APPUNTI DI MATEMATICA DISCRETA (MODULO DI STRUTTURE DISCRETE)

# Corso di laurea in Informatica L-31 2019/2020

# Università degli studi di Catania

SAMUELE GALLINA

MODULO DI “STRUTTURE DISCRETE”

INSIEMI

Un insieme in matematica è definito come una collezione di oggetti. Gli oggetti dunque possono appartenere o non appartenere a un insieme

Esempio:

* a ∈ A significa che a appartiene all’insieme A
* a ∉ A significa che a non appartiene all’insieme A

DEFINIZIONE:

Due insiemi A e B sono uguali se tutti gli elementi di A sono contenuti in B e viceversa, in simboli si scrive: A ⊆ B AND B ⊆ A ,la prima scritta vuol dire “tutti gli elementi di A sono in B”, la seconda vuol dire “tutti gli elementi di B sono in A”, dunque: A=B 🡸🡺 A ⊆ B AND B ⊆ A

DEFINIZIONE:

* “SINGOLETTO” : insieme che contiene un solo elemento come ad esempio {a}
* “ ⊘ “ : insieme vuoto ,ovvero insieme che non contiene nemmeno un elemento

DEFINIZIONE:

CARDINALITA’ : numero degli elementi di un insieme: insieme A, cardinalità di A 🡺 |A| , se per esempio A ha 4 elementi segue che |A|=4

DEFINIZIONE:

INSIEME DISCRETO:

Insieme ordinato tale che tra due elementi successivi dell’insieme non ce ne sia un altro. Ogni insieme finito è discreto, anche l’insieme vuoto.

INSIEMI PIU’ IMPORTANTI:

* N: insieme dei naturali N={0,1,2,3…}
* Z: insieme degli interi relativi Z={… -2,-1,0,1,2,3…}
* Q: insieme dei razionali Q={n/m | n,m ∈ Z}
* R: insieme dei reali R={x | x razionale o irrazionale}
* C: insieme dei complessi C={x | x reale o immaginario}

Vale la relazione : N ⊂ Z ⊂ Q ⊂ R ⊂ C N e Z sono insiemi discreti, Q ne discreto ne continuo, R e C continui

## Operazioni

Unione:

* A ꓴ B = {x | x ∈ A oppure x ∈ B} , operazione commutativa e associativa

Intersezione:

* A ꓵ B ={x | x ∈ A e x ∈ B} , operazione commutativa e associativa

DEFINIZIONE

Due insiemi si dicono congiunti se hanno almeno un elemento in comune, disgiunti se no

PROPRIETA’

* A ꓵ A = A = A ꓴ A
* A ꓵ ( B ꓴ C ) = (A ꓵ B) ꓴ (A ꓵ C)
* A U ( B ꓵ C ) = (A U B) ꓵ (A U C)
* A ꓵ ( A U B )= A
* A U (A ꓵ B )=A

Differenza:

A\B= {x| x ∈ A e x ∉ B}

Definiamo il complemento di A come U\A = Ac esso si dice complemento di A per U dove U è un universo che contiene A

* (Ac )c =A

Leggi di De Morgan

* (A ꓵ B) c = A c  U B c
* {\displaystyle a\in A}EsEs(A U B) c  = A c ꓵ B c

DIFFERENZA SIMMETRICA:

A ∆ B = (A\B) U (B\A) = (A U B) \ (A ꓵ B)

## INSIEME DELLE PARTI

Insieme delle parti di T: insieme che contiene tutti i sottoinsiemi di T

T={1,2,3}

P(T)={⊘, {1} , {2} , {3} , {1,2} , {1,3} , {2,3} , {1,2,3} }

Segue che |P(T)|= 2^(|T|)

L’insieme delle parti è esempio di Famiglia di insiemi, la famiglia di insiemi è un insieme tale che i suoi elementi sono degli insiemi

Proprietà:

1. P(AꓵB)=P(A) ꓵ P(B)
2. P(AUB) ⊃ P(A) ꓵ P(B)

Dim della 1:

* Caso ⊂: Supponiamo X ∈ P(A ∩ B), allora X ⊂ A ∩ B quindi X ⊂ A e X ⊂ B. Possiamo allora concludere che X ∈ P(A) e X ∈ P(B) da cui X ∈ P(A) ∩ P(B)
* Caso ⊃: Viceversa, supponiamo adesso che X ∈ P(A) ∩ P(B), allora X ∈ P(A) e X ∈ P(B). Quindi, X ⊆ A e X ⊆ B ovvero X ⊆ A ∩ B che implica X ∈ P(A ∩ B).

PARTIZIONE DI U

F è una partizione di U se tutti gli elementi di F sono sottoinsiemi di U,essi sono disgiunti e l’unione di tutti questi elementi è uguale ad U

## Coppia ordinata

(x,y) è qualcosa di questo tipo,simile a un insieme ma qui l’ordine conta, infatti la coppia (x,y) può essere uguale alla coppia (y,x) se e solo se x=y

INSIEME PRODOTTO

A x B={ (x,y) | x ∈ A e y ∈ B }

A x B in genere è diverso da B x A

Il concetto delle coppie si può estendere alle n-uple

(x1, x2, … x n)

## Relazione binaria

Insieme R

Predicato di due variabili definito in U

R ⊆ U x U

{ (x , y) | (x , y) ∈ A x B e R(x , y) } questo è un sottoinsieme di A x B tale che i suoi elementi rispettino la relazione R, viene detto grafico della Relazione

## Funzione

f : A -> B Dominio -> Codominio

Per ogni x ∈ A esiste uno ed un solo elemento y di B tale che (x , y) ∈ f (f non è altro che una relazione)

* Funzione identica f : A->A
* f : A x B -> A si dice canonica su A

Data f : A->B e dato X sottoinsieme proprio di A, si dice immagine di X, il sottoinsieme di B denotato con f(X). f(X)={ y | y ∈ B e (∃x ∈ X) | f(x)=y }

* Se f(A)=B f è surgettiva
* Se f: A->B porta punti distinti su punti distinti si dice f iniettiva
* Se f è sia surgettiva che iniettiva si dice biettiva

## Teorema

Se A e B sono finiti ed esiste una f iniettiva tale che f: A->B allora segue che |A| ≤ |B|

Dimostrazione:

Considerando f(A) e che f(A) ⊆ B sappiamo che ogni elemento di f(A) è l’immagine di uno ed un solo elemento di A dato che f è iniettiva. Allora |f(A)|=|A| , ricordandoci che f(A) ⊆ B e che la cardinalità di un insieme è maggiore o uguale di un suo sottoinsieme segue che | f(A) |=|A| ≤ |B|

## Proprietà relazioni

Sia R(x , y) definita in U x U , essa è:

* Riflessiva se ∀x ∈ U 🡺 R(x,x) ovvero, la relazione vale su ogni coppia in cui i due fattori coincidono
* Simmetrica se ∀ x , y ∈ U tale che R(x , y) 🡺 R(y , x)
* Transitiva se ∀ x , y , z ∈ U tale che R(x , y) e R(y , z) 🡺 R(x , z)

Se valgono tutte e 3 si dice Relazione di equivalenza:

* x ≈ y
* [ x ] = { y ∈ U | x ≈ y} insieme classe di equivalenza di x , esso contiene tutti gli elementi y che sono equivalenti con x (ovvero R(x , y) dove R è relazione di equivalenza)

## Teorema

Due classi di equivalenza o sono disgiunte o coincidenti

Dimostrazione:

* caso 1) nessun elemento in comune 🡺 disgiunti
* caso 2) Siano [x] e [z] , esse abbiano un elemento w in comune quindi segue che w ≈ x , w ≈ z , per la proprietà transitiva segue che x ≈ z. Sia y ∈ [x] e quindi y ≈ x , per la proprietà transitiva segue che y ≈ z quindi y ∈ [z] . Dunque qualunque sia l’elemento di [x] esso sta in [z], dunque [x] ⊆ [z]. In maniera identica si dimostra che [z] ⊆ [x]

## Insieme quoziente di U rispetto a R

Data R su U consideriamo F, la famiglia di insiemi composta da tutti le classi di equivalenza. F per costruzione è sottoinsieme di P(U) quindi segue che :

* ∀ X ∈ F tale che X ≠ ⊘ e ꓴx ∈ F = U (l’unione di tutti gli insiemi di F è uguale ad U) , infatti per ogni x ∈ U 🡺 x ∈ [x]
* Per ogni X,Y ∈ F tale che X ≠ Y si ha che XꓵY = ⊘

Quindi R individua una partizione F su U detto insieme quoziente di U rispetto a R , si indica con U\R

In modo analogo data una partizione F di U, si individua R tale che F=U\R

Data R in U risulta individuata U->U\R che porta ogni x ∈ U a [x]. Essa è un’applicazione surgettiva detta applicazione canonica del quoziente

## Pre-ordine

Una relazione si dice di pre-ordine se gode di proprietà riflessiva e transitiva Un U in cui è definito un pre-ordine si dice pre-ordinato

## Def di R antisimmetrica

Se ∀x, y ∈ U | R(x,y) e R(y,x) 🡺 x=y (ovvero le due relazioni sono vere solo se x=y)

## Ordine

Si dice ordinamento un pre-ordinamento che gode anche della proprietà antisimmetrica Un U in cui è definito ordinamento si dice ordinato

## Massimi e massimali / minimi e minimali

* Un elemento M ∈ U (ordinato) si dice massimo se ∀x ∈ U 🡺 x≤M
* Un elemento si dice massimale per un U ordinato se non c’è alcun elemento in U che lo supera

Stessi concetti per minimo e minimale

Un massimo è sempre un massimale ma non vale il viceversa

Un ordinamento si dice totale se per ogni coppia (x , y) segue che x ≤ y oppure y ≤ x , in caso contrario si dice parziale

## HIDDING SET

Sia H ⊆ U e sia A una famiglia si sottoinsiemi di U tutti diversi dall’insieme vuoto. H si dice Hidding set per A se e solo se ∀X ∈ A segue che X ꓵ H ≠ ⊘.

Sia H un Hidding set , se ∀ x ∈ H segue che H\{x} non è Hidding set ,allora H è Hidding set minimale

## Insieme chiuso rispetto a un’operazione

Un insieme si dice chiuso rispetto a un’operazione se applicando l’operazione a elementi dell’insieme otterremo come risultato sempre e comunque elementi dell’insieme

Ad esempio sia F chiusa rispetto all’unione, segue che ∀ X, Y ∈ F 🡺 X ꓴ Y ∈ F

## Famiglia complemento

Sia F una famiglia di sottoinsiemi di U

Fc ={ Xc ∈ F } questo insieme si dice famiglia complemento di F

Proprietà : (F c ) c = F

## Teorema

F è chiusa rispetto all’unione se e solo se F c  è chiusa rispetto all’intersezione

Dimostrazione:

1. F chiusa rispetto a unione. Siano A e B ∈ F allora A c  e B c  ∈ F. Per De Morgan A c  ꓵ B c  = (A ꓴ B) c ,poiché A ꓴ B sta in F allora (A ꓴ B) c ∈ F c
2. Viceversa sia F c  chiusa rispetto a intersezione . Siano A , B ∈ F. Sappiamo che A c  , B c  (A ꓵ B)c ∈ F c  . Per De Morgan A c  ꓵ B c  = (A ꓴ B) c che sta in F c  quindi A ꓴ B sta in F

TEORIA DEI NUMERI

N.B. N ⊂ Z ⊂ Q ⊂ R ⊂ C

√(2) 🡸 numero di Pitagora

Valore assoluto:

* |n| ≥ 0 ∀n |n|= n se n ≥ 0 , -n se n < 0

ASSIOMA DEL BUON ORDINAMENTO

* Dato S un insieme di numeri naturali,in S esiste un minimo n tale che ∀t ∈ S 🡺 n ≤ t

### Principio di induzione

E’ una tecnica dimostrativa:

* Se una proprietà P vale sul caso base e sul successore di un caso tale che la P vale

Segue che varrà su tutti i casi

Dim:

Supponiamo esista n tale che P(n) sia falsa, costruiamo l’insieme S={ n : n ∈ N , P(n) è falsa }. Per l’assioma del buon ordinamento esiste un s di S che è il minimo, essendo in S segue che P(s) è falsa, inoltre s=/=0 dato che abbiamo supposto P(0) vera. Ci sarà un elemento minore di s che però non sta in S, per esempio s-1, allora P(s-1) è vera, ma per il principio di induzione la proprietà dovrebbe essere vera anche sul successivo ovvero s, contraddizione.

### DIVISIONE TRA INTERI

Dati a,b ∈ Z con b≠0, chiamati rispettivamente dividendo e divisore,esistono q,r ∈ Z chiamati rispettivamente quoziente e resto tale a=q\*b + r con 0≤ r < |b|

* Il resto r è detto anche modulo infatti r=a mod b (in C++ a%b)
* Il quoziente q è detto anche floor, esso è l’intero più grande che è minore o uguale a a/b

DIMOSTRAZIONE

CASO 1 , a>0 , b>0:

Costruiamo S = {a − kb : k ∈ Z, a − kb ≥ 0} , esiste un minimo r ed è almeno 0. K lo denoto con q tale che r=a-qb segue che a=qb + r. Se r è il minimo segue che q è il massimo numero tale che a-qb≥0. Se esistesse un k>q verrebbe contraddetta l’ipotesi che a-qb è il minimo. Se r è il minimo segue che r<b. Per assurdo sia 0≤b≤r segue che r=b+h (con h positivo). Possiamo scrivere a=qb + b + h = (q + 1)b + h. Dunque segue che h=a – (q+1)b e segue che a-(q+1)b < a-qb che è r , abbiamo contraddetto che r fosse il minimo.

Caso 2, a<0 , b>0

Esistono q’ e 0≤r’<b tale che |a| = q’b + r’ e quindi − a = q’b + r’

1. Se r’=0 abbiamo finito
2. Se r’>0 segue che 0 < b – r’ < b , riscrviamo l’uguaglianza di prima così: a = (−q’ )b + (−r’ ) = (−q’ )b −b +b + (−r’ ) = (−q’ −1)b + (b −r’ ) , chiamiamo -q’-1=q e b-r’=r. Finito

Caso 3 , a>0 , b<0

Esistono q’ ed 0 ≤ r’ < |b| tale che a = q’ |b| + r’ e quindi a = q’ (−b) + r’ quindi a= (-q’) b + r’ Chiamiamo -q’=q e abbiamo finito.

Caso 4 , a<0 , b<0

esistono q’ ed 0 ≤ r’ < |b| ovvero 0 ≤ r’ < −b tale |a| = q’ |b| + r’ segue che: a=-(q’)|b| - |b| +|b| -r’ = (q’ + 1)b + (-b-r’) , chiamiamo q’+1=q e -b-r’=r . Finito

### Divisibilità

Dati due interi n,m ∈ Z , m è divisore di n se esiste k∈Z tale che n=m\*k , se m è divisore di n si denota con m | n, altrimenti m ∤ n

* n è pari se esiste k ∈ Z tale che n=2\*k
* n è dispari se esiste k ∈ Z tale che n=2\*k +1

### Teoremi

1. se a | b e a | c 🡺 a | (b+c)
2. se a | b 🡺 a | b\*c
3. se a | b e b | c 🡺 a | c

Dim 1:

a|b 🡺 ∃x : b=ax . a|c 🡺 ∃y : c=ay. Segue che b+c=ax+ay=a(x+y) . Sia x+y=z segue che b+c=az

Dim 2:

a|b 🡺 ∃x : b=ax , moltiplicando entrambi i membri per c rimane l’uguaglianza, bc=acx, chiamiamo cx=y . Finito

Dim 3:

a|b 🡺 ∃x : b=ax . b|c 🡺 ∃y : c=by. Segue che by=axy e anche c=axy , chiamiamo xy=z quindi c=az

## Teorema

Ogni a ∈ Z è divisore di 0, quindi 0 è multiplo di ogni intero relativo, 0 è divisore solo di se stesso

Dim:

∀ a ∈ Z 🡺 a\*0=0, dunque a|0. Se 0|a esiste un x tale che 0x=a, ovvero a=0(sempre) quindi 0|0

## Teorema

Siano a,b ∈ Z, se a | b e b | a 🡺 |a| = |b|

Dim:

b = ax , a = by segue che a=axy ovvero (1-xy)a=0 ovvero o a=0 oppure xy=1.

1. Se a=0 allora anche b=0
2. Se xy=1 allora o entrambi 1 o entrambi -1, segue che y= ± 1 quindi a= ±b

## Teorema dei Divisori banali

Sia a ∈ Z 🡺 ± a | a e ± 1 | a qualunque sia il valore di a

### M.C.M.

Dati a , b ∈ Z non entrambi nulli esistono infiniti numeri che sono multipli sia di a che di b,di questo infinito insieme per l’assioma del buon ordinamento esisterà un minimo,questo numero è il MCM(a,b)

### M.C.D.

Dati a,b ∈ Z non entrambi nulli,esistono infiniti numeri che sono divisori sia di a che di b, di questo infinito insieme esisterà un elemento max, esso è il MCD(a,b)

### Algoritmo di Euclide per trovare il MCD(a,b)

Supposto b ≤ a

* se b=0 oppure b | a 🡺 MCD(a,b)=b
* altrimenti: si riconsideri il fatto che a=q\*b + r, si calcoli r facendo a%b , MCD(a,b)= MCD(b,r)

Dimostriamo che se a=qb+ r con 0<r<b alloora MCD(a,b)=MCD(b,r)

Sia d divisore di a e b🡺 esistono h e k tale che a=hd=qkd + r 🡺 r=(h-qk)d ovvero d è divisore di r. Se d è divisore di b e r esistono h’ e k’ tale che a = qb + r = qkd + hd 🡺 a=d(qk + h) ovvero d è divisore anche di a

## Teorema

Se a,b non sono entrambi nulli esistono h e k ∈ Z tale che MCD(a,b)=a\*h + b\*k

## Definizione

Si dice numero primo p un numero ∈ Z che ha come unici divisori quelli banali, escluso l’1

## Definizione

a e b si dicono coprimi se MCD(a,b)=1

## Proprietà

1. P1) Due interi consecutivi sono coprimi
2. P2) se c |(a\*b) e c ed a sono coprimi 🡺 c | b
3. P3) Se a|c e b|c e a e b sono coprimi 🡺 (a\*b)|c

Dim 1:

Siano n e n + 1 due numeri interi consecutivi, allora per h = 1 e k = −1 abbiamo 1 = h · (n + 1) + k · n

Dim 2:

Siano a, b, c ∈ Z tali che c | a · b e c, a coprimi. Quindi, esiste h tale che hc = ab ed esistono k, k’ tali che 1 = ka + k’c. Moltiplicando per b ambo i termini dell’ultima uguaglianza otteniamo b = kab + k’cb da cui b = khc + k’cb = c(kh + k’b) e quindi c | b

Dim 3:

Siano a, b, c ∈ Z tali che a | c e b | c, ed a e b coprimi. Allora esistono h, k, h’ , k’ tali che c = ah, c = bk, e 1 = ah’ + bk’ . Moltiplicando per c ambo i termini dell’ultima uguaglianza otteniamo c = ah’c + bk’c = ah’bk + bk’ah = ab(h’k + k’h) e quindi ab | c.

## Teorema

Ogni numero intero n > 1 si può esprimere come prodotto di numeri primi positivi in modo unico a meno dell’ordine dei fattori

Dim: La dimostrazione si divide in 2 dimostrazioni, dimostriamo prima che questa fattorizzazione esiste, e dimostriamo poi che è unica

ESISTENZA:

Costruiamo l’insieme degli n>1 tale che S = {n : n ∈ N, non prodotto di numeri primi} Per l’assioma di buon ordinamento, possiamo scegliere il minimo dell’insieme S, denotiamolo con s. Per definizione, s non è primo perché se lo fosse sarebbe prodotto ( con un solo fattore) di primi positivi (se stesso) e quindi non sarebbe in S. Quindi, s ha divisori diversi da quelli banali e quindi almeno un divisore positivo 1 < d < s. Allora, esiste c ∈ N tale che s = d · c, e anche 1 < c < s. Poiché, c ed d sono minori di s, che ricordiamo è il più piccolo elemento in S, allora c e d sono prodotti di primi positivi, e quindi anche s lo è.

UNICITA’

Scriviamo n così n = p1 · p2 · . . . · pr = q1 · q2 · . . . · qs . Dimostriamo con induzione:

* Caso base: r = 1. Se n = p1 allora n è primo, e quindi non ha divisori diversi da quelli banali, ossia se stesso e ±1. Quindi, da p1 = q1 · q2 · . . . · qs otteniamo che s = 1 e q1 = p1.
* Caso induttivo: supponiamo la tesi sia vera per r e dimostriamola per r + 1. Se n = p1 · p2 · . . . · pr · pr+1 = q1 · q2 · . . . · qs abbiamo che q1 è un divisore di p1 · p2 · . . . · pr · pr+1 e quindi, per quanto precedentemente visto, deve dividere almeno uno dei fattori. Ma sono tutti fattori primi, quindi, q1 deve essere uguale ad almeno uno dei fattori, che, a meno di riordinare il prodotto, possiamo assumere sia p1. Dividendo membro a membro per p1 otteniamo p2 · . . . · pr · pr+1 = q2 · . . . · qs. I fattori del primo membro sono r , possiamo applicare l’ipotesi induttiva. I fattori p2, . . . , pr , pr+1 coincidono con i fattori q2, . . . , qs a meno dell’ordine.

## Teorema

I numeri primi sono infiniti

Dim:

Siano per assurdo n (n finito)

p1=2 , p2=3 … pn. Siano h e k tale che h = p1 · p2 · . . . · pn , k = p1 · p2 · . . . · pn + 1 . Essi sono consecutivi e quindi coprimi. K non essendo primo si dovrebbe poter scrivere come fattorizzazione di numeri primi che sono compresi tra p1 e pn, ma ciò non lo renderebbe più coprimo con h

## Teorema sulla densità dei numeri primi

∏(n) è la funzione che restituisce il numero di “numeri primi” minori o uguali di n

Per il teorema segue che per ogni n ci sono n/ln(n) numeri primi minori o uguali di n

## Criteri di divisibilità

N è divisibile per:

* 2 se la sua ultima cifra è 0,2,4,6,8
* 3 se la somma delle cifre di n è divisibile per 3
* 5 se la sua ultima cifra è 0 o 5
* 7 se facendo n=10\*q+r segue che q-2\*r è divisibile per 7
* 13 se facendo n=10\*q+r segue che q+4\*r è divisibile per 13
* 17 se facendo n=10\*q+r segue che q-5\*r è divisibile per 17
* 19 se facendo n=10\*q+r segue che q+2\*r è divisibile per 19
* 23 se facendo n=10\*q+r segue che q+7\*r è divisibile per 23
* 11 se la differenza tra la somma delle cifre in posizione pari e la somma delle cifre in posizione dispari è divisibile per 11

## Teorema

n è divisibile per 7 se e solo se q − 2r è divisibile per 7 (considerando n=10q + r)

Dim:

Supponiamo n sia divisibile per 7. Allora esiste h tale che n = 7h. D’altro canto, dividendo n per 10 otteniamo n = 10q + r. Quindi, abbiamo 7h = 10q + r sottraendo 21r da entrambi i membri otteniamo 7h − 21r = 10q − 20r e quindi 7(h − 3r) = 10(q − 2r) Quindi, il numero primo 7 divide il prodotto 10(q − 2r) e dal momento che non divide 10 allora divide q − 2r. Viceversa, supponiamo q − 2r sia divisibile per 7. Allora esiste k tale che q − 2r = 7k e quindi q = 7k + 2r. Allora n = 10q + r = 10(7k + 2r) + r = 70k + 21r = 7(10k + 3r)

## Definizione Radice numerica

Per n ∈ Z 🡺 p(n) è la somma delle cifre di n reiterata

## Teorema

Sottraendo a un qualsiasi numero n la sua radice numerica p(n) ottengo un multiplo di 9

Dim:

Un qualunque n si può scrivere come Σ(k ,i=0) ( ai · 10^i ) (sommatoria che va da i=0 fino a k di ai\*10^i) mentre la sua p(n) si può scrivere come Σ(k ,i=0) ( ai ) . (in entrambe ai è la i-esima cifra del numero)

n-p(n)= Σ(k ,i=0) ( ai · 10^i ) - Σ(k ,i=0) ( ai ) = Σ(k ,i=0) ( ai \* (10^i -1) ) = Σ(k ,i=0) ( ai \* 9 \* bi ) = = 9\*Σ(k ,i=0) ( ai\*bi )

## ARITMETICA MODULARE

Riguarda il calcolo dei resti delle divisioni tra interi rispetto a un divisore fissato

a e b sono in relazione congruenza di modulo m se a-b è multiplo di m.

Si denota così a≡ b (mod m) “a è congruo b mod m” , significa che a mod m = b mod m

La relazione di congruenza modulo m è una relazione di equivalenza.

Dato m ≥ 0, [a] m è la classe rappresentata da a nella relazione di congruenza modulo m

[a] m = { b ∈ Z | a≡b(mod m) }

## Teorema

Fissato m > 1 ,le classi di equivalenza della relazione di congruenza modulo m sono m

[0] m , [1] m , [2] m … [m-1] m

DIM:

Sia a ∈ Z e sia r il resto della divisione intera di a per m, ovvero, applicando l’algoritmo di divisione a = qm + r con 0 ≤ r < m. Quindi, dal momento che r può assumere solo i valori che vanno da 0 a m − 1 le classi di equivalenza sono solo quelle dell’enunciato del teorema. Dimostriamo adesso che le classi [0]m, [1]m, [2]m, . . . [m − 1]m, sono tutte distinte. Ragioniamo per assurdo e supponiamo che esistano x, y ∈ Z, x =/= y e 0 ≤ x, y < m − 1 tali che [x]m = [y]m. Sia x>y e x-y=km quindi multiplo di m, ma x-y è minore di m e maggiore di 0 quindi contraddizione.

Esercizio

Dato a ∈ Z, in che classe di resto sta?

* [a] m = [r] m se m=5 , a=22 segue che r=2 quindi 22 ∈ [2] 5

## Teorema

Dati a e b tale che tale che a≡b(mod m) , e c e d tale che c≡d(mod m) segue che:

* a+c≡b+d (mod m)
* a\*c≡b\*d (mod m)

Per ipotesi esistono k1, k2 ∈ Z tale che a − b = k1m e c − d = k2m.

Dim 1:

(a + c) − (b + d) = (a − b) + (c − d) = (k1 + k2)m che dimostra la proprietà.

Dim 2:

Abbiamo a = b + k1m e c = d + k2m, quindi ac−bd = (b+k1m)(d +k2m)−bd = bk2m+dk1m+k1k2m = (bk2+dk1+k1k2)m che dimostra la proprietà.

## Proprietà

* P1) a+b ≡ (a mod m + b mod m) (mod m)
* P2) a^n ≡ (a mod m)^n (mod m)
* P3) a^h \* b^k ≡ (a mod m)^h \* (b mod m)^k (mod m)

## Teorema

Preso m > 1 , una qualunque sequenza di m interi consecutivi contiene un intero divisibile per m

Dim:

Sia la sequenza di m interi: n, n + 1, n + 2, . . . , n + m – 1.

L’intero n sta in una delle classi di congruenza degli interi della sequenza. Supponiamo stia nella classe [i]m per 0 ≤ i ≤ m − 1. Quindi n ≡ i(mod m) ed allora n + 1 ≡ i + 1(mod m) ovvero n + 1 ∈ [i + 1]m.

* Se i=0 🡺 n ∈ [0]m a
* Se i>0 🡺 0 < i < m , incrementando i esattamente m − i volte, con m − i < m , otteniamo che n + (m − i) ≡ i + (m − i)(mod m) ossia n + (m − i) ≡ m(mod m) ≡ 0(mod m). In conclusione, n + (m − i) è il numero multiplo di m nella sequenza di m numeri consecutivi.

## Divisione modulare

Siano a,b entrambi più grandi di 0. Esiste un x tale che a\*x ≡ 1 ( mod b) se e solo se a e b sono coprimi

Dim:

Supponiamo a, b siano coprimi. Esistono h, k tali che ha + kb = 1. Quindi, ha = 1 − kb e quindi, dal momento che (1 − kb) mod b = 1 abbiamo che ha ≡ 1(mod b) e h = a^-1 mod b.

Viceversa supponiamo esista x tale che xa ≡ 1(mod b). Dalla definizione di congruenza, ciò implica che esiste k tale che xa − 1 = kb e quindi xa + (−k)b = 1 ovvero MCD(a, b) = 1 e quindi a, b coprimi.

## Funzione φ (phi)

I numeri minori o uguali ad n e coprimi con n sono φ(n)

φ(n)= | {x | 0< x ≤ n e MCD(n,x)=1 } |

* φ(n)=n-1 se n è primo
* φ(n)=φ(p^k)= p^k – p^(k-1) dove p è è primo e k≥2
* φ(n)=(p1 -1 )\* (p2 -1) se n=p1 \* p2 e p1 e p2 sono numeri primi

## Teorema

Sia n=k\*h, con h,k > 0 e coprimi.

* φ(n)= φ(h) \* φ(k)

## Teorema

Sia n > 1 e consideriamo la sua fattorizzazione n= p1^(k1) \* p2^(k2) \* … \* pm^(km)

* φ(n) = ( p1^(k1) - p1(k1-1) ) \* … \* ( pm^(km) – pm^(km-1) )

Dim: (induzione)

* Caso base: se m = 1 allora n = p^k1 ed il teorema è vero
* Supponiamo il teorema sia vero per ogni intero n’ la cui fattorizzazione presenta al più m − 1 numeri primi diversi. Se denotiamo con n’= p1^k1 · p2^k2 · . . . · pm-1^(km−1). Segue n = n’ · p^km . φ(n) = φ(n’) · φ(pm^km ) = (p1^k1 – p^(k1−1) ) · (p2^k2 – p2^(k2−1) ) · . . . · (pm-1^(km−1)−pm-2^(km−2)) · (pm^km− pm-1^(km−1))

Questo perché n’ e p^km sono coprimi

## Teorema di Eulero

Siano n,m > 0 e coprimi 🡺 n^(φ(m) ) ≡ 1 (mod m)

Calcolo dell’inverso k=( n mod m)^ (φ(m) - 1 ) mod m

Questo numero k ha questa proprietà n\*k ≡ 1 (mod m)

### Teorema

Se p è primo e MCD(a,p)=1 allora 🡺 a^(p-1) ≡ 1 (mod p)

### Teorema

Se MCD(a,n)=1 🡺 per ogni x > 0 segue che a^x ≡ a^(x mod φ(n)) (mod n)

Dim:

Se calcoliamo la divisione intera x/φ(n) otteniamo quoziente q e resto r = x mod φ(n) e quindi x = q · φ(n) + x mod φ(n). Allora: a^x = a^(q·φ(n)+x mod φ(n)) = (a^φ(n) )^q · a^(x mod φ(n)). MCD(a, n) = 1 e quindi per il teorema di Eulero a^φ(n) ≡ 1(mod n) segue che: (a^φ(n) )^q · a^(x mod φ(n)) ≡ (1)^q · a^(x mod φ(n)) (mod n) ≡ a^(x mod φ(n)) (mod n)

### Teorema

n ≡ p(n) (mod 9) per ogni n (N.B. p(n) è la radice numerica di n)

Vale a dire che n – p(n) è multiplo di 9 sempre

### Numeri primi di Mersenne

Dato un numero p primo segue che 2^p -1 sarà anch’esso primo.

Si chiamano numeri primi di Mersenne i numeri nella forma Mp=2^p - 1

Ad oggi si conoscono i primi 51 numeri primi di Mersenne, di cui il più grande ha 24 milioni di cifre

### Funzione Sigma

Dato n si definisce ẟ(n) la somma di tutti i divisori di n (compreso n)

Esempio: ẟ(6) = 1+2+3+6=12

Un numero si dice perfetto se ẟ(n) = 2\*n ad esempio 6 è un numero perfetto

### Congettura di Goldbach

Ogni numero pari maggiore di 4 si può scrivere come somma di due numeri primi

### Funzione d(n)

Ad ogni n associo d(n) che è il minimo valore tale che n – d(n) e n + d(n) sono entrambi primi.

n e d(n) sono sempre coprimi

### Congettura di Collatz

Il seguente algoritmo termina sempre(ovvero si arriva al caso base n=1)

{ 1 se n=1

f(n)= { n/2 se n è pari

{ 3\*n + 1 se n è dispari

(Si riapplica f(n) sul risultato , se il risultato è 1 la funzione ricorsiva termina )

Per ogni n viene generata una sequenza di interi detta traiettoria di n, abbiamo quindi una funzione c(n) che associa ad ogni n il numero di elementi della sua traiettoria.

La congettura è stata verificata per ogni n < 10^18

CALCOLO COMBINATORIO

* Quanti sono i possibili codici pin di una carta bancomat a 5 cifre? 10^5
* Possibili password di 8 simboli alfa-numerici? 62^8 (62=26+26+10)

### Disposizioni

1. Dati gli insiemi A e B con |A|=k e |B| = n , calcolare il numero delle applicazioni di A in B Questo è il numero delle disposizioni con ripetizione di n elementi di classe k, denotato con Fn,k
2. Dati gli insiemi A e B con |A|=k e |B| = n , calcolare il numero delle applicazioni iniettive di A in B Questo è il numero delle disposizioni semplici di n elementi di classe k, denotato con Dn,k

### Combinazioni

1. Dato B con |B|= n ,preso k ≤ n trovare il numero di sottoinsiemi di B di k elementi Questo è il numero di combinazioni di n elementi di classe k, denotato con Cn,k
2. Dato B con |B|= n ,preso k ≤ n Trovare il numero di combinazioni di n elementi di classe k con ripetizioni , denotato con Cn,k r

* Fn,k = n^k
* Dn,k  = (n!)/((n-k)!)
* Cn,k = (n!)/((k!)((n-k)!))
* Cn,k r = ((n+k-1)!)/((k!)((n-1)!))

Esempio

Insieme di 7 variabili, i monomi possibili di grado 3 sono ((9)!)/((3!)((4)!))

### Probabilità discrete

Le probabilità che accada un evento sono definite sulla spazio di campioni S, ovvero l’insieme che contiene ogni possibile caso, i suoi elementi sono detti eventi elementari.

S= evento certo (succede sempre) , ⊘= evento nullo (non succede mai)

Definiamo F come il numero di casi favoreli, ovvero su un S di 10 elementi per esempio F è 3,ovvero ci sono 3 casi che soddisfano una certa condizioni. Se S rappresentasse una busta con 10 biglie e la mia condizione perché la biglia sia un caso favorevole fosse “biglia rossa” e le biglie rosse fossero 3 allora avrei 3 casi favorevoli su 10.

P(a) si definisce come come probabilità che si verifichi l’evento a.

P(a) = Fa/n dove n è |S| (nel caso di prima sarebbe stato 3/10)

### Assiomi

* 0 ≤ P(a) ≤ 1
* P(S) = 1 , P(⊘) = 0
* P( A ꓴ B) = P(A) + P(B) – P(A ꓵ B)

### Probabilità condizionata

P(A | B) = P(A and B)/P(B) è la probabilità che si verifichi A al verificarsi di B

Due eventi sono indipendenti se:

* P(A | B) = P(A)
* P(B | A) = P(B)

Ovvero P(A | B) = P(A) \* P(B)

REGOLA DI BAYES:

* P(B | A) = (P(A | B) \* P(B) )/P(A)

## Teorema probabilità totale

Sia A un evento e siano B1, B2, . . . , Bn n eventi mutualmente esclusivi, tali che P(Bi) =/= 0 per ogni i ed inoltre P(B1 ∨ B2 ∨ · · · ∨ B) = 1, ovvero gli eventi sono esaustivi.

P(A) = P(A|B1)P(B1) + P(A|B2)P(B2) + · · · P(A|Bn)P(Bn)

Dim:

B1, B2, . . . , Bn sono esaustivi, almeno uno di loro si deve verificare.

P(A) = P(A ∧ B1) + · · · + P(A ∧ Bn) 🡺 P(A ∧ Bi) = P(A|Bi) · P(Bi)

### PROBLEMI D’URNA

Se siamo di fronte a un problema d’una dobbiamo usare diverse formule in base al particolare problema

* Fn,k se l’ordine conta e la pallina viene rimessa dentro l’urna dopo essere stata pescata
* Dn,k se l’ordine conta e la pallina non viene rimessa dentro
* Cn,k se l’ordine non conta e la pallina non viene rimessa dentro
* Cn,k r se l’ordine non conta e la pallina viene rimessa dentro

### Paradosso del compleanno

Bastano 23 persone perché la probabilità che almeno 2 di queste facciano il compleanno lo stesso giorno sia maggiore di ½ (il 50%)

Per approfondire <https://it.wikipedia.org/wiki/Paradosso_del_compleanno>

### Variabile casuale e valore medio

La variabile casuale è una funzione X che associa ad un numero un evento

L’evento è definito come il fatto che X sia uguale a x

Valore atteso E[X] = Σx x\*P[X=x]

Proprietà lineare: E[ X + Y ] = E[X] + E[Y]

Esempio:

Se lanciamo due dadi, qual è il valore atteso del massimo dei 2 valori? Qui X avrà come valore il valore massimo della coppia risultante dal lancio dei due dadi.

Abbiamo 36 casi possibili {(1, 1),(1, 2), . . . ,(6, 5),(6, 6)} tutti con la stessa possibilità di avvenire ovvero 1/36

* Di coppie con "6" ne abbiamo 11
* Di coppie con "5" ma senza "6" ne abbiamo 9
* Di coppie con "4" ma senza "5" o "6" be abbiamo 7
* Di coppie con "3" ma senza "4", "5", o "6" ne abbiamo 5
* Di coppie con "2" ma senza "3", "4", "5" o "6" ne abbiamo 3
* Di coppie con solo "1" ne abbiamo solo 1

E[X]= [6\*11/36 + 5\*9/36 + 4\*7/36 + 3\*5/36 + 2\*3/36 + 1\*1/36] che è circa 4,47

Questo significa che lanciando due dadi la possibilità che il maggiore nella coppia sia maggiore di 4 è alta(quindi conviene scommetterci)

## Prova di bernoulli

Sia p la probabilità di successo.

Il valore atteso per ottenere successo è E[X]= 1/p

Esempio: se volessi ottenere da un lancio di dado il 6 , E[X]= 1/(1/6) = 6 dovrei lanciare 6 volte secondo il valore atteso

### Paradosso dei 2 bambini

Un padre ha 2 figli, uno di essi è maschio. Quale è la possibilità che anche il secondo sia maschio anche lui?

* 1/3

Per approfondire: <https://it.wikipedia.org/wiki/Paradosso_dei_due_bambini>

### Paradosso delle 3 carte

Abbiamo 3 carte

1. Carta con bordi rossi
2. Carta con bordi bianchi
3. Carta con un bordo rosso e un bordo bianco

Prendo una carta e ne guardo un solo lato, esso è rosso, quale è la probabilità che anche l’altro lato sia rosso?

* 2/3

Per approfondire: <https://it.wikipedia.org/wiki/Paradosso_delle_tre_carte>

### Paradosso di Monty Hall

Siamo in un gioco e dobbiamo scegliere quale porta aprire tra 3 possibilità, dietro a 2 si queste c’è una capra, nell’altra un’auto(in caso la vinciamo :D )

Scegliamo una porta, e il conduttore ci fa vedere il contenuto di una delle due porte non scelte ovvero una capra. Quindi tra la porta che abbiamo scelto e quella non aperta di sicuro c’è l’automobile.

Il conduttore ci chiede “vuoi cambiare porta per scegliere quella che non ho aperto?”

Domanda: conviene cambiare?

* Si, la porta inizialmente scelta ha probabilità di successo di 1/3 , quella rimasta di 2/3

Per approfondire: <https://it.wikipedia.org/wiki/Problema_di_Monty_Hall>

Esiste una versione equivalente di questo problema, detto dilemma del prigioniero o paradosso dei 3 prigionieri : <https://it.wikipedia.org/wiki/Dilemma_del_prigioniero>

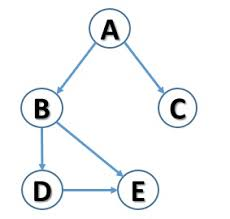
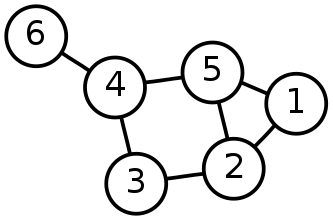
### Paradosso delle 10 scatole

Ci sono 10 scatole, una contiene un premio le altre 9 nulla. Ne scegliamo una all’inizio (senza aprirla) successivamente , vengono aperte 8 scatole ,tutte vuote. Rimangono quindi 2 scatole, ci viene chiesto se vogliamo cambiare, conviene?

* Si , la possibilità di quella scelta è 1/10 mentre quella dell’altra è 9/10

GRAFI

I grafi sono strutture matematiche discrete che rivestono interesse sia per la matematica che per un'ampia gamma di campi applicativi. In informatica sono molto importanti in quanto strutture dati molto efficienti in certi casi

.  

GRAFO DIREZIONATO GRAFO NON DIREZIONATO(detto anche digrafo)

Sia G un grafo non orientato, G=(V,E) dove:

* V={1,2,3 … n} gli elementi sono detti nodi/vertici
* E={e1,e2,… em} gli elementi sono sottoinsiemi di V di cardinalità 2, questi elementi sono detti archi, en={In , Jn} quindi In ha un collegamento diretto con Jn, e viceversa

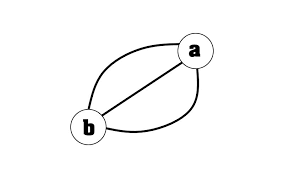
Sia G un grafo orientato, G=(V,E) dove:

* Valgono le stesse proprietà di prima ma in questo gli elementi di E adesso sono coppie ordinate quindi en=(In,Jn) ovvero vale la proprietà “esiste l’arco che porta da In a Jn” ma non è detto il viceversa

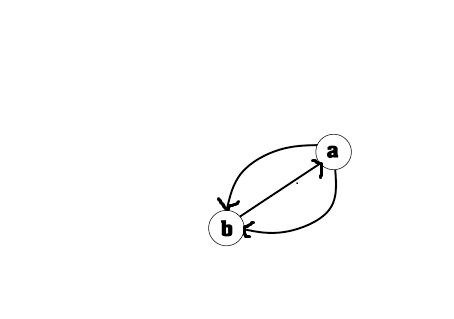
### Multigrafo

E’ un grafo in cui esistono 2( o più) nodi I e J tale che è possibile fare I->J in più modi

Questo è un esempio con un grafo non orientato

Esistono 3 modi per fare a->b e 3 modi per fare b->a

Questo è un esempio con grafo orientato

Esistono 2 modi per fare a->b e uno per fare b->a

### Grado di un nodo

Definiamo grado di un nodo v denotato con ẟ(v) il numero di archi ad esso incidenti

* Per un Grafo orientato per ogni v definiamo ẟ(v)- il numero di archi in entrata e ẟ(v)+ il numero di archi in uscita , la somma di tutti i ẟ(v)- è uguale alla somma di tutti i ẟ(v)+ che è uguale a |E|
* Per un grafo non orientato definiamo solo ẟ(v), la somma di tutti i ẟ(v) è uguale a 2\*|E|

### Teorema

In un grafo non orientato, il numero di vertici che hanno archi dispari è pari

### Grafo regolare

Un grafo non orientato è regolare se tutti i vertici sono dello stesso grado r, segue che |V|=2\*|E| /r

### Grafo completo

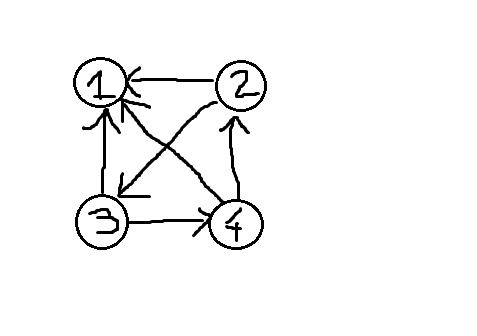
Un grafo si dice completo se ogni possibile coppia di vertici è collegata da un arco, segue che il numero di archi sarà |V|! / ((2!)\*(|V|-2)!)

Un grafo completo è denotato con Kn, dove n è il numero di nodi, segue che Kn è un grafo regolare di grado n-1

### Torneo

Il torneo è un grafo completo, assegnando a ogni arco un verso otterremo un Torneo, ovvero un grafo orientato in cui ogni possibile coppia è legata da un arco(con un solo verso)

Esempio di Torneo:

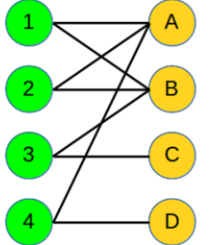


### Teorema

Un grafo orientato è completo se dato |V|= n segue che |E|= n(n-1)

### Grafo bipartito

Un grafo si dice bipartito se V si può partizionare in due insiemi V1 e V2, tale che ogni vertice di V1 può essere collegato (tramite arco) solo con uno o più vertici di V2 e viceversa. Esempio:

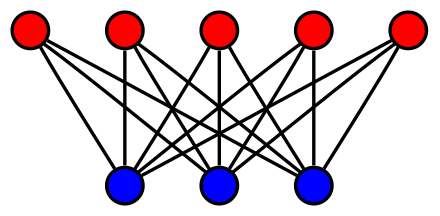


### Grafo bipartito completo

Un grafo bipartito si dice completo se per ogni coppia (v,u) esiste un arco dove v appartiene a V1 e u a V2.

Un grafo bipartito completo si indica con Kn,m dove n=|V1| e m=|V2|

Esempio( K5,3)



### Sottografo

Un grafo G1 si dice sottografo di G2 se si può ottenere “eliminando” da G2 uno o più vertici e/o uno o più archi.

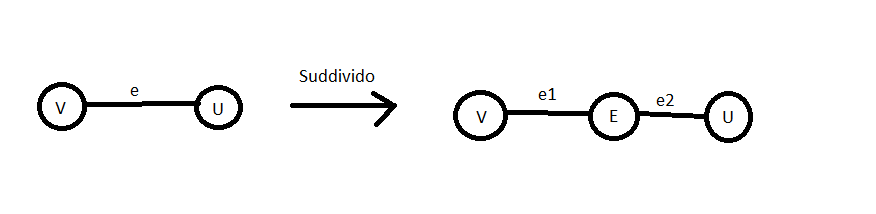
Quindi se G1 è sottografo di G2 accadrà che V1 ⊆ V2 e E1 ⊆ E2

### Isomorfismo

Due grafi (o entrambi orientati o entrambi non orientati) G1 = (V1, E1) e G2 = (V2, E2) si dicono isomorfi se esiste una applicazione biunivoca f dall’insieme dei vertici V1 nell’insieme dei vertici V2 tale che (f(u), f(v)) è un arco di E2 se e solo se (u, v) è un arco di E1. (segue che ẟ(v) = ẟ(u) OR ẟ(v)-= ẟ(u)- AND ẟ(v)+ = ẟ(u)+)

Se due grafi sono isomorfi segue che |V1|=|V2| AND |E1|=|E2|

### Suddivisione arco



### Grafi omeomorfi

Sue grafi sono omeomorfi se facendo una serie di suddivisioni arrivo a un isomorfismo trai due grafi

### Percorso

Un percorso in un grafo (digrafo) è una sequenza di nodi v1,v2… ,vk tale che per ogni i (1 ≤ i < k) segue che (vi ,vi+1) è un arco del grafo.

v1 è detto origine del percorso, vk destinazione, la lunghezza del percorso è k-1

### Cammino

Un percorso è detto cammino se non viene percorso più di una volta ogni vertice( viene detto cammino diretto se il grafo è orientato)

### Circuito

Il circuito è un percorso chiuso,ovver0 origine e destinazione coincidono

### Ciclo

Il ciclo è un cammino chiuso dove tutti i vertici del percorso (tranne primo e ultimo) sono diversi

### Grafo aciclico

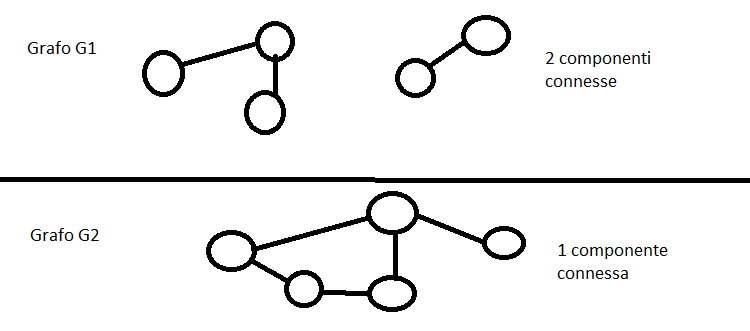
Un grafo è aciclico se non ha cicli

### Connessione

I vertici u e v sono connessi se esiste un percorso che porta da u a v, la connessione tra vertici è una relazione di equivalenza

### Componenti connesse

Una componente è connessa se tutti i vertici di quella componente sono connessi,ogni grafo è composto da 1 o più componenti connesse



Un grafo si dice connesso se ha una sola componente connessa

### Digrafo debolmente connesso

Un digrafo è debolmente connesso se eliminando l’orientamento degli archi otteniamo un grafo connesso

### Connessione

In un digrafo due vertici v,u sono fortementi connessi se esiste sia il percorso v -> u sia u->v

### Grafo fortemente connesso

Sia un grafo formato da più componenti connesse,ogni componente può essere vista come un sottografo che chiamiamo componente fortemente connessa se in questo sottografo tutti i vertici sono fortemente connessi. Un grafo si dice fortemente connesso se ha una sola componente fortemente connessa

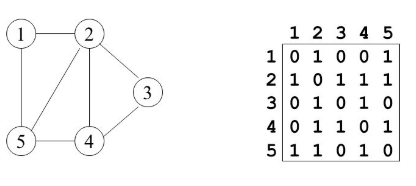
### Grafo k-connesso

* G è k-connesso rispetto agli archi se comunque presi u e v esistono k cammini ad archi disgiunti tra u e v
* G è k-connesso rispetto agli archi se comunque presi u e v esistono k cammini a nodi disgiunti tra u e v

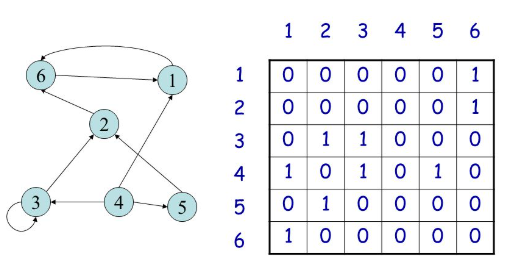
### RAPPRESENTAZIONE DI UN GRAFO CON MATRICE

Dato un grafo di n nodi è possibile rappresentarlo con una matrice booleana n\*n, dove nella posizione (i,j) ci sarà true se esiste l’arco da i a j, false altrimenti. Nei grafi non orientati otterremo sempre una matrice simmetrica, per i grafi orientati non è detto

Esempio di rappresentazione di grafo non orientato:



Esempio di rappresentazione di grafo orientato:



### Teorema

Sia G un digrafo, se accade che ẟ(i)-> 0 oppure ẟ(i)+> 0 per ogni i,allora sicuramente ci sarà un ciclo (condizione sufficiente ma non necessaria)

Dim:

Dimostriamo il primo caso. La dimostrazione del secondo caso è analoga. Prendiamo un vertice i0. Dal momento che +(i) > 0 esiste un vertice i1 tale che vi è un arco da i0 a i1. Lo stesso discorso vale per i1. Quindi esiste un vertice i2 tale che vi è un arco da i1 ad i2. Iteriamo questo processo sino a quando non abbiamo una sequenza i0, i1, i2,..., in di n + 1 vertici tali che ognuno è connesso da un arco al successivo. Se |V| = n per il Pigeonhole Principle almeno 2 di questi n + 1 vertici devono coincidere.

### Teorema

Sia G un digrafo, se in G esiste un sottografo G’ tale che ẟ(i)-> 0 oppure ẟ(i)+> 0 per ogni i (di V’) allora G sarà ciclico. (teorema simile al precedente, ma in questo caso la condizione oltre ad essere sufficiente è anche necessaria)

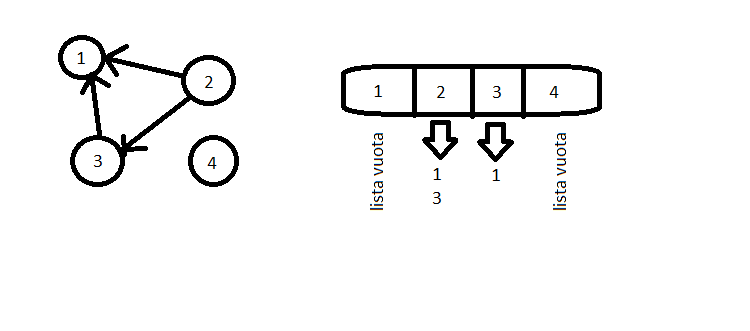
### Teorema

Il numero di percorsi di lunghezza k>= 1 , è dato dal valore M^k (i,j) . (valore nella posizione (i,j) della matrice M^k)

* Esempio: M^3 (3,5)=2 significa che esistono 2 percorsi da 3 a 5 di lunghezza 3

### RAPPRESENTAZIONE DI UN GRAFO CON LISTE DI ADIACENZA

Questa tecnica di rappresentazione consiste nel creare un array di liste, ad esempio nella posizione 1 ci sarà la lista contenente gli elementi raggiungibili direttamente da 1



### Circuito Euleriano

Un circuito si dice Euleriano se passa per tutti i vertici del circuito e per tutti gli archi una sola volta (“una sola volta” vale per gli archi, non per i vertici) . Un grafo si dice Euleriano se possiede un circuito Euleriano

### Teorema

Un grafo è Euleriano se e solo se è connesso ed i suoi vertici hanno tutti grado pari

### Cammino Euleriano

Simile al circuito euleriano ma in questo caso non si ha appunto un ciclo(dunque origine e destinazione non coincidono)

### Teorema

Un grafo possiede un cammino Euleriano se e solo se è connesso e al più due nodi hanno grado dispari. I due vertici di grado dispari saranno primo e ultimo nodo del cammino

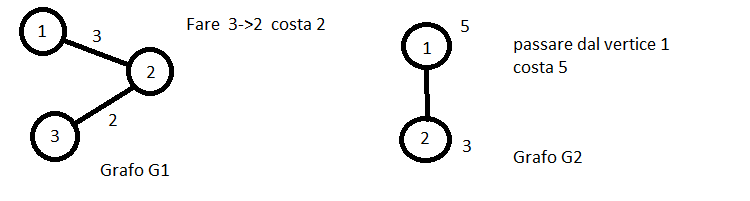
### Cammino Hamiltoniano

Un cammino si dice Hamiltoniano per G se passa una ed una sola volta per tutti i vertici di G. Si fa eccezione per primo e ultimo nodo,se questi due coincidono allora avremo un ciclo Hamiltoniano. Un grafo si dice Hamiltoniano se possiede un ciclo Hamiltoniano

Nota: Non esiste un algoritmo veloce per stabilire se un Grafo è Hamiltoniano o meno.

### Grafi pesati

Un grafo si dice pesato se esiste l’applicazione: E -> R oppure V -> R



* Avendo E -> R il costo α del cammino v1, v2 … vk è α = c(v1,v2) + c(v2,v3) … + c(vk-1 , vk)
* Avendo V -> R il costo α del cammino v1, v2 … vk è α = c(v1) + c(v2) … + c(vk)

Ricordando che da un vertice v potrebbe essere possibile arrivare ad un altro vertice w in più modi si definisce cammino di costo minimo da v a w il cammino con l’α più piccolo (stesso concetto per cammino di costo massimo)

Quando abbiamo a che fare con dei grafi pesati cambia la rappresentazione matriciale. Per esempio la matrice associata a G1 non sarà più una matrice booleana ma una matrice di interi, nella posizione (i,j) ci sarà 0 se non è possibile fare i->j , invece ci sarà il costo dell’arco se è possibile farlo

Matrice dei costi di G1

|  |  |  |
| --- | --- | --- |
| 0 | 3 | 0 |
| 3 | 0 | 2 |
| 0 | 2 | 0 |

Se invece dobbiamo rappresentare un grafo con V->R ad esempio G2 costruiremo la solita matrice booleana che dice se esiste l’arco (i,j) o meno e poi assoceremo un vettore al grafo di lunghezza n (n sarebbe |V|, nella posizione 1 ci sarà il costo del vertice 1, nella posizione 2 il costo del vertice 2 ecc

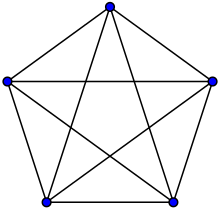
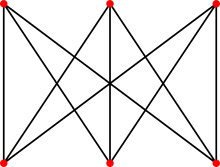
Ad esempio il vettore coi costi dei nodi di G2 sarebbe:

|  |  |
| --- | --- |
| 5 | 3 |

### Grafo planare

Si chiama grafo planare un grafo che è possibile rappresentare sul piano evitando intersezioni tra gli archi

### Due grafi NON planari importanti

Questo grafo è K5 Questo grafo è K3,3

### Teorema di Kuratowski

Un grafo è planare se e solo se non ha alcun sottografo omeomorfo con K5 oppure K3,3

### Teorema

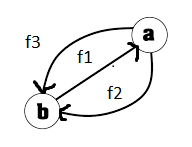
Se G è un grafo connesso e planare con almeno 3 nodi (|V|>=3) segue che |E|≤ 3\*|V| - 6

### Teorema

Se G è un grafo connesso e planare con almeno 4 nodi (|V| > 3) e non sono presenti cicli di lunghezza 3 segue che |E| ≤ 2\*|V| - 4

### Contare le facce

In un grafo disegnato senza intersecare gli archi possiamo contare anche le facce



### Teorema

Se G è un grafo connesso e planare segue che v – e + f =2 (v=numero di nodi , e=numero di archi , f= numero di facce)

### Teorema

Se G è un grafo connesso con |V|>= 3 e abbiamo che ẟ(v)>=2 per ogni v segue che G ha un ciclo

Dim:

Ordiniamo i vertici e chiamiamoli v1, v2,..., vn con n = |V| 3. Partiamo allora dal vertice v1 e costruiamo un cammino il più lungo possibile senza ripetizione di vertici. Supponiamo, senza ledere la generalità del discorso, che il cammino più lungo senza ripetizione di vertici sia v1, v2,..., vk . Se k = n allora abbiamo trovato un cammino hamiltoniano. In ogni caso, dal vertice vk possiamo ancora raggiungere un altro vertice, visto che il suo grado è almeno 2. Dal momento che ci siamo fermati, vuol dire che possiamo raggiungere un vertice già visto, quindi uno tra v1,..., vk2 il che dimostra l’esistenza di un ciclo

### Teorema

Se G è un grafo connesso e aciclico segue che |E|=|V| - 1

Dim:

Dimostriamo il teorema per induzione su |V.| Il teorema è banalmente vero se |V| =< 2. Supponiamo allora |V|>=3. Essendo il grafo connesso ed aciclico, deve esistere un vertice di grado 1 altrimenti il grafo avrebbe un ciclo, per quanto dimostrato prima, oppure sarebbe disconnesso, in grado di vertice con grado 0. Prendiamo allora un vertice v di grado 1 e rimuoviamolo dal grafo assieme all’arco su esso incidente. Il grafo indotto da V \ {v} è connesso, altrimenti dovremmo avere 2 vertici, u, w che sono connessi solo da un cammino passante per v, ossia u,..., u’ , v, w’ ,..., w ma ciò implicherebbe che v ha grado maggiore di 1. Quindi, tale grafo indotto è connesso ed aciclico e quindi per induzione ha |V| 2 archi. Aggiungendo v e l’arco ad esso incidente, abbiamo quindi che |E| = |V| 1.

### Grafo planare massimale/triangolare

Un grafo planare si dice massimale o triangolare se aggiungendo un arco a una coppia qualsiasi di vertici (non già collegati da un arco) perdo la condizione di planarità

### Colorazione di un grafo

Assegnamo un colore(etichetta) ad ogni vertice del grafo a condizione che due vertici adiacenti non abbiano lo stesso colore.

Indichiamo con X(G) il numero minimo di colori per colorare G

Un grafo è k-colorabile se rispetta questo vincolo colorando il grafo con al più colori

#### Grafo completo Kn

X(Kn)=n

#### Grafo con ciclo semplice Cn

Ossia, abbiamo v1,..., vn vertici e gli archi sono (v1, v2),(v2, v3), … ,(vn1, vn),(vn, v1). In pratica tutti i vertici del grafo fanno parte del ciclo. (questo particolare ciclo lo chiamiamo “semplice”)

X(Cn) = 2+ n mod 2

#### Grafo bipartito

X(Km,n)=2

### Teorema di Brooks

Sia G un grafo connesso con n vertici, segue che X(G) ≤ ẟ1 + 1 dove ẟ1 è il grado più alto di tutti

### Teorema di Brooks(versione forte)

Sia G un grafo connesso con n vertici, se G non è completo e non è un ciclo semplice con numero dispari di vertici segue che X(G) ≤ ẟ1 dove ẟ1 è il grado più alto di tutti

### Teorema dei 4 colori

Sia G un grafo planare segue che X(G) ≤ 4

### ALGORITMO MIGLIORE PER COLORARE UN GRAFO

1. Poni n=|V|
2. Per k=1 ad n {
3. Verifica se si può colorare il grafo con k colori, se si, termina
4. }

Il passo 3 si esegue nella seguente maniera

1. Genera permutazione di V
2. Sia c=1 il primo colore dei k colori
3. Per i=1 ad n {
4. Colora vi di c se si può, altrimenti se c=k termina a vai alla permutazione successiva,altrimenti passa al colore successivo (c=c+1) colorando vi con c
5. }

L’algoritmo è veramente troppo poco efficiente ,infatti consideriamo che dobbiamo analizzare nel caso peggiore n! permutazioni, se n=100 allora avremo da analizzare 9^157 permutazioni, un numero troppo alto per qualunque macchina di calcolo

Si utlizzano algoritmi approssimativi detti greedy, che danno un risultato più o meno soddisfacente solo se siamo “fortunati”,ovvero ci capitano permutazioni che fanno avvicinare la colorazione a quella dell’algoritmo che calcola in modo esatto (se riesce a terminare il processo)

Il problema della colorazione di un grafo appartiene a quella serie di problemi detti NP-Hard ,ovvero a cui non si trova un algoritmo risolutivo che abbia tempi di calcolo fattibili

Altri problemi NP-Hard sui grafi

1. Rendere aciclico un grafo eliminando meno vertici possibile, è detto problema della ricerca del feedback vertex set minimo (MFVS)
2. Trovare il massimo insieme indipendente: ovvero il sottoinsieme più grande di vertici non connessi tra loro da nessun arco
3. Trovare vertex cover , ovvero sottoinsieme di cardinalità minima ,C di V tale che tutti gli archi di E abbiano un estremo in C

ALBERI

### Albero libero

* Un albero libero è un grafo connesso e aciclico. Infatti un albero con |V| vertici ha |V|-1 archi
* Una foresta è un insieme di 1 o più alberi, quindi un grafo aciclico ma possibilmente con più di una componente connessa

### Albero radicato

* Identifichiamo un nodo detto Radice, da cui discendono tutti gli altri nodi
* Il nodo soprastante a un altro è detto padre, negli alberi ,il padre di un nodo è unico.
* Un nodo che non ha figli si dice foglia

In questi alberi identifichiamo due fattori :

* Fattore di ramificazione: numero massimo di figli di un nodo
* Altezza: cammino radice-foglia più lungo