

1. Data una formula P quand'è che si dice soddisfacibile?

DATA UNA FORMULA P DICO CHE LA FORMULA È SODDISFACIBILE SE ESISTE UNA INTERPRETAZIONE I DELLE VARIABILI PROPOZITIONALI PRESENTI NELLA FORMULA, OVVERO UN'ASSEGNAZIONE DEL VALORE DI VERITÀ T/F PER OGNI VARIABILE PROPOZIONALE, TALE CHE $I(P)$ È VERA.

2. Quali sono i 2 principi fondamentali della logica proposizionale?

DUE FORMULE PARTICOLARI CI DANNO I 2 PRINCIPI FONDAMENTALI DELLA LOGICA PROPOZIZIONALE, PER OGNI PROPOSIZIONE P SI HA:

- PRINCIPIO DEL TERZO ESCLUSO

$P \vee \neg P$, TAUTOLOGIA, OSSIA SEMPRE VERA.

- PRINCIPIO DI NON CONTRADDIZIONE

$P \wedge \neg P$, IN SODDISFACIBILE, OSSIA SEMPRE FALSE.

3. Dato un insieme di proposizioni \mathcal{P} e una proposizione P , qual è la definizione della giustificazione logica, $\mathcal{P} \models P$ così denotata?

SIA \mathcal{P} UN INSIEME DI PROPOSIZIONI E P UNA PROPOSIZIONE, DICARO CHE \mathcal{P} GIUSTIFICA P O CHE P È UNA CONSEGUENZA LOGICA DI \mathcal{P} E LO DENOTIAMO CON $\mathcal{P} \models P$ SE OGNI' INTERPRETAZIONE I CHE SODDISFA TUTTE LE FORMULE DI \mathcal{P} SODDISFA ANCHE P .

4. Qual è la definizione di formula in Forma Normale Congiuntiva (CNF)?

UNA FORMULA P È IN FORMA NORMALE CONGIUNTIVA (CNF) SE È SCRITTA COME CONJUNZIONE DI DISGIUNZIONI $\Rightarrow (P \vee q) \wedge (\neg p \vee r \vee s)$.

5. Cosa dice l'assioma di estensionalità?

L'ASSIOMA DI ESTENSIONALITÀ DICE: 2 INSIEMI $A \in B$ SONO uguali SE HANNO GLI STESSI ELEMENTI
 $A = B \Leftrightarrow (\forall x)(x \in A \Leftrightarrow x \in B)$.

6. Dati due insiemi A e B come è definita la loro differenza simmetrica?

LA DIFF. SIMMETRICA DI 2 INSIEMI $A \in B$ È L'UNIONE DELLE 2 DIFF.,
OVVERO $(A \setminus B) \cup (B \setminus A)$, QUINDI È L'INSIEME FORMATO DA QUEGLI ELEMENTI
DEL PRIMO O DEL SECONDO INSIEME CHE NON APPARTENGONO A ENTRAMBI.

7. Dati tre insiemi A , B e C dimostrare che $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

$$1^{\text{a}} \text{ PARTE} \quad A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$$

$$x \in A, x \notin (B \cup C) \Rightarrow x \notin B, x \notin C \Rightarrow x \in (A \setminus B), x \in (A \setminus C)$$

$$2^{\text{a}} \text{ PARTE} \quad (A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C)$$

$$\begin{aligned} x \in A, & \quad x \notin B \Rightarrow x \in A \setminus (B \cup C) \\ x \in A, & \quad x \notin C \end{aligned}$$

8. Come è definito l'insieme delle parti di un insieme A e quanti sono i suoi elementi?

DATO UN INSIEME A , L'INSIEME DELLE PARTI DI A È UN INSIEME I CUI ELEMENTI SONO
TUTTE LE PARTI O SOTTOSIEMI DI A , E SI INDICHERÀ CON $\mathcal{P}(A)$ O $\text{pow}(A)$.
LA CARDINALITÀ: $|\mathcal{P}(P)| = 2^m$, DOVE $m = n^{\circ}$ ELEMENTI DI A .

9. Data una famiglia di insiemi \mathcal{F} , quali condizioni deve verificare per essere una partizione dell'insieme A ?

UNA FAMIGLIA DI INSIEMI \mathcal{F} È UNA PARTIZIONE DELL'INSIEME A SE SODDISFA
3 CONDIZIONI:

- $\forall X \in \mathcal{F}$ si ha che $X \subseteq A$
- $\bigcup_{X \in \mathcal{F}} X = A$
- $\forall X, Y \in \mathcal{F}, X \neq Y$ si ha $X \cap Y = \emptyset$

10. Cos'è il paradosso di Russell e sulla costruzione di quale insieme è definito?

DATO $S = \{A : A \text{ È UN INSIEME, } A \notin A\}$

INSIEME DI TUTTI GLI INSIEMI CHE NON APPARTENGONO A SE STESSI

$S \in S$?
SI \rightarrow DA DEFINIZIONE NE DOBBIANO DESCRIRE CHE $S \notin S$
NO \rightarrow DA DEFINIZIONE NE DOBBIANO DESCRIRE CHE $S \in S$

CONTRODISSONE!

COME EVITARE LA CONTRODISSONE?

$S = \{A : A \subseteq U, A \notin A\}$

$S \in S$? $\Rightarrow S \notin S$, MA SE $S \in S \Rightarrow S \subseteq U$ OPPURE

$S \in S \Rightarrow$ CONTRODISSONE

E QUINDI LA CONTRODISSONE SI PUÒ EVITARE ASSUMENDO CHE $S \not\subseteq U$.

11. Sia S un insieme finito e R una relazione definita su S . Quali proprietà deve verificare R per essere una relazione di equivalenza?

DATO S DIREMO CHE R DEFINITA IN S È UNA RELAZIONE DI EQUIVALENZA SE ESSA È RIFLESSIVA, SIMMETRICA E TRANSITIVA

- RIFLESSIVA: SE $\forall x \in S$ È VERO $R(x, x)$
- SIMMETRICA: SE $\forall x, y \in S$, SE $R(x, y)$ È VERO ALLORA LO SARÀ ANCHE $R(y, x)$
- TRANSITIVA: SE $\forall x, y, z \in S$, SE $R(x, y)$ E $R(y, z)$ SONO VERE, ALLORA $R(x, z)$ È VERO

12. Dimostrare il seguente teorema

Due classi di equivalenza o sono disgiunte o coincidono.

SIANO $[x] \in [z]$ DUE CLASSI DI EQUIVALENZA E SUPponiamo che esse abbiano UN ELEMENTO IN COMUNE: $w \sim x$, $w \sim z$, PER LA TRANSITIVA $x \sim z$.
SIA ORA $y \in [x]$, cioè $y \sim x$. PER LA TRANSITIVA $y \sim z$, cioè $y \in [z]$.
QUINDI, $[x] \subseteq [z]$.
ANALOGAMENTE SI DIMOSTRA CHE $[z] \subseteq [x]$.

13. Qual è la definizione di funzione iniettiva?

DATA UN'APPLICAZIONE $f: A \rightarrow B$ SE PER Ogni PUNTI DISTINTI SU PUNTI DISTINTI ALLORA LA FUNZIONE SI DICE INIETTIVA FORMALMENTE
 $\forall x, y \in A$, SE $x \neq y$, ALLORA $f(x) \neq f(y)$.

14. Dimostrare il seguente teorema

Se A e B sono due insiemi finiti ed esiste una funzione iniettiva $f : A \rightarrow B$ allora $|A| \leq |B|$.

Considero l'immagine $f(A)$. So che $f(A) \subseteq B$ e sappiamo che ogni elemento di $f(A)$ è l'immagine di uno ed un solo elemento di A . Poiché la funzione f è iniettiva, quindi in $f(A)$ ci sono tanti elementi quanti ce ne sono in A . Ne concludiamo che $|A| = |f(A)| \leq |B|$.

PARTE 2: 15-28

15. Cosa dice il Principio di Induzione?

Dice che:

- Se una proprietà P è posseduta dal numero 0 è
- La proprietà P è posseduta anche dal successore di ogni numero naturale che possiede la proprietà P , allora
- La proprietà P è posseduta da tutti i numeri naturali

DIM. RAGIONO PER ASSURDO E SUPPONGO FALSE LA TESI, cioè che esiste ALMENO UN NATURALE m PER CUI $P(m)$ È FALSE. $S = \{n : n \in \mathbb{N}, \text{ e } P(n) \text{ È FALSO}\}$
PER IP. DI ASSURDO S NON È VUOTO. PER L'ASSIOMA DEL BUON ORDINAMENTO ESISTE IN S UN EL. MINIMO s . PER DEFINIZIONE DI S , $P(s)$ È FALSE. DALLE IPOTESI $s \neq 0$ poiché $P(0)$ È VERA.
QUINDI POICHÉ $S \subset \mathbb{N}$, DEVE ESSERE $s > 0$. ALLORA ESISTE IL SUO PREDECESSORE, $s-1$, DAL MOMENTO CHE $s-1 < s$ ABBIANO CHE $s-1 \notin S$ QUANDO $P(s-1)$ È VERA. MA QUESTO IMPLICA, PER IL CASO (b) CHE $P(s)$ È VERA. **CONTRODIREZIONE**

16. Dimostrare il seguente

Dati $a, b, c \in \mathbb{Z}$, se $a \mid b$ e $a \mid c$ allora $a \mid (b+c)$.

DATO CHE $a \mid b$ ESISTE $x : b = ax$, E DATO CHE $a \mid c$ $\exists y : c = ay$.

QUINDI $b+c = ax+ay = a(x+y)$ E Ponendo $z = x+y$ NO TROVATO UN INTERO TALE CHE $b+c = az$ DIMOSTRANNO CHE $a \mid (b+c)$

17. Descrivere l'algoritmo di Euclide per il calcolo del M.C.D.

L'ALGORITMO DI EUCLIDE PER IL CALCOLO DEL M.C.D. SI BASA SU DIVISIONI SUCCESSIVE.

SIANO $a, b \in \mathbb{N}$, $b \leq a$

(CASO BASE) SE $b=0$, $\text{MCD}(a, b)=a$. ALTRIMENTI

(PASSO INDUTTIVO) VISTO CHE $a = qb + r$, CON $0 \leq r < b$ AVREMO $\text{MCD}(a, b) = \text{MCD}(b, r)$

NOTIAMO CHE SE $b | a$ ALLORA $a = qb$ ED IL RESTO $r=0$ E QUINDI $\text{MCD}(a, b) = \text{MCD}(b, 0) = b$ PER IL CASO BASE. QUINDI, SE $b \nmid a$ OTTERNO IN UN PASSO CHE $\text{MCD}(a, b) = b$

ES. $\text{MCD}(20, 13) = \text{MCD}(13, 7) = \text{MCD}(7, 6) = \text{MCD}(6, 1) = \text{MCD}(1, 0)$

$\text{MCD}(20, 5) = \text{MCD}(5, 0)$ $b=0; r=0$

18. Dimostrare il seguente

Dati $a, b \in \mathbb{N}$ non entrambi uguali a 0, se esistono $h, k \in \mathbb{Z}$ tali che $a \cdot h + b \cdot k = 1$ allora $\text{MCD}(a, b) = 1$.

$$a \cdot h + b \cdot k = 1 \Rightarrow \text{MCD}(a, b) = 1$$

$$d = \text{MCD}(a, b); \quad d | a \in d | b$$

\rightarrow ALLORA $d | ah + bk$

UNICO DIVISORE POSITIVO DI 1 È 1

19. Dimostrare che i numeri primi sono infiniti.

SUPPONGO PER ASSURDO CHE SIANO FINITI E QUINDI $\exists m$: I NUMERI PRIMI SIANO $p_1 = 2, p_2 = 3, \dots, p_m$.

CONSIDERO ALLORA I NUMERI POSITIVI

$$h = p_1 \cdot p_2 \cdot \dots \cdot p_m \in k = p_1 \cdot p_2 \cdot \dots \cdot p_m + 1$$

h e k essendo il secondo il successore del primo, SONO COMMI.

NOTIAMO CHE k NON PUÒ ESSERE PRIMO PERCHÉ È DIVERSO DA $p_1 = 2, p_2 = 3, \dots, p_m$ CHE ABBIAMO SUPPOSTO ESSERE TUTTI I NUMERI PRIMI. SE NON È PRIMO, DAL TEOREMA SULLA FATTORIZZAZIONE SAPPIAMO CHE k SI PUÒ SCRIVERE IN MODO UNICO COME PRODOTTO DI PRIMI POSITIVI. MA QUESTI PRIMI POSITIVI DEVONO ESSERE COMPRESI TRA $p_1 = 2, p_2 = 3, \dots, p_m$ E QUINDI NON SAREBBERE COPRIMO CON h .

20. Descrivere il funzionamento del Crivello di Eratostene

IL CRIVELLO DI ERATOSTENE È USATO SE ABBIANO LA NECESSITÀ DI CALCOLARE TUTTI I NUMERI PRIMI $\leq m$.

- 1) COSTRUISCO UNA TABELLA CON TUTTI I NUMERI DA 2 A m .
- 2) INIZIANDO A TAGLIARE TUTTI I MULTIPLI DI 2 DALLA TABELLA (NON 2).
- 3) Poi tolgo tutti i multipli di 3, 5, 7 (ma non 3, 5, 7).
- 4) Dopo aver cancellato tutti i multipli del numero più grande che sia $\leq \sqrt{m}$ CI FERMATEO.

21. Dimostrare che la relazione di congruenza è una relazione di equivalenza

DIMOSTRAZIONE: **RIFLESSIVA:** $\forall a \in \mathbb{Z}$ è vero che $a \equiv a \pmod{m}$? SÌ, PERCHÉ $0 = a - a$ È MULTIPLO DI m (POICHE' 0 È MULTIPLO DI QUALUNQUE NUMERO).

SIMMETRICA: SE $a \equiv b \pmod{m}$ ALLORA $a - b = km$ PER QUALCHE $k \in \mathbb{Z}$ E QUINDI, MOLTIPLICANDO PER -1 OTTENIAMO $b - a = (-k)m$ OSSIA $b \equiv a \pmod{m}$.

TRANSITIVA: SE $a \equiv b \pmod{m}$ E $b \equiv c \pmod{m}$ $\exists l, k \in \mathbb{Z}$: $a - b = lm$ E $b - c = km$. SOMMANDO MEMBRI A MEMBRI OTTENIAMO: $a - c = (l+k)m$ E QUINDI $a \equiv c \pmod{m}$.

22. Dimostrare che dato $m \in \mathbb{N}$ e dati $a, b \in \mathbb{Z}$ tali che $a \equiv b \pmod{m}$, allora comunque prendiamo $c, d \in \mathbb{Z}$ tali che $c \equiv d \pmod{m}$ abbiamo

$$a + c \equiv b + d \pmod{m}$$

$$a \equiv b \pmod{m}$$

$$\Rightarrow a + c \equiv b + d \pmod{m}$$

$$c \equiv d \pmod{m}$$

DIM. PER IP. $\exists k_1, k_2 \in \mathbb{Z} : a - b = k_1 m$
 $c - d = k_2 m$

QUINDI $(a + c) - (b + d) = (a - b) + (c - d) = (k_1 + k_2)m$

CHE DIMOSTA LA PROPRIETA'

23. Dimostrare che dato $m \in \mathbb{N}$ e dati $a, b \in \mathbb{Z}$ tali che $a \equiv b \pmod{m}$, allora comunque prendiamo $c, d \in \mathbb{Z}$ tali che $c \equiv d \pmod{m}$ abbiamo

$$a \cdot c \equiv b \cdot d \pmod{m}$$

ABBIAMO $a = b + k_1 m$

$$c = d + k_2 m$$

QUINDI $ac - bd = (b + k_1 m)(d + k_2 m) - bd =$

$$= bk_2 m + dk_1 m + k_1 k_2 m^2 =$$

$$= (bk_2 + dk_1 + k_1 k_2 m) m$$

CHE DIMOSTA LA PROPRIETA'

24. Dare la definizione della funzione ϕ di Eulero, e la formula generale per il calcolo di $\phi(n)$ per ogni intero n .

SIA m UN INTERO POSITIVO $m > 0$, VOGLIO CONTARE QUANTI SONO I NUMERI CHE PRECEDONO m E CHE SIANO COPRIMI CON m .

$$\phi(m) = |\{x : x \in \mathbb{N}, 0 < x \leq m \text{ e } \text{MCD}(m, x) = 1\}|$$

25. Cosa afferma il Teorema di Eulero riguardo all'applicazione della funzione ϕ al calcolo della esponenziazione modulare?

IL TEOREMA DI EULERO MOSTRA COME LA FUNZIONE ϕ DI EULERO SI POSSA APPLICARE ALLA ESPONENZIAZIONE MODULARE, E AFFERMA CHE:
SIANO $m, n > 0$, SE $\text{MCD}(m, n) = 1$ ALLORA $n^{\phi(m)} \equiv 1 \pmod{m}$

26. Come si definisce l'inverso di un intero n modulo m e quando esiste?

SIANO $a, b \in \mathbb{N}$, $a, b \geq 0$. ALLORA ESISTE $x \in \mathbb{N}$: $a \cdot x \equiv 1 \pmod{b} \iff a$ e b SONO COPRIMI.
L'ELEMENTO x , DENOTATO CON $a^{-1} \pmod{b}$ O a^{-1} VIENE DETTO "INVERSO DI a MODULO b ".

27. Quali sono i numeri perfetti e come sono collegati ai numeri primi di Mersenne?

- I NUMERI PRIMI DI MERSENNE SONO NUMERI PRIMI DELLA FORMA $M_p = 2^p - 1$
 $M_2 = 2^2 - 1 = 3$, $M_3 = 2^3 - 1 = 7$, $M_5 = 2^5 - 1 = 31$, $M_7 = 2^7 - 1 = 127$, $M_{13} = 2^{13} - 1 = 8191$
 MA NON PERDERSI $M_{11} = 2^{11} - 1 = 2047$ NON È PRIMO
- CONSIDERO LA FUNZIONE SIGMA DATO $m \in \mathbb{N}$ $\sigma(m) = \sum_{\text{divisori di } m} d$
 SOMMA DI TUTTI I DIVISORI POSITIVI DI m .
- $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 9$, $\sigma(4) = 7$, $\sigma(5) = 6$, $\sigma(6) = 12$
- UN NUMERO $m \in \mathbb{N}$ SI DICE PERFETTO SE $\sigma(m) = 2m$
 $6 = 1 + 2 + 3$ $\sigma(6) = 1 + 2 + 3 + 6 = 12$
 $28 \dots$
 $496 \dots$

I NUMERI PERFETTI PARI SONO LEGATI AI PRIMI DI MERSENNE PERCHÉ
 $2^m - 1$ È UN NUMERO PRIMO, ALLORA $2^{m-1} \cdot (2^m - 1)$ È PERFETTO.
 INFATTI $6 = 2^1 \cdot (2^2 - 1)$, $28 = 2^{3-1} \cdot (2^3 - 1)$, $496 = 2^{5-1} \cdot (2^5 - 1)$

28. Descrivere la Congettura di Collatz.

LA CONGETTURA LEGA LA TEORIA DEI NUMERI AD UN PROBLEMA DI TERMINAZIONE DI UN ALGORITMO ITERATIVO.

L'ALGORITMO È BASATO SULLA SEGUENTE FUNZIONE

$$f(m) = \begin{cases} 1 & \text{SE } m=1 \\ m/2 & \text{SE } m \in \text{PARI} \\ 3m+1 & \text{SE } m \in \text{DISPARI} \end{cases}$$

L'ALGORITMO È IL SEGUENTE:

```
LEGGI UN INTEGO  $x \geq 1$ 
WHILE ( $x > 1$ ) DO
    IF  $x \bmod 2 = 0$   $x = x/2;$ 
    ELSE  $x = 3 \cdot x + 1;$ 
END - WHILE
```

IL PROBLEMA È: L'ALGORITMO SI FERMA SEMPRE OPPURE $\exists x$ PARTENDO DAL QUALE NON SI RAGGIUNGE MAI IL VALORE 1?

AD OGGI, LA CONGETTURA È STATA VERIFICATA PER TUTTI GLI $m < 10^{18}$

PARTE 3: 23-41

29. Dati due insiemi A e B , con $|A| = k$, $|B| = n$ quante sono le applicazioni di A in B ?

NUMERO DELLE DISPOSIZIONI CON RIPETIZIONE DI m ELEMENTI DI CLASSE K : DENOTATO CON $F_{m,k}$

$$F_{m,k} = m^k$$

$$\text{es: } F_{2,2} = 2^2$$

30. Dati due insiemi A e B , con $|A| = k$, $|B| = n$ quante sono le applicazioni iniettive di A in B ?

NUMERO DELLE DISPOSIZIONI SEMPLICI DI m ELEMENTI DI CLASSE K : DENOTATO CON $D_{m,k}$

$$D_{m,k} = m \cdot (m-1) \cdot \dots \cdot (m-k+1)$$

$$\text{es: } D_{50,41} = 50 \cdot 49 \cdot \dots \cdot 40 \approx 1,5 \cdot 10^{18}$$

31. Dato un insieme B , con $|B| = n$, e preso un intero $k \leq n$, quanti sono i sottoinsiemi di B composti di k elementi?

NUMERO DELLE COMBINAZIONI DI m ELEMENTI DI CLASSE K : DENOTATO CON $C_{m,k}$

$$C_{m,k} = \frac{m \cdot (m-1) \cdots (m-k+1)}{k!} = \frac{D_{m,k}}{k!} = \binom{m}{k}$$

32. Enunciare e dimostrare il Teorema binomiale (formula di Newton).

È UNA FORMULA CHE CONSENTE DI ELEVARE A UNA QUALESiasi POTENZA UN BINOMIO.

SIANO $a, b \in \mathbb{R}$ $(a+b)^m = \sum_{k=0}^m \binom{m}{k} a^{m-k} \cdot b^k$

DIM. LA POTENZA $(a+b)^m$ È IL PRODOTTO DI m FATTORI TUTTI uguali a $(a+b)$.
 $(a+b) \cdot (a+b) \cdots \cdot (a+b)$

OTTENIAMO UNA SOMMA DI MONOMI TUTTI DI GRADO m IN a e b DEL TIPO $a^{m-k} b^k$
CON $0 \leq k \leq m$.

IN PARTICOLARE, I MONOMI $a^m b^0 = a^m$ E $a^0 b^m = b^m$ COMPARIRANNO NELLA SOMMA
UNA SOLA VOLTA, ESATTAMENTE QUANDO IL OGNI FATTORE PRENDIAMO a o b .
QUANTE VOLTE COMPARÉ NELLA SOMMA IL MONOMIO $a^{m-1} b^1$? TANTE VOLTE
QUANTI SONO I MODI DI SCEGLIERE $m-1$ DEGLI m FATTORI, DA CUI
SCEGLIERE a PER SVILUPPARE IL PRODOTTO. OVVERO $\binom{m}{m-1} = m-1$.

IN GENERALE, IL MONOMIO $a^{m-k} b^k$ COMPARÉ TANTE VOLTE QUANTI SONO
I MODI DI SCEGLIERE $m-k$ DEGLI m FATTORI DA CUI SCEGLIERE a PER
SVILUPPARE IL PRODOTTO. OVVERO $\binom{m}{k}$.

33. Cosa afferma il Principio dei cassetti, detto anche principio del buco della piccionaia (in inglese Pigeonhole principle)?

IL PRINCIPIO AFFERMA CHE SE DOBBIANO FAR ENTRARE $m+1$ PICCIONI IN UNA PICCIONAIA CHE CONTIENE m CASSETTE, ALLORA ALMENO UNA CASSETTA DOVRÀ CONTENERE PIÙ DI UN PICCIONE.

34. Quali sono gli assiomi della Teoria della Probabilità ?

SIANO $A \in B$ DUE EVENTI QUALSIASI.

$$A_1 \quad 0 \leq P(A) \leq 1$$

$$A_2 \quad P(S) = 1 \in P(\emptyset) = 0$$

$$A_3 \quad P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

35. Quando due eventi si dicono indipendenti ?

DUE EVENTI SI DICONO INDEPENDENTI SE

- $P(A|B) = P(A)$
- $P(B|A) = P(B)$

QUINDI SE $A \in B$ SONO INDEPENDENTI $P(A \cap B) = P(A) \cdot P(B)$

DEFINIZIONE:
PROBABILITÀ DI A, CONDIZ. AL VERIFICARSI DI B
 \downarrow
 $P(A|B) = \frac{P(A \cap B)}{P(B)}$

36. Cosa dice la Regola di Bayes ?

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \text{ OVVERO } P(A|B) \cdot P(B) = P(A \cap B)$$

$$\Rightarrow P(A \cap B) = P(B \cap A)$$

$$P(B|A) = \frac{P(B \cap A)}{P(A)} \text{ OVVERO } P(B|A) \cdot P(A) = P(B \cap A)$$

Regola di Bayes: $P(B|A) = \frac{P(A|B) \cdot P(B)}{P(A)}$

ES: $P(E) = \frac{1}{10}$, $P(S) = \frac{4}{10}$ e $P(S|E) = \frac{7}{10}$

$$P(E|S) = \frac{P(S|E) \cdot P(E)}{P(S)} = \frac{\frac{7}{10} \cdot \frac{1}{10}}{\frac{4}{10}} = \frac{7}{40}$$

37. Enunciare e dimostrare il Teorema della Probabilità Totale.

SIA A UN EVENTO E SIANO B_1, B_2, \dots, B_m M EVENTI MUTUAMENTE ESCLUSIVI, TALI CHE $P(B_i) \neq 0 \forall i$ ED INOLTRE $P(B_1 \vee B_2 \vee \dots \vee B_m) = 1$, OVVERO GLI EVENTI SONO ESAUSTIVI.

$$\text{ALLORA } P(A) = P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + \dots + P(A|B_m)P(B_m) =$$

$$= \sum_{i=1}^m P(A|B_i)P(B_i)$$

DIM. DAL MOMENTO CHE GLI EVENTI B_1, B_2, \dots, B_m SONO ESAUSTIVI, ALMENO UNO DI LORO SI DEVE VERIFICARE.

QUINDI SE A SI VERIFICA, CI SARÀ UN EVENTO B_j TALE CHE ANCHE B_j SI VERIFICA.

DAL MOMENTO CHE GLI EVENTI B_i SONO MUTUAMENTE ESCLUSIVI ABBIANO

$$P(A) = P(A \wedge B_1) + \dots + P(A \wedge B_m)$$

DALLA DEFINIZIONE DI PROBABILITÀ CONDIZIONATA ABBIANO PER OGNI i

$$P(A \wedge B_i) = P(A|B_i) \cdot P(B_i)$$

E UTILIZZANDO TALE UGUALANZA SI COMPLETA LA DEMOSTRAZIONE.

38. Classificare il problema delle estrazioni da un'urna.

LE ESTRAZIONI DA UN'URNA SI POSSANO CLASSIFICARE IN 4 MODI, COMBINANDO I SEGUENTI 2 CRITERI:

- ESTRAZIONI ORDINATE OPPURE NO. OVVERO, SE L'ORDINE DI ESTRAZIONE DELLE PALLINE È IMPORTANTE OPPURE NO.
- ESTRAZIONI CON REINSERIMENTO OPPURE NO. OVVERO, SE AD OGNI ESTRAZIONE DI UNA PALLINA, LA PALLINA ESTRATTA VIENE REINSERITA NELL'URNA.

SUPPONIAMO DI ESTRARRE k PALLINE DA UN'URNA CONTENENTE m PALLINE.

NEI 4 CASI POSSIBILI, IL NUMERO TOTALE È

- $D_{m,k}^{\circ} = m^k$ OVVERO NUMERO DELLE DISPOSIZIONI CON RIPETIZIONE, SE L'ORDINE È IMPORTANTE E LA PALLINA, DOPO OGNI ESTRAZIONE, VIENE REINSERITA NELL'URNA.
- $D_{m,k} = m \cdot (m-1) \cdots (m-k+1)$ OVVERO NUMERO DELLE DISPOSIZIONI SEMPLICI, SE L'ORDINE È IMPORTANTE MA LA PALLINA ESTRATTA NON VIENE REINSERITA NELL'URNA.
- $C_{m,k} = \binom{m}{k} = \frac{m!}{k!(m-k)!}$ OVVERO COMBINAZIONI SEMPLICI, SE L'ORDINE NON È IMPORTANTE E LA PALLINA ESTRATTA NON VIENE REINSERITA NELL'URNA.
- $C_{m,k}^2 = \frac{(m+k-1)!}{k!(m-1)!}$ OVVERO NUMERO COMBINAZIONI CON RIPETIZIONE SE L'ORDINE NON È IMPORTANTE E LA PALLINA ESTRATTA VIENE REINSERITA NELL'URNA.

39. Cos'è una variabile casuale e come è definito il suo valore medio o valore atteso?

- UNA VARIABILE CASUALE È UNA FUNZIONE X CHE ASSOCIA UN NUMERO REALE AD UN EVENTO. DEFINIAMO QUINDI UN EVENTO COME IL FATTO CHE LA VARIABILE X ASSUME UN VALORE x OVVERO $X = x$.
- POSSIAMO ALLORA DEFINIRE IL CONCETTO DI VALORE MEDIO O VALORE ATTESO DI UNA VARIABILE CASUALE X COME

$$E[X] = \sum_x x \cdot P[X=x]$$

ES: SE LA VARIABILE CASUALE X CONTIENE IL VALORE OTTENUTO DOPO IL LANCIO DI UN DADO ABBIANO CHE

$$E[X] = \sum_x x \cdot P[X=x] = 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} = \frac{21}{6} = 3,5$$

40. Descrivere la prova di Bernoulli.

LA PROVA DI BERNOULLI (O PROVA BINOMIALE) È UN ESPERIMENTO PROBABILISTICO CHE HA ESATTAMENTE 2 RISULTATI: SUCCESSO O FALLIMENTO.

- ABBIANO QUINDI UN ESPERIMENTO CON 2 USCITE:
 - SUCCESSO CON PROBABILITÀ p
 - INSUCCESSO CON PROBABILITÀ $q = 1 - p$
- TUTTI I TENTATIVI SONO INDIPENDENTI L'UNO DALL'ALTRO E
- LA PROBABILITÀ DI SUCCESSO RIMANE COSTANTE p
- SE X È LA VARIABILE CASUALE CHE TIENE CONTO DEL NUMERO DI TENTATIVI, ABBIANO

$$E[X] = 1 \cdot p + 2 \cdot q \cdot p + 3 \cdot q^2 \cdot p + \dots = \sum_{k=1}^{\infty} k \cdot q^{k-1} \cdot p = \frac{p}{q} \sum_{k=0}^{\infty} k \cdot q^k$$

- SUPPONIAMO DI ESSERE BRANI A CALCOLARE SOMMATORIE INFINITE ED OTTENIAMO

$$\sum_{k=0}^{\infty} k \cdot q^k = \frac{q}{(1-q)^2} \quad \text{POICHÉ PER } q < 1 \quad \sum_{k=0}^{\infty} q^k = \frac{1}{1-q}$$

- QUINDI, IL VALORE ATTESO DEI NUMERI DI TENTATIVI DA FARE PER OTTENERE "SUCCESSO" È $E[X] = \frac{p}{q} \cdot \frac{q}{(1-q)^2} = \frac{p}{q^2} = \frac{1}{p}$
- NE segue che minore è la probabilità dell'evento successo, maggiore è il numero di tentativi che bisogna fare. ES. numero atteso di lanci di una moneta per avere testa? $\frac{1}{1/2} = 2$

41. Descrivere il Paradosso dei 3 prigionieri e la sua soluzione.

- IL PARADOSSO E' IL SEGUENTE:

- "CI SONO 3 CONDANNATI A MORTE, A, B, C, CHIUSI IN 3 CELLE SEPARATE. IL RE HA DECISO DI GRAZIARNE UNO, CHE HA SCELTO A CASO. IL CARCERIERE SA CUI DEI 3 SARÀ GRAZIATO MA NON PUÒ RIVELARNE IL NOME. A PARLA CON IL CARCERIERE E LO IMPLORA DI DIRGLI CUI, TRA B O C, SARÀ GIUSTIZIATO. GLI DICE: "SE B SARÀ GRAZIATO ALLORA DAMMI IL NOME DI C, SE INVECE SARÀ C AD ESSERE GRAZIATO DAMMI IL NOME DI B. SE INVECE DOVESSI ESSERE IO AD ESSERE GRAZIATO, ALLORA SCEGLINE UNO A CASO TRA B E C." "

- "IL CARCERIERE DICE AD A CHE B SARÀ GIUSTIZIATO. A È CONTENTO PERCHÉ RITIENE CHE A QUESTO PUNTO LA PROBABILITÀ DI ESSERE GRAZIATO SIA CAMBIATA DA $1/3$ A $1/2$ PERCHÉ ADesso È TRA LUI E C. DURANTE L'ORA D'ARIA DEI PRIGIONIERI, DÀ LA NOTIZIA IN SEGRETTO A C. C È MOLTO CONTENTO PERCHÉ PENSA CHE LA PROBABILITÀ DI A DI ESSERE GRAZIATO SIA RIMASTA $1/3$ MENTRE LA SUA $2/3$."

- QUALE DEI 2 PRIGIONIERI HA RAGIONE? O HANNO TORTO ENTRAMBI?

- PRIMA DELLA RISPOSTA DEL CARCERIERE, A SA CHE LA SUA PROBABILITÀ DI ESSERE GRAZIATO È $P(A) = 1/3$ CHE È LA STESSA PROBABILITÀ CHE HANNO GLI ALTRI 2 PRIGIONIERI

- QUALI SONO GLI SCENARI CHE PORTANO IL CARCERIERE A DIRE CHE B SARÀ GIUSTIZIATO?
 - 1) SICURAMENTE SE C È GRAZIATO ($\frac{1}{3}$). QUINDI SCENARIO 1 HA PROBABILITÀ GLOBALE $1/3$
 - 2) CON PROBABILITÀ $1/2$ SE È A AD ESSERE GRAZIATO ($\frac{1}{3}$). QUINDI 2) HA PROBABILITÀ GLOBALE $1/6$
- E NOTIAMO CHE LA PROBABILITÀ CHE IL CARCERIERE DICA AD A CHE B SARÀ GIUSTIZIATO È LA SOMMA DELLE 2 PROBABILITÀ SOPRA, QUINDI $1/2$

- NE CONCLUDIAMO CHE UNA VOLTA ACCERTATO CHE B SARÀ GIUSTIZIATO, LA PROBABILITÀ CHE C SIA GRAZIATO È IL DOPPIO DELLA PROBABILITÀ CHE A SIA GRAZIATO.
- QUINDI, $P(A) = 1/3 \in P(C) = 2/3$.

- POSSIAMO ANCHE DEMOSTRARE QUANTO DETTO UTILIZZANDO LA REGOLA DI BAYES. SE INDICHINO CON b, c RISPECTIVAMENTE GLI EVENTI "CARCERIERE DICE AD A CHE B/C SARÀ GIUSTIZIATO", CALCOLIAMO $P(A|b)$.

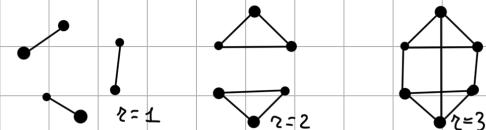
- LA REGOLA DI BAYES DICE CHE: $P(A|b) = \frac{P(b|A) \cdot P(A)}{P(b)} = \frac{\frac{1}{2} \cdot \frac{1}{3}}{\frac{1}{2}} = \frac{1}{3}$

- QUINDI LA PROBABILITÀ CHE A SIA GRAZIATO NON È CAMBIATA, E QUINDI, DAL MOMENTO CHE B SARÀ GIUSTIZIATO, LA PROBABILITÀ CHE C SIA GRAZIATO È DIVENTATA $2/3$.

42. Enunciare il Teorema sui grafi detto Handshaking Theorem.

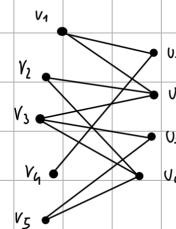
SIA $G = (V, E)$ UN GRAFO NON ORIENTATO, ALLORA LA SOMMA DEI GRADI DI OGNI VERTICE È UGUALE AL DOPPIO DEL NUMERO DEGLI ARCHI, OSSIA $2|E|$.

43. Dare la definizione di grafo regolare



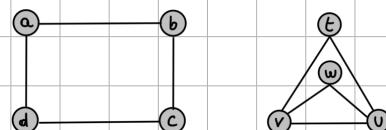
SIA $G = (V, E)$ UN GRAFO NON ORIENTATO. SE I VERTICI DEL GRAFO HANNO TUTTI LO STESSO GRADO r ALLORA DICHIAMO CHE G È REGOLARE DI GRADO r . $|V| = \frac{2|E|}{r}$. SE r È DISPARI ALLORA $|V|$ È PARI, OVVERO UN GRAFO REGOLARE DI GRADO DISPARI MA UN NUMERO PARI DI VERTICI.

44. Dare la definizione di grafo bipartito



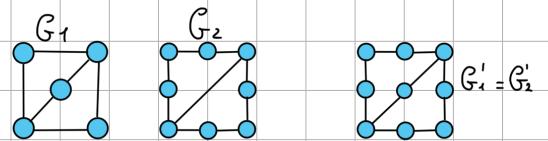
SIA $G = (V, E)$ UN GRAFO NON ORIENTATO. DICHIAMO CHE G È BIPARTITO SE POSSIAMO PARTIZIONARE L'INSIEME DEI VERTICI IN 2 INSIEMI, V_1 E V_2 IN MANIERA TALE CHE TUTTI GLI ARCHI DI G HANNO COME ESTREMI UN VERTICE IN V_1 E L'ALTRO VERTICE IN V_2 .

45. Dare la definizione di Isomorfismo tra grafi.



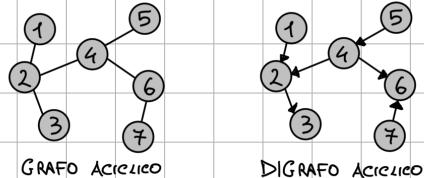
2 GRAFI, SIA ENTRAMBI ORIENTATI CHE ENTRAMBI NON ORIENTATI, $G_1 = (V_1, E_1) \in G_2 = (V_2, E_2)$ SI DICONO ISOMORFI SE ESISTE UNA APPLICAZIONE BIUNIVOCAMENTE DALL'INSIEME DEI VERTICI V_1 NELL'INSIEME DEI VERTICI V_2 TALE CHE $(f(u), f(v))$ È UN ARCO DI E_2 SE E SOLO SE (u, v) È UN ARCO DI E_1 . LA BIIEZIONE f È DETTA ISOMORFISMO.

46. Dare la definizione di Omeomorfismo tra grafi.



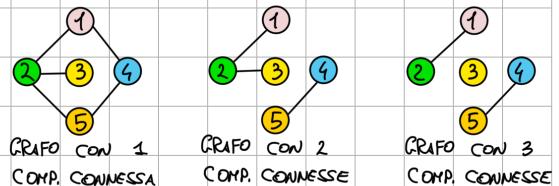
2 GRAFI NON ORIENTATI, $G_1 = (V_1, E_1)$ E $G_2 = (V_2, E_2)$ SI DICONO OMEOMORFI SE ATTRAVERSO UNA SERIE DI SUDDIVISIONI DI ARCHI DI G_1 E G_2 SI POSSANO OTTENERE 2 GRAFI G'_1 E G'_2 CHE SONO ISOMORFI.

47. Dare la definizione di grafo aciclico, sia nel caso di grafo orientato che nel caso di grafo non orientato



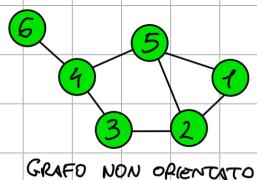
UN GRAFO (DIGRAFO) $G = (V, E)$ SI DICE ACICLICO SE NON POSSIENE CICLI.

48. Dare la definizione di componente connessa di un grafo



SIA $G = (V, E)$ UN GRAFO E SIA $V = V_1 \cup V_2 \cup \dots \cup V_k$ LA PARTIZIONE INDOTTA DALLA RELAZIONE DI CONNESSIONE TRA I VERTICI. SIA $G_i = (V_i, E_i)$ IL SOTTOGRAFO INDOTTO DA V_i PER OGNI $i = 1, \dots, k$. TALI SOTTOGRAFI SI CHIAMANO COMPONENTI CONNESSE DI G .

49. Descrivere e confrontare le 2 rappresentazioni di un grafo



- MATRICE
- SUPPONIAMO ALLORA CHE $V = \{1, 2, \dots, m\}$. COSTRUIAMO UNA MATAICE QUADRATA $M_{m \times m}$ COSÌ FATTA
 - $M_{i,j} = 1$ SE I VERTICI $i \in j$ SONO CONNESSI DA UN ARCO
 - $M_{i,j} = 0$ SE I VERTICI $i \in j$ NON SONO CONNESSI DA UN ARCO
 - M DI UN GRAFO NON ORIENTATO È SIMMETRICA $\Rightarrow M_{i,j} = M_{j,i}$
 - ASSOCIAMO AL GRAFO UNA LISTA (ARRAY) DI DIM. m , OSSIA IL NUMERO DEI NODI, ED OGNI ELEMENTO DELLA LISTA È A SUA VOLTA UNA LISTA DOVE METTIAMO TUTTI I VERTICI COLLEGATI AL VERTICE CORRISPONDENTE. NELL'ES. LA LISTA HA $m+1$ VALORI
 - MENO MEMORIA, PERO' NELLA MATRICE IL TEMPO DI VERIFICA È COSTANTE, NELLA LISTA NON È COSTANTE, SI FANNO FINO A m CONTROLLI.
- LIS
- | | | | | | |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| 2 | 1 | 2 | 3 | 1 | 4 |
| 5 | 3 | 4 | 5 | 2 | |
| 5 | 6 | 4 | | | |
- LISTE DI ADIACENZA

0	1	0	0	1	0
1	0	1	0	1	0
0	1	0	1	0	0
0	0	1	0	1	1
1	1	0	1	0	0
0	0	0	1	0	0

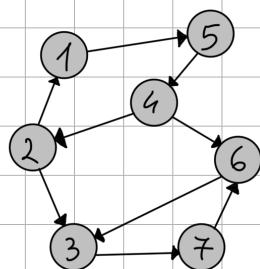
MATRICE DI ADIACENZA

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓
2	1	2	3	1	4
5	3	4	5	2	
5	6	4			

LISTE DI ADIACENZA

50. Dato un grafo (digrafo) $G = (V, E)$ e la sua matrice di adiacenza M , come facciamo a trovare il numero di percorsi di lunghezza $k \geq 1$ per ogni coppia di vertici i e j ?

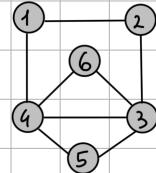
SIA DATO UN GRAFO (DIGRAFO) $G = (V, E)$ E SIA M LA SUA MATRICE DI ADIACENZA.
IL NUMERO DI PERCORSI DI LUNGHEZZA $k \geq 1$ PER OGNI COPPIA DI VERTICI $i \in j$ È DATO
DAL VALORE DELLA MATAICE $M^k[i, j]$



$$M = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

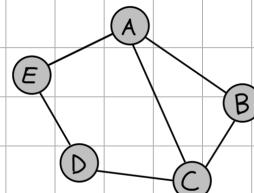
$$M^4 = \begin{bmatrix} 1 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

51. Dare la definizione di circuito Euleriano.



1 - 2 - 3 - 5 - 4 - 3 - 6 - 4 - 1

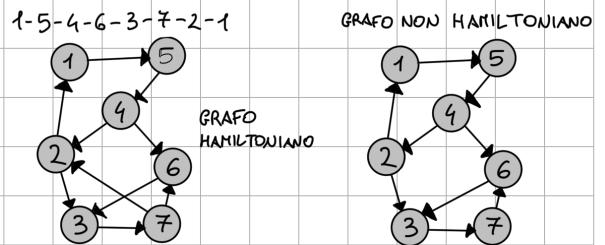
52. Dato un grafo $G = (V, E)$, cosa afferma il Teorema di Eulero riguardo all'esistenza nel grafo di un cammino euleriano?



A - B - C - D - E - A - C

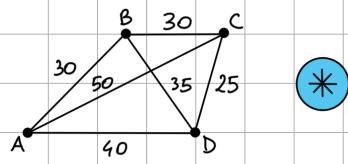
UN GRAFO $G = (V, E)$ POSSIEDE UN CAMMINO EURELIANO SE E SOLO SE È CONNESSO ED I SUOI VERTICI, TRANNE MASSIMO 2 HANNO TUTTI GRADO PARI. I DUE VERTICI DI GRADO DISPARI, SARANNO IL PRIMO E L'ULTIMO VERTICE DEL CAMMINO.

53. Dare la definizione di cammino Hamiltoniano.



SIA $G = (V, E)$ UN GRAFO (DGRAFO) CONNESSO. UN CAMMINO HAMILTONIANO DI G È UN CIRCUITO CHE PASSA UNA ED UNA SOLA VOLTA PER TUTTI I VERTICI DI G . SE IL CAMMINO È CHIUSO, OVVERO SE È UN CICLO, TALE CICLO SI DICE CICLO HAMILTONIANO. UN GRAFO SI DICE HAMILTONIANO, SE POSSIEDE UN CICLO HAMILTONIANO.

54. Definire il problema del commesso viaggiatore, conosciuto con l'abbreviazione TSP (Traveling Salesman Problem).



- È CARATTERIZZATO DAL PROBLEMA DI TROVARE UN CIRCUITO HAMILTONIANO CHE MINIMIZZA IL COSTO (DISTANZA) TOTALE PER UN GRAFO PESATO, DOVE AD OGNI ARCO È ASSOCIAUTO UN PESO POSITIVO.

- * SE UN COMMESO VIAGGIATORE DEVE ATTRAVERSARE TUTTI I NODI, PARTENDO DA A E TORNANDO AD A, QUAL È IL PERCORSO CHE MINIMIZZA IL COSTO TOTALE?

- POSSIAMO RISOLVERE IL PROBLEMA ANALIZZANDO TUTTI I CIRCUITI HAMILTONIANI.

$$- ABCDA \Rightarrow 30 + 30 + 25 + 40 = 125$$

$$- ABDCA \Rightarrow 30 + 35 + 25 + 50 = 140$$

$$- ACBDA \Rightarrow 50 + 30 + 35 + 40 = 155$$

$$- ACDBA \Rightarrow 50 + 25 + 35 + 30 = 140$$

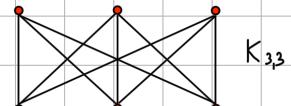
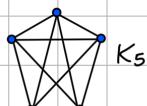
$$- ADBCA \Rightarrow 40 + 35 + 30 + 50 = 155$$

$$- ADCBA \Rightarrow 40 + 25 + 30 + 30 = 125$$

→ E CON 30 VERTICI? $2^{30} \approx 4,42 \cdot 10^{30}$ CAMMINI

✗ UNA SOLUZIONE COMPUTAZIONALMENTE SEMPLICE

55. Cosa afferma il Teorema di Kuratowski riguardo alla planarità di un grafo?



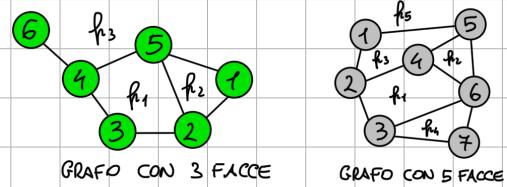
UN GRAFO È PLANARE SE E SOLO SE NON CONTIENE ALCUN SOTTOGRAFO CHE SIA OMOMORFO A K_5 O A $K_{3,3}$.

56. Qual è il numero massimo di archi che un grafo planare con n vertici può avere?

Se $G = (V, E)$ è un grafo connesso e planare, se $|V| \geq 3$ allora $|E| \leq 3|V| - 6$.

Se $|V| > 3$ e non ci sono cicli di lunghezza 3 allora $|E| \leq 2|V| - 4$.

57. Come sono legati il numero di vertici, archi e facce di un grafo planare? Ovvero cosa ci dice la formula di Eulero?

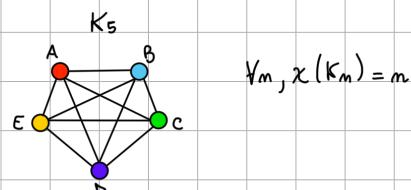


SE INDICHIAMO CON "v" IL NUMERO DEI VERTICI, "e" IL NUMERO DEGLI ARCHI E CON "f" IL NUMERO DELLE FACCCE, SIA $G = (V, E)$ UN GRAFO PLANARE CONNESSO, $v - e + f = 2$ (FORMULA DI EULERO).

58. Se G è un grafo connesso e aciclico, quanti archi ha?

SIA $G = (V, E)$ UN GRAFO CONNESSO E ACICLICO, $|E| = |V| - 1$.

59. Quand'è che un grafo si dice k -colorabile e come è definito il numero cromatico di un grafo?



- UN GRAFO È k -COLORABILE SE È POSSIBILE COLORARE I SUOI VERTICI, UTILIZZANDO AL PIÙ k COLORI.
- IL NUMERO CROMATICO DI UN GRAFO G , $\chi(G)$ È IL NUMERO MINIMO DI COLORI NECESSARI PER COLORARE IL GRAFO.

60. Cosa afferma il Teorema di Brooks riguardo al numero cromatico di un grafo?

• NELLA VERSIONE FORTE G SE NON È UN GRAFO COMPLETO E NON È UN CYCLO SEMPLICE CON $|V|$ DISPARI, $\chi(G) \leq \Delta$

SIA $G = (V, E)$ UN GRAFO CONNESSO CON m VERTICI, E SIANO $\delta_1 \geq \delta_2 \geq \dots \geq \delta_m$ I GRADI DEI VERTICI DEL GRAFO IN ORDINE DECREScente. ALLORA $\chi(G) \leq \Delta + 1$.

$\Delta \rightarrow$ GRADO VERTICE PIÙ ALTO