Progressioni aritmetiche nei sottoinsiemi dei naturali

Maurizio Monge

20 settembre 2008

L'obiettivo di queste note è quello di proporre alcuni risultati classici sull'esistenza (e non esistenza) di progressioni aritmetiche nei sottoinsiemi dei naturali.

1 Introduzione

Per ogni $a \leq b$, indicheremo per comodità con $[a,b]$ l'intervallo di interi $\{a, a+1, \ldots, b-1, b\}$. Sarà inolte importante tenere conto della seguente definizione

Definizione 1.1. Sia $A \subseteq \mathbb{N}$ un sottoinsieme dei naturali. Chiameremo *densità superiore* la quantità

$$\delta(A) = \limsup_{N\to\infty} \frac{\left|A \cap [1,N]\right|}{N}.$$

La densità superiore è una generalizzazione della *densità asintotica*, definita come sopra ma in cui si pretende che esista il limite al posto del limite superiore. Questa definizione permette di lavorare con insiemi che non soddisfino la condizione stringente di possedere una densità asintotica.

Possiamo ora enunciare il risultato principale sull'esistenza di progressioni aritmetiche nei sottoinsiemi dei naturali, che è senz'altro il *teorema di Szemerédi*. Questo teorema dà una risposta affermativa ad una congettura di Erdős e Turán del 1936:

Teorema 1.2 (Szemerédi, 1975)**.** *Sia $A \subseteq \mathbb{N}$ un sottoinsieme dei naturali con densità superiore positiva $\delta(A) = \delta > 0$. Allora per ogni $k \in \mathbb{N}$, A contiene una progressione aritmetica $a, a+r, \ldots, a+r(k-1)$ non banale (ovvero con $r > 0$) di lunghezza k.*

Ciò che rende questo risultato sorprendente è che molti altri schemi sono assai più facili da eliminare dai sottoinsiemi dei naturali, come succede ad esempio con le progressioni geometriche a, ar, ar^2 (non banali, ovvero con $r > 1$). Ci basta infatti considerare i numeri liberi da quadrati per renderci conto che l'analogo per le progressioni geometriche non può essere vero: essi infatti non possono contenere progressioni geometriche di lunghezza tre e hanno densità asintotica

$$\delta = \prod_{p\in\Pi} \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Si noti che se è vero il teorema di Szemerédi come sopra enunciato, esso deve essere forzatamente vero in una versione quantitativa e apparentemente più forte, ovvero per

ogni $\delta > 0$ e k intero positivo, deve esistere un N tale che ogni sottoinsieme di $[1,N]$ contenente almeno δN elementi ha almeno una progressione aritmetica di lunghezza k.

Diamo per buono il teorema di Szemerédi, e fissando $\delta > 0$ e $k \geq 3$, supponiamo infatti per assurdo che sia possibile trovare per N arbitrariamente grande degli insiemi $A_N \subseteq [1,N]$ di cardinalità $\geq \delta N$ senza progressioni aritmetiche lunghe k.

Prendiamo quindi una successione di interi positivi $(N_i)_{i\geq 1}$ tali che $N_{i+1} \geq 4N_i$ per cui esistano degli $A_{N_i} \subseteq [1,N_i]$ di cardinalità almeno δN_i senza progressioni lunghe k.

Costruiamo allora un sottoinsieme di $\mathbb{N}$ nel seguente modo: partendo da 1, al passo i-esimo lasciamo un intervallo vuoto lungo $3N_i$ e mettiamo una copia di traslata di A_{N_i}, e così via per tutti gli $i = 1,2,\ldots$:

$$B = \bigcup_{i=1}^{\infty} \left[\left(4 \cdot \sum_{k=1}^{i-1} N_k + 3N_i \right) + A_{N_i} \right].$$

In questo modo otteniamo un sottoinsieme $B \subseteq \mathbb{N}$ che ha densità superiore almeno $\delta/4$, ed è possibile che osservare che ogni sua progressione aritmetica di lunghezza k è interamente contenuta in uno degli A_{N_i} con cui è stato costruito.

Ma essendo gli A_{N_i} liberi di progressioni aritmetiche lunghe k otteniamo un assurdo grazie al teorema di Szemerédi. E quindi deve esistere un N tale che ogni sottoinsieme di $[1,N]$ di cardinalità almeno δN contiene progressioni aritmetiche di lunghezza k.

Abbiamo quindi dimostrato che nel teorema di Szemerédi è possibile rimpiazzare la densità superiore con la *densità superiore di Banach*, ovvero la quantità

$$\delta^*(A) = \limsup_{N-M\to\infty} \frac{\left|A \cap [M,N]\right|}{N-M},$$

perché un insieme $A \subseteq \mathbb{N}$ ha densità superiore di Banach almeno δ^* precisamente quando esistono intervalli $[M,N] \subseteq \mathbb{N}$ arbitrariamente ampi in cui A ha densità almeno δ^*. Il teorema di Szemerédi viene talvolta enunciato in questa forma.

Il discorso appena fatto ci fa notare che ha senso cercare di ottenere dalle dimostrazioni del teorema di Szemerédi delle stime 'buone' per questo N.

Storicamente, uno dei primi risultati nello studio delle progressioni aritmetiche nei sottoinsiemi dei naturali fu il *teorema di van der Waerden*, che data qualunque colorazione dei naturali con un numero finito di colori, m poniamo, stabilisce l'esistenza di progressioni arbitrariamente lunghe monocromatiche.

Chiaramente se associamo ad ogni colore un numero in $[1,m]$, allora una colorazione corrisponde a una funzione $f : \mathbb{N} \to [1,m]$. Possiamo quindi dare l'enunciato preciso del teorema:

Teorema 1.3 (van der Waerden, 1927)**.** *Sia $c : \mathbb{N} \to [1,m]$ una 'colorazione' dei naturali con m colori, m un qualunque intero positivo. Allora esistono progressioni aritmetiche monocromatiche non banali arbitrariamente lunghe (ovvero per ogni $k \geq 1$, esistono $a, a+r, \ldots, a+r(k-1) \in \mathbb{N}$ con $c(a) = c(a+r) = \cdots = c(a+r(k-1))$ e $r > 0$).*

L'elegante dimostrazione di questo teorema verrà esposta più avanti in queste note.

Si noti che per ogni colorazione con m colori deve esistere almeno un colore x tale che i numeri del colore x

$$\left\{ n \in \mathbb{N} : c(n) = x \right\}$$

hanno densità superire almeno $1/m$, quindi il teorema di van der Waerden può essere visto come un indebolimento del teorema di Szemerédi.

Ma differenza di quanto possa sembrare, il teorema di Szemerédi è un risultato molto più difficile del teorema di van der Waerden, e già il caso per $k = 3$, ovvero il problema di stabilire l'esistenza di progressioni aritmetiche di lunghezza tre, presenta notevoli difficoltà.

Storicamente fu necessario infatti attendere fino al 1953 per vedere la dimostrazione di Roth del caso per $k = 3$ utilizzando l'analisi di Fourier, mentre le dimostrazioni prima per $k = 4$ e poi in completa generalità furono successivamente fornite da Szemerédi che trasformò il problema in un problema di regolarità di grafi.

Può essere interessante sapere che altre dimostrazioni del caso generale sono state successivamente date da Furstenberg (utilizzando tecniche di teoria ergodica, in particolare il teorema di ricorrenza di Furstenberg che è una generalizzazione del teorema di ricorrenza di Poincaré), Gowers (utilizzando l'analisi di Fourier, e questa è la dimostrazione che fornisce le stime quantitative migliori attualmente note), più un'altra dimostrazione di Gowers e altri utilizzando teoremi di regolarità di ipergrafi.

In un'altra congettura molto più forte di Erdős e Turán, si ipotizzava che per ogni k esistesse un $\varepsilon > 0$ tale che per N sufficientemente grande ogni sottoinsieme di $[1,N]$ di cardinalità almeno $N^{1-\varepsilon}$ dovesse contenere progressioni aritmetiche di lunghezza k.

La motivazione che stava dietro questa ipotesi era il problema di dimostrare l'esistenza di progressioni aritmetiche arbitrariamente lunghe di numeri primi (questo seguirebbe infatti immediatamente dalla congettura se fosse vera, grazie al teorema dei numeri primi).

L'esistenza di progressioni aritmetiche arbitrariamente lunghe fra i primi è stata cionondimeno stabilita nel 2004, quando è stato annunciato il

Teorema 1.4 (Green-Tao, 2004)**.** *I numeri primi contengono progressioni aritmetiche arbitrariamente lunghe.*

Per dimostrare questo risultato (molto difficile), Green e Tao hanno definito un opportuno concetto di *pseudocasualità* sui sottoinsiemi dei naturali, dimostrato che un sottoinsieme di un insieme pseudocasuale con densità relativa positiva contiene progressioni aritmetiche arbitrariamente lunghe, e applicato questo ragionamento a un opportuno sottoinsieme pseudocasuale dei naturali in cui i primi hanno ancora densità relativa positiva.

2 L'esempio di Behrend

Tornando alla seconda congettura di Erdős e Turán, essa risultò essere falsa anche nel caso $k = 3$, e il controesempio fu fornito da Salem e Spencer nel 1942.

Presentiamo qua il controesempio di Behrend, che fornisce la migliore costruzione di sottoinsiemi dei naturali liberi da progressioni aritmetiche attualmente nota.

Teorema 2.1 (Behrend)**.** *Sia N un intero sufficientemente grande, allora esiste un sottoinsieme $A \subseteq [0,N-1]$ di cardinalità almeno $N\exp(-C\sqrt{\log N})$, dove C è una costante assoluta, che non contiene progressioni aritmetiche di lunghezza tre.*

Dimostrazione. La dimostrazione si basa sull'osservazione geometrica che una retta (in $\mathbb{R}^n$) può intersecare una sfera in al più due punti.

Più precisamente, definendo una progressione aritmetica lunga k in $\mathbb{Z}^n$ come una tupla $a, a+r, \ldots, a+(k-1)r$ per $a, r \in \mathbb{Z}^n$, $r \neq (0,\ldots,0)$, ci serve notare che l'insieme

$$\Big\{x \in \mathbb{Z}^n : |x|^2 = D\Big\}.$$

non può contenere progressioni aritmetiche di lunghezza tre in $\mathbb{Z}^n$, per ogni $n \geq 1$.

Per trasporre questo esempio in un intervallo di naturali $[0, N-1]$, siano n e M interi positivi che determineremo a posteriori, e consideriamo

$$S(D) = \Big\{x \in [0, M-1]^n : x_1^2 + \cdots + x_n^2 = D\Big\}.$$

Al variare di D in $[0, n(M-1)^2]$ questi insiemi sono tutti distinti e ricoprono il cubo $[0, M-1]^n \subseteq \mathbb{Z}^n$, e quindi per il principio dei cassetti deve esistere un $R \in [0, n(M-1)^2]$, tale che $S = S(R)$ ha cardinalità almeno

$$|S| \geq \frac{M^n}{n(M-1)^2+1} \geq \frac{M^{n-2}}{n}.$$

Mandiamo ora S in $\mathbb{N}_0$ tramite la mappa

$$P(x) = P(x_1, \ldots, x_n) = \sum_{k=1}^{n} x_k (2M)^{k-1}.$$

Possiamo notare facilmente che:

1. P è biunivoca,
2. se $P(x) + P(y) = 2P(z)$, allora $x + y = 2z$,
3. $P(x) \leq M(2M)^{n-1}$ per ogni $x \in S$,

queste affermazioni sono infatti ovvie se si nota che $P(x)$ è precisamente il numero intero che ha gli $x_1, \ldots, x_n$ come cifre quando scritto in base $2M$, e che ciascuna cifra è compresa fra 0 e $M-1$ (e quindi ad esempio nell'addizione $P(x) + P(Y)$ non ci sono 'riporti').

Se prendiamo ora $n = \lfloor \sqrt{\log N} \rfloor$ e $M = \lfloor \frac{N^{1/n}}{2} \rfloor$, allora $P(S)$ è un sottoinsieme di $[0, N-1]$ che non contiene progressioni aritmetiche di lunghezza 3. Inoltre $P(S)$ ha cardinalità almeno (siccome $M = \lfloor \frac{N^{1/n}}{2} \rfloor \geq \frac{N^{1/n}}{4}$ per N abbastanza grande)

$$\begin{aligned} |P(S)| = |S| &\geq \frac{M^{n-2}}{n} \\ &\geq \frac{N^{1-2/n}}{n4^n} \\ &\geq N \exp(-\log n - 2n \log 2 - \frac{2}{n} \log N) \\ &\geq N \exp(-C\sqrt{\log N}). \end{aligned}$$

□

3 Il teorema di Roth

Ritornando invece ai risultati positivi, anche le dimostrazioni del teorema di Szemerédi più corte richiedono un certo lavoro. Presentiamo qui la dimostrazione del teorema di Roth, ovvero la versione ridotta con $k = 3$, che utilizza la trasformata di Fourier discreta e fornisce stime quantitative abbastanza buone.

Teorema 3.1 (Roth)**.** *Sia $\delta > 0$, e $N \geq \exp\exp(C\delta^{-1})$, con C costante assoluta. Allora ogni sottoinsieme $A \subseteq [1,N]$ tale che $|A| \geq \delta N$ contiene una progressione aritmetica (non banale) di lunghezza tre.*

A meno di passare a un δ più grande, per N grande fissato supporremo di avere precisamente $|A| = \delta N$.

3.2 Analisi di Fourier su $\mathbb{Z}$

Sia $f : \mathbb{Z} \to \mathbb{C}$ tale che $\sum_{n\in\mathbb{Z}} |f(n)| < \infty$, definiamo la sua *trasformata di Fourier* come

$$\hat{f}(\alpha) \;=\; \sum_{n\in\mathbb{Z}} e^{-2\pi i n\alpha}.$$

L'ipotesi su f di assoluta sommabilità garantisce che la serie infinita che definisce $\hat{f}$ converge uniformemente, e quindi $\hat{f}$ è una funzione continua sul toro $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ (o periodica su $\mathbb{R}$). Sotto queste ipotesi la formula di inversione di Fourier e l'identità di Plancherel sono conseguenze immediate della familiare

$$\int_{\mathbb{T}} e^{2\pi i n\alpha} \mathrm{d}\alpha \;=\; \begin{cases} 1 & \text{se } n = 0, \\ 0 & \text{per qualunque altro } n \text{ intero.} \end{cases}$$

Grazie a questa formula seguono infatti immediatamente, usando la convergenza uniforme della serie che definisce $\hat{f}$,

- la formula di inversione di Fourier

$$f(n) \;=\; \int_{\mathbb{T}} \hat{f}(\alpha) e^{2\pi i n\alpha} \mathrm{d}\alpha,$$

- l'identità di Plancherel

$$\int_{\mathbb{T}} |\hat{f}(\alpha)|^2 \mathrm{d}\alpha \;=\; \sum_{n\in\mathbb{Z}} |f(n)|^2,$$

- e la stima della norma L^∞ della trasformata con la norma L^1 di f

$$|\hat{f}(\alpha)| \;\leq\; \sum_{n\in\mathbb{Z}} |f(n)|, \qquad \text{per ogni } \alpha \in \mathbb{T}.$$

3.3 Dimostrazione del teorema di Roth

Introduciamo la forma trilineare

$$\begin{aligned} \Lambda_3(f,g,h) &= \sum_{a,r\in\mathbb{Z}} f(a)g(a+r)h(a+2r) \\ &= \int_{\mathbb{T}} \hat{f}(\alpha)\hat{g}(-2\alpha)\hat{h}(\alpha)\mathrm{d}\alpha, \end{aligned}$$

dove la seconda scrittura si dimostra immediatamente essere uguale alla prima, perché

$$\begin{aligned}\int_{\mathbb{T}} \hat{f}(\alpha)\hat{g}(-2\alpha)\hat{h}(\alpha)\mathrm{d}\alpha &= \int_{\mathbb{T}} \sum_{t,u,v\in\mathbb{Z}} f(t)e^{-2\pi it\alpha}g(u)e^{-2\pi iu(-2\alpha)}h(v)e^{-2\pi iv\alpha}\mathrm{d}\alpha \\ &= \int_{\mathbb{T}} \sum_{\substack{t,u,v\in\mathbb{Z}\\ t-2u+v=0}} f(t)g(u)h(v)\mathrm{d}\alpha \\ &= \sum_{\substack{t,u,v\in\mathbb{Z}\\ t-2u+v=0}} f(t)g(u)h(v) \\ &= \sum_{a,r\in\mathbb{Z}} f(a)g(a+r)h(a+2r).\end{aligned}$$

L'importanza di questa definizione nasce dal fatto che $\Lambda_3(1_A,1_A,1_A)$ risulta essere uguale al numero di progressioni aritmetiche di lunghezza tre in A (incluse le δN progressioni banali, dove $r=0$). Per provare il teorema di Roth è quindi sufficiente mostrare che

$$\Lambda_3(1_A,1_A,1_A) > \delta N.$$

Siccome per motivi tecnici conviene usare funzioni con valore medio zero, diamo la

Definizione 3.4 (funzione bilanciata)**.** Diciamo che la *funzione bilanciata* di A è

$$\phi_A \;=\; 1_A - \delta 1_{[1,N]}.$$

Poiché A ha densià δ in $[1,N]$ abbiamo chiaramente che $\sum \phi_A(n) = 0$. Espandendo ora il secondo argomento di Λ_3 come $\delta 1_{[1,N]} + \phi_A$ otteniamo

$$\Lambda_3(1_A,1_A,1_A) \;=\; \delta \sum_{n,d\in\mathbb{Z}} 1_A(n)1_A(n+2d) + \Lambda_3(1_A,\phi_A,1_A), \tag{1}$$

e notiamo, considerando i sottoinsiemi degli elementi pari e dispari di A, che

$$\frac{|A|^2}{2} \le \sum_{n,d\in\mathbb{Z}} 1_A(n)1_A(n+2d) \le |A|^2.$$

Il termine principale nella (1) diventa quindi circa $\delta^3 N^2$ (e almeno $\frac{\delta^3 N^2}{2}$), che è anche il numero di progressioni aritmetiche lunghe tre che ci aspetteremmo di trovare in A se esso fosse un sottoinsieme casuale di $[1,N]$, ottenuto prendendo ogni numero con probabilità δ. Questa osservazione motiva la

Definizione 3.5 (ε-uniformità)**.** Diciamo che l'insieme A è *ε-uniforme* se

$$\sup_{\alpha\in\mathbb{T}} \left|\widehat{\phi_A}(\alpha)\right| \le \varepsilon N.$$

Lemma 3.6 (Uniformità $\Rightarrow$ Come se fosse casuale)**.** *Se A è ε-uniforme per $\varepsilon = \frac{\delta^2}{4}$, allora $\Lambda_3(1_A,1_A,1_A) \ge \frac{\delta^3 N^2}{4}$ (si noti che $\frac{\delta^3 N^2}{4} > \delta N$ ad esempio se $N \ge \frac{8}{\delta^2}$).*

Dimostrazione. E' sufficiente mostrare che sotto questa ipotesi di regolarità il termine $\Lambda_3(1_A,\phi_A,1_A)$ è realmente un termine di errore che soddisfa la stima

$$\Lambda_3(1_A,\phi_A,1_A) \le \frac{\delta^3 N^2}{4}.$$

Ma questa stima segue immediatamente dall'identità di Plancherel, poiché:

$$\begin{aligned}\big|\Lambda_3(1_A,\phi_A,1_A)\big| &\le \sup_{\alpha\in\mathbb{T}}\big|\widehat{\phi_A}(\alpha)\big|\cdot\int_0^1|\widehat{1_A}(\alpha)^2|\mathrm{d}\alpha\\ &\le \varepsilon N\cdot\delta N\\ &\le \frac{\delta^3N^2}{4}.\end{aligned}$$

□

Il cuore della dimostrazione del teorema di Roth è ora costituito dal seguente risultato:

Lemma 3.7 (Mancanza di uniformità ⇒ Struttura additiva)**.** *Se A non è ε-uniforme, allora esiste una progressione aritmetica P lunga almeno $L=\lfloor\sqrt{\frac{\varepsilon N}{64\pi}}\rfloor$ tale che*

$$|A\cap P|>(\delta+\varepsilon/8)|P|.$$

Dimostrazione. Supponiamo di avere che

$$\big|A\cap P\big|\le(\delta+\varepsilon/8)\big|P\big| \tag{2}$$

per ogni progressione aritmetica P di lunghezza $\ge L$, e prendiamo un arbitrario numero reale $\alpha\in[0,1)$. Allora per principio di Dirichlet di approssimazione diofantea esiste un naturale q, $1\le q\le 4\pi L$, tale che, se indichiamo con $\|x\|$ la distanza di x dal più vicino intero, valga $\|q\alpha\|\le\frac{1}{4\pi L}$. Definendo ora l'insieme P_0 come la progressione aritmetica di L elementi

$$P_0 \;=\; \Big\{q\ell,\quad \text{per } \ell=1,2,\dots,L\Big\},$$

possiamo vedere che siccome $2\pi\|q\ell\alpha\|\le\frac12\le\frac{\pi}{6}$ per ogni $\ell=1,2,\dots,L$, allora

$$\Re\big(e^{-2\pi i\ell q\alpha}\big)\ge\frac12\qquad\text{per ogni }\ell=1,2,\dots,L,$$

e quindi

$$\big|\widehat{1_{P_0}}(\alpha)\big|\;\ge\;\frac{L}{2}.$$

Siccome ϕ_A ha valore medio zero, abbiamo che anche $\phi_A*1_{P_0}$, che è definita come

$$(\phi_A*1_{P_0})(n)=\sum_{m\in\mathbb{Z}}\phi_A(m)1_{P_0}(n-m),$$

ha valore medio zero. Quindi dato che per ogni funzione g a valori in $\mathbb{R}$ la sua parte positiva si può scrivere come $g^+=\frac{|g|+g}{2}$, segue che ponendo $g=\phi_A*1_{P_0}$ e facendo la media

$$\begin{aligned}\sum_{n\in\mathbb{Z}}(\phi_A*1_{P_0})^+(n) &= \frac12\sum_{n\in\mathbb{Z}}\big|(\phi_A*1_{P_0})(n)\big|\\ &\ge \frac12\big|\widehat{\phi_A}(\alpha)\widehat{1_{P_0}}(\alpha)\big|\\ &\ge \frac{L}{4}\big|\widehat{\phi_A}(\alpha)\big|.\end{aligned} \tag{3}$$

Ma abbiamo che

$$\begin{aligned}(\phi_A * 1_{P_0})(n) &= \sum_{\ell=1}^{L} \phi_A(n-\ell q) \\ &= \sum_{\ell=1}^{L} 1_A(n-\ell q) - \delta \sum_{\ell=1}^{L} 1_{[1,N]}(n-\ell q) \\ &= \big|A \cap P_n\big| - \delta \big|P_n \cap [1,N]\big|\end{aligned}$$

dove $P_n = n - P_0$. Dall'ultima uguaglianza otteniamo che se $P_n \subseteq [1,N]$, siccome stavamo supponendo che valga la (2), allora

$$\begin{aligned}(\phi_A * 1_{P_0})(n) &\leq (\delta + \frac{\varepsilon}{8})|P_n| - \delta|P_n| \\ &\leq \frac{\varepsilon L}{8},\end{aligned} \tag{4}$$

mentre nel caso cattivo in cui $P_n \nsubseteq [1,N]$ ci accontenteremo di dire che

$$(\phi_A * 1_{P_0})(n) \leq L. \tag{4'}$$

Notiamo anche che per tutti gli n tali che $A \cap P_n \neq \emptyset$ allora $P_n \subseteq [1,N]$ eccetto al più per $2Lq$ di essi, e quindi mettendo insieme le (4) e (4') segue, sapendo che i casi cattivi sono al più $2Lq$, che

$$\begin{aligned}\sum_{n\in\mathbb{Z}} (\phi_A * 1_{P_0})^+(n) &\leq N\frac{\varepsilon L}{8} + 2L^2 q \\ &\leq \frac{\varepsilon NL}{4},\end{aligned} \tag{5}$$

visto che avevamo scelto $L = \lfloor \sqrt{\frac{\varepsilon N}{64\pi}} \rfloor$ e $q \leq 4\pi L$. Mettendo insieme le (3) e (5) abbiamo quindi che $|\widehat{\phi_A}(\alpha)| \leq \varepsilon N$, e quindi che A è ε-uniforme visto che α era arbitrario. □

Possiamo ora concludere la

Dimostrazione del teorema di Roth. Supponiamo che A non contenga progressioni aritmetiche di lunghezza tre. Questa assunzione ci fornirà una contraddizione per N abbastanza grande.

Abbiamo dai lemmi che se A non contiene progressioni lunghe tre allora A non è ε-uniforme per $\varepsilon = \frac{\delta^2}{4}$, e quindi deve esistere una progressione P_1 di lunghezza almeno

$$N_1 \geq \Big\lfloor \sqrt{\frac{\delta^2 N}{256\pi}} \Big\rfloor \geq \sqrt{\frac{\delta^2 N}{1024\pi}}$$

tale che

$$|A \cap P_1| \geq \Big(\delta + \frac{\delta^2}{32}\Big)|P_1|,$$

cioè A ristretto a P_1 ha densità $\delta_1 \geq \delta + \frac{\delta^2}{32}$. Possiamo quindi restringerci a questa progressione P_1 e mapparla nell'insieme $[1,N_1]$, mentre $A \cap P_1$ viene mappato in un $A_1 \subseteq [1,N_1]$ di cardinalità $\delta_1 N_1$ che ancora non contiene progressioni di lunghezza tre.

Iterando questo argomento $\lceil \frac{32}{\delta} \rceil$ volte otteniamo un densità $\delta' \geq 2\delta$, e iterando altre $\lceil \frac{32}{\delta'} \rceil \leq \lceil \frac{32}{2\delta} \rceil$ volte arriviamo ad una densità di almeno 4δ, etc. In particolare se $2^\ell \geq \frac{1}{\delta}$, per arrivare alla densità 1 ci bastano

$$\begin{aligned} \lceil \frac{32}{\delta} \rceil + \lceil \frac{32}{2\delta} \rceil + \cdots + \lceil \frac{32}{2^\ell \delta} \rceil \leq & \frac{64}{\delta} + \ell + 1 \\ \leq & \frac{C_1}{\delta} \end{aligned}$$

passi. Otteniamo quindi un assurdo se dopo $k = \lceil \frac{C_1}{\delta} \rceil$ passi N_k contiene ancora almeno $\frac{8}{\delta^2}$ elementi. Ma

$$N_k \geq \frac{\delta^2 N^{2^{-k}}}{1024\pi},$$

quindi ci basta che

$$\frac{1}{2^k} \log N + 2\log\delta - \log 1024 - \log\pi \geq \log 8 - 2\log\delta,$$

ovvero

$$N \geq \exp\,\exp\Big(\frac{C}{\delta}\Big),$$

per N abbastanza grande e C costante assoluta. □

4 Il teorema di van der Waerden

Presentiamo in questa sezione la dimostrazione del teorema di van der Waerden. Il confronto della relativamente breve dimostrazione di questo teorema col lavoro necessario per dimostrare il teorema di Roth, ovvero Szemerédi per le progressioni aritmetiche di lunghezza tre, ci fa capire quanto più complicato sia quest'ultimo.

Teorema 4.1 (van der Waerden)**.** *Sia $c : \mathbb{N} \to [1,m]$ una 'colorazione' dei naturali con m colori, m un qualunque intero positivo. Allora esistono progressioni aritmetiche monocromatiche non banali arbitrariamente lunghe (ovvero per ogni $k \geq 1$, esistono $a, a+r, \ldots, a+r(k-1) \in \mathbb{N}$ con $c(a) = c(a+r) = \cdots = c(a+r(k-1))$ e $b > 0$).*

Purtroppo la dimostrazione che proponiamo non permette di fornire stime quantitative buone, e quelle che otterremo avranno crescita dell'ordine della funzione di Ackermann. E' curioso no tate che le stime quantitative migliori per van der Waerden si ottengono dal teorema di Szemerédi (e in particolare dalla dimostrazione di Gowers tramite l'analisi di Fourier).

Dimostrazione del toerema di van der Waerden. La dimostrazione si basa sul concetto di *ventola policromatica*, che definiamo ora. Useremo la notazione $[a,r,k]$ per denotare la progressione aritmetica $a, a+r, \ldots, a+r(k-1)$ di lunghezza k.

Definizione 4.2. sia $c : [1,N] \to [1,m]$ una colorazione dell'intervallo $[1,N]$ con m colori. Dati interi $k \geq 1$, $d \geq 0$ e $a \in [1,N]$ diciamo che una *ventola di raggio k, grado d e punto base a* è una d-tupla di progressioni aritmetiche $[a,r_1,k], [a,r_2,k], \ldots, [a,r_d,k]$ in $[1,N]$ di lunghezza k e punto base a, ed inoltre richiediamo che $r_i > 0$ per $i = 1,2,\ldots,d$. Le progressioni $[a+r_i, r_i, k-1]$, per $i = 1,2,\ldots,d$, saranno dette le *pale* della ventola. Diciamo che una ventola è *policromatica* se il suo punto base e le sue d pale sono tutte monocromatiche con $d+1$ colori distinti. In altre parole, esistono $c_0, c_1, \ldots, c_d$ colori distinti tali che $c(a) = c_0$ e $c(a+jr_i) = c_i$ per $i = 1,\ldots,d$ e $j = 1,\ldots,k$.

Possiamo ora iniziare la dimostrazione vera e propria, procedendo per induzione su k. Il teorema per $k = 1$ è ovvio, quindi possiamo supporre $k \geq 2$ e di aver già dimostrato il caso per $k-1$. Quindi, per ogni m esiste un intero positivo $N_{\text{vdW}}(k-1,m)$ tale che ogni m-colorazione dell'intervallo di interi $[1, N_{\text{vdW}}(k-1,m)]$ contiene una progressione aritmetica di lunghezza k.

Internamente al passo induttivo per il k in questione, ragioneremo ora per induzione sull'intero $d \geq 0$, dimostrando che vale la seguente

Asserzione. *Esiste un intero positivo $N_{\text{Fan}}(k,m,d)$ tale che ogni m-colorazione dell'intervallo $[1, N_{\text{Fan}}(k,m,d)]$ contiene*

1. *o una progressione aritmetica monocromatica di lunghezza k,*
2. *oppure una ventola policromatica di raggio k e grado d.*

Il passo $d = 0$ è banale, essendo una ventola di grado 0 costituita soltanto dal punto base, e inoltre non appena arriveremo a dimostrare il passo per $d = m$ saremo a posto, perché è impossibile con una m-colorazione avere una ventola di grado $\geq m$, e quindi dovrà forzatamente aversi l'esistenza di una progressione aritmetica di lunghezza k.

Assumiamo ora che $d > 1$ e di aver già dimostrato l'asserzione per $d-1$. Definiamo il numero che candiamo a essere $N = N_{\text{Fan}}(k,m,d)$ come $N = 2N_1N_2$, dove

$$N_1 \;=\; N_{\text{Fan}}(k,m,d-1), \qquad N_2 \;=\; N_{\text{vdW}}(k-1,(mN_1)^d).$$

Scriviamo ora la seconda metà dell'intervallo $[1,N]$ come l'unione di N_2 copie consecutive di intervalli lunghezza N_1:

$$[N_1N_2+1,N] \;=\; I_1 \cup I_2 \cup \cdots \cup I_{N_2}, \qquad \text{con } I_j \;=\; (N_2+j-1)N_1 + [1,N_1],$$

per $j = 1,2,\ldots,N_2$. Grazie all'ipotesi induttiva e alla scelta che abbiamo fatto di N_1, ciascun I_j contiene o una progressione monocromatica di lunghezza k, oppure una ventola policomatica

$$V_j \;=\; ([a_j, r_{j1}, k], [a_j, r_{j2}, k], \ldots [a_j, r_{j(d-1)}, k]),$$

di raggio k e grado $d-1$ con punto base e le pale di colori $c_{j0}, c_{j1}, \ldots, c_{j(d-1)}$. Se c'è almeno un j in cui si verifica la prima possibilità siamo a posto, per cui supponiamo che si verifichi sempre la seconda, per ogni $j = 1,\ldots,N_2$. Associamo ora alla ventola j-esima il suo 'tipo', ovvero la $2d$-tupla

$$(a_j \text{ rem } N_1, r_{j1}, \ldots, r_{j(d-1)}, c_{j0}, c_{j1}, \ldots, c_{j(d-1)}) \in [1,N_1]^d \times [1,m]^d.$$

Il tipo di una ventola quindi identifica univocamente la posizione del punto base rispetto all'inizio dell'intervallo I_j, le 'inclinazioni' delle pale e i colori del punto base e delle pale. Queste ventole possono avere $(mN_1)^d$ possibili tipi diversi, e quindi associare all'intervallo I_j il tipo della ventola V_j, per $j = 1,2,\ldots,N_2$, equivale a definire una colorazione dell'intervallo $[1,N_2]$ con $(mN_1)^d$ diversi colori. Ma per come avevamo definito N_2 possiamo ora trovare una progressione aritmetica di lunghezza $k-1$, e questo ci garantisce l'esistenza di $k-1$ ventole

$$V_{j_1}, V_{j_2}, \ldots, V_{j_{k-1}}$$

tutte dello stesso tipo e in progressione aritmetica. Si noti che ad esempio i punti base delle ventole $a_{j_1}, a_{j_2}, \ldots, a_{j_{k-1}}$ formano una progressione aritmetica di lunghezza $k-1$. Inoltre siccome le ventole si trovano tutte nella seconda metà dell'intervallo $[1,N]$, esiste un a tale che $a, a_{j_1}, a_{j_2}, \ldots, a_{j_{k-1}}$ è una progressione aritmetica. Consieriamo quindi la ventola definita dalle progressioni

$$[a, a_{j_1} - a, k], [a, a_{j_1} + r_{j_1 1} - a, k], [a, a_{j_1} + r_{j_1 2} - a, k], \ldots, [a, a_{j_1} + r_{j_1 (d-1)} - a, k].$$

Essa è una ventola di grado d e raggio k, e si noti inoltre che le pale sono tutte monocromatiche e di colori distinti. Infatti la prima pala ha come colore il colore (comune) dei punti base delle ventole $V_{j_1}, V_{j_2}, ...$, e come colore della n-esima pala il colore (comune) delle $(n-1)$-esime pale delle ventole $V_{j_1}, V_{j_2}, ...$, per $n = 2, \ldots, d$. Siccome tali ventole erano policomatiche per ipotesi, questi colori sono tutti distinti.

Consideriamo ora il colore del punto a. Se è uguale al colore di qualche pala, allora abbiamo trovato una progressione aritmetica monocromatica di lunghezza k, e siamo a posto. In caso contrario, abbiamo una ventola policromatica di grado d e raggio k, e questo conclude il passo induttivo su d. Siccome questo ci permette ora di passare a dimostrare l'esistenza progressioni monocromatiche o di ventole con $d+1$ pale, $d+2$, e così via, otteniamo la dimostrazione del passo induttivo del teorema non appena il numero di pale raggiunge il numero di colori. □

Riferimenti bibliografici

[Beh] Felix A. Behrend, *On the sets of integers which contain no three terms in arithmetical progression.*, Proc. Nat. Acad. Sci. **23** (1946), 331-332.

[Gow] T. Gowers, *A new proof of Szemerédi's theorem*, GAFA **11** (2001), 465-588.

[Rot] K.F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 245-252.

[Tao] T. Tao, *A quantitative ergodic theory proof of Szemerédi's theorem*, preprint.

[vdW] B.L. Van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw. Arch. Wisk. **15** (1927), 212-216.