Marco D'Anna

Semigruppi numerici e applicazioni

Catania - Marzo 2014

0. Definizioni e proprietà iniziali

Semigruppo (commutativo):
$(S, +)$, con $+$ operazione associativa (e commutativa).

Monoide (commutativo):
$(M, +)$, con $+$ operazione associativa (e commutativa) e $\exists$ 0.

Esempio. $\mathbb{N}^h$ è un monoide commutativo.

Definizione. $S \subseteq \mathbb{N}$ è detto semigruppo numerico se:
- sottomonoide di $(\mathbb{N}, +)$;
- $|\mathbb{N} \setminus S| < \infty$.

Definizione. Se $S \neq \mathbb{N}$, $\quad f(S) := \max(\mathbb{N} \setminus S)$
(numero di Frobenius)

Esempio. $S = \{0, 5, 7, 10, 12, 13, 14, 15, 17, \rightarrow\}$
Posso descrivere gli elementi del semigruppo in modo sintetico?

$5 \in S \ \Rightarrow \ n \cdot 5 \in S, \ \forall n \in \mathbb{N}$

$7 \in S \Rightarrow \ 7 + n \cdot 5 \in S, \ \forall n \in \mathbb{N}$ (osserviamo che $7 \equiv 2 \pmod 5$)

Vado avanti: $\forall i = 0, 1, 2, 3, 4$ prendo

$$\min\{s \in S \setminus \{0\} \mid s \equiv i \pmod 5\}$$

e ottengo $\{5, 21, 7, 13, 14\}$

$S = \{n \cdot 5\} \cup \{21 + n \cdot 5\} \cup \{7 + n \cdot 5\} \cup \{13 + n \cdot 5\} \cup \{14 + n \cdot 5\}$

Ma in S posso sommare tutti gli elementi tra loro; quindi

$S = \{n_1 \cdot 5 + n_2 \cdot 7 + n_3 \cdot 13 \mid n_i \in \mathbb{N}\} =: \langle 5, 7, 13 \rangle$

Proposizione. Ogni semigruppo numerico è finitamente generato ed ha un unico insieme minimale di generatori. □

$$S = \langle g_1, g_2, \ldots, g_k \rangle = \{ \sum_{i=1}^{n} n_i g_i \mid n_i \in \mathbb{N} \}.$$

Che proprietà devono avere i generatori perché S sia un semigruppo numerico (i.e. $|\mathbb{N} \setminus S| < \infty$)?

Teorema. $S = \langle g_1, g_2, \ldots, g_k \rangle$ s.n. $\Leftrightarrow$ MCD$(g_1, g_2, \ldots, g_k) = 1$.

Dimostrazione. ($\Rightarrow$) Ovvia.
($\Leftarrow$) Esercizio! (Sugg.: si usi l'identità di Bezout per trovare in S due elementi consecutivi; si utilizzi la divisione col resto per provare che, se $s, s+1 \in S$, allora, $\forall\ n \geq (s-1)s + (s-1)$, $n \in S$.)

1. Motivazioni

• Struttura semplice $\not\Rightarrow$ problemi semplici.

• Interazioni con vari campi della matematica:
- teoria dei numeri (problema di Frobenius, equazioni diofantee);
- combinatoria (contare numero di punti interi in un tetraedro);
- algebra commutativa (anelli locali o graduati uno-dimensionali);
- geometria algebrica (singolarità di curve, s. di Weierstrass);
- teoria dei codici (semigruppo di Weierstrass, ordered domains);
- programmazione lineare intera;
- problemi di fattorizzazione.

Interazioni in entrambi i versi: i s.n. possono essere uno strumento per risolvere problemi o ottenere informazioni in questi settori della matematica e problemi sui s.n. possono essere affrontati con strumenti presi da questi settori.

2. Problema di Frobenius

$S = \langle g_1, g_2, \ldots, g_k \rangle \subsetneq \mathbb{N}$, con $\mathrm{MCD}(g_1, g_2, \ldots, g_k) = 1$.

Problema. Determinare $f(S)$ in funzione di $g_1, g_2, \ldots, g_k$.

• $k = 2$. Sylvester (1884): Sia $S = \langle a, b \rangle$, con $\mathrm{MCD}(a, b) = 1$.
Allora $f(S) = ab - a - b$.
La dimostrazione può essere fatta da uno studente del primo anno.

• $k = 3$. Fel (2006): formula complicata, coinvolge la matrice delle relazioni, non è polinomiale.

• $k \geq 4$. Curtis (1990): non può esistere una formula polinomiale (né esplicita né implicita).

2. Congettura di Wilf

$S = \langle g_1, g_2, \ldots, g_k \rangle = \{0, s_1, s_2, \ldots, s_{n-1}, s_n, \rightarrow\}; \qquad s_n = f(S) + 1$

$n(S) := |S \cap \{0, 1, \ldots, f(S)\}|$

$k(S) :=$ cardinalità dell'insieme minimale di generatori.

Congettura. Wilf (1978): $k(S)n(S) \geq f(S) + 1$

Esercizio. Verificare che, per $S = \langle a, b \rangle$, vale
$2n(S) = f(S) + 1 = ab - a - b + 1 = (a-1)(b-1)$.

La congettura è stata verificata in alcuni casi particolari, per tutti i semigruppi con numero di Frobenius ≤ 50. Contributi più significativi da Sammartano ($2k(S) \geq s_1$) e Moscariello-Sammartano (2011 e 2013).

3. Semigruppi simmetrici e anelli di Gorenstein

$S = \langle g_1, g_2, \ldots, g_k \rangle$, $\quad M := S \setminus \{0\}$; $\quad K$ campo

$R = K[T^{g_1}, \ldots, T^{g_k}] = \{\sum a_s T^s \,|s \in S,\ a_s \in K\}$, $\quad \mathfrak{m} = (T^{g_1}, \ldots, T^{g_k})$

Osservazione. $R \subseteq K[T]$ dominio, ma non è un UFD.
Ad es., $T^6 = (T^2)^3 = (T^3)^2 \in K[T^2, T^3]$.

Osservazione. $R \cong K[X_1, \ldots, X_k]/\mathrm{Ker}(\phi)$, dove

$$\phi : K[X_1, \ldots, X_k] \longrightarrow R$$
$$X_i \longmapsto T^{g_i}$$

Osservazioni. • R ha dimensione 1:
le uniche catene di primi sono della forma: $(0) \subset P$.
• $(T^s)(T^u) = T^{s+u}$: moltiplicazione $\longrightarrow$ addizione.

Osservazione. Il campo delle frazioni di R è $K(T)$:

$$T^{-1} = \frac{T^{f(S)+1}}{T^{f(S)+2}}$$

Per ogni $g(X) \in \mathfrak{m} \setminus \{0\}$ si ha:

$$t = \dim_K \left(\frac{((g) : \mathfrak{m})}{(g)} \right) = \dim_K \left(\frac{(R : \mathfrak{m})}{R} \right)$$

(dove $(I : J) = \{h \in K(T) \mid hJ \subseteq I\}$).

Definizione. R Gorenstein se $t = 1$.
(ogni ideale (g), con $0 \neq g(X) \in \mathfrak{m}$, è irriducibile).

Proposizione. $t = \dim_K ((R : \mathfrak{m})/R) =$

$$= |\{n \in \mathbb{Z} \mid T^n \in (R : \mathfrak{m}) \setminus R\}| =$$

$$= |\{n \in \mathbb{Z} \mid n + M \subseteq S, n \notin S\}|$$

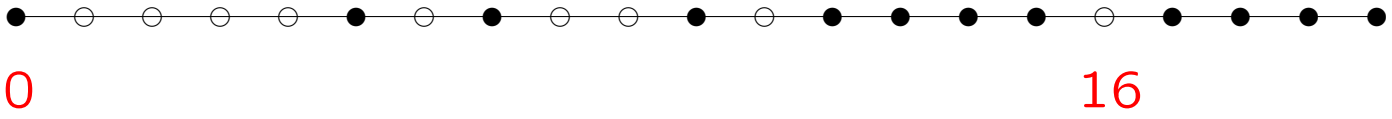
Torniamo ai semigruppi:
$S = \langle g_1, g_2, \ldots, g_k \rangle = \{0, s_1, s_2, \ldots, s_{n-1}, s_n, \rightarrow\}$;
$f = f(S) = \max(\mathbb{N} \setminus S)$; $\quad s_n = f(S) + 1$; $\quad M = S \setminus \{0\}$

Osservazione. $s \in S \;\Rightarrow\; f - s \notin S$
(altrimenti $f(S) = (f - s) + s \in S$; assurdo).

Definizione. S è simmetrico se $\forall\, x \in \mathbb{Z}$

$$x \in S \iff f - x \notin S$$

Esempio. (S non simmetrico):
$S = \{0, 5, 7, 10, 12, 13, 14, 15, 17, \rightarrow\}$; $\quad f = 16$



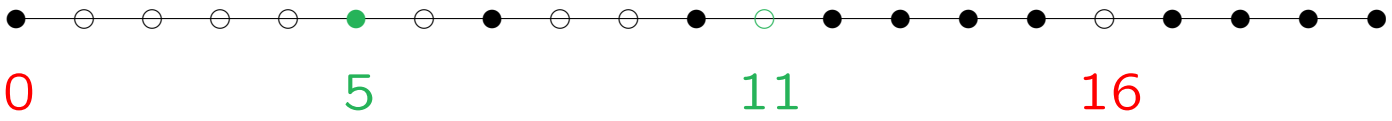
Torniamo ai semigruppi:
$S = \langle g_1, g_2, \ldots, g_k \rangle = \{0, s_1, s_2, \ldots, s_{n-1}, s_n, \rightarrow\}$;
$f = f(S) = \max(\mathbb{N} \setminus S)$; $\quad s_n = f(S) + 1$; $\quad M = S \setminus \{0\}$

Osservazione. $s \in S \;\Rightarrow\; f - s \notin S$
(altrimenti $f(S) = (f - s) + s \in S$; assurdo).

Definizione. S è simmetrico se $\forall\, x \in \mathbb{Z}$

$$x \in S \iff f - x \notin S$$

Esempio. (S non simmetrico):
$S = \{0, 5, 7, 10, 12, 13, 14, 15, 17, \rightarrow\}$; $\quad f = 16$



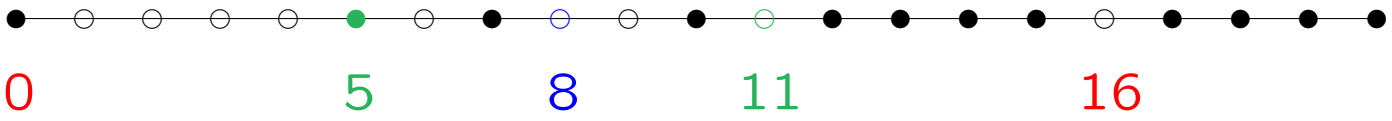
Torniamo ai semigruppi:
$S = \langle g_1, g_2, \ldots, g_k \rangle = \{0, s_1, s_2, \ldots, s_{n-1}, s_n, \rightarrow\}$;
$f = f(S) = \max(\mathbb{N} \setminus S)$; $\quad s_n = f(S) + 1$; $\quad M = S \setminus \{0\}$

Osservazione. $s \in S \;\Rightarrow\; f - s \notin S$
(altrimenti $f(S) = (f - s) + s \in S$; assurdo).

Definizione. S è simmetrico se $\forall\, x \in \mathbb{Z}$

$$x \in S \iff f - x \notin S$$

Esempio. (S non simmetrico):
$S = \{0, 5, 7, 10, 12, 13, 14, 15, 17, \rightarrow\}$; $\quad f = 16$



Proposizione. S simmetrico $\iff$

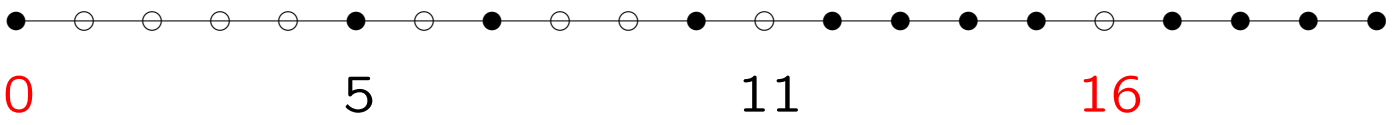
$$|S \cap \{0, 1, \ldots, f\}| = |(\mathbb{N} \setminus S) \cap \{0, 1, \ldots, f\}|$$

Dimostrazione. La seguente funzione è sempre ben definita e iniettiva:

$$\phi : S \cap \{0, 1, \ldots, f\} \longrightarrow (\mathbb{N} \setminus S) \cap \{0, 1, \ldots, f\}$$
$$n \longmapsto f - n$$

S simmetrico $\iff$ ϕ suriettiva. □

Nell'esempio si ha: $|S \cap \{0, 1, \ldots, f\}| = 8$ e
$|(\mathbb{N} \setminus S) \cap \{0, 1, \ldots, f\}| = 9$



Poniamo $(S - M) = \{n \in \mathbb{Z} \mid n + M \subseteq S\}$, $\quad t = |(S - M) \setminus S|$

Osservazione. $f \in (S - M) \setminus S$ (e quindi $t \geq 1$).

Proposizione. S simmetrico $\iff t = 1$

Dimostrazione. ($\Rightarrow$) PA: $\exists\, x \in (S - M) \setminus S, \quad x \neq f$;
S simmetrico $\Rightarrow f - x \in S \Rightarrow (f - x) + x = f \in S$; assurdo.

($\Leftarrow$) PA: S non simmetrico; sia $h = \max\{x \notin S \mid f - x \notin S\}$;
allora, $\forall s \in M$, $h + s \in S$
(altrimenti $h + s \notin S \Rightarrow f - (h + s) = s' \in S$ e $f - h = s + s' \in S$).
Dunque $h \in (S - M) \setminus S$ e $t > 1$; assurdo. $\square$

Teorema. Kunz (1971): $R = K[T^{g_1}, \ldots, Y^{g_k}]$, $S = \langle g_1, g_2, \ldots, g_k \rangle$;
allora: R Gorenstein $\iff$ S simmetrico.

4. Semigruppi numerici e codici di valutazione

Sia $\mathcal{A}$ un alfabeto con q elementi.
Una parola di lunghezza m è un elemento di $\mathcal{A}^m$.
Un codice a blocchi di lunghezza m è un sottoinsieme $\mathcal{C} \subseteq \mathcal{A}^m$.

Sia $q = p^h$ (p primo) e $\mathcal{A} = \mathbb{F}_q$ (campo con q elementi).

Definizione. Codice lineare a blocchi di lunghezza m è un sottospazio $\mathcal{C} \leq (\mathbb{F}_q)^m$.

Esempio. $\mathcal{C} = \{(a_1, \ldots, a_m) \in (\mathbb{Z}_2)^m \mid a_1 + \cdots + a_{m-1} = a_m\}$.

L'informazione è contenuta in $(a_1, \ldots, a_{m-1})$; la componente a_m ha una funzione di controllo, per sapere se ci sono stati errori di trasmissione.

Definizione. Siano $\mathbf{v} = (v_1, \ldots, v_m)$, $\mathbf{w} = (w_1, \ldots, w_m)$;
la distanza tra $\mathbf{v}$ e $\mathbf{w}$ è $d(\mathbf{v}, \mathbf{w}) := |\{i \mid v_i \neq w_i\}|$.
Si definisce distanza minima di $\mathcal{C}$ l'intero:

$$d(\mathcal{C}) = \min\{d(\mathbf{v}, \mathbf{w}) \mid \mathbf{v} \neq \mathbf{w} \in \mathcal{C}\} = \min\{d(\mathbf{v}, \mathbf{0}) \mid \mathbf{v} \in \mathcal{C} \setminus \{\mathbf{0}\}\}$$

(nell'esempio $d(\mathcal{C}) = 2$)

Proposizione. Se $\mathcal{C} \leq (\mathbb{F}_q)^m$ ha: $k = \dim_{\mathbb{F}_q}(\mathcal{C})$ e $d = d(\mathcal{C})$, allora

$$d \leq m - k + 1$$

Sia $e = \lfloor (d-1)/2 \rfloor$; allora $\mathcal{C}$ può correggere e errori:
$\mathbf{v} \in \mathcal{C}$ parola trasmessa, $\mathbf{w}$ parola ricevuta;
$d(\mathbf{v}, \mathbf{w}) \leq e \Rightarrow \mathbf{v}$ è l'unica parola di $\mathcal{C}$ t.c. $d(\mathbf{v}, \mathbf{w}) = e$.

Il problema è avere un algoritmo efficiente che da $\mathbf{w}$ mi permetta di ricostruire $\mathbf{v}$.

Funzioni peso e codici di valutazione.
Siano R un anello commutativo e unitario, F un campo, $F \subset R$.

$\phi : R \to \mathbb{N} \cup \{-\infty\}$ è una funzione peso se:
- $\phi(r) = -\infty \Leftrightarrow r = 0$
- $\phi(r) = 0$, $\forall\ r \in F$
- $\phi(r+t) \leq \max\{\phi(r), \phi(t)\} \quad (\phi(r) < \phi(t) \ \Rightarrow =)$
- $\phi(rt) = \phi(r) + \phi(t)$
- $\phi(r) = \phi(t) \Rightarrow \exists\ \lambda \in F \setminus \{0\}$ tale che $\phi(r - \lambda t) < \phi(t)$.

Osservazione. $\phi(R) := \{\phi(r) \mid r \in R \setminus \{0\}\}$ è un sottomonoide di $(\mathbb{N}, +)$. A meno di ridefinire ϕ dividendo per il massimo comun divisore, $\phi(R)$ è un s.n.

Proposizione. Se R ha una funzione peso è un dominio; inoltre, se scelgo $r_s \in R$ tale che $\phi(r_s) = s$ $(\forall s \in \phi(R))$, $\{r_s \mid s \in \phi(R)\}$ è una base di R come F-spazio vettoriale.

Esempio. (Curva Hermitiana) $\mathcal{H}_r : X^{r+1} - Y^r - Y = 0$ in $\mathbb{A}^2(F)$

$$R = \frac{F[X,Y]}{(X^5 - Y^4 - Y)} = F[u,v]$$

$(r = 4,\ F = \mathbb{F}_{16},\ u = \overline{X},\ v = \overline{Y})$

Poniamo $\phi(u) = 4$ e $\phi(v) = 5$; poiché $u^5 = v^4 + v$,
una base di R su F è $\{u^i v^j \ | 0 \leq i \leq 4,\ 0 \leq j\}$.

Inoltre: $\phi(u^i v^j) = 4i + 5j$ e,
poiché $0 \leq i, h \leq 4$, si ha $4i + 5j = 4h + 5k \Rightarrow i = h,\ j = k$.

Quindi ϕ è funzione peso e $\phi(R) = \langle 4, 5\rangle = \{0, 4, 5, 8, 9, 10, 12, \rightarrow\}$

($\phi(R)$ è il semigruppo di Weierstrass di $\mathcal{H}_4$ in $P_\infty = (0 : 0 : 1)$)

Definiamo in F^m somma e prodotto componente per componente. Si ha $F \hookrightarrow F^m$ $(1 \mapsto (1, \ldots, 1))$.

Sia $\Psi : R \longrightarrow F^m$ un omomorfismo di anelli
(tale che $1 \mapsto (1, \ldots, 1)$).

Sia $\phi(R) = \{0 = s_0, s_1, \ldots, s_n, \rightarrow\}$ e $\{r_{s_i} \mid i \in \mathbb{N}\}$ una base di R.
Sia $V_l = \langle r_{s_0}, \ldots, r_{s_l} \rangle_K$.

Definizione. Sia $\mathcal{E}_l = \Psi(V_l)$ e $\mathcal{C}_l = \mathcal{E}_l^{\perp}$;
$\mathcal{E}_l$ e $\mathcal{C}_l$ sono detti l-esimi codici di valutazione.

Sia $N_l = \{(i, j) \in \mathbb{N}^2 \mid s_i + s_j = s_l\}$ e $\nu_l = |N_l|$.

Proposizione. $d(\mathcal{C}_l) \geq d(l) := \min\{\nu_m \mid m > l\}$.

Osservazioni. • $d(l)$ dipende soltanto dalla funzione peso ϕ e non dall'omomorfismo Ψ.

• Si dimostra che questa limitazione migliora la limitazione inferiore che si ottiene (nel caso dei cosiddetti codici one-point) con teoremi profondi di geometria algebrica.

• Si cercano semigruppi per cui $d(l)$ sia facilmente calcolabile e grande.

• $d(l)$ dipende dalle proprietà di fattorizzazione nel semigruppo: se $a + b = s$, allora a e b sono divisori di s. Quindi ν_l coincide con il numero di divisori di s_l.

• C'è un ottimo algoritmo di correzione d'errore che corregge fino a $\lfloor \frac{l+1-2g}{2} \rfloor$ per $\mathcal{C}_l$ (dove $g = |(\mathbb{N} \setminus S) \cap \{0, 1, \ldots, f(S)\}|$).

Esempio. $R = \frac{F[X,Y]}{(X^5 - Y^4 - Y)} = F[u,v]$, $\phi(u^i v^j) = 4i + 5j$, $F = \mathbb{F}_{16}$.

La curva $\mathcal{H}_4$ ha 64 punti a coordinate in F. Si definisce:

$$\begin{aligned} \Psi : R &\longrightarrow F^{64} \\ f(u,v) &\longmapsto (f(P_1), \ldots, f(P_{64})) \end{aligned}$$

l	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s_l	4	5	8	9	10	12	13	14	15	16	17	18	19	20	21
r_{s_l}	u	v	u^2	uv	v^2	u^3	u^2v	uv^2	v^3	u^4	u^3v	u^2v^2	uv^3	v^4	u^4v
ν_l	2	2	3	4	3	4	6	6	4	5	8	9	8	9	10
$d(l)$	2	3	3	3	4	4	4	4	5	8	8	8	9	10	12

Si verifica che per $l = 16$, $s_{16} = 22$ e $\nu_{16} = 12$.
Inoltre, $\forall\ l > 16$ si ha $\nu_l = l - 5$ (e quindi $d(l) = l - 4$).

Per $l = 32$ è un ottimo codice.

GRAZIE PER L'ATTENZIONE!