Appunti di Metodi Algebrici per l'Informatica

Prof. Andrea Previtali

Dipartimento di Matematica e Applicazioni
Università di Milano-Bicocca
U5-3050 via Roberto Cozzi 55, 20125 Milano
email: andrea.previtali@unimib.it
URL: https://sites.google.com/unimib.it/andreaprevitali/home-page

28 settembre 2025

A Monica, Gaia e Linda

Introduzione

Cosa sono queste Note

Scopo di queste note è fornire un testo di riferimento per il corso di Metodi Algebrici per l'Informatica tenuto presso l'Università di Milano-Bicocca a partire dall'a.a. 2025-2026. Non vanno pertanto considerate complete e infatti spesso fornirò riferimenti a materiali e testi in cui trovare elementi di approfondimento relativi ad argomenti trattati o accennati durante le lezioni.

Software

Mia aspirazione è fornire anche alcuni rudimenti di linguaggi di programmazione simbolica, e.g. GAP, MAGMA, Pari/GP e SageMath (vedi [GAP25, BCFS25, Coh25, Ste25])con l'intento di stimolare l'aspetto sperimentale insito nella (ri)scoperta di risultati (vecchi) e nuovi in Matematica. Tali programmi e relativi manuali sono scaricabili ai seguenti link MAGMA, Magma Handbook, GAP, PARI/Gp e SageMath.

Caricherò di volta in volta esempi di codice in Magma da utilizzare per la risoluzione di (alcuni) esercizi proposti nel testo sulla piattaforma di Moodle relativa al corso.

Alcuni esercizi proposti in questi appunti o nei test di autovalutazione di Wims potrebbero richiedere calcoli non immediati. Come i vari programmi menzionati implementino questi calcoli è una questione che, per ovvi motivi di tempo e di spazio, non toccherò in questo corso. A chi al termine del corso avesse sviluppato interesse ad approfondire tematiche computazionali consiglio di dare un'occhiata ai relativi manuali per farsi un'idea di quali complicazioni nascano quando si vogliono ottenere risposte dettagliate in casi concreti.

Modalità d'esame

Buona parte dell'esame verrà erogata sulla piattaforma di Wims. Tale piattaforma utilizza, in forma non visibile all'utente, i programmi sopra menzionati e molti altri. Una volta effettuata l'iscrizione al corso (di Algebra) si potrà accedere a vari contenuti.

- Ai test di autovalutazione. Resi visibili con cadenza settimanale vi consentiranno di capire se siete in sintonia con il corso. Il loro svolgimento entro due settimane dalla loro attivazione permetteranno inoltre di acquisire un bonus (vedi Moodle). Resteranno comunque disponibili per tutto l'anno accademico.
- Ai questionari di iscrizione all'esame dove sono riportati date, orari e luoghi di svolgimento dell'esame.
- Agli esami stessi.

L'esame consiste in:

- una serie di domande a scelta multipla.
- una serie di esercizi di routine scelti tra quelli proposti nei test di autovalutazione.

- in un esercizio aperto più complesso per misurare la vostra capacità di rielaborazione dei contenuti.

- in una domanda aperta di teoria.

La durata complessiva della prova ammonta a 120 minuti.

Bibliografia

Oltre a queste Note consiglio si dare un'occhiata ai testi e agli articoli riportati in bibliografia. Molti sono ottenibili tramite Mathscinet. Per esperienza voi studenti sembrate gradire testi in italiano scritti da italiani o tradotti principalmente dall'Inglese.

Tra i primi segnalo

- ??

Nella seconda fattispecie meritano menzione:

- L. Childs, *Algebra. Un'introduzione concreta*. ETS, 1989, [Chi84]. Fornisce un approccio algoritmico con molta enfasi su questioni di complessità computazionale.

WIMS

WIMS realizza un'interfaccia tra finestre del vostro browser preferito e molti programmi - quelli sopra menzionati e molti altri. Si possono creare esercizi, accedere a esercizi già disponibili in pacchetti di tipo "modtool" e caricare librerie "slib" create da altri utenti. Per chi fosse interessato c'è molto da fare. Consiglio di dare un'occhiata alla documentazione disponibile ad esempio sul sito locale WimsBicocca sull'omonimo Tab o una versione più completa su WimsNice

Indice

1 Logica Proposizionale e algebre di Boole

Vorrei iniziare analizzando alcuni temi di esame del corso di Fondamenti dell'Informatica; in particolare le domande di Logica Proposizionale.

1.1 Logica proposizionale e Connettivi Logici

Ricordo che tale disciplina studia la validità di formule ottenute combinando proposizioni mediante i connettivi logici. Detto $\mathcal{P}$ l'insieme delle proposizioni, esistono funzioni ad uno o due argomenti:

- Negazione: $\neg : \mathcal{P} \to \mathcal{P}$
- Congiunzione: $\wedge : \mathcal{P} \times \mathcal{P} \to \mathcal{P}$
- Disgiunzione (inclusiva): $\vee : \mathcal{P} \times \mathcal{P} \to \mathcal{P}$
- Implicazione: $\to$: $\mathcal{P} \times \mathcal{P} \to \mathcal{P}$
- Doppia Implicazione: $\leftrightarrow$: $\mathcal{P} \times \mathcal{P} \leftrightarrow \mathcal{P}$

La Logica Proposizionale studia come determinare il valore di verità di un formula in funzione dei valori di verità assegnati alle proposizioni che in tale formula occorrono. Ricordo che i valori di verità sono due, vero o falso, solitamente denotati V ed F. La negazione è un connettivo con un solo argomento e scambia V con F, ossia una proposizione p è vera sse $\neg p$ è falsa. Si può pensare alla negazione come una funzione dall'insieme dei valori di verità $W = \{\mathrm{V}, \mathrm{F}\}$ in sé stesso.

Esercizio 1.1 *Mostrare che esistono esattamente quattro funzioni da W in sé.*

Analoga domanda si può porre se consideriamo formule contenenti due proposizioni, ossia stabilire quante sono le funzioni da $W \times W$ in W. Ad esempio il connettivo congiunzione induce la funzione associa V alla coppia (V, V) ed F alle altre coppie. Altrimenti detto $p \wedge q$ è vera sse sono vere p e q.

Proposizione 1.2 *Esistono* 16 *funzioni da $W \times W$ in W.*

Dim. Esistono 4 coppie definite su W. Per ciascuna di esse ho due scelte, per un totale di $2^4 = 16$ possibilità. □

In modo equivalente abbiamo 16 connettivi logici a due argomenti, ossia 16 modi per combinare tra loro due proposizioni. Tre sono elencate sopra, quali sono le altre? Il primo passo consiste nel sostituire V ed F con 1 e 0. Il motivo è che $0, 1$ possono essere manipolati con strumenti matematici. Ad esempio questi valori possono essere moltiplicati ed è facile constatare che il prodotto corrisponde esattamente alla congiunzione. Infatti $1 \cdot 1 = 1$ e $0 \cdot a = 0$ per $a \in \{\mathrm{V}, \mathrm{F}\}$ traduce esattamente $\mathrm{V} \wedge \mathrm{V} = \mathrm{V}$ e $\mathrm{F} \wedge \mathrm{A} = \mathrm{F}$ per $A = \mathrm{V}, \mathrm{F}$. Cosa succede con la somma? Il primo problema è che $1 + 1 = 2$, ma 2 non è un valore di verità. La soluzione vincente consiste nel interpretare $0, 1$ come pari e dispari

e quindi, osservando che la somma di due numeri dispari è pari, porre $1+1=0$. Con tale imposizione abbiamo

$$0+0=0, 0+1=1+0, 1+1=0.$$

Questo è il comportamento del connettivo logico XOR o della disgiunzione esclusiva (**aut** in latino), ove p XOR q è vera sse una tra p e q è vera ma non entrambe. Notate che $\neg$ è descritta da

$$x \mapsto 1+x.$$

Proposizione 1.3 *La disgiunzione inclusiva (**vel** in latino) è descritta dalla funzione* $(x,y) \mapsto x+y+xy$, $x,y=0,1$.

Dim. Con leggero abuso di notazione, denotiamo con $\vee$ tale funzione. Allora $1 \vee 1 = 1+1+1\cdot 1 = 1$. Inoltre $x \vee 0 = x$ vale 0 sse $x=0$. □

Ricordo che la tavola di verità per l'implicazione è

$$1 \to a = a, 0 \to a = 1,$$

ove $a = 0, 1$.

Esercizio 1.4 *Provare che $p \to q$ è logicamente equivalente (assume gi stessi valori di verità) di $(\neg p) \vee q$.*

Attenzione alla posizione delle parentesi.

Esercizio 1.5 *Provare che $\neg(p \vee q) = (\neg p) \wedge (\neg q) \neq (\neg p) \vee q$.*

Immagino abbiate usato le tavole di verità per le precedenti formule. Se usate la formulazione matematica l'esercizio si traduce nel provare che

$$1+(x+y+xy) = (1+x)(1+y) \neq (1+x)y.$$

1.2 Algebre di Boole

L'uguaglianza sembra ovvia, la diseguaglianza un po' meno. Seguono entrambe da una proprietà algebrica che vale per gli interi e per i polinomi, oggetti che tratteremo nelle prossime lezioni, ossia la proprietà **distributiva** del prodotto rispetto alla somma. In formule

$$(x+y)z = xz+yz.$$

Teorema 1.6 *Per ogni x,y,z vale $(x+y)z = xz+yz$.*

Dim. Se $z=0$ entrambe i termini si annullano. Se $z=1$ l'espressione diventa $x+y=x+y$, una tautologia. □

In forza di questo Teorema otteniamo

$$(1+x)(1+y) = (1+y)+x(1+y) = 1+y+x+xy = 1+x+y+xy,$$

dove la seconda uguaglianza si ottiene osservando che $x+y=y+x$, ossia che la somma gode della proprietà **c**ommutativa. Infine $1+x+y+xy=y+xy=(1+x)y$ è falsa per $x=0$ in quanto diventa $1+y=y$. Cosa suggerisce di considerare $x=0$? Se fossimo di fronte a dei polinomi dedurremmo che $1+x+y+xy=y+xy$ implica, cancellando $y+xy$, che $1+x=0$, condizione palesemente non soddisfatta da $x=0$. Possiamo cancellare? La risposta è sì se applichiamo la regola che ha condotto alla definizione della somma, ossia

$$2=1+1=0.$$

Se sommiamo $x+xy$ ad entrambi i termini otteniamo

$$1+x=1+x+y+xy+x+xy=x+xy+x+xy=0.$$

Più in generale ogni valore di verità x ammette un **opposto**, ossia un y tale che $x+y=0=y+x$. Qui abbiamo l'ulteriore miracolo $y=x$.

Esercizio 1.7 *Stabilire se vale la legge distributiva della somma rispetto al prodotto, ossia se per ogni* x,y,z, $xy+z=(x+z)(y+z)$.

Esercizio 1.8 *Mostrare che sia somma che prodotto soddisfano la proprietà* ***associativa****, ossia per ogni* x,y,z $(x\star y)\star z=x\star(y\star z)$, *ove* $\star=+,\cdot$.

Per ricapitolare sull'insieme W sono definite due operazioni binarie, ossia funzioni da $W\times$W in W che soddisfano varie proprietà. Si dice che W ammette la struttura di **anello**. Mostriamo che $B_0=W$ è il livello zero di una sequenza di anelli. Il termine successivo B_1 può essere pensato come un insieme di polinomi i cui coefficienti variano in B_0 nella variabile x. Ogni polinomio b soddisfa $2b=0$. Poiché il prodotto codifica la congiunzione, abbiamo $x^2=x$, ossia x è quello che si dice un elemento **idempotente**. Si ha che

$$B_1=\{0,1,x,1+x\}$$

possiede esattamente quattro elementi. Notate che possiamo interpretare questi polinomi come funzioni da W in sé, $0,1$ sono polinomi costanti, x indica l'identità e $1+x$ la negazione.

Al passo successivo abbiamo B_2, l'anello dei polinomi in due variabili, x,y, sottoposto alle condizioni $2b=0$ e $x^2=x$, $y^2=y$. Segue che

$$B_2=\{a+bx+cy+dxy : a,b,c,d=0,1\}$$

possiede esattamente 16 elementi. Questi codificano tutte le funzioni da $W\times W$ in W.

Esercizio 1.9 *Mostrare che* $p^2=p$, *per ogni* $p\in B_2$

Esercizio 1.10 *Identificare ogni elemento di* B_2 *come combinazione dei connettivi logici* $\neg,\vee,\wedge,\rightarrow,\leftrightarrow$.

In generale B_n, l'insieme dei polinomi in n variabili $x_1, \ldots, x_n$ codifica le funzioni da W^n, il prodotto cartesiano di n copie di W in W. La sua cardinalità vale 2^{2^n} ed i suoi elementi sono somme di monomi della forma

$$x_{i_1} \cdots x_{i_k}, 1 \leq i_1 < \ldots < i_k \leq n, 0 \leq k \leq n$$

(se k vale 0 si ha il polinomio costantemente uguale a 1).

Vediamo in dettaglio un esempio più concreto. Nel Tema d'Esame del Giugno 2023 viene chiesto di stabilire la natura della seguente formula in tre variabili proposizionali

$$\neg((s \wedge \neg t) \to (t \vee q)) \vee (s \to (t \vee q)).$$

Ne viene fornita una soluzione tramite le tavole di verità. Noi traduciamo invece il problema in termini matematici/polinomiali e calcoliamo.

1.3 Magma

Possiamo affrontare il problema con carta e penna ma ritengo sia più proficuo utilizzare un programma di manipolazione simbolica tra quelli menzionati. Per varie ragioni preferisco utilizzare Magma. Inizio ad implementare le funzioni negazione, disgiunzione e implicazione. Quest'ultima vale $\neg p \vee q$, ossia

$$(1 + x) + y + (1 + x)y = 1 + x + y + y + xy = 1 + x + xy.$$

La sintassi in Magma è abbastanza autoesplicativa:

```
neg:=func<x|1+x>;
vel:=func<x,y|x+y+x*y>;
imp:=func<x,y|1+x+x*y>;
```

L'insieme dei coefficienti $W = B_0$ costituisce un esempio di **campo**, un analogo minimale dell'insieme dei numeri reali, dei numeri complessi o dei razionali; esempi che sicuramente avete incontrato in nel carso di Algebra Lineare. Questo è il primo esempio di una famiglia doppiamente infinita di campi aventi cardinalità finita detti campi di Galois (GF o Galois Fields). Su questi coefficienti costruiamo l'anello dei polinomi in tre variabili:

```
F:=GF(2);
A:=PolynomialRing(F,3);
```

Mentre la condizione $2p = 0$ è già codificata in queste istruzioni, dobbiamo imporre che $x^2 = x$ per ogni variabile. A tal fine si deve costruire una struttura **quoziente** introducendo un'opportuna **relazione di equivalenza**. Questo concetto è stato già introdotto l'anno scorso quindi non darò per scontato che sappiate cosa è una relazione di equivalenza.

```
B<s,t,q>,bb:=quo<A|[A.i^2-A.i:i in [1..Rank(A)]]>;
```