Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Claudio Di Comite, Roberto Peluso

Sulla determinazione di alcuni k-archi completi con l'aiuto di una calcolatrice elettronica

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **53** (1972), n.1-2, p. 94–99.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1972_8_53_1-2_94_0>

Geometrie finite. — *Sulla determinazione di alcuni k-archi completi con l'aiuto di una calcolatrice elettronica* (*). Nota (**) di CLAUDIO DI COMITE e ROBERTO PELUSO, presentata dal Socio B. SEGRE.

SUMMARY. — In a Galois plane of order p, with p prime, $p \neq 2$, $p \neq 3$, $p \not\equiv 1 \pmod 3$ e $p \not\equiv 1 \pmod 4$, complete $(p+9)/2$-arcs are constructed, with the aid of an electronic calculating machine.

INTRODUZIONE

Sia $S_{2,p}$ un piano lineare sopra un campo finito di ordine p, con p primo, $p \neq 2$, $p \neq 3$, $p \not\equiv 1 \pmod 3$ e $p \not\equiv 1 \pmod 4$.

In [1] si sono costruiti $(p+9)/2$-archi di $S_{2,p}$ non contenuti in coniche e si è provato, mediante un ben noto teorema di B. Segre (cfr. [5] e [9], pag. 273) che, per $p = 11$, detti archi sono completi.

Il problema della completezza dei $(p+9)/2$-archi costruiti in [1], per $p > 11$, si può risolvere mediante una calcolatrice elettronica. Calcolatrici elettroniche in ricerche concernenti i k-archi sono già state impiegate da L. Lunelli ed M. Sce, i quali hanno costruito, tra l'altro, mediante una calcolatrice elettronica, 10-archi completi di $S_{2,11}$ e 12-archi completi di $S_{2,13}$ (cfr. [2]).

In questa Nota si descrive un procedimento per la verifica, con una calcolatrice elettronica, della completezza dei $(p+9)/2$-archi costruiti in [1], per $p > 11$.

Con tale procedimento si è verificato che i predetti $(p+9)/2$-archi risultano completi per tutti i valori di p presi in considerazione e precisamente per $p \leq 419$. Per $p \leq 83$ ci si è serviti del calcolatore IBM 1130 degli Istituti di Matematica dell'Università di Bari e, per i successivi valori di p (≤ 419), si è usato il calcolatore IBM 360/65 in dotazione al C.S.A.T.A. (Bari).

1. – Si consideri un piano proiettivo $S_{2,p}$ sopra il campo finito γ_p di ordine p, con p primo, $p \neq 2$, $p \neq 3$, $p \not\equiv 1 \pmod 3$ e $p \not\equiv 1 \pmod 4$.

Si premettono alcune considerazioni su γ_p.

Gli elementi di γ_p (campo delle classi dei resti modulo p) si indicheranno con $0, 1, \cdots, p-1$. Per le ipotesi fatte su p, gli elementi $p-1$ e $p-3$ sono non-quadrati in γ_p (cfr. [1] e [9]) e, conseguentemente, 3 è un quadrato in γ_p.

Si ponga $f(\lambda) = 1 + \lambda + \lambda^2$, con $\lambda \in \gamma_p$. In [1] si è provato che non esiste un $\lambda \in \gamma_p$ tale che $f(\lambda) = 0$. Si indichi con σ_p l'insieme degli elementi di γ_p

(*) Lavoro eseguito con contributo del C.N.R. nell'ambito dei Gruppi di Ricerca Matematica.

(**) Pervenuta all'Accademia il 25 luglio 1972.

tali che $f(\lambda)$ sia un non–quadrato in γ_p. È noto che il numero degli elementi di σ_p è $(p+1)/2$ (cfr. [9], n. 79 ed [1]).

Risulta:

$$f(0)=f(p-1)=1 \quad , \quad f(1)=f(p-2)=3 ,$$

conseguentemente, essendo gli elementi 1 e 3 quadrati in γ_p, si ha:

$$0\,,\;1\,,\;p-1\,,\;p-2\notin\sigma_p\,. \tag{1.1}$$

Si osservi infine che, essendo $f(\lambda^{-1})=f(\lambda)\,\lambda^{-2}$, con $\lambda\in\gamma_p-\{0\}$, risulta:

$$\lambda\in\sigma_p \iff \lambda^{-1}\in\sigma_p\,. \tag{1.2}$$

Fissato su $S_{2,p}$ un sistema di coordinate omogenee $(x\,,y\,,z)$, sia K_p il sottoinsieme di $S_{2,p}$ costituito dai $(p+1)/2$ punti $P_\lambda\,(\lambda+\lambda^2+\lambda^3,\,\lambda+\lambda^2,\,1+\lambda+\lambda^2)$, con $\lambda\in\sigma_p$, e dai 4 punti $O_2\,(0\,,1\,,0)$, $Q_1\,(1\,,1\,,1)$, $Q_2\,(p-2\,,1\,,1)$ e $Q_3\,(1\,,1\,,p-2)$. Si è provato in [1] che:

PROPOSIZIONE. – *K_p è un $(p+9)/2$–arco di $S_{2,p}$, il quale, per $p=11$, risulta completo.*

Si faranno ora alcune considerazioni su K_p, atte ad abbreviare lo studio della completezza di K_p, per $p>11$, mediante una calcolatrice elettronica.

Le $(p+7)/2$ secanti di K_p passanti per O_2 sono le rette di equazioni

$$x=\lambda z\,,\qquad \text{con}\quad \lambda\in\sigma_p\cup\{1\,,p-2\,,(p-1)/2\}\ ^{(1)}. \tag{1.3}$$

Le tangenti per O_2 a K_p sono quindi le $(p-7)/2$ rette di equazioni

$$x=\lambda z\,,\qquad \text{con}\quad \lambda\in\gamma_p-\sigma_p-\{1\,,p-2\,,(p-1)/2\}$$

e la retta di equazione $z=0$.

Si indichi con τ_p l'insieme $\gamma_p-\sigma_p-\{1\,,p-2\,,(p-1)/2\}$. Risulta ovviamente $1\notin\tau_p$; per la (1.1) gli elementi 0 e $p-1$ appartengono a τ_p e dalla (1 . 2), essendo $p-2$ e $(p-1)/2$ l'uno l'inverso dell'altro, segue che:

$$\lambda\in\tau_p-\{0\}\iff\lambda^{-1}\in\tau_p-\{0\}\,.$$

Si possono allora costruire due sottoinsiemi di τ_p:

$$\tau'_p=\{0\,,p-1\,,a_1\,,\cdots,a_h\},$$
$$\tau''_p=\{b_1\,,\cdots,b_h\},\qquad \text{con}\quad h=(p-11)/4\,,$$

tali che:

$$\tau'_p\cup\tau''_p=\tau_p\quad,\quad\tau'_p\cap\tau''_p=\varnothing\quad\text{e}\quad a_ib_i=1,\quad\text{con}\quad 1\le i\le h\,. \tag{1.4}$$

(1) Gli elementi 1 e $p-2$ non appartengono a σ_p (cfr. (1.1)) e, per la (1.2), anche l'elemento $(p-1)/2$, essendo l'inverso di $p-2$, non appartiene a σ_p.

Si indichi con T la simmetria su $S_{2,p}$ di equazioni: $x' = z$, $y' = y$, $z' = x$. Si verifica che:

$$T(O_2) = O_2 \quad , \quad T(Q_1) = Q_1 \quad , \quad T(Q_2) = Q_3$$

$$\text{e} \quad T(P_\lambda) = P_{\lambda^{-1}} \quad (\text{cfr. } (1.2)), \qquad \text{con} \quad \lambda \in \sigma_p \,.$$

Risulta pertanto $T(K_p) = K_p$.

Inoltre, indicati con S' e S'' i sottoinsiemi di $S_{2,p}$ costituiti rispettivamente dai punti delle rette

$$x = 0 \quad , \quad x = a_i z \,, \qquad \text{con} \quad 1 \leq i \leq h \,,$$

e da quelli delle rette

$$z = 0 \quad , \quad x = b_i z \,, \qquad \text{con} \quad 1 \leq i \leq h \,,$$

risulta (cfr. (1.4)) $T(S') = S''$. Ne consegue che, per provare che K_p è completo, è sufficiente provare che i punti delle rette

$$x = \lambda z \qquad \text{con} \quad \lambda \in \tau'_p \tag{1.5}$$

appartengono a delle secanti di K_p.

Le rette (1.5) passano tutte per $O_2 \in K_p$, quindi, per dimostrare che K_p è completo, è sufficiente provare che, per ogni $\lambda \in \tau'_p$ e per ogni $\mu \in \gamma_p$, esiste una secante di K_p (ovviamente distinta dalle rette (1.3)) contenente il punto $P(\lambda, \mu, 1)$.

Questa verifica si può fare, per p non eccessivamente grande, con una calcolatrice elettronica e, a tal fine, si riportano qui di seguito le equazioni delle rette secanti di K_p diverse dalle (1.3):

$$x + (p-1)\,y = 0$$

$$y + (p-1)\,z = 0$$

$$x + y + z = 0$$

$$x + (p - 1 + \lambda^3)\,y + (p-1)\,\lambda^3 z = 0, \qquad \text{con} \quad \lambda \in \sigma_p \,,$$

$$x + (2 + 3\lambda + 3\lambda^2 + \lambda^3)\,y + (p-1)(3\lambda + 3\lambda^2 + \lambda^3)\,z = 0 \,,$$
$$\text{con} \quad \lambda \in \sigma_p \,,$$

$$(p-1)(1 + 3\lambda + 3\lambda^2)\,x + (1 + 3\lambda + 3\lambda^2 + 2\lambda^3)\,y + \lambda^3 z = 0 \,,$$
$$\text{con} \quad \lambda \in \sigma_p \,,$$

$$(1+\lambda+\mu)\,x + (p-1)(1+\lambda+\lambda^2)(1+\mu+\mu^2)\,y + \lambda\mu(\lambda+\mu+\lambda\mu)\,z = 0 \,,$$
$$\text{con} \quad \lambda\,, \mu \in \sigma_p \quad \text{e} \quad \lambda \neq \mu \,.$$

2. – Per i cinque numeri primi 23, 47, 59, 71, 83, la verifica della completezza dei corrispondenti archi K_p si è ottenuta col seguente programma adattato per il calcolatore IBM 1130, presso gli Istituti di Matematica dell'Università di Bari:

```
   INTEGER P,A(904), B(990), C(990), S(20)
   DO 20 KK=1, 5
   READ(2, 50)P
   L=(P-1)/2
   DO 1 I=1, L
   A(I)=I*I
 1 A(I)=MOD(A(I), P)
   K=0
   N=(P*P-1)/8+3*(P+1)/2+3
   No=N-L
   DO 2 I=No, N
 4 K=K+1
   B(I)=K*K+K+1
   B(I)=MOD(B(I), P)
   DO 3 J=1, L
   IF(B(I)-A(J))3, 4, 3
 3 CONTINUE
 2 C(I)=K
   M=(P-11)/2
   K=1
   DO 5 J=1,M
 6 K=K+1
   IF(K-L)7, 6, 7
 7 DO 8 I=No, N
   IF(C(I)-K)8, 6, 8
 8 CONTINUE
 5 A(J)=K
   S(3)=A(1)
   M=(P-3)/4
   K=1
   DO 11 I=4,M
   L=I-1
10 K=K+1
   S(I)=A(K)
   DO 11 J=3, L
   A(K)=S(I)*S(J)
   A(K)=MOD(A(K), P)
   IF(A(K)-1)11, 10,11
11 CONTINUE
   S(1)=0
   S(2)=P-1
   A(1)=0
   B(1)=1
   C(1)=S(2)
   K=1
   N1=N-1
   DO 9 I=No, N1
   L=I+1
   DO 9 J=L, N
   K=K+1
   A(K)=1+C(I)+C(J)
   A(K)=MOD(A(K), P)
   B(K)=B(I)*B(J)
   B(K)=MOD(B(K), P)
   B(K)=S(2)*B(K)
   B(K)=MOD(B(K), P)
   C(K)=C(I)*C(J)
   C(K)=MOD(C(K), P)
   C(K)=C(K)*(C(I)+C(J)+C(K))
 9 C(K)=MOD(C(K), P)
   J=K+1
   DO 12 I=No, N
   K=K+1
   C(K)=C(I)*C(I)
   C(K)=MOD(C(K), P)
   C(K)=C(I)*C(K)
   C(K)=MOD(C(K), P)
   A(K)=P-2+3*B(I)
   A(K)=MOD(A(K), P)
   B(K)=A(K)+2*C(K)
   B(K)=MOD(B(K), P)
   A(K)=S(2)*A(K)
12 A(K)=MOD(A(K), P)
   L=K
   K=K+1
   B(K)=S(2)
   C(K)=0
   K=K+1
   B(K)=1
   C(K)=1
   DO 14 I=J, L
   K=K+1
   B(K)=C(I)+S(2)
   B(K)=MOD(B(K), P)
   C(K)=C(I)*S(2)
14 C(K)=MOD(C(K), P)
   DO 15 I=J, L
   K=K+1
   B(K)=P+1+B(I)-C(I)
   B(K)=MOD(B(K), P)
   C(K)=P+B(K)-2
   C(K)=MOD(C(K), P)
   C(K)=S(2)*C(K)
15 C(K)=MOD(C(K), P)
   LL=L+1
   DO 16 I=1, P
```

```
      No=I—1
      DO 16 J=1,M
      DO 17 K=1,L
      N1=A(K)*S(J)+B(K)*No+C(K)
      N1=MOD(N1, P)
      IF(N1)17, 16, 17
   17 CONTINUE
      DO 13 K=LL, N
      N1=B(K)*No+C(K)+S(J)
      N1=MOD(N1, P)
      IF(N1)13, 16,13
   13 CONTINUE
      WRITE(3, 51)
      GO TO 20
   16 CONTINUE
      WRITE(3, 52)
   20 CONTINUE
      STOP
   50 FORMAT(I3)
   51 FORMAT(1H, 12HNON COMPLETO)
   52 FORMAT(1H, 8HCOMPLETO)
      END
```

Poichè il predetto calcolatore non possiede il sottoprogramma proprio che effettua il resto della divisione fra due numeri interi, al programma principale si è aggiunto il sottoprogramma seguente:

```
      FUNCTION MOD(I , J)
      K=I
    1 MOD=K
      K=K—J
      IF(K) 2, 1, 1
    2 RETURN
      END
```

Successivamente, sostituendo le istruzioni

```
      INTEGER P, A(904), B(990), C(990), S(20)
              DO 20 KK=1, 5
```

rispettivamente con

```
      INTEGER P, A(22156), B(22578), C(22578), S(104)
              DO 20 KK=1, 7
```

e fornendo come dati da leggere i sette numeri primi 107, 179, 227, 239, 311, 383, 419, si è provato ancora che K_p è completo per tali valori di p, sul calcolatore IBM 360/65 in dotazione al C.S.A.T.A. (Bari). Non è stato necessario fare uso del sottoprogramma MOD, giacchè esso è un sottoprogramma proprio di tale calcolatore.

Per valori più grandi di p, volendo evitare di occupare eccessivo spazio di memoria si renderebbe necessario costruire un sottoprogramma che calcoli l'inverso di un elemento in γ_p e modificare il programma principale in modo da memorizzare, per ciascuna retta, solamente il secondo ed il terzo coefficiente.

BIBLIOGRAFIA

[1] C. DI COMITE, *Intorno a certi* $(q+9)/2$*-archi di* $S_{2,q}$, « Rend. Acc. Naz. Lincei », ser. VIII, *36* (6) (1964).

[2] M. SCE e L. LUNELLI, *Sulla ricerca dei k-archi completi mediante calcolatrice elettronica*, Convegno reticoli e geometrie proiettive (Palermo 1957). Roma, Cremonese (1958).

[3] B. SEGRE, *Sulle ovali nei piani lineari finiti*, « Rend. Acc. Naz. Lincei », ser. VIII, *17* (1954).

[4] B. SEGRE, *Ovals in a finite projective plane*, « Canad. J. Math. », *7* (1955).

[5] B. SEGRE, *Curve razionali normali e k-archi negli spazi finiti*, « Ann. Mat. pura appl. », ser. IV, *39* (1955).

[6] B. SEGRE, *Intorno alla geometria sopra un campo di caratteristica due*, « Rev. Fac. Sci. Univ. Istambul », ser. A, *21* (1956).

[7] B. SEGRE, *Sui k-archi nei piani finiti di caratteristica due*, « Revue de Math. Pures et appl. », *2* (1957).

[8] B. SEGRE, *Le geometrie di Galois*, « Ann. di Mat. pura appl. », ser. IV, *48* (1959).

[9] B. SEGRE, *Lectures on modern geometry*, Ed. Cremonese (1961).

[10] B. SEGRE, *Istituzioni di Geometria Superiore*, « Ist. Mat. Univ. », Roma 1965.

[11] B. SEGRE, *Introduction to Galois geometries*, « Mem. Acc. Naz. Lincei », ser. VIII, *8* (1967).