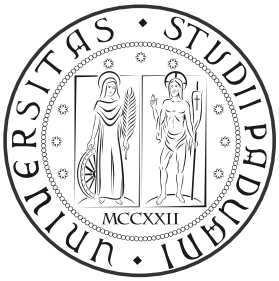

Università di Padova

Tesi di Laurea Magistrale in Matematica

Il Problema dell'Hamiltonianità nei Grafi di Cayley

Autore:
Alessandro Paolini

Relatore:
Prof. Andrea Lucchini

16 Luglio 2012

Indice

Introduzione

In letteratura, un problema classico in teoria dei grafi è quello della ricerca di cicli hamiltoniani, ovvero di percorsi chiusi che passino esattamente una volta per tutti i vertici di un dato grafo. Grafi che possiedono questa proprietà vengono detti hamiltoniani. L'obiettivo del lavoro che segue è analizzare questo problema per una classe di grafi con particolari proprietà algebriche. Nel nostro caso, fissati un gruppo G ed un suo insieme di generatori S, i vertici saranno gli elementi di G, e gli archi saranno della forma $(g, gs), (g, gs^{-1})$ con $s \in S$: tali grafi sono detti grafi di Cayley, e indicati con $Cay(G, S)$.

Il problema dell'hamiltonianità per questi grafi è del tutto aperto. La congettura di Lovasz, formulata negli anni '70, è che $Cay(G, S)$ sia hamiltoniano per qualsiasi gruppo finito G e per qualsiasi insieme di generatori S per G. Tale congettura è stata dimostrata in diversi casi particolari, ma mancano risultati davvero generali, e più di un autore ne mette in dubbio la validità.

Il primo dei due capitoli della tesi contiene una panoramica dei principali risultati presenti in letteratura. In particolare, vengono descritti i metodi utilizzati da diversi autori per dimostrare la congettura di Lovasz in presenza di ipotesi opportune su un gruppo G (riguardanti ad esempio l'ordine di G o la struttura del suo gruppo derivato). Particolare attenzione verrà dedicata al caso dei gruppi diedrali, per i quali i risultati ottenuti sono solo parziali e che rappresentano l'esempio più clamoroso di gruppi con struttura particolarmente semplice, ma per i quali sembra già arduo produrre risposte complete e generali. Alla fine di questa prima parte vengono evidenziate le differenze con l'analogo orientato dei grafi di Cayley, detti digrafi di Cayley, in cui si ammettono solo archi della forma (g, gs) con $s \in S$, mostrando anche un risultato non presente in

letteratura riguardante l'assenza di cammini hamiltoniani per infiniti digrafi su gruppi semplici.

Nel secondo capitolo, la congettura di Lovasz viene affrontata da un diverso punto di vista. Il problema che ci si pone è di trovare efficaci limitazioni superiori alla cardinalità di un insieme S di generatori per un generico gruppo G, tale che $Cay(G, S)$ sia hamiltoniano. Siano infatti $d(G)$ la minima cardinalità di un insieme S di generatori di G, e $d^*(G)$ la minima cardinalità di un insieme S di generatori di G con l'ulteriore proprietà che $Cay(G, S)$ sia hamiltoniano. È ancora aperto, come osserva L. Babai in un suo lavoro, il problema di determinare se per ogni gruppo G valga $d(G) = d^*(G)$. Quello che si cerca di fare in questa parte del lavoro è dare una buona stima per $d^*(G)$. All'inizio di questo capitolo viene presentato il recente risultato di I. Pak, che consiste di una limitazione a $d^*(G)$ in funzione del numero di fattori di una serie di composizione di G: più precisamente, è $d^*(G) \leq r + 2m + 1$, dove r, m sono rispettivamente il numero di fattori abeliani e non abeliani della serie di composizione. Per mostrare questo fatto, si utilizza un importante risultato in teoria dei gruppi, che deriva dalla classificazione dei gruppi semplici: un gruppo semplice può sempre essere generato da due elementi, di cui uno di ordine 2.

Successivamente, vengono presentati alcuni risultati originali, fulcro di questa tesi. Otteniamo infatti dei nuovi risultati che migliorano notevolmente le stime fornite da Pak. A questo scopo, dovremo anche dimostrare un nuovo risultato sulla generazione dei gruppi semplici non abeliani: faremo vedere che anche il prodotto diretto di due gruppi semplici isomorfi non abeliani è generato da due elementi, uno dei quali è un'involuzione. La dimostrazione di questo fatto si basa su recenti risultati di diversi autori in teoria dei gruppi. Come conseguenza, la precedente stima viene migliorata in $d^*(G) \leq r + \frac{4}{3}m + 2$. In un gran numero dei casi, determinati dalla struttura di G, si può addirittura sostituire il coefficiente $\frac{4}{3}$ con un 1. Infine, una applicazione di un teorema di Fleischner ci consente di dimostrare che il coefficiente di m nella stima si può sostituire con $\alpha \in]0, 1[$, a meno di una costante additiva c_α con $c_\alpha = O(\frac{1}{\alpha^{2+\epsilon}})\, \forall \epsilon > 0$, dove α e c_α non dipendono dal gruppo G.

Molti grafi vertex-transitive, che si incontrano di frequente in matematica applicata, sono grafi di Cayley, dunque ci si può ricondurre allo studio di questi ultimi: ad esempio, è così che si dimostra che ogni grafo vertex-transitive di ordine p^2 o p^3 è hamiltoniano. Inoltre, i grafi di Cayley forniscono esempi di costruzioni esplicite di expanders, anch'essi grafi di fondamentale importanza nelle applicazioni, soprattutto negli ultimi anni. Il fatto che risultati importanti, avanzati e molto recenti in teoria dei gruppi possano essere utili nelle applicazioni, come in matematica discreta, e la mia passione per l'algebra, in particolare proprio per la teoria dei gruppi finiti, sono le principali motivazioni che mi hanno spinto a scegliere di affrontare un argomento come questo in una tesi di Laurea Magistrale in Matematica.

CAPITOLO 1

Descrizione del problema: hamiltonianità per classi di gruppi

In questo capitolo, dopo aver introdotto le definizioni e sottolineato le proprietà di base dei grafi di Cayley, verranno mostrate le principali tecniche per trovare cammini e cicli hamiltoniani, e saranno esaminate diverse classi di gruppi di cui si tenta di dire che l'hamiltonianità vale sempre. Supporremo sempre, da qui fino alla fine del lavoro, che ogni gruppo G preso in considerazione sia *finito*. Per esempio, la risposta è affermativa per gruppi abeliani e p-gruppi, mentre per i gruppi diedrali la questione è ancora aperta.

1. Definizioni e prime proprietà

Definizione 1.1. *Dati un gruppo G e un insieme di generatori S per G, il rispettivo* grafo di Cayley*, denotato nel seguito con $Cay(G, S)$, è il grafo avente per vertici gli elementi di G e per archi tutti e soli quelli della forma (g, gs) e (g, gs^{-1}), con $g \in G$ e $s \in S$. Diremo che g è* connesso ad *h se $g = hs\, \exists s \in S$ oppure $g = hs^{-1}\, \exists s \in S$. Denoteremo semplicemente con s l'arco (g, gs).*

Se si permette agli archi di essere solo della forma (g, gs), con $g \in G, s \in S$, si parla di digrafo di Cayley $\overrightarrow{Cay}(G, S)$.

Ciò che cambia fra le due definizioni è che nel caso dei digrafi si tiene conto anche dell'orientazione, mentre per i grafi ogni arco può considerarsi non orientato. Nel seguito, ci occuperemo prevalentemente di grafi, evidenziando differenze e particolarità per i digrafi. Osserviamo che poichè S genera G, il grafo $Cay(G, S)$ è un grafo connesso.

Parlando di un percorso all'interno di un grafo, vi sono due modi per descriverlo. Il primo modo è specificarne i vertici: in questo caso, la descrizione del cammino è $(v_0, v_1, \ldots, v_m)$, con i $\{v_i\}_{i=0}^{m}$ vertici. Da qui, si può anche capire chi è l'arco s_{i+1} che

congiunge il vertice v_i a v_{i+1}: per definizione è $s_{i+1} = {v_i}^{-1} v_{i+1}$. Il secondo modo è specificare il vertice di partenza v_0 e la sequenza di archi che vengono di volta in volta applicati, $[s_1, \ldots, s_k]$. Quando non verrà specificato v_0 avremo assunto implicitamente $v_0 = 1$.

Indicheremo poi, se α, β sono archi o sequenze di archi, con $[\alpha, \beta]$ la sequenza ottenuta giustapponendo le due sequenze (o archi) una dopo l'altra, e con il simbolo $*$ fra un intero positivo n e una sequenza di archi la concatenazione di tale sequenza di archi n volte. Ad esempio:

$$2 * [a, 3 * [b, c], a^2] = [a, b, c, b, c, b, c, a^2, a, b, c, b, c, b, c, a^2].$$

Ricordiamo la seguente:

Definizione 1.2. *Dato un grafo $G(V, E)$, un percorso a estremi distinti in tale grafo che incontra ciascun vertice $v \in V$ una e una sola volta si dice* cammino hamiltoniano. *Un* ciclo hamiltoniano *è un percorso chiuso nel grafo che transita esattamente una volta per ciascun vertice v di $G(V, E)$. Diremo che un grafo è* hamiltoniano *se contiene un ciclo hamiltoniano.*

Percorsi con le stesse caratteristiche in un digrafo si dicono rispettivamente cammini hamiltoniani orientati *e* cicli hamiltoniani orientati. *Un digrafo è* hamiltoniano *se possiede un ciclo hamiltoniano orientato.*

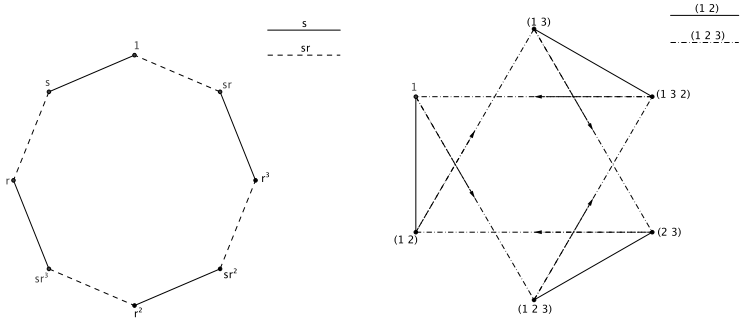

Figura 1.1. I grafi di Cayley $Cay(D_4, \{s = (12)(34), sr = (13)\})$, dove $r = (1234)$, e $Cay(S_3, \{(12), (123)\})$.

È facile estrarre un ciclo hamiltoniano da entrambi i grafi in Figura 1.1: nel grafo $Cay(D_4, \{s, sr\})$ un ciclo è evidentemente $4 * [s, sr]$, e in $Cay(S_3, \{(12), (123)\})$ un ciclo è, ad esempio, $2 * [(12), 2 * (123)]$.

Esempio 1.1 (Ipercubo). Siano $G_n = \mathbb{Z}_2^n$, e_i il vettore con componente i-esima 1 e le altre nulle, $i = 1, \ldots, n$, $S_n = \{e_1, \ldots, e_n\}$, $n \geq 2$. Costruiamo induttivamente un ciclo hamiltoniano in $Cay(G_n, S_n)$. Per $n = 2$ è semplice: $(0,0) \overset{e_1}{\mapsto} (1,0) \overset{e_2}{\mapsto} (1,1) \overset{e_1}{\mapsto} (0,1) \overset{e_2}{\mapsto} (0,0)$. Supponiamo ora di riuscire a costruire un tale ciclo per n fissato, e mostriamo che anche $Cay(G_{n+1}, S_{n+1})$ è hamiltoniano. Per ipotesi induttiva, abbiamo un ciclo hamiltoniano su $Cay(G_n \times \{0\}, S_{n+1})$ che coinvolge archi diversi da e_{n+1}, sia tale ciclo $[l_1, \ldots, l_{2^n}]$. Si ha che:

$$2 * [[l_i]_{i=1}^{2^n-1}, e_{n+1}]$$

è il ciclo hamiltoniano desiderato.

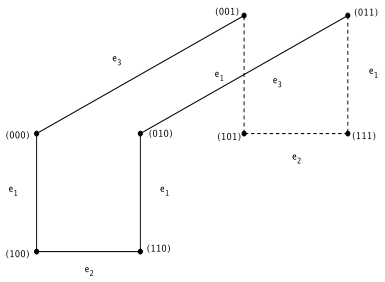

Figura 1.2. Il grafo dell'ipercubo in tre dimensioni, $Cay(\mathbb{Z}_2^3, \{e_1, e_2, e_3\})$.

In matematica discreta, esiste una classe di grafi particolarmente interessante. Premettiamo la seguente:

Definizione 1.3. *Dato un grafo $\mathbb{G} = G(V, E)$, un* automorfismo *di un grafo è una permutazione τ dei vertici del grafo, tale che per ogni $a, b \in V$, (a, b) è un arco se e solo se anche $(\tau(a), \tau(b))$ è un arco.*

Tutti gli automorfismi di un grafo formano un gruppo con l'operazione di composizione; chiameremo tale gruppo con $Aut(\mathbb{G})$.

Definizione 1.4. *Un grafo $\mathbb{G} = G(V, E)$ si dice* vertex-transitive *se per ogni coppia di vertici $a, b \in V$ esiste un automorfismo τ di $\mathbb{G}$ tale che $\tau(a) = b$.*

Tra questi, vi sono anche i grafi di Cayley. Infatti:

Proposizione 1.1. *Ogni grafo di Cayley $Cay(G, S)$ è vertex-transitive.*

Dim. Sia $Cay(G, S) = \mathbb{G}(G, E)$, e siano $g, h \in G$. La trasformazione $k \mapsto ak$, $k \in G$, dove $a = hg^{-1}$, manda g in h, e chiaramente preserva le coppie di archi fra i trasformati. □

Esistono grafi vertex-transitive che non sono hamiltoniani: ne sono stati trovati quattro finora. Nessuno di questi, però, è un grafo di Cayley. Ad oggi, non sono stati trovati grafi di Cayley non hamiltoniani, mentre per molte classi di gruppi, con generatori arbitrari, e per svariati gruppi con particolari generatori, la congettura di Lovasz si risolve affermativamente. Questo capitolo è dedicato ad illustrare i casi di cui si può dire tutto o quasi, presentando i problemi per i casi ancora incompleti. La congettura, posta da Lovasz nel 1970 e aperta ancora oggi, è la seguente.

Congettura (Lovasz). *Ogni grafo di Cayley $Cay(G, S)$ è hamiltoniano.*

Questa congettura è posta solo per i grafi. È facile, come vedremo, trovare esempi di digrafi senza nemmeno cammino hamiltoniano. Una cosa che invece è chiara è che se si prende un insieme sufficientemente grande di generatori (basti pensare $S = G$) allora il rispettivo grafo è banalmente hamiltoniano. Il problema discusso nel prossimo capitolo sarà vedere in generale quanto si riesce a ridurre le dimensioni di questo insieme.

Problema. *Quanto piccolo può essere un insieme di generatori S per G di modo che $Cay(G, S)$ sia hamiltoniano?*

Vedremo che si potrà sempre prendere S tale che $|S| \leq \log_2(|G|)$. Questa stima, sebbene la migliore possibile in alcuni casi, ad esempio $Cay(\mathbb{Z}_2{}^n, \{e_1, \ldots, e_n\})$, in altri rimane ancora molto larga: vedremo come si può migliorare.

2. Tecniche di costruzione di cicli hamiltoniani e caso abeliano

Enunciamo e dimostriamo dei lemmi di aiuto per la costruzione o ricostruzione di cammini e cicli hamiltoniani in un grafo di Cayley. In presenza di un quoziente di

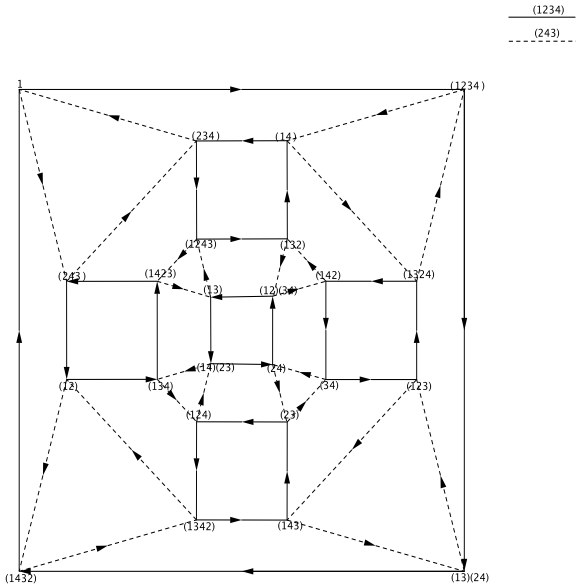

Figura 1.3. Il grafo $Cay(S_4, \{(1234), (243)\})$.

un gruppo G su un suo sottogruppo normale N, denoteremo $\bar{g}$ la proiezione di g sul quoziente G/N.

Lemma 1.1 (del quoziente). *Sia G un gruppo con insieme di generatori S. Sia $N \trianglelefteq G$, N ciclico. Se in $Cay(G/N, \bar{S})$ vi è un ciclo hamiltoniano $[\bar{g}_1, \cdots, \bar{g}_n]$, tale che $g_1 \dots g_n$ genera N, allora $|N| * [g_1, \dots, g_n]$ è un ciclo hamiltoniano in $Cay(G, S)$.*

Dim. Sia $|G/N| = n$, e sia $[\bar{g}_1, \dots, \bar{g}_n]$ il ciclo hamiltoniano sul quoziente. Allora, il percorso $|N| * [g_1, \dots, g_n]$ è un ciclo hamiltoniano su G: questo perchè il prodotto $g_1 \cdots g_n$ genera N, quindi ad ogni elemento del percorso è associata in maniera biunivoca, se $N = \langle x \rangle$, una potenza i-esima di x, $i = 1, \dots, |N|$, e un j tra 1 e n, corrispondente a un prodotto $g_1 \cdots g_j$: i vertici del percorso $|N| * [g_1, \dots, g_n]$ sono dunque tutti elementi distinti. □

Esempio 1.2. Sia $p \equiv 1 \mod 6$, e consideriamo il gruppo $G = C_p \rtimes C_6$, con $C_p = \langle a \rangle$, $C_6 = \langle b \rangle$, e l'azione di C_6 su C_p è definita da: $a^b = a^\epsilon$, con ϵ radice primitiva sesta dell'unità in $\mathbb{Z}_p$, la cui esistenza è garantita dall'ipotesi su p.

Mostriamo che $\alpha = b^3$, $\beta = ab^2$ sono dei generatori per G. Chiaramente α ha ordine 2, mentre si ha:

$$\beta^2 = b^2 a^{b^2} ab^2 = b^2 a^{\epsilon^2+1} b^2 = b^4 (a^{b^2})^{1+\epsilon^2} = b^4 a^{\epsilon^2-\epsilon}, \quad \beta^3 = b^{-2} a^{\epsilon^2-\epsilon+1} b^2 = 1,$$

essendo $x^2 - x + 1$ il polinomio minimo di ϵ su $\mathbb{Z}_p$, dunque $|\beta| = 3$. Inoltre, si ha:

$$[\alpha, \beta] = b^{-5} a^{-1} b^3 ab^2 = (a^{-1})^{b^5} a^{b^2} = a^{2\epsilon^2},$$

di ordine p in G. Se poniamo $\gamma = \alpha\beta^{-1}$, è dunque:

$$\langle \alpha, \beta \rangle \supseteq \langle [\alpha, \beta], \gamma \rangle = \langle a^{2\epsilon^2}, ba^{-1} \rangle = \langle a, b \rangle = G.$$

Il grafo $Cay(G, \{\alpha, \beta\})$ è hamiltoniano. Consideriamo infatti il quoziente su $\langle a \rangle$, ciclico di ordine p. $Cay(\bar{G}, \{\bar{\alpha}, \bar{\beta}\})$ ha il ciclo hamiltoniano:

$$[\bar{\beta}, \bar{\beta}, \bar{\alpha}, \bar{\beta}^{-1}, \bar{\beta}^{-1}, \bar{\alpha}] = [ab^2, ab^2, b^3, (ab^2)^{-1}, (ab^2)^{-1}, b^3].$$

Il prodotto di tutti questi archi vale:

$$(ab^2)^2 b^3 (ab^2)^{-2} b^3 = ab^2 ab^3 a^{-1} b^{-2} a^{-1} b^3 = aa^{b^4} (a^{-1})^b (a^{-1})^{b^3} = aa^{\epsilon^4} a^{-\epsilon} a^{-\epsilon^3} = a^{2(1-\epsilon)},$$

che è un generatore di C_p. Per il Lemma 1.1, troviamo il seguente ciclo hamiltoniano in G:

$$p * [ab^2, ab^2, b^3, (ab^2)^{-1}, (ab^2)^{-1}, b^3].$$

Poter prendere gli inversi degli elementi di S è un fatto essenziale per l'hamiltonianità. Più avanti, mostreremo infatti che il digrafo $\overrightarrow{Cay}(C_p \rtimes C_6, \{b^3, ab^2\})$ di hamiltoniano non possederà nemmeno un cammino.

Presentiamo altri risultati di costruzione di cammini e cicli che useremo diverse volte nel seguito.

Lemma 1.2 (Partenza arbitraria di cammini e cicli). *Sia G gruppo, S un insieme di generatori tale che $Cay(G, S)$ possieda un cammino o un ciclo hamiltoniano $[s_1, \ldots, s_k]$, di partenza v_0. Allora, per ogni $g \in G$, il percorso che parte da g e di archi*

gli stessi $[s_1, \ldots, s_k]$ *è ancora un cammino (ciclo) hamiltoniano. In particolare, dato un cammino (ciclo) hamiltoniano, ne si può decidere arbitrariamente la partenza.*

Dim. Proviamo questo risultato per un cammino, per un ciclo si procede allo stesso modo. Sia $|G| = m$, e $[s_1, \ldots, s_{m-1}]$ la sequenza di archi di un cammino hamiltoniano, dove s_i connette g_i e g_{i+1}, e g_1 è il punto di partenza del cammino. Preso un qualsiasi g in G, posto $h = g{g_1}^{-1}$ si ha $hg_1 = g$. L'insieme $\{hg_1, hg_2, \ldots, hg_m\}$ è G, essendo la moltiplicazione a sinistra una permutazione degli elementi del gruppo, e ogni s_i connette ancora hg_i a hg_{i+1}. Si ha un cammino hamiltoniano di partenza g, scelto arbitrariamente, e archi $[s_1, \ldots, s_{m-1}]$. □

Lemma 1.3 (Estensione di cammini). *Sia G gruppo, $N \trianglelefteq G$, tale che G è generato da $S = S_1 \cup S_2$, con $\langle S_1 \rangle = N$, $\bar{S_2} = G/N$, e $Cay(N, S_1)$, $Cay(G/N, \bar{S_2})$ possiedono un cammino hamiltoniano. Allora, anche $Cay(G, S)$ ha un cammino hamiltoniano.*

Dim. Siano $n = |N|$, $r = |G/N|$. Sia $[\bar{s_1}, \ldots, \bar{s}_{r-1}]$ un cammino hamiltoniano su G/N, dove s_i congiunge rispettivamente Ng_i a Ng_{i+1}, $i = 1, \ldots, r-1$, $s_i \in S_2 \, \forall i = 1, \ldots, r-1$. Poichè N possiede un cammino hamiltoniano $[t_1, \ldots, t_{n-1}]$ con archi in S_1, su ogni classe laterale si trova un cammino hamiltoniano di archi $[t_1, \ldots, t_{n-1}]$, che parte in un qualsiasi elemento della classe. Si ha quindi che:

$$[[[t_i]_{i=1}^{n-1}, s_j]_{j=1}^{r-1}, [t_k]_{k=1}^{n-1}]$$

è un cammino hamiltoniano su $Cay(G.S)$. □

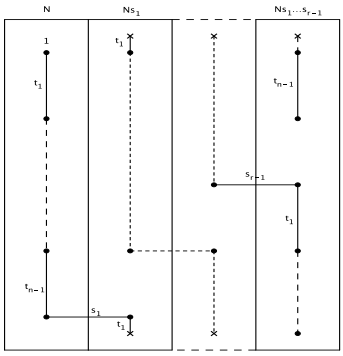

Figura 1.4. Il procedimento di ricostruzione per quozienti dei cammini hamiltoniani, come nel Lemma 1.3.

Si noti che i Lemmi 1.1, 1.2, 1.3 continuano a valere anche nel caso orientato. Per non appesantire le notazioni, abbiamo presentato solo le dimostrazioni nel caso non orientato.

Si è visto che i sottogruppi normali sono della massima importanza per costruire cammini e cicli nel gruppo di partenza. Nel caso abeliano, in cui tutti i sottogruppi sono normali, si può dire la cosa più soddisfacente.

Proposizione 1.2. *Sia G un gruppo abeliano, S un insieme di generatori per G. Allora, il grafo $Cay(G, S)$ è hamiltoniano.*

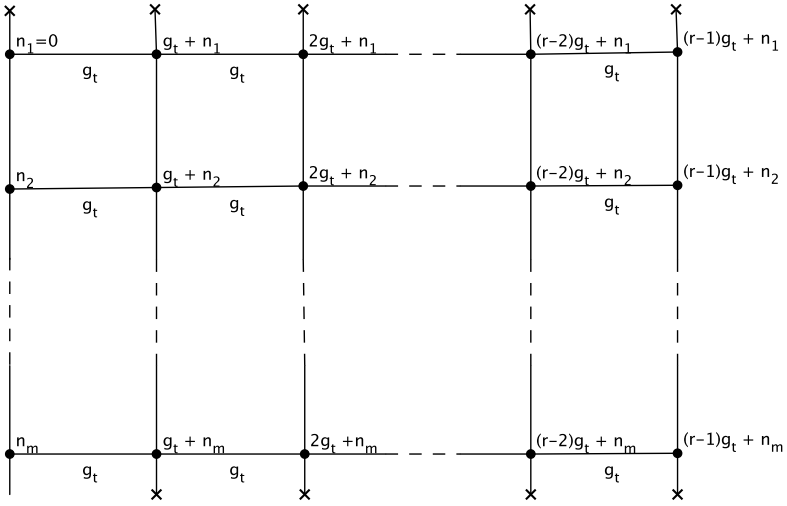

Figura 1.5. Il passo induttivo descritto nella Proposizione 1.2.

Dim. Ragioniamo per induzione su $|S|$. Nel caso base, $S = \{g\}$, G è un gruppo ciclico, e ovviamente, detto s l'ordine di g, si ha il ciclo $[g, g, \ldots, g]$, dove g è ripetuto s volte, a partire da un qualsiasi elemento del gruppo.
Sia ora $S = \{g_1, \ldots, g_t\}$, e supponiamo che il fatto che vogliamo dimostrare valga per ogni gruppo abeliano generato da al massimo $t - 1$ elementi. Sia r l'ordine di g_t modulo N. A priori, l'insieme S può contenere un elemento g ed anche il suo inverso $-g$. Consideriamo il sottogruppo $N = \langle S' \rangle$, dove $S' = S \setminus \{g_t, -g_t\}$, e sia $m = |N|$. Per ipotesi, N possiede un

ciclo hamiltoniano, sia esso $(n_1 = 0, n_2, \ldots, n_m)$. Si hanno inoltre in G tutti gli archi del tipo g_t, che collegano, in particolare, ogni $ag_t + n_i$ con $(a+1)g_t + n_i$, $0 \leq a \leq r-2, 1 \leq i \leq m$.

Ogni elemento di G si scrive poi in modo unico come $ag_t + n_i, 0 \leq a \leq r-1, 1 \leq i \leq m$. Infatti, se si ha, per i valori di a, b, i, j ammissibili, $ag_t + n_i = bg_t + n_j$, è $(b-a)g_t = n_i - n_j \in N$, e l'unico multiplo di g_t, con coefficiente fra 0 e $r-1$, a stare in N, è proprio 0, da cui $b = a$, e $n_i = n_j$. Tali elementi, al variare di a e i, sono dunque mr, e sono tutti gli elementi di G, essendo:

$$|G| = \frac{|N||\langle g_t \rangle|}{|N \cap \langle g_t \rangle|} = |N|[\langle g_t \rangle : N \cap \langle g_t \rangle] = mr.$$

Abbiamo un sottografo come quello in Figura 1.6 Da qui riusciamo sempre ad estrarre un ciclo hamiltoniano: i ragionamenti dipendono solo da parità e disparità di r. Sia infatti $[l_1, \ldots, l_m]$ il ciclo hamiltoniano in N. Andiamo a discutere i casi:

- r dispari: $[\frac{r-1}{2} * [[l_i]_{i=1}^{m-2}, g_t, [-l_{m-i}]_{i=2}^{m-1}, g_t], [l_i]_{i=1}^{m-1}, (r-1) * (-g_t), l_m]$;
- r pari: $[\frac{r-2}{2} * [g_t, [l_i]_{i=1}^{m-2}, g_t, [-l_{m-i}]_{i=2}^{m-1}], g_t, [l_i]_{i=1}^{m-1}, (r-1) * (-g_t), [-l_{m-i}]_{i=1}^{m-1}]$.

□

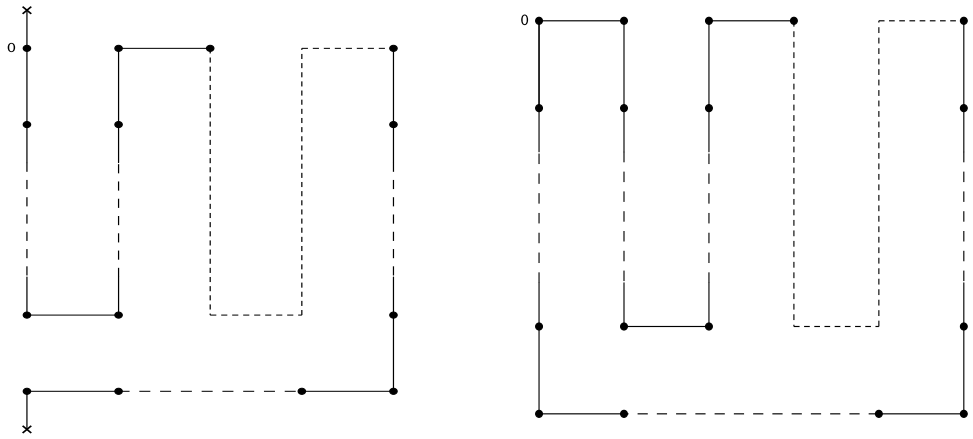

Figura 1.6. L'estrazione del ciclo nel caso abeliano: i due casi r pari ed r dispari della Proposizione 1.2

Per i grafi su gruppi abeliani, si è risolto il problema dell'hamiltonianità. Per i digrafi, la cosa cambia completamente: troviamo subito un esempio di un digrafo su un gruppo ciclico senza ciclo hamiltoniano.

Esempio 1.3. Mostriamo che $\overrightarrow{Cay}(\mathbb{Z}_6, \{2, 3\})$ non possiede un ciclo hamiltoniano orientato. Sia per assurdo C un tale ciclo, e supponiamo che esso contenga un arco orientato 3: esiste quindi $x \in \mathbb{Z}_6$ che va a finire in $x+3$. In C, l'elemento $x+1$ non può muoversi di arco 2 altrimenti arriverebbe anche lui a $x+3$, dunque deve muoversi di arco 3. Se c'è un arco 3, allora, tutti gli archi sono 3, assurdo perchè 3 divide 6, dunque vi sarebbero 3 cicli orientati disgiunti.

Non può quindi esserci nessun arco della forma 3, e non possono nemmeno, con conti simili, esserci solo archi della forma 2. Non può esistere un tale ciclo orientato.

Si può comunque trovare un cammino hamiltoniano sui digrafi in gruppi in cui tutti i sottogruppi sono normali. Ricordiamo che un gruppo *hamiltoniano* è un gruppo non abeliano, in cui tutti i sottogruppi sono normali.

Proposizione 1.3. *Se G è un gruppo abeliano o hamiltoniano, allora ogni grafo $\overrightarrow{Cay}(G, S)$ possiede un cammino hamiltoniano.*

Dim. Sia $s \in S$, con S insieme minimale di generatori, e siano $n = |G|, d = |s|$. Ragioniamo per induzione sull'ordine del gruppo. Per ipotesi, $\langle s \rangle$ è normale in G, e $|s| \geq 2$ per minimalità di S. Per induzione, vi è un cammino hamiltoniano $[\bar{s}_1, \dots \bar{s}_{\frac{n}{d}-1}]$ in $\overrightarrow{Cay}(G/\langle s \rangle, \bar{S})$. Per Il Lemma 1.3, troviamo un cammino hamiltoniano nel digrafo di Cayley $\overrightarrow{Cay}(G, S)$. □

3. Il caso più sorprendente: i p-gruppi

Nella Proposizione 1.2 abbiamo visto che la congettura di Lovasz è risolta in maniera affermativa per la classe dei gruppi abeliani. Esiste un'altra classe di gruppi, i p-gruppi, per cui vale la stessa cosa. Anzi, vale addirittura di più: ogni *digrafo* di Cayley su un p-gruppo è hamiltoniano. Il programma per mostrare questo fatto, dato un insieme arbitrario S di generatori per il p-gruppo G, è il seguente:

a) Trovare un sottogruppo normale N_S di G che dipenda solo da S, tale che il quoziente G/N_S contenga un ciclo hamiltoniano orientato;
b) Trovare una condizione algebrico-combinatorica su G ed S che permetta di estendere l'hamiltonianità da quozienti a gruppi più grandi;
c) Trovare una sequenza subnormale fino a N_S, con quozienti successivi che soddisfino la condizione in b).

Questo procedimento è l'idea che Morris[1] utilizza in [**25**], ed è, ad oggi, essenzialmente l'unico procedimento per trovare cicli hamiltoniani, anche non orientati, nei p-gruppi. Il procedimento è costruttivo, permette di esibire il ciclo hamiltoniano orientato. Supporremo d'ora in poi che S sia un insieme minimale di generatori. Sia $H = \langle S^{-1}S \rangle$, ovvero $H = \langle a^{-1}S \rangle$ per un qualsiasi $a \in S$, e consideriamo il sottogruppo normale di G: $H^G = \langle H^g : g \in G \rangle$. Esso ha le seguenti proprietà:

- G/H^G è ciclico. Infatti, è: $G = \langle S \rangle = \langle a, a^{-1}S \rangle = \langle a, H \rangle \leq \langle a, H^G \rangle$.
- H^G è un sottogruppo proprio di G. Innanzitutto, $a^{-1}S$ possiede $|S| - 1$ elementi non banali, e per minimalità di S si ha che $\langle a^{-1}S \rangle = H$ è sottogruppo proprio di G. Essendo poi G nilpotente, H è contenuto dentro a un sottogruppo massimale M normale in G, dunque $H^g \leq M \, \forall g \in G$, da cui $H^G \leq M < G$.

Si ha il seguente risultato valido in generale.

Proposizione 1.4. *Sia G p-gruppo, H un suo sottogruppo. Esiste una serie subnormale di H^G:*

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = H^G,$$

tale che H_i/H_{i-1}, $i = 1, \ldots, n$ è generato da un coniugato di H tramite G, ovvero esiste $g \in G$ tale che $H_i = H^g H_{i-1}$.

Dim. Ragioneremo per induzione sull'ordine di G. Sia N un sottogruppo di H^G, massimale rispetto a queste due condizioni:

- Esiste una serie subnormale $1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = N$ di N dove ciascun quoziente successivo è generato da un coniugato di H tramite G;
- $N \trianglelefteq H^G$.

Dimostriamo il risultato per assurdo. Sia $N \neq H^G$: esiste $g \in G$ tale che $H^g \not\leq N$. Poniamo $K = \langle H^g, N \rangle = NH^g \leq H^G$. Si può assumere $H \subsetneq G$, poichè $H = G$ è banalmente generato da un qualsiasi suo coniugato; è allora $H^G \subsetneq G$. Per induzione, ponendo $K^* = K^{H^G}$, esiste una serie subnormale $1 = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_m = K^*$ tale che i quozienti successivi sono generati da un coniugato di K tramite H^G. Essendo $K_0 = 1$, esiste un $h \in H^G$ tale che

[1] L'autore Dave Witte ha cambiato il suo cognome in Morris nel 2002.

$K_1 = K^h \supseteq N^h = N = H_n$, ed è $N \trianglelefteq K_1$ poichè $N \trianglelefteq H^G$, quindi è anche $N \trianglelefteq K$. Possiamo dunque giustapporre le due serie subnormali sopra, ottenendo:

$$1 = H_0 \trianglelefteq \cdots \trianglelefteq H_n \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_m = K^*.$$

Ogni quoziente del tipo H_i/H_{i-1}, per ipotesi, è generato da un coniugato di H tramite G. I K_i, $i \geq 1$ sono tali che esiste $h \in H^G$, con $K_i = K^h K_{i-1}$. Ma $K^h K_{i-1} = (NH^g)^h K_{i-1} = H^{g'} K_{i-1}$, poichè $N \subseteq K_{i-1}$, dunque K_i è generato da un coniugato di H tramite G. Analogamente si procede per mostrare che l'ultimo quoziente rimasto, K_1/N, è generato da un coniugato tramite G di H^G. Abbiamo quindi trovato un K^* con $N \subsetneq K^* \trianglelefteq H^G$, con serie subnormale come nell'ipotesi su N: per massimalità, questo è un assurdo che nasce dall'aver supposto $N \subsetneq H^G$. Deve quindi valere l'uguaglianza. □

Ora, la condizione algebrica di cui parlavamo prima, di cui omettiamo la poco interessante dimostrazione. Se $H \leq G$, denotiamo con $\overrightarrow{Cay}(G,S)_{/H}$ il grafo orientato ottenuto da $\overrightarrow{Cay}(G,S)$ contraendo ciascuna classe laterale Hg in un unico vertice.

Proposizione 1.5. *Sia G gruppo, $\langle S \rangle = G$, e siano $K \trianglelefteq H \leq G$. Supponiamo che esistano:*

- *un ciclo hamiltoniano orientato in $\overrightarrow{Cay}(G,S)_{/H}$, di partenza Hg e archi $[t_i]_{i=1}^n$;*
- *un ciclo hamiltoniano orientato in $\overrightarrow{Cay}(H/K, (\overline{t_1 \cdots t_{n-1} S)^{g^{-1}}})$[2], di partenza K e archi $[\overline{(t_1 \cdots t_{n-1} s_j)^{g^{-1}}}]_{j=1}^m$.*

Allora, il percorso di partenza Kg e archi $[[t_i]_{i=1}^{n-1}, s_j]_{j=1}^m$ è un ciclo hamiltoniano orientato in $Cay(G,S)_{/K}$.

Possiamo dimostrare il risultato prima citato per i p-gruppi. Costruiremo il nostro ciclo hamiltoniano partendo da un piccolo quoziente del gruppo, e andando a quozienti sempre più grandi, fino a ottenere l'intero gruppo. Per non appesantire le notazioni, scriveremo S al posto della proiezione di S nel gruppo quoziente che prendiamo in considerazione.

Teorema 1.1. *Sia G un p-gruppo, $\langle S \rangle = G$. Allora, $\overrightarrow{Cay}(G,S)$ è hamiltoniano.*

[2] In particolare, deve valere $\langle \overline{(t_1 \cdots t_{n-1} S)^{g^{-1}}} \rangle K/K = H/K$.

Dim. Possiamo supporre che S sia un insieme minimale di generatori. Sia al solito $H = \langle S^{-1}S\rangle$. Per la Proposizione 1.4, esiste $1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = H^G$, tale che ogni quoziente successivo è generato da un opportuno coniugato di H. G/H^G è ciclico di ordine una potenza di un primo, perciò necessariamente troviamo un $a \in S$ generatore di tutto il quoziente G/H^G: $\overrightarrow{Cay}(G/H^G, S)$ è hamiltoniano.

Quello che vogliamo mostrare, e che implica la tesi, è la cosa seguente: se $\overrightarrow{Cay}(G,S)_{/H_i}$ è hamiltoniano, allora anche $\overrightarrow{Cay}(G,S)_{/H_{i-1}}$ è hamiltoniano: la tesi deriva dal fatto che per $i = n$ si ha già un ciclo hamiltoniano, poichè $\overrightarrow{Cay}(G,S)_{/H_n} = \overrightarrow{Cay}(G/H^G, S)$.

Ragioneremo per induzione sull'ordine di G. Supponiamo che $\overrightarrow{Cay}(G,S)_{/H_i}$ sia hamiltoniano. Scegliamo $g \in G$ tale che $H^{g^{-1}}H_{i-1} = H_i$, e scegliamo $H_i g$ come punto di partenza del ciclo hamiltoniano nell'ipotesi, sia esso $[t_1, \ldots, t_n]$. Mostriamo che vale l'uguaglianza $\langle (t_1 \cdots t_{n-1}S)^{g^{-1}}\rangle H_{i-1}/H_{i-1} = H_i/H_{i-1}$. Si ha, nel quoziente su H_{i-1}:

$$\langle (t_1 \cdots t_{n-1}S)^{g^{-1}}\rangle \equiv \langle (t_1 \ldots t_n)^{g^{-1}}, (t_n^{-1}S)^{g^{-1}}\rangle \equiv \langle (t_1 \ldots t_n)^{g^{-1}}, H^{g^{-1}}\rangle \supseteq H^{g^{-1}}, \quad (*)$$

e nello stesso tempo $H_i g t_1 \cdots t_n = H_i g$ per l'hamiltonianità, cioè $(t_1 \cdots t_n)^{g^{-1}} \in H_i$, e per $(*)$ e per $H^{g^{-1}} \subseteq H_i$ si ha quindi nel quoziente su H_{i-1}: $H_i \equiv H^{g^{-1}} \leq \langle (t_1 \cdots t_{n-1}S)^{g^{-1}}\rangle \leq H_i$, cioè $\langle (t_1 \cdots t_{n-1}S)^{g^{-1}} H_{i-1}\rangle / H_{i-1} = H_i/H_{i-1}$.

S è un insieme di generatori minimale, quindi $H \subsetneq G$, è dunque $H^G \subsetneq G$ e quindi anche $H_i \subsetneq G$. Possiamo applicare l'induzione al grafo $\overrightarrow{Cay}(H_i/H_{i-1}, (t_1 \cdots t_{n-1}S)^{g^{-1}})$: vi troviamo un ciclo hamiltoniano orientato di partenza H_{i-1} e archi $[t_1 \ldots t_{n-1}s_j]_{j=1}^m$. Siamo nelle ipotesi della Proposizione 1.5: troviamo allora un ciclo hamiltoniano orientato nel digrafo $\overrightarrow{Cay}(G,S)_{/H_{i-1}}$. □

Questo risultato, mostrato in maniera abbastanza tecnica, è molto importante, e ha svariate conseguenze anche nelle applicazioni. Si costruisce prima una serie subnormale come nella Proposizione 1.4, di modo da trovare un ciclo hamiltoniano orientato. Questo metodo sembra fornire abbastanza velocemente tale ciclo per ogni p-gruppo. L'esempio che segue mostra il metodo applicato a p-gruppi con classe di nilpotenza grande. La serie subnormale che emergerà dal metodo sarà molto particolare.

Esempio 1.4. Sia $G = C_p \wr C_p = \mathbb{Z}_p{}^p \rtimes \langle\sigma\rangle$ con $\sigma = (12\ldots p)$, e consideriamo $\overrightarrow{Cay}(G,S)$, dove $S = \{(1,0,\ldots,0), \sigma\}$. Costruiamo la serie subnormale come nel Teorema 1.1, e

mostriamo il metodo per costruire il ciclo hamiltoniano orientato. Alla fine, lo esibiremo esplicitamente per $p = 3$.

- $H = \langle S^{-1}S \rangle = \langle \sigma^{-1}(1, 0, \ldots, 0) \rangle$, sia $r = \sigma^{-1}(1, 0, \ldots, 0)$. E' $r^p = (1, 1, \ldots, 1)$, dunque $|H| = |r| = p^2$.

- Sia $K = \langle r, r^\sigma \rangle$, con $r^\sigma = \sigma^{-1}(0, 1, 0, \ldots, 0)$.. E' $H^G = \langle (\sigma^{-1}(1, 0, \ldots, 0))^g : g \in G \rangle \supseteq K$. Mostriamo che in realtà è $K = H^G$. Dentro a K vi è:

$$(r^\sigma)^{-1} r = (\sigma^{-1}(0, 1, 0, \ldots, 0))^{-1} \sigma^{-1}(1, 0, \ldots, 0) = (1, -1, 0, \ldots, 0),$$

e moltiplicando e coniugando si trovano anche i "traslati" di tale elemento. Vi è dunque in K il seguente sottogruppo di C_p^p:

$$\langle (1, -1, 0, \ldots, 0), (0, 1, -1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1, -1) \rangle,$$

spazio vettoriale di dimensione $p - 1$ su C_p e ordine quindi p^{p-1}. Ci sono anche elementi di altra forma in K, quindi $|K| \geq |\langle r, r^\sigma \rangle| \geq p^p$, ed essendo H^G sottogruppo proprio in G e $H^G \supseteq K$, le disuguaglianze di prima sono tutte uguaglianze, in particolare $H^G = K = \langle r, r^\sigma \rangle$. Poniamo $H_k = H^G$.

Ora, non è vero che H è normale in H^G: infatti, coniugando r per r^σ si ha:

$$r^{r^\sigma} = r^{\sigma^{-1}(0,1,0,\ldots,0)} = (1, -1, 0, \ldots, 0)\sigma^{-1}(0, 1, 0, \ldots, 0) =$$

$$= \sigma^{-1}(1, -1, 0, \ldots, 0)^\sigma (0, 1, 0, \ldots, 0) = \sigma^{-1}(-1, 1, 0, \ldots, 0, 1) \notin H,$$

poichè le potenze di r della forma $\sigma^{-1}a$ con $a \in C_p^p$ sono tutte del tipo $\sigma^{-1}(i + 1, i, \ldots, i)$, $i = 0, \ldots, p - 1$. Consideriamo però $H_{k-1} = \langle r, r^{a_1} \rangle$, dove $a_0 = \sigma$, $a_1 = r^{a_0} = r^\sigma$, cioè $r^{a_1} = \sigma^{-1}(-1, 1, 0, \ldots, 0, 1)$. In questo sottogruppo, troviamo:

$$r(r^{a_1})^{-1} = \sigma^{-1}(2, -1, 0, \ldots, 0, -1)\sigma = (-1, 2, -1, 0, \ldots, 0)$$

e quindi anche $(1, -2, 1, 0, \ldots, 0)$; ripetendo il procedimento, ci sono in H_{k-1} anche i seguenti elementi:

$$\sigma^{-1}(-1, 1, 0, \ldots, 1)(1, -2, 1, 0, \ldots, 0) = \sigma^{-1}(0, -1, 1, 0, \ldots, 0, 1),$$

$$\sigma^{-1}(1, 0, \ldots, 0)(0, 1, -1, 0, \ldots, -1)\sigma = (-1, 1, 1, -1, 0, \ldots, 0),$$

$$(1, -1, -1, 1, 0, \ldots, 0)(-1, 2, -1, 0, \ldots, 0) = (0, 1, -2, 1, 0, \ldots, 0),$$

quindi in H_{k-1} c'è il seguente sottospazio di C_p^p:

$$\langle (1,-2,1,0,\dots,0),(0,1,-2,1,\dots,0),\dots,(0,\dots,0,1,-2,1)\rangle$$

di dimensione $p-2$ su C_p, dunque $H_{k-1} \geq pp^{p-2} = p^{p-1}$, ed è $|H_{k-1}| = p^{p-1}$ poichè H è sottogruppo proprio in H_k e quindi H^{H_k} è sottogruppo proprio in H_k, ma H^{H_k} contiene r e r^{r^σ}, perciò contiene anche H_{k-1}, costretto ad essere proprio in H_k anch'esso. Per motivi d'ordine è dunque $H_{k-1} = \langle r, r^{a_1}\rangle = \langle r, S_1\rangle$, con $S_1 = \langle e_1 - 2e_2 + e_3, e_2 - 2e_3 + e_4, \dots, e_{p-2} - 2e_{p-1} + e_p\rangle$.

Induttivamente e nella stessa maniera, si può mostrare che troviamo una serie subnormale con sottogruppi:

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{k-1} \trianglelefteq H_k = H^G,$$

$$H_{k-i} = \langle r, r^{a_i}\rangle = \langle r, S_i\rangle, \quad a_0 = \sigma, a_{i+1} = r^{a_i},$$

cioè esplicitamente $a_i = \sigma^{-1}(1-i,1,0,\dots,0,(-1)^i\binom{i}{i},(-1)^{i-1}\binom{i}{i-1},\dots,\binom{i}{2})$, e:

$$S_i = \{\left(\binom{i+1}{0},-\binom{i+1}{1},\dots,(-1)^{i+1}\binom{i+1}{i+1},0,\dots,0\right),\dots,$$

$$\dots,\left(0,\dots,0,\binom{i+1}{0},-\binom{i+1}{1},\dots,(-1)^{i+1}\binom{i+1}{i+1}\right)\}.$$

Notiamo che se $p > 2$ è $a_{p-2} = \sigma^{-1}(3,1,0,-1,-2,\dots,3)$, e:

$$(\sigma^{-1}(1,0,\dots,0))^{a_{p-2}} = (-2,-1,0,1,2,\dots,-3)\,\sigma^{-1}a_{p-2} =$$

$$= \sigma^{-1}(-1,0,1,2,\dots,-3,-2)(3,1,\dots,3) =$$

$$= \sigma^{-1}(2,1,\dots,1) = r^{p+1} \in H,$$

dunque è $H_1 = \langle r, r^{a_{p-2}}\rangle = \langle r\rangle = H$, e $k = p-1$.

Abbiamo così trovato una serie subnormale di H^G di $p-1$ fattori, i primi $p-2$ (dall'alto) dei quali ciclici di ordine p e tali che $H_{k-i-1}H^{a_i} = H_{k-i}$, e l'ultimo ciclico di ordine p^2, che è H stesso.

Analizziamo in dettaglio la situazione quando $p = 3$. In questo caso, la serie è data da $1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 = H^G$, dove $H_1 = \langle \sigma^{-1}(1,0,0)\rangle$, $H_2 = \langle \sigma^{-1}(1,0,0), \sigma^{-1}(0,1,0)\rangle$.

- $G/H^G = \langle H^G\sigma/H^G\rangle$, dunque un ciclo Hamiltoniano orientato su quel quoziente è banalmente $[\sigma,\sigma,\sigma]$, di partenza arbitraria.

- Esaminiamo H^G/H_1. Vale: $H^\sigma H = H^G$. Facciamo partire il precedente ciclo da $H^G\sigma^{-1}$. Secondo le notazioni del Teorema 1.1, $t_1 = t_2 = \sigma$, e a generare $H^\sigma H_1/H_1$ è

l'insieme: $(\sigma^2 S)^\sigma = \sigma S \sigma = \{1, \sigma^{-1}(0,1,0)\}$. Il percorso $3 * [\sigma^{-1}(0,1,0)]$ è ciclo hamiltoniano orientato in $\overrightarrow{Cay}(H^G/H_1, \{\sigma^{-1}(0,1,0)\})$, cioè nelle notazioni della Proposizione 1.5 è $s_1 = s_2 = s_3 = (1,0,0)$. La regola dice quindi che in $\overrightarrow{Cay}(G,S)/_{H_1}$ trovo il ciclo hamiltoniano orientato di partenza $H_1\sigma^{-1}$ e archi $3 * [\sigma, \sigma, (1,0,0)]$.

- Ci rimane da vedere H_1/H_0. Ma esso è proprio H, coniugato tramite l'identità. Bisogna far partire il circuito prima trovato da 1, dunque traslarlo in avanti di un passo, per ottenere il ciclo di partenza H_1 e archi:

$$[\sigma, (1,0,0), 2 * [\sigma, \sigma, (1,0,0)], \sigma].$$

Il prodotto $t_1 \dots t_8$ come nel Teorema 1.1 è questa volta:

$$\sigma(1,0,0)\sigma^2(1,0,0)\sigma^2(1,0,0) = (1,0,0)^{\sigma^{-1}}(1,0,0)(1,0,0)^\sigma\sigma^{-1} = (1,1,1)\sigma^{-1} = \sigma^{-1}(1,1,1).$$

Calcolando $\sigma^{-1}(1,1,1)S$ si hanno gli elementi $(1,1,1)$ e $\sigma^{-1}(2,1,1) = r^4$, che genera H poichè $\langle r \rangle = H$ e $(4,9) = 1$. Nelle notazioni della Proposizione 1.5, è $s_1 = \dots = s_9 = (1,0,0)$, e otteniamo infine il seguente ciclo hamiltoniano orientato su tutto G, di partenza 1:

$$9 * [\sigma, (1,0,0), 2 * [\sigma, \sigma, (1,0,0)], (1,0,0)].$$

4. I gruppi diedrali: il primo caso incompleto

La classe dei gruppi diedrali $D_{2n} = \langle r, s : r^n = s^2 = 1, r^s = r^{-1} \}$ presenta il primo caso in cui non è stata dimostrata l'hamiltonianità al variare di S minimale che genera D_{2n}. Mostriamo che, in realtà, con il lavoro che verrà svolto in questo paragrafo ci si ricondurrà a dover risolvere tale problema sotto due condizioni strette su S ed n soddisfatte allo stesso tempo, cioè:

- n sia dispari;
- S contenga più di 3 involuzioni.

Iniziamo con un'osservazione. Un gruppo G è diedrale se e solo se è generato da due involuzioni. Se è $G = D_{2n}$, nelle notazioni di prima è $G = \langle s, sr \rangle$, e vale $(sr)^2 = srsr = r^s r = r^{-1}r = 1$. Viceversa, sia G un gruppo generato da due involuzioni, $G = \langle b, c \rangle$. Poniamo $|bc| = n$. Se accade che $\langle b \rangle \cap \langle bc \rangle \neq 1$, allora b appartiene al gruppo abeliano $\langle bc \rangle$, quindi b e bc commutano, dunque lo fanno

anche b e c, e in questo caso il gruppo è $C_2 \times C_2$. Negli altri casi, è $\langle b\rangle \cap \langle bc\rangle = 1$, e $(bc)^b = cb = (bc)^{-1}$, dunque il gruppo G è D_{2n} per definizione.

Mostriamo che per determinare cicli hamiltoniani dobbiamo lavorare, in sostanza, solo sulle involuzioni di S.

Proposizione 1.6. *Sia $D_{2n} = \langle R \cup I\rangle$, $n \geq 2$, con $R \subseteq \langle r\rangle$, $I \subseteq D_{2n} \setminus \langle r\rangle$. Se $Cay(\langle I\rangle, I)$ è hamiltoniano, allora anche $Cay(D_{2n}, R \cup I)$ è hamiltoniano.*

Dim. Sia $|\langle I\rangle| = m$, e sia $[s_1, \dots s_m]$ il ciclo hamiltoniano in $Cay(\langle I\rangle, I)$. Poichè $n \geq 2$, è $I \neq \emptyset$, quindi m è ben definito. Inoltre, m è pari poichè $\langle I\rangle$ contiene involuzioni. Prendiamo un cammino hamiltoniano in $Cay(\langle R\rangle/\langle R\rangle \cap \langle I\rangle, \bar{R})$, sia esso $[\bar{r}_1, \dots, \bar{r}_{k-1}]$. E' $k = \frac{2n}{m}$; infatti, $\langle R\rangle$ è caratteristico in $\langle r\rangle$, dunque normale in D_{2n}, e si ha:

$$G = \langle R \cup I\rangle = \langle R\rangle\langle I\rangle \Longrightarrow 2n = |G| = \frac{|\langle R\rangle||\langle I\rangle|}{|\langle R\rangle \cap \langle I\rangle|} = m\left|\frac{\langle R\rangle}{\langle R\rangle \cap \langle I\rangle}\right|.$$

Mostriamo che $[r_1, \dots, r_{k-1}, s_i]_{i=1}^m$ è un ciclo hamiltoniano su D_{2n}. I primi $2k$ elementi vertici del ciclo sono distinti, poichè lo sono i primi k e i secondi k, ed essi appartengono a due classi laterali distinte di $\langle R\rangle$. Si nota poi che:

$$(\prod_{i=1}^{k-1} r_i)s_j(\prod_{i=1}^{k-1} r_i)s_{j+1} = s_j(\prod_{i=1}^{k-1} r_i)^{s_j}(\prod_{i=1}^{k-1} r_i)s_{j+1} = s_j(\prod_{i=1}^{k-1} r_i)^{-1}(\prod_{i=1}^{k-1} r_i)s_{j+1} = s_j s_{j+1}. \quad (*)$$

Facciamo ora vedere che tutti gli elementi del percorso $[r_1, \dots, r_{k-1}, s_i]_{i=1}^m$ sono distinti. Se denotiamo $\rho = \prod_{i=1}^{k-1} r_i$, consideriamo due generici vertici di tale percorso:

$$x = \rho s_1 \cdots \rho s_t r_1 \cdots r_a, \quad y = \rho s_1 \cdots \rho s_u r_1 \cdots r_b,$$

dove $0 \leq t, u \leq m-1$, $0 \leq a, b \leq k-1$. Con tale posizione, sottintendiamo che possono eventualmente mancare gli s_i, dunque x e y possono valere anche $1, r_1, \dots, r_{k-2}, \rho$. Supponiamo che sia $x = y$. Bisogna che x e y stiano almeno nella stessa classe laterale di $\langle r\rangle$, dunque deve essere $t \equiv u \mod 2$. Distinguiamo dunque due casi:

- siano t e u pari. Per $(*)$, si ha che $x = y$ si riscrive $s_1 \cdots s_t r_1 \cdots r_a = s_1 \cdots s_u r_1 \cdots r_b$;
- siano t e u dispari. Sempre per $(*)$, l'uguaglianza $x = y$ diventa:

$$s_1 \cdots s_{t-1} \rho s_t r_1 \dots r_a = s_1 \cdots s_{u-1} \rho s_u r_1 \cdots r_b,$$

ma $s_1 \cdots s_{t-1}, s_1 \cdots s_{u-1}$ appartengono a r per disparità di t e u, tali prodotti commutano quindi con ρ, e anche in questo caso $x = y$ si può riscrivere nella maniera equivalente $s_1 \cdots s_t r_1 \cdots r_a = s_1 \cdots s_u r_1 \cdots r_b$.

In ogni caso, $x = y$ equivale a $s_1 \cdots s_t r_1 \cdots r_a = s_1 \cdots s_u r_1 \cdots r_b$. Supponiamo che valga $a \neq b$, ovvero senza perdita di generalità $a > b$. Allora la precedente uguaglianza si riscrive: $(s_1 \cdots s_u)^{-1}(s_1 \cdots s_t) = r_{a+1} \cdots r_b$. Dunque $r_{a+1} \cdots r_b$, ma $[\bar{r}_1, \ldots \bar{r}_{k-1}]$ è ciclo su $\langle R \rangle / \langle R \rangle \cap \langle I \rangle$, dunque $r_{a+1} \cdots r_b = 1$, assurdo perchè $a, b \leq k-1$. Segue che $a = b$, ed essendo $t, u \leq m-1$ dall'uguaglianza di partenza si trova $t = u$. Tutte queste informazioni, assieme al fatto che:

$$(\prod_{i=1}^{k-1} r_i) s_1 \ldots (\prod_{i=1}^{k-1} r_i) s_m = s_1 \ldots s_m = 1,$$

ci consentono di concludere che $[r_1, \ldots, r_{k-1}, s_i]_{i=1}^{m}$ è un percorso chiuso che transita per ogni vertice di D_{2n} esattamente una volta. Tale percorso è quindi un ciclo hamiltoniano. □

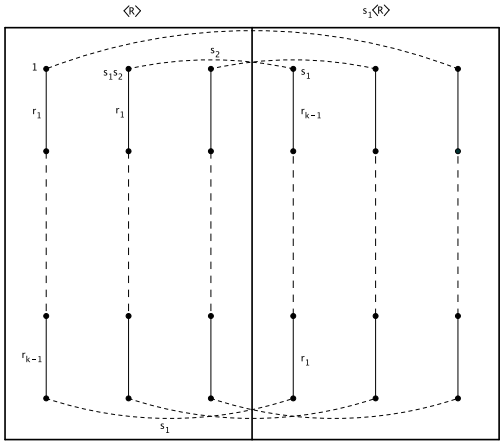

Figura 1.7. Il ciclo hamiltoniano in $Cay(D_{2n}, S)$, $S = R \cup I$, quando $r \in R$.

Poichè si trova sempre un ciclo hamiltoniano in un grafo di un gruppo generato da due involuzioni, a sua volta diedrale, abbiamo che se D_{2n} è generato da S, con S che possiede al massimo 2 involuzioni, allora, $Cay(D_{2n}, S)$ è hamiltoniano.

Ci mettiamo quindi nel caso in cui l'insieme S che genera D_{2n} contiene da tre involuzioni in su, le quali a due a due non generano D_{2n}. Mostriamo il seguente fatto, utile a capire quando ciò accade. Se $m_1, \ldots, m_k \in \mathbb{Z}$, denotiamo con $(m_1, \ldots, m_k)$ il più grande intero positivo che divide tutti gli interi $m_1, \ldots, m_k$.

Proposizione 1.7. *Siano $r, s \in D_{2n}$. Allora, $S = \{s, sr^{a_1}, \ldots, sr^{a_k}\}$ genera D_{2n} se e solo se $(a_1, \ldots, a_k, n) = 1$.*

Dim. Sia $(a_1, \ldots, a_k, n) = 1$. Esistono così $h_1, \ldots, h_k, l$ interi, con $a_1h_1 + \cdots + a_kh_k + nl = 1$. Dunque, $r^{a_1h_1+\cdots+a_kh_k+nl} = r$, cioè essendo $r^n = 1$ è $(r^{a_1})^{h_1} \ldots (r^{a_k})^{h_k} = r$, e chiaramente $r^{a_1}, \ldots, r^{a_k} \in \langle S \rangle$.

Viceversa, sia $(a_1, \ldots, a_k) = d$ e $(d, n) \neq 1$. In questo caso, è $S \subseteq \{s, sr^d\}$, e vale $\langle s, sr^d \rangle = D_{2\frac{n}{(d,n)}} \subsetneq D_{2n}$. □

Nel caso di tre involuzioni nell'insieme S che genera D_{2n}, possiamo supporre $S = \{s, sr^a, sr^b\}$, con $(a, b, n) = 1$. L'idea, in questo caso, è la seguente. Si ha:

$$s(sr^a)(sr^b)s(sr^a)(sr^b) = r^a(r^{b+a})^s r^b = r^a r^{-b-a} r^b = 1,$$

dunque partendo da un vertice e moltiplicando ordinatamente s, sr^a, sr^b due volte, ottieniamo un ciclo con 6 vertici, che è un "mattone" nel grafo in Figura 1.8. Un sottografo di $Cay(D_{2n}, \{s, sr^a, sr^b\})$ fa quindi parte dei grafi "brick product" esaminati in [**2**], per i quali si prova, in maniera analoga al caso particolare in Figura 1.8, il seguente risultato generale.

Proposizione 1.8. *Ogni grafo di Cayley cubico su un gruppo diedrale è hamiltoniano.*

Possiamo riassumere quanto detto finora nella seguente:

Proposizione 1.9. *Sia $\langle S \rangle = D_{2n}$, con S che contiene al massimo 3 involuzioni. Allora, $Cay(D_{2n}, S)$ è hamiltoniano.*

Recentemente, diversi autori si sono concentrati sulla classificazione completa dei grafi di Cayley su gruppi di piccolo ordine: un recente articolo mostra l'hamiltonianità dei grafi di Cayley su gruppi di ordine minore o uguale a 100. La seguente proposizione

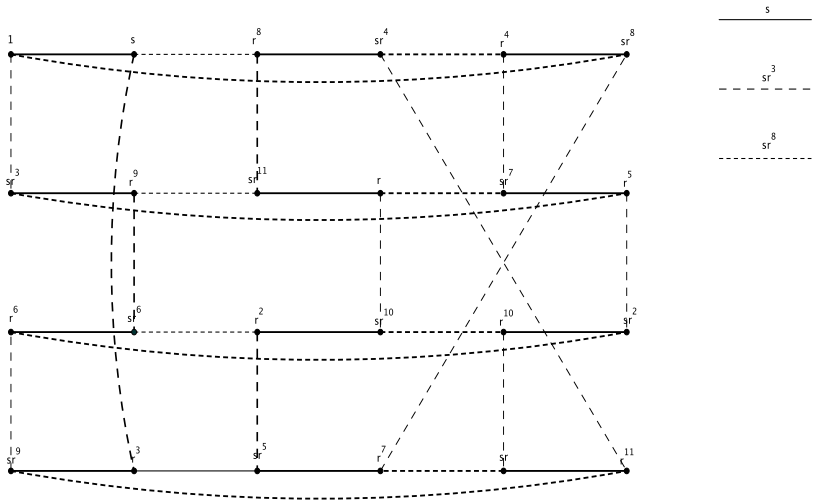

Figura 1.8. Il grafo di Cayley e il ciclo hamiltoniano in $Cay(D_{24}, \{s, sr^3, sr^8\})$.

implicherà l'hamiltonianità per grafi su gruppi diedrali i cui ordini coinvolgono pochi primi.

Proposizione 1.10. *Sia n divisibile da al massimo 3 primi distinti. Allora, nessun insieme di generatori di D_{2n} del tipo $S = \{s, sr^a, sr^b, sr^c\}$, con $(a, b, c, n) = 1$, è minimale.*

Dim. Se uno fra $(a, b, n), (b, c, n), (a, c, n)$ è 1, allora per la Proposizione 1.7 S non è minimale. Supponiamo allora che essi siano tutti diversi da 1. Mostriamo che in tal caso è necessariamente $s \in \{sr^a, sr^b, sr^c\}$.

Le classi di coniugio di $sr^i, i \in \mathbb{N}$, sono: $\{sr^i : i \in \mathbb{N}\}$ se n è dispari, e $\{sr^{2i} : i \in \mathbb{N}\}$, $\{sr^{2i+1} : i \in \mathbb{N}\}$ se n è pari. Possiamo supporre in ogni caso che esista uno fra sr^a, sr^b, sr^c, per esempio sr^a, tale che esiste r^k potenza di r, con $(sr^a)^{r^k} = s$, ovvero $sr^{a+2k} = s$ e $a + 2k \equiv 0 \mod n$. Infatti, nel caso in cui n sia dispari, o in quello in cui n sia pari e nello stesso tempo uno fra a, b, c sia pari, allora questo è vero per come sono fatte le classi di coniugio. In caso contrario, n è diviso da 2, p, e q con p e q dispari. Dalle ipotesi, a, b, c, tutti dispari, devono essere divisi ciascuno da almeno uno fra p e q, e ciascuno fra p e q deve

dividere esattamente due fra a, b, c, ma allora esiste una coppia di elementi fra a, b, c, siano a e b, che non ha divisori p e q in comune, sarebbero dunque coprimi, il che è un assurdo.

$\langle sr^a, sr^b, sr^c\rangle = H$ se e solo se $\langle sr^a, sr^b, sr^c\rangle^{r^k} = \langle s, sr^{b-a}, sr^{c-a}\rangle = H^{r^k}$; per concludere, dobbiamo dire che $H^{r^k} = D_{2n}$, cioè $(b-a, c-a, n) = 1$. Tutte le ipotesi su a, b, c, n ci dicono che se è $n = p^\alpha q^\beta r^\gamma$ allora, senza perdita di generalità, p è l'unico primo divisore di (a, b, n), q l'unico di (a, c, n), r è l'unico di (b, c, n). Dunque $q \nmid b-a$, $r \nmid c-a$, $p \nmid c-a$, e quindi $(b-a, c-a, n) = 1$, come volevamo. □

Nel caso in cui la fattorizzazione di n coinvolga pochi primi, basta esaminare solo la situazione in cui le involuzioni sono al massimo 3. La Proposizione 1.9 ci permette di concludere questo.

Proposizione 1.11. *Se n è diviso al massimo da tre primi distinti, allora $Cay(D_{2n}, S)$ è hamiltoniano per ogni S insieme di generatori.*

In particolare, la questione è risolta per tutti i grafi sui gruppi diedrali di ordine inferiore a 420, e in tal caso si riesce ad esplicitare il ciclo hamiltoniano lavorando sulle involuzioni dell'insieme di generatori. Rimane però aperta la seguente congettura, se fosse vera la quale il problema dell'hamiltonianità nei diedrali sarebbe risolto.

Congettura. *Mostrare che se I è un qualsiasi insieme di involuzioni che genera D_{2n}, allora $Cay(D_{2n}, I)$ è hamiltoniano.*

C'è stato però un passo significativo di recente. La dimostrazione del teorema che segue è contenuta in [**1**].

Teorema 1.2. *Ogni grafo di Cayley di valenza almeno 3 su un gruppo diedrale D_{2n}, con n pari, è tale che:*

- se tale grafo non è bipartito, allora per ogni g, g' in D_{2n} esiste un cammino hamiltoniano che parte da g e arriva a g';

- se tale grafo è bipartito in due insiemi S e S', allora per ogni $g \in S, g' \in S'$, esiste un cammino hamiltoniano che parte da g e arriva a g'.

La dimostrazione è fatta di diversi sottocasi e risultati intermedi, e la omettiamo. Il risultato sopra implica l'hamiltonianità degli stessi grafi nelle ipotesi del precedente Teorema, dunque abbiamo che:

Corollario 1.1. *Sia n pari. Allora, $Cay(D_{2n}, S)$ è hamiltoniano per ogni insieme di generatori S per D_{2n}.*

Un'altra direzione da poter intraprendere per risolvere il problema, riconducendolo a risolvere completamente la questione dell'hamiltonianità per digrafi di gruppi ciclici (vedi Paragrafo 6), è data dal seguente risultato, la cui dimostrazione è in [**5**].

Proposizione 1.12. *Se $\overrightarrow{Cay}(\mathbb{Z}_n, S)$ è hamiltoniano ogniqualvolta S è un insieme di generatori minimale con almeno 3 elementi, allora ogni digrafo di Cayley su D_{2n} è hamiltoniano.*

La determinazione di un ciclo hamiltoniano è un problema molto più difficile di quella di un cammino hamiltoniano. A chiusura di paragrafo, mostriamo un risultato che risolve completamente la faccenda per i cammini hamiltoniani per i digrafi sui gruppi diedrali.

Proposizione 1.13. *Sia G un gruppo che ammetta un sottogruppo normale N di indice 2, con la proprietà che ogni sottogruppo di N è normale in G. Allora, ogni digrafo $\overrightarrow{Cay}(G, S)$ possiede un cammino hamiltoniano orientato.*

Dim. Sia S insieme di generatori minimale per G. Si ragiona per induzione su $n = |G|$, trovando un cammino $(1, g_1, \ldots, g_{n-1})$, tale che $g_{n-1} \notin N$.

Sia $g \in S \setminus N$, e siano $H = \langle S \setminus \{g\} \rangle$, $m = |H| < |G|$. Il caso $H \leq N$ è semplice: avremmo per ipotesi $H \trianglelefteq G$, ed ogni sottogruppo di H è normale nell'intero G per ipotesi, dunque in H stesso. Sia in H, gruppo abeliano o hamiltoniano per ipotesi, sia in G/H, ciclico, si trovano quindi, grazie alla Proposizione 1.3, due cammini hamiltoniani orientati. Per il Lemma 1.3, dunque,troviamo un cammino hamiltoniano orientato in $\overrightarrow{Cay}(G, S)$.

Supponiamo dunque $H \not\leq N$. Si osservi che H soddisfa le ipotesi di questa proposizione. Infatti, $H \cap N$ è un sottogruppo normale di indice 2 in H, tale che ogni suo sottogruppo K, essendo normale in N, è normale anche in G, dunque $K \trianglelefteq H$. Per induzione sull'ordine

di G troviamo quindi un cammino hamiltoniano in $\overrightarrow{Cay}(H, S \setminus \{g\})$, sia esso $[a_1, \ldots, a_{m-1}]$, con $h = a_1 \ldots a_{m-1} \notin H \cap N$, quindi $h \notin N$. Da $hN \neq N$ e $gN \neq N$ si ha $hgN = N$ poichè $[G : N] = 2$, dunque $hg \in N$. Se mostriamo che $(hg)^i \notin H, i = 1, \ldots, \frac{n}{m} - 1$, si può concludere che si ha il seguente cammino hamiltoniano:

$$[[a_1, \ldots, a_{m-1}, g]_{i=1}^{\frac{n}{m}-1}, [a_1, \ldots, a_{m-1}]], \quad (*)$$

poichè in tal caso gli $(hg)^i$ si trovano in classi laterali distinte di H.

Mostriamo che $N = \langle H \cap N, hg \rangle$. Poichè $hg \in N$ è $G = \langle H, g \rangle = \langle H \cap N, h, g \rangle$. Poniamo $\tilde{N} = \langle H \cap N, hg, g^2 \rangle \leq N$. E' $\tilde{N} \trianglelefteq G$. Essendo poi $G = \langle \tilde{N}, g \rangle = \tilde{N}\langle g \rangle$, con $g^2 \in \tilde{N}$, è $[G : \tilde{N}] = 2$, ma da $\tilde{N} \leq N$ segue $\tilde{N} = N$, cioè $N = \langle H \cap N, hg, g^2 \rangle$. Essendo $\langle hg \rangle \leq N$ è per ipotesi $\langle hg \rangle \trianglelefteq G$, dunque $g \in \langle hg \rangle h^{-1}$ e $g^2 \in \langle hg \rangle h^{-2}$, ma $h^2 \in H \cap N$, così si può rimuovere g^2 fra i generatori di N, ed è $N = \langle H \cap N, hg \rangle$.

Se esistesse $1 \leq i \leq \frac{n}{m} - 1$ tale che $(hg)^i \in H$, allora:

$$N = (H \cap N)\langle hg \rangle \Longrightarrow i < \frac{n}{m} = [G : H] = [N : H \cap N] = [\langle hg \rangle : \langle hg \rangle \cap (H \cap N)] = i,$$

assurdo. Deve essere $i = \frac{n}{m}$, e il percorso in $(*)$ è un cammino hamiltoniano. □

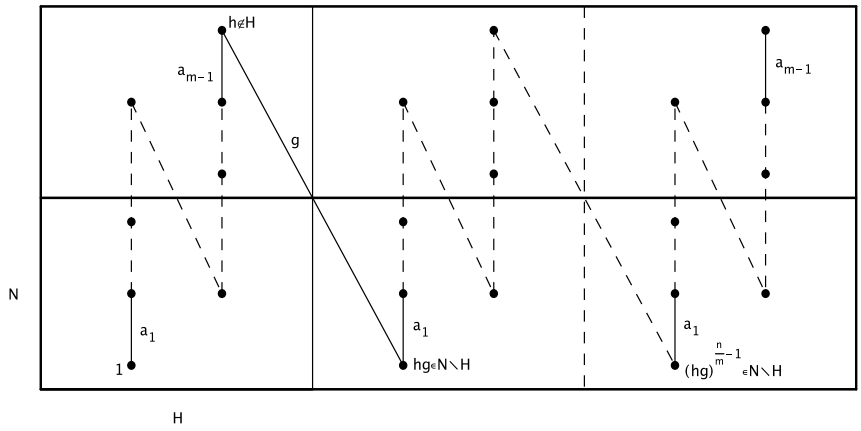

Figura 1.9. Il cammino hamiltoniano come nel secondo caso della Proposizione 1.13.

Questa è proprio la situazione dei gruppi diedrali: $\langle r \rangle \trianglelefteq D_{2n}$, e ogni sottogruppo di $\langle r \rangle$ è in esso caratteristico, dunque normale in D_{2n}. Siamo nelle ipotesi della Proposizione 1.13, e si può concludere:

Proposizione 1.14. *Sia $\langle S \rangle = D_{2n}$. Allora, ogni digrafo $\overrightarrow{Cay}(D_{2n}, S)$ possiede cammino hamiltoniano orientato.*

Diciamo infine che molti di questi risultati si generalizzano a gruppi "di tipo diedrale", in cui si richiede che il gruppo su cui agisce C_2 non sia necessariamente ciclico, ma abeliano. Si veda la survey [**6**].

5. Condizioni indipendenti da S per l'hamiltonianità di $Cay(G, S)$

Sono state trovate altre condizioni su un gruppo G, oltre a quelle esaminate finora, perchè $Cay(G, S)$ sia hamiltoniano indipendentemente dall'insieme S di generatori. Una di queste è una condizione sul suo sottogruppo derivato G'.

Teorema 1.3. *Sia G tale che $G' \cong C_p$. Allora, per ogni S con $\langle S \rangle = G$, $Cay(G, S)$ è Hamiltoniano.*

La dimostrazione di questo risultato è in [**15**]. Essa è divisa in molti casi, a seconda del comportamento degli elementi di S, per esempio se contiene elementi centrali, e a seconda che G sia nilpotente o meno. Tutti i casi, eccetto uno, si mostrano grazie al Lemma 1.1: si trova un ciclo $[a_1, \ldots, a_m]$ sul quoziente su G/G', tale che $\langle a_1 \cdots a_m \rangle = G'$, oppure si trovano due diversi cicli $[b_1, \ldots, b_m]$ e $[c_1, \ldots, c_m]$, con $b_1 \cdots b_m \neq c_1 \cdots c_m$, dunque uno dei due prodotti genera $G' \cong C_p$.

Mostriamo, per brevità, come si procede nel caso eccezionale del teorema, di un certo interesse: G non nilpotente, S ha qualche elemento nel derivato.

Proposizione 1.15. *Sia S insieme minimale di generatori per G, con G non nilpotente, tale che $G' \cong C_p$, $S \cap G' \neq \emptyset$. Allora, $Cay(G, S)$ è hamiltoniano.*

Dim. Sia $s \in S \cap G'$. S è insieme minimale di generatori, dunque $s \neq 1$, in particolare $\langle s \rangle = G'$. Sia H il gruppo abeliano G/G', con $|H| = m$, nel cui grafo di Cayley $Cay(H, \bar{S})$

troviamo un ciclo $[x_1G', \dots, x_mG']$. H agisce su G' per coniugio[3]. Se mostriamo che vale:

$$s^{x_1+x_1x_2+\cdots+x_1x_2\cdots x_m} = 1,$$

riusciamo a concludere che $Cay(G,S)$ è hamiltoniano. Infatti, si hanno due possibilità per $x_1\cdots x_m$: $|x_1\cdots x_m| = p$ oppure $x_1\cdots x_m = 1$. Nel primo caso si conclude per il Lemma 1.1. Se $x_1\cdots x_m = 1$, consideriamo il seguente percorso:

$$[x_1, (p-1)*s^{-1}, x_2, (p-1)*s^{-1}, \dots, x_m, (p-1)*s^{-1}].$$

I vertici di questo percorso, a parte l'ultimo, sono tutti distinti fra loro, poichè, presi p alla volta, descrivono le m classi laterali di G', e il prodotto di tutti questi elementi vale:

$$x_1s\cdots x_ms = s^{-x_1}x_1x_2sx_3s\cdots x_ms = \cdots = s^{-x_1-x_1x_2-\cdots-x_1\cdots x_m}x_1\cdots x_m = 1,$$

e dunque il percorso è proprio un ciclo hamiltoniano.

Dobbiamo mostrare che $s^{x_1+x_1x_2+\cdots+x_1\dots x_m} = 1$. Siccome $x_1, x_1x_2, \dots, x_1\dots x_m$ sono elementi distinti di H essendo $[x_1, \dots, x_m]$ hamiltoniano in H, la tesi equivale a mostrare che $s^{\sum_{h\in H} h} = 1$.

Abbiamo il morfismo $H \to Aut(\langle s\rangle)$ che manda h nell'automorfismo $s \mapsto s^h$, di nucleo $C_H(s)$. Così $H/C_H(s) \leq Aut(\langle s\rangle) \cong C_{p-1}$, dunque $H/C_H(s) = \langle\gamma\rangle$, con $s^\gamma = s^r$, $r \in \{1, \dots, p-1\}$. Si ha che $H \neq C_H(s)$: se così non fosse, allora commutando s con $\langle s\rangle$ e H, sarebbe $\langle s\rangle \subseteq Z(G)$, e $G/\langle s\rangle = G/G'$ è abeliano, in particolare nilpotente, seguirebbe che G stesso è nilpotente, proibito dall'ipotesi.

Deve quindi essere $s^r \neq s$. Se $[H : C_H(s)] = a = |\gamma|$, allora $s^{\gamma^a} = s = s^{r^a}$, cioè $s^{r^a-1} = 1$. Infine, se $b = |C_H(s)|$, si ha:

$$s^{\sum_{h\in H} h} = s^{\sum_{i=0}^{a-1} b\gamma^i} = s^{b(1+r+\cdots+r^{a-1})} = s^{b\frac{r^a-1}{r-1}} = 1,$$

come volevamo. □

Vediamo che con il Teorema 1.3, e con delle considerazioni sul sottogruppo di Frattini di G, si può considerare $G' \cong C_q$ con q *potenza* di un primo p. Ricordiamo le seguenti proprietà.

Proposizione 1.16. *Sia G gruppo finito. Allora:*

[3]Fra gli elementi di H useremo notazione additiva.

i) $Frat(G)$ *consiste degli elementi di* G *che non appartengono ad alcun insieme minimale di generatori di* G*.*

ii) Sia $S \subseteq G$*, tale che* $\bar{S}$ *genera* $G/Frat(G)$*. Allora,* S *genera* G*.*

Il Teorema 1.3 si può estendere come segue.

Teorema 1.4. *Sia* G *gruppo finito, tale che* G' *è gruppo ciclico di ordine una potenza di un primo. Allora,* $Cay(G, S)$ *è hamiltoniano per ogni* S *insieme di generatori per* G*.*

Dim. Poniamo $N = G'$. Se N è ciclico di ordine primo questo risultato è il Teorema 1.3. Sia quindi $N \cong C_{p^n}$, e siano $\bar{G} = G/Frat(N)$, $\bar{N} = N/Frat(N)$. N ha un unico sottogruppo massimale isomorfo a $C_{p^{n-1}}$, dunque $Frat(N) \cong C_{p^{n-1}}$ ed è $\bar{N} \cong C_p$. Come nel caso di $|N|$ primo, troviamo un ciclo hamiltoniano $[\bar{t_1}\bar{N}, \ldots, \bar{t_s}\bar{N}]$ nel grafo di Cayley di $\bar{G}/\bar{N}$, tale che $\bar{t_1} \cdots \bar{t_s}$ genera $\bar{N}$. Per la Proposizione 1.16, si ha che $\langle t_1 \cdots t_s \rangle = N$, e si conclude ancora una volta col Lemma 1.1. □

Grazie a questo risultato e ad altre considerazioni, si può provare il seguente risultato, presente in [**14**].

Teorema 1.5. *Ogni grafo di Cayley su gruppi di ordine* pq*,* $4q$*,* p^2q *con* $2 < p < q$*,* $2p^2$*,* $2pq$*,* $8p$*,* $4p^2$ *è hamiltoniano.*

La dimostrazione di questo risultato si basa sull'analisi dei sottogruppi di Sylow dei gruppi nell'enunciato del teorema. Si escludono i casi con commutatore ciclico, discutendo i rimanenti: si ricade sempre in casi conosciuti, come gruppi diedrali, o loro generalizzazioni[4]. A titolo di esempio, mostriamo come si procede in uno di questi casi.

Esempio 1.5. Mostriamo che se $|G| = 2pq, 2 < p < q$, allora $Cay(G, S)$ è hamiltoniano per ogni S insieme di generatori. Un gruppo di tale ordine è sempre risolubile, si trova quindi un pq-Hall N, di indice 2 in G, ed è $N = PQ$, $|P| = p$, $|Q| = q$, e $N \trianglelefteq G$. Poichè $p < q$, l'unico divisore di p congruo a 1 modulo q è 1, e Q è l'unico, quindi caratteristico, q-Sylow in

[4]Molti dei risultati dello scorso paragrafo valgono anche per gruppi diedrali generalizzati.

$N \trianglelefteq G$, dunque $Q \trianglelefteq G$. Si ha $|G/Q| = 2p$, ed essendo $|Q| = q \nmid 2p$ esiste un complemento $H \leq G$, tale che $G = Q \rtimes H$.

Se G/Q è abeliano, allora $G' \subseteq Q$, e si applica il Teorema 1.4. Sia allora $H \cong G/Q$ non abeliano. Un gruppo di ordine $2p$ è ciclico o diedrale. In quest'ultimo caso si ha $G = Q \rtimes D_{2p} \cong C_q \rtimes D_{2p}$. Vediamo come agisce D_{2p} su Q. $Aut(Q) = C_{q-1}$, ciclico, dunque $G' \subseteq C_G(Q)$, in particolare $C_p = D'_{2p} \subseteq C_G(Q)$, un pezzo dell'azione è banale e si ha $G \cong (C_p \times C_q) \rtimes C_2 = C_{pq} \rtimes C_2$. E in questo caso, $G' = C_{pq}$ se e solo se C_2 non centralizza nè C_p nè C_q, ovvero $G = D_{2pq}$, diedrale con fattorizzazione piccola, e si conclude per la Proposizione 1.11.

Un lavoro molto più generale e diviso in numerosi sottocasi, ma portato a termine essenzialmente con le stesse tecniche usate finora, è il seguente risultato recente, apparso nel 2011, in [**16**].

Proposizione 1.17. *Siano p, q, r primi distinti, e sia G gruppo di ordine n, con n che può valere:*

$$kp, k < 32 \wedge k \neq 24, \quad kpq, k \leq 5, \quad kp^2, k \leq 4, \quad kp^3, k \leq 2, \quad pqr,$$

dove k è un intero positivo. Allora, $Cay(G, S)$ è hamiltoniano per ogni insieme S di generatori per G.

Ancora più di recente, in [**20**], sono state indebolite delle ipotesi nel Teorema 1.4.

Proposizione 1.18. *a) Sia G di ordine dispari, tale che $|G'| \cong C_{p^a q^b}$. Allora, $Cay(G, S)$ è Hamiltoniano per ogni S insieme di generatori per G.*

b) Sia G di ordine dispari, tale che $|G'| = pq$. Allora, $Cay(G, S)$ è hamiltoniano per ogni S insieme di generatori per G.

6. Differenze sostanziali tra grafi e digrafi

Nei precedenti paragrafi ci siamo concentrati prevalentemente sui grafi di Cayley, parlando di digrafi solo quando il risultato si poteva estendere al caso orientato. La situazione in cui è coinvolta l'orientazione è comunque di interesse, e vale la pena

mostrare i fatti principali per i grafi orientati ed evidenziare le differenze con il caso non orientato.

Sebbene per i digrafi sui p-gruppi valga sempre l'hamiltonianità, come mostrato nella Sezione 3, nel caso orientato il gruppo C_6 con generatori 2 e 3 mostra un esempio di digrafo non hamiltoniano su un gruppo ciclico, mentre i grafi sui gruppi abeliani sono sempre hamiltoniani.

Si possono dare delle condizioni necessarie e sufficienti per l'hamiltonianità di un digrafo su un gruppo ciclico? La risposta è sì se l'insieme S di generatori ha cardinalità 2.

Proposizione 1.19. *Siano $S = \{a, b\}$ con $\langle S\rangle = \mathbb{Z}_n$, $m = (n, a-b)$ e sia $r \in \mathbb{Z}$ tale che*

$$(a-b)r \equiv bm \mod n.$$

Allora, $\overrightarrow{Cay}(\mathbb{Z}_n, S)$ ha un ciclo hamiltoniano se e solo se esiste $k \in \mathbb{Z}$, con $r \leq k \leq m + r$, tale che $(k, \frac{n}{m}) = 1$.

La dimostrazione di questo fatto è contenuta in [**17**]. Il risultato che segue, condizione sufficiente per l'hamiltonianità di un digrafo su un gruppo abeliano, è invece conseguenza del Lemma 1.1.

Proposizione 1.20. *Siano G un gruppo abeliano, $\langle S\rangle = G$, con $S = \{s_1, \ldots, s_r\}$, H un sottogruppo ciclico di G tale che $H = \langle s_2 - s_1, \ldots s_r - s_1\rangle$, $m = [G : H]$. Se esistono interi non negativi $n_1, \ldots, n_r$, tali che $\sum_{i=i}^{r} n_i = m$, e $\sum_{i=1}^{r} n_i s_i$ genera H, allora:*

$$|H| * [[n_i * s_i]_{i=1}^{r}]$$

è un ciclo hamiltoniano orientato in $\overrightarrow{Cay}(G, S)$.

Non si può sempre trovare un ciclo hamiltoniano orientato nei digrafi. È stato mostrato che di cammini orientati, nei casi abeliani, se ne trovano sempre. Mostriamo che si riescono a trovare esempi di digrafi senza nemmeno cammino hamiltoniano orientato. Una condizione per questa eventualità è quella che segue.

Proposizione 1.21. *Sia* $\overrightarrow{Cay}(G, \{a, b\})$, *dove* $|a| = 2, |b| = 3$, *e si abbia* $|ab^{-1}| < \frac{|G|}{9}$. *Allora, tale digrafo non possiede cammino hamiltoniano.*

Dim. Sia $|G| = m$. Indichiamo con $[u_1, \ldots, u_c]$ una sequenza di archi. Supponiamo allora che un cammino hamiltoniano esista; nella scrittura di prima, $c = m - 1$, e $u_i \in \{a, b\} \forall i$. Non si possono avere due a consecutive, e nemmeno tre b consecutive, altrimenti abbiamo una collisione. Quello che vogliamo mostrare è che non possono esserci molte sequenze del tipo $[\ldots, a, b, a, \ldots]$. Supponiamo che ce ne sia una di così nel grafo.

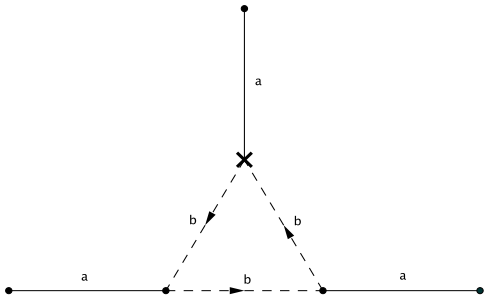

Figura 1.10. Situazione della sequenza nella Proposizione 1.21.

In Figura 1.10, consideriamo il vertice evidenziato con una croce, tale che i vertici a cui è connesso tramite archi di tipo b fanno parte di una sottosequenza del tipo $[\ldots, a, b, a, \ldots]$. A tale vertice non può arrivare nè da esso può partire un arco di tipo b, altrimenti si avrebbero collisioni, ma allora tale elemento può solo essere quello iniziale del cammino, da cui esce un arco di tipo a, oppure quello finale, a cui arriva un arco di tipo a. L'elemento considerato può essere solo quello di partenza o quello di arrivo, in particolare possono esserci al massimo due sequenze della forma $[\ldots, a, b, a, \ldots]$. Il prodotto di tutti gli archi del cammino hamiltoniano in questo generico caso è quindi:

$$b^i(ab^2)^r(ab)^\epsilon(ab^2)^s(ab)^\delta(ab^2)^t a^k b^j, i, \in \{0, 1, 2\}, k, j, \epsilon, \delta \in \{0, 1\}, r, s, t \in \{0, \ldots, \frac{|G|}{9} - 1\}.$$

Questo fatto non è ancora del tutto soddisfacente. Infatti in questo caso otteniamo, prendendo il massimo valore che i vari parametri possono assumere, la stima:

$$|G| - 1 = i + 3r + 2\epsilon + 3s + 2\delta + 3t + k + j \leq$$
$$2 + 3(\tfrac{|G|}{9} - 1) + 2 + 3(\tfrac{|G|}{9} - 1) + 2 + 3(\tfrac{|G|}{9} - 1) + 2 = 8 + |G| - 9 = |G| - 1,$$

che ancora non porta ad un assurdo. Ma la condizione $i = 2, \epsilon = 1, \delta = 1, j = 1$ non è ammissibile, poichè, in tal caso, nè l'arco di partenza nè quello di arrivo sono a, contro le nostre precedenti considerazioni. Quindi, $i + 2\epsilon + 2\delta + j \leq 6$, da cui:

$$|G| - 1 = (i + 2\epsilon + 2\delta + j) + 3(r + s + t) + k \leq 6 + |G| - 9 + 1 = |G| - 2,$$

ed arriviamo finalmente ad un assurdo. □

Esempio 1.6. Riprendiamo l'Esempio 1.2, esaminando il caso orientato. Consideriamo il digrafo $\overrightarrow{Cay}(G, \{\alpha, \beta\})$, dove $G = C_p \rtimes C_6$, $p \equiv 1 \mod 6$, $p > 9$, $C_p = \langle a \rangle$, $C_6 = \langle b \rangle$, $\alpha = b^3$, $\beta = ab^2$, ϵ radice primitiva sesta dell'unità in $\mathbb{Z}_p$. È $|\alpha| = 2$, $|\beta| = 3$. Se $\gamma = \alpha\beta^{-1}$, si ha:

$$\gamma = ba^{-1}, \quad \gamma^2 = b^2a^{-\epsilon-1}, \quad \gamma^3 = b^3a^{-2\epsilon}, \quad \gamma^6 = 1,$$

perciò $|\langle\gamma\rangle| = 6 < \frac{|G|}{9} = 6\frac{p}{9}$. Dunque, per la Proposizione 1.21, $\overrightarrow{Cay}(G, \{\alpha, \beta\})$ non possiede nemmeno cammino hamiltoniano orientato.

Vediamo ora un'altra applicazione della Proposizione 1.21. Per quanto riguarda i grafi, i gruppi semplici sono uno dei casi più facili in cui dimostrare la presenza di cicli hamiltoniani, ed è grazie a questo che si basano molte dimostrazioni sull'hamiltonianità di gruppi più complicati. Nel caso orientato, svariati gruppi semplici 2-generati, un numero infinito di questi, nemmeno possiedono un cammino orientato. Diamo prima la seguente:

Definizione 1.5. *Il gruppo $G \neq 1$ si dice* (k, l, m)-generato *se esistono $x, y \in G$, con $x^k = y^l = (xy)^m = 1$, tali che $\langle x, y \rangle = G$.*

La Proposizione 1.21 ha come conseguenza il seguente fatto.

Proposizione 1.22. *Sia G gruppo finito $(2, 3, k)$-generato, con $x^2 = y^3 = (xy)^k = 1$, tale che $|G| > 9k$. Allora, esiste $z \in G$, tale che $\overrightarrow{Cay}(G, \{x, z\})$ non possiede cammino hamiltoniano orientato.*

Dim. Sia $z = y^{-1}$. Vale $|x| = 2$, $|z| = 3$, e $|xz^{-1}| = |xy| = k < \frac{|G|}{9}$. Si conclude per la Proposizione 1.21. □

Molti gruppi semplici sono di questa forma. Il seguente risultato, contenuto in [**4**], è dovuto a Conder.

Teorema 1.6. *Per ogni $k \geq 7$, esiste n_k tale che, per ogni $n \geq n_k$, A_n è $(2,3,k)$-generato.*

In particolare, se n_7 è come nel Teorema 1.6, ponendo $m_7 = \max\{5, n_7\}$ si ha che, per ogni $n \geq m_7$, A_n è $(2,3,7)$-generato, e $|A_n| > 63$. La Proposizione 1.22 e la semplicità di A_n quando $n \geq 5$ ci portano quindi a questo risultato.

Proposizione 1.23. *Esistono infiniti gruppi semplici $\{T_n\}_n$, $T_n = \langle x_n, y_n \rangle$, tali che $\overrightarrow{Cay}(T_n, \{x_n, y_n\})$ non possiede cammino hamiltoniano orientato.*

In realtà, questo non è solo il caso di A_n per n grande. Ricordiamo prima il seguente risultato presente in [**18**].

Teorema 1.7. *Esiste $N \in \mathbb{N}$ tale che $\forall n \in \mathbb{N}, n \geq N$, si ha $SL(2,n) = \langle a_n, b_n \rangle$, con $|a_n| = 2$, $|b_n| = 3$, $|a_n b_n| = 7$.*

Prendiamo $N \in \mathbb{N}$, $n \geq N$, a_n, b_n come nel Teorema 1.7, e sia $c_n = {b_n}^{-1}$. E' $|a_n| = 2, |c_n| = 3, |a_n {c_n}^{-1}| = 7$, che è minore di $\frac{|SL(2,n)|}{9}$, per n abbastanza grande. Questo fatto vale, al limite alzando la soglia sopra cui n deve stare, chiamiamola N', anche per $PSL(2,n)$, il quale è semplice per ogni $n \geq 3$. Per la Proposizione 1.21, anche $PSL(2,n)$, per n abbastanza grande, è tale che $\overrightarrow{Cay}(PSL(2,n), \{a_n, c_n\})$ non possiede cammino hamiltoniano orientato.

Con ragionamenti analoghi, si possono trovare altre successioni di gruppi semplici $(2,3,k)$-generati con digrafo di Cayley privo di cammino hamiltoniano. Si veda la survey [**23**] per questo.

CAPITOLO 2

Stime per l'hamiltonianità, scelti i generatori

Il problema che ci si pone in questo capitolo è diverso da quello affrontato nel precedente. Senza ipotesi particolari sul gruppo G, cercheremo un insieme opportuno di generatori S che renda hamiltoniano il grafo $Cay(G, S)$. Cercheremo di scegliere S "non troppo grande". In particolare, il nostro lavoro è in direzione di una congettura più debole di quella di Lovasz. Definiamo infatti la seguente quantità.

Definizione 2.1. *Sia G gruppo. Denotiamo con $d(G)$ la minima cardinalità di un insieme di generatori per G.*

La nuova congettura è la seguente.

Congettura (Babai). *Dato G gruppo, esiste S insieme di generatori per G, con $|S| = d(G)$, tale che $Cay(G, S)$ è hamiltoniano.*

Da una parte, il nostro approccio è concorde alle ipotesi di *esistenza*, non di arbitrarietà, di un insieme di generatori buoni per G. Dall'altra parte, il metodo di lavoro di questo capitolo è del tutto generale, e farà uso di diversi risultati avanzati in teoria dei gruppi finiti.

1. Gruppi generati da insiemi con particolari involuzioni

Diamo subito una definizione che ci serve per i risultati che mostreremo.

Definizione 2.2. *Sia G un gruppo, X un sottoinsieme di G. Diciamo che $a \in G$* stabilizza *X se per ogni $x \in X$ è anche $xa \in X$, in altre parole se è $Xa = X$.*

L'idea che seguiamo ora per la costruzione di insiemi di generatori di cardinalità bassa è quella di Igor Pak, presente in [**21**]. Andremo ad investigare gruppi semplici

e comportamento dei loro generatori. Siamo in particolare interessati alla presenza di involuzioni. Questo perchè i due seguenti risultati intermedi, che coinvolgono involuzioni e loro comportamento, sono il punto di partenza della nostra costruzione. Diremo, nel seguito, che S è un insieme di *buoni generatori* per G se $Cay(G, S)$ possiede un cammino hamiltoniano.

Lemma 2.1. *Sia G gruppo generato da tre involuzioni a, b, c tali che $ab = ba$. Allora, il grafo $Cay(G, \{a, b, c\})$ è hamiltoniano.*

Dim. Faremo vedere ricorsivamente l'esistenza di un ciclo hamiltoniano. Costruiremo per $1 \leq i \leq n$ un insieme X_i ed un ciclo C_i avente gli elementi di X_i come vertici, incontrati una ed una sola volta, tali che $X_i \subsetneq X_{i+1}$, con la proprietà che b e c stabilizzano X_i per ogni i, con n il minimo intero tale che $X_n = G$. C_n sarà quindi il ciclo da noi desiderato.

Sia $X_1 = H = \langle b, c\rangle$; poichè $|b| = 2 = |c|$, si ha ovviamente $|H| = 2m$, $m \in \mathbb{N}$; inoltre, H è un gruppo diedrale, essendo generato da due involuzioni. Abbiamo quindi il ciclo hamiltoniano: $C_1 = m*[b, c]$ dove compaiono esattamente $2m$ elementi, chiaramente distinti. E' chiaro che b e c stabilizzano X_1 per le proprietà di sottogruppo di H.

Costruiamo la ricorsione. Dobbiamo in qualche modo utilizzare l'altro generatore a e la proprietà di commutazione con b. Supponiamo che siano stati costruiti X_i, con $X_i b = X_i c = X_i$, e C_i ciclo di vertici gli elementi di X_i e che transita per ciascuno di essi un'unica volta.

Se a stabilizza X_i, è $X_i\langle a, b, c\rangle = X_i$, cioè $X_i G = X_i$, è quindi $G = X_i$, cioè $i = n$ e abbiamo già trovato il ciclo hamiltoniano C_n su tutto G.

Supponiamo invece che a non stabilizzi X_i. Esiste dunque un $x \in X_i$ tale che $xa \notin X_i$. Sia $y = xa$. La classe laterale sinistra yH di H è disgiunta da X_i: in caso contrario, si avrebbe $yh = z \in X_i \exists h \in H$, cioè $y = zh^{-1}$, e h stabilizza X_i poichè $h \in \langle b, c\rangle$ e b e c stabilizzano X_i per ipotesi induttiva, seguirebbe $y \in X_i$, assurdo poichè $y \notin X_i$ per sua definizione. Poniamo quindi $X_{i+1} = X_i \sqcup yH$. Sia b che c stabilizzano X_i e yH, dunque tutto X_{i+1}. Da $y = xa$, poichè a è un'involuzione, si ha che $x = ya$. Concentriamoci sulla posizione di x nel ciclo C_i. In questo ciclo, da x partono due archi, che possono essere solo della forma a, b, c. Non può essere $xa \in X_i$ per l'ipotesi su y; x è quindi connesso a xb e xc. Se prendiamo dunque x come punto di partenza di C_i, la sequenza di archi nel ciclo è $[c, [l_k]_{k=1}^{|X_i|-2}, b]$, dove $l_k \in \{a, b, c\} \forall k = 1, \ldots, |X_i| - 2$.

Questa informazione, assieme alla commutazione fra a e b, ci consente di unire due cicli in uno. Consideriamo infatti lo stesso C_i e il ciclo in yH dato dalla moltiplicazione a sinistra per y del ciclo nella base della ricorsione: l'unione insiemistica dei vertici di questi due cicli disgiunti dà X_{i+1}. Analogamente a quanto fatto per H, troviamo anche in yH un naturale ciclo hamiltoniano, sia yb la sua partenza. Essendo $ab = ba$ è $xba = xab = yb$, e produciamo finalmente un ciclo hamiltoniano C_{i+1} di vertici gli elementi di X_{i+1}: esso è quello di punto di partenza x, e archi $[c, [l_k]_{k=1}^{|X_i|-2}, a, (m-1) * [c, b], c, a]$. □

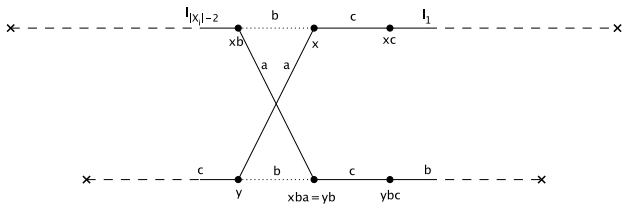

Figura 2.1. Costruzione del ciclo X_{i+1} dai due cicli in X_i e yH nel passo induttivo del Lemma 2.1.

Lemma 2.2 (Rankin). *Sia G un gruppo generato da a e b, tali che $(ab)^2 = 1$. Allora, $Cay(G, \{a, b\})$ è hamiltoniano.*

Dim. Procediamo ricorsivamente. Per $i \geq 1$, al passo i costruiremo un insieme X_i ed un ciclo C_i avente vertici gli elementi di X_i incontrati una e una sola volta in tale ciclo, con $X_{i-1} \subsetneq X_i$, e che hanno la seguente proprietà: b stabilizza X_i, e se a non stabilizza X_i, diciamo $g = xa \notin X_i$ con $x \in X_i$, allora xb^{-1} e x stanno in C_i, e sono ivi connessi tramite b. Raggiungeremo quindi a un certo punto $X_i = G$, in corrispondenza C_i sarà il ciclo hamiltoniano desiderato.

Per la base: sia $X_1 = \langle b \rangle = H$, $C_1 = |b| * [b]$. Naturalmente le condizioni sopra sono soddisfatte.

Sia ora costruito X_i, e vogliamo costruire X_{i+1}. Se a stabilizza X_i, allora qualsiasi prodotto che coinvolge a e b stabilizza X_i, cioè $X_i = G$, e abbiamo finito. Se a non stabilizza X_i, allora

c'è un $x \in X_i$ tale che $xa \notin X_i$, per costruzione di X_i si ha che $xb^{-1} \in X_i$, e tale elemento è connesso ad x tramite b nel ciclo C_i. Consideriamo la classe laterale xaH, che possiede un ciclo hamiltoniano in maniera naturale. Aggiungiamo degli archi della forma a, b per connettere fra loro gli elementi x, xa, xab, xb^{-1}. xb^{-1} è connesso ad x tramite b, x è connesso a xa tramite a, xa è connesso a xab tramite b, e xab è connesso tramite a a $xaba = xb^{-1}$ essendo ab involuzione.

Abbiamo quindi un quadrato che coinvolge i quattro vertici, come in figura. Poniamo $X_{i+1} = X_i \sqcup xaH$. Se ai due cicli hamiltoniani di vertici rispettivamente X_i e xaH aggiungiamo gli archi (x, xa) e (xab, xb^{-1}) e rimuoviamo gli archi (xb^{-1}, x) e (xa, xab), otteniamo un ciclo C_{i+1}. Tale ciclo è stabilizzato da b e ha come vertici gli elementi di X_{i+1}, dunque la prima condizione del Lemma è soddisfatta; inoltre, se un certo a non stabilizza X_{i+1}, perciò $g = za \notin X_{i+1}$ con $z \in X_{i+1} \setminus X_i$ poichè per X_i tutte le condizioni già valgono, z non può valere nè x nè xab, e negli altri casi si ha sempre, in C_{i+1}, un arco della forma b che giunge z, dunque anche la seconda ipotesi del Lemma è soddisfatta. □

2. Gruppi simmetrici, semplici e stima di Pak

I risultati mostrati nella precedente sezione sono il punto di partenza per determinare un insieme di generatori S di G, con $|S| = O(\log|G|)$, tale che $Cay(G, S)$ sia hamiltoniano. Ci serviremo di risultati sulla classificazione dei gruppi semplici, in particolare sulla loro generazione.

Mostriamo gli esempi fondamentali di applicazione dei Lemmi 2.1 e 2.2.

Esempio 2.1. Consideriamo il gruppo $PSL(2,p) = SL(2,p)/\langle diag(-1,-1)\rangle$, con p primo, $p \equiv 1 \mod 4$, condizione che ci assicura l'esistenza di un $a \in \mathbb{F}_p$ con $a^2 = -1$. Si ha che $PSL(2,p)$ è generato da S, con:

$$S = \{\alpha, \beta, \gamma\}, \quad \alpha = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}, \beta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \gamma = \begin{pmatrix} a & 0 \\ a & -a \end{pmatrix}.$$

Si ha che $\alpha^2 = \beta^2 = \gamma^2 = 1$, e $\alpha\beta = \beta\alpha$ in $PSL(2,p)$. Per il Lemma 2.1, $Cay(PSL(2,p), S)$ è hamiltoniano per ogni $p \equiv 1 \mod 4$.

I grafi dell'esempio appena mostrato sono importanti perchè forniscono esempi di grafi detti *expanders*, ovvero grafi tali che per ogni sottoinsieme di vertici X nel grafo,

il numero di vertici fuori da X connessi a X tramite un arco del grafo sono più di $\epsilon|X|$ per un fissato $\epsilon > 0$. La ricerca di costruzioni esplicite di expanders è un problema importante, di grande interesse in combinatoria. I grafi di Cayley sui $PSL(2, p)$, con $p \equiv 1 \mod 4$ e i generatori come sopra, forniscono esempi di queste costruzioni.

Altri grafi importanti sono particolari grafi di Cayley su gruppi simmetrici. Mostriamo due esempi di grafi hamiltoniani, generati rispettivamente da 3 e 2 elementi.

Esempio 2.2. Nel gruppo S_{2n+1}, gli elementi $\sigma = (1\,2)$, $\tau = (1\,2)(3\,4)\dots(2n-1\,2n)$ e $\tau' = (2\,3)(4\,5)\dots(2n\,2n+1)$ sono involuzioni. Si ha che $\langle\sigma, \tau, \tau'\rangle = S_{2n+1}$, infatti $\tau\tau'$ è il ciclo $(1\,3\,5\dots2n-1\,2n+1\,2n\,2n-2\dots4\,2)$, che assieme allo scambio σ genera tutto il gruppo simmetrico. E' poi $\sigma\tau = (3\,4)\dots(2n-1\,2n) = \tau\sigma$. Siamo nelle ipotesi del Lemma 2.1: $Cay(S_{2n+1}, \{\sigma, \tau, \tau'\})$ possiede un ciclo hamiltoniano.

Esempio 2.3. Il gruppo simmetrico S_n è generato dall'n-ciclo $\sigma = (1\,2\,\dots\,n)$ e dall'$(n-1)$-ciclo $\tau = (2\,n\,n-1\,\dots\,3)$, poichè $\sigma\tau = (1\,n)$, scambio che assieme al ciclo σ genera tutto il gruppo. Lo stesso prodotto $\sigma\tau$ di ordine 2 ci dice, per il Lemma 2.2, che $Cay(S_n, \{\sigma, \tau\})$ è hamiltoniano. Troviamo quindi in ogni gruppo simmetrico un insieme di soli 2 generatori che forniscono ad esso un ciclo hamiltoniano.

Il Lemma 2.2 è di grande importanza, perchè di permette di concludere che un gruppo generato da 2 elementi - diremo 2-*generato* - dove uno dei due generatori è un'involuzione, possiede sempre un ciclo hamiltoniano, per opportune scelte dei generatori.

Proposizione 2.1. *Sia G un gruppo tale che $G = \langle a, b\rangle$, con $|a| = 2$. Allora, esistono $s, t \in G$, tali che $G = \langle s, t\rangle$, e $Cay(G, \{s, t\})$ è hamiltoniano.*

Proof. Poniamo $s = ab^{-1}$, $t = b$. È chiaro che così come $\langle a, b\rangle = G$, è pure $\langle s, t\rangle = G$, poichè $st = a$. Si ha inoltre $(st)^2 = a^2 = 1$, dunque, per la Proposizione 2.1, $Cay(G, \{s, t\})$ è hamiltoniano. □

Esempio 2.4. In questo esempio, mostriamo che $G = A_5 \wr A_5 = \langle S\rangle$, dove:

$$S = \{a, b\}, \quad a = (y, 1, 1, 1, 1)(235), \quad b = (1, 1, 1, 1, x)(12)(34),$$

dove $x, y \in A_5$ sono tali che $\langle x, y\rangle = A_5$, x ha ordine 2 e y ha ordine 5, per esempio $x = (23)(45)$, $y = (12345)$. Come conseguenza, essendo:

$$b^2 = ((1,1,1,1,x)(12)(34))^2 = (1,1,1,1,x)(1,1,1,1,x)^{(12)(34)} = 1,$$

per la Proposizione 2.1 esistono $s, t \in G$ generatori per G, tali che $Cay(G, \{s, t\})$ è hamiltoniano.

Sia $H = \langle a, b\rangle \leq {A_5}^5 \rtimes A_5$. Calcolando le potenze di a, si ha che:

$$a^2 = (y,1,1,1,1)(y,1,1,1,1)^{(253)}(253) = (y^2,1,1,1,1)(253),$$

$$a^3 = (y^2,1,1,1,1)(y,1,1,1,1)^{(235)} = (y^3,1,1,1,1),$$

di conseguenza vale che $(y,1,1,1,1), (253), (235) \in H$. In H sta anche il prodotto $b(235)$, cioè $c = (1,1,1,1,x)(13452)$, le cui potenze sono:

$$c^2 = (1,1,1,1,x)(1,1,1,1,x)^{(12543)}(13452)^2 = (1,1,1,x,x)(14235),$$

$$c^3 = (1,1,1,x,x)(1,1,1,1,x)^{(15324)}(14235)(13452) = (1,1,x,x,x)(15324),$$

$$c^4 = (1,1,x,x,x)(1,1,1,1,x)^{(14235)}(15324)(13452) = (x,1,x,x,x)(12543),$$

$$c^5 = (x,1,x,x,x)(1,1,1,1,x)^{(13452)}(12543)(13452) = (x,x,x,x,x).$$

Dunque, $(x,x,x,x,x) \in H$. E in H vi sono anche:

$$(y,1,1,1,1)^{(1,1,1,1,x)(12)(34)} = (y,1,1,1,1)^{(12)(34)} = (1,y,1,1,1),$$

$$(1,y,1,1,1)^{(235)} = (1,1,y,1,1), \quad (1,1,y,1,1)^{(235)} = (1,1,1,1,y),$$

$$(1,1,y,1,1)^{(1,1,1,1,x)(12)(34)} = (1,1,y,1,1)^{(12)(34)} = (1,1,1,y,1).$$

Quindi $H \supseteq \langle (y,1,1,1,1), \ldots, (1,1,1,1,y), (x,x,x,x,x)\rangle$. Poichè $\langle x, y\rangle = A_5$, che è gruppo semplice, si ha che H contiene la base ${A_5}^5$ del prodotto intrecciato G, e di conseguenza anche $(12)(34)$ e (235), due generatori del complemento A_5 della base. Si conclude che $H = G$, come volevamo.

L'esempio più importante di questo paragrafo riguarda i gruppi semplici non abeliani. Ricordiamo prima questo fondamentale risultato, la cui dimostrazione fa uso della classificazione dei gruppi semplici, presente in [**11**].

Teorema 2.1. *Sia T un gruppo semplice non abeliano. Allora, per ogni elemento $x \neq 1$ in G, esiste un elemento y di G, tale che $\langle x, y\rangle = G$.*

Ogni gruppo semplice non abeliano ha ordine pari, in particolare contiene un elemento x con $x^2 = 1$. Per il Teorema 2.1, esiste quindi un elemento $y \in T$, tale che $\langle x, y \rangle = T$. La Proposizione 2.1 ci fornisce dunque il risultato che segue riguardo all'hamiltonianità dei grafi sui gruppi semplici.

Proposizione 2.2. *Sia T un gruppo semplice non abeliano. Allora, esistono s, t tali che $\langle s, t \rangle = T$ e $Cay(T, \{s, t\})$ è hamiltoniano.*

Grazie ai risultati finora ottenuti, alla ricostruzione dei cammini, e al teorema di Jordan-Hölder sull'unicità della serie di composizione di un gruppo, possiamo trovare in ogni gruppo finito G un cammino hamiltoniano con un numero relativamente basso di generatori.

Teorema 2.2 (Stima di Pak). *Sia G gruppo, e siano r e m i numeri di fattori di composizione rispettivamente abeliani e non abeliani di G. Allora esiste un insieme S di generatori per G, con $|S| \leq r + 2m$, tale che $Cay(G, S)$ contiene un cammino hamiltoniano.*

Dim. Nella serie di composizione di G, siano $A_1, \ldots, A_r$ e $T_1, \ldots, T_m$ i fattori di composizione rispettivamente abeliani, quindi ciclici, e non abeliani di G. Più in dettaglio, se:

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{r+m-1} \trianglelefteq N_{r+m} = G$$

è la serie di composizione di G, si ha: $A_i = N_{j_i+1}/N_{j_i}, T_k = N_{j_k+1}/N_{j_k}$, per una certa biiezione j a valori fra 0 e $r + m - 1$. Ogni gruppo ciclico A_i ha ovviamente un unico generatore c_i che rende hamiltoniano il rispettivo grafo su A_i. Per la Proposizione 2.2, ogni gruppo semplice T_k ha due generatori $\langle s_k, t_k \rangle$ tale che $Cay(T_k, \{s_k, t_k\})$ è hamiltoniano. Consideriamo gli elementi $g_i, a_k, b_k \in G$, tali che $A_i = \langle g_i N_{j_i} \rangle / N_{j_i}$, $T_k = \langle a_k N_{j_k}, b_k N_{j_k} \rangle / N_{j_k}$, e poniamo $S = \bigcup_{i=1}^{r} \{g_i\} \cup \bigcup_{k=1}^{m} \{a_k, b_k\}$. E' chiaro che $|S| \leq r + 2m$, e $\langle S \rangle = G$. Inoltre, ciascun quoziente nella catena di composizione, isomorfo a uno degli A_i o a uno dei T_k, possiede un ciclo hamiltoniano, quindi in particolare un cammino. Possedere un cammino, per il Lemma 1.3, è una proprietà che si estende per serie subnormali, dunque anche $Cay(G, S)$ possiede un cammino hamiltoniano. □

Se decidiamo noi l'insieme S di generatori per un gruppo G, di modo che $Cay(G, S)$ possieda un cammino hamiltoniano è chiaro come modificare, di poco, tale insieme

in maniera che il cammino hamiltoniano si estenda a un ciclo hamiltoniano: si aggiunge eventualmente a S l'arco mancante che collega ultimo e primo elemento del cammino.

Abbiamo una buona stima per il numero di generatori che rendono $Cay(G, S)$ hamiltoniano.

Teorema 2.3. *Sia G gruppo, $|G| \geq 3$. Allora, esiste S insieme di generatori per G, $|S| \leq \log_2 |G|$, tale che $Cay(G, S)$ è hamiltoniano.*

Dim. Siano A_i, $i = 1, \ldots, r$, T_j, $j = 1, \ldots, m$ i fattori rispettivamente abeliani e non abeliani della serie di composizione di G. Il più piccolo gruppo semplice non abeliano è A_5, di ordine 60; dunque per ogni $j = 1, \ldots, m$ si ha $|T_j| \geq 60 > 4$. Abbiamo:

$$2^{r+2m} = 2^r 4^m \leq \prod_{i=1}^{r} |A_i| \prod_{j=1}^{m} |T_j| = |G|.$$

L'uguaglianza è raggiunta se e solo se ci sono solo gruppi abeliani di ordine 2 nella catena di composizione, cioè se e solo se $G = \mathbb{Z}_2^n$, e si è già visto che in quel caso $Cay(G, \{e_1, \ldots, e_n\})$ è hamiltoniano, $n = \log_2 2^n$. Negli altri casi, per il teorema precedente si ha che G ha un insieme di generatori S, $|S| \leq r+2m < \log_2 |G|$, con rispettivo grafo che possiede un cammino hamiltoniano. Siano g e h rispettivamente vertice iniziale e finale di tale cammino. Ponendo $S' = S \cup \{h^{-1}g\}$ si ha che $Cay(G, S')$ è hamiltoniano, e $|S'| \leq |S|+1 = r+2m+1 \leq \log_2 |G|$, da cui la tesi. □

La motivazione che ci spinge a dare un miglioramento alla stima di Pak è la seguente. Concentriamo per ora l'attenzione sull'addendo r della stima. Esiste sempre un gruppo abeliano con r fattori di composizione che ha bisogno di almeno r buoni generatori: infatti, il gruppo $A_r = \mathbb{Z}_2^r$ è tale che $d(A_r) = r$. Anche al crescere di r, dunque, la stima di Pak sembra essere, almeno in questo caso abeliano, la migliore possibile. Questo ragionamento non vale per l'addendo $2m$ della stima. Se infatti è vero che per un gruppo semplice non abeliano T vale $m = 1, d(t) = 2 = 2m$, per il prodotto diretto $T \times T$ è $m = 2$, ma come vedremo è $d(T \times T) = 2 < 2m = 4$. Lo scopo del prossimo paragrafo sarà investigare il comportamento dei generatori di

prodotti diretti di gruppi semplici, in particolare del caso T^2, quando T è semplice non abeliano: riusciremo a migliorare il coefficiente di m per la stima di Pak.

In chiusura di questo paragrafo, concludiamo con un esempio che mostra come la stima di Pak sia ancora distante dall'effettivo comportamento di un grafo $Cay(G, S)$: troviamo una successione di gruppi G_m, ciascuno costituito da $m+1$ fattori di composizione non abeliani, ma tale che esiste S_m generatore di G, con $|S_m| = 2$, e $Cay(G_m, S_m)$ hamiltoniano.

Esempio 2.5. Sia T un gruppo semplice non abeliano, e consideriamo, fissato m, il gruppo $G = T \wr C_m = B \rtimes C_m$, dove $B = T^m$ è la base del prodotto semidiretto. Al variare di m, G possiede $m+1$ fattori di composizione, le m copie di T e C_m. In G troveremo due generatori α, β tali che $\beta^2 = 1$. Se $\langle x, y\rangle = T$ con x involuzione e $C_m = \langle\sigma\rangle$, con $\sigma = (12\dots m)$ che agisce su B, siano infatti $\alpha = (y, 1, \dots, 1)\sigma$ e $\beta = (x, 1, \dots, 1)$. Si verifica che, per $k \geq 2$, $\alpha^k = (y, \dots, 1)\sigma^k(1, y, \dots, y, 1, \dots, 1)$, dove le y nell'ultimo fattore sono $k-1$: infatti, per il caso base si ha:

$$(y, 1, \dots, 1)\sigma(y, 1, \dots, 1)\sigma = (y, 1, \dots, 1)\sigma^2\sigma^{-1}(y, 1, \dots, 1)\sigma =$$

$$= (y, 1, \dots, 1)\sigma^2(y, 1, \dots, 1)^\sigma = (y, 1, \dots, 1)\sigma^2(1, y, 1, \dots, 1),$$

e il passo induttivo è analogo. In particolare quindi si ha che:

$$\alpha^m = (y, 1, \dots, 1)\sigma^m(1, y, y, \dots, y) = (y, y, \dots, y).$$

Abbiamo poi che:

$$\alpha\beta\alpha^{-1} = (y, 1, \dots, 1)(x, 1, \dots, 1)^{\sigma^{-1}}(y^{-1}, 1, \dots, 1) = (1, \dots, 1, x),$$

Per $i = 1, \dots, m$, poniamo β_i l'elemento di B avente x in posizione i-esima e 1 altrove (dunque, $\beta_1 = \beta$). Sia $H = \langle\alpha, \beta\rangle$. La relazione sopra ci dice che $(1, \dots, 1, x) = \beta_m \in H$, e coniugando ripetutamente tale elemento per α^{-1} troviamo in H anche $\beta_2, \dots \beta_{m-1}$. Si ha dunque $H = \langle\alpha, \beta_1, \dots, \beta_m\rangle$. Sia $K = H \cap B \leq H$. Definiamo, per $i = 1, \dots, m$, U_i come il sottogruppo di B identificato con il prodotto di tutti i fattori T in G, tranne l'i-esimo, e consideriamo le proiezioni $\pi_i : K \to U_i$, $i = 1, \dots, m$. Si ha che $\ker\pi_i \subseteq T_i$, dove T_i è il sottogruppo identificato con la i-esima copia di T in B, dunque $\ker\pi_i \trianglelefteq T_i$; gli unici sottogruppi normali di T_i sono quelli banali, e si ha che $\beta_i \in \ker\pi_i$, perciò l'unica possibilità

è che $\ker \pi_i$ sia proprio T_i. Si ha quindi, scritto in maniera completa in G, che:

$$K \supseteq T_1 \cup T_2 \cup \cdots \cup T_m,$$

quindi H contiene il prodotto di tutte le copie di T poichè $H \supseteq K$; in particolare, contiene $(y^{-1}, 1, \ldots, 1)$, e quindi anche il suo prodotto per α, cioè σ, ultimo generatore che ci mancava per concludere che di fatto è $H = G$.

G è quindi generato da due elementi, uno dei quali è un'involuzione. Per la Proposizione 2.1, esistono quindi $s, t \in G$, tali che $Cay(G, \{s, t\})$ è hamiltoniano.

3. Un importante risultato sul quadrato di gruppi semplici

In questa sezione, viene mostrato un risultato fondamentale per poter migliorare la stima di Pak, per quanto riguarda il coefficiente del numero m di fattori semplici non abeliani di un gruppo G. Questo risultato ha interesse proprio, ed è il fulcro di questo capitolo. Mostreremo che il quadrato di ogni gruppo semplice non abeliano può essere generato da due elementi, uno dei quali è un'involuzione. Questo ha conseguenze immediate sull'hamiltonianità di grafi su tali gruppi. Sfrutteremo questo fatto lavorando sulle serie di composizione di gruppi arbitrari, potendo raggruppare almeno due gruppi alla volta.

La seguente proposizione ci servirà più volte.

Proposizione 2.3. *Sia $G = \prod_{i=1}^{n} S_i^{\alpha_i}$, con gli S_i gruppi semplici non isomorfi, $\alpha_i \in \mathbb{N}$. Sia $S \subseteq G$ tale che $\langle \pi_i(S) \rangle = S_i^{\alpha_i}\ \forall i$, dove π_i è la proiezione su $S_i^{\alpha_i}$. Allora, $\langle S \rangle = G$.*

Dim. Supponiamo che sia $\langle S \rangle = H \leq G$. L'ipotesi dice: $\pi_i(H) = \pi_i(\langle S \rangle) = \langle \pi_i(S) \rangle = S_i^{\alpha_i}$ per ogni i. Fissato i troviamo quindi un $N_i \trianglelefteq H$ tale che $H/N_i \cong S_i^{\alpha_i}$. Ogni S_i compare dunque α_i volte come fattore nella serie di composizione di H, il quale possiede tutti i fattori di composizione di G, e poichè $H \leq G$ è $H = G$. □

Vediamo intanto in che modo raggruppare i gruppi semplici nella serie di composizione.

Proposizione 2.4. *Siano T_i, $i = 1, \ldots n$, gruppi semplici a due a due non isomorfi, tali che $T_i = \langle x_i, y_i \rangle$, con x_i involuzione $\forall i$. Sia $G = \prod_{i=1}^{n} T_i$. Allora,*

$G = \langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle$. *In particolare, esistono* $s, t \in G$, *tali che* $Cay(G, \{s, t\})$ *è hamiltoniano.*

Dim. Sia $H = \langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle \leq T_1 \times \cdots \times T_n$. Per ogni i, $\pi_i(H) = \langle x_i, y_i \rangle = T_i$, e per la Proposizione 2.3 è $H = T_1 \times \cdots \times T_n$. La seconda tesi segue grazie alla Proposizione 2.1. □

Esaminiamo invece cosa succede nel caso di due gruppi isomorfi.

Proposizione 2.5. *Sia* T *un gruppo semplice, tale che* $T = \langle x_1, y_1 \rangle$, $T = \langle x_2, y_2 \rangle$. *Allora:*

$$T^2 = \langle (x_1, x_2), (y_1, y_2) \rangle \iff (x_1, y_1)^\sigma \neq (x_2, y_2) \forall \sigma \in Aut(T).$$

In particolare, se x_1, x_2 *sono involuzioni e le condizioni sopra sono verificate, allora esistono* $s, t \in T^2$, *tali che* $Cay(T^2, \{s, t\})$ *è hamiltoniano.*

Dim. Sia $H = \langle (x_1, x_2), (y_1, y_2) \rangle \leq T_1 \times T_2$ con $T_1 \cong T_2$, e consideriamo le proiezioni π_i sui T_i. Siano $N_i = \ker \pi_i$, $i = 1, 2$. Si ha[1] $N_1 \subseteq T_2, N_2 \subseteq T_1$. E' $N_1 \trianglelefteq H$, dunque $N_1 = \pi_2(N_1) \trianglelefteq \pi_2(H) = T_2$, ovvero $N_1 \trianglelefteq T_2$. Analogamente, $N_2 \trianglelefteq T_1$. Per semplicità dei T_i, abbiamo i seguenti casi per gli N_i.

- $N_1 = T_2, N_2 = T_1$: in questo caso, $H \supseteq \langle T_1, T_2 \rangle = T_1 \times T_2$, come voluto.
- $N_1 = T_2$, $N_2 = \{1\}$. Allora, $H/N_1 \cong T_1 \cong T_2 \cong H/N_2 \cong H$, assurdo. Il simmetrico è analogo.
- $N_1 = \{1\}$, $N_2 = \{1\}$. Fissato $t_1 \in T_1$, poichè $T_1 = \langle x_1, y_1 \rangle$ esiste $t_2 \in T_2$ tale che $(t_1, t_2) \in H$, e in questo caso tale t_2 è unico, infatti da $(t_1, t_2), (t_1, t_2') \in H$ seguirebbe $(1, t_2(t_2')^{-1}) \in N_1 = 1$, dunque $t_2 = t_2'$. È quindi $N_1 = N_2 = \{1\}$ se e solo se $|H| = |T_1| = |T_2|$, e il modo di associare ad un T_1 l'unico $t_2 \in T_2$ tale che $(t_1, t_2) \in H$ definisce una biiezione di T_1 in T_2 che è anche omomorfismo, in particolare, se $T_1 \cong T_2 \cong T$, questo è un automorfismo σ di T. In questo caso, dunque, è $H = \{(t, t^\sigma) : t \in T\} \exists \sigma \in Aut(T)$, ovvero $(x_1, y_1)^\sigma = (x_2, y_2)$ per un certo automorfismo σ di T.

E' chiaro poi che se $(x_1, y_1)^\sigma = (x_2, y_2) \exists \sigma \in Aut(T)$, allora vale:

$$\langle (x_1, x_2), (y_1, y_2) \rangle = \langle (x_1, x_1^\sigma), (y_1, y_1^\sigma) \rangle = \{(t, t^\sigma) : t \in T\} \subsetneq T^2,$$

[1] Per T_1 e T_2 intendiamo anche le rispettive identificazioni di T_1 e T_2 in $T_1 \times T_2$.

e si conclude. □

Perchè segua l'hamiltonianità nei grafi su gruppi del tipo T^2, T gruppo semplice non abeliano, rimane da verificare che *esistono sempre due insiemi di generatori* $\{x_1, y_1\}$ *e* $\{x_2, y_2\}$ *per* T*, con* x_i *involuzioni, tali che almeno uno fra* x_2 *e* y_2 *non sia coniugato rispettivamente a* x_1 *o* y_1 *tramite uno stesso automorfismo* σ *di* T.

Ci verranno in aiuto risultati di diversi autori. Diremo che un gruppo G è (n, m)-*generato* se esiste $\{x, y\}$ insieme di generatori per G, con $|x| = n, |y| = m$.

Proposizione 2.6. *Sia* T *gruppo semplice. Allora, esistono due insiemi di generatori* $\{x_1, y_1\}$ *e* $\{x_2, y_2\}$ *per* T*, con* x_i *involuzioni, tali che* $(x_1, y_1)^\sigma \neq (x_2, y_2) \forall \sigma \in Aut(T)$.

Dim. Se T possiede due distinte classi di elementi di ordine 2, diciamo C_1 e C_2, rispetto all'azione di $Aut(T)$, allora basta prendere $x_i \in C_i$, $i = 1, 2$, e un qualsiasi y_i che genera assieme a x_i, cosa sempre possibile per il Teorema 2.1. In ([**26**], Lemma 1) vi è una lista dei gruppi semplici che possiedono una sola classe di coniugio di elementi di ordine 2; essi sono:

$$A_5,\ A_6,\ A_7,\ PSL(2,q),\ PSL(3,q),\ PSL(4,q),$$

$$PSU(3,q),\ PSU(4,q),\ G_2(q),\ {}^2G_2(q),\ {}^3D_4(q^3),\ Sz(q),$$

$$M_{11},\ M_{22},\ M_{23},\ J_1,\ J_3,\ McL,\ ON,\ Ly,\ Th.$$

Per [**26**, Lemma 2], per i gruppi semplici fuori dalla lista di sopra le due o più classi di coniugio di involuzioni non si riuniscono mai in un'unica classe di coniugio sotto il rispettivo gruppo di automorfismi; i gruppi di sopra sono effettivamente gli unici da discutere. Per [**12**, Teorema 1.6], dato un gruppo di questa lista, esiste sempre un insieme di generatori $\{x, y\}$, con x involuzione, y di ordine primo con 6. Basta quindi, per ogni gruppo, trovare o una coppia di generatori di cui una involuzione e un'altra di ordine non primo con 6, oppure due coppie di generatori $\{x_i, y_i\}$, $i = 1, 2$, con x_1, x_2 involuzioni, e $|y_1| \neq |y_2|$. Ecco la lista dei risultati che ci permette di assicurare l'esistenza di tali generatori.

- Nell'introduzione in ([**8**]), si osserva che A_5, $PSL(2, q)$ con $q \neq 9$, $PSL(3, q)$ con $q \neq 4$, $SL(4, q)$ con q non potenza di 2 e quindi anche $PSL(4, q)$, $q \neq 2^m$, $G_2(q)$, ${}^2G_2(q)$, J_1, J_3, ON, Ly e Th sono $(2, 3)$-generati, ed è $PSL(2, 9) = A_6$.
- $A_6 = \langle (12)(34), (1235)(46) \rangle$, $A_7 = \langle (12)(34), (1234567) \rangle = \langle (14)(23), (34567) \rangle$;

- Da [**3**], M_{11}, M_{22} e M_{23} sono $(2,4)$- generati, $McL = \langle a, b\rangle = \langle a, ab\rangle$ dove $|a| = 2$, $|b| = 5$ e $|ab| = 11$, $PSL(3,4)$ è $(2,4)$-generato.
- Da [**19**, Teorema 1], ${}^3D_4(q^3)$ è $(2,3)$-generato.
- Per [**9**, Teorema 1], per ogni elemento non identico di $Sz(q)$ esiste un'involuzione che genera assieme ad esso.
- Per [**22**, Lemma 5], sia G della forma: $PSL(4,2^m)$, $PSU(3,q)$, $PSU(4,q)$ ma non della forma

  $PSL(4,2), PSU(3,3), PSU(3,5), PSU(4,2), PSU(4,3)$. Allora, per ogni $x \in G$, $x \neq 1$, esistono $y, z \in G$, tali che $G = \langle x, y^g\rangle$ e $x = y^g z^h \exists g, h \in G$, dunque è $G = \langle x, z^h\rangle$. Prendendo x involuzione, siamo a posto con questi casi se y e z hanno ordine diverso. Gli ordini di y e di z nei vari casi sono i seguenti:

$$PSL(4,2^m) : |y| = 2^{3m} - 1, |z| = 2^{2m} + 1;$$

$$PSU(3,q) : |y| = \frac{q^2 - q + 1}{(q+1,3)}, |z| = q - 1;$$

$$PSU(4,q) : |y| = \frac{q^3 + 1}{(q+1,4)}, |z| = \frac{q^2 + 1}{(2,q-1)}.$$

  Per $PSL(4,2^m)$, è $|y| \neq |z|$ essendo $|y|$ e $|z|$ diversi mod 4; per $PSU(3,q)$, si ha di sicuro $|y| \geq \frac{q^2-q+1}{3}$, ed è $\frac{q^2-q+1}{3} > |z| \leftrightarrow q^2 - q + 1 > 3q - 3 \leftrightarrow q \neq 2$, mentre $PSU(3,2)$ non è semplice; per $PSU(4,q)$, si ha $|y| \geq \frac{q^3+1}{4}$, $|z| \leq q^2 + 1$, e $\frac{q^3+1}{4} > q^2 + 1 \leftrightarrow q \leq 5$, per $q = 4$ è $|y| = 65, |z| = 17$;
- Infine, grazie a dei test con il programma GAP:
  $PSL(4,2) = A_8 = \langle (16)(78), (12345)(678)\rangle = \langle (16)(78), (1762345)\rangle$,
  $PSU(3,3) = \langle a, b\rangle$ con $|a| = 2, |b| = 6$, $PSU(4,2) = \langle a, b\rangle$, $|a| = 2, |b| = 9$, $PSU(4,3) = \langle a, b\rangle$, $|a| = 2, |b| = 6$ [ATLAS], $PSU(3,5) = \langle a, b\rangle, |a| = 2, |b| = 8$.

Si riesce quindi sempre a trovare una coppia di generatori come desiderato. □

Abbiamo provato così il seguente risultato molto importante.

Teorema 2.4. *Sia T gruppo semplice. Allora esistono $x, y \in T^2$, con $x^2 = 1$, tale che $T = \langle x, y\rangle$. In particolare, esiste $\{s, t\}$ insieme di generatori per T^2, tale che $Cay(T, \{s, t\})$ è hamiltoniano.*

4. Miglioramento della stima di Pak

L'ingrediente fondamentale per procedere nel nostro lavoro è stato evidenziato a fine dello scorso paragrafo. Altri fatti importanti in teoria dei gruppi che verranno utilizzati sono l'esistenza di una particolare serie subnormale di un gruppo G, e il fatto che la congettura di Schreier si risolva positivamente. Evidenziamo subito questo risultato, riportato in [**13**, Teorema 1.46].

Teorema 2.5 (Congettura di Schreier). *Sia T gruppo semplice finito non abeliano. Allora, $Aut(T)/T$ è risolubile.*

Ciò che vogliamo fare è raggruppare i gruppi semplici non abeliani in tale serie subnormale di G. Mostriamo i risultati di cui abbiamo bisogno in questa direzione.

Proposizione 2.7. *Siano $S_1, \dots, S_n$ gruppi semplici non isomorfi, e sia $1 \leq m \leq n$. Sia $G = S_1 \times \cdots \times S_m \times S_{m+1}^2 \times \cdots \times S_n^2$. Allora, esiste un insieme S di generatori per G, con $|S| = 2$, tale che $Cay(G, S)$ possiede un ciclo hamiltoniano.*

Dim. Per ogni $1 \leq i \leq m$ possiamo prendere $x_i, y_i \in S_i$, con x_i involuzione, tali che $\langle x_i, y_i \rangle = S_i$. Per il Teorema 2.4, possiamo trovare anche per ciascun S_i^2, con $m+1 \leq i \leq n$, una coppia (x_i, y_i) con $|x_i| = 2$ tale che $\langle x_i, y_i \rangle = S_i^2$. Sia $S = \{(x_1, \dots x_n), (y_1, \dots, y_n)\} \subseteq G$, e sia π_i la proiezione da $\langle S \rangle$ su S_i se $1 \leq i \leq m$, su S_i^2 se $m+1 \leq i \leq n$. Per costruzione, tali proiezioni sono suriettive. La Proposizione 2.3 ci consente di concludere che $\langle S \rangle = G$, dove S consiste di due elementi, uno dei quali involuzione. La tesi segue. □

Abbiamo una buona stima per il numero di generatori di un prodotto diretto di gruppi semplici che ci assicurano l'esistenza di un cammino hamiltoniano.

Proposizione 2.8. *Sia $G = S_1^{\alpha_1} \times \cdots \times S_t^{\alpha_t}$, con gli S_i gruppi semplici non abeliani non isomorfi, e $1 \leq \alpha_1 \leq \cdots \leq \alpha_t$. Sia $\alpha_t = 2n + \epsilon$, con n, ϵ rispettivamente quoziente e resto della divisione di α_t per 2. Allora, esiste un insieme di generatori S per G, con $|S| \leq 2(n + \epsilon)$, tale che $Cay(G, S)$ possiede un cammino hamiltoniano.*

Dim. Possiamo scrivere G nel seguente modo:

$$G = \prod_{j=1}^{n+\epsilon} S_1^{\delta_{1j}} \times \cdots \times S_t^{\delta_{tj}}, \qquad \delta_{ij} = \begin{cases} 2 & \alpha_i \geq 2j \\ 1 & \alpha_i = 2j-1 \\ 0 & \text{altrimenti} \end{cases}.$$

Ciascuno dei fattori della produttoria è della forma della Proposizione 2.7, dunque possiede 2 generatori che forniscono al rispettivo grafo di Cayley un ciclo, in particolare un cammino hamiltoniano. Tali fattori sono anche $n+\epsilon$ fattori di una serie subnormale di G: ricostruendo per quozienti, si ha allora che G possiede $2(n+\epsilon)$ generatori che forniscono a G un cammino hamiltoniano. □

Da adesso, il nostro scopo è utilizzare le stime trovate finora per ottenerne una analoga, che valga in generale, per il numero minimo di generatori buoni di un qualsiasi gruppo G, e che migliori quella fornita da Pak. Diamo qualche definizione utile per il seguito.

Definizione 2.3. *Sia G un gruppo. Il* radicale risolubile *di G, detto $R(G)$, è il prodotto di tutti i sottogruppi normali risolubili di G.*

Segue subito che se G è risolubile allora $R(G) = G$. $R(G)$ è normale in G perchè prodotto di sottogruppi normali. Si vede facilmente che $R(G)$ è addirittura caratteristico in G. Inoltre, $R(G)$ è risolubile: infatti, possiamo andare successivamente al quoziente per sottogruppi normali risolubili, e la risolubilità è una proprietà che si ricostruisce da normali e quozienti. Si noti che l'ipotesi di finitezza di G, assunta fin dal principio, è essenziale. Ricordiamo poi che lo *zoccolo* di un gruppo G, detto $Soc(G)$, è il sottogruppo generato da tutti i sottogruppi normali minimali di G.

Vale il seguente fatto noto in teoria dei gruppi.

Proposizione 2.9. *Sia G gruppo finito non risolubile. Allora, si ha:*

$$Soc(G/R(G)) \cong S_1 \times \cdots \times S_m,$$

dove $m \geq 1$ e S_i è un gruppo semplice non abeliano per ogni $i = 1, \ldots, m$.

Tale proposizione ci presenta un metodo per costruire una serie subnormale di G, dove in realtà ogni sottogruppo della serie è normale addirittura in G, i cui quozienti sono alternativamente gruppi risolubili e prodotti diretti di gruppi semplici non abeliani. In G, definiamo $T_0 = 1$, e per ogni $i \geq 1$ siano $R_i \trianglelefteq G$ tale che $R(G/T_{i-1}) = R_i/T_{i-1}$, e $T_i \trianglelefteq G$ tale che $Soc(G/R_i) = T_i/R_i$. Per la Proposizione 2.9, questa serie subnormale $T_0 \trianglelefteq R_1 \trianglelefteq T_1 \trianglelefteq \dots$ a un certo punto raggiunge G. Richiediamo che T_i/R_i sia non banale per ogni $i \geq 1$, mentre può esserlo il quoziente R_i/T_{i-1}: in questo modo, per il più grande s tale che $T_s/R_s \neq 1$, $s+1$ è il più piccolo i per cui $G/R_i = 1$, ovvero $R_{s+1} = G$, $R_s \subsetneq G$.

Definiamo le seguenti quantità. Per ogni $i = 1, \dots, s+1$, sia r_i la minima lunghezza di una serie subnormale di R_i/T_{i-1} a fattori ciclici. Per $i = 1, \dots, s$ sia ρ_i il numero di fattori semplici non abeliani non isomorfi nella serie di composizione di T_i/R_i, il quale si può scrivere dunque nella maniera:

$$T_i/R_i = \prod_{j=1}^{\rho_i} S_{ij}^{\alpha_{ij}}, \qquad 1 \leq \alpha_{i1} \leq \dots \leq \alpha_{i\rho_i},$$

e definiamo:

$$m_i = \alpha_{i\rho_i} = \max_{j=1,\dots,\rho_i} \alpha_{ij}.$$

Per ogni m_i, siano n_i e ϵ_i tali che $m_i = 2n_i + \epsilon_i$, $\epsilon_i \in \{0, 1\}$.

Con le notazioni finora introdotte, si ha che:

Proposizione 2.10. *Sia G gruppo. Allora, esiste un insieme di generatori S per G, con:*

$$|S| = \sum_{i=1}^{s+1} r_i + \sum_{i=1}^{s} 2(n_i + \epsilon_i),$$

tale che $Cay(G, S)$ possiede un cammino hamiltoniano.

Dim. Per ogni $i = 1, \dots, s+1$, R_i/T_{i-1} ha una serie subnormale di r_i fattori ciclici, a cui basta un solo generatore per produrre un ciclo, dunque un cammino hamiltoniano. Ricostruendo per quozienti, si ha che R_i/T_{i-1} possiede r_i generatori che forniscono ad esso un cammino hamiltoniano.

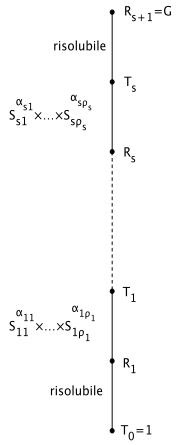

Figura 2.2. La serie subnormale presa in considerazione.

Per ogni $i = 1, \ldots, s$, $T_i/R_i = \prod_{j=1}^{\rho_i} S_{ij}^{\alpha_{ij}}$, con gli α_{ij} crescenti in senso lato. Se $\alpha_{i\rho_i} = m_i = 2n_i + \epsilon_i$, per la Proposizione 2.8 si ha che esiste un insieme di generatori per T_i/R_i di cardinalità $2(n_i + \epsilon_i)$, che fornisce al rispettivo grafo di Cayley un cammino hamiltoniano.

Gli R_i/T_{i-1}, $i = 1, \ldots, s+1$, e i T_i/R_i, $i = 1, \ldots, s$, sono una serie subnormale di G; dunque, ricostruendo per quozienti, otteniamo infine S, con $|S| = \sum_{i=1}^{s+1} r_i + \sum_{i=1}^{s} 2(n_i + \epsilon_i)$, tale che $Cay(G, S)$ possiede un cammino hamiltoniano. □

Definiamo $r^* = \sum_{i=1}^{s+1} r_i$. In questo modo, abbiamo stimato il comportamento della parte risolubile di G. È chiaro poi che è $r^* \leq r$. Stimiamo ora n_i ed ϵ_i in funzione delle lunghezze delle serie di composizione di T_i/R_i. Sia:

$$\mu_i = \sum_{j=1}^{\rho_i} \alpha_{ij}.$$

Per definizione di serie di composizione è $\sum_{i=1}^{s} \mu_i = m$, dove m, come definito nei precedenti paragrafi, è il numero di fattori semplici non abeliani nella serie di composizione di G.

Determiniamo allora una stima dei generatori buoni per avere cammini hamiltoniani nei T_i/R_i a seconda del comportamento di m_i e ρ_i. L'osservazione chiave in questa discussione sarà il caso in cui un T_i/R_i è uguale a 1: sopra ad esso, avremo solo un pezzo risolubile, sarà dunque l'ultimo fattore non risolubile della serie subnormale.

a) Sia m_i pari. Allora, $\epsilon_i = 0$, e si ha:

$$2(n_i + \epsilon_i) = 2n_i = m_i = \alpha_{i\rho_i} \leq \alpha_{i1} + \cdots + \alpha_{i\rho_i} = \mu_i.$$

b) Sia m_i dispari, e $\rho_i \geq 2$. Abbiamo che:

$$2(n_i + \epsilon_i) = (2n_i + 1) + 1 = m_i + 1 \underset{\rho_i \geq 2}{\leq} \alpha_{i1} + \cdots + \alpha_{i\rho_i} = \mu_i.$$

c) Sia m_i dispari, $m_i \geq 3$, e $\rho_i = 1$. Si ha che $n_i \geq 1$, $\epsilon_i = 1$, dunque:

$$2(n_i + \epsilon_i) = 2n_i + 2 = \frac{2n_i + 2}{2n_i + 1}(2n_i + 1) = \frac{m_i + 1}{m_i} m_i = \frac{m_i + 1}{m_i}\mu_i,$$

in particolare essendo $k \mapsto \frac{k+1}{k}$ funzione monotona decrescente sugli interi positivi, e $m_i \geq 3$, si ha $\frac{m_i+1}{m_i} \leq \frac{4}{3}$, cioè $2(n_i + \epsilon_i) \leq \frac{4}{3}\mu_i$.

d) Sia $m_i = \rho_i = 1$. Consideriamo $H = G/R_i$, in cui $Soc(H) = T$ gruppo semplice. Affermiamo che è $C_H(T) = 1$. Innanzitutto, poichè $T = Soc(H)$, è $T \trianglelefteq H$, cioè $N_H(T) = H$, perciò $C_H(T) \trianglelefteq H$. Di sicuro, $T \cap C_H(T) = 1$, altrimenti, essendo T semplice e $T \cap C_H(T) \trianglelefteq T$, si avrebbe $C_H(T) = T$ e quindi in particolare T abeliano, assurdo. Se poi fosse $C_H(T) \neq 1$, allora dentro a $C_H(T) \trianglelefteq H$ esisterebbe un sottogruppo normale minimale di H, dunque $C_H(T)$ avrebbe intersezione non banale con lo zoccolo di H, che è T, assurdo per quanto detto. Si ha quindi che $H = H/C_H(T) \leq Aut(T)$. Ma per il Teorema 2.5, $Aut(T)/T$ è risolubile essendo T semplice, dunque anche H/T è risolubile. Questo vuol dire, per la corrispondenza in G, che anche G/T_i è risolubile. T_i/R_i è l'ultimo fattore della serie subnormale in cui compaiono fattori di composizione non abeliani, l'intero i per cui succede questo deve quindi corrispondere a s. In questo caso, ovviamente, ci servono due generatori per fornire al grafo di Cayley di $T = T_i/R_i$ un cammino hamiltoniano.

Definamo l'ultima, importante quantità di cui faremo utilizzo:

$$n := \inf\{m_i : m_i \geq 3, m_i \text{ dispari}, \rho_i = 1\},$$

con la convenzione $\inf\{\emptyset\} = \infty$. Notiamo che $n \geq 3$, dunque $\frac{n+1}{n} \leq \frac{4}{3}$, ponendo $\frac{\infty+1}{\infty} = 1$. Andiamo a descrivere le conseguenze di quanto fatto finora.

Se nessuno dei T_i/R_i consiste di un solo gruppo semplice, ovvero nei casi *a*), *b*) e *c*), allora per ciascuno dei T_i/R_i bastano al massimo $\frac{n+1}{n}\mu_i$ buoni generatori, cioè ricostruendo per quozienti tutti i fattori T_i/R_i forniscono al massimo $\frac{n+1}{n}m$ di tali generatori. Tale stima continua ad avere senso nel caso $n = \infty$: questo perchè se non accade mai nè il caso $m_i = \rho_i = 1$, nè il caso m_i dispari, $m_i \geq 3$, $\rho_i = 1$, allora le nostre maggiorazioni ci forniscono un massimo di $\frac{\infty+1}{\infty}m = m$ buoni generatori.

Se invece uno dei T_i/R_i è un gruppo semplice, ovvero nel caso *d*), allora $i = s$ e $\mu_s = 1$: per $j \leq s-1$, in T_j/R_j si può ragionare come prima e trovare al massimo $\frac{n+1}{n}\mu_j$ buoni generatori, mentre nel gruppo semplice T_s/R_s si possono trovare 2 buoni generatori; e in questo caso, ricostruendo per quozienti, poichè $\mu_s = 1$ si hanno $\frac{n+1}{n}\sum_{i=1}^{s-1}\mu_i + 2 = \frac{n+1}{n}(m-1) + 2$ buoni generatori per la parte che consiste delle sezioni non risolubili.

Mettendo insieme i T_i/R_i con i R_i/T_{i-1} e ricostruendo un'ultima volta per quozienti, siamo arrivati al seguente risultato.

Teorema 2.6. *Sia G gruppo. Allora, esiste S insieme di generatori per G, con $Cay(G,S)$ che possiede un cammino hamiltoniano, tale che:*

- $|S| \leq r^* + \frac{n+1}{n}m$, *se* $m_s \neq 1$;
- $|S| \leq r^* + \frac{n+1}{n}(m-1) + 2$, *se* $m_s = 1$.

In particolare, esiste S insieme di generatori per G, con $Cay(G,S)$ hamiltoniano, tale che:

- $|S| \leq r + \frac{4}{3}m + 2$, *se* $m \neq 1$;
- $|S| \leq r + 3$, *se* $m = 1$.

Confrontiamo la seconda parte del Teorema 2.6 con la stima di Pak. Quest'ultima afferma che si trova S insieme di generatori con $Cay(G,S)$ hamiltoniano, tale che

$|S| \leq r + 2m + 1$. La stima di Pak e quella da poco trovata sono equivalenti nel caso in cui $m = 1$. Non appena vale $m > 1$, si ha invece che $r + \frac{4}{3}m + 2 \lneq r + 2m + 1$. La nuova stima è quindi davvero un miglioramento di quella di Pak.

5. Un risultato asintotico

Siamo riusciti a fornire una stima più precisa per il numero minimo di generatori da dare a un gruppo perchè il corrispondente grafo di Cayley sia hamiltoniano. Da queste dimostrazioni, può sembrare che la stima vada migliorandosi all'aumentare dell'ordine di G. L'obiettivo di questo capitolo è mostrare che al crescere di $|G|$ il coefficiente da dare a m, numero di fattori non abeliani nella serie di composizione, può essere preso piccolo a piacere, a meno di una costante additiva.

Introduciamo la seguente:

Definizione 2.4. *Sia $\mathbb{G}$ un grafo. Il* quadrato *di $\mathbb{G}$, detto $\mathbb{G}^2$, è il grafo di vertici i vertici di $\mathbb{G}$, e di archi gli archi di $\mathbb{G}$ più gli archi che collegano ciascuna coppia di elementi (a, c) ogniqualvolta esiste b in $\mathbb{G}$ tale che a è connesso a b e b è connesso a c in $\mathbb{G}$.*

Faremo uso del seguente importante risultato in teoria dei grafi, dimostrato in [**10**] da H. Fleischner.

Teorema 2.7. *Per ogni grafo connesso $\mathbb{G}$, si ha che $\mathbb{G}^2$ è hamiltoniano.*

In particolare si ha:

Corollario 2.1. *Sia G gruppo, k=d(G). Allora, esiste un insieme di generatori S, con $|S| \leq 2k^2 + k$, tale che $Cay(G, S)$ è hamiltoniano.*

Dim. Sia S' un insieme di generatori per G composto da k elementi, $S' = \{s_1, \ldots, s_k\}$. Per il Teorema 2.7, il grafo $Cay(G, S')^2$ è hamiltoniano. I vertici del grafo rimangono gli elementi del gruppo G; ai k generatori del precedente grafo bisogna aggiungere quelli relativi a tutti gli archi della forma st, dove s e t stanno in $\{s_1, \ldots, s_k, {s_1}^{-1}, \ldots, {s_k}^{-1}\}$, che sono $4k^2$ archi, ma di questi almeno la metà sono inversi di archi già presenti, quindi basta prendere un insieme di al massimo $2k^2 + k$ generatori per ottenere il ciclo hamiltoniano desiderato. □

Poichè per ogni gruppo finito G si ha $d(G) \leq \log_2 |G|$, discende in modo più breve, grazie al Teorema 2.7, una variante del risultato riguardo ad un insieme di generatori piccolo che induce grafo hamiltoniano: in questo caso, è infatti:

$$|S| \leq 2\log_2^2 |G| + \log_2 |G| = O(\log_2^2 |G|).$$

Ricordiamo il seguente risultato, fulcro dell'articolo [**24**] di Wiegold.

Teorema 2.8. *Sia S gruppo semplice finito non abeliano. Allora, vale:*

$$d(S^\lambda) \leq \log_{|S|} \lambda + 2.$$

In particolare, si ha:

Corollario 2.2. *Sia $G = S_1 \times \cdots \times S_t$, con S_i gruppo semplice finito non abeliano per ogni i. Allora, vale $d(G) \leq log_{60} t + 2$.*

Dim. Alcuni degli S_i potrebbero essere isomorfi. Scriviamo quindi $G \cong T_1^{n_1} \times \cdots \times T_m^{n_m}$, con $n_1 \leq \cdots \leq n_m$, $n_1 + \cdots + n_m = t$, e i T_i non isomorfi a due a due. Per il Teorema 2.8 e per la Proposizione 2.3, si ha:

$$d(G) = max\{\log_{|T_1|} n_1 + 2, \ldots, \log_{|T_m|} n_m + 2\} \leq \log_{60} n_m + 2,$$

essendo A_5, di ordine 60, il più piccolo gruppo semplice non abeliano. In particolare, essendo $n_m \leq t$, segue la tesi. □

Prima di mostrare il risultato asintotico, ricordiamo l'ultimo fatto di cui ci serviremo, ([**7**], Teorema 1).

Teorema 2.9. *Sia G gruppo finito. Se $Soc(G) = S_1 \times \cdots \times S_m$, con S_i semplice non abeliano $\forall i$, allora $d(G) \leq 3m$.*

Possiamo finalmente enunciare e dimostrare la stima asintotica per il minimo numero di buoni generatori per un gruppo G.

Teorema 2.10. *Per ogni $\alpha \in]0,1[$, esiste c_α tale che dato un gruppo G, $Cay(G,S)$ possiede un cammino hamiltoniano per un certo insieme di generatori S di G tale che $|S| \leq r + \alpha m + c_\alpha$, dove r e m sono i numeri dei fattori rispettivamente abeliani e*

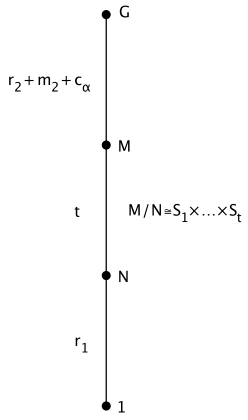

Figura 2.3. La serie subnormale come nel Teorema 2.10.

non abeliani della serie di composizione di G. Inoltre, per $\alpha \to 0$, si ha $c_\alpha = O(\frac{1}{\alpha^{2+\epsilon}})$ per ogni $\epsilon > 0$.

Dim. Sia $N = R(G)$, e sia M il sottogruppo normale di G tale che $M/R(G) = Soc(G/R(G))$. Procediamo per induzione sull'ordine di G. $R(G)$ possiede r_1 fattori di composizione abeliani, con $r = r_1 + r_2$ per un certo r_2. Il quoziente M/N è invece un prodotto diretto di t gruppi semplici non abeliani, siano essi S_i, $i = 1, \ldots, t$, con $m = t + m_2$ per un certo m_2.

In G/M per induzione troviamo un insieme di generatori di ordine $r_2 + m_2 + c_\alpha$ tale che il rispettivo grafo di Cayley su G/M possiede un cammino hamiltoniano. Su $R(G)$, composto da r_1 fattori ciclici, è chiaro che si trova un cammino hamiltoniano grazie a r_1 generatori. Vediamo invece cosa succede nel quoziente M/N. Per il Corollario 2.2, si ha che $d(M/N) \leq \log_{60} t + 2$. Per il Teorema 2.7, nel quadrato del grafo troviamo sempre un ciclo, in particolare un cammino hamiltoniano: otteniamo quindi un insieme di $2\log_{60}^2 t + 9\log_{60} t + 10$ generatori che forniscono un ciclo, in particolare un cammino hamiltoniano a M/N.

Vi sono due casi che andiamo ad esaminare:

- $2\log_{60}^2 t + 9\log_{60} t + 10 \leq \alpha t$. In questo caso, M/N ha αt generatori che garantiscono la presenza di un cammino hamiltoniano. Risalendo dai quozienti, alla fine troviamo che G ha un cammino hamiltoniano grazie a un insieme di generatori di cardinalità:

$$r_1 + \alpha t + r_2 + \alpha m_2 + c_\alpha = r + \alpha m + c_\alpha.$$

- $\alpha t < 2\log_{60}^2 t + 9\log_{60} t + 10$. Sia $f(t) = \frac{2\log_{60}^2 t + 9\log_{60} t + 10}{t}$: essa è una funzione monotona decrescente, dunque dire $\alpha < f(t)$ equivale a dire $t < h(\alpha)$, con h inversa di f. Per il Teorema 2.9, abbiamo che tutto il quoziente G/N è generato da al massimo $3t$ elementi, quindi possiede un insieme di generatori di ordine al massimo $18t^2+3t < 18h(\alpha)^2+3h(\alpha)$ che danno un cammino hamiltoniano a G/N. A questo punto, basta porre $c_\alpha = 18h(\alpha)^2+3h(\alpha)$, e risalendo da N e G/N troviamo anche in questo caso un cammino hamiltoniano per G con $r_1 + c_\alpha \leq r + \alpha m + c_\alpha$ generatori.

Per $x \to +\infty$, la funzione $f(x)$ è maggiorata da $\frac{1}{x^{1-\delta}}$ per ogni $\delta > 0$, dunque la stessa cosa succede invertendo le funzioni e andando per $x \to 0$: in un tale intorno si ha $h(x)$ maggiorata da $\frac{1}{x^{1+\delta'}}$, dove $\delta' = \frac{\delta}{1-\delta}$, dunque $c_\alpha = O(\frac{1}{\alpha^{2+\epsilon}})$ per ogni $\epsilon > 0$. □

Si noti che per $\alpha = \frac{1}{2}$, si ha che $h(\alpha) = 40$, dunque $c_\alpha = 28920$, mentre per $\alpha = 1$ si ha $c_\alpha = 5253$.

Ringraziamenti

Il primo dei miei ringraziamenti va senza dubbio al mio relatore, il professor Andrea Lucchini, il quale mi ha introdotto all'argomento oggetto di questa tesi, mi ha sempre seguito da vicino e in modo attento, mi ha positivamente spronato e indirizzato verso le migliori strade, e mi ha presentato ogni approccio interessante possibile alla materia. Lo ringrazio di profondo cuore per la sua supervisione. Ringrazio assieme a lui anche la professoressa Eloisa Detomi per aver accettato a farmi da controrelatrice, e per essersi presa cura di leggere interamente la mia tesi, portando alla mia attenzione fondamentali osservazioni senza le quali questo lavoro non sarebbe tale.

Ringrazio la mia famiglia, mia mamma Patrizia, mio papà Giuseppe, e mio fratello Andrea, per avermi sostenuto dall'inizio della mia carriera universitaria fino al completamento di questo lavoro, almeno. Assieme a loro ringrazio mio zio Roberto e mia nonna Wilma, e chiaramente anche la mia ragazza, Giulia, che mi sopporta già da diversi anni e che è riuscita a farlo una volta in più anche nei miei momenti più stressanti e di alienazione. Ringrazio i miei amici, in particolare il mio migliore amico Simone, e i miei amici Casellani - troppi per citarli, ma loro lo sanno - per avermi distratto nei momenti giusti. E sostenuto sempre.

Alla facoltà di Matematica ho trovato un ambiente stupendo dal punto di vista culturale. Ringrazio sentitamente tutti i miei colleghi universitari. Ho qualche nome in particolare: Jacopo, ovvero Ska, per la sua genialità e il suo modo di vedere la geometria, oltre che la sua psichedelia; Dino, alias Sfaccimm', per la serenità e allo stesso tempo l'intelligenza con cui ha intrapreso questi studi, assieme ad Andrea e a Simone, ovvero il Tonno; la Mima, solare ragazza che mi ha prestato gli appunti necessari al momento del bisogno; e poi gli altri miei compagni di studi nei vari esami,

come Gasta, cioè il fisico-matematico mio amico di sempre, Boa, analista dalle grandi idee, e poi Aldo, il Bene, il categorico Fosco, Marianno, e tanti altri.

Ho avuto tanti momenti di meditazione su questa tesi. Devo ringraziare anche qualche musicista, ovvero i Tool, i Pink Floyd, gli Area, in particolare il grande, indimenticato Demetrio, Fred V e Grafix, Ryuichi Sakamoto, i Sensorium, Noisia, i Soundgarden, gli Isis, Netsky, i Transatlantic, Amon Tobin, i Neurosis, Camo e Krooked, i The Tangent, e anche Skrillex, per essermi rimbalzati in testa fra un teorema e l'altro, e avermi dato la carica necessaria ad essere produttivo. Senza troppo illudermi.

Infine, ma questo è il capoverso più sentito, ringrazio l'Università di Padova tutta. Grazie a tutto il corpo docente e ai segretari della facoltà di Matematica - di cui non ho nemmeno un lamento, nemmeno uno - e grazie alle varie esperienze che ho potuto sperimentare grazie alla mia Università, come quella davvero formativa delle 150 ore, e quella indimenticabile del tutorato, sono cresciuto veramente, e sono stato valorizzato come prima di cinque anni fa non credevo fosse possibile. Spero che un giorno tutto quello che questa Università ha dato ai suoi studenti, in particolare la facoltà di Matematica, venga ad essa reso, basterebbe in egual misura. E i miei compagni di corso sanno di cosa sto parlando. Sentirete un giorno parlare di qualcuno di loro. O di noi. Chissà.

Bibliografia

[1] B. Alspach, C. C. Chen, M. Dean, *Hamilton paths in Cayley graphs on generalized dihedral groups*, Ars. Math. Comtemp. 3 (2010) 29-47.

[2] B. Alspach, C. Q. Zhang, *Hamiltonian cycles in cubic Cayley graphs on dihedral groups*, Ars Combin. 28 (1989) 101-108.

[3] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *The ATLAS of finite groups* (1985)

[4] M. D. E. Conder, *Generators for alternating and symmetric groups*, J. London Math. Soc. 22 (1980) 75–86.

[5] S. J. Curran, *Hamilton cycles in Cayley digraphs on abelian and dihedral groups*, Congr. Numer. 165 (2003) 77-97.

[6] S. J Curran, J. A. Gallian, *Hamiltonian cycles and paths in Cayley graphs and digraphs - A survey*, Discrete Math. 156 (1996) 1-18.

[7] F. Dalla Volta, A. Lucchini, *Minimal number of generators and composition length of socle in finite groups*, Quart. J. Math. Oxford Ser. 47 (1996) 157-163.

[8] L. Di Martino, N. Vavilov, $(2,3)$-*generation of* $SL(n,q)$*, cases* $n = 5, 6, 7$, Comm. Algebra 22 (1994) 1321-1347.

[9] M. J. Evans, *A note on two-generator groups*, Rocky Mountain Journal of Mathematics 17 (1987) 887-889.

[10] H. Fleischner, *The square of every two-connected graph is hamiltonian*, Journal of Combinatorial Theory 16 (1974) 29-34.

[11] R. Guralnick, W. Kantor, *Probabilistic generation of finite simple groups*, Journal of Algebra 234 (2000) 743-792.

[12] R. Guralnick, G.Malle, *Product of conjugacy classes and fixed point spaces*, J. Amer. Math. Soc. 25 (2012) 77-121.

[13] D. Gorenstein, *Finite Simple Groups: An Introduction to Their classification* (1985).

[14] D. Jungreis, E. Friedman, D. Witte, *Cayley graphs on groups of low order are hamiltonian*, Preprint.

[15] K. Keating, D. Witte, *On Hamilton cycles in Cayley graphs in groups with cyclic commutator subgroup*, Cycles in Graphs (1985) 89-102.

[16] K. Kutnar, D. Marusic, D. Morris, J. Morris, P. Sparl, *Hamiltonian cycles in Cayley graphs whose order has few prime factors*, Ars Math. Contemp. 5 (2012) 27-71.

[17] D. X. Li, *Hamiltonian circuits in Cayley digraphs on cyclic groups*, Journal of Southwest China Normal University 28 (2003) 687-689.

[18] A. Lucchini, $(2, 3, k)$*-generated groups of large rank*, Arch. Math. 73 (1999) 241-248.

[19] G. Malle, *Small rank exceptional Hurwitz groups*, Groups of Lie type and their geometries (1995) 173-184.

[20] D. Morris, *Odd-order Cayley graphs with commutator subgroup of order pq are hamiltonian*, Preprint (2012).

[21] I. Pak, R. Radoicic, *Hamiltonian paths in Cayley graphs*, Disc. Math. 309 (2009) 5501-5508.

[22] A. Stein, $1\frac{1}{2}$*-Generation of Finite Simple Groups*, Contributions to Algebra and Geometry 39 (1998) 349-358.

[23] M. C. Tamburini, M. Vsemirnov, *Hurwitz groups and Hurwitz generation*, Handbook of algebra 4 (2006) 385-426.

[24] J. Wiegold, *Growth sequences of finite groups IV*, J. Austral. Math. Soc. 29 (1980) 14-16.

[25] D. Witte, *Cayley digraphs of prime-power order are Hamiltonian*, J. Combin. Theory 40 (1986) 107-112.

[26] H. Yamaki, *The order of a group of even order*, Proc. Am. Math. Soc. 136 (2008) 397-402.