Introduzione ai grafi expanders (per algebristi)

Carlo Casolo

giugno 2008

1 Introduzione

In modo informale, con il termine *expander graphs* s'intendono grafi che siano al contempo "sparsi" e "altamente connessi". Proprio la congiunzione di questi requisiti, apparentemente poco compatibili, rende tali grafi (la cui semplice esistenza è forse già controintuitiva) interessanti e, soprattutto, estremamente utili in diversi campi di applicazione. I grafi expander sono stati introdotti da Bassalygo e Pinsker nei primi anni '70 e, da allora, oltre a rappresentare uno stimolante argomento di studio, hanno trovato impiego in diversi settori della matematica e dell'informatica teorica (combinatorica, analisi funzionale, meccanica statistica e probabilità, derandomizzazione, teoria dei codici, teoria della complessità, solo per citarne alcuni), oltre che, nella pratica, nel disegno esplicito di algoritmi e reti con elevato grado di efficienza.
In queste note cercheremo di dare solo un'idea introduttiva della teoria astratta dei grafi expanders e, se ci sarà tempo, accenneremo ad alcune (poche) applicazioni. Poiché questo è un seminario di algebra, la nostra attenzione sarà comunque indirizzata verso gli aspetti più legati a tale disciplina, sia nella teoria che nelle applicazioni: per un quadro molto più ampio e approfondito, consiglio il sostanzioso articolo di Hoory, Linial e Wigderson [1] (dal quale, per altro, buona parte del materiale di queste note è stato prelevato).

1.1 Definizioni.

Useremo il termine "grafo" nella sua accezione più semplice; quindi un *grafo* $\Gamma = (V, E)$ è costituito da un insieme non vuoto di *vertici* V, ed un insieme E di *archi*, dove E è una scelta di sottoinsiemi di ordine 2 di V (quindi ogni arco è costituito da un coppia di vertici distinti). Tuttavia, molto di ciò che diremo vale anche per quelli che chiameremo "multigrafi", dove cioè si ammettono archi multipli (la stessa coppia di vertici può costituire gli estremi di più di un arco, ma non di infiniti) e anche i loop (archi con un solo estremo). Considereremo solo grafi finiti (ovvero su

un insieme finito di vertici), e se $\Gamma = (V, E)$ è un grafo, denoteremo con $|\Gamma|$ il numero dei suoi vertici, che chiameremo *ordine* di Γ, ed a cui riserviamo la lettera n. Il grado di un vertice v è il numero di archi incidenti a v (cioè archi di cui v è un estremo). Per quanto riguarda la teoria degli expanders, l'interesse (per ragioni che cercheremo di indicare) si concentra sui grafi *regolari*; un grafo Γ si dice regolare se i suoi vertici hanno tutti lo stesso grado; se tale grado comune è uguale a k si dice che Γ è un grafo k–regolare. Due vertici x, y sono *adiacenti*, e scriviamo $x \sim y$, se $\{x, y\}$ è un arco; il grafo Γ si dice *connesso* se per ogni coppia di vertici x, y esiste un cammino da x a y (cioè una successione di vertici $x = x_0, x_1, \ldots, x_n = y$, con $x_i \sim x_{i+1}$ e tutti i successivi archi distinti). Ricordiamo inoltre che un grafo si dice *bipartito* se l'insieme V dei suoi vertici ammette una partizione $V = A \cup B$ in due termini non vuoti, tale che ogni arco del grafo ha un estremo in A e l'altro in B. Ci sono diversi buoni testi di teoria dei grafi da consultare; per fissare un riferimento, scelgo il libro di B. Bollobas [4].

Il concetto di espansione (che è alla base della teoria dei grafi expanders) ha, come già detto, motivazioni e applicazioni in diversi ambiti; a me sembra però che il senso delle definizioni che stiamo per dare possa essere meglio intuito pensando ad un grafo come allo schema di una rete che distribuisca qualcosa, che sia al contempo economica (da qui la richiesta che il grafo sia sparso) ed efficiente, cioè capace di diffondere rapidamente (alta connettività), Un grafo è sparso se il numero di archi è piccolo rispetto a quello dei vertici. Naturalmente, si tratta di una definizione generica e non formale, il cui senso si comprende meglio pensando ad una famiglia $(X_i)_{i\geq 0}$ di grafi di ordine crescente; diremo che tale famiglia è costituita da grafi sparsi se esiste una costante c tale che, per ogni $X_i = (V_i, E_i)$, $|E_i| \leq c|V_i|$. Nella costruzione delle famiglie di expanders, questo requisito è ottenuto richiedendo che i grafi della famiglia siano k-regolari, per un fissato $k \geq 2$ (il numero di archi di un grafo k-regolare è $\frac{k}{2}|V|$). La nozione, ancora vaga, di "connettività" di un grafo viene formalizzata in diversi modi (non sempre equivalenti). Nella teoria classica, una delle maniere di assegnare un parametro (in questo caso un numero intero) che misuri la connettività di un grafo Γ è quello di determinare qual è il minimo numero di archi che è necessario togliere da Γ per renderlo sconnesso. Questa misura è però ancora grossolana (se Γ è k-regolare, si tratta di un intero tra 0 e k), può essere soggetta a perturbazioni locali, e non cattura compiutamente l'idea di capacità di diffusione. Infatti, più che assumere che occorra togliere un certo numero di archi per sconnettere il grafo in pezzi di cui non si ha alcun controllo, quello che sembra ragionevole richiedere è che per sconnettere il grafo in "pezzi grossi" occorra togliere molti più archi che per staccarne un pezzo piccolo.

Ora, se F è un sottoinsieme non vuoto dell'insieme V dei vertici del grafo Γ, gli archi che occorre togliere da Γ per staccare dal resto il sottografo indotto da F, sono

chiaramente quelli che hanno un estremo in F e l'altro nel complementare $V \setminus F$. L'insieme di tali archi si chiama la *frontiera* di F, e si denota con ∂F,

Sia $\Gamma = (V, E)$ un grafo (non necessariamente finito). Il **parametro di espansione** (o costante di Cheeger) di Γ è definito da

$$h(\Gamma) = \inf \left\{ \frac{|\partial F|}{\min\{|F|, |V \setminus F|\}} \,\middle|\, F \subseteq V,\ 0 < |F| < \infty \right\}. \tag{1}$$

Se V è finito (che è il caso che ci interessa) si ha chiaramente

$$h(\Gamma) = \inf \left\{ \frac{|\partial F|}{|F|} \,\middle|\, F \subseteq V,\ 0 < |F| \leq |V|/2 \right\}. \tag{2}$$

Esempi. 1) Consideriamo il grafo completo K_n (con $n \geq 3$). Se $F \neq \emptyset$ è un sottoinsieme di m vertici (quindi $1 \leq m \leq n$), allora $|\partial F| = m(n-m)$ e quindi $|\partial F|/|F| = n - m$, da cui segue che

$$h(K_n) = n - \left[\frac{n}{2}\right] = \begin{cases} n/2 & \text{se } n \text{ è pari} \\ (n+1)/2 & \text{se } n \text{ è dispari} \end{cases}$$

2) Esaminiamo ora il caso del ciclo C_n ($n \geq 3$). Se $F \neq \emptyset$ è un suo sottoinsieme di vertici con $|F| \leq n/2$, allora $2 \leq |\partial F| \leq 2|F|$, e il valore minimo di $|\partial F|/|F|$ si ottiene prendendo come F un insieme di $[n/2]$ vertici consecutivi. Si ha dunque

$$h(C_n) = \frac{2}{[n/2]} = \begin{cases} 4/n & \text{se } n \text{ è pari} \\ 4/(n-1) & \text{se } n \text{ è dispari} \end{cases}$$

3) Un esempio un po' più elaborato, ma sostanzialmente della stessa natura del precedente, è quello di una griglia quadrata. Fissato $n \geq 2$, sia $V_n = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, l'insieme dei vertici, e ogni vertice (a, b) sia adiacente ai vertici $(a \pm 1, b)$ e $(a, b \pm 1)$ (ovviamente, la somma è modulo n). Il grafo che si ottiene, che denotiamo con X_n è 4-regolare, e può essere rappresentato come l'insieme di punti e archi in un reticolo quadrato di lato n, con gli ovvi archi aggiuntivi sul perimetro. Supponiamo, per semplicità, che n sia pari, e consideriamo l'insieme F dei vertici delle prime $n/2$ righe dal basso; quindi $F = \{(a, b) \in V_n \mid 0 \leq b < n/2\}$, e $|F| = n^2/2$. I soli vertici di F che sono adiacenti a qualche vertice del suo complementare sono quelli appartenenti alle due righe esterne di F, ed ognuno è incidente ad un solo arco che esce da F; quindi $|\partial F| = 2n$. Dunque

$$h(X_n) \leq \frac{|\partial F|}{|F|} = \frac{2n}{n^2/2} = \frac{4}{n},$$

e, in particolare, $\lim_{n\to\infty} |h(X_n)| = 0$.

Veniamo quindi alla definizione fondamentale.

Definizione. Sia $k \geq 3$; una famiglia infinita di grafi finiti $\Gamma_n = (V_n, E_n)$, $1 \leq n \in \mathbb{N}$, si dice una *famiglia di k–expanders* se

- Γ_n è k–regolare per ogni $n \geq 1$;
- $\lim_{n\to\infty} |V_n| = \infty$;
- esiste $\epsilon > 0$ tale che $h(\Gamma_n) \geq \epsilon$ per ogni $n \geq 1$.

1.2 Esempi.

L'esistenza, per ogni grado $k \geq 3$, di famiglie di k-expanders, non è questione particolarmente difficile, e si dimostra mediante cosiddetti metodi probabilistici. Infatti, già nel 1973, Pinsker provò il seguente risultato.

Teorema 1. *Esiste $\delta > 0$, tale che per ogni $k \geq 3$, ed ogni $n \geq 2$, esiste un grafo k-regolare X, tale $|X| = n$ e $h(X) \geq \delta$.*

La dimostrazione richiede un po' di predisposizione per i conteggi, ma altrimenti non è difficile (quello che si fa è, sostanzialmente, stimare quanti sono i grafi k-regolari con n vertici e quanti quelli tra essi il cui parametro di espansione è minore di $k/2$, quindi verificare che la differenza non è zero); tuttavia non credo ci sia tempo per svolgerla in modo soddisfacente. La rimpiazziamo con un argomento euristico che, se non prova il Teorema 1, lo rende per lo meno plausibile. Fissato un vertice x di un grafo k-regolare ($k \geq 3$) con n vertici, la probabilità che un altro vertice y sia adiacente a x è k/n; quindi se S è un insieme non vuoto di vertici, il numero (probabilisticamente) atteso di vertici un estremo dei quali sia il nostro x e l'altro sia in S è $k|S|/n$; e dunque, se S e T sono sottoinsiemi non vuoti di vertici, il numero atteso di archi con un estremo in S e l'altro in T è $\frac{k}{n}|S||T|$. Ponendo $0 < |S| \leq \frac{n}{2}$ e $T = V \setminus S$, si ha che il valore atteso per $|\partial S|/|S|$ è $\frac{k(n-|S|)}{n}$, il cui minimo (il parametro di espansione) è $k/2$.

In effetti, si può dimostrare che esiste un $\delta > 0$ tale che se X è un grafo regolare di grado almeno 3, la probabilità che $h(X) \geq \delta$ tende a 1 al tendere di $|X|$ a infinito. Quindi, fissato $k \geq 3$, una famiglia casuale di grafi k-regolari di ordine strettamente crescente è una famiglia di expanders con probabilità 1.
A dispetto di ciò, la costruzione esplicita (e, possibilmente, algoritmicamente efficiente) di famiglie di expanders è soggetta a problemi molto sottili e spesso ardui. Naturalmente, si tratta di una questione di grande interesse, e non soltanto teorico, in considerazione delle varie applicazioni, anche pratiche, che trovano gli expanders.

I primi esempi di famiglie esplicite di expanders sono dovuti a Margulis (1973); in seguito diversi altri metodi per costruire famiglie di expanders sono stati trovati; e nella maggior parte dei casi, la dimostrazione che le famiglie di grafi proposte costituiscono famiglie di expanders, richiede analisi e strumenti tutt'altro che banali (che variano dall'algebra lineare, alla combinatoria, alla teoria dei numeri, alla teoria delle rappresentazioni dei gruppi, etc.). Una ragione di questo fatto, è che la definizione combinatoria (quella che abbiamo dato) di parametro di espansione è adatta ad essere trattata con successo dal punto di vista probabilistico, ma diventa molto difficile da trattare quando la si debba valutare in casi espliciti. A tal fine, risulta più maneggevole (comunque in maniera non banale) una definizione di tipo algebrico di famiglie di expanders.
Descriveremo questo approccio, basato sull'algebra lineare, nel prossimo paragrafo; prima vediamo (senza provare nulla) alcuni esempi di famiglie di expanders. I metodi generali finora noti per produrre famiglie del genere sono essenzialmente due: il primo, e più antico, legato alle rappresentazioni di certi gruppi finitamente generati, il secondo, più recente e forse più elementare, basato sull'iterazione di certe operazioni tra grafi. Questi metodi saranno descritti, rispettivamente, nella seconda e terza parte di queste note. Gli esempi che seguono sono del primo genere.

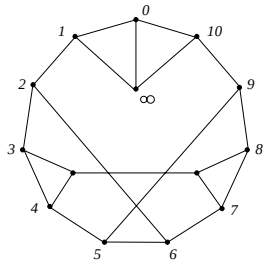
Esempio 1. (Margulis [15]) Questa è, in ordine di tempo, la prima famiglia esplicita di expanders ad essere stata individuata, e tuttora una delle più semplici da generare. Fissato $m \geq 3$, l'insieme dei vertici è $V_m = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Siano $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, e consideriamo le trasformazioni su V_m:

$$S = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

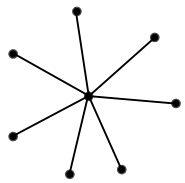
Ogni vertice $v = \begin{pmatrix} x \\ y \end{pmatrix}$ è adiacente ai vertici Sv, Tv, $Sv + e_1$, $Tv + e_2$, ed agli altri quattro vertici ottenuti applicando le quattro trasformazioni inverse. Si ottiene così un grafo M_m, 8-regolare di ordine m^2. Una dimostrazione (diversa da quella originale) che la famiglia M_m ($m \geq 3$) è una famiglia di expanders, dovuta a Gabber e Galil, che utilizza strumenti di algebra lineare, è riportata in [1]. Gabber e Galil trovano anche un esplicito limite inferiore al parametro di espansione: $h(M_m) \geq \frac{8-5\sqrt{2}}{2} > \frac{4}{9}$.
Si sarà osservato che i grafi M_m non sono semplici, dato che ammettono loops e archi multipli; tuttavia queste occorrenze sono in un numero finito, che non dipende da m, quindi asintoticamente non hanno rilevanza. Se poi si vuole insistere per grafi semplici, non è difficile aggiungere a M_m un numero finito (e fisso) di vertici su cui

far arrivare loops e doppi dei lati, ottenendo ancora grafi 8-regolari con parametro di espansione sostanzialmente invariato.

Esempio 2. (Lubotzky, Phillips, Sarnak [11], 1988). Una famiglia di expanders 3-regolari. In questo caso, i grafi sono indicizzati dai numeri primi $p \geq 5$: l'insieme dei vertici del grafo X_p è l'insieme degli elementi del campo $\mathbb{Z}/p\mathbb{Z}$; un elemento $0 \neq x \in \mathbb{Z}/p\mathbb{Z}$ è adiacente a $x+1$, $x-1$ e x^{-1}, mentre 0 è adiacente a $-1,\ 1,\ 0$. Per questa famiglia di grafi, la dimostrazione che il parametro di espansione è inferiormente limitato da un numero positivo ricorre a risultati piuttosto profondi di teoria dei numeri. Nel prossimo capitolo vedremo una parziale spiegazione (esercizio 18).
Anche in questo caso, i grafi X_p non sono semplici: vi sono loops ai vertici 0, 1, -1 e, per certi valori di p, due archi doppi. Per ricavarne grafi semplici, basta aggiungere un vertice ∞ adiacente a 0, 1, -1 (togliendo i loop a questi), inserire un vertice negli eventuali due archi di troppo e congiungere questi nuovi vertici tra loro. La figura mostra il grafo X_{11} dopo l'operazione.



Concludiamo questo paragrafo con un esempio banale, che potrebbe però aiutare a farsi una ragione del perché si lavori con grafi regolari. Per ogni $n \geq 2$, consideriamo la stella a n raggi T_n (la figura mostra T_7):



Si tratta di grafi sparsi (secondo la definizione che abbiamo dato: infatti T_n ha n archi e $n+1$ vertici), e quasi banali da generare. Sia F un sottoinsieme di vertici di T_n, con $0 < |F| = m \leq (n+1)/2$; se F contiene il vertice centrale allora $|\partial F| = n - (m-1)$, se invece F non contiene il vertice centrale, $|\partial F| = m$; si ricava quindi $h(T_n) = 1$. Dunque, a parte la regolarità, la famiglia dei T_n soddisfa i requisiti di espansione.
Il punto è che la definizione di frontiera che abbiamo dato e la conseguente definizione di paramento di espansione, sono formulate con riferimento agli archi (infatti, in

letteratura si parla di edge–expansion). Si possono però assumere concetti analoghi facendo riferimento ai vertici: se V è l'insieme dei vertici del grafo Γ, e F è un sottoinsieme non vuoto di V, la (vertex)–frontiera $\partial^v F$ di F è l'insieme dei vertici di $V \setminus F$ che sono adiacenti a qualche vertice di F, e quindi il parametro di (vertex)-espansione di Γ è

$$h^v(\Gamma) = \min\{|\partial^v F|/|F| \mid F \subseteq V,\ 0 < |F| \leq |V|/2\}.$$

Si vede allora che $h^v(T_n) = 2/n$, che tende a zero al tendere di n a infinito.
In generale, si ha $h^v(\Gamma) \leq h(\Gamma)$. Quindi, prescindendo dalla regolarità, le condizioni che definiscono famiglie di vertex-expanders sono più restrittive (lasciano fuori, ad esempio, le stelle T_n) di quelle per le famiglie di expanders come noi le stiamo considerando. Tuttavia, si vede subito che se il grafo Γ è k-regolare allora

$$\frac{1}{k} h^v(\Gamma) \leq h(\Gamma) \leq h^v(\Gamma). \tag{3}$$

Quindi per grafi con un fissato grado di regolarità, le due teorie coincidono (almeno per quanto concerne le famiglie di expanders).

1.3 Teoria spettrale.

Sia $\Gamma = (V, E)$ un (multi)grafo finito, e per ogni coppia di vertici u, v denotiamo con A_{uv} il numero di archi i cui estremi sono u e v. La **matrice di adiacenza** di Γ è la matrice $A(\Gamma)$ (che è conveniente vedere come una matrice a coefficienti nel campo complesso $\mathbb{C}$) i cui elementi sono i numeri interi A_{uv}. Se $|V| = n$, $A(\Gamma)$ è una matrice quadrata di ordine n, simmetrica (ed i cui termini diagonali, nel caso di grafi semplici, sono tutti nulli). Inoltre, per ogni $u \in V$,

$$\sum_{v \in V} A_{uv} = d_\Gamma(u). \tag{4}$$

La matrice di adiacenza A di un multigrafo con n vertici è simmetrica a valori reali (di fatto interi) e quindi, per il Teorema Spettrale, è diagonalizzabile sui reali. In particolare, tutti i suoi autovalori sono reali. Li denoteremo, contendone la molteplicità, con

$$\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}$$

e chiameremo questo lo *spettro* di A.

Esempi. 1) Calcoliamo lo spettro della matrice di adiacenza $A(K_n)$ del grafo completo su n vertici. Si ha, chiaramente, $A(K_n) = J_n - I_n$, dove J_n è la matrice $n \times n$ in cui ogni elemento è 1, e I_n la matrice identica di ordine n. Ne segue che gli autovalori

di $A(K_n)$ sono tutti e soli del tipo $\lambda - 1$, dove λ è autovalore di J_n. Ora, J_n ha rango 1, quindi il suo nucleo ha dimesione $n-1$, e pertanto 0 è autovalore di J_n con molteplicità $n-1$. L'altro autovalore di J_n è n (che, necessariamente, ha molteplicità 1). Pertanto, gli autovalori di $A(K_n)$ sono: $n-1$ con molteplicità 1, e -1 con molteplicità $n-1$.

2) Vediamo la matrice di adiacenza $A = A(C_n)$ di un n–ciclo C_n. Se $v_0, v_1, \ldots, v_{n-1}$ sono i vertici di C_n elencati in modo che vertici consecutivi siano adiacenti (e v_{n-1} adiacente a v_0), allora

$$A = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 1 \\ 1 & 0 & 1 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ . & . & . & \ldots & . & . \\ 0 & 0 & . & \ldots & 0 & 1 \\ 1 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix} = B + B^T \qquad \text{dove} \qquad B = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ . & . & . & \ldots & . \\ 0 & 0 & . & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Si osservi che $B^T = B^{-1}$; quindi B e B^T hanno gli stessi autospazi (relativi ad autovalori che sono l'uno l'inverso dell'altro). Ne segue che gli autovalori di A sono del tipo $\lambda + \lambda^{-1}$ dove λ è un autovalore di B. Ora, come si calcola facilmente, il polinomio caratteristico di B è $(-1)^n(x^n - 1)$; quindi gli autovalori di B sono le radici n–esime dell'unità, ovvero $\lambda_t = \cos\frac{2\pi t}{n} + i \sin\frac{2\pi t}{n}$ con $t = 0, 1, \ldots, n-1$. Ne segue che gli autovalori di A sono i numeri reali $\lambda_t + \lambda_t^{-1} = \lambda_t + \overline{\lambda_t} = 2\cos\frac{2\pi t}{n}$, con $t = 0, 1, \ldots, n-1$. Si osservi che $\mu_0 = 2\cos 0 = 2$, che ha molteplicità 1 (come deve essere dato che C_n è connesso). Gli altri autovalori hanno molteplicità 2, tranne eventualmente -2, che occorre se e solo se n è pari ed, in tal caso, ha molteplicità 1.

Gli esempi che abbiamo fornito si riferiscono entrambi a classi di grafi regolari. Dalla definizione di matrice di adiacenza segue immediatamente che un grafo Γ è k-regolare se e soltanto se la somma degli elementi di ciascuna riga (e di ciascuna colonna) di $A(\Gamma)$ è k (vedi (4)). Quindi, se Γ è k-regolare, il vettore $(1, 1, \ldots, 1)$ è un aurovettore per $A(\Gamma)$ con autovalore k. Più in generale, si provano facilmente i fatti seguenti.

Proposizione 2. *Sia Γ un grafo k-regolare, e sia $\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}$ lo spettro della sua matrice d'adiacenza. Allora*

(i) $\mu_0 = k$;

(ii) $|\mu_i| \leq k$ *per ogni* $i = 0, 1, \ldots, n-1$;

(iii) Γ *è connesso se e solo se* $\mu_0 > \mu_1$ *(ovvero k è autovalore di molteplicità* 1*).*

(iv) Γ *è bipartito se e solo se* $\mu_{n-1} = -k$.

Daremo più tardi un cenno della dimostrazione. Prima, vediamo subito il risultato (dovuto a Alon, Milman e Dodziuk - vedi [5]) che stabilisce la fondamentale connessione tra il parametro di espansione di un grafo k-regolare e quello che viene chiamato *intervallo spettrale principale* (ovvero la differenza $\mu_0 - \mu_1$).

Teorema 3. *Sia Γ un grafo connesso, k–regolare, con n vertici, e sia $\mu_0 \geq \cdots \geq \mu_{n-1}$ lo spettro della matrice di adiacenza di Γ. Allora*

$$\frac{k - \mu_1}{2} \leq h(\Gamma) \leq \sqrt{2k(k - \mu_1)}.$$

Se Γ è un grafo connesso e k-regolare, indichiamo con $\mu_1(\Gamma)$ il massimo autovalore di $A(\Gamma)$ diverso da k. Dal Teorema 3 e dalla definizione di famiglie di expanders, segue immediatamente

Corollario 4. *Una famiglia $(\Gamma_n)_{n\geq 1}$ di grafi connessi k–regolari, tale che $|\Gamma_n| \to \infty$ quando $n \to \infty$, è una famiglia di k–expanders se e solo se esiste un numero reale $\epsilon > 0$ tale che $k - \mu_1(\Gamma_n) \geq \epsilon$ per ogni $n \geq 1$.*

Si capisce che una famiglia $(\Gamma_n)_{n\geq 1}$ di k–expanders sarà tanto più pregiata quanto maggiore è il limite inferiore dei parametri $h(\Gamma_n)$. Si può provare che questo, asintoticamente, non può essere molto grande. Sussiste infatti il seguente Teorema, dovuto a Alon e Boppana (e che, se capisco bene, è un caso particolare di un risultato di Serre).

Teorema 5. *Sia $k \geq 2$, e sia Γ_n, $1 \leq n \in \mathbb{N}$, una famiglia di grafi connessi k–regolari, tale che $\lim_{n\to\infty} |V_n| = \infty$. Allora*

$$\liminf_{n\to\infty} \mu_1(\Gamma_n) \geq 2\sqrt{k-1}.$$

Sia $k \geq 3$. Un grafo finito connesso e k–regolare Γ si dice un *grafo di Ramanujan* se ogni autovalore $\mu \neq \pm k$ della sua matrice di adiacenza soddisfa $|\mu| \leq 2\sqrt{k-1}$. Il Teorema 5 ci dice che le famiglie di k–expanders teoricamente più efficienti sono quelle (se esistono) costituite da grafi di Ramanujan. Negli ultimi anni, famiglie infinite di grafi k–regolari di Ramanujan sono state costruite (da Margulis, da Lubotzy, Phillips e Sarnak, e da Morgenstern) per ogni $k = q + 1$, dove q è una potenza di un numero primo. Torneremo su queste costruzioni, che utilizzano grafi di Cayley in gruppi semplici finiti, nella prossima sezione; per una trattazione completa ed accessibile del caso $k = p + 1$ (p un primo dispari) rimandiamo comunque al testo [2] di Davidoff, Sarnak e Valette, La costruzione esplicita di famiglie infinite di grafi di Ramanujan per un $k \geq 3$ arbitrario è tuttora una questione aperta. Recentemente, è stato provato da Friedman che, per ogni $k \geq 3$ e $\epsilon > 0$, la probabilità che per un grafo

connesso k–regolare Γ, si abbia $\mu_1(\Gamma) \leq 2\sqrt{k-1} + \epsilon$ tende ad 1 quando il numero di vertici di Γ tende ad infinito (e quindi un grafo casuale k-regolare è asintoticamente di Ramanujan) .

Nel resto di questa sezione cerchiamo di dare un'idea di come gli strumenti di algebra lineare siano utilizzati nella dimostrazione di alcuni degli enunciati di sopra. Si tratta, come si vedrà, di metodi tutto sommato elementari, che tuttavia (a me sembra) hanno effetti miracolosi.
Per studiarne gli autovalori, è opportuno interpretare la matrice di adiacenza $A = A(\Gamma)$ (di un grafo con n vertici) come la matrice di un endomorfismo di uno spazio n-dimensionale. Se V denota l'insieme dei vertici di Γ, lo spazio che risulta conveniente considerare (essenzialmente dal punto di vista notazionale) è il $\mathbb{C}$-spazio vettoriale $\mathcal{C}(\Gamma) = \{f \mid f : V \to \mathbb{C}\}$ di tutte le applicazioni da V in $\mathbb{C}$. È uno spazio di dimensione n, una base del quale è costituita dalle applicazioni che assumono valore 1 in uno dei vertici e valore 0 sugli altri, e l'azione della matrice A su $\mathcal{C}(\Gamma)$ si descrive direttamente: se $f \in \mathcal{C}(\Gamma)$, allora per ogni $x \in V$ si ha

$$(Af)(x) = \sum_{y \in V} A_{xy} f(y) = \sum_{x \sim y} A_{xy} f(y), \tag{5}$$

dove $x \sim y$ indica che y varia nell'insieme dei vertici adiacenti a x (che sono tutti e soli i vertici y per cui $A_{xy} \neq 0$). Se Γ è un grafo semplice, allora

$$(Af)(x) = \sum_{x \sim y} f(y). \tag{6}$$

per ogni $f \in \mathcal{C}(\Gamma)$ ed ogni $x \in V$.

Vediamo la dimostrazione dei punti (i)–(iii) della Proposizione 2. Sia Γ k–regolare, e sia A la sua matrice d'adiacenza. Abbiamo già osservato che k è un autovalore di A. Sia μ un autovalore di A e sia $0 \neq f \in \mathcal{C}(\Gamma)$ un autovettore relativo a μ. Scegliamo $x \in V$ tale che $|f(x)|$ (modulo complesso) sia massimo. Osserviamo che, rimpiazzando eventualmente f con $\overline{f(x)}f$, possiamo assumere $0 < f(x) \in \mathbb{R}$. Allora

$$|\mu| f(x) = |\mu f(x)| = |Af(x)| = \Big| \sum_{y \in V} A_{xy} f(y) \Big| \leq \sum_{y \in V} A_{xy} |f(y)| \leq f(x) \sum_{y \in V} A_{xy} = k f(x).$$

Quindi $|\mu| \leq k$, il che prova i punti (i) e (ii) dell'enunciato.
Sia ora $0 \neq f$ un autovettore relativo a k e, come prima, sia $x \in V$ tale che $|f(x)|$ è massimo. Allora

$$kf(x) = Af(x) = \sum_{y \in V} A_{xy} f(y) = \sum_{y \sim x} A_{xy} f(y). \tag{7}$$

Dunque

$$f(x) = \sum_{y \sim x} \frac{A_{xy}}{k} f(y).$$

Poiché, per ogni $y \sim x$, $0 < A_{xy}/k \leq 1$ e $\sum_{y \sim x} A_{xy}/k = 1$, l'uguaglianza (7) ci dice che il numero complesso $f(x)$ appartiene all'inviluppo convesso dei punti $f(y)$ con $y \sim x$. Poiché ognuno di questi punti è contenuto nel cerchio di raggio $|f(x)|$, la sola possibilità è che $f(y) = f(x)$ per ogni $y \sim x$. Quindi, f è costante sulle componenti connesse di Γ. Pertanto, se Γ è connesso, l'autospazio di A relativo a k consiste in tutte e sole le applicazioni costanti su V, ed ha dunque dimensione 1. Ne segue che la molteplicità di k come autovalore di A è 1, ovvero che $k = \mu_0 > \mu_1$.
Se Γ non è connesso, sia U l'insieme dei vertici di una sua componente connessa e definiamo $f, g \in \mathcal{C}(\Gamma)$ ponendo, per ogni $x \in V$,

$$f(x) = \begin{cases} 1 & \text{se } x \in U \\ 0 & \text{se } x \in V \setminus U \end{cases} \qquad g(x) = \begin{cases} 0 & \text{se } x \in U \\ 1 & \text{se } x \in V \setminus U \end{cases}$$

Allora, f e g sono elementi indipendenti di $\mathcal{C}(\Gamma)$ e, come si verifica facilmente, autovettori di A relativi a k. Quindi la molteplicità di $\mu_0 = k$ è almeno 2 e pertanto $\mu_0 = \mu_1$. ■

Torniamo a considerazioni generali con $\Gamma = (V, E)$ (per il momento senza assunzione di regolarità). Lo spazio $\mathcal{C}(\Gamma)$ è dotato del prodotto scalare hermitiano standard

$$< f, g >= \sum_{x \in V} f(x)\overline{g(x)}.$$

per ogni $f, g \in \mathcal{C}(\Gamma)$; rispetto al quale, l'operatore associato ad A è hermitiano (cioè $< f, Af >=< Af, f >$ per ogni $f \in \mathcal{C}(\Gamma)$). Definiamo ora $D = D(\Gamma)$ come la matrice diagonale $n \times n$, i cui elementi sono

$$D_{xy} = \begin{cases} d_\Gamma(x) & \text{se } x = y \\ 0 & \text{se } x \neq y \end{cases}$$

L'*Operatore di Laplace* di Γ è l'operatore su $\mathcal{C}(\Gamma)$ associato alla matrice $L(\Gamma) = D - A$. Fissiamo un'*orientazione* di Γ: non è altro che una ordinamento lineare sull'insieme V dei vertici. Questa assegna ad ogni arco di Γ un verso, nel senso che possiamo descrivere ogni arco $e \in E$ come una coppia ordinata di vertici $e = \{e_-, e_+\}$, dove $e_- < e_+$ sono gli estremi di e. Posto $\mathcal{E}(\Gamma)$ il $\mathbb{C}$-spazio $\{u \mid u : E \to \mathbb{C}\}$, si definisce l'applicazione lineare $\delta : \mathcal{C}(\Gamma) \to \mathcal{E}(\Gamma)$ ponendo, per ogni $f \in \mathcal{C}(\Gamma)$, ed $e \in E$,

$$\delta f(e) = f(e_+) - f(e_-). \tag{8}$$

Si verifica allora facilmente la composizione $\delta^*\delta$, dove $\delta^* : \mathcal{E}(\Gamma) \to \mathcal{C}(\Gamma)$ è l'applicazione trasposta di δ, coincide con l'operatore di Laplace[1] su $\mathcal{C}(\Gamma)$.

Assumiamo da qui in avanti che Γ sia connesso e k-regolare. Poiché A è hermitiana, esiste una base ortonormale di $\mathcal{C}(\Gamma)$ composta da autovettori di A, e da questo (applicando la Proposizione 2) discende che per ogni $0 \neq f \in \mathcal{C}(\Gamma)$,

$$\frac{< Af, f >}{< f, f >} \in [\mu_{n-1}, \mu_0]. \tag{9}$$

Ora, l'autospazio di A relativo all'autovalore k è lo spazio, che denotiamo con $\mathcal{Z}$, delle funzioni costanti $V \to \mathbb{C}$. Poiché A è hermitiano, gli auovettori relativi agli autovalori diversi da k, appartengono allo spazio ortogonale $\mathcal{Z}^\perp$, che si verifica immediatamente essere

$$\mathcal{Z}^\perp = \{f \in \mathcal{C}(\Gamma) \mid \sum_{x \in V} f(x) = 0\}.$$

Possiamo quindi concludere che per ogni $f \in \mathcal{C}(\Gamma)$ tale che $\sum_{x \in V} f(x) = 0$, si ha

$$\frac{< Af, f >}{< f, f >} \in [\mu_{n-1}, \mu_1]; \tag{10}$$

e, in particolare, μ_1 è il massimo tra i valori $\frac{<Af,f>}{<f,f>}$, con $f \in \mathcal{Z}^\perp$.
Anche l'operatore di Laplace è reale simmetrico, e quindi hermitiano; e per esso valgono le considerazioni fatte sopra per A. Poiché Γ è k-regolare, la matrice D dei gradi non è altro che kI_n (dove I_n è la matrice identica di ordine n).e quindi la matrice dell'operatore di Laplace è $L = kI_n - A$. I suoi autovalori sono (dal più piccolo al più grande),

$$0 \leq k - \mu_1 \leq \cdots \leq k - \mu_{n-1}. \tag{11}$$

Poiché Γ è connesso, l'autovalore 0 di L ha molteplicità 1, e l'autospazio corrispondente coincide con l'autospazio di A relativo all'autovalore k, cioè $\mathcal{Z}$. Abbiamo cioè che il nucleo dell'operatore di Laplace di Γ è costituito dalle funzioni costanti in $\mathcal{C}(\Gamma)$. Poiché L è hermitiano, gli auovettori relativi agli autovalori di L diversi da 0, appartengono

[1] Fissato l'orientamento su Γ, una funzione $u \in \mathcal{E}(\Gamma)$ si può vedere come un,assegnazione di "flusso" ad ogni arco del grafo. L"operatore $\delta^* : \mathcal{E}(\Gamma) \to \mathcal{C}(\Gamma)$ risulta definito da

$$(\delta^* u)(x) = \sum_{x = e_+} u(e) - \sum_{x = e_-} u(e)$$

(per ogni $u \in \mathcal{E}(\Gamma)$ ed ogni $x \in V$); quindi δ^* è una versione discreta della *divergenza* in geometria differenziale. Similmente, l'operatore δ definito da (8) (che misura la variazione di $f \in \mathcal{C}(\Gamma)$ lungo gli archi), si può vedere com la versione discreta del *gradiente*. Quindi la composizione $\delta^*\delta$ (la divergenza del gradiente) rappresenta la versione discreta dell'usuale operatore di Laplace.

allo spazio ortogonale $\mathcal{Z}^{\perp}$. Come per A, per ogni $f \in \mathcal{C}(\Gamma)$ tale che $\sum_{x\in V} f(x) = 0$, si ha

$$\frac{< Lf, f >}{< f, f >} \geq k - \mu_1. \tag{12}$$

Possiamo ora dimostrare la prima disuguaglianza del Teorema 3.
Sia F un sottoinsieme non–vuoto di V; definiamo $f \in \mathcal{C}(\Gamma)$ ponendo, per ogni $x \in V$,

$$f(x) = \begin{cases} |V| - |F| & \text{se } x \in F \\ -|F| & \text{se } x \in V \setminus F \end{cases}$$

Si ha quindi

$$\sum_{x\in V} f(x) = |F|(|V| - |F|) - |V \setminus F||F| = 0,$$

e dunque (con le notazioni si sopra), $f \in \mathcal{Z}^{\perp}$. Inoltre

$$< f, f >= \sum_{x\in V} f(x)^2 = (|V| - |F|)^2|F| + |F|^2(|V| - |F|) = |V||F|(|V| - |F|). \tag{13}$$

Fissato un orientamento di Γ, sia $\delta : \mathcal{C}(\Gamma) \to \mathcal{E}(\Gamma)$ l'applicazione lineare definita in (8). Allora, per ogni $e \in E$,

$$\delta f(e) = f(e_+) - f(e_-) = \begin{cases} \pm|V| & \text{se } e \in \partial F \\ 0 & \text{se } e \notin \partial F \end{cases} \tag{14}$$

Sia $L = \delta^*\delta$ l'operatore di Laplace di Γ. Allora, tenendo conto di (14)

$$< Lf, f >=< \delta f, \delta f >= \sum_{e\in E} (\delta f(e))^2 = |V|^2|\partial F|.$$

Applicando ora la disuguaglianza (12), si ricava

$$k - \mu_1 \leq \frac{< Lf, f >}{< f, f >} = \frac{|V|^2|\partial F|}{|V||F|(|V| - |F|)} = \frac{|V||\partial F|}{|F|(|V| - |F|)}. \tag{15}$$

Prendendo F tale che $|F| \leq |V|/2$, dalla (15) segue

$$\frac{|\partial F|}{|F|} \geq \frac{k - \mu_1}{2}.$$

da cui l'asserto. ■

La dimostrazione della seconda disuguaglianza del Teorema 3 è più elaborata, ma utilizza strumenti simili; per questa rimandiamo a [2]. [1] o [6]. Invece, vediamo un'altra interessante proprietà del secondo autovalore. Per l'enunciato, fissiamo la

seguente notazione; se Γ è k-regolare, denotiamo con $\mu = \mu(\Gamma)$ il massimo tra i valori assoluti degli autovalori di $A(\Gamma)$ diversi da k; quindi $\mu = \max\{|\mu_1|, |\mu_{n-1}|\}$; se X e Y sono insiemi di vertici di Γ, intendiamo con $E(X,Y)$ l'insieme degli archi di Γ che hanno un estremo in X e l'altro in Y.

Lemma 6. (Expander Mixing Lemma) *Sia $\Gamma = (V,E)$ un grafo k-regolare con n vertici. Allora, per ogni $X, Y \subseteq V$,*

$$\left| |E(X,Y)| - \frac{k|X||Y|}{n} \right| \leq \mu\sqrt{|X||Y|}.$$

Diamo solo una traccia della dimostrazione. Sia A la matrice di adiacenza di Γ e siano f_X e f_Y le funzioni caratteristiche di X e di Y (come elementi dello spazio $\mathcal{C}(\Gamma)$). Allora

$$< f_X, Af_Y >= \sum_{x\in X} \sum_{x\sim y\in Y} A_{xy} = |E(X,Y)|. \tag{16}$$

Decomponiamo quindi $f_X = c_X + \alpha$, $f_Y = c_Y + \beta$, con c_X, c_Y costanti e α, β elementi di $\mathcal{Z}^{\perp}$; si vede che $c_X = |X|/n$ e $c_Y = |Y|/n$. Sostituendo in (16) , e tenendo conto delle relazioni di ortoogonalità si ha

$$|E(X,Y)| =< c_X, Ac_Y > + < \alpha, A\beta >= k\frac{|X||Y|}{n} + < \alpha, A\beta > . \tag{17}$$

Quindi

$$\left| |E(X,Y)| - \frac{k|X||Y|}{n} \right| = | < \alpha, A\beta > |. \tag{18}$$

A questo punto, si scrivono α e β come combinazioni lineari rispetto ad una base ortonormale (di autovettori relativi agli autovalori $\mu_1, \ldots, \mu_{n-1}$), si maggiora quindi il termine a destra di (18), tenendo conto che μ è il massimo dei valori assoluti $|\mu_1|, \ldots, |\mu_{n-1}|$, e applicando la diseguaglianza di Cauchy–Schwartz, si ottiene

$$| < \alpha, A\beta > | \leq \mu\sqrt{< \alpha, \alpha >}\sqrt{< \beta, \beta >} \leq \mu\sqrt{< f_X, f_X >}\sqrt{< f_Y, f_Y >} = \mu\sqrt{|X||Y|}$$

da cui l'enunciato. ∎

1.4 Passeggiate casuali.

Guardiamo al Lemma appena provato. La quantità $\frac{k|X||Y|}{n}$ esprime il valore atteso del numero di archi tra X e Y in condizioni casuali (vedi la discussione a pagina 4); dunque, il membro di sinistra nell'enunciato del Mixing Lemma misura la discrepanza tra il comportamento del grafo regolare Γ da quello casuale. Il Lemma dice quindi

che quanto più piccolo è il valore μ (e quindi quanto più grande è il parametro di espansione) tanto più prossimo è Γ ad un comportamento casuale.
Questa osservazione, se vogliamo generica, è alla radice di un'altra rilevante funzione svolta dai grafi expander, questa volta nell'ambito della teoria delle passeggiate casuali su un grafo. Si tratta di un aspetto molto importante della teoria degli expanders (e che è fondamentale in diverse applicazioni, come quelle alla derandomizzazione e all'analisi degli algoritmi di tipo "Monte–Carlo"), per il quale, in carenza di tempo e, soprattutto, di competenza da parte del sottoscritto, ci limiteremo ad un fugace cenno.

Una *passeggiata* su un grafo $\Gamma = (V, E)$ è semplicemente una successione $x_0, x_1, x_2, \ldots$ di vertici di Γ, tale che, per ogni i, x_{i+1} è adiacente a x_i; se, ad ogni passo, il termine x_{i+1} è scelto in modo casuale, ed indipendente dalle scelte precedenti, tra i vertici adiacenti a x_i, si parla allora di *passeggiata casuale*.
Supponiamo di avere iniziato una passeggiata casuale in x_0, e per $i \geq 0$, denotiamo con p_i la distribuzione di probabilità (su V) che descrive la probabilità di trovarsi al passo i in un certo vertice; cioè, per ogni $v \in V$, $p_i(v)$ è la probabilità che $v = x_i$ (quindi, p_i è un elemento dello spazio $\mathcal{C}(\Gamma)$, a valori reali positivi e somma 1). È un fatto fondamentale che, se Γ è connesso e non bipartito, allora le distribuzioni p_i convergono ad una distribuzione stazionaria.
Se Γ è un grafo k-regolare e connesso, allora si dimostra che, per ogni $i \geq 0$

$$p_{i+1} = \frac{A(\Gamma)}{k} p_i$$

(la matrice $\hat{A} = A(\Gamma)/k$ sè quella che si chiama matrice di transizione di Markov). In tal caso, la distribuzione stazionaria corrisponde ad un autovettore relativo all'autovalore $1 = k/k$ di $\hat{A}$; per quanto abbiamo visto in precedenza, esiste quindi un'unica distribuzione stazionaria per $\hat{A}$, che è quella uniforme $\mathbf{u}$ (cioè $\mathbf{u}(x) = 1/n$, per ogni $x \in V$. dove $n = |V|$).
Ora, un importante risultato mette in relazione la rapidità con cui le distribuzioni p_i tendono alla distribuzione uniforme, con il secondo autovalore di $\hat{A}$ (e, quindi, di $A = A(\Gamma)$). Precisamente, denotando con p la distribuzione di probabilità iniziale, e con μ il massimo tra i valori assoluti degli autovalori $\neq k$ di $A(\Gamma)$, si ha

per ogni $i \geq 1$

$$||\hat{A}^i p - \mathbf{u}|| \leq (\mu/k)^i \sqrt{n}. \tag{19}$$

(dove la norma è quella dello spazio $\mathcal{C}(\Gamma)$).

Quindi, la convergenza è rapida quando μ è piccolo, ovvero (ricordando che Γ è regolare) quando l'intervallo spettrale principale di $A(\Gamma)$ (e dunque il parametro di espansione di Γ) è grande.

Esprimendosi in modo spicciolo, ciò vuol dire che, iniziando da un qualsiasi vertice una passeggiata casuale in un grafo Γ che abbia parametro di espansione grande, dopo un numero relativamente piccolo di passi la probabilità di trovarsi in un qualunque vertice di Γ è grosso modo la stessa per ogni vertice. Un'ulteriore conferma che i grafi expander distribuiscono in modo molto efficiente.

* * *

Esercizio 1. Sia $\Gamma = (V, E)$ un grafo. Si provi che $h(\Gamma) = 0$ se e soltanto se Γ è sconnesso.

Esercizio 2. Un grafo ha diametro 2 se per ogni coppia di vertici non adiacenti esiste un terzo vertice che è adiacente ad entrambi. Sia Γ un grafo di diametro 2 (non necessariamente regolare); si provi che $h(\Gamma) \geq 1$. È possibile trovare una famiglia di expanders costituita tutta da grafi di diametro 2?

Esercizio 3. Dato un grafo $\Gamma = (V, E)$, costruiamo il grafo bipartito $D\Gamma$ nel modo seguente: l'insieme dei vertici di $D\Gamma$ è l'unione disgiunta $V_1 \cup V_2$ di due copie di V; quindi, sono date due biezioni $\alpha_1 : V_1 \to V$ e $\alpha_2 : V_2 \to V$. Un vertice $u \in V_1$ è adiacente a $v \in V_2$ se e solo se $\{\alpha_1(u), \alpha_2(v)\}$ è un arco in Γ. Si provi che $h(D\Gamma) \geq h(\Gamma)/2$; si concluda che, se per un $k \geq 3$ esistono famiglie di k-expanders, allora ne esistono costituite da grafi bipartiti.

Esercizio 4. Per ogni $n \geq 2$ il grafo *bipartito completo* $K_{n,n}$ è definito come il grafo il cui insieme di vertici è l'unione disgiunta $A \cup B$ di due insiemi di cardinalità n, ed ogni vertice di A è adiacente ad ogni vertice di B (e non ci sono altri archi). Si determini il parametro di espansione del grafo bipartito completo $K_{n,n}$. [Si distiguano i casi n pari e n dispari]

Esercizio 5. Si dimostri la relazione (3) a pagina 6.

Esercizio 6. Sia Γ un grafo connesso 3–regolare. Si provi che $h(\Gamma) \leq 1$.

Esercizio 7. *n–Cubi.* Sia $n \geq 2$; con il termine n-cubo, si intende il grafo Q_n il cui insieme dei vertici è quello delle n—uple a coefficienti in $\{0, 1\}$, ed i cui archi sono tutte e sole le coppie di tali n–uple che differiscono esattamente per una componente.

(1) Sia $A_n = A(Q_n)$ la matrice di adiacenza del cubo Q_n. Si provi che, per ogni $n \geq 2$ e considerato un opportuno ordinamento dei vertici di Q_{n+1}, si ha

$$A_{n+1} = \begin{pmatrix} A_n & I_n \\ I_n & A_n \end{pmatrix}.$$

(2) Procedendo per induzione su $n \geq 2$, si provi che gli autovalori di $A(Q_n)$ sono tutti e soli del tipo $n-2t$, con $t \in \mathbb{N}$ e $0 \leq t \leq n$; e che la molteplicità dell'autovalore $n-2t$ è $\binom{n}{t}$. [Si osservi che se A, M, P sono matrici quadrate con P invertibile, M diagonale e $PA = MP$, allora

$$\begin{pmatrix} P & P \\ P & -P \end{pmatrix} \begin{pmatrix} A & I \\ I & A \end{pmatrix} = \begin{pmatrix} M+I & 0 \\ I & M-I \end{pmatrix} \begin{pmatrix} P & P \\ P & -P \end{pmatrix}$$

(dove I è la matrice identica), e si applichi il punto precedente].

(3) Si provi che, per ogni $n \geq 2$, $h(Q_n) = 1$.

Esercizio 8. Sia Γ un grafo k–regolare. Si provi che la molteplicità di k come autovalore di $A(\Gamma)$ è uguale al numero di componenti connesse di Γ. Si provi che se Γ è bipartito allora $-k$ è un autovalore di $A(\Gamma)$.

Esercizio 9. Per $n \geq 2$, determinare lo spettro della matrice di adiacenza della stella T_n (definita a pagina 5), verificando che $h(T_n) >> \mu_0$.

Esercizio 10. Dato $n \geq 2$, si determini lo spettro della matrice di adiacenza del grafo completo bipartito $K_{n,n}$.

2 Expanders e Gruppi

Il legame (piuttosto profondo) tra la teoria dei gruppi e quella dei grafi expanders si manifesta principalmente nel fatto che diverse delle più interessanti costruzioni esplicite di famiglie di expanders sono realizzate mediante grafi di Cayley in gruppi (finiti). La cosa forse non stupisce, dato che quello dei grafi Cayley è un metodo fondamentale per generare (o, almeno, definire in modo compatto) grafi regolari. Di fatto, i grafi di Cayley sono molto più che regolari; infatti per ogni coppia di vertici x e y in un grafo di Cayley, esiste un automorfismo del grafo che manda x in y.

2.1 Grafi di Cayley.

In questo paragrafo richiamiamo brevemente la definizione e le principali proprietà dei grafi di Cayley.

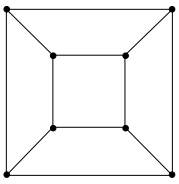
Sia G un gruppo, ed S un sottoinsieme di G con le seguenti proprietà

(C1) $1_G \notin S$;

(C2) $S = S^{-1}$.

Il **Grafo di Cayley** $\Gamma[G, S]$ è il grafo il cui insieme dei vertici è G, e gli archi sono tutti i sottoinsiemi $\{g, gs\}$, al variare di $g \in G$ ed $s \in S$. (Si osservi che la condizione (C1) su S serve a far sì che $g \neq gs$, per ogni $g \in G$ ed $s \in S$, mentre la condizione (C2) serve a rendere simmetrica la relazione di adiacenza, poiché infatti $\{g, gs\} = \{gs, (gs)s^{-1}\}$). Di fatto, se S è un sottoinsieme del gruppo G che non contiene 1_G, daremo significato anche alla notazione $\Gamma[G.S]$, intendendo con ciò il grafo di Cayley definito da $S \cup S^{-1}$.

Esempi. 1) Sia G il gruppo delle simmetrie di un quadrato; allora $|G| = 8$ e $G = \langle \rho, \tau \rangle$, dove ρ è una rotazione di un angolo d $\pi/2$ e τ la una riflessione con asse una delle diagonali; si ha $|\rho| = 4$, $|\tau| = 2$ e, come si verifica subito, $\tau\rho\tau = \rho^{-1}$ (di fatto, G è isomorfo al gruppo diedrale di ordine 8). Posto $S = \{\rho, \rho^{-1}, \tau\}$, si trova che il grafo di Cayley $\Gamma[G, S]$ è isomorfo al grafo del cubo



2) Sia $G = S_3$ il gruppo simmetrico su 3 punti, e sia $S = \{(12), (23)\}$. Allora il grafo di Cayley $\Gamma[G, S]$ è un 6-ciclo. Più in generale, si osserva facilmente che se x, y sono due involuzioni (cioè elementi di ordine 2) di un gruppo finito G, e $G = \langle x\ y \rangle$

(in questo caso un semplice argomento mostra che G è un gruppo diedrale), allora $\Gamma[G, \{x, y\}]$ è un ciclo di lunghezza $|G|$.

3) Sia $n \geq 2$ e sia $G = \langle x_1 \rangle \times \cdots \times \langle x_n \rangle$, il prodotto diretto di n gruppi ciclici di ordine 2. Posto $S = \{x_1, \ldots, x_n\}$, il grafo di Cayley $\Gamma[G, S]$ è isomorfo al n–cybo Q_n (esercizio 7).

Proposizione 7. *Sia G un gruppo finito ed S un sottoinsieme di G che soddisfa le condizioni (C1) e (C2); sia $|S| = k$. Allora*

(1) *$\Gamma[G, S]$ è un grafo k-regolare;*

(2) *il numero di componenti connesse di $\Gamma[G, S]$ è uguale all'indice $[G : \langle S \rangle]$; in particolare, $\Gamma[G, S]$ è connesso se e solo se S è un sistema di generatori di G.*

Dimostrazione. Che $\Gamma = \Gamma[G, S]$ sia un grafo (semplice) risulta dalla costruzione. Inoltre è chiaramente k-regolare: infatti per ogni vertice $g \in G$, l'insieme dei vertici adiacenti a g è dato dai vertici gs, con $s \in S$, che, al variare di $s \in S$, sono tutti distinti (legge di cancellazione per i gruppi). Questo prova il punto (1).
Per il punto (2), poniamo $H = \langle S \rangle$. Siano $x, y \in G$ e $x = g_0, g_1, g_2, \ldots, g_n = y$ un cammino in Γ dal vertice x a y. Allora esistono $s_1, \ldots s_n \in S$ tali che $g_1 = xs_1$, $g_2 = g_1 s_2 = xs_1 s_2$, e così via, sino a $y = g_{n-1}s_n = (xs_1 \cdots s_{n-1})s_n = xs_1 \cdots s_{n-1}s_n$. Posto $h = s_1 \cdots s_n$, si ha $h \in H$ e $y = xh$, da cui $xH = yH$. Viceversa, siano $x, y \in G$ tali che $xH = yH$. Allora $y \in xH$, e quindi, per le proprietà di S, esistono $s_1, \ldots, s_n \in S$ (con $s_{i+1} \neq s_i^{-1}$) tali che $y = xs_1 \cdots s_n$. Ponendo $g_1 = xs_1$ e, per ogni $i = 2, \ldots, n$, $g_i = xs_1 \cdots s_{i-1}s_i$, si ricava il cammino x, $g_1, \ldots g_{n-1}$, $g_n = y$ in Γ. Abbiamo quindi provato che due vertici x, y di Γ appartengono alla stessa componente connessa se e solo se $xH = yH$, il che prova il punto (2). In particolare, l'insieme dei vertici della componente connessa che contiene 1_G è costituito dagli elementi di H, e Γ è connesso se e solo se $H = G$, ovvero S è un sistema di generatori di G. ∎

In un grafo connesso Γ, la *distanza* $d_\Gamma(x, y)$ tra due vertici x e y è definita come la lunghezza minima di un cammino tra x e y, e il *diametro* di Γ è il massimo delle distanze tra i suoi vertici. Osserviamo allora come dalla dimostrazione del punto (2) segua che se $\Gamma = \Gamma[G, S]$ è connesso, e $x, y \in G$, la distanza $d_\Gamma(x, y)$ coincide con la lunghezza minima $\ell_S(h)$ di un elemento $h \in \langle S \rangle$ tale che $y = xh$ (ovvero, il minimo $t \geq 0$ tale che $h = s_1 \cdots s_t$, con $s_i \in S$, e intendendo che $\ell_S(1) = 0$).

Ricordo che un *isomorfismo* tra i due grafi $\Gamma = (V, E)$ e $\Gamma' = (V', E')$ è una biezione $\phi : V \to V'$, tale che, per ogni $x, y \in V$, $\{x, y\} \in E \Leftrightarrow \{\phi(x), \phi(y)\} \in E'$. Un isomorfismo da Γ in se stesso si dice *automorfismo* di Γ. Come in molte altre situazioni, è immediato verificare che l'insieme $Aut(\Gamma)$ degli automorfismi di un grafo Γ è un gruppo rispetto alla composizione. Un grafo $\Gamma = (V, E)$ si dice *vertex–transitivo* se

per ogni coppia di vertici $v, w \in V$ esiste un automorfismo α di Γ tale che $\alpha(v) = w$. Chiaramente un grafo vertex–transitivo è regolare.
Sia G un gruppo, $\Gamma = \Gamma[G, S]$ un grafo di Cayley, e sia $g \in G$. Allora la moltiplicazione a sinistra $\lambda_g : G \to G$, definita da $x \mapsto gx$ (per ogni $x \in G$), è una biezione dell'insieme dei vertici di Γ che conserva la relazione di adiacenza; infatti, per ogni $x \in G$ e ogni $s \in S$, si ha $\lambda_g(\{x, xs\}) = \{gx, (gx)s\}$. Quindi λ_g induce un automorfismo del grafo Γ (la posizione $g \mapsto \lambda_{g^{-1}}$ definisce un omomorfismo iniettivo del gruppo G nel gruppo $Aut(\Gamma)$). Se x, y è una coppia di vertici del grafo di Cayley $\Gamma[G, S]$, ponendo $g = yx^{-1}$, si ha $\lambda_g(x) = y$. Dunque ogni grafo di Cayley e vertex–transitivo.

Proposizione 8. *Sia G un gruppo finito ed S un sottoinsieme di G che soddisfa le condizioni (C 1) e (C 2). Allora, per ogni $g \in G$, la moltiplicazione a sinistra per g induce un automorfismo di $\Gamma = \Gamma[G, S]$, e G è isomorfo ad un sottogruppo di $Aut(\Gamma)$ che è transitivo sull'insieme dei vertici di Γ. In particolare, Γ è vertex–transitivo.*

Questa proprietà dei grafi di Cayley è molto importante. Consente di valutare il comportamento locale del grafo a partire da qualsiasi vertice ci piaccia, in particolare a partire dal vertice 1_G. Così, ad esempio, il diametro di un grafo di Cayley connesso $\Gamma = \Gamma[G, S]$ coincide con $\sup_{g \in G} d_\Gamma(1_G, g)$; per quanto osservato in precedenza, possiamo quindi affermare che, se S è un sistema di generatori di G, allora

$$diam(\Gamma[G, S]) = \sup_{g \in G} \ell_S(g). \tag{20}$$

Grafi di Cayley e rappresentazioni. Sia G un gruppo finito, S un sottoinsieme di G che soddisfa le condizioni (C1) e (C2), e sia $\Gamma = \Gamma[G, S]$ il grafo di Cayley associato ad S. Come nel capitolo 1, denotiamo con $\mathcal{C}(\Gamma)$ lo spazio delle applicazioni $f : G \to \mathbb{C}$ (poiché G è l'insieme dei vertici di Γ), e con $A = A(\Gamma)$ la matrice di adiacenza di Γ. Ora, sullo spazio $\mathcal{C}(\Gamma)$, G opera in modo naturale mediante la *rappresentazione regolare* (sui complessi); precisamente, denotando con $r : G \to Aut(\mathcal{C}(\Gamma))$ la rappresentazione regolare di G, per ogni $f \in \mathcal{C}(\Gamma)$ ed ogni $x, g \in G$ si ha: $(r(x)f)(g) = f(gx)$. Poniamo

$$A_r = A_r(S) = \sum_{x \in S} r(x).$$

Allora, per ogni $f \in \mathcal{C}(\Gamma)$, ed ogni $g \in G$

$$Af(g) = \sum_{y \sim g} f(y) = \sum_{x \in S} f(gx) = \sum_{x \in S} (r(x))(g) = A_r f(g). \tag{21}$$

Quindi A_r coincide con l'operatore A dato dalla matrice di adiacenza del grafo di Cayley generato da S. Ora, è noto che la rappresentazione regolare di G sui complessi è

la somma ortogonale delle rappresentazioni *irriducibili* di G (ognuna con molteplicitàà uguale alla sua dimensione). Per ogni rappresentazione complessa irriducibile ρ di G, definiamo

$$A_\rho = A_\rho(S) = \sum_{x \in S} \rho(x). \tag{22}$$

Dunque, l'operatore A_r (che per (21) coincide con A) è somma ortogonale – con opportuna molteplicità – degli A_ρ, al variare di ρ tra tutte le rappresentazioni irriducibili di G; segue allora la seguente importante osservazione.

Proposizione 9. *Sia A la matrice di adiacenza del grafo di Cayley $\Gamma = \Gamma[G, S]$. Allora*

(i) $A = A_r(S)$, dove r è la rappresentazione regolare di G;

(ii) l'insieme degli autovalori di A coincide con l'unione degli insiemi degli autovalori delle matrici $A_\rho(S)$, al variare di ρ tra tutte le rappresentazioni irriducibili di G.

Osserviamo che (se $|S| = k$) l'autovalore banale k di A corrisponde all'autovalore relativo alla rappresentazione banale 1_G (quella che associa ad ogni elemento di G l'identità). Se S è un sistema di generatori di G, tale autovalore non appartine ad alcuna altra A_ρ con $\rho \neq 1_G$. Concludiamo pertanto che, se S è un sistema di genratori di G che soddisfa (C1) e (C2),

il primo autovalore non–banale μ_1 di A coincide con il massimo tra gli autovalori degli operatori A_ρ, al variare di ρ tra le rappresentazioni irriducibili non–banali di G.

Quindi, in linea di principio, per valutare l'intervallo spettrale di un grafo di Cayley $\Gamma[G, S]$ è sufficiente determinare gli autovalori degli operatori $A_\rho(S)$ associati alle rappresentazioni irriducibili non–banali ρ di G. Ciò, in generale, non è più semplice che trattare direttamente la matrice di adiacenza; tuttavia, quando si abbiano abbastanza informazioni sulle rappresentazioni di G, e di certi gruppi ad esso correlati, questo metodo si rivela efficace, come vedremo nella prossimo paragrafo. Per il momento, come prima applicazione della Proposizione 9, proviamo che non esistono famiglie di expanders costituite solo da grafi di Cayley di gruppi *abeliani*. La dimostrazione è una variazione di una di Lubotzky e Weiss [12].

Proposizione 10. *Sia A un gruppo finito abeliano, ed $S = S^{-1}$ un sistema di generatori di A, con $|S| = k$. Sia μ il massimo autovalore $\neq k$ di $\Gamma[A, S]$. Allora*

$$|A| \leq \Big(\frac{2k}{k - \mu} + 1\Big)^k.$$

Dimostrazione. Le rappresentazioni irriducibili di A sono gli elementi del suo duale $\hat{A}$, ovvero gli omomorfismi $A \to S^1$, dove $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ è il toro complesso.

Se $\rho \in \hat{A}$, allora A_ρ è semplicemente la moltiplicazione in $\mathbb{C}$ per $\sum_{s\in S}\rho(s)$. Quindi, per la proposizione 9,

$$\mu = \max\Big\{ \sum_{s\in S}\rho(s) \;\Big|\; 1 \neq \rho \in \hat{A}\Big\}. \tag{23}$$

Ponimao $r = \left[\frac{2k}{k-\mu}\right] + 1$. Suddividiamo quindi il cerchio S^1 in r settori di uguale ampiezza $2\pi/r$ a partire dal punto $\eta = e^{\frac{\pi i}{r}}$. Questa partizione di S^1 determina una partizione nell'insieme delle k–uple $(S^1)^k$.
Sia $S = \{s_1, \ldots, s_k\}$ e supponiamo (per assurdo) che esistano due elementi $\alpha, \beta \in \hat{A}$, con $\alpha \neq \beta$, tali che le k-uple $(\alpha(s_1), \ldots, \alpha(s_k))$ e $(\beta(s_1), \ldots, \beta(s_k))$ appartengano allo stesso termine della partizione di $(S^1)^k$. Allora, per ogni $i = 1, \ldots, k$, il valore $\alpha^{-1}\beta(s_i)$ appartiene all'arco (η^{-1}, η) di S^1, e quindi

$$\sum_{i=1}^{k} \alpha^{-1}\beta(s_i) \geq k \cdot \cos\frac{\pi i}{r}.$$

Poiché $1 \neq \alpha^{-1}\beta \in \hat{A}$, da (23) segue $\mu \geq k \cdot \cos\frac{\pi i}{r} \geq k(1 - \frac{2}{r})$; da cui discende l'assurdo $r \leq 2k/(k-\mu)$. Dunque, al variare di $\alpha \in \hat{A}$, le k-uple $(\alpha(s_1), \ldots, \alpha(s_k))$ appartengono a distinti termini della partizione assegnata a $(S^1)^k$. Pertanto

$$|A| = |\hat{A}| \leq r^k$$

da cui l'enunciato. ∎

Da questo segue chiaramente che, fissato k, nessuna famiglia infinita di grafi di Cayley k-regolari di gruppi abeliani può essere una famiglia di expanders..

Grafi di Schreier. Sia G un gruppo finito, e sia $\pi : G \to Sym(X)$ una rappresentazione di G come gruppo di permutazioni dell'insieme (finito) X. Per ogni $g \in G$ e $x \in X$, scriviamo $x^g = x^{\pi(g)}$. Sia S un sottoinsieme fissato di G, con $S = S^{-1}$.
Il *Grafo di Schreier* $Sch[\pi, S]$ è il grafo il cui insieme dei vertici è l'insieme X, e gli archi sono tutte le coppie (x, x^s) al variare di $x \in X$ e $s \in S$ (considerando $(x, x^s) = (y, y^t)$ se e solo se $x = y$ e $s = t$, oppure $y = x^s$ e $t = s^{-1}$).
Si tratta di un grafo regolare di grado $k = |S|$, che in generale non è né semplice (ci possono essere diversi loops, corrispondenti ai punti fissi di elementi di S, ed archi multipli), né vertex–transitivo[2]. Nel caso in cui π è la rappresentazione definita dalla moltiplicazione a destra di G su se stesso, il grafo di Schreier $Sch[\pi, S]$ coincide con il grafo di Cayley $\Gamma[G, S]$.

[2]Citiamo, infatti, il seguente risultato di J. Gross (1977): *Ogni grafo regolare di grado pari è un grafo di Schreier.*

Sia ora $\pi : G \to Sym(X)$ una rappresentazione di G come gruppo di permutazioni; ad essa è associata in modo naturale una rappresentazione lineare ρ_π (detta "permutation representation") di G sul $\mathbb{C}$-spazio V generato da X. In modo esplicito, sia V lo spazio delle funzioni $X \to \mathbb{C}$: per ogni $f \in V$ e $g \in G$, si pone

$$(\rho_\pi(g)f)(x) = f(x^g)$$

per ogni $x \in X$. Sia S un sottoinsieme finito di G, sia $\Sigma = Sch[\pi, S]$ il grafo di Shreier associato a π ed S, e $A(\Sigma)$ la sua matrice d'adiacenza. Ragionando come nel caso dei grafi di Cayley, si vede facilmente che

$$A(\Sigma) = A_{\rho_\pi},$$

dove A_{ρ_π} è definita come in (22). Poiché, come abbiamo osservato sopra, ogni autovalore di A_{ρ_π} è un autovalore di A_r (dove r è la rappresentazione regolare di G) e poiché $A_r = A(\Gamma[G, S])$, concludiamo che

Proposizione 11. *Sia $\pi : G \to X$ un'azione di un gruppo finito G su un insieme X, e sia S un sistema di generatori di G con $S = S^{-1}$. Allora, per ogni componente connessa Δ del grafo di Schreier $Sch[\pi, S]$ si ha*

$$\mu_1(\Delta) \leq \mu_1(\Gamma[G, S]).$$

Quindi, grafi di Schreier associati a grafi di Cayley che sono expanders, sono a loro volta expanders. Con questa metodo è, ad esempio, costruita e trattata la famiglia di grafi expanders dell'esempio 2 a pagina 5 (vedi esercizio 18).

2.2 La costante di Kazhdan.

Il primo, e per due decenni l'unico, metodo generale per costruire famiglie di grafi expanders (quello introdotto da Margulis, da Lubotzy ed altri) consiste nel considerare la famiglia dei grafi di Cayley in immagini finite di un gruppo infinito e finitamemente generato H, rispetto a sistemi di generatori immagine di un fissato sistema finito di generatori di H. Con questo metodo (o suoi derivati) sono costruiti gli esempi riportati nel capitolo 1 e le famiglie di grafi di Ramanujan che vedremo più avanti[3].
Sia H un gruppo infinito (gruppo madre), finitamente generato che, per comodità, assumiamo anche residualmente finito (cioè l'intersezione dei sottogruppi normali di indice finito di H è banale), e fissiamo un sistema finito S di generatori di H (con S che soddisfa (C2)). Per ogni $n \geq 1$, sia $\pi_n : H \to G_n$ un omomorfismo suriettivo di

[3]Un metodo più recente – ed anche più elementare – basato su certe operazioni di prodotto di grafi, sviluppato da Reingold, Vadhan e Wigderson, sarà l'argomento principale del prossimo capitolo.

H in un gruppo finito G_n, con $|G_{i+1}| > |G_i|$. In questa situazione si prova che se H soddisfa certe proprietà (in genere non proprio facili da stabilire), allora la famiglia di grafi di Cayley $\Gamma(G_n, \pi_n(S))$ è una famiglia di expanders.
Di queste proprietà del gruppo madre, le più importanti nel nostro contesto sono la proprietà (T) di Kazhdan ed una sua discendente, la proprietà (τ) di Lubotzy. Entrambe sono definite in modo naturale nel contesto di gruppi di Lie ed hanno importanti applicazioni in diversi altri problemi. Di nessuna delle due daremo le definizioni più generali, cosa che ci porterebbe forse troppo lontano (in primo luogo da ciò che conosco); ci accontenteremo, quando andrà bene, di descrizioni equivalenti ristrette al caso discreto, e di osservazioni parzialmente informali, augurandoci di poter comunque dare un'idea della loro rilevanza alla questione che ci interessa, e del loro utilizzo (per l'approfondimento rimando al libro di Lubotzy [3], ed a quello in preparazione, *On property* (τ), di Lubotzy e Zuk). Cominciamo con la proprietà (T).

Sia H un gruppo (qui, il caso infinito è quello rilevante). Indichiamo le rappresentazioni (sui complessi) di H mediante coppie (V, ρ), intendendo che V è lo spazio su cui H agisce e ρ l'omomorfismo $H \to Aut(V)$ definito dalla rappresentazione. Denotiamo con $(H)_0$ l'insieme delle rappresentazioni *unitarie* (a meno di equivalenza, e continue nel caso di un gruppo topologico) di H che sono prive di vettori invarianti. Un gruppo H soddisfa la proprietà (T) se la rappresentazione banale 1-dimensionale è isolata da $(H)_0$, secondo una certa topologia, detta topologia di Fell, definita sull'insieme delle rappresentazioni (continue) di H.

Per gruppi discreti, la proprietà (T) implica la finita generazione, ed in tal caso la definizione è equivalente alla seguente (vedi [3]).
Sia H un gruppo finitamente generato e sia $S = S^{-1}$ un sistema finito di generatori di H; allora H soddisfa la *proprietà* (T) *di Kazhdan*, se esiste una costante $\kappa = \kappa(H, S) > 0$ tale che per ogni $(V, \rho) \in (H)_0$ ed ogni $v \in V$,

$$\max_{s \in S} ||\rho(s)v - v|| \geq \kappa ||v||. \tag{24}$$

Si prova che la proprietà (T) per il gruppo finitamente generato H *è indipendente dalla scelta del sistema finito di generatori* S; anche se la costante $\kappa(H, S)$, che è detta "costante di Kazhdan" di H relativa a S, non lo è (infatti, è possibile descrivere un gruppo H ed una successione S_n $(n \in \mathbb{N})$ di sistemi di generatori, tutti dello stesso ordine, tali che $\kappa(H, S_n) > 0$ per ogni $n \in \mathbb{N}$, ma $\lim_{n \to \infty} \kappa(H, S_n) = 0$ - vedi [3] per i dettagli).

Se G è un gruppo finito, la proprietà (T) è fuori discussione; tuttavia un esame sommario, in questo caso, delle implicazioni della costante $\kappa(G, S)$, può essere propizio al formarsi di un'idea, almeno intuitiva, delle ragioni dell'importanza di tale nozione

per l'analisi dell'intervallo spettrale dei grafi di Cayley. Siano quindi G un gruppo finito, S un sistema di generatori per G, $\Gamma = \Gamma[G, S]$, ed A la matrice d'adiacenza di Γ. Posto $\mu = \mu_1(\Gamma)$, l'osservazione (10) del Capitolo 1 ci dice che

$$\mu = \max_{u \in \mathcal{Z}^\perp} \frac{< Au, u >}{||u||^2} \tag{25}$$

dove il prodotto è quello hermitiano standard dello spazio $\mathcal{C}(\Gamma) = \{f \mid f : G \to \mathbb{C}\}$, $\mathcal{Z}^\perp$ è il sottospazio delle funzioni a somma 0, e $|| \cdot ||$ è la norma su $\mathcal{C}(\Gamma)$ ($||u|| = \sqrt{< u, u >}$). Osserviamo anche che la rappresentazione regolare r di G su $\mathcal{C}(\Gamma)$ è una rappresentazione unitaria; infatti, per ogni $g \in G$ ed $u \in \mathcal{C}(\Gamma)$

$$< r(g)u, r(g)u >= \sum_{x \in G} |(r(g)u)(x)|^2 = \sum_{x \in G} |u(xg)|^2 = \sum_{x \in G} |u(x)|^2 =< u, u > .$$

Inoltre, $\mathcal{Z}$ e $\mathcal{Z}^\perp$ sono spazi invarianti per r; anzi, $\mathcal{Z}$ è lo spazio di tutti i vettori invarianti, e quindi $\mathcal{Z}^\perp$ non contiene vettori invarianti per la rappresentazione r. Dunque

$$(\mathcal{Z}^\perp, r) \in (G)_0. \tag{26}$$

Ora, per quanto visto nel paragrafo precedende, possiamo in (25) sostituire ad A l'operatore $A_r = \sum_{s \in S} r(s)$. Un calcolo elementare dà, per ogni $u \in \mathcal{C}(\Gamma)$, $s \in S$,

$$\frac{||r(s)u - u||^2}{||u||^2} = 2 - 2\frac{< r(s)u, u >}{||u||^2}.$$

Pertanto, se $|S| = k$,

$$\frac{< Au, u >}{||u||^2} = \frac{< A_r u, u >}{||u||^2} = \sum_{s \in S} \left(1 - \frac{1}{2}\frac{||r(s)u - u||^2}{||u||^2}\right) = k - \frac{1}{2}\sum_{s \in S} \frac{||r(s)u - u||^2}{||u||^2}. \tag{27}$$

Dunque, per (25),

$$k - \mu = \frac{1}{2} \inf_{0 \neq u \in \mathcal{Z}^\perp} \sum_{s \in S} \frac{||r(s)u - u||^2}{||u||^2} \geq \frac{1}{2} \left(\inf_{0 \neq u \in \mathcal{Z}^\perp} \max_{s \in S} \frac{||r(s)u - u||^2}{||u||^2} \right). \tag{28}$$

Ora, per la definizione di costante di Kazhdan $\kappa(G, S)$ e l'osservazione (26), si ha

$$\max_{s \in S} \frac{||r(s)u - u||}{||u||} \geq \kappa(G, S)$$

e quindi, sostituendo nella (27),

$$k - \mu \geq \frac{1}{2}\kappa(G, S)^2 \tag{29}$$

che delinea una stima inferiore per l'intervallo spettrale principale di Γ.

Se H è finitamente generato, le rappresentazioni regolari delle immagini finite di H sono rappresentazioni di H e, come visto sopra, sono unitarie. Quanto abbiamo osservato per il caso finito è quindi, in nuce, la prova del seguente fondamentale risultato.

Teorema 12. *Sia H un gruppo finitamente generato, $\mathcal{N}$ una famiglia di sottogruppi normali di indice finito di H e, per ogni $N \in \mathcal{N}$, sia $\pi_N : H \to H/N$ la proiezione. Se H soddisfa la proprietà (T), allora per ogni sistema finito S di generatori di H, con $S = S^{-1}$, la famiglia dei grafi di Cayley $\Gamma[H/N, \pi_N(S)]$ (al variare di $N \in \mathcal{N}$) è una famiglia di expanders.*

Provare che un gruppo finitamente generato H soddisfa la proprietà (T) non è cosa banale (come c'è da aspettarsi, né i gruppi liberi né i gruppi abeliani finitamente generati soddisfano (T)), ma molto è stato fatto (vedi Lubotzki [3]). La teoria si è sviluppata nell'ambito dei gruppi algebrici; un metodo è quello di individuare H come un *reticolo* di un gruppo di Lie G: un risultato di Kazhdan assicura che H ha la proprietà (T) se e soltanto se ciò vale per G.
Grazie al lavoro di diversi studiosi si conoscono quali tra i gruppi di Lie definiti su campi locali soddisfano (T): in genere, una condizione sufficiente è che il rango di Lie sia almeno 2. Quindi, ad esempio, per ogni $n \geq 3$, $G = SL(n, \mathbb{R})$ soddisfa (T) e conseguentemente (in quanto reticolo di G) $SL(n, \mathbb{Z})$ soddisfa (T). Ciò significa, per il Teorema 12, che fissato un *qualsiasi* sistema finito di generatori S di $SL(n, \mathbb{Z})$ (con $S = S^{-1}$ e $1 \notin S$), la famiglia di grafi di Cayley $\Gamma[SL(n, \mathbb{Z}/m\mathbb{Z}), S_m]$ (dove $m \geq 2$ e S_m è la riduzione di S modulo m) è una famiglia di expanders. Ad esempio, possiamo prendere come S l'insieme delle matrici elementari (quelle con 1 sulla diagonale ed un ± 1 in una sola altra posizione); osservando che $|S| = 2n(n-1)$, per ogni $m \geq 2$, la proiezione modulo m è iniettiva su S, si conclude che la famiglia dei grafi $\Gamma_m = \Gamma[SL(n, \mathbb{Z}/m\mathbb{Z}), S_m]$ è una famiglia di grafi expanders $2n(n-1)$–regolari.

Il gruppo $SL(2, \mathbb{Z})$ (così come il gruppo di Lie $SL(2, \mathbb{R})$) non soddisfa la proprietà (T); tuttavia, per esso vale un risultato simile al Teorema 12.
So osserva, infatti, che la proprietà (T) non è necessaria affinché le immagini finite di un gruppo finitamente generato e residualmente finito (o una certa famiglia di esse) costituiscano una famiglia di expanders. Per affrontare questo aspetto, Lubotzy ha introdotto la proprietà (τ). Non ne diamo una precisa definizione: sia H un gruppo finitamente generato e sia $\mathcal{N}$ una famiglia di sottogruppi di indice finito di H, si dice che H soddisfa (τ) rispetto ad $\mathcal{N}$ se la condizione che definisce (T) è soddisfatta limitatamente alla considerazione delle rappresentazioni unitarie di H il cui nucleo contiene un sottogruppo in $\mathcal{N}$ (se questo vale quando $\mathcal{N}$ è la famiglia

di tutti i sottogruppi (normali) di indice finito di H, si dice che H soddisfa (τ)). Si dimostra (vedi Lubotzy [3], 4.3.2) che, se $\mathcal{N}$ è costituita da sottogruppi normali, allora H soddisfa (τ) rispetto a $\mathcal{N}$ se e solo se per ogni sistema finito $S = S^{-1}$ di generatori di H la famiglia di grafi di Cayley $\Gamma[H/N, SN/N]$ $(N \in \mathcal{N})$ è una famiglia di expanders.
Nel nostro contesto, il caso più importante è quello di $H = SL(2, \mathbb{Z})$, dove la famiglia $\mathcal{N}$ è costituita dai "congruence subgroups"

$$\Gamma(m) = Ker\,(SL(2, \mathbb{Z}) \to SL(2, \mathbb{Z}/m\mathbb{Z})) \tag{30}$$

per ogni $m \geq 2$. Che $SL(2, \mathbb{Z})$ soddisfi (τ) rispetto a $\mathcal{N}$ è una conseguenza di un profondo rislutato di Selberg (vedi [3] §4.4). È quindi possibile dedurre il seguente risultato.

Teorema 13. (Lubotzy) *Per ogni primo p si considerino gli elementi di $SL(2, p)$*

$$\tau = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

e sia $S_p = \{\sigma, \tau, \tau^{-1}\}$ (modulo matrici scalari). Allora la famiglia di grafi di Cayley $\Gamma_p = \Gamma[PSL(2, p), S_p]$ (con p che varia sull'insieme di tutti i numeri primi) è una famiglia di expanders.

Da questo deriva (mediante riduzione a grafi di Schreier) la famiglia di expanders dell'esempio 2 a pagina 5 (vedi esercizio 18).

Come la (T) di Kazhdan, anche la proprietà (τ) di Lubotzy (che è una proprietà più debole) ha diverse applicazioni, e solleva numerosi interessanti quesiti, per i quali rimandiamo al libro [14]. Citiamo soltanto il seguente risultato, dovuto a Lubotzky e Weiss [12] (vedi teorema 18): se un gruppo H ha la proprietà (τ) allora esiste $c > 0$ tale che $|K/K'| \leq c^n$ per ogni sottogruppo K di indice n. Da ciò segue, ad esempio, che $SL(2, \mathbb{Z})$, che soddisfa (τ) rispetto alla famiglia dei congruence subgroups, non soddisfa (τ) in generale (e conseguentemente non soddisfa (T)); infatti $SL(2, \mathbb{Z})$ ammette un sottogruppo libero di indice finito.

2.3 Grafi di Ramanujan.

Ricordiamo, dal primo capitolo, che un grafo finito connesso e k–regolare Γ si dice un *grafo di Ramanujan* se ogni per autovalore $\mu \neq \pm k$ di $A(\Gamma)$ si ha $|\mu| \leq 2\sqrt{k-1}$. Dal punto di vista dell'ampiezza dell'intervallo spettrale, i grafi di Ramanujan sono asintoticamente i migliori.

Fissato $k \geq 3$, famiglie infinite di grafi di Ramanujan k–regolari, sono state costruite da Lubotzky, Phillips e Sarnak [11] e da Margulis [15] nel caso $k = q + 1$, con q un numero primo, e sucessivamente da Morgenstern [18] nel caso in cui q è una potenza di un primo..

Teorema 14. *Per ogni primo p ed ogni intero $m \geq 1$, esistono infiniti grafi di Ramanujan $(p^m + 1)$–regolari.*

Anche in questo contesto, una delle maniere di vedere i grafi che (fissato il grado) costituiscono la famiglia, è come grafi di Cayley di quozienti modulo "congruence subgroups' di un certo gruppo algebrico; in questo caso, la proprietà (τ) (rispetto ai congruence subgroups) deve essere soddisfatta, ma non basta da sola a fornire la stima spettrale voluta. Per ottenerla, occorre fare appello a diversi e anche profondi risultati di teoria dei numeri, ed in particolare alla cosiddetta Congettura di Ramanujan (che è un teorema dovuto a Eichler e Deligne).

La descrizione dei grafi costruiti da Lubotzky et al. può essere sviluppata in modo abbastanza semplice (tutt'altro discorso è stabilirne le proprietà). Vediamo il caso in cui $k = p + 1$ con p un numero primo congruo a 1 modulo 4. Per un teorema di Jacobi, esistono $8(p + 1)$ quadruple distinte $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$, tali che

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p. \tag{31}$$

Tra queste quadruple (con le condizioni su p) ce ne sono esattamente $p+1$ con $a_0 > 0$ e a_1, a_2, a_3 pari. Denotiamo con $\mathcal{S}_p$, l'insieme di tali quadruple.
Sia quindi q un primo, anch'esso congruo a 1 modulo 4, e tale che p non è un quadrato modulo q. Fissiamo ℓ un intero tale che $\ell^2 \equiv -1 \pmod{q}$.
Sia quindi $S_{p,q}$ l'insieme degli elementi del gruppo $PGL(2, q)$

$$\begin{pmatrix} a_0 + \ell a_1 & a_2 + \ell a_3 \\ -a_2 + \ell a_3 & a_0 - \ell a_1 \end{pmatrix} \tag{32}$$

(modulo matrici scalari) al variare di (a_0, a_1, a_2, a_3) in $\mathcal{S}_p$. Si verifica che (se q è abbastanza grande) $S_{p,q}$ contiene $p+1$ elementi ed è chiuso per inversione; si definisce quindi il grafo di Cayley

$$X_{p,q} = \Gamma[PGL(2, q), S_{p,q}]. \tag{33}$$

I grafi $X_{p,q}$ sono grafi di Ramanujan (e, al crescere di q, ne costituiscono una famiglia infinita).

Una descrizione parallela dei grafi $X_{p,q}$, che è più adatta per stabilire alcune delle loro proprietà, consiste nel vederli come quozienti di alberi regolari infiniti. Seguendo [2] (e limitandoci ancora al caso $p \equiv 1 \pmod{4}$), sia

$$\mathbb{H}(\mathbb{Z}) = \{a_0 + a_1 i + a_2 j + a_3 k \mid a_0, a_1, a_2, a_3 \in \mathbb{Z}\}$$

l'algebra dei quaternioni interi, e sia S_p l'insieme degli elementi di $\mathbb{H}(\mathbb{Z})$ le cui coordinate soddisfano l'uguaglianza (31) e le condizioni descritte subito sotto; quindi $|S_p| = p + 1$. Si denota con Λ il monoide moltiplicativo generato da $S_p \cup \{p, -p\}$ in $\mathbb{H}(\mathbb{Z})$, osservando che per ogni elemento $u = b_0 + b_1 i + b_2 j + b_3 k \in \Lambda$, la sua *norma* $N(u) = b_0^2 + b_1^2 + b_2^2 + b_3^2$ è una potenza di p. Su Λ si considera la relazione $u \sim v$ se e solo se esistono $a, b \in \mathbb{N}$ tali che $\pm p^a u = p^b v$; si prova che $\sim$ è una congruenza sul monoide Λ. Di più, si prova che l'insieme quoziente $H = \Lambda/\sim$ è un gruppo, e che denotando con ρ la proiezione $\Lambda \to H$, si ha che ρ è iniettiva su S_p (cioè $|\rho(S_p)|p+1$). Si considera quindi il grafo di Cayley (su un gruppo infinito)

$$Y = \Gamma[H, \rho(S_p)]. \tag{34}$$

Il punto fondamentale è che Y è un albero infinito $(p + 1)$–regolare[4].
Sia q un primo dispari, e sia $\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{Z}/q\mathbb{Z})$ la riduzione modulo q. Allora $\tau_q(\Lambda)$ è contenuto nel gruppo $\mathbb{H}(\mathbb{Z}/q\mathbb{Z})^*$ degli elementi invertibili di $\mathbb{H}(\mathbb{Z}/q\mathbb{Z})$; si verifica inoltre che τ_q induce un omomorfismo $\Phi_q : H \to \mathbb{H}(\mathbb{Z}/q/Z)/Z$, dove $Z = (\mathbb{Z}/q\mathbb{Z})^*$ è il centro di $\mathbb{H}(\mathbb{Z}/q\mathbb{Z})$, e che (per q abbastanza grande) $|\Phi_q(\rho(S_p)| = p + 1$. Se $q \equiv 1 \pmod 4$ (che è quanto assumiamo per semplicità) il grafo di Cayley[5]

$$\Gamma[\Phi_q(H), \Phi_q(\rho(S_p)] \tag{35}$$

è isomorfo al grafo $X_{p,q}$ in (33). L'isomorfismo proviene dal fatto, noto, che l'algebra dei quaternioni $\mathbb{H}(Z/qZ)$ è isomorfa all'alegbra delle matrici $M_2(\mathbb{Z}/qZ)$: se $q \equiv 1 \pmod 4$, tale isomorfismo ψ è definito associando al quaternione $a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}(\mathbb{Z}/q\mathbb{Z})$ la matrice in (32), dove $\ell^2 = -1$ in $\mathbb{Z}/q\mathbb{Z}$.

La congettura che per ogni $k \geq 3$ esistono infiniti grafi k–regolari di Ramanujan (quindi con un numero arbitrariamente grande di vertici) è, per quanto ne so, ancora aperta. Ciò non toglie che non sia difficile trovare, per qualsiasi $k \geq 3$, singoli grafi di Ramanujan k-regolari non completi: si veda ad esempio l'esercizio 20.
Come abbiamo accennato nel primo capitolo, un risultato di Friedman asserisce che al crescere del numero di vertici, un grafo regolare si avvicina, probabilisticamente, ad essere di Ramanujan.

2.4 Famiglie di Cayley expanders.

Per quali famiglie di gruppi è possibile definire sistemi di generatori di cardinalità limitata, in modo che i corrispondenti grafi di Cayley formano una famiglia di ex-

[4]Ci sono diverse altre descrizioni concettuali di questo grafo (vedi [11] e Serre, *Trees*, cap. II).

[5]Il grafo in (35) è il grafo quoziente (cioè il grafo delle orbite) dell'albero Y modulo l'azione di $\ker \Phi_q$.

panders? Per descrivere alcuni dei notevoli risultati ottenuti su questa interessante questione cominciamo col fissarne in modo appropriato i termini.

Definizione. Una famiglia (infinita) di gruppi finiti $\mathcal{G}$ è detta una famiglia di *Cayley expanders* se esistono $k \in \mathbb{N}$ e $0 < \epsilon \in \mathbb{R}$ tali che ogni $G \in \mathcal{G}$ ammette un sistema di generatori S, con $|S| = k$ e $h(\Gamma[G, S]) \geq \epsilon$.

Dai risultati citati nella sezione precedente segue che se $\mathcal{G}$ è costituita da quozienti finiti H/K_i $(i \in I)$ di un gruppo finitamente generato H, e H soddisfa (τ) relativamente alla famiglia $\{K_i \mid i \in I\}$, allora $\mathcal{G}$ è una famiglia di Cayley expanders.
In tal modo si prova che, fissato $n \geq 3$, la famiglia $SL(n, p)$ (al variare di p tra i numeri primi), è una famiglia di Cayley–expanders; un risultato analogo vale per gli altri tipi di gruppi finiti di Lie,di rango maggiore o uguale a 2.
Più recentemente, Kassabov e Nikolov (2205) hanno dimostrato che, per $d \geq 3$, $m \geq 1$, il gruppo (discreto) $SL(d, \mathbb{Z}[x_1, \ldots, x_m])$ soddisfa la proprietà (τ) (un risultato interessante per diverse ragioni). Utilizzando ciò, Kassabov ha quindi provato che la famiglia di tutti i gruppi $SL(d, q)$ (al variare di $d \geq 3$ e q potenza di un numero primo) è una famiglia di Cayley–expanders. Combinando a sua volta questo con un risultato di Nikolov che afferma che ogni gruppo finito di Lie è un prodotto di un numero finito e uniformemente limitato di quozienti di gruppi $SL(d, q)$, si prova che quella costituita da tutti i gruppi finiti di tipo Lie e rango sufficientemente grande è una famiglia di Cayley–expanders.
Nel frattempo, Lubotzky dimostrò che la famiglia $SL(2, q)$ (q potenza di un primo) è una famiglia di Cayley–expanders (un fatto che non discende semplicemente - come il Teorema 13 - dalla proprietà (τ) per $SL(2, \mathbb{Z})$ relativamente ai congruence subgroups, ma la cui dimostrazione richiede anche tecniche utilizzate per costruire grafi di Ramanujan di grado $q + 1$). Un risultato essenziale che, grosso modo, consente di superare la condizione sui ranghi posta sopra.

A questo punto, il caso dei gruppi alterni rimaneva cruciale. Fu presto risolto da Kassabov [9].

Teorema 15. *La famiglia costituita da tutti i gruppi alterni $Alt(n)$ (con $n \in \mathbb{N}$) è una famiglia di Cayley–expanders (il grado è ≤ 200); un risultato analogo vale per la famiglia i tutti i gruppi simmetrici $Sym(n)$.*

Tale linea d'indagine è quindi culminata con il recente lavoro di Kassabov, Lubotzky e Nikolov [10], in cui, raccogliendo quanto provato in precedenza, si dimostra il seguente notevole risultato.

Teorema 16. *La famiglia di tutti i gruppi finiti semplici diversi dai gruppi di Suzuki, è una famiglia di Cayley–expanders (e i parametri k ed ϵ possono essere esplicitamente stimati).*

Il caso dei gruppi finiti semplici di Suzuki è ancora aperto: è chiaro, a questo punto, che il provare che quella dei gruppi di Suzuki è una famiglia di Cayley–exopanders completerebbe la dimostrazione che la famiglia di tutti i gruppi semplici finiti è una famiglia di Cayley–expanders. Ciò che distingue, da questo punto di vista, la famiglia dei gruppi di Suzuki dalle altre famiglie infinite di gruppi semplici è che i gruppi di Suzuki non sono generati da copie di gruppi tipo $SL(2,q)$ (circostanza che è essenziale nella dimostrazione del teorema 16).

Finora, abbiamo considerato famiglie costituite da gruppi semplici o quasisemplici. Ciò è dovuto forse primariamente ai metodi sviluppati per affrontare la questione, che per molta parte la ricollegano alla teoria dei gruppi algebrici. Per gruppi non semplci risultano preferibili tecniche più direttamente legate alla teoria dei grafi, e forse più elementari, che vedremo nel prossimo capitolo.
Per il momento, osserviamo che la Proposizione 10 mostra che nessuna famiglia infinita di gruppi abeliani è Cayley–expander. Questo risultato è esteso in Lubotzky e Weiss [12] a gruppi risolubili con lunghezza derivata limitata.

Teorema 17. *Una famiglia infinita costituita da gruppi risolubili di lunghezza derivata limitata non è una famiglia di Cayley expanders.*

Sempre in [12] si prova un risultato interessante e più generale, che è spesso utile per escludere la possibilità di Cayley expanders.

Teorema 18. *Sia $\Gamma_i = \Gamma[G_i, S_i]$ $(i \in \mathbb{N})$ una famiglia di grafi di Cayley, con $|S_i| \leq k$. Supponiamo che $(\Gamma_i)_{i\in\mathbb{N}}$ sia una famiglia di expanders; allora esiste una costante $c > 0$ tale che, per ogni $i \in \mathbb{N}$ ed ogni sottogruppo M di indice finito in G_i*

$$|M/M'| \leq c^{|G_i:M|}.$$

Famiglie di Cayley expanders costituite da gruppi risolubili esistono (naturalmente con lunghezze derivate illimitate). Il seguente esempio è tratto da [12]:

Esempio. Sia $d \geq 3$, p un primo fissato, e per ogni $n \geq 1$ consideriamo il congruence subgroup

$$N_m = \Gamma(p^m) = Ker\,(SL(3,\mathbb{Z}) \to SL(2,\mathbb{Z}/p^m\mathbb{Z})).$$

N_1 ha indice finito nel gruppo finitamente generato $SL(d,\mathbb{Z})$; quindi N_1 è finitamente generato, inoltre si verifica facilmente che eredita da $SL(d,\mathbb{Z})$ la proprietà (T). Quindi, fissato un sistema finito di generatori S di N_1, dal teorema 12 segue che la famiglia dei grafi di Cayley

$$\Gamma[N_1/N_m, SN_m/N_m]$$

è una famiglia di expanders. Ora, ogni $P_m = N_1/N_m$ è un p–gruppo (si può calcolare che il suo ordine è $p^{(m-1)(d^2-1)}$), e quindi $\{P_m\}_{m\geq 2}$ è una famiglia di Cayley expanders costituita da p–gruppi.

Un problema collegato a quanto riportatto in questo captiolo, e che si presenta in modo più o meno naturale (vedi [12]), è chiedersi se il fatto che una famiglia (infinita) di grafi di Cayley sia una famiglia di expanders è una proprietà dei gruppi coinvolti oppure dipende anche dalla scelta dei generatori. Detto meglio: sia $(G_i)_{i\in\mathbb{N}}$ una famiglia di gruppi finiti, $k \geq 3$ e, per ogni $i \in \mathbb{N}$, siano S_i, T_i sistemi di generatori del gruppo G_i, con $|S_i| \leq k$, $|T_i| \leq k$. Assumiamo che la famiglia di grafi di Cayley $\Gamma[G_i, S_i]$ sia una famiglia di expanders; è vero che anche $\Gamma[G_i, T_i]$ è una famiglia di expanders?
La questione non è balzana come sembra, dato che, come abbiamo visto ad esempio per quozienti di gruppi con la proprietà (T), per molte famiglie di gruppi si osserva una certa indipendenza fra le proprietà di espansione dei grafi di Cayley e i sistemi di generatori (si veda [12] per una discussione approfondita di questo tema). Tuttavia, in generale, la risposta è negativa. Infatti, dal Teorema 15 di Kassabov segue che esiste $k \geq 3$ tale che per ogni ogni $n \geq 3$, il gruppo simmetrico $Sym(n)$ ammette un sistema di generatori Σ_n di ordine k, in modo che i grafi di Cayley $\Gamma[Sym(n), \Sigma_n]$ costituiscono una famiglia di expanders; d'altra parte, per ogni $n \geq 3$, la coppia di permutazioni $\tau_n = (1\,2)$ e $\rho_n = (1\,2\,\cdots n)$ genera $Sym(n)$, e si verifica che l'intervallo spettrale dei grafi cubici di Cayley $\Gamma[Sym(n), \{\tau_n, \rho_n, \rho_n^{-1}\}]$ tende a zero quando $n \mapsto \infty$.
Altre esempi di classi di gruppi che dimostrano come la proprietà di espansione dei grafi di Cayley dipenda anche dal sistema di generatori, sono costruiti mediante prodotti intrecciati e sono legati ad un diverso approccio, che vedremo nel prossimo capitolo.

* * *

Esercizio 11. Si provi che matrici di adiacenza di grafi isomorfi hanno lo stesso spettro.

Esercizio 12. Sia $\Gamma = (V, E)$ un grafo semplice, il *grafo complementare* è definito come $\overline{\Gamma} = (V, V^{[2]} \setminus E)$ (dove $V^{[2]}$ è l'insieme dei sottoinsiemi di ordine 2 di V); quindi $\overline{\Gamma}$ è definito sullo stesso insieme di vertici di Γ, e due vertici sono adiacenti in $\overline{\Gamma}$ se e solo se non sono adiacenti in Γ. Quindi, se $A = A(\Gamma)$ è la matrice di adiacenza di Γ, e J la matrice i cui elementi sono tutti 1, la matrice di adiacenza di $\overline{\Gamma}$ è $J - I - A$.
(1) Sia Γ un grafo k–regolare; supponendo noto lo spettro di $A(\Gamma)$ si descriva lo spettro di $A(\overline{\Gamma})$.
(2) Si provi che il grafo complementare di un grafo di Cayley è un grafo di Cayley.

Esercizio 13. Sia $n \geq 2$, e sia $D_{2n} = \langle x, y \mid y^n = x^2 = 1,\ y^x = y^{-1} \rangle$ il gruppo diedrale di ordine $2n$. Posto $S = \{y, y^{-1}, x\}$, si descriva il grafo di Cayley $\Gamma[D_{2n}, S]$

Esercizio 14. Sia G un gruppo ed S un sottoinsieme di generatori di G che soddisfa (C1) e (C2). Si provi che il grafo d Cayley $\Gamma(G, S)$ è bipartito se e soltanto se esiste $N \trianglelefteq G$ con $|G : N| = 2$ e $N \cap S = \emptyset$.

Esercizio 15. Per ogni $n \geq 2$ determinare gli autovalori della matrice di adiacenza del n-cubo Q_n utilizzando la Proposizione 9 (e l'esempio 3 a pagina 19). Estendere l'analisi al caso di un p-gruppo abeliano elementare $G = \langle x_1 \rangle \times \cdots \times \langle x_n \rangle$ (dove $|x_i| = p$ per ogni $i = 1, \ldots, n$), con $S = \{x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}\}$. Qual'è la costante di Kazhdan $\kappa(G, S)$ per G ed S come nella seconda parte dell'esercizio?

Esercizio 16. (Y. Luz) Sia p un primo fissato. Per ogni $n \geq 3$, in $SL(n, p)$ si considerino la matrice τ_n, in cui 1 compare su tuuta la diagonale principale e nella posizione (1,2), e 0 altrove, e la matrice σ_n i cui elementi sono 1 sulla diagonale immediatamente sopra quella principale, $(-1)^{n-1}$ nella posizione $(n, 1)$ e 0 altrove. Si provi che la famiglia $Y_n = \Gamma[SL(n, p), \{\tau_n, \tau_n^{-1}, \sigma_n, \sigma_n^{-1}\}]$ non è una famiglia di expanders. [sugg.: $SL(n, p)$ opera transitivamente su $\mathbb{F}_p^n \setminus \{0\}$; se $\{Y_n\}_{n \geq 3}$ fosse una famiglia di expanders, allora (Proposizione 11) anche i grafi di Schreier $\overline{Y}_n$ associati a tali azioni costituirebbero una famiglia di expanders; se $e_1, \ldots, e_n$ è la base canonica di $\mathbb{F}_p^n$, quando $n \geq 6$ si calcoli la frontiera del sottoinsieme $X = \{e_3, \ldots, e_{[n/2]}\}$ dei vertici del grafo di Schreier $\overline{Y}_n$, $\ldots$]

Esercizio 17. Sia $n \geq 1$, e $d = 2^n$. Sia $V = \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ visto come gruppo additivo, e $S = \{(x, 0) \mid x \text{ dispari}\} \cup \{(0, y) \mid y \text{ dispari}\}$. Sia Γ il grafo di Cayley $\Gamma[V, S]$. SI osservi che $|S| = d$; si applichino le osservazioni della prima parte della dimostrazione della Proposizione 10 per provare che il massimo autovalore non banale di Γ è $\mu_1 = d/2$.

Esercizio 18. Sia p un numero primo. Allora $SL(2, p)$ opera sulla retta proiettiva $P(1, p) = \{0, 1, \ldots, p-1, \infty\}$ mediante funzioni di Möbius; alla matrice $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ è associata la funzione $\sigma(X)$

$$z \mapsto \frac{az + b}{cz + d}$$

con $z \in P(1, p)$. Il nucleo di questa azione è l'insieme delle matrici scalari; per cui il gruppo $H = PSL(2, p)$ opera fedelmente su $P(1, p)$. Provare che i grafi cubici dell'esempio 2 a pagina 5 sono grafi di Schreier, relativamente all'azione σ. A partire dal Teorema 13, ed utilizzando le osservazioni riguardo ai grafi di Schreier (Proposizione 11), concludere che, al variare di p, costituiscono una famiglia di expanders.

Esercizio 19. Sia $d \geq 3$ e sia T_d l'abero infinito d-regolare. Si provi che $h(T_d) = d-2$.

Esercizio 20. *Grafi di Paley.* Sia q una potenza di un primo dispari, con $q \equiv 1 \pmod 4$. Il grafo di Paley P_q è il grafo i cui vertici sono gli elementi del campo $GF(q)$ di ordine q, e per ogni $a, b \in GF(q)$, a è adiacente a b se $a - b \neq 0$ è un quadrato in $GF(q)$.

(1) Si provi che P_q è un grafo di Cayley. Se α è un generatore del campo $GF(q)$, si osservi che la moltiplicazione per α induce un automorfismo di P_q; si concluda che il gruppo degli automorfismi di P_q è transitivo sull'insieme degli archi.

(2) Sia A la matrice di adiacenza del grafo P_q, e $\overline{A}$ quella del suo grafo complementare (vedi esercizio 12). Usando, se serve, il punto (1), si provi che esistono $a, b \in \mathbb{N}$ tali che

$$A^2 = \frac{q-1}{2} I_q + aA + b\overline{A}.$$

(3) Si provi che P_q è isomorfo al suo grafo complementare. Dedurre da ciò e dal punto 2 (oltre che dall'esercizio 11) che lo spettro di A è costituito da tre autovalori, $k,\ \mu,\ -1-\mu$, con molteplicità, rispettivamente, 1, $(q-1)/2$, $(q-1)/2$.

(4) Provare che gli autovalori non banali di A sono

$$\mu_{1,2} = \frac{-1 \pm \sqrt{q}}{2}.$$

[Sfruttare, ad esempio, il fatto che la somma dei quadrati degli autovalori di A è uguale alla traccia di A^2]. Per finire, osservare che P_q è un grafo di Ramanujan.

3 Il prodotto Zig–Zag

In questo capitolo descriveremo un'altra tecnica, del tutto diversa da quelle viste nel capitolo precedente, per costruire famiglie di expanders. Essa si basa su un particolare prodotto di grafi (il prodotto "zig–zag", introdotto da Reingold, Vadhan e Wigderson [21]), che dà luogo a costruzioni di tipo ricorsivo di grafi regolari di grado fisso.
Se Γ è un grafo d-regolare, poniamo $\delta = \delta(\Gamma) = \mu/d$, dove μ è il massimo valore assoluto degli autovalori della matrice di adiacenza di Γ diversi da $\mu_0 = k$ (in altri termini è, in valore assoluto, il massimo tra gli autovalori di $A(\Gamma)$ come operatore sulle funzioni in $\mathcal{C}(\Gamma)$ a somma zero); per $n, d \in \mathbb{N}$ e $\varepsilon \geq 0$ diremo che un grafo Γ è un (n, d, ε)–grafo se Γ è d-regolare con n-vertici e $\delta(\Gamma) \leq \varepsilon$); scriviamo solo (n, d)-grafo se non ci interessa specificare - o non sappiamo valutare - l'ultimo parametro (si osservi che, con la definizione data, se Γ non è connesso oppure è bipartito, $\mu = k$ e $\delta = 1$)[6].
Osserviamo che se, per $i \geq 1$, H_i è un (n_i, d_i, δ_i)-grafo, con $d_i = d_j$ per ogni $i, j \geq 1$, $\lim_{i\to\infty} n_i = \infty$, ed esiste $\delta < 1$ tale che $\delta_i < \delta$ per ogni $i \geq 1$, allora $(H_i)_{i\geq 1}$ è una famiglia di expanders.

3.1 Il prodotto zig-zag.

In teoria dei grafi si applicano diversi metodi per combinare tra loro due grafi: tuttavia, per la maggior parte di questi prodotti (diretto, lessicografico, tensoriale etc.), il risultato del prodotto di due grafi completi, che è anch'esso un grafo completo, ha di solito grado molto maggiore dei gradi dei singoli fattori. Questi metodi, quindi, non sembrano adatti a produrre famiglie di expanders; ma poiché ce ne serviremo più avanti, citiamo due casi. Nel primo (potenza standard di un grafo) si parte da un grafo Γ con matrice d'adiacenza A: per ogni $m \geq 1$, il grafo Γ^m è il grafo la cui matrice d'adiacenza è A^m. Per $m \geq 2$, Γ^m non è un grafo semplice: infatti, si vede che per ogni coppia di vertici x, y, $(A^m)_{xy}$ è uguale al numero di passegiate nel grafo base Γ da x a y di lunghezza m. Se Γ è un (n, d, δ)–grafo, allora Γ^2 è un (n, d^2, δ^2)-grafo (si veda l'esercizio 21).
Il *prodotto tensoriale* dei grafi Γ e Δ è il grafo $\Gamma \otimes \Delta$, la cui matrice di adiacenza è il prodotto di Kronecker $A(\Gamma) \otimes A(\Delta)$ delle matrici d'adiacenza dei due fattori. Diversamente dalla potenza standard, il prodotto tensoriale di grafi semplici è anch'esso un grafo semplice. Se Γ è un (n_1, d_1, δ_1)–grafo e Δ è un (n_2, d_2, δ_2)–grafo, allora $\Gamma \otimes \Delta$ è un $(n_1 n_2, d_1 d_2, \varepsilon)$-grafo, con $\varepsilon \leq \max\{\delta_1, \delta_2\}$ (questo dipende dal fatto che gli autovalori del prodotto tensoriale $A(\Gamma) \otimes A(\Delta)$ sono i prodotti degli autovalori di $A(\Gamma)$ per quelli di $A(\Delta)$).

[6] Per quanto concerne questa sezione, si può anche tacitamente assumere che, per ragioni di brevità, lasciamo da parte il caso bipartito.

Veniamo ora a prodotti tra grafi regolari che hanno la proprietà cruciale che il grado del prodotto dipende solo da quello del secondo fattore.
Cominciamo con il più semplice *riprodotto* (in inglese: *replacement product*).

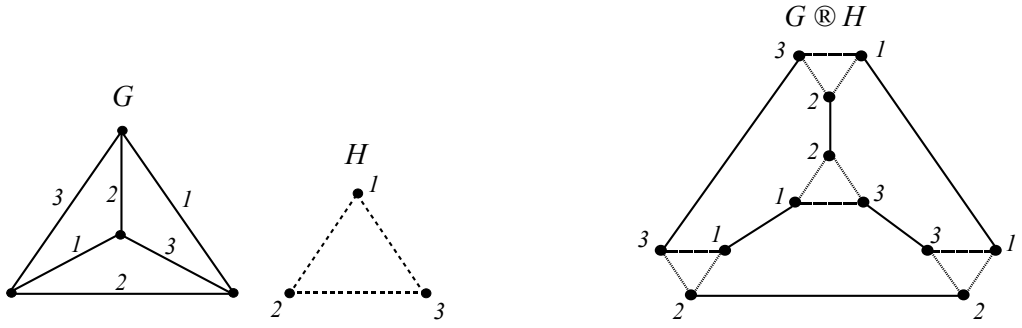
Siano $G = (V(G), E(G))$ un (n, d, δ_1)-grafo, $H = (V(H), E(H))$ un (d, k, δ_2)-grafo. Costruiamo un grafo $G \circledR H$ (che chiamiamo "G riprodotto H") nel modo seguente:

- si numerano i vertici di H come $V_2 = \{1, 2, \ldots, d\}$; per ogni vertice v di G, si assegna una numerazione $v(1), v(2), \ldots, v(d)$ degli archi incidenti a v in G;

- l'insieme dei vertici di $G \circledR H$ è l'insieme delle coppie ordine $V(G) \times V(H)$

- gli archi di $G \circledR H$ sono di due tipi: $(v, i), (w, j) \in V(G) \times V(H)$ sono adiacenti se
  - $v = w$ e i, j sono adiacenti in H (arco di tipo H), oppure
  - $v \neq w$, v è adiacente a w in G, e $v(i) = w(j) = \{v, w\} \in E(G)$ (arco di tipo G).

Detto in modo informale, un riprodotto di G per H si ottiene immaginando, per ogni vertice v di G, di "staccare" da esso gli archi incidenti, moltiplicando cioè il vertice v di G in una d-upla di vertici (uno per ogni arco di G incidente a v), $(v, 1), \ldots, (v, d)$; quindi, per ogni ex-vertice v di G, il grafo H viene replicato sui vertici $(v, 1), \ldots, (v, d)$.
La figura seguente mostra un riprodotto del grafo completo $G = K_4$ per il triangolo $H = K_3$



(in questo esempio le numerazioni, per ciascun vertice di G, degli archi ad esso incidenti, possono essere assegnate in modo omogeneo, ovvero $v(i) = w(i)$ se v, w sono adiacenti in G: ciò si deve al fatto che l'insieme degli archi di G è 3-colorabile - cioè esiste un'assegnazione di un colore $\{1, 2, 3\}$ ad ogni arco di G in modo che archi consecutivi abbiano sempre colori diversi[7]).
Il riprodotto non è univocamente determinato, ma dipende dalle assegnazioni $v(i)$. Alcuni aspetti di fondo restano però invarianti: se G è un (n, d, δ_1)-grafo e H un

[7]Un classico Teorema di Vizing (vedi [4]) afferma che gli archi di un grafo d-regolare sono sempre colorabili con d o $d + 1$ colori. Il caso in cui gli archi di G sono d-colorabili semplifica la definizione di riprodotto, ma non è essenziale.)

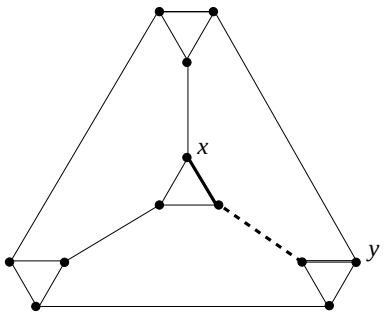
(d, k, δ_2)–grafo, allora GⓇH è un $(nd, k+1)$–grafo (osserviamo che il grado del prodotto dipende solo da quello del secondo fattore). Di fatto, il riprodotto è una nozione da tempo impiegata in teoria dei grafi, in genere per ricondurre al caso dei grafi cubici diverse questioni riguardanti il grafi regolari (se G è un grafo d-regolare, il riprodotto GⓇC_d, dove C_d è il ciclo di lunghezza d, è un grafo cubico).

È anche possibile dare un limite superiore al parametro δ del riprodotto GⓇH, in funzione di δ_1 e δ_2 dei fattori (vedi [21]); ma, da questo punto di vista, risulta molto più efficiente un altro tipo di prodotto, strettamente legato al riprodotto, inventato di recente da Reingold, Vadhan e Wigderson [21], e da loro chiamato prodotto zig–zag.

Non ne daremo una precisa definizione formale ma, piuttosto, una descrizione. Siano, come prima, G un (n, d, δ_1)-grafo e H un (d, k, δ_2)-grafo. Si comincia con il fare un riprodotto di G per H; quindi si definisce un *Prodotto zig–zag* GⓏH nel modo seguente:

– l'insieme di vertici è, ancora, $V(G) \times V(H)$;

– gli archi si ottengono considerando cammini nel riprodotto costituiti, nell'ordine, da un arco di tipo H, uno di tipo G, ed un terzo ancora di tipo H. (La figura seguente mostra un arco $\{x, y\}$ nel prodotto K_4ⓏK_3); quindi $\{(u, i), (w, j)\}$ (con $v, w \in V(G)$ e $i, j \in V(H) = \{1, 2, \ldots, d\}$) è un arco di GⓏH se e solo $v \sim w$ in G ed esistono $r, s \in V(H)$ tali che $i \sim r$, $s \sim j$ in H, e $v(r) = w(s)$.



Si osservi che, una volta scelto, a partire da un vertice x, un arco di tipo H in GⓇH, c'è poi un solo arco di tipo G con cui è possibile proseguire. Si vede quindi facilmente che se G è un (n, d, δ_1)-grafo e H un (d, k, δ_2)–grafo, il prodotto zig–zag GⓏH è un (nd, k^2)–grafo. È essenziale, nelle applicazioni, la circostanza che il grado del prodotto zig-zag dipenda solo dal grado del secondo fattore, mentre altre proprietà sono legate a quelle di entrambi i fattori: in particolare le proprietà di espansione. Infatti, che si possa provare che $\delta(G$Ⓩ$H)$ non cresce troppo in funzione di δ_1 e δ_2, e che quindi il prodotto zig-zag possa essere impiegato per ampliare grafi con buona

costante di espansione in grafi con simili attitudini, è l'aspetto più importante del prodotto zig-zag.

Il risultato fondamentale è quindi il seguente teorema di Reingold, Vadhan e Wigderson.

Teorema 19. ([21]) *Siano G un (n, d, δ_1)-grafo e H un (d, k, δ_2)–grafo. Allora il prodotto zig–zag $G \textcircled{z} H$ è un $(nd, k^2, f(\delta_1, \delta_2))$–grafo, con*

(1) $f(\delta_1, \delta_2) < 1$ *se* $\delta_1, \delta_2 < 1$,

(2) $f(\delta_1, \delta_2) \leq \delta_1 + \delta_2$.

Il punto (1) assicura che se $\{G_i\}_{i\in I}$, $\{H_i\}_{i\in I}$ sono famiglie di expanders (e la prima *non necessariamente di grado fisso*), allora anche $\{G_i \textcircled{z} H_i\}_{i\in I}$ è una famiglia di expanders. Il punto (2) consente invece la costruzione ricorsiva di famiglie di expanders: prima di dare un cenno della dimostrazione, vediamo subito come ciò si attua.
Fissato $d \geq 2$, si comincia da un $(d^4, d, 1/4)$-grafo H. Questo si può trovare mediante una ricerca esaustiva (dato che l'ordine d^4 è costante), ed in genere non è troppo difficile ottenerlo anche per via diretta, dato che il grado è relativamente grande rispetto all'ordine del grafo (alcuni esempi si trovano nell'esercizio 23). Si pone poi, induttivamente, $G_1 = H^2$ e, per ogni $i \geq 2$,

$$G_i = G_{i-1}^2 \textcircled{z} H.$$

Proposizione 20. *Per ogni $n \geq 1$, G_n è un $(d^{4n}, d^2, 1/2)$-grafo. Quindi $(G_n)_{n\geq 1}$ è una famiglia di expanders.*

Dimostrazione. L'affermazione è vera per la scelta di H quando $n = 1$. Supponiamo sia vera per $n \geq 1$; allora, per quanto osservato in precedenza G_n^2 è un $(d^{4n}, d^4, (1/2)^2)$-grafo, e quindi per il Teorema 19, $G_{n+1} = G_n^2 \textcircled{z} H$ è un $(d^{4(n+1)}, d^2, \delta)$-grafo, con $\delta \leq f(\frac{1}{4}, \frac{1}{4}) \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$. ∎

Come osservato all'inizio di questa sezione, la notazione che abbiamo adottato oscura i grafi bipartiti, intorno ai quali il teorema 19 finisce col dire nulla: ma in [21], è sviluppata anche una teoria significativa di prodotti zig–zag per grafi bipartiti. Osserviamo anche che, recentemente, Alon, Schwartz e Shapira [6] hanno proposto una simile costruzione ricorsiva di famiglie di expanders utilizzando, invece del prodotto zig-zag, una variante più semplice del riprodotto.

Seguendo [1], accenniamo ora alla dimostrazione di una forma più debole del Teorema 19 (che però è sufficiente per la costruzione ricorsiva di famiglie di expanders, vedi esercizio 24): con le notazioni del Teorema, posto $\delta = \delta(G \textcircled{z} H)$, proviamo che $\delta \leq \delta_1 + \delta_2 + \delta_2^2$.

Per lo studio degli autovalori, è conveniente lavorare con matrici d'adiacenza *normalizzate*: dove se A è la matrice d'adiacenza di un grafo d-regolare, la matrice normalizzata è A/d.

Sia X l'insieme dei vertici di G, $[d] = \{1, 2, \ldots, d\}$ quello di H, e $V = X \times [d]$ l'insieme dei vertici del prodotto zig-zag $\Gamma = G \textcircled{z} H$, così come del riprodotto $G \textcircled{R} H$ che sta a monte di Γ. Siano $A = \frac{1}{d}A(G)$, $B = \frac{1}{k}A(H)$ le matrici d'adiacenza normalizzate di G e H rispettivamente.

In $G \textcircled{R} H$, consideriamo i sottografi (V, E_H), i cui archi sono tutti e soli quelli del tipo H (vedi definizione di $G \textcircled{R} H$) e (V, E_G), i cui archi sono tutti e soli quelli del tipo G, e siano rispettivamente Q e P le matrici d'adiacenza normalizzate. Ora, (V, E_H) è un grafo costituito da n copie di H a due a due sconnesse; quindi Q è una matrice ad n blocchi diagonali uguali a B; cioè $Q = B \otimes I_n$. Per quanto riguarda P, si osserva che (V, E_G) è costituito da $nd/2$ archi del tipo $((v, i), (w, j))$, con $v(i) = w(j)$ (e dunque $v \sim w$ in G), a due a due sconnessi; quindi P è una matrice di permutazione di ordine due su V definita da

$$P_{(v,i),(w,j)} = \begin{cases} 1 & \text{se } v(i) = w(j) \\ 0 & \text{altrimenti} \end{cases} \tag{36}$$

Per definizione di prodotto zig-zag e per l'esercizio 21, la matrice d'adiacenza normalizzata di $\Gamma = G \textcircled{z} H$ è $F = QPQ$.

Sia, come al solito, $\mathcal{Z}^\perp$ lo spazio delle funzioni $f \in \mathcal{C}(\Gamma)$ a somma zero. Ricordando l'identità (10), quello che ci proponiamo di provare è

$$\frac{| < Ff, f > |}{||f||^2} \leq \delta_1 + \delta_2 + \delta_2^2. \tag{37}$$

per ogni $f \in \mathcal{Z}^\perp$. Sia quindi $f \in \mathcal{Z}^\perp$; definiamo $f^{||}$ nel modo seguente,

$$f^{||}(x, i) = \frac{1}{d} \sum_{j \in [d]} f(x, j)$$

($f^{||}$ descrive la media su ogni copia di H nel grafo (V, E_H)). Poniamo quindi $f^\perp = f - f^{||}$; allora, la somma dei valori di $f^\perp$ sui vertici di una copia di H è 0. Si osservano quindi i seguenti fatti

(1) $Qf^{||} = f^{||}$.

(2) $||Qf^\perp|| \leq \delta_2 ||f^\perp||$.

Ora, espandendo il prodotto, si ha

$$| < Ff, f > | \leq | < Ff^{||}, f^{||} > | + 2 | < Ff^{||}, f^\perp > | + | < Ff^\perp, f^\perp > |. \tag{38}$$

Definiamo $g \in \mathcal{C}(G)$, ponendo per ogni $x \in X$, $g(x) = \sqrt{d} f^{||}(x, i)$ (questo non dipende dalla scelta di $i \in [d]$). Si verifica allora che $||f^{||}||^2 = ||g||^2$, e che, per come è definita

la matrice P, $<Pf^{||}, f^{||}>=<Ag, g>$, dove A è la matrice di adiacenza normalizzata di G. Poiché, chiaramente, $\sum_{x\in X} g(x) = 0$, si ha

$$| <Pf^{||}, f^{||}> | = | <Ag, g> | \leq \delta_1 ||g||^2 = \delta_1 ||f^{||}||^2.$$

Quindi, tenendo conto del fatto che Q è hermitiana, e del punto (1),

$$| <Ff^{||}, f^{||}> | = | <PQf^{||}, Qf^{||}> | = | <Pf^{||}, f^{||}> | \leq \delta_1 ||f^{||}||^2 \tag{39}$$

Poiché P è una matrice di permutazione (quindi conserva le distanze), e il punto (2),

$$| <Ff^{||}, f^{\perp}> | = | <Pf^{||}, Qf^{\perp}> | \leq ||Pf^{||}|| \cdot ||Qf^{\perp}|| \leq \delta_2 ||f^{||}|| \cdot ||f^{\perp}||, \tag{40}$$

e similmente

$$| <Ff^{\perp}, f^{\perp}> | \leq ||Qf^{\perp}||^2 \leq \delta_2^2 ||f^{\perp}||^2. \tag{41}$$

Mettendo tutto nella (38),

$$| <Ff, f> | \leq \delta_1 ||f^{||}||^2 + 2\delta_2 ||f^{||}|| \cdot ||f^{\perp}|| + \delta_2^2 ||f^{\perp}||^2. \tag{42}$$

Siccome, come si vede facilmente, $f^{||}$ e $f^{\perp}$ sono ortogonali, si ha $||f||^2 = ||f^{||}||^2 + ||f^{\perp}||^2$; quindi $2||f^{||}|| \cdot ||f^{\perp}|| = ||f||^2 - (||f^{||}|| - ||f^{\perp}||)^2 \leq ||f||^2$. Da (42) segue

$$| <Ff, f> | \leq (\delta_1 + \delta_2 + \delta_2^2) ||f||^2$$

per ogni $f \in \mathcal{Z}^{\perp}$, che è quello che si voleva provare.

3.2 Prodotti e grafi di Cayley.

Il legame tra i prodotti di grafi descritti nel paragrafo precedente e i grafi di Cayley è ancora terreno da esplorare a fondo, anche se, come vedremo, diverse interessanti connessioni e applicazioni sono state notate.
Diciamo innanzi tutto che né il riprodotto, né il prodotto zig-zag, di grafi di Cayley sono in generale grafi di Cayley (vedi esercizio 26).

Un'azione di un gruppo H su un insieme X è un omomorfismo $H \to Sym(X)$. Se anche X è un gruppo, allora con il termine azione di H su X si intende in genere un omomorfismo di H nel gruppo degli automorfismi di B. In entrambi i casi, denotiamo con x^h il trasformato di $x \in X$ tramite la permutazione (o l'automorfismo) associata a $h \in H$. Se $H \to Aut(X)$ è un'azione del gruppo H sul gruppo X, denotiamo con

$$X \rtimes H$$

il *prodotto semidiretto* associato (per fissare le notazioni: si tratta dell'insieme $X \times H$ dotato dell'operazione $(x,h)(x_1,h_1) = (xx_1^{h^{-1}}, hh_1)$).

Per rendere più funzionale la descrizione del legame tra prodotti semidiretti e prodotto zig–zag fra grafi di Cayley, è conveniente assumere una versione generalizzata di questi ultimi. Sia data un'azione del gruppo H sul gruppo X, e sia Y un sottoinsieme non vuoto (e non contenente 1_X) di X; con $\Gamma[X, Y^H]$ si intende il (multi)grafo (che chiameremo ancora *grafo di Cayley*) i cui vertici sono gli elementi di X e archi le terne del tipo $(x,y,g) \in X \times Y \times H$, dove gli estremi di (x,y,g) sono x e xy^g. Si osservi che per $H = 1$ si ottiene il grafo di Cayley (semplice) $\Gamma[X, Y \cup Y^{-1}]$; in generale, $\Gamma[X, Y^H]$ è un multigrafo regolare di grado $|Y \cup Y^{-1}||H|$.
Possiamo ora enunciare il risultato di base (Alon, Lubotzky, Wigderson [7]).

Teorema 21. *Siano B, H gruppi finiti, e sia data un'azione (come gruppo di automorfismi) di H su B. Sia $G = B \rtimes H$ il prodotto semidiretto definito da tale azione. Supponiamo che esista un elemento $x \in B$ tale che la sua orbita tramite H, $x^H = \{x^h \mid h \in H\}$ sia un sistema simmetrico di generatori per B. Infine, sia T un sistema di generatori per H. Allora*

1) *$R = \{(x,1)\} \cup \{(1,h) \mid h \in T\}$ è un sistema di generatori di G e*

$$\Gamma[G,R] = \Gamma[B, x^H] \circledR \Gamma[H,T];$$

2) *$S = \{(x^{t^{-1}}, ts) \mid t,s \in T\}$ è un sistema di generatori di G e*

$$\Gamma[G,S] = \Gamma[B, x^H] \circledcirc \Gamma[H,T];$$

Si osservi che mentre $\Gamma[B, x^H]$ è un grafo di Cayley standard (cioè semplice) se e soltanto se l'orbita x^H è regolare (ovvero $|x^H| = |H|$), il risultato del prodotto è comunque un grafo di Cayley standard.

Dimostrazione. Gli archi del grafo $\Gamma[B, x^H]$ sono le terne (v,x,g), con $v \in B$, x come nelle ipotesi e $g \in H$. Sia $H = \{g_1, \ldots, g_d\}$, e per ogni $v \in B$ listiamo gli archi incidenti a v nel grafo $\Gamma[B, x^H]$ mediante $v(i) = (v, x, g_i)$, dove (v, x, g_i) è un arco i cui estremi sono v e vx^{g_i}. Nel riprodotto $\Gamma[B, x^H] \circledR \Gamma[H,T]$ (che è un grafo semplice) definito da tali assegnazioni, il vertice (v, g_i) è adiacente ai vertici

$(v, g_i t) = (v, g_i)(1, t)$ per ogni $t \in T$;

$(vx^{g_i^{-1}}, g_i) = (v, g_i)(x, 1)$.

Da ciò segue immediatamente che $\Gamma[B, x^H] \circledR \Gamma[H,T]$ è il grafo di Cayley $\Gamma[B \rtimes H, R]$, con $R = \{(x,1)\} \cup \{(1,h) \mid h \in T\}$, il che prova il punto 1).

Osservando poi che per ogni $s,t \in T$, $(1,t)(x,1)(1,s) = (x^{t^{-1}},t)(1,t) = (x^{t^{-1}},ts)$, si ottiene il punto 2). ∎

Esempio 1. La condizione sull'orbita generatrice è certamente soddisfatta se B è un modulo irriducibile per H. Ad esempio, per ogni primo $p \geq 3$, sia $H_p = SL(2,p)$, e T_p il sistema di 3 generatori descritto nel Teorema 13, che rende la famiglia degli H_p una famiglia di Cayley expanders. Sia B_p il gruppo additivo dello spazio vettoriale $\mathbb{F}_p^2$, su cui H_p opera nel modo naturale. H_p opera transitivamente su $B_p^* = B_p \setminus \{0\}$; ovvero B_p^* è un'unica orbita per H_p, e $\Gamma[B_p, B_p^*]$ è quindi il grafo completo K_{p^2}. Dunque, detto $G_p = B_p \rtimes H_p$, fissato $0 \neq x \in B_p$ e posto $S_p = \{(x^t, t^{-1}s) \mid t,s \in T_p\}$, per il Teorema 21 si ha

$$\Gamma[G_p, S_p] = K_{p^2} \circledcirc \Gamma[H_p, T_p].$$

Questo è un $(p^2|SL(2,p)|, 9, \delta_p)$–grafo, e per il Teorema 19,

$$\delta_p \leq \delta(K_{p^2}) + \delta(\Gamma[H_p, T_p]) = 1/p^2 + \delta(\Gamma[H_p, T_p]).$$

Poiché i grafi $\Gamma[H_p, T_p]$ sono una famiglia di expanders, si conclude che anche i grafi $\Gamma[G_p, S_p]$ sono una famiglia di expanders[8].

Questo esempio non è tuttavia adatto ad essere implementato per una costruzione ricorsiva di gruppi e grafi di Cayley, analoga a quella della Proposizione 20. Individuare una costruzione del genere non è semplice; di fatto, ne è stato sinora fornito un solo importante esempio, in Rozenman, Shalev e Wigderson [20]. Per descriverlo, ricordiamo la nozione di *prodotto intrecciato permutazionale*. Siano A, H gruppi, con $H \leq Sym(m)$: il prodotto intrecciato permutazionale $A \wr H$ è il prodotto semidiretto $A^m \rtimes H$, dove per ogni $(a_1, \ldots, a_m) \in A^m$ e $g \in H$, $(a_1, \ldots, a_m)^g = (a_{g^{-1}(1)}, \ldots, a_{g^{-1}(m)})$. Se H è un fissato gruppo di permutazioni, definiamo le potenze intrecciate di A nel modo seguente:

$$\wr^1 H = H \quad \text{e, per} \quad n \geq 1, \ \wr^{n+1} H = (\wr^n H) \wr H.$$

Per ogni $m \geq 1$ denotiamo con A_m il gruppo alterno $Alt(m)$ (per ogni $n \geq 1$, $\wr^n A_m$ opera in modo naturale su m^n (più precisamente sull'albero m-regolare con radice di altezza n).

Teorema 22. (Rozenman, Shalev, Wigderson [20]) *Per d sufficientemente grande*[9] *la famiglia dei gruppi $G_n = \wr^n A_d$ (per $n \geq 1$) è una famiglia di Cayley expanders.*

La dimostrazione utilizza ricorsivamente i teoremi 19 e 21, e parte da un risultato intermedio nel Teorema 15 di Kassabov, che afferma che per d sufficientemente grande,

[8] Potremo così affermare che il gruppo delle affinità $\mathbb{Z}^2 \rtimes SL(2,\mathbb{Z})$ soddisfa la proprietà (τ) rispetto ai nuclei delle riduzioni modulo un primo.

[9] In [20] si stima $d \geq 10^{10^9}$.

esiste un sistema S_1 di generatori di A_d, con un numero relativamente piccolo di elementi, tale che $\delta(\Gamma[A_d, S_1]) \leq 1/1000$. A parte questo, la dimostrazione utilizza metodi elementari (non ricorre, ad esempio, alla teoria delle rappresentazioni) ma contiene diversi aspetti interessanti anche dal punto di vista della teoria dei gruppi. Posto $(G_1, S_1) = (A_d, S_1)$ con d e S_1 come nel risultato di Kassabov, gli autori provano che per ogni $n \geq 1$ esiste un sistema simmetrico di generatori S_n di $G_n = \wr^n A_d$ tale che $|S_n| \leq |S_1|^4$ e $\delta(\Gamma[G_n, S_n]) \leq 1/1000$. Supponendo di aver già provato quanto serve per $G_n = \wr^n A_d$, il problema nel transito a $G_{n+1} = (G_n)^d \rtimes A_d$ è (come imposto dal teorema 21) quello di trovare, se c'è, una A_d-orbita generatrice Y in G_n^d, che sia in qualche modo associata al sistema di generatori $S = S_n$ di G_n, e tale che il grafo di Cayley $\Gamma[G_n^d, Y]$ abbia un parametro δ sufficientemente piccolo per poter applicare poi il teorema 19. Una candidatura naturale per Y è quella di un'orbita di cardinalità massima: ora, A_d opera su G_n^d permutando le componenti, e tale orbita è costituita dall'insieme $S^{(d)}$ dei *vettori bilanciati* in S, ovvero gli elementi di G_n^d in cui ogni elemento di S compare esattamente $[d/|S|]$ volte (qui, d è molto più grande di $|S|$) e le restanti componenti sono 1. Il fatto che $d > |S|$ assicura che $S^{(d)}$ è un'orbita per il gruppo alterno A_d (e si osserva che la condizione $d > |S|$ è sufficinte a garantire che $S^{(d)}$ è una singola orbita, indipendentemente da come è fatto S). Ma questo $S^{(d)}$ ancora non basta per produrre un grafo di Cayley su G_n^d con la limitazione per δ che occorre: si procede allora ampliando preventivamente l'insieme S in G_n; cosa che si realizza ricorrendo al seguente risultato

Lemma 23. (Nikolov [19]) *Ogni elemento di G_n è un commutatore*[10].

Dunque ogni $y \in S$ si può scrivere $y = [a_y, b_y]$, con $a_y, b_y \in G_n$; si considera in G_n l'insieme

$$S^* = S \cup \{a_y,\ b_y,\ a_y^{-1},\ b_y^{-1},\ a_y^{-1}b_y^{-1},\ b_y a_y \ \mid \ y \in S\}.$$

S^* è simmetrico e, chiaramente, $|S^*| \leq 7|S|$. Ora, per un opportuno intero c (sul cui valore, per semplicità, sorvoliamo); si considera il multinsieme $X = cS \cup S^*$ (questo significa che in X gli elementi di S vengono considerati con molteplicità c). Il sistema di generatori per G_n^d cercato è l'insieme dei vettori bilanciati in X, ovvero $Y = X^{(d)}$. Per quanto osservato prima (Y è ancora molto più piccolo di d), Y è un'unica A_d–orbita, e il fatto cruciale, provato in [20], è che $\delta(\Gamma[G_n^d, Y]) \leq 1/50$. Si applicano ora il punto 2) del teorema 21 e il teorema 19 per ricavare un sistema simmetrico di generatori P di $G_{n+1} = G_n^d \rtimes A_d$, con $|P| = |S_1|^2$ e tale che

$$\delta(\Gamma[G_{n+1}, P]) \leq \delta(\Gamma[G_n^d, Y]) + \delta(\Gamma[A_d, S_1]) \leq 1/50 + 1/1000.$$

Infine, si pone S_{n+1} il multinsieme dei prodotti di due elementi di P (o meglio, l'insieme delle parole di lunghezza 2 in P); si ha $|S_{n+1}| \leq |S_1|^4$, e $\Gamma[G_{n+1}, S_{n+1}] =$

[10] Che ogni elemento di A_d, per $d \geq 5$, sia un commutatore è un vecchio risultato di Ore.

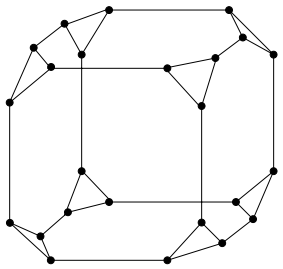
$(\Gamma[G_{n+1}, P])^2$; da cui, per quanto osservato all'inizio di questo capitolo, segue

$$\delta(\Gamma[G_{n+1}, S_{n+1}]) \leq 1/50 + (1/1000)^2 \leq 1/1000.$$

Questo completa la descrizione del passo induttivo e dell'idea generale della dimostrazione del Teorema 22.

Osservazione. Per ogni $n \geq 1$, c'è un naturale omomorfismo $\phi_n : G_{n+1} \to G_n$ (G_{n+1} opera sull'albero d-regolare di altezza $n+1$, la proiezione su G_n si ottiene considerando l'azione sino al livello n). In [20] gli autori provano che, per ogni n, $\phi_n(S_{n+1}) = S_n$, e da ciò deducono che esiste un insieme S_∞ di elementi del gruppo degli automorfismi dell'albero con radice d-regolare infinito T, che coincide con S_n quando se ne consideri l'azione sino all'altezza n. Posto G_∞ il gruppo degli automorfismi di T generato da S_∞, esiste quindi, per ogni $n \geq 1$, la proiezione $\Phi_n : G_\infty \to G_n$ (non è altro che la restrizione all'altezza n in T). Dunque, la famiglia G_n è costituita da quozienti finiti di G_∞, e G_∞ soddisfa la proprietà (τ) rispetto alla famiglia $(\ker \Phi_n)_{n\geq 1}$ (sezione 2.2).

Esempio 2. Un altro semplice caso in cui (con le notazioni del Teorema 21) si verifica l'ipotesi che B sia generato da una singola H–orbita *regolare*, è quello di un prodotto intrecciato *standard* (ovvero, H è considerato nella rappresentazione regolare) $C_m wr H$, dove C_m è il gruppo ciclico di ordine m. In questo caso $G = B \rtimes H$, dove B è la cosiddetta base del prodotto intrecciato; quindi $B = Dir_{h\in H} X_h$, dove $X_h \simeq C_m$ per ogni $h \in H$, ed H opera su B permutando regolarmente le componenti. Posto x un generatore di X_1, chiaramente x^H è un sistema di generatori di B (e $|x^H| = |H|$). Nel caso speciale $m = 2$, se $d = |H|$, il grafo di Cayley $\Gamma[B, x^H]$ è un d-cubo Q_d (vedi esempio 3 a pagina 15). Sia T un sistema di generatori di H, e $R = \{(x, 1)\} \cup \{(1, h) \mid h \in T\}$; allora, per il Teorema 21, $\Gamma[G, R] = Q_d \circledR \Gamma[H, T]$.
Per esempio, la figura seguente mostra il grafo di Cayley di $C_2 wr H$, dove $H = \langle h \rangle = C_3$, rispetto al sistema di generatori $R = \{(x, 1), (1, h), (1, h^{-1})\}$.



Qui il problema è che per il cubo Q_d l'intervallo spettrale principale normalizzato è $2/d$ (esercizio 7), che tende a zero (il cubo è anche bipartito ma non è questo il punto); e, poichè l'azione di H su B è regolare, qualsiasi scelta di una singola H-orbita in B porta alla medesima conclusione. Ed è forse sorprendente che *due* orbite

siano sufficienti a far sì che i grafi di Cayley dei gruppi $B = C_2^d$ costituiscano una famiglia di expanders (nel senso più ampio di avere un limite inferiore al parametro di espansione, ma non necessariamente un limite al grado: il bello del prodotto zig-zag è proprio che questa seconda condizione può essere messa da parte), e che quindi il prodotto finisca per fornire una famiglia di expanders di grado limitato. Questo è l'argomento del prossimo paragrafo.

3.3 Orbite per H–moduli.

Consideriamo sempre prodotti semidiretti $G = B \rtimes H$. Come abbiamo osservato, la condizione nelle ipotesi del Teorema 21, che il sistema di generatori per il gruppo B sia costituito da un'unica H-orbita, è un fattore che limita l'applicabilità del risultato. In [7], Alon, Lubotzky e Wigderson osservano che se T è un sitema di generatori di H, ed $a_1, \ldots, a_c$ sono elementi di B l'unione delle cui H-orbite genera B, allora, posto $S = \{(1,t)(a_i,1)(1,s) \mid i = 1, \ldots, c,\ s,t \in T\}$, il grafo di Cayley $\Gamma[G,S]$ risulta una *unione* (vedi [7] per la definizione precisa) di c prodotti zig-zag $\Gamma[B, a_i^H] ⓩ \Gamma[H,T]$. In tal caso $\Gamma[G,S]$ è regolare di grado cd^2 (dove $d = |T|$), ma, come si verifica facilmente, continua a soddisfare le proprietà del prodotto zig-zag semplice. Si ottiene quindi un criterio per famiglie di expanders che, per comodità, enunciamo direttamente nel caso dei gruppi.

Proposizione 24. *Sia $G_i = B_i \rtimes H_i$ $(i \in I)$ una famiglia di prodotti semidiretti di gruppi finiti, tali che*

(1) La famiglia di gruppi $\{H_i\}_{i\in I}$ è una famiglia di Cayley expanders di grado d;

(2) esistono $1 \leq c \in \mathbb{N}$ e $0 < \beta < 1$, tali che, per ogni $i \in I$, esistono c elementi $b_{i,1}, \ldots b_{i,c}$ di B_i, l'unione delle cui H_i-orbite genera B_i, e $\delta(\Gamma[B_i, b_{i,1}^G \cup \cdots \cup a_{ic}^G]) < \beta$.

Allora $\{G_i\}_{i\in I}$ è una famiglia di Cayely expanders (di grado cd^2).

Quindi, il problema è: data un'azione di H su B, è possibile trovare un numero limitato (nel contesto di una famiglia infinita di coppi B, H) di H–orbite in B, che diano luogo a grafi di Cayley che costituiscano una famiglia di expanders?
Nella sezione precedente abbiamo visto un importante esempio in cui una sola orbita è sufficiente: in quel caso era fondamentale che ogni elemento del gruppo $B = \wr^n A_d$ fosse un commutatore. In questa sezione consideriamo il caso opposto in cui B è abeliano; e più precisamente, il gruppo additivo di un H-modulo su un campo finito. È sorprendente che, almeno in questo contesto, la risposta alla domanda formulata sopra sia in molti casi affermativa. Quanto segue è tratto da due interessanti lavori: Alon–Lubotzky–Wigderson [7] e Meshulam, Wigderson [17]; fissiamo anche la notazione: H un gruppo finito, $\mathbb{F}_p$ il campo di ordine p (p un primo), e B il gruppo additivo di un $\mathbb{F}_p[H]$-modulo.

Se B è irriducibile sono sempre sufficienti *due orbite*.

Teorema 25. ([7]) *Sia p un primo. Esiste $0 < \beta_p < 1$ tale che per ogni rappresentazione irriducibile $H \to GL(V)$ (dove V è un $\mathbb{F}_p$–spazio vettoriale), se $B = (V, +)$, esistono due elementi a_1, a_2 di B tali che*

$$\delta(\Gamma[B, a_1^H \cup a_2^H]) \leq \beta_p. \tag{43}$$

In [7] si prova inoltre che la probabilità che una coppia di elementi presi a caso soddisfi (43) tende a 1 al tendere di $\dim V$ a infinito.
La dimostrazione è un argomento probabilistico, e non procura un algoritmo per trovare le due orbite. Descrizioni *esplicite* dei due elementi a_1, a_2 sono state fornite (Meshulam e Wigderson [17]) solo in alcuni casi particolari, e sarebbe interessante averne di più.

Esempio 3. ([7]) Per ogni primo p, sia S_p il sistema di 3 generatori che rende la famiglia $\Gamma[SL(2,p), S_p]$ una famiglia di expanders (Teorema 13). $SL(2,p)$ opera come un gruppo di permutazioni 2-transitivo sulla retta proiettiva $P(1,p)$ (esercizio 18). Fissato un primo q, sia $B_p = \mathbb{F}_q^{p+1}$ il modulo di permutazione per $SL(2,p)$ associato a tale azione. B_p è la somma del modulo banale per un modulo irriducibile: un caso in cui il Teorema 25 si può comunque applicare. Quindi, la famiglia dei gruppi $B_p \rtimes SL(2,p)$ è una famiglia di Cayley expanders (in [17] sono esplicitamente descritte le due orbite di $SL(2,p)$ su B_p che consentono di applicare il Teorema). Questo fornisce un altro esempio di dipendenza dai generatori della proprietà di espansione dei grafi di Cayley di una famiglia di gruppi (vedi esercizio 28).

Nel caso in cui B non sia irriducibile, vale un risultato simile al teorema 25, ma il numero di orbite necessario dipende dalla distribuzione dei cosiddetti ranghi degli elementi di B. Per ogni $a \in B$, definiamo il *rango* di a come la dimensione del sottospazio di B generato dall'orbita a^H; e per ogni $r \in \mathbb{N}$, denotiamo con $k_r(B,H)$ il numero di elementi di B di rango r.

Teorema 26. (Alon, Lubotzky, Wigderson [7]) *Fissato il campo $\mathbb{F}_p$, sia B un $\mathbb{F}_p[H]$–modulo, e sia $d \in \mathbb{N}$ tale che $k_r(B,H) \leq d^r$, per ogni $r \in \mathbb{N}$. Allora esiste un intero $c = O(d)$ ed esistono c elementi $a_1, \ldots a_c \in B$ per cui*

$$\delta(\Gamma[B, a_1^H \cup a_2^H \cup \cdots \cup a_c^H]) \leq 1/2. \tag{44}$$

La questione si sposta quindi alla stima dei valori $k_r = k_r(B,H)$. Se B è irriducibile di grado n, allora, chiaramente, $k_0 = 1$ e $k_n = |B| - 1$, per cui si può prendere $d = p$, indipendentemente da B ed H. Per affrontare il problema con più generalità, è naturale concentrarsi sul caso in cui B sia il modulo regolare per H sul campo

$\mathbb{F}_p$, ovvero B è il gruppo additivo dell'anello gruppale $\mathbb{F}_p[H]$ (e l'azione di H è per moltiplicazione a sinistra); quindi $G = \mathbb{F}_p[H] \rtimes H \simeq C_p wr H$.
Questa è la situazione studiata da Meshulam e Wigderson in [17] e, in parte, ripresa e generalizzata in [14]. Se $p \not| |H|$ (come, di norma, supporremo), allora, per il Teorema di Wedderburn

$$\mathbb{F}_p[H] = \bigoplus_{i=1}^{t} M_{d_i}(\mathbb{F}_{p^{e_i}}) \tag{45}$$

(dove $M_r(K)$ è l'anello delle matrici di ordine r su K), e $|H| = \sum_{i=1}^{t} e_i d_i^2$. Per ogni $a \in \mathbb{F}_p[H]$, $rango(a)$ è uguale alla dimensione dell'ideale sinistro $\mathbb{F}_p[H]a$; quindi, se $a = (A_1, \ldots, A_t)$ (nella decomposizione (45)), allora

$$rango(a) = \sum_{i=1}^{t} e_i d_i rk(A_i).$$

Si dimostra poi (§2 in [17]) che per ogni $0 \leq r \leq d$, il numero di matrici in $M_d(\mathbb{F}_{p^e})$ di rango r è limitato superiormente da p^{2edr}. Ne segue abbastanza facilmente che, per ogni $0 \leq r \leq |H|$,

$$k_r = k_r(\mathbb{F}_p[H], H) \leq \sum_{(r_1, \ldots r_t)} \prod_{i=1}^{t} p^{2r_i e_i d_i} = |K_r| p^{2r} \tag{46}$$

dove $K_r = \{(r_1, \ldots, r_t) \in \mathbb{N}^t \ \mid \ 0 \leq r_i \leq d_i, \ \sum_{i=1}^{t} e_i d_i r_i = r\}$. Accettato questo, è facile concludere che $|K_r|$, e di conseguenza k_r, è limitato esponenzialmente in funzione del rango r se *il numero di rappresentazioni irriducibili di grado d di $\mathbb{F}_p[H]$ è limitato esponenzialmente in funzione di d.*
Per formulare per bene questo risultato, fissiamo la seguente notazione. Siano $\mathcal{H} = \{H_i\}_{i \in I}$ una famiglia di gruppi finiti, e p un numero primo. Per $d \in \mathbb{N}$ e $i \in I$, sia $\nu_d(H_i)$ il numero di rappresentazioni irriducibili di dimensione d di $\mathbb{F}_p[H_i]$. Diciamo che la famiglia $\mathcal{H}$ soddisfa la proprietà $\mathcal{K}_p$ se esiste una costante $K > 0$ tale che $\nu_d(H_i) \leq K^d$, per ogni $d \in \mathbb{N}$ e $i \in I$.

Proposizione 27. (Meshulam, Wigderson [17]) *Sia $t \geq 1$, e $\mathcal{H} = \{H_i\}_{i \in I}$ una famiglia di gruppi finiti t–generati. Se $\mathcal{H}$ soddisfa $\mathcal{K}_p$, con p un primo che non divide alcun $|H_i|$, allora c'è una costante $c = c(K, t))$ tale che per ogni $i \in I$, esistono $a_{i,1}, \ldots, a_{i,c}$ in $\mathbb{F}_p[H_i]$ tali che*

$$\delta(\Gamma[\mathbb{F}_p[H_i],\, H_i a_{i,1} \cup \cdots \cup H_i a_{i,c}]) \leq 1/2.$$

In congiunzione con la Proposizione 24 si deduce,

Teorema 28. *SIa $\mathcal{H}$ una famiglia di gruppi finiti, e sia p un primo con $p \not| |H|$, per ogni $H \in \mathcal{H}$. Supponiamo che $\mathcal{H}$ sia una famiglia di Cayley expanders e che soddisfi $\mathcal{K}_p$. Allora la famiglia dei prodotti semidiretti*

$$\mathbb{F}_p[H] \rtimes H \quad (H \in \mathcal{H})$$

è una famiglia di Cayley expanders.

In [14], Lubotzky e Zuk provano che, per ogni primo p ed ogni intero $t \geq 1$, *la famiglia di tutti i gruppi finiti t–generati il cui ordine non è diviso da p soddisfa $\mathcal{K}_p$*; e quindi tale condizione è superflua nelle ipotesi del Teorema 28 (e, anche, la costante c nella Proposizione 27, dipende solo dal primo p e da t). Questo fatto discende dalla classificazione dei gruppi semplici finiti.
Vediamo il caso particolare, che non richiede la classificazione dei gruppi semplici, in cui, per un primo $q \neq p$, $\mathcal{H}$ è la famiglia di tutti i q-gruppi finiti t-generati (ad esempio una delle famiglie di Cayley expanders dell'esempio a pagina 31). Sia $H \in \mathcal{H}$ e $d \geq 1$; allora il numero di rappresentazioni (non necessariamente irriducibili) di H su $\mathbb{F}_p$ di grado al più d coincide, a meno di coniugio, con il numero di omomorfismi $\pi : H \to GL(d, p)$; quindi (per il Teorema di Sylow) è minore o uguale al numero di omomorfismi $H \to Q$, dove Q è un fissato q–sottogruppo di Sylow di $GL(d, p)$. Ora, è un fatto piuttosto semplice che $|Q| \leq q^{\alpha d}$ per qualche costante α (che dipende solo da p e q); poiché H è t–generato il numero di omomorfismi $H \to Q$ è al più $p^{\alpha dt}$. Quindi $\nu_d(H) \leq p^{\alpha dt}$ (che non dipende da $H \in \mathcal{H}$).

Meshulam e Wigderson adottano in [17] un anaologo approccio e provano, con tecniche simili ma ovviamente meno immediate, che la proprietà $\mathcal{K}_p$ è soddisfatta dalla famiglia $\mathcal{M}$ dei gruppi *monomiali*[11], trovando in questo caso parametri espliciti, i cui valori consentono di procedere iterativamente. Dopo aver osservato che se H è un gruppo monomiale e $p \not| |H|$, anche $\mathbb{F}_p[H] \rtimes H$ è monomiale, replicando tale passaggio, si costruisce, a partire da un gruppo ciclico G_1, una sequenza di gruppi *risolubili* G_n e di loro sistemi simmetrici di generatori S_n, tali che i grafi di Cayley che si ottengono sono una famiglia di expanders regolari con grado che cresce "molto lentamente". Più precisamente,

Teorema 29. (Meshulam e Wigderson [17]) *Sia $\{p_i\}_{i \geq 1}$ una sequenza di numeri primi distinti, e per ogni $i \geq 1$, sia C_i il gruppo ciclico di ordine p_i. Sia $G_1 = C_1$ e, per $n \geq 2$, $G_i = \mathbb{F}_{p_n}[G_{n-1}] \rtimes G_{n-1} = C_n \, wr \, G_{n-1}$. Allora, per ogni $n \geq 1$, esiste un sistema di generatori S_n di G_n tale che*

$$\delta(\Gamma[G_n, S_n]) \leq \frac{1}{2}.$$

[11] Un gruppo finito H è monomiale se ogni $\mathbb{C}$–rappresentazione irriducibile di H è indotta da una rappresentazione lineare (cioè di grado 1) di un sottogruppo di H.

e, per n abbastanza grande, $|S_n| \leq \log^{(n/2)} |G_n|$.

(dove con $\log^{(t)}$ si intende la funzione logaritmo iterata t volte). In un senso che è chiarito in [17], questo risultato è anche migliore possibile (vedi pure l'esercizio 29). Per quanto riguarda costruzioni ricorsive di gruppi risolubili, si tratta del meglio sinora ottenuto.

3.4 Grafi di Schreier.

La stretta relazione tra riprodotti di grafi regolari e prodotti di gruppi si presenta in modo ancor più naturale quando, invece che ai più esclusivi grafi di Cayley, si guarda, in generale, ai grafi di Schreier.
Siano infatti G e H gruppi di permutazioni, rispettivamente, sull'insieme X e sull'insieme Y (supporremo che le rappresentazioni $\pi_G : G \to Sym(X)$ e $\pi_H : H \to Sym(Y)$ siano fedeli: quindi $G = \pi_G(G) \leq Sym(X)$ e $H = \pi_H(H) \leq Sym(Y)$); siano M ed S sistemi simmetrici di generatori di G e H, rispettivamente, ed infine siano $\Gamma = Sch[\pi_G, M]$ e $\Delta = Sch[\pi_H, S]$ i corrispondenti grafi di Schreier. Assumiamo che $|M| = |Y|$ (è la condizione per poter comporre un riprodotto $\Gamma ® \Delta$) e sia $\phi : Y \to M$ una fissata biezione. Si considerano ora le permutazioni σ_s (per ogni $s \in S$) e ρ sull'insieme prodotto $X \times Y$, definite da

$$\begin{cases} \sigma_s(x, y) = (x, y^s) \\ \rho(x, y) = (x^{\phi(y)}, y), \end{cases} \tag{47}$$

per ogni $(x, y) \in X \times Y$. Sia infine W il sottogruppo di $Sym(X \times Y)$ generato da tali permutazioni:

$$W = \langle \rho, \sigma_s \mid s \in S \rangle,$$

e $S^* = \{\sigma_s \mid s \in S\} \cup \{\rho\}$. La definizione è data in modo che si abbia

$$Sch[W, S^*] = Sch[\pi_G, M] ® Sch[\pi_H, S].$$

La struttura gruppale di W (che potremmo chiamare un *riprodotto* di G per H) non è del tutto ovvia; si vede facilmente che $W/\langle \rho^W \rangle \simeq H$, e che W è comunque un sottogruppo del prodotto intrecciato permutazionale $G \wr H$, ma in generale non coincide con quest'ultimo (anche nel caso in cui sia G che H siano considerati nelle loro rappresentazioni regolari - vedi esercizio 30). Sarebbe interessante poter dire qualcosa di più preciso su questo prodotto di gruppi ed eventualmente testare la sua utilità per la descrizione di expanders (che forse è dubbia: la rappresentazione di W su $X \times Y$ non è in generale regolare, anche se quelle di G ed H lo sono, quindi $Sch[W, S^*]$ non è in generale un grafo di Cayley).

* * *

Esercizio 21. Siano $\Gamma = (V, E)$ e $\Gamma' = (V, E')$ due grafi definiti sullo stesso insieme di vertici V, e siano A, A' le rispettive matrici di adiacenza. Definiamo il grafo $\Gamma\Gamma'$ sullo stesso insieme V di vertici e gli archi di sono le coppie (e, e') con $e \in E$, $e' \in E'$, e ed e' con un estremo in comune.

(a) Si provi che la matrice di adiacenza di $\Gamma\Gamma'$ è AA', e che se Γ è un (n, d)-grafo e Γ' è un (n, d')-grafo, allora $\Gamma\Gamma'$ è un (n, dd')-grafo,

(b) Si dimostri direttamente che se Γ è un grafo bipartito, allora Γ^2 è sconnesso.

Esercizio 22. Siano G e H rispettivamente un (n, d)-grafo e un (d, k)-grafo, entrambi connessi con almeno due vertici, e sia $R = G\circledR H$ un loro riprodotto. Si provi che se R è bipartito allora H è bipartito. Si faccia un esempio in cui, dati G ed H con H bipartito, esistono due diversi riprodotti di G per H, dei quali uno è bipartito e l'altro no.

Esercizio 23. ([21]) Sia $q = p^a$ potenza di un numero primo, $\mathbb{F}_q$ il campo con q elementi, e $V = \mathbb{F}_q \times \mathbb{F}_q$. Consideriamo il grafo H_q sull'insieme di vertici V e la relazione di adiacenza definita nel modo seguente: $(a, b) \in V$ è adiacente a tutti e soli i vertici (x, y) tali che $y = ax - b$. H_q è un (q^2, q)-grafo connesso.

(a) Si provi che, per ogni $a, a', b, b' \in \mathbb{F}_q$, il numero di vertici adiacenti sia ad (a, b) che a (a', b') è 1 se $a \neq a'$, e 0 se $a = a'$.

(b) Sia B la matrice d'adiacenza del grafo su V, definito dalla relazione d'adiacenza

$$(a, b) \sim (a', b') \;\Leftrightarrow\; a = a',\, b \neq b'.$$

Si provi che $B = K_q \otimes I_q$ dove I_q è la matrice identica e K_q è la matrice d'adiacenza del grafo completo su q vertici. In particolare gli autovalori di B coincidono con quelli di K_q (con molteplicità moltiplicata per q).

(c) Sia A la matrice d'adiacenza di H_q; usando i punti (a) e (b) provare che

$$A^2 = J + (q-1)I - B$$

dove I è la matrice identica di ordine q^2 e J la matrice di ordine q^2 con tutti gli elementi uguali ad 1.

(d) Sia $f \in \mathcal{C}(H_q)$, con $\sum_{v \in V} f(v) = 0$. Allora $Jf = 0$. Concludere che gli autovalori diversi da q^2 di A^2 sono tutti e soli del tipo $q - 1 - \alpha$ dove α è un autovalore di B. Ricordando la discussione sugli autovalori del grafo completo (pagina 7), dedurre che gli autovalori di A, sono, in valore assoluto, $q,\ \sqrt{q},\ 0$.
Concludere che H_q è un $(q^2, q, 1/\sqrt{q})$-grafo.

(e) Posto $d = q^2$, usando il Teorema 19 si provi che $H = ((H_q \otimes H_q)\circledZ H_q)\circledZ H_q$ è un $(d^4, d, 3/\sqrt{q})$-grafo (quindi, con un'opportuna scelta di q, può essere usato come base per la costruzione di una famiglia di expanders secondo la Proposizione 20).

Esercizio 24. Con le notazioni nelle ipotesi del Teorema 19, provare che la limitazione $\delta \leq \delta_1+\delta_2+\delta_2^2$ è sufficiente per la costruzione ricorsiva di famiglie di expanders (partire con H un $(q^4, q, 1/5)$-grafo).

Esercizio 25. Si provi che il grafo $G®H$ della figura a pagina 36 è un grafo di Cayley per il gruppo alterno A_4.

Esercizio 26. Siano $C_{10} = \langle a \rangle$, $C_3 = \langle b \rangle$ gruppi ciclici di ordine, rispettivamente, 10 e 3, e siano $\Gamma = \Gamma[C_{10}, \{a, a^{-1}, a^5\}]$, $\Delta = \Gamma[C_3, \{b, b^{-1}\}]$. Si provi che il riprodotto $\Gamma®\Delta$ non può essere un grafo di Cayley. [sugg.: se $\Gamma®\Delta = \Gamma[G, S]$, allora $|G| = 30$ e, dall'esame del grafo, si deduca che $S = \{x, y, y^{-1}\}$ con $|x| = 2$ e $|y| = 3$; d'altra parte un gruppo di ordine 30 contiene un solo sottogruppo di ordine 3 ...]

Esercizio 27. Sia B il gruppo additivo del campo $\mathbb{F}_q$ di ordine $q = p^n$ (con p primo e $n \geq 1$). Allora il gruppo moltiplicativo $H = \mathbb{F}_q^*$ opera naturalmente su B e transitivamente su $B \setminus \{0\}$. Sia α un elemento primitivo di $\mathbb{F}_q$ (cioè un generatore di H) e $T = \{\alpha, \alpha^{-1}\}$. Posto $S = \{(\alpha, 1), (\alpha^{-1}, 1), (\alpha, \alpha^{-2}), (\alpha^{-1}, a^2)\}$, si trovi una maggiorazione (in funzione di q) del valore del parametro δ del grafo $\Gamma[B \rtimes H, S]$.

Esercizio 28. Sia q un primo fissato, e per ogni $p \geq 3$ siano $G_p = \mathbb{F}_q^{p+1} \rtimes SL(2, p)$, come nell'esempio 3 e S_p come nel teorema 13. Sia e_1 il primo vettore della base canonica di $\mathbb{F}_q^{p+1}$ (che, si ricordi, è un modulo di permutazione). Si provi che la famiglia di grafi di Cayley $\Gamma[G_p, S_p \cup \{e_1, -e_1\}]$ non è una famiglia di expanders.

Esercizio 29. Sia $(H_i)_{i \geq 1}$ una famiglia di gruppi finiti, e $(p_i)_{i \geq 1}$ una sequenza infinita di numeri primi distinti. Provare che la famiglia di gruppi $C_{p_i} \, wr \, H_i = \mathbb{F}_{p_i}[H_i] \rtimes H_i$ non è mai una famiglia di Cayley expanders. [sugg.: usare il Teorema 18]

Esercizio 30. Sia H un gruppo finito, e B un $\mathbb{F}_p H$-modulo irriducibile, per un primo p. Si considerino sia B che H nella loro rappresentazione regolare (come gruppi di permutazioni di se stessi), sia S un sistema di generatori di H, e come sistema di generatori di B si consideri un'orbita b^H (con $0 \neq b \in B$). Si provi che il riprodotto di B per H con questi dati (secondo il paragrafo 3.4) è isomorfo al prodotto semidiretto naturale $B \rtimes H$.

Appendice: parametri dei grafi expanders.

Concludiamo dando una sommaria descrizione delle connessioni tra il parametro di espansione (o il valore δ) di un grafo ed altri importanti parametri classici in teoria dei grafi.

Diametro. Il diametro $diam(\Gamma)$ di un grafo connesso $\Gamma = (V, E)$ è definito come la massima distanza tra due vertici di Γ,

$$diam(\Gamma) = \max\{d_\Gamma(x, y) \mid x, y \in V\}.$$

Ad esempio, il diametro di un grafo di Cayley $\Gamma[G, S]$ è il valore massimo fra le lunghezze $\ell_S(g)$ degli elementi $g \in G$ (vedi sezione 2.1).
È piuttosto intuitivo che grafi con buone proprietà di espansione abbiano un diametro relativamente piccolo. Ciò è confermato dai fatti.
Sia $\Gamma = (V, E)$ un grafo. Per $x \in V$ e $r > 0$, si definisce la palla di raggio r e centro x; $B(x, r) = \{y \in V \mid d_\Gamma(x, y) \leq r\}$.
Sia Γ è un (n, k)–grafo, $h = h(\Gamma)$ il suo parametro di espansione, e sia $B = B(x, r)$ una palla di raggio $r \in \mathbb{N}$ in Γ, con $|B| \leq n/2$. Allora, per definizione di h,

$$|B(x, r + 1)| \geq (1 + h/k)|B|.$$

Da ciò segue che se Γ_n è una famiglia di k-expanders; allora esiste $\alpha > 1$ tale che per ogni $n \geq 1$, ed ogni vertice x di Γ_n, $|B(x, r)| \geq \min\{|\Gamma_n|/2, \alpha^r\}$. Tenendo conto che due palle di cardinalità $> |\Gamma_n|/2$ hanno intersezione non vuota, si conclude che $diam(\Gamma_n)$ è $O(\log |\Gamma_n|)$.
Per esempio se, per ogni primo $p \geq 3$, S_p è il sistema di generatori di $SL(2, p)$ come nel Teorema 13, allora (tenendo conto che $|SL(2, p)| \leq p^3$)

$$diam\, \Gamma[SL(2, p), S_p] = O(\log p);$$

cosa di cui non sembra nota una dimostrazione elementare. Dal Teorema 16 segue che esistono $k \in \mathbb{N}$ e $R > 0$ tali che quasi ogni gruppo semplice non–abeliano G ammette un sistema di k generatori rispetto al quale ogni elemento di G ha lunghezza al più $R(\log |G|)$. Di fatto, un risultato più esplicito era già noto:

Esiste una costante $R > 0$ tale che per ogni gruppo semplice finito non–abeliano G esiste un sistema di 7 generatori S con $diam\, \Gamma[G, S] \leq R \log |G|$ (Babai, Kantor e Lubotzky [8]).
Va da sé che la limitazione logaritmica (che si vede facilmente essere la migliore possibile) al diametro in una famiglia di grafi regolari è una condizione più debole dell'essere quella una famiglia di expanders; ad esempio, il sistema di generatori per

i gruppi $SL(2,p)$ dell'esercizio 16, definiscono grafi di Cayley che non sono expanders ma hanno diametro logaritmico (Kassabov e Riley).

Numero cromatico. Una *colorazione* (dei vertici) di un grafo $\Gamma = (V, E)$ è un'applicazione $\gamma : V \to C$, dove C è un insieme non vuoto (i cui elementi sono detti colori), tale che per ogni $u, v \in V$, se u e v sono adiacenti allora $\gamma(u) \neq \gamma(v)$.
Sia $1 \leq k \in \mathbb{N}$; un grafo Γ si dice k-colorabile se esiste una colorazione di Γ con k colori. Per ogni grafo finito Γ esiste un numero minimo k per cui Γ è k-colorabile: tale k è detto *numero cromatico* di Γ e si indica con $\chi(\Gamma)$. Banalmente, $\chi(\Gamma) = 1$ se e solo se Γ non contiene alcun arco, e $\chi(\Gamma) = 2$ se e solo se Γ è bipartito (e contiene almeno un arco)[12],
Strettamente legato al numero cromatico è il concetto di *indice di stabilità* $\alpha(\Gamma)$ del grafo Γ: esso è definito come la massima cardinalità di un sottoinsieme stabile di (cioè un insieme X di vertici tale che nessuna coppia di elementi di X è adiacente in Γ). C'è un semplice legame tra indice di stabilità e numero cromatico; infatti, se il grafo Γ ammette una colorazione allora l'insieme (chiamiamolo X) dei vertici di uno stesso colore è, per definizione, un sottoinsieme stabile di Γ, e dunque $|X| \leq \alpha(G)$. Da questa osservazione segue che *se* Γ *è un grafo con* n *vertici allora*

$$\alpha(\Gamma)\chi(\Gamma) \geq n. \tag{48}$$

Sia ora Γ un (n, k, δ)-grafo, e sia X un insieme stabile di Γ. Allora, con le notazioni del Mixing Lemma 6, $E(X, X) = \emptyset$ e dunque per il Lemma stesso,

$$\frac{k|X|^2}{n} \leq k\delta|X|$$

e dunque $\alpha(\Gamma) \leq \mu n/k$. In congiunzione con (48) si ottiene quindi

Proposizione 30. *Sia* Γ *un* (n, k, δ)*-grafo; allora*

$$\chi(\Gamma) \geq 1/\delta.$$

Calibro (girth). Un altro importante parametro di un grafo è il calibro (in inglese: girth); il calibro $g(\Gamma)$ di un grafo Γ è la minima lunghezza di un ciclo non-banale (cioè di lunghezza almeno 3) che compare come sottografo di Γ; se Γ non ha cicli non–banali (ovvero, nel caso connesso, Γ è un albero) si dice che Γ ha calibro ∞. Ad esempio, il calibro di un grafo di Cayley $\Gamma[G, S]$ è la lunghezza minima di un ciclo non

[12] Un classico risultato di Brooks (vedi [4]) afferma che per ogni grafo connesso Γ, si ha $\chi(\Gamma) \leq \Delta(\Gamma) + 1$ (dove $\Delta(\Gamma)$ è il massimo dei gradi dei vertici di Γ), e l'uguaglianza vale solo per Γ completo oppure un ciclo dispari.

banale che inizia nel vertice 1_G, e quindi è il minimo $t \geq 3$ per cui è possibile scrivere $1 = s_1 s_2 \cdots s_t$, con $s_i \in S$ e $s_{i+1} \neq s_i^{-1}$, per $i = 1, \ldots, t-1$.

Un interessante e vecchia questione riguarda l'esistenza di grafi connessi il cui numero cromatico e calibro siano entrambi arbitrariamente grandi. Anche questa è una richiesta di una possibile connivenza tra connessione (numero cromatico grande) e sparsità (calibro grande). La dimostrazione dell'esistenza di grafi con tali requisiti, dovuta a Erdös (1959), segna l'avvio dell'utilizzo di metodi probabilistici in teoria dei grafi. I primi esempi espliciti furono trovati da Lovasz; una decina di anni più tardi. Non è sorprendente che nuovi esempi (che sono inoltre grafi di Cayley) si rinvengano tra le costruzioni di expanders. Precisamente, si tratta dei grafi di Ramanujan costruiti da Lubotzky, Phillips e Sarnak [11] e Margulis [16]. Infatti, se X è un grafo di Ramanujan k–regolare, allora, per definizione, $\delta(X) \leq 2\sqrt{k-1}/k$; se $X_{p,q}$ è uno dei grafi descritti nella sezione 2.3, allora $k = p+1$, e quindi, per la proposizione 30, $\chi(X_{p,q}) \geq \sqrt{p}/2$; dall'altra parte, usando il fatto che, in i grafi $X_{p,q}$ sono quozienti dell'albero infinito $(p+1)$–regolare (il cui calibro è, in un certo senso, infinito) si dimostra in [11] che $g(X_{p,q}) \geq 2 \log_p q$.

Esercizio 31. Si usi la limitazione $O(\log n)$ per il diametro dei grafi expanders, per dimostrare che non esistono famiglie infinite di gruppi abeliani che sono Cayley expanders. [sugg.: il numero di soluzioni intere non–negative di $x_1 + \cdots + x_k \leq d$ è uguale a $\binom{d+k}{k}$]

Riferimenti bibliografici

[1] S. Hoory, N. Linial and A. Wigderson, Expander Graphs and their Applications. *Bull. A. M. S.* **43** (2006), 439–561.

[2] G. Davidoff, P. Sarnak, and A. Valette, Elementary Number Theory, Group Theory and Ramanujan Graphs. *London Math. Soc. Students Texts* **55**, Cambridge, 2003.

[3] A. Lubotzky, Discrete groups, expanding graphs and invariant measures. *Progress in Mathematics* **125**, Birkhauser, 1994.

[4] B. Bollobas, Modern graph theory. *Graduate Texts in Mathematics* **184**, Springer–Verlag, 1998.

[5] N. Alon, Eigenvalues and expanders. *Combinatorica* **6** (1986), 83–96.

[6] N. Alon, O. Schwartz and A. Shapira, An elementary Construction of Constant–Degree Expanders. *Proc. Eighteenth Annual ACM-SIAM SODA* (2007), 454-458.

[7] N. Alon, A. Lubotzky and A. Wigderson, Semi-direct product in groups and zig-zag product in graphs: connections and applications. *42nd IEEE Symposium on Foundations of Computer Science* (Las Vegas, NV, 2001), 630–637.

[8] L. Babai, W.M. Kantor and A. Lubotzky, Small–diameter Cyley graphs for finite simple groups. *European J. Combin* **10** (1989), 507–522.

[9] M. Kassabov, Symmetric groups and expander graphs. *Invent. Math.* **170** (2007), 327–354.

[10] M. Kassabov, A. Lubotzky and N. Nikolov, Finite simple groups as expanders. *Proc. Natl. Acad. Sci. USA* **103** (2006), 6116–6119.

[11] A. Lubotzky, R. Phillips and P. Sarnak, Ramanujan Graphs. *Combinatorica* **8** (1988), 261–277.

[12] A. Lubotzky and B. Weiss, Groups and Expanders. *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.* **10** (1993), 95–109.

[13] A. Lubotzky and E. Zelmanov, Dimension expanders. *J. Algebra* **319** (2008), 730–738.

[14] A. Lubotzky and A. Zuk, On property (τ). In preparazione.

[15] G. A. Margulis, Explicit construction of Expanders. *Problemy Peredaci Informacii* **9** (1973), 71–80.

[16] G. A. Margulis, Explicit group–theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators, *J. Problems of Information Transmission* **24** (1988), 39–46.

[17] R. Meshulam and A. Wigderson, Expanders in Group Algebras. *Combinatorica* **24** (2004), 659–680.

[18] M. Morgenstern, Existence and explicit constructions of $(q+1)$–regular Ramanujan graphs for every prime power q. *J. Combin. Theory Ser. B* **62** (1994), 44-62, 1994.

[19] N. Nikolov, On the commutator width of perfect groups. *IBull. London Math. Soc.* **36** (2004), 30–36.

[20] E. Rozenman, A. Shalev and A. Wigderson, Iterative Construction of Cayley Expander Graphs. *Theory of Computing* **2** (2006), 91–120.

[21] O. Reingold, S. Vadhan and A. Wigderson, Entropy waves, the zig-zag graph product, and new constant-degree expanders. *Ann. of Math.* **155** (2002), 157–187.