$$

Questo tableaux non è un tableaux chiuso e quindi la formula non è dimostrabile nella logica intuizionistica, come volevasi dimostrare.

Esempio 5. *Vediamo un'altro esempio.*
Prendiamo la legge di De Morgan:

$$\neg(A \vee B) \to (\neg A) \wedge (\neg B)$$

Parto con la dimostrazione:

$$F(\neg(A \vee B) \to (\neg A) \wedge (\neg B))$$

Procedo con l'implicazione:

$$\frac{F(\neg(A \vee B) \to (\neg A) \wedge (\neg B))}{T(\neg(A \vee B)), F((\neg A) \wedge (\neg B))}$$

Qui entra il problema della strategia. In questa situazione potrei applicare il T di $\neg$ o l'F di $\wedge$. Nella mia testa, o nel prover, devo comunque ricordare che ad un certo punto avevo la scelta, in modo da poter fare backtracking qualora non si chiuda il tableaux. Si ricorda che questo non poteva avvenire in logica classica. Lo segnalo con un asterisco:

$$*T(\neg(A \vee B)), F((\neg A) \wedge (\neg B))$$

Procedo prima con il T di $\neg$:

$$\frac{T(\neg(A \vee B)), F((\neg A) \wedge (\neg B))}{F(A \vee B), F((\neg A) \wedge (\neg B))}$$

Ma anche qui ho più scelte (l'F di $\vee$ e l'F di $\wedge$), me lo segno con due asterischi:

$$** F(A \vee B), F((\neg A) \wedge (\neg B))$$

Scelgo la F di $\vee$ perché non crea branch:

$$\frac{F(A \vee B), F((\neg A) \wedge (\neg B))}{FA, FB, F((\neg A) \wedge (\neg B))}$$

Procedo con la F di $\wedge$, creando due branch:

$$\frac{FA, FB, F((\neg A) \wedge (\neg B))}{FA, FB, F(\neg A) / FA, FB, F(\neg B)}$$

Ma:

$$\frac{FA, FB, F(\neg A) / FA, FB, F(\neg B)}{TA / TB}$$

e quindi il tableaux non è chiuso. Effettuo il backtracking cominciando dal primo asterisco. Torno alla formula e rimuovo l'asterisco:

$$T(\neg(A \vee B)), F((\neg A) \wedge (\neg B))$$

Applico quindi la F di $\wedge$:

$$\frac{T(\neg(A \vee B)), F((\neg A) \wedge (\neg B))}{T(\neg(A \vee B)), F(\neg A) / T(\neg(A \vee B)), F(\neg B)}$$

Studiamo i due branch in parallelo ma devo mettere un asterisco, potendo fare sia T che F di $\neg$:

$$*T(\neg(A \vee B)), F(\neg A) / T(\neg(A \vee B)), F(\neg B)$$

Conviene fare il F di $\neg$ perché conserviamo l'altra parte di formula:

$$\frac{T(\neg(A \vee B)), F(\neg A)/T(\neg(A \vee B)), F(\neg B)}{T(\neg(A \vee B)), TA/T(\neg(A \vee B)), TB}$$

Procedo con la T di $\neg$:

$$\frac{T(\neg(A \vee B)), TA/T(\neg(A \vee B)), TB}{F(A \vee B), TA/F(A \vee B), TB}$$

e quindi, con l'F di $\vee$:

$$\frac{F(A \vee B), TA/F(A \vee B), TB}{FA, FB, TA/FA, FB, TB}$$

Nel primo branch ho FA e TA e quindi ho una formula con sia F che T, ovvero A. Discorso analogo nel secondo con B e quindi il tableaux è chiuso. Quindi questa legge di De Morgan è dimostrabile in logica proposizione intuizionistica. Mi basta una percorso che porta ad un tableaux chiuso (e volendo qui si potrebbe vedere che è anche l'unica facendo gli altri percorsi mancanti).
Si può vedere, facendo i conti che l'altra formula di De Morgan:

$$\neg(A \wedge B) \to (\neg A) \vee (\neg B)$$

non è dimostrabile, non arrivando mai ad un tableaux chiuso. Non ho mai una strategia vincente quindi la formula non è dimostrabile nella logica intuizionistica. Dietro a questo comportamento si ha un motivo semantico che vedremo.

Esempio 6. *Tramite i tableaux si vede che la legge della doppia negazione:*

$$\neg\neg A \to A$$

non è dimostrabile (per di più avendo un solo cammino) in logica intuizionistica.

Si vedrà che la legge del terzo escluso o la legge della negazione, se aggiunti (ne basta uno dei due) alla logica intuizionistica la trasformano nella logica classica e viceversa, se nella logica classica non dimostro il terzo escluso o la doppia negazione ottengo la logica intuizionistica.

Esempio 7. *Tramite i tableaux si vede che la legge della conversa (non sono sicuro di aver sentito bene il nome):*

$$A \to \neg\neg A$$

è dimostrabile (per di più avendo un solo cammino) in logica intuizionistica. Si può quindi vedere come valendo un solo verso dell'implicazione (non vale la legge della doppia negazione) non può valere l'equivalenza $A \iff \neg\neg A$ *in logica intuizionistica.*

Il backtracking ha conseguenze nella complessità dell'algoritmo di decisione della logica proposizionale intuizionistica che è stato dimostrato da Stackman avere complessità spaziale pari a:

$$O(n + \log n)$$

Il backtracking si può iterare a seconda dell'ordine delle regole.
Non posso dire nell'intuizionismo che vale A sse non vale $\neg\neg A$. Infatti il sse altro non è che:

$$A \iff \neg\neg A$$

e quindi dovrei avere sia che:

$$A \to \neg\neg A$$

$$\neg\neg A \to A$$

ma abbiamo solo la prima valida.

Esempio 8. *Ci chiediamo se la formula:*

$$A \to B$$

equivale, come in logica classica, a:

$$\neg A \vee B$$

ovvero:

$$A \to B \iff \neg A \vee B$$

Già da subito possiamo dire che non vale in quanto si avrebbe dipendenza tra connettivi, cosa che abbiamo detto non esistere in logica intuizionistica.
Vediamo se sono dimostrabili i due versi:

$$(A \to B) \to (\neg A \vee B)$$

$$(\neg A \vee B) \to (A \to B)$$

Facendo i passaggi si dimostra che la prima formula non è dimostrabile e quindi già sappiamo che non vale il sse. Comunque possiamo fare i conti e veder che il secondo verso è dimostrabile in logica intuizionistica.

Vediamo un trucco per le strategia: *se si ha una formula la cui regola restringe S a S_T se ho formule complesse segnate T mi conviene aspettare ad applicare queste T e applicare la F delle regole che restringono, ovvero quelle di $\neg$ e $\rightarrow$.*
Abbiamo quindi descritto un genuino sistema di decisione con però un piccolo problema per il quale serve un esempio.

Esempio 9. *Proviamo a vedere se la formula della doppia negazione del principio del terzo escluso è dimostrabile nella logica intuizionistica. Studiamo quindi la formula:*

$$\neg\neg(A \vee \neg A)$$

Si ha quindi:

$$F(\neg\neg(A \vee \neg A))$$

E quindi:

$$\frac{F(\neg\neg(A \vee \neg A))}{T(\neg(A \vee \neg A))}$$

Da cui segue:

$$\frac{T(\neg(A \vee \neg A))}{F(A \vee \neg A)}$$

Proseguendo:

$$\frac{F(A \vee \neg A)}{FA, F(\neg A)}$$

E infine:

$$\frac{FA, F(\neg A)}{TA}$$

Coi soliti passaggi si arriverebbe (si noti il condizionale) a dire che non è dimostrabile arrivando nell'unico percorso possibile ad un tableaux non chiuso.
Anche Fitting arriva a questa conclusione

Ma per capire meglio il problema serve un teorema.

Teorema 1 (Teorema di Kolmogorov-Glivenko)**.** *Se una formula A è dimostrabile in logica classica allora e solo allora è dimostrabile in logica intuizionistica la doppia negazione di tale formula, a livello proposizionale (a livello predicativo se cose si complicano particolarmente).*

Ma questo stona rispetto all'esempio appena fatto. Il terzo escluso è dimostrabile in logica classica e quindi ci aspetteremmo che la sua doppia

negazione sia dimostrabile in logica intuizionistica, contraddicendo il teorema. Proviamo a rivedere i conti:

$$F(\neg\neg(A \vee \neg A))$$

E quindi:

$$\frac{F(\neg\neg(A \vee \neg A))}{T(\neg(A \vee \neg A))}$$

da cui segue:

$$\frac{T(\neg(A \vee \neg A))}{F(A \vee \neg A)}$$

applicando però T di $\neg$ mi premuro di riscrivere la formula a cui ho applicato la regola, ottenendo al posto del risultato precedente:

$$\frac{T(\neg(A \vee \neg A))}{F(A \vee \neg A), T(\neg(A \vee \neg A))}$$

questo complica molto il calcolo ma si dimostrerà che comunque ripetere le formule non rende il calcolo infinito.
Ora avrei più scelte quindi lo segnalo con il solito asterisco:

$$*F(A \vee \neg A), T(\neg(A \vee \neg A))$$

Proseguo in primis con l'F dell'or:

$$\frac{F(A \vee \neg A), T(\neg(A \vee \neg A))}{FA, F(\neg A), T(\neg(A \vee \neg A))}$$

Anche qui ho più scelte, lo segnalo:

$$** FA, F(\neg A), T(\neg(A \vee \neg A))$$

Proseguo con F di $\neg$:

$$\frac{FA, F(\neg A), T(\neg(A \vee \neg A))}{TA, T(\neg(A \vee \neg A))}$$

Proseguo con T di $\neg$:

$$\frac{TA, T(\neg(A \vee \neg A))}{TA, F(A \vee \neg A)}$$

E quindi:

$$\frac{TA, F(A \vee \neg A)}{TA, FA, F(\neg A)}$$

Avendo TA e FA mi posso fermare avendo chiuso il tableaux (si nota che risolvere il $\neg$ avrebbe portato ad avere TA, TA non chiudendo il tableaux). Si è quindi dimostrato che la formula è dimostrabile, confermando quanto detto nel teorema di di Kolmogorov-Glivenko.
Ripetere ogni volta la regola come fatto al secondo passaggio, però renderebbe il tableaux ingestibile e renderebbe il calcolo semi-decidibile, perché se la formula non è dimostrabile posso andare avanti all'infinito a ripetere le formule, comportando un serio problema. Si nota inoltre che abbiamo subito scelto il percorso che portava alla chiusura ma ci sono stati due punti in cui abbiamo scelto una regola rispetto ad un'altra. La seconda scelta nella formula con $*$ avrebbe portato ad un tableaux non chiuso (e si vedeva quasi ad occhio che lo avrebbe fatto). Anche in merito alla formula con $**$ si nota che la seconda scelta avrebbe portato ad un tableaux che non chiudeva.
Possiamo dire che la regola di poter riusare le formule a cui applichi la regola riportandola nel tableaux è una sorta di **meta-regola**. L'aggiunta di questa meta-regola è un calcolo completo rispetto alla logica proposizionale intuizionistica, ovvero tutte le formule intuizionistiche dimostrabili hanno un tableaux chiuso.
Le uniche formule che eventualmente richiedono al ripetizione, ovvero l'uso di questa meta-regola, sono le formule T di $\neg$ e T di $\rightarrow$. Possiamo quindi riformulare quelle due regole.
Per il $\rightarrow$:

$$T \rightarrow = \frac{S, T(A \rightarrow B)}{S, FA, T(A \rightarrow B)/S, TB}$$

notando che nella seconda parte non devo ripetere la formula.
Per il $\neg$:

$$T\neg = \frac{S, T(\neg A)}{S, FA, T(\neg A)}$$

Con le regole così modificate (queste due modificate più tutte le altre non modificate) abbiamo un **calcolo completo e corretto** per la logica proposizionale intuizionistica. Non ci sono quindi formule dimostrabili intuizionisticamente per cui non esiste un tableaux chiuso con le regole descritte. D'ora in poi per i due casi useremo sempre le due nuove regole modificate anche se potenzialmente non è sempre necessario. Se ottengo un tableaux chiuso senza ripetizione lo ottengo anche con ma se lo ottengo con la ripetizione non per forza lo ottengo senza. Volendo posso ricordarmi della ripetizione usando un "placeholder" senza dover riscrivere ogni volta la formula intera per segnalare che in caso non riesca a chiudere il tableaux senza la ripetizione posso usare la ripetizione.
Esplicitare i due casi in cui può servire la ripetizione della formula è un grande aiuto dal punto di vista computazionale, essendo solo due casi.

In logica classica predicativa si ha una situazione analoga per quanto riguarda l'istanziazione dei parametri, con la T di $\forall$ e la F di $\exists$ (controllare appunti di fondamenti dell'informatica).
La logica classica proposizionale non richiederebbe mai un artificio simile a quello della meta-regola, così come non richiede backtracking perché vale la **proprietà di Chruch-Rosser** che ci assicura che se un tableaux deve chiudere chiuderà qualsiasi percorso si scelga.
Ricordando che $\neg\neg A \to A$ non è dimostrabile intuizionisticamente ma sappiamo che vale classicamente essendo una tautologia classica. Ma allora, per il teorema di Kolmogorov-Glivenko al formula:

$$\neg\neg(\neg\neg A \to A)$$

è dimostrabile in logica intuizionistica e si può verificare coi soliti passaggi (usando per di più una sola volta una ripetizione, nonostante potenzialmente se ne creino di più durante la dimostrazione).

3.2 Semantica

Abbiamo parlato finora di **sintassi**, parliamo ora della **semantica**, in termini di **modelli di Kripke**