

Geometrie pseudo-euclidee sui campi di Galois

Fernando Di Gennaro¹, Franco Eugeni², Nadia Gatti³

Sunto: In questo capitolo viene definito un prodotto interno in $AG(2, q)$, sia nel caso q dispari che nel caso q pari. Si prende, successivamente in esame la geometria del triangolo, notando, nel caso dispari, una configurazione analoga al caso reale euclideo, mentre nel caso pari risulta tutto un po' stravolto, tanto che la non commutatività del prodotto interno induce una perpendicolarità ordinata. Nella parte finale viene riportata la classificazione delle coniche, studiata da Tallini (vedi bibliografia).

Parole chiave: geometrie pseudo-euclidee.

1. Introduzione

In questo paragrafo vengono ripresi alcuni risultati ottenuti in altri lavori, con lo scopo di fornire prerequisiti relativi al concetto di geometria finita.

Applicando, in concreto, i concetti di metrica pseudo-euclidea si riporta un modello di autenticazione.

Nella parte finale si prende in esame la classificazione delle coniche, nel caso dispari.

Sarebbe altrettanto interessante riuscire a classificare una conica in un piano di Galois di ordine pari, sapendo a priori la difficoltà e la complessità di questo tipo di studio.

¹ Dipartim. M.E.T., Università di Teramo; e-mail: fernando.digennaro@libero.it

² Dipartimento M.E.T., Università di Teramo; e-mail: eugenif@tin.it

³ Dipartimento M.E.T., Università di Teramo; e-mail: nadiagatti@libero.it

2. Forme quadratiche definite sui campi di Galois

Sia $F = GF(q)$ un campo di Galois di ordine q qualsiasi. Distinguendo il caso pari dal caso dispari, poniamo:

$$F_0 = F_0(q) = \{a : a \in F, \exists x \in F \text{ con } x^2 = a, q \text{ dispari}\}$$

$$F_0 = F_0(q) = \{d : d \in F, \exists x \in F \text{ con } x^2 + x + d = 0, q \text{ pari}\}$$

ed $F_1 = F \setminus F_0$.

Nel caso dispari, gli elementi di F_0 si chiamano "quadrati" del campo e quelli dell'insieme F_1 "non quadrati"; nel caso pari, gli elementi di F_0 si chiamano di "categoria zero" e quelli dell'insieme F_1 di "categoria uno".

La cardinalità di F_0 risulta essere $(q+1)/2$ se q è dispari e $q/2$ se q è pari, sussiste inoltre la seguente regola per il prodotto:

$$F_0 F_0 = F_1 F_1 = F_0, \quad F_0 F_1 = F_1 F_0 = F_1$$

Si osserva, dunque, che gli elementi di F_0 coincidono con i numeri positivi del campo dei reali $\mathfrak{R}$ e gli elementi di F_1 con i negativi; dunque tali elementi si comportano seguendo la regola del prodotto definita in $\mathfrak{R}$; si nota, però, che non sussiste l'analogo additivo, ossia, a differenza del caso reale, la somma di due quadrati può essere un non quadrato.

Proposizione 1. Se k è un elemento non quadrato di $GF(q)$ con q dispari, allora esistono sempre in $GF(q)$ due quadrati la cui somma sia proprio k .

Dimostrazione. Supponiamo, per assurdo che l'equazione $x^2 + y^2 = k$ non abbia nessuna soluzione in $GF(q)$.

Dunque:

$$\forall x \in GF(q), k - x^2 \in F_1$$

ed assume esattamente $\left(\frac{q+1}{2}\right)$ valori tutti distinti di $GF(q)$, che dovrebbero essere tutti elementi di F_1 ; ciò è assurdo essendo i non quadrati solamente $\frac{(q-1)}{2}$.

Dalla proposizione si ha, per esempio che a differenza di quanto accade nel caso reale, l'equazione $x^2 + y^2 + 1 = 0$ ammette sempre soluzione in $GF(q)$, q dispari, considerando gli elementi x ed y non necessariamente diversi da zero.

Generalizzando tale proposizione si ottiene:

Proposizione 2. Sia $f(x_1, x_2, \dots, x_n)$ una qualsivoglia forma quadratica, nelle indeterminate $x_1, x_2, \dots, x_n$, a coefficienti in $GF(q)$, che non sia il quadrato di una forma lineare. Scelto comunque un elemento h di $GF(q)$, esiste almeno una n -upla di elementi di $GF(q)$ $(\dot{x}_1, \dot{x}_2, \dots, \dot{x}_n)$, tale che $f(\dot{x}_1, \dot{x}_2, \dots, \dot{x}_n) = h$.

Come immediata conseguenza delle due proposizioni, si può provare il seguente Teorema:

Teorema dell'annullamento di una forma. Sia $f(x_1, x_2, \dots, x_n)$, $n \geq 3$, una forma quadratica qualunque a coefficienti in $GF(q)$. Esiste sempre qualche n -upla di elementi, non tutti nulli, di $GF(q)$, $(\dot{x}_1, \dot{x}_2, \dots, \dot{x}_n)$ tale che $f(\dot{x}_1, \dot{x}_2, \dots, \dot{x}_n) = 0$.

Dimostrazione. Supponendo la f non degenerare, (ossia il determinante della matrice dei coefficienti diverso da zero), e riducendo la f a forma diagonale, si ottiene:

$$f = a_1 x_1^2 + a_2 x_2^2 + \dots + a_n x_n^2 \quad \text{con } a_i \neq 0 \quad \text{per } i = 1, \dots, n.$$

Basta dunque provare il teorema per la (1.1). Si consideri la forma quadratica $g(x_1, x_2) = a_1 x_1^2 + a_2 x_2^2$; essa non è il quadrato di una forma lineare.

Esiste, allora, per la proposizione 2, una coppia $(\dot{x}_1, \dot{x}_2)$ di elementi di $GF(q)$ tale che $a_1 \dot{x}_1^2 + a_2 \dot{x}_2^2 = -a_3$.

La n -upla non tutta nulla $(\dot{x}_1, \dot{x}_2, 1, 0, \dots, 0)$ annulla la (1.1).

3. Definizione di pseudo-prodotto⁴ interno

Ci preoccupiamo, ora di introdurre assiomaticamente un prodotto interno a valori in F che soddisfi i seguenti requisiti:

- 1) che sia una forma bilineare a valori in F ;
- 2) che sia indifferentemente definito, sia nel caso di campi di ordine pari che di ordine dispari;
- 3) che induca una "norma" intesa come forma quadratica, definita non nulla.

Sia $V = VG(2, q)$ lo spazio vettoriale di dimensione due sul campo F , poniamo la seguente definizione:

Definizione 1. Sia $V = VG(2, q)$, si dice *pseudo - prodotto interno* su V , una legge:

$$f : V \times V \rightarrow F$$

⁴ La dizione pseudo-prodotto indica solo che l'applicazione f è a valori in un campo di Galois e non nel campo reale (o complesso), pur soddisfacendo tutte le proprietà formali di un prodotto interno a valore reale.

$$(u, v) \rightarrow f(u, v) = u * v,$$

tale che:

a) La forma f è bilineare, cioè $\forall u, v, w \in V$ e $\forall \lambda \in F$:

- $u * (v + w) = u * v + u * w$
- $(v + w) * u = v * u + w * u$
- $(\lambda u) * v = u * (\lambda v) = \lambda(u * v)$;

b) la forma $f(u, u) = u * u = 0 \Leftrightarrow u = \mathbf{0}$.

c) se $u \neq v$, allora $f(u, v) - f(v, u) = 0, 1$ a seconda che q sia dispari o pari.

Sia $\{e_1, e_2\}$ una base di V

$$u = xe_1 + ye_2$$

$$v = x'e_1 + y'e_2$$

$$e_i * e_j = a_{ij}, \quad i, j = 1, 2$$

allora risulta:

$$u * v = (xe_1 + ye_2) * v = x(e_1 * v) + y(e_2 * v) =$$

$$= x[e_1 * (x'e_1 + y'e_2)] + y[e_2 * (x'e_1 + y'e_2)] =$$

$$= xx'e_1 * e_1 + xy'e_1 * e_2 + yx'e_2 * e_1 + yy'e_2 * e_2 =$$

$$= xx'a_{11} + xy'a_{12} + yx'a_{21} + yy'a_{22}.$$

Definizione 2. Una base ordinata (e_1, e_2) si dice *pseudo- canonica* se

$$e_1 * e_2 = 1, \quad e_2 * e_2 = -\theta, \quad e_1 * e_2 = \varepsilon, \quad e_2 * e_1 = 0$$

essendo $\theta \in F_1$ ed $\varepsilon = 0$ oppure 1 secondo che q sia dispari o pari .

Teorema 1. L'espressione di uno pseudo-prodotto interno rispetto ad una base canonica è la seguente:

$$u * v = xx' - \theta yy', \text{ se } q \text{ è dispari}$$

$$u * v = xx' + xy' + \theta yy', \text{ se } q \text{ è pari}$$

Dimostrazione. Sia q dispari, allora dall'espressione:

$$u * v = a_{11}xx' + a_{12}xy' + a_{21}x'y + a_{22}yy', \text{ essendo } a_{11} = e_1 * e_1 = 1, \\ a_{22} = e_2 * e_2 = -\theta, \quad a_{12} = a_{21} = 0 \text{ risulta } u * v = xx' - \theta yy'.$$

Nel caso pari si ha:

$$a_{11} = e_1 * e_1 = 1, \quad a_{22} = e_2 * e_2 = -\theta, \quad a_{12} = e_1 * e_2 = 1, \quad a_{21} = e_2 * e_1 = 0 \\ \text{da cui si ottiene } u * v = xx' + xy' - \theta yy'.$$

Il prodotto induce una norma, cioè una funzione:

$$N : V \times V \rightarrow F$$

$$\forall u, v \in V, \quad N(u, v) = (u - v) * (u - v).$$

Se $u = xe_1 + ye_2$ e se $v = 0$, e la base (e_1, e_2) è una base *pseudo - canonica*, allora si ha:

$$N(u, 0) = \begin{cases} x^2 - \theta y^2 & \text{per } q \text{ dispari} \\ x^2 + xy + \theta y^2 & \text{per } q \text{ pari} \end{cases}$$

Se P_1, P_2 sono due punti di un piano pseudo-euclideo, si definisce la norma di due punti, ponendo:

$$N(P_1, P_2) = N(P_1 P_2, 0)$$

essendo $P_1 P_2 = (x_2 - x_1)e_1 + (y_2 - y_1)e_2$, per cui si ottiene

$$N(P_1, P_2) = a_{11}(x_2 - x_1)^2 + (a_{12} + a_{21})(x_2 - x_1)(y_2 - y_1) + a_{22}(y_2 - y_1)^2$$

4. La geometria del triangolo nel caso dispari

Lavorando in piani di Galois di ordine dispari, si è provato che esiste, per la geometria del triangolo, una configurazione analoga a quella del caso reale.

Utilizzando la nozione di punto medio, si trovano le equazioni parametriche di due generiche mediane del triangolo e, risolvendo il sistema, il loro punto d'intersezione. Si prova, inoltre facilmente che tale punto appartiene alla terza mediana ed è proprio il baricentro del triangolo, ossia :

Teorema 2. Sia $EG(2,q)$ un piano pseudo-euclideo, con $q=p^n$ dispari e $p \neq 3$. In tal caso le tre mediane si incontrano in un punto **B** detto **baricentro** di coordinate

$$B = \left(\left(\frac{x_1 + x_2 + x_3}{3} \right), \left(\frac{y_1 + y_2 + y_3}{3} \right) \right).$$

Per determinare il punto d'intersezione dei tre assi del triangolo, trovate, ovviamente, le equazioni degli assi relativi a due lati, si risolve il sistema, ottenendo come soluzione un punto C.

Cambiando le coppie degli assi e ripetendo il calcolo, si ottiene il medesimo punto.

Non ci si accontenta di trovare tale punto, ma si vuole provare, che esso è proprio il centro della circonferenza passante per i vertici del triangolo.

Introduciamo, dunque la nozione di circonferenza, come luogo dei punti $P(x,y)$ che hanno norma costante Λ rispetto ad un fissato punto $C(\alpha, \beta)$, detto centro.

$$(x - \alpha)^2 - \theta(y - \beta)^2 = \Lambda.$$

Per cui data un'equazione del tipo:

$$x^2 - \theta y^2 + ax + by + c = 0$$

è semplice trovare le formule per il centro e per la norma:

$$\alpha = -\frac{a}{2}; \quad \beta = -\frac{b}{2\theta}; \quad 4\Lambda = a^2 - \frac{b^2}{\theta} - 4c.$$

Dunque, dopo aver determinato l'equazione della circonferenza passante per i vertici del triangolo ed utilizzando le formule scritte sopra per il centro, si prova il seguente:

Teorema 3. I tre assi dei lati di un triangolo di $EG(2,q)$, q dispari, passano tutti per uno stesso punto C , detto **circocentro**, che è il centro della circonferenza circoscritta.

Per studiare le intersezioni delle altezze, bisogna determinare le equazioni delle medesime condotte dai tre vertici ai lati opposti; così confrontando a due a due le equazioni trovate e, ponendo alcune notazioni, si determina l'ortocentro del triangolo, ossia si prova che:

Teorema 4. Le tre altezze di un triangolo di $EG(2,q)$, q dispari, si incontrano in uno stesso punto (**ortocentro**).

Analizziamo, ora un caso particolare e precisamente quello del triangolo equilatero.

Dato un triangolo di vertici $P_1(x_1, y_1), P_2(x_2, y_2), P_3(x_3, y_3)$ di $EG(2, q)$, q dispari, imponiamo alla retta P_1M_1 , mediana uscente da P_1 , di coincidere con l'asse del lato P_2P_3 .

La mediana P_1M_1 avrà equazione parametrica:

$$\begin{cases} x = x_1 + t(x_2 + x_3 - 2x_1) \\ y = y_1 + t(y_2 + y_3 - 2y_1) \end{cases} \quad (P_1M_1)$$

Eliminando t , si ottiene :

$$\frac{x - x_1}{(x_2 + x_3 - 2x_1)} = \frac{y - y_1}{(y_2 + y_3 - 2y_1)} \quad (P_1M_1)$$

L'asse del lato P_2P_3 è data dall'equazione:

$$2(x_3 - x_2)x + 2\theta(y_3 - y_2)y = (x_3^2 - x_2^2) - \theta(y_3^2 - y_2^2)$$

che si può anche scrivere :

$$2(x_3 - x_2)x + 2\theta(y_3 - y_2)y = N(P_3) - N(P_2).$$

Se eguagliamo i due coefficienti angolari otteniamo:

$$\theta(y_3 - y_2)(y_2 + y_3 - 2y_1) = (x_3 - x_2)(x_2 + x_3 - 2x_1)$$

$$\theta[(y_3^2 - y_2^2) - 2(y_1y_3 - y_1y_2)] = x_3^2 - x_2^2 - 2(x_1x_3 - x_1x_2) \quad (1)$$

Calcoliamo, ora $N(P_1P_2)$:

$$N(P_1P_2) = (x_2 - x_1)^2 - \theta(y_2 - y_1)^2 = x_2^2 + x_1^2 - 2x_1x_2 - \theta(y_2^2 + y_1^2 - 2y_1y_2)$$

e allo stesso modo $N(P_1P_3)$ e $N(P_2P_3)$:

$$N(P_1P_3) = x_3^2 + x_1^2 - 2x_1x_3 - \theta(y_3^2 + y_1^2 - 2y_1y_3)$$

$$N(P_2P_3) = x_3^2 + x_2^2 - 2x_2x_3 - \theta(y_3^2 + y_2^2 - 2y_2y_3)$$

Facendo la differenza delle norme dei due lati, si ha:

$$N(P_1P_3) - N(P_1P_2) = x_3^2 - x_2^2 - 2x_1x_3 + 2x_1x_2 - \theta \left[(y_3^2 - y_2^2 - 2y_3(y_1 - y_2)) \right]$$

Si può dunque affermare che:

$$N(P_1P_3) = N(P_1P_2) \Leftrightarrow \text{vale la (1).}$$

Allo stesso modo imponendo l'eguaglianza tra la mediana P_2M_2 e l'asse relativa al lato P_1P_3 , si ottiene:

$$\theta \left[(y_3^2 - y_1^2) - 2(y_2y_3 - y_2y_1) \right] = x_3^2 - x_1^2 - 2(x_2x_3 - x_2x_1) \quad (2)$$

Facendo nuovamente la differenza tra le norme dei due lati, si ottiene:

$$N(P_2P_3) - N(P_1P_2) = x_3^2 - x_1^2 - 2x_1x_3 + 2x_1x_2 - \theta \left[y_3^2 - y_1^2 - 2y_2(y_3 - y_1) \right]$$

Si può affermare che :

$$N(P_1P_2) = N(P_2P_3) \Leftrightarrow \text{vale la (2).}$$

In definitiva

$$N(P_1P_2) = N(P_2P_3) = N(P_1P_3) \Leftrightarrow \text{valgono la (1) e la (2).}$$

Ossia:

Il triangolo di vertici P_1, P_2, P_3 è *equilatero* se e solo se le altezze e le mediane coincidono.

Segue allora:

Teorema 5. In un triangolo equilatero di $EG(2,q)$ ogni mediana è anche altezza e asse; per cui baricentro, ortocentro e circocentro sono coincidenti.

Tutto questo non è sicuramente banale in quanto tale regolarità si perde andando a valutare piani di Galois di ordine pari.

5. La geometria del triangolo nel caso pari

Nel caso di piani di ordine pari, si è già introdotto un prodotto interno, che essendo non commutativo, induce una perpendicolarità un po' stravolta.

Si tratta di una perpendicolarità ordinata, ossia, diremo che due vettori u e v sono perpendicolari nel verso v verso u , se $u * v = 0$, usando la seguente notazione:

$$u \perp v \Leftrightarrow u * v = 0$$

In tale ambiente, tra l'altro non ha alcun senso parlare di asse di un segmento o di punto medio in accordo con il fatto che 2 non è invertibile.

Considerando, dunque lo pseudo-prodotto interno e la norma da esso indotta, definiti nel paragrafo2, vogliamo introdurre la nozione di pseudo-asse di un segmento come luogo geometrico dei punti equidistanti dagli estremi del segmento.

Dato un segmento P_1P_2 , chiameremo pseudo-asse il luogo dei punti P , per i quali vale la relazione:

$$N(P_1, P) = N(P_2, P)$$

Svolgendo i calcoli, si ha:

$$(y_1 + y_2)x + (x_1 + x_2)y = N(P_1) + N(P_2)$$

che è parallela alla retta P_1P_2 .

Sempre partendo dalla nozione classica di circonferenza, come luogo dei punti $P(x, y)$ che hanno norma costante R rispetto ad un punto $C(\alpha, \beta)$, detto centro, si trova l'equazione:

$$(x - \alpha)^2 + (x - \alpha)(y - \beta) + \theta(y - \beta)^2 = R$$

Per cui, data un'equazione del tipo:

$$x^2 + xy + \theta y^2 + ax + by + c = 0$$

per confronto, si trovano le formule per il centro e per la norma.
Ossia:

$$\alpha = b, \beta = a, R = b^2 + ab + \theta a^2 + c = N(b, a) + c = N(\alpha, \beta) + c$$

Dunque, mentre siamo impossibilitati a definire il baricentro di un triangolo, nel caso pari, siamo in grado di trovare l'intersezione degli pseudo-assi e dimostrare che è proprio il centro della circonferenza passante per i tre vertici del triangolo.

Ovvero:

Teorema 6. I tre assi di un triangolo, definito in un piano pseudo-euclideo di ordine pari, si incontrano in un medesimo punto che è anche il centro della circonferenza passante per i tre vertici.

Vediamo, ora, qualche esempio concreto.

Esaminiamo un piano pseudo-euclideo su $F = GF(8) = GF(2^3)$.

Ricordiamo che gli elementi di tale campo sono:

$$\{0, 1, i, i+1, i^2, i^2+1, i^2+i, i^2+i+1\}, \text{ con } i^3 = i+1.$$

L'elemento di prima categoria con il quale si costruisce la norma è $\theta = i+1$.

Assumiamo come vertici del triangolo i punti:

$$P_1(i+1, i^2), \quad P_2(1, i), \quad P_3(i^2 + i, i^2 + i + 1)$$

Le equazioni dei lati sono:

$$(i+1)x + y + 1 = 0 \quad P_1P_2$$

$$(i^2 + 1)x + (i^2 + i + 1)y = 0 \quad P_2P_3$$

$$(i+1)x + (i^2 + 1)y + i^2 + i + 1 = 0 \quad P_1P_3$$

Per determinare l'asse di P_1P_2 , si eguagliano le norme $N(P, P_1)$ e $N(P, P_2)$, con $P(x, y)$ variabile.

Per cui, da $N(P, P_1) = N(P, P_2)$, si ottiene l'equazione dello pseudo-asse di P_1P_2 , che è parallelo al lato P_1P_2 :

$$(i+1)x + y + i^2 + i = 0 \quad r$$

Allo stesso modo, eguagliando $N(P, P_2)$ e $N(P, P_3)$, si ottiene l'equazione dello pseudo-asse del lato P_2P_3 :

$$(i^2 + 1)x + (i^2 + i + 1)y + i^2 + i + 1 = 0 \quad s$$

che risulta parallelo al lato P_2P_3 .

Analogamente, dalla $N(P, P_1) = N(P, P_3)$, si ottiene l'equazione dello pseudo-asse di P_1P_3 , che è parallelo al lato P_1P_3 .

L'intersezione dello pseudo-asse r con il lato P_1P_3 è il punto $A(i^2 + i, i^2 + i + 1)$ che coincide con il vertice P_3 .

L'intersezione dello pseudo-asse s con il lato P_2P_3 è il punto B coincidente con il punto $A(i^2 + i, i^2 + i + 1)$.

L'intersezione dello pseudo-asse s con il lato P_1P_2 è il punto $C(0,1)$ e con il lato P_1P_3 è il punto $D(1, i+1)$.

Infine le intersezioni dello pseudo-asse t con il lato P_1P_2 è il punto $E(i, i^2 + i + 1)$ e con il lato P_2P_3 è il punto $F(0,0)$.

Dunque:

Uno pseudo-asse passa per il vertice opposto.

Assumiamo, ora, come vertici del triangolo i punti:

$$P_1(i+1, i^2), \quad P_2(1, i), \quad P_3(i, 1)$$

Le equazioni dei lati sono:

$$(i+1)x + y + 1 = 0 \quad P_1P_2$$

$$x + y + i + 1 = 0 \quad P_2P_3$$

$$(1+i^2)x + y = 0 \quad P_1P_3$$

Procedendo come sopra, si trova che l'equazione dello pseudo-asse di P_1P_2 è:

$$(1+i)x + y + i^2 + i = 0 \quad r$$

quella dello pseudo-asse di P_2P_3 è:

$$x + y + i + 1 = 0 \quad s$$

che coincide con il lato P_2P_3 .

Dunque:

Uno pseudo-asse coincide con uno dei lati.

Analizziamo un ultimo caso in cui i tre pseudo-assi intersecano i lati del triangolo in sei punti distinti e diversi dai vertici.

Siano:

$$P_1(i^2, i), \quad P_2(i^2 + i, i + 1), \quad P_3(i, i^2 + i + 1)$$

Le equazioni dei lati sono:

$$x + iy = 0 \quad P_1P_2$$

$$x + y + i^2 + 1 = 0 \quad P_2P_3$$

$$i^2x + y + i^2 = 0 \quad P_1P_3$$

Procedendo come sopra, si trova che le equazioni degli pseudo-assi sono:

$$\text{pseudo-asse di } P_1P_2 \quad x + iy + i^2 + 1 = 0 \quad r$$

$$\text{pseudo-asse di } P_2P_3 \quad x + iy = 0 \quad s$$

$$\text{pseudo-asse di } P_1P_3 \quad i^2x + y + i^2 = 0 \quad t$$

Le intersezioni tra i lati e gli pseudo-assi sono i sei punti seguenti:

$$rI \begin{cases} P_1P_3 \rightarrow A(i + 1, i + 1) \\ P_2P_3 \rightarrow A'(i^2 + 1, 0) \end{cases}$$

$$sI \begin{cases} P_1 P_3 \rightarrow B(0, i) \\ P_1 P_2 \rightarrow B'(i^2 + 1, i^2 + i + 1) \end{cases}$$

$$tI \begin{cases} P_1 P_2 \rightarrow C(1, i^2 + 1) \\ P_2 P_3 \rightarrow C'(i^2 + i, i^2) \end{cases}$$

6. Un' applicazione: un sistema di autenticazione

Un sistema di autenticazione è basato su una funzione f di due variabili ed una chiave segreta K .

La procedura è la seguente:

1. un individuo S manda un messaggio M ed un autenticatore, che dipende da M e da K , $a = f(K, M)$;
2. un individuo R a cui sono stati inviati M ed a riceve un messaggio M' ed un autenticatore a' . Per un problema di trasmissione o per manomissione di una spia B , può succedere che sia $M \neq M'$ oppure $a \neq a'$.
3. R calcola $a'' = f(K, M')$. Se $a' = a''$ allora R considera il messaggio M' come originale, ovvero $M' = M$, altrimenti M risulta alterato.

Un buon modello di tale sistema si ottiene considerando un piano proiettivo finito di ordine q , π_q . Si assume che i messaggi siano punti di una fissata retta r di π_q e le chiavi siano i punti di $\alpha_q = \pi_q - r$. Data, dunque, una chiave K ed un messaggio M , si ammette come autenticatore la retta passante per K e per M . Rappresentando i punti in coordinate omogenee, si può pensare la retta r come la retta impropria, a meno di proiettività.

Un messaggio M è un punto del tipo $(0,1,m)$ ed una chiave K un punto del tipo $(1,x_0,y_0)$. In modo più sintetico, scriviamo $M = [m]$ e $K = [x_0, y_0]$.

La retta $y - y_0 = m(x - x_0)$, espressa in coordinate non omogenee, risulta essere l'autenticatore; dunque, noto il messaggio M e la chiave K , la retta a per K ed M , è individuata dalla coppia $(m, h = y_0 - mx_0)$; noto m , la retta è individuata solo dal numero h , ossia $a = [h]$.

La valutazione della probabilità di rottura del sistema, valutata da Gilbert, Mac Williams e Sloane, conduce a dire che tale probabilità è

$$\frac{1}{\sqrt{\#chiavi}} \text{ e quindi nel nostro caso è } \frac{1}{q}.$$

L'esame di tale probabilità è stato fatto dagli autori citati in termini di ipotesi di equidistribuzione della probabilità.

Un esame più dettagliato è stato affrontato in [3] da Di Gennaro, Eugeni e Maturo e conduce a delle idee che ripeteremo, nel seguente. Conoscendo, dunque, a priori la distribuzione di probabilità della chiave e tenendo conto delle probabilità condizionate che dipendono dai criteri, con cui l'individuo B effettua le sue scelte, si evidenziano alcuni casi particolari.

L'individuo B potrebbe scegliere a caso fra tutti i punti del piano, senza alcuna informazione, potrebbe conoscere la funzione $f(x, y)$ oppure potrebbe decidere di scegliere un punto secondo una sua distribuzione di probabilità.

Nei tre casi, si ottengono, utilizzando la formula di Bayes e le probabilità condizionate, valori differenti.

Risulta interessante considerare un nuovo sistema di autenticazione basato sui concetti di metrica pseudo-euclidea.

Si è già visto la sostanziale differenza tra $GF(q)$ con q dispari e $GF(q)$ con q pari.

Nel caso dispari, fissato un vettore $u = (u_1, u_2)$, esiste a meno di parallelismo e per la commutatività del prodotto scalare, un solo vettore $v = (v_1, v_2)$ perpendicolare ad u .

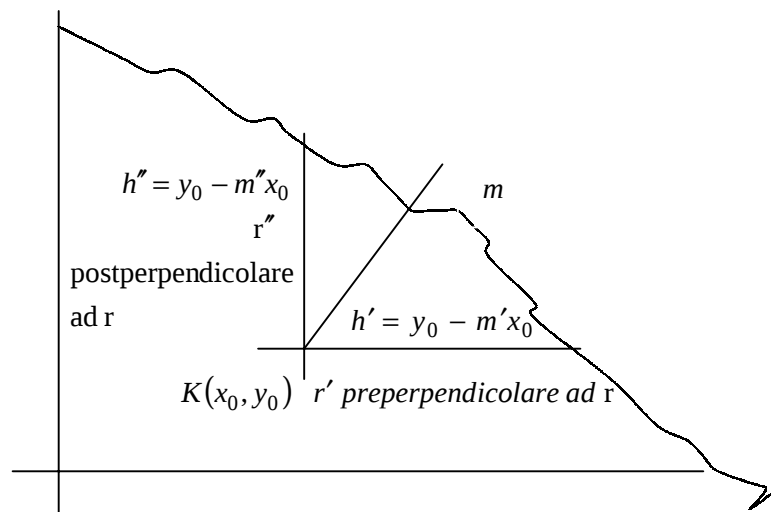
Nel caso pari, si possono definire, a meno di parallelismo e per la non commutatività del prodotto scalare, due vettori v' e v'' , perpendicolari ad u .

Distinguiamo le due perpendicolarità ordinate nominando v' pre-perpendicolare ad u , se si verifica che $v' \cdot u = 0$ e v'' post-perpendicolare ad u se risulta che $u \cdot v'' = 0$.

Dunque, mentre nel caso dispari, data una retta ed un punto P , esiste una sola retta passante per P e perpendicolare alla retta data, nel caso pari, esistono due rette.

Precisamente, poniamo:

- $r' \perp r$ se e solo se i vettori paralleli ad r' sono pre-perpendicolari a quelli paralleli ad r
- $r \perp r''$ se e solo se i vettori paralleli ad r'' sono post-perpendicolari a quelli paralleli ad r



Se $K = [x_0, y_0]$ è la chiave ed $M = [m]$ è il messaggio, si può inviare il numero $h^* = y_0 - m^* x_0$, dove m^* è il coefficiente angolare della retta per K perpendicolare alla retta KM per q dispari e di una fra le rette pre-perpendicolare o post-perpendicolare per q pari.

Nel caso dispari la sostituzione dell'autenticatore $h = y_0 - mx_0$ con l'autenticatore h^* , non modifica la probabilità di indovinare la chiave, avendo le due rette la stessa cardinalità.

Nel caso pari, invece, è possibile diminuire la probabilità che B indovini la chiave. Supponiamo che il mittente e il destinatario concordano, oltre alla chiave, una variabile z_0 , che assume valore 0, se si sceglie la pre-perpendicolare ed 1 se si sceglie la post-perpendicolare.

In questo modo la chiave K risulta sostituita dalla chiave $K^* = [x_0, y_0, z_0]$.

Indichiamo, allora con m' ed m'' , rispettivamente i coefficienti angolari delle generiche rette pre-perpendicolari e post-perpendicolari alla retta KM .

Sia $m^* = m' + z_0(m'' - m')$ ed assumiamo come autenticatore il numero $h^* = y_0 - m^* x_0$.

Se il mittente R invia il messaggio $M = [m]$ e l'autenticatore h^* , la spia B può calcolare m' ed m'' e sa che la chiave K si trova o sulla retta r' pre-perpendicolare ad M , di equazione $y = m'x + h^*$ oppure sulla retta r'' post-perpendicolare ad M , di equazione $y = m''x + h^*$, ma non sa a quale delle due rette appartiene la chiave.

L'unione delle due rette, supponendole distinte ha cardinalità $2q - 1$, maggiore della cardinalità q di r , per cui la probabilità che l'individuo B indovini la chiave risulta inferiore rispetto al sistema di autenticazione iniziale.

7. Proprietà affini e metriche delle coniche su un piano pseudo-euclideo di ordine dispari

Analogamente al caso classico, si passa dal piano affine al piano proiettivo, aggiungendo la retta impropria $x_3 = 0$ ed introducendo le coordinate omogenee (x_1, x_2, x_3) .

Denotiamo, dunque con $P = PG(2, q)$ il piano proiettivo.

Definizione 3. Sia $P = PG(2, q)$; si definisce **conica** C di P :

$$\sum_{i,j}^{1,2,3} a_{ij} x_i x_j = 0, \quad \text{con } a_{ij} \in G_q \quad \text{e } a_{ij} = a_{ji}$$

Siano C una conica ed r una retta:

- r è secante se incontra C in due punti distinti;
- r è esterna se non ha punti in comune con C ;
- r è tangente in un punto se incontra C solo in un punto.

I punti di una qualsiasi conica non degenera di $P = PG(2, q)$ sono $q+1$ e a tre a tre non allineati.

Tale proposizione si può invertire in virtù del seguente teorema:

Teorema (di B. Segre). Ogni insieme di $q+1$ punti di $P = PG(2, q)$ (q dispari), di cui mai tre allineati, risulta una conica non degenera⁵.

In maniera analoga al caso classico, si dà la definizione di polarità rispetto ad una conica, nel modo seguente:

⁵ Tale teorema fu in primo luogo presentato da B. Segre come congettura. Tale congettura fu giudicata improponibile da molti matematici discreti. Tuttavia Segre riuscì a dimostrare la sua congettura e a fondare l'intera teoria dei K -archi.

Definizione 4. Sia $P = PG(2, q)$; si definisce **polare** di un punto

$P(y_1, y_2, y_3)$ rispetto a $\mathcal{C}$, la retta di equazione: $\sum_{i \neq j}^{1,2,3} a_{ij} y_i x_j = 0$

Una conica $\mathcal{C}$ si dice *ellisse, parabola o iperbole* a seconda che la retta impropria $x_3 = 0$, sia esterna, tangente o secante la conica $\mathcal{C}$.

Nei tre casi si ha:

$$\begin{cases} a_{12}^2 - a_{11}a_{22} \in F_1 & \text{ellisse} \\ a_{12}^2 - a_{11}a_{22} = 0 & \text{parabola} \\ a_{12}^2 - a_{11}a_{22} \in F_0 & \text{iperbole} \end{cases}$$

Le nozioni e le proprietà affini delle coniche si introducono e si stabiliscono in modo del tutto analogo al caso classico; passando alle proprietà metriche delle coniche, si definisce *asse di una conica* come diametro coniugato alla propria direzione ortogonale, ossia come asse di simmetria ortogonale di $\mathcal{C}$.

Chiamiamo *vertici* le intersezioni di $\mathcal{C}$ con gli assi.

Una parabola possiede sempre uno ed un solo asse, dato dalla polare del punto improprio in direzione ortogonale ai diametri.

L'equazione della parabola si riduce alla seguente forma canonica:

$$y^2 = 2ax$$

Un problema nello studio di una conica a centro è quello di stabilire l'esistenza degli assi.

Supponiamo che il centro di $\mathcal{C}$ sia $O(0,0)$, allora risulta:

$$a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + a_{33} = 0.$$

Sia $y = mx$ un diametro di C , la polare del suo punto improprio $(1, m, 0)$ ha equazione:

$$(a_{11} + a_{12}m)x + (a_{12} + a_{22}m)y = 0.$$

Essa è ortogonale alla $y = mx$ se e soltanto se risulta:

$$\theta a_{12}m^2 + m(a_{22} + \theta a_{11}) + a_{12} = 0 \quad (3)$$

Gli assi di C hanno coefficienti angolari m soddisfacenti (3).

Se la (3) è identicamente soddisfatta, ossia:

$$\begin{cases} a_{12} = 0 \\ a_{22} = -\theta a_{11} \end{cases}$$

allora C è una circonferenza e quindi ogni diametro di C è un asse.

In caso contrario, se :

$$\begin{cases} a_{12} = 0 \\ a_{22} + \theta a_{11} \neq 0 \end{cases}$$

allora C ha due assi, dati esattamente dall'asse x e dall'asse y .

Se $a_{12} \neq 0$ la conica C ha esattamente due assi oppure non possiede assi, a seconda che si abbia:

$$(a_{22} + \theta a_{11})^2 - 4\theta a_{12}^2 \in F_0$$

$$(a_{22} + \theta a_{11})^2 - 4\theta a_{12}^2 \in F_1$$

Si ottengono allora le seguenti forme canoniche, a seconda che sia, $-1 \in F_1$, cioè $q \equiv -1 \pmod{4}$ oppure $-1 \in F_0$:

$$-1 \in F_1 \quad \begin{cases} \frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 & \text{ellisse (con 4 vertici)} \\ \frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 & \text{iperbole (con 2 vertici)} \end{cases}$$

$$-1 \in F_0 \quad \begin{cases} \frac{x^2}{a^2} - \theta \frac{y^2}{b^2} = 1 & \text{ellisse (con 2 vertici)} \\ \frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 & \text{iperbole (con 4 vertici)} \\ \frac{x^2}{a^2} - \frac{y^2}{b^2} = 0 & \text{iperbole (senza vertici)} \end{cases}$$

Bibliografia

- [1] Di Gennaro F., Eugeni F. (1997) Strutture pseudo-euclidee su Campi di Galois, *Le Matematiche*, 52, 129-142
- [2] Cerasoli M., Eugeni F., Protasi M. (1992), *Elementi di Matematica discreta*, Zanichelli, Bologna
- [3] Di Gennaro F., Eugeni F., Maturo A., (1999) Sulla probabilità di indovinare la chiave ed alterare i messaggi in sistemi di autenticazione basati su piani proiettivi finiti, in *Atti del Congresso nazionale della Mathesis*, Teramo
- [4] Di Gennaro F., Eugeni F., (1997) La retta di Eulero in un piano pseudo-euclideo di ordine dispari, in *Atti del Congresso Nazionale Mathesis*, Caserta

- [5] Di Gennaro F., Eugeni F., La geometria del triangolo in un piano pseudo-euclideo di ordine pari
- [6] Tallini G. (1972), Introduzione alle geometrie di Galois, Testo di una Conferenza tenuta all'IAC, (non pubblicata)
- [7] Beutelspaker B. (1994), *Cryptology*, The Mathematical Association of America Ed., Washington
- [8] Segre B. (1961), *Lectures on Modern Geometry*, Ed. Cremonese, Roma