Bollettino
Unione Matematica Italiana

*Sezione A – La Matematica nella Società e nella Cultura*

Lorenzo Robbiano

# Tre Amici e la Computer Algebra

*Bollettino dell'Unione Matematica Italiana, Serie 8*, Vol. **9-A**—*La Matematica nella Società e nella Cultura* (2006), n.1, p. 1–23.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_2006_8_9A_1_1_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 2006.

Bollettino U. M. I.
La matematica nella Società e nella Cultura
Serie VIII, Vol. IX-A, Aprile 2006, 1-23

# Tre Amici e la Computer Algebra

Lorenzo Robbiano

Prima del prologo vorrei fornire qualche informazione al lettore. Quello che segue non è un articolo divulgativo (la dimostrazione di questo fatto è alla fine), si tratta di un racconto, un oggetto letterario che ha come tema la computer algebra. Vengono spesso citati i due volumi [KR00], [KR05] del libro Computational Commutative Algebra scritto da me e da Martin Kreuzer, perché in esso si trovano molte spiegazioni tecniche ai fatti matematici descritti nel racconto stesso. Viene spesso citato il software CoCoA, frutto del lavoro quasi ventennale del mio gruppo di ricerca di Genova, con il quale si mostra come risolvere i problemi. Chiaramente per il lettore non specialista possono sorgere delle difficoltà, nel caso in cui il suo interesse si sposti dal piano letterario a quello matematico. Per agevolare questo tipo di lettore, e forse anche gli altri, alla fine del racconto si trovano una appendice e una bibliografia essenziale. Nella prima vengono chiarite alcune questioni tecniche discusse, usate, o comunque citate nel testo. Nella seconda viene fornito un elenco di libri attuali, nei quali sono trattati i vari temi della computer algebra e delle sue molteplici e multiformi applicazioni.

## Prologo

Seguendo le conversazioni di un matematico Orticultore, un Fotografo e un Ballerino, si incontrano quadrati corti e quadrati magici, CoCoA e gin, carte geografiche, problemi logici, funzioni di Hilbert, palindromi dipinte su meridiane, basi di Gröbner, regine e pozzi petroliferi; il tutto filtrato dall'esperienza contadina, la magia del

colore e della musica e una certa conoscenza dell'algebra computazionale.

## CoCoA e Quadrati Corti

*Ci sono due strategie ottimali per scrivere un articolo divulgativo di matematica.*
*1. Non rivelare mai la propria strategia.*
*2.*

Una sera di autunno, ai margini del bosco che delimita un pendio coltivato, tre amici passeggiano e chiacchierano come al solito. Incuriosito dalle loro argomentazioni, mi sono permesso di seguirli, ascoltarli e riportare i loro discorsi. Naturalmente, per ragioni di *privacy* non riferirò i loro nomi, ma li indicherò con le iniziali. Ecco di seguito il resoconto.

B: Oggi i funghi si sono nascosti. Non se ne trova neppure uno.

F: Forse è meglio se ci sediamo e parliamo un poco.

O: Qualche tempo fa ho deciso di approfondire un argomento che mi ha sempre affascinato, la computer algebra, e così ho comprato il libro Computational Commutative Algebra 1 di Kreuzer e Robbiano edito dalla Springer ([KR00]) e sto per comprare anche il secondo volume Computational Commutative Algebra 2 ([KR05]), di cui comunque già conosco abbastanza bene il contenuto.

B: Computer algebra ... ne ho sentito parlare, ma precisamente di che cosa si tratta?

O: Già il nome presenta qualche problema. Chi la chiama algebra computazionale, chi computer algebra, chi calcolo simbolico(1). Ma è inutile disquisire, in matematica il problema dei nomi è intrinseco. Pensate, non conosco nessun matematico che nella terminologia usata durante la sua carriera sia riuscito a restare coerente persino con se stesso. E allora lasciamo perdere il discorso sul nome, preferisco farvi un esempio. Io sono rimasto particolarmente affascinato dalla soluzione ottenuta con CoCoA del problema dei «quadrati corti».

F: Quadrati corti, CoCoA?

O: Se calcoli il quadrato di un polinomio a coefficienti razionali, vedrai che in generale esso ha nel suo supporto un numero di termini superiore a quelli che sono nel supporto del polinomio stesso. Ad esempio il polinomio $x^2+3x+1$ ha tre termini, mentre il polinomio $(x^2+3x+1)^2 = x^4+6x^3+11x^2+6x+1$ ne ha cinque.

B: Anche se mi da un po' fastidio questo linguaggio tecnico, direi che fin qui ci arrivo anche io.

O: Potrà sembrare incredibile, ma non è sempre così. Il seguente polinomio di grado 12, che ha 13 termini nel suo supporto,

$$\begin{aligned} f =& x^{12} + \frac{2}{5}\,x^{11} - \frac{2}{25}\,x^{10} + \frac{4}{125}\,x^9 - \frac{2}{125}\,x^8 + \frac{2}{125}\,x^7 - \frac{3}{2750}\,x^6 \\ & - \frac{1}{275}\,x^5 + \frac{1}{1375}\,x^4 - \frac{2}{6875}\,x^3 + \frac{1}{6875}\,x^2 - \frac{1}{6875}\,x - \frac{1}{13750} \end{aligned}$$

ha come quadrato

$$\begin{aligned} f^2 =& x^{24} + \frac{4}{5}\,x^{23} + \frac{44}{3125}\,x^{19} + \frac{2441}{171875}\,x^{18} - \frac{2016}{171875}\,x^{17} \\ & - \frac{16719}{37812500}\,x^{12} + \frac{141}{9453125}\,x^{11} - \frac{3}{859375}\,x^7 + \frac{13}{8593750}\,x^6 \\ & + \frac{1}{4296875}\,x^5 + \frac{1}{47265625}\,x + \frac{1}{189062500} \end{aligned}$$

che ne ha solo 12.

B: Che stranezza, ma perché hai citato proprio questo astruso esempio?

O: Pochi anni fa, risolvendo con il sistema CoCoA circa centocinquantamila sistemi polinomiali, A è riuscito a dimostrare[(2)] che quello che vi ho detto è l'esempio più facile di polinomio a coefficienti razionali il cui quadrato è più «corto» del polinomio stesso.

F: Sono contento che l'abbia risolto A, siamo amici e anche lui fa delle belle fotografie. Ora incomincio a capire che cosa fa CoCoA. Ma stavi parlando del libro di Kreuzer e Robbiano. È un libro su CoCoA?

O: Certamente no, ma usa CoCoA come software di riferimento per lo sviluppo dei suoi novantanove «tutorials». Si tratta di mini-progetti, o piccole tesi o approfondimenti o divagazioni che, utilizzando le teorie algebriche spiegate nel libro, stimolano a guardarsi intorno, uscire dai rigidi fondamenti dell'algebra computazionale e spaziare nel vasto mondo delle applicazioni.

B: Va bene, ma ora non ti mettere a parlare come i cattedratici. Raccontami qualche uso dell'algebra computazionale. Altrimenti, se continui col tono serioso, ti faccio un seminario sui *giri spin* del *quick step* o sull'*opening out* della *rumba*.

O: No, per favore. Ma come faccio a dirti che cosa è l'algebra computazionale? Potrei cavarmela suggerendoti di leggere attentamente il libro?

F: Un momento, ti ricordi che cosa stava scritto su quel *fortune cookie* al ristorante cinese? *The best gift you can bestow on others is a good example*. Perchè dunque non procedi come hai incominciato e ci racconti degli esempi interessanti? O preferisci una disquisizione sulla profondità di campo o sulla saturazione del colore?

O: Basta, mi state ricattando. Mi arrendo e procederò per esempi. Ne riparliamo domani.

Si sta facendo più freddo e i tre amici ritornano verso il paese. Un sottile strato di nebbia sfuma i contorni delle cose e F sta scattando alcune fotografie in puro «stile R». Anche B si è distratto e mentalmente ripercorre i passi per l'esibizione di balli standard del giorno dopo.

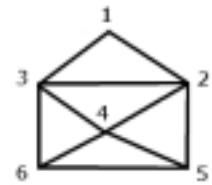
## Coloriamo le Carte Geografiche

*Teorema:* Tutti i numeri interi positivi sono interessanti.
*Dimostrazione:* Per assurdo esiste il più piccolo intero positivo non interessante.
Ma allora quel numero è molto interessante!
Contraddizione. QED

Sulla piazza del paese si è radunata molta gente. I tre amici sono seduti al tavolo di un bar e con aria incuriosita osservano, perfetti interpreti di quello che viene definito turismo statico.

O: Sapete come si fa a colorare una carta geografica con tre colori in modo che due regioni confinanti abbiano colori diversi?
F: Non mi dirai che questo problema si risolve con la computer algebra!
O: E invece sì. Puoi procedere nel seguente modo. Crei un modello matematico della carta geografica usando un grafo i cui vertici rappresentano le regioni e i cui lati rappresentano le adiacenze. Poi a ciascun vertice assegni, come nome, una indeterminata.
B: Scusa ma non capisco.

A questo punto O prende una penna e traccia un disegno su un piccolo taccuino che porta sempre con sé, dove prende appunti sulle fasi della luna e sulle rotazioni delle semine.


F: Quanti *megapixel* ha il tuo disegno?
O: Non è un numero interessante.
B: Che cosa contiene la busta?
O: Avete sempre voglia di scherzare? Intanto quella che chiami busta non è altro che il grafo i cui vertici rappresentano le regioni e i cui lati rappresentano il fatto che due regioni siano confinanti. Di conseguenza, la busta *contiene* l'essenza matematica del problema. Adesso che vedete il disegno, potete capire meglio anche il seguito. Prendete un campo finito che contenga almeno tre elementi (se volete risolvere il problema con $n$ colori, prendete un campo che contenga $n$ elementi). Associate ogni colore ad un elemento del campo, attribuite i possibili colori ad ogni vertice del grafo e poi esprimete con una equazione polinomiale il fatto che due vertici abbiano colori diversi[3]. In tale modo costruite un ideale nell'anello dei polinomi. Calcolate una

base di Gröbner ridotta[4] di tale ideale. Se ottenete 1, il problema non è risolubile, altrimenti è risolubile e dalla suddetta base potete dedurre, con qualche calcolo in più, anche le soluzioni. Ad esempio il codice CoCoA che risolve il problema nel caso suddetto è il seguente.

```
Use P ::= Z/(3)[x[1..6]];
F(X) := X*(X-1)*(X+1);
VerticesEq:= [F(x[I]) | I In 1..6 ];
Edges := [[1,2],[1,3],[2,3], [2,4], [2,5], [3,4],
          [3,6], [4,5], [4,6], [5,6]];
EdgesEq :=[(F(x[A[1]])-F(x[A[2]]))/(x[A[1]]-x[A[2]])
                  | A In Edges ];
I := Ideal(VerticesEq) + Ideal(EdgesEq) +
       Ideal(x[1]-1, x[2]);
ReducedGBasis(I);
[x[2], x[1]-1, x[3]+1, x[4]-1, x[6], x[5]+1]
```

Se ad esempio 0 significa blu, 1 rosso, $-1$ verde, si ha:
nazione 1 = rosso; nazione 2 = blu; nazione 3 = verde;
nazione 4 = rosso; nazione 5 = verde; nazione 6 = blu.

F: Pablo Picasso diceva che i calcolatori sono inutili, perché possono dare solo risposte. Ma in qualche caso bisogna ammettere che le risposte sono veramente interessanti.

## Chi Mente?

*ella va amica da cima a valle*
(Robbiano, verso palindromico dipinto su una meridiana a Castelletto d'Orba)

Non piove più. Il filo dei pensieri di O passa attraverso la famosa palindrome dedicata alle nuvole: *e voi pesate metà se piove*. Palindromi, enigmi, rebus simbolici, trappole semantiche, fascino e limiti della logica. In perfetta sintonia interviene improvvisamente F e interrompe il silenzio.

F: La computer algebra può anche risolvere problemi logici[5]?

B: Prima che tu risponda, forse facendo una disquisizione che non

capirei, ti faccio una domanda specifica. Su una rivista ho trovato la seguente domanda.

TRE COLLEGHI, A, B, C CONVERSANO. A DICE: «B MENTE»; B DICE: «C MENTE»; C DICE: «A E B MENTONO». CHI MENTE?

O: Benissimo, questo è un problema che si può risolvere ricorrendo ad un modello polinomiale. Seguitemi, il discorso non è difficile. Per rispondere alla domanda, codifichiamo VERO con 1 e FALSO con 0 nel campo $\mathbb{Z}/2\mathbb{Z}$. Poi usiamo tre indeterminate $a, b, c$ che corrispondono ai tre colleghi. La frase – a DICE: «b MENTE» – corrisponde ad $a = 0,\ b = 1$ oppure $a = 1,\ b = 0$, quindi viene codificata con l'ideale $I_{12} = I_1 \cap I_2$ dove $I_1 = (a,\ b - 1)$, $I_2 = (a - 1,\ b)$. Analogamente la frase – b DICE: «c MENTE» – corrisponde a $b = 0,\ c = 1$ oppure $b = 1,\ c = 0$, quindi viene codificata con l'ideale $I_{34} = I_3 \cap I_4$ dove $I_3 = (b,\ c - 1)$, $I_4 = (b - 1,\ c)$. Se ci riflettete un poco, la frase – c DICE: «a e b MENTONO» – viene codificata con $I_{5678} = I_5 \cap I_6 \cap I_7 \cap I_8$, dove $I_5 = (a, b, c - 1)$, $I_6 = (a, b - 1, c)$, $I_7 = (a - 1,\ b,\ c)$, $I_8 = (a - 1,\ b - 1,\ c)$ Ora mettiamo insieme tutte le condizioni considerando l'ideale $J = I_{12} + I_{34} + I_{5678}$ e calcoliamo una base di Gröbner ridotta di $J$. Eccovi il codice CoCoA che fa esattamente quello che vi ho detto.

```
Use S::=Z/(2)[a,b,c];
I1:=Ideal(a, b-1);    I2:= Ideal(a-1, b);
I12:=Intersection(I1,I2);
I3:=Ideal(b, c-1);    I4:= Ideal(b-1, c);
I34:=Intersection(I3,I4);
I5:=Ideal(a, b, c-1); I6:= Ideal(b-1, a, c);
I7:= Ideal(b, a-1, c); I8:= Ideal(b-1, a-1, c);
I5678:=Intersection(I5,I6,I7,I8);
J:= I12 + I34 + I5678; ReducedGBasis(J);
    ------------------
    [a, b+1, c]
```

La risposta di CoCoA è dunque che l'unica soluzione al nostro problema è $a = 0,\ b = 1,\ c = 0$, quindi a e c mentono, mentre b dice il vero.

F: La risposta mi sta bene, infatti la posso verificare facilmente, ma chi mi garantisce che sia l'unica possibile?
O: La base di Gröbner ridotta. Come vedi, si tratta di tre polinomi lineari che esplicitamente forniscono solo la soluzione che vi ho detto.

## Poniamo le Basi

*Se non puoi realizzare l'ideale, idealizza il reale.*
(Dal «Manuale di filosofia genovese»)

F: Mi sembra di capire che tutti gli esempi di cui ci hai parlato si risolvono calcolando basi di Gröbner. Sono così importanti?
O: Si tratta di basi speciali di ideali polinomiali e sono il piedistallo della computer algebra. Fino a qualche anno fa erano viste come oggetti stravaganti, ma oggi vengono scoperte e riscoperte continuamente e soprattutto usate nei più svariati settori anche fuori dalla matematica.
B: In che senso sono basi ideali?
O: Non ho detto *basi ideali* ma *basi di ideali*. Però a pensarci bene hai ragione anche tu. Seguitemi un momento, vi faccio un altro esempio così ci capiamo meglio. Voi due sapete che cosa sono i sistemi lineari e che cosa è la riduzione gaussiana. Considerate due polinomi lineari omogenei $f_1 = x_1 - 2x_2 + 3x_3$, $f_2 = x_1 + x_2 - 3x_3$ e il sistema lineare associato

$$\begin{cases} x_1 - 2x_2 + 3x_3 &= 0 \\ x_1 + x_2 - 3x_3 &= 0 \end{cases}.$$

Se chiamate $I$ l'ideale generato dai due polinomi $f_1, f_2$, allora l'insieme $\{f_1, f_2\}$ non è una base di Gröbner di $I$.
F: Mi sembra di ricordare che per parlare di basi di Gröbner si deve avere un ordinamento sui termini. Non è vero?
O: Hai perfettamente ragione. Ma nel caso di polinomi lineari basta ordinare le indeterminate. Nel nostro esempio è tacitamente assunto che si abbia $x_1 > x_2 > x_3$. Con un passo di riduzione

gaussiana si ottiene il polinomio lineare $f_3 = 3x_2 - 6x_3$ e il sistema equivalente

$$\begin{cases} x_1 - 2x_2 + 3x_3 &= 0 \\ \quad 3x_2 - 6x_3 &= 0 \end{cases}.$$

Come detto, il sistema è equivalente e l'ideale non cambia, ossia l'ideale generato da $\{f_1,\ f_3\}$ è $I$. Ora abbiamo un nuovo sistema di generatori $\{f_1,\ f_3\}$ e questa è una base di Gröbner di $I$.

B: Finalmente!

O: Ma la storia non finisce qui. Intanto è chiaro che si può sostituire $f_3$ con $f_3' = x_2 - 2x_3$ e anche $\{f_1,\ f_3'\}$ è una base di Gröbner di $I$, con in più la proprietà che i suoi elementi sono polinomi monici. Infine, si può fare ancora un passo di riduzione e ottenere $f_1' = f_1 + 2f_3' = x_1 - x_3$. In conclusione, il sistema di partenza è equivalente al sistema

$$\begin{cases} x_1 - \ x_3 &= 0 \\ x_2 - 2x_3 &= 0 \end{cases}.$$

L'insieme di generatori $\{x_1 - x_3,\ x_2 - 2x_3\}$ di $I$ è la base di Gröbner ridotta di $I$.

F: Perché hai detto «la base» e non «una base»?

O: Proprio questa è la straordinaria proprietà della base di Gröbner ridotta, quella di essere unica *una volta fissato l'ordinamento*. Il fatto ha conseguenze molto interessanti anche dal punto di vista teorico. Ma siccome voi non volete sentir parlare troppo di teoria, ritorno all'esempio appena descritto. Esso fornisce solo una indicazione, in realtà si riesce a fare la stessa cosa per sistemi polinomiali, o, come dicono gli algebristi, per gli ideali, anche se le cose si complicano notevolmente.

B: Ancora questi ideali! In realtà, che cosa hanno di ideale?

È scesa la sera e O si avvia rapidamente a coprire le serre. Di ideali si riparlerà presto.

## La Formula di Erone

*Dove sta esattamente l'ortocentro?*
(Dal volume: «Le domande del contadino»)

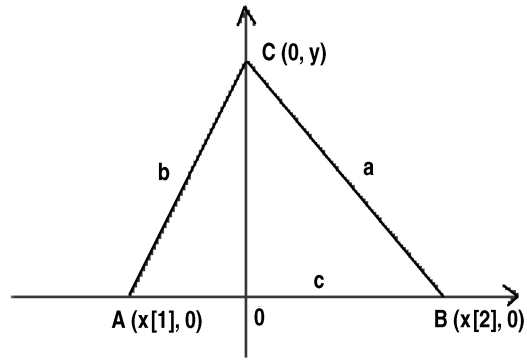
Lontano dalla strada principale i tre amici passeggiano. B è totalmente assorbito da pensieri che intrecciano *linee di ballo, diagonali, spin, giri a destra e a sinistra, opening out, triangoli, giri naturali con uscita in promenade*. Nel frattempo F sta meditando su una strana fotografia in cui si intersecano un'infinità di triangoli di forme diverse che si perdono all'orizzonte. Pitagora, Erone, Escher, realtà immaginarie, fotografie del pensiero, ... queste meditazioni sono interrotte da O che, quasi stesse parlando con se stesso dice:

O: Chi avrebbe mai detto che la formula di Erone potesse essere dedotta dal calcolatore.
B: Erone, il libertino greco?
O: Se fosse libertino proprio non lo so, ma so che con il suo nome si intende la nota formula

$$16\,s^2 = (a+b+c)(a+b-c)(a-b+c)(-a+b+c)$$

che esprime l'area $s$ di un qualsiasi triangolo in funzione delle lunghezze $a, b, c$ dei suoi lati.
F: Che cosa vuoi dire quando affermi che la formula può essere dedotta dal calcolatore? Non ci vorrai convincere che l'ossimoro si è trasformato in realtà!
B: Ossimoro? Potrei sapere di che cosa state parlando?
O: A volte siete proprio insopportabili! Oltre al fatto di essere tutti juventini, spesso mi chiedo che cosa ci accomuna e ci rende amici. Comunque sia, conoscendo il suo scetticismo, credo di capire che quando parlava di ossimoro, F si riferisse all'espressione «intelligenza artificiale». Ebbene sì, in questo caso il calcolatore può esibirsi in qualcosa che assomiglia all'intelligenza umana, nel senso che la formula di Erone può essere *scoperta* dal calcolatore. Vi spiego come.

Dicendo così, estrae dalla tasca il solito taccuino e disegna




O: L'idea è quella di considerare un ideale generato da quattro polinomi. I primi due traducono in formula il teorema di Pitagora applicato ai due triangoli rettangoli OBC e AOC, il terzo esprime la lunghezza del lato AB in funzione delle coordinate dei suoi estremi e l'ultimo il fatto che la doppia area del triangolo coincide con il prodotto della base per l'altezza. Siamo a livello di scuola secondaria. In questi polinomi compaiono le indeterminate $x_1, x_2, y, a, b, c, s$. Se si riuscisse ad *eliminare* $x_1, x_2, y$ dall'ideale, si andrebbe a vedere se ci sono relazioni polinomiali che legano $a, b, c, s$. Ed ecco il codice CoCoA che risolve la questione.

```
Use Q[x[1..2],y,a,b,c,s];
A := [x[1], 0];
B := [x[2], 0];
C := [ 0, y];
Hp := Ideal(a^2 - (x[2]^2+y^2), b^2 - (x[1]^2+y^2),
           c - (x[2]-x[1]), 2s-cy);
E := Elim(x[1]..y,Hp);
F := Monic(Comp(Gens(E),1));
F;
a^4 -2a^2b^2 +b^4 -2a^2c^2 -2b^2c^2 +c^4 +16s^2

Factor(F-16s^2);
[[a + b + c, 1], [a + b - c, 1], [a - b + c, 1],
 [-a + b + c, 1]]
```

Il risultato si traduce nella relazione:

$$16\,s^2 = (a+b+c)(a+b-c)(a-b+c)(-a+b+c)$$

che è appunto la formula di Erone.

F: Ricordo l'appello di Shreeram S. Abhyankar ([Abh76]) che suggeriva di *eliminare gli eliminatori della teoria dell'eliminazione*. Vuoi dire che gli algebristi computazionali hanno accolto l'appello e hanno riportato alla moda quella teoria?

B: Ormai con le basi di Gröbner si fa di tutto, ti stupisci che si faccia anche l'eliminazione?

O: Infatti, usando particolari ordinamenti, detti appunto di eliminazione, si può calcolare l'ideale che si ottiene intersecando l'ideale dato con il sottoanello generato dalle indeterminate che non sono eliminate. I geometri sanno che questa operazione corrisponde alla proiezione di una varietà da uno spazio affine su un sottospazio affine di dimensione inferiore[(6)]. Come vedete, dando in pasto il codice CoCoA al computer si ottiene un polinomio che, opportunamente riscritto usando raffinati algoritmi di fattorizzazione multivariata, esprime la formula di Erone. Il computer ha *scoperto* la formula di Erone. Non è un fatto straordinario?

F: Forse ci si può spingere oltre e chiedere al calcolatore di dimostrare tutti i teoremi?

O: No, Gödel ci ha fatto capire che la risposta è no. Si può cercare di dimostrare alcuni teoremi, ma anche questa limitata ambizione è destinata a scontrarsi con problemi in parte matematici, in parte filosofici. Kreuzer e Robbiano dedicano interamente l'ultima sezione di [KR05] a questo affascinante problema. Rubo un paio delle loro citazioni, che, con la solita dose di umorismo, rappresentano bene alcune intrinseche difficoltà della dimostrazione automatica.

*The* real *world is* complex.
True *statements may be* false.

*How about proving a theorem*
*without knowing which?*
(from «Mathematical Nightmares»)

B: Basta, mi state portando troppo fuori dalla realtà. Vi siete accorti che ha incominciato a nevicare?

Ora la sintesi del bianco e del silenzio rende la scena ancora più irreale. I triangoli, le formule, i teoremi, gli algoritmi lasciano spazio a nuove sensazioni, rese più intense dall'aria fredda nella quale si diffonde da lontano una parvenza di musica. Forse l'adagietto della Quinta di Mahler, o il tema di Nuovo Cinema Paradiso di Morricone?

## Giochiamo a Scacchi

*La matematica è come il gioco degli scacchi,*
*è adatta ai giovani, non è troppo difficile,*
*è divertente e non è pericolosa per lo stato.*
(Platone)

Finita la nevicata, resta la solita atmosfera un poco triste, un poco euforica e una strana mescolanza di malinconia e sensualità. I tre amici si ritrovano seduti accanto al camino.

F: Mio zio dice spesso che *due terzi della popolazione non conosce le frazioni, all'altra metà non interessano*.

B: Mio cugino dice spesso che *nel mondo ci sono due gruppi di persone, quelli che credono che nel mondo ci siano due gruppi di persone e quelli che non ci credono*.

O: Sono contento che vi stiate divertendo. A me piace molto ascoltare il mio amico K, scacchista di fama internazionale, quando mi parla di problemi di scacchi. Ad esempio mi ha sempre affascinato il problema delle otto regine[7].

B: Otto regine? Troppe per i miei gusti.

O: Se la smettete di scherzare vi racconto il problema e la sua soluzione con la computer algebra. Dunque la questione è molto semplice. Quante regine si possono mettere su una scacchiera in modo che non si attacchino l'una con l'altra? Tutti gli appassionati di scacchi sanno che la risposta è otto. Con un poco di ingegno si riesce anche a mano a trovare una soluzione. Ma la cosa affascinante è che tutto si può tradurre in ideali e basi di Gröbner e dunque farlo risolvere al calcolatore. Inoltre, si riesce

anche a calcolare in quanti modi distinti si possono mettere le otto regine sulla scacchiera. E se questo non vi basta, vi dico che il metodo è tale per cui il numero di righe e colonne della scacchiera è semplicemente un parametro del problema.

F: Vuoi dire che si può risolvere su una scacchiera $n \times n$ con $n$ a piacere?

B: Ma che piacere? A chi interessa sapere quante regine si possono piazzare su una scacchiera $4 \times 4$? E poi, su tale scacchiera a trazione integrale si chiamerebbero ancora regine?

O: Che tu ne abbia piacere o no, il problema delle regine si risolve con CoCoA, come mostra il seguente codice.

```
Chessboard := 8;
Use ChessRing ::=
           Z/(2)[x[1..Chessboard, 1..Chessboard]];
Define QueenIdeal(Csb)
  I := Ideal();
  Foreach Sq In (1..Csb) >< (1..Csb) Do
    I := I + QueenMovesFrom(Sq,Csb)*x[Sq[1],Sq[2]];
  EndForeach;
  Return I;
EndDefine;
Define QueenMovesFrom(Sq, Csb)
  H := [ x[ Sq[1], I ] | I In (Sq[2]+1)..Csb ];
  V := [ x[ I, Sq[2] ] | I In (Sq[1]+1)..Csb ];
  D := [ x[ Sq[1]+I, Sq[2]+I ] |
         I In 1..Min(Csb-Sq[1],Csb-Sq[2]) ];
  AD := [ x[ Sq[1]+I, Sq[2]-I ] |
         I In 1..Min(Csb-Sq[1], Sq[2]-1) ];
  Return Ideal(H) +Ideal(V) +Ideal(D) +Ideal(AD);
EndDefine;

Queen := ChessRing/QueenIdeal(Chessboard);
P_Queen := HilbertSeries(Queen);
Use Q[t];
P_Queen;
Dim(Queen); Multiplicity(Queen);
  ----------------
  8
  ----------------
  92
```

O: Senza entrare nei dettagli tecnici, vi faccio notare che basta sostituire `Chessboard := 8` con `Chessboard := 4` (o qualunque altro numero naturale) per risolvere il problema su scacchiere non standard. Inoltre vedete che `Multiplicity(Queen)` fornisce 92. È la risposta alla domanda: in quanti modi si possono mettere le 8 regine sulla scacchiera così che non si attacchino tra di loro? La chiave di tutto è la straordinaria efficienza di CoCoA nel calcolare le funzioni di Hilbert.
B: Quale è stata la funzione di Hilbert?
O: Ha avuto e ha un enorme rilievo nella matematica attuale. Oops ... ci sono caduto. Ovviamente parlavo di funzioni di Hilbert, intese come particolari funzioni numeriche che i nostri antenati chiamavano formule di postulazione.
B: Erano mendicanti?
O: Sei insopportabile.
F: Si possono sostituire le regine con le torri, con gli alfieri, o con i pedoni?
O: Domanda intrigante. Con le torri e con gli alfieri non c'è problema. Per i pedoni la questione è differente. Il modello matematico ha bisogno dei polinomi non commutativi, dove le cose cambiano radicalmente.
F: Dove è la difficoltà?
O: Mentre per regine, torri e alfieri se la mossa che va da una casella $x$ a una casella $y$ è lecita, lo è anche quella che va da $y$ a $x$, i pedoni vanno solo avanti, non camminano al contrario.
B: E, come dice mio cugino, *non è facile leggere la oirartnoc*.
O: Appunto, è un vero piacere spiegarti le cose e vedere come le capisci al volo.

## Magie dell'Algebra

Ottimista: *Se l'economia continua ad andare così, presto tutti andremo a chiedere l'elemosina*
Pessimista: *A chi?*

Quando la luce taglia in diagonale le facciate degli antichi palazzi, vengono alla mente le parole della giornalista Phyllis Macchioni[8]:

*Genoa [...] first seduces you, puts you under its spell, and then only little by little allows you to see its magic.* Riquadri dove la luce si imbeve di colore uscendo dal buio dei vicoli, dove la fotografia può rivelare simmetrie nascoste. Geometria del colore allo stato puro. Assorto in questi pensieri F incontra O e B.

F: Credevo che l'espressione «quadrato magico» si riferisse solo alla fotografia. Ma ho sentito dire che ha una storia più lunga.

O: Molto più lunga. Pensate che nel 2200 a.c. i cinesi decorarono il guscio di una tartaruga divina con un quadrato magico. Molto più tardi, nel medioevo alcuni alchimisti credettero che i quadrati magici possedessero la chiave per convertire i metalli in oro.

B: Non come le moderne banche centrali che quotidianamente cercano di convertire l'oro in carta priva di valore.

O: Sia gli alchimisti che i banchieri centrali sono destinati al fallimento, con la differenza che il fallimento degli alchimisti non nuoce a nessuno, mentre quello dei banchieri ci porterà a crisi economiche inimmaginabili. Ma torniamo ai nostri quadrati. Il più famoso è sicuramente il *quadrato magico di Giove* dipinto nel 1514 da Albrecht Dürer nella sua litografia Melencolia. Eccolo

| | | | |
|---|---|---|---|
| **16** | **3** | **2** | **13** |
| **5** | **10** | **11** | 8 |
| **9** | **6** | **7** | **12** |
| **4** | **15** | **14** | **1** |

Vi consiglio di non guardarlo troppo, perché quando crederete di averne scoperto tutte le proprietà, ne troverete una nuova. Ecco perché gli astrologi del Rinascimento pensavano che esso potesse curare la *melencolia*, uno stato depressivo che distrugge l'entusiasmo dell'artista per il suo lavoro.

F: Se ha questo potere, lo porterò con me durante le mie gite fotografiche.

B: E io alle mie gare di ballo. Ma ora sono curioso, puoi descriverci le sue proprietà principali?

O: La somma delle entrate delle sue righe, delle sue colonne e delle sue due diagonali è 34. Queste due proprietà lo fanno chiamare *quadrato magico di dimensione 4 e di somma magica 34*. Ma il

quadrato di Dürer ha altre proprietà. Ad esempio la somma delle entrate delle sottomatrici $2 \times 2$ centrate sulle due diagonali è 34; la data di composizione si legge nelle due entrate centrali della quarta riga; tutti i numeri da 1 a 16 sono usati una e una sola volta come entrate. Vi basta?

F: Sì, ma la computer algebra entra in gioco anche qui [(9)]?

O: Figuratevi se ai matematici non veniva voglia di contare quanti sono i quadrati magici di varia dimensione, con data somma magica e così via. Solo che per questo problema la pura potenza delle funzioni di Hilbert può non essere sufficiente. Altri strumenti matematici devono essere usati, quali gli ideali torici e le basi di Hilbert.

F: Ideali torici? Ma chi inventa questi nomi così buffi?

B: Non ti sembra che il nome Hilbert sia un poco inflazionato?

O: Sì, ma questo tipo di inflazione non è pericoloso.

F: Naturalmente ora ci propinerai il codice CoCoA che conta il numero dei quadrati magici.

O: No, questa volta no, il mio amico R mi ha pregato di non svelare troppi segreti. L'unica cosa che vi posso dire è che i quadrati con tutte le proprietà di quello magico di Giove ... sono pochissimi. Ma non chiedetemi quanti, la magia si nutre anche di mistero.

B: È come il fascino della musica. Quella che ti mette addosso la voglia di ballare.

Da lontano arrivano note confuse, sembra di percepire il ritmo del samba. O è bossa nova? Sensazioni brasiliane. Brasile, dove i genovesi parlano *senza accento!*

## Cocktail, Geometria, Petrolio

VeNoM
*Versare un bicchiere di* gin *in uno shaker,*
*aggiungere un cucchiaino di* CoCoA,
*mescolare e agitare*
(da «Cocktail matematici»)

Nell'inverno i lavori dell'orto quasi si fermano e i tre amici si trovano più spesso a conversare.

B: Parliamo un poco di cose concrete. Mi hanno detto che esiste un famoso cocktail a base di gin e cacao.

O: Se ne parla anche nel libro [KR05]. È un cocktail che produce esempi molto interessanti per i geometri algebrici.

F: I geometri algebrici bevono molti liquori?

O: Molte *varietà*, recentemente il gin è quello preferito. Sapete che «gin» è una sigla per indicare «Generic initial ideal»[(10)]. Solo che per calcolare gin $(I)$, dove $I$ è un ideale omogeneo, bisogna vincere una scommessa.

B: Ancora ideali! Ma la scommessa mi interessa.

O: Mi lasciate parlare? Dicevo che data l'importanza anche teorica del gin viene voglia di calcolarlo esplicitamente. Ma siccome per fare il calcolo si deve prima fare un cambiamento generico di coordinate, e quindi introdurre un grande numero di nuove indeterminate, anche il più potente calcolatore fa poca strada. E qui gli algebristi computazionali ne hanno inventata una bella. Invece di fare un cambiamento generico di coordinate, ne fanno uno *random*. In altre parole, invece di riempire la matrice di trasformazione con indeterminate, la riempono con numeri a caso.

F: E se i numeri a caso non sono abbastanza a caso?

O: Senti, la probabilità che non siano a caso è sostanzialmente la stessa che tu avresti di indovinare un numero intero, da me pensato. Quanto credete che sia? Io dico zero.

B: Non sottovalutare la mia fortuna. Avevo indovinato che avresti detto zero.

O: Lasciamo perdere. Comunque sia, con quel trucco, o scommessa se preferite, si fanno calcoli molto interessanti almeno per i geometri algebrici.

F: Ho letto la celebre frase attribuita a Charles Darwin: *il matematico è un uomo cieco in una stanza buia, che cerca un gatto nero che non c'è*. E se parlo con la gente, mi rendo conto che queste forme di pregiudizio sono forti anche al giorno d'oggi. Non parliamo poi dei pregiudizi sull'utilità dell'algebra. Come te lo spieghi?

O: Forse la gente non sa che oggi con l'algebra si studiano modelli

polinomiali per problemi di statistica, di robotica, di elettronica. E che dire dei recentissimi sviluppi di modelli polinomiali per i giacimenti petroliferi [(11)]?

B: Speriamo che riescano a far scendere il prezzo della benzina. Ma mi sembra che sia tu ora quello che scherza.

O: Niente affatto, chiedi a R e vedrai che ne avrai conferma.

F: Si è fatto veramente tardi. Vi saluto e spero di continuare presto questi discorsi. Non credo che capirò molto, ma mi è venuta voglia di comprare il libro.

B: E a me di provare ad usare CoCoA.

È notte e fa freddo. Sulla strada ancora leggermente innevata i tre amici si sono allontanati e non si vedono più. Mi giungono ancora alcune parole, pronunciate non so da chi .... *la luna e i falò, G, le diapositive, il valzer lento, C, F* ... anche per me è l'ora di tornare a casa.

*Ci sono solo due tipi di articoli divulgativi;*
*quelli che non si possono leggere oltre la prima frase*
*e quelli che non si possono leggere oltre la prima pagina.*

## APPENDICE

Come detto all'inizio, qui il lettore può trovare suggerimenti e osservazioni per una migliore comprensione della parte matematica del racconto.

(1) Le locuzioni «computer algebra», «algebra computazionale», «calcolo simbolico» nel testo sono considerate equivalenti, anche se per alcuni autori calcolo simbolico riguarda una più ampia serie di argomenti. Tutti i temi matematici trattati sono ampiamente descritti nei già citati volumi [KR00] e [KR05]. Tra i testi basilari della computer algebra moderna mi piace menzionare [AL94], [CLS92], [CLS04], [GG03], [GKW03], [GKW03], [GP02], [Ste04], [Stu96], [Stu02].

(2) La semplice idea di base è la seguente. Se un polinomio $f(x)$ ha coefficienti generici, il suo quadrato ha coefficienti che sono poli-

nomi di secondo grado nei coefficienti di $f(x)$. Per avere molti coefficienti nulli nel quadrato è necessario che molti polinomi di secondo grado si annullino. Ecco spiegato il perché si devono risolvere tanti sistemi polinomiali. Per i dettagli si vedano il lavoro [A02] e il Tutorial 43 in [KR00].

(3) Come quasi tutti gli esempi considerati nel testo, questo è chiaramente un «esempio giocattolo» usato a fini espositivi, ma serve ad illustrare l'idea di base che è la seguente. Se ho ad esempio due vertici, i loro nomi sono $x$ e $y$ e ho scelto $\mathbb{Z}/(3)$ come campo con tre elementi (tutti i campi con tre elementi sono isomorfi), le equazioni che si deducono subito sono $x(x-1)(x+1)=0$, $y(y-1)\ (y+1)=0$, il che significa semplicemente che ad ogni vertice viene associato uno dei tre possibili colori. Se i due vertici sono adiacenti (nel nostro problema questo significa che le regioni da essi rappresentate sono confinanti), dobbiamo esprimere con una equazione polinomiale il fatto che i colori dei due vertici devono essere *diversi*. Osserviamo che per tutte le coppie di colori è verificata l'equazione $x(x-1)(x+1)-y(y-1)(y+1)=x^3-y^3-x+y=0$. Tra queste ci sono anche le coppie uguali e sono quelle che verificano $x-y=0$. Il polinomio $x^3-y^3-x+y$ è divisibile per $x-y$ e facendo la divisione si ha $x^2+xy+y^2-1$. Quindi l'equazione che esprime il fatto che i due vertici $x$, $y$ hanno colori diversi è $x^2+xy+y^2-1=0$.

(4) Il concetto di *base di Gröbner ridotta* gioca un ruolo essenziale nella computer algebra (vedi anche le sezioni successive). Se ad esempio si considerano i polinomi $f_1=x^2-y^2+z-1$, $f_2=x^3-xy^2+xz$ $-x-2y+2z-1$, $f_3=2y-2z+1$ e se $x>y>z$, si può dimostrare (o semplicemente verificare con CoCoA) che la terna $\{f_1,f_2,f_3\}$ è base di Gröbner dell'ideale $I$ da essi generato. Allora possiamo *scartare* il polinomio $f_2$ perché il suo termine di testa è multiplo del termine di testa di $f_1$, poi possiamo dividere $f_3$ per 2 in modo da renderlo *monico*. A questo punto abbiamo $f_1=x^2-y^2+z-1$, $f_3'=y-z+1/2$. Ora possiamo *riscrivere* il polinomio $f_1$, usando $f_3'$, nel senso che da $f_3$ si ricava $y=z-1/2$ e si sostituisce in $f_1$. Si ottiene $f_1'=x^2-z^2$ $+2z-5/4$, $f_3'=y\ -z+1/2$. Finalmente abbiamo la coppia $\{f_1',f_3'\}$ che è la *base di Gröbner ridotta* di $I$. Per ulteriori approfondimenti si veda ad esempio [KR00] Sez. 2.4.

(5) Il problema logico qui discusso è un problema giocattolo usato spesso nelle esposizioni a studenti di scuole secondarie. La sua traduzione in linguaggio polinomiale, che nel testo è illustrata in modo particolareggiato, mostra una delle molte facce applicative dell'algebra computazionale.

(6) Se si considera la curva nello spazio a tre dimensioni sul campo $K$ descritta parametricamente da $x = t^3, y = t^2, z = t$, si vede che la sua rappresentazione cartesiana è data ad esempio dal sistema delle due equazioni $x - yz = 0$, $y - z^2 = 0$. La proiezione della curva sul piano $xy$ si ottiene intersecando l'ideale $(x - yz,\ y - z^2)$ con l'anello $K[x, y]$. In questo caso si vede facilmente, senza bisogno di CoCoA, che la risposta è $(x^2 - y^3)$, la qual cosa significa che l'equazione cartesiana della curva proiettata sul piano $xy$ è $x^2 - y^3 = 0$. L'operazione di intersecare l'ideale $(x - yz,\ y - z^2)$ con l'anello $K[x, y]$ si può descrivere dicendo che si elimina l'indeterminata $z$ dall'ideale suddetto. Tale operazione è algoritmica (si fa calcolando una speciale base di Gröbner) e quindi fa rientrare la problematica dell'eliminazione nella computer algebra. Per ulteriori informazioni sul concetto di *eliminazione* si veda ad esempio [KR00] Sez. 3.4.

(7) Molti problemi di scacchi possono essere risolti con la computer algebra. L'esempio considerato delle otto regine non è un esempio giocattolo e il codice CoCoA che lo risolve non è facile da spiegare ai non addetti ai lavori. Infatti esso mette in gioco funzioni di Hilbert, dimensione, molteplicità, nozioni classiche ma non banali. Per approfondire questi argomenti, segnalo il Capitolo 5 di [KR05] e, per i meno esperti, la sua lunga introduzione.

(8) L'articolo di Phyllis Macchioni da cui è tratta la citazione si trova al sito `http://www.evalu8.org/staticpage?page=review&s iteid=3706`. La citazione completa è: *Genova is not a city that opens itself up to those passing through in a hurry, heading for other faraway places. It is a city that puts you under its spell, and then allows you to see its magic little by little.*

(9) In questo caso preferisco rimandare il lettore curioso al Tutorial 84 di [KR05], dove i quadrati magici vengono svelati a patto che egli lavori un po' per conto suo con CoCoA, e dove si osa suggerire la conclusione che ... Albrecht Dürer avrebbe anche potuto fare meglio.

(10) Il gin matematico di cui si parla è trattato ad esempio nel Tutorial 75 di [KR05]. La parte più interessante per il calcolo del gin è l'uso di algoritmi probabilistici, con probabilità di fallimento praticamente nulla.
(11) Si fa riferimento ad una recentissima collaborazione tra il nostro gruppo di ricerca e la SHELL sull'uso di modelli polinomiali, e quindi di CoCoA, per l'ottimizzazione dell'estrazione del petrolio.

## RIFERIMENTI BIBLIOGRAFICI

[A02] J. ABBOTT, *Sparse squares of polynomials*, Math. Comp. **71** (2002), 407-413.
[Abh76] S. ABHYANKAR, *Historical ramblings in algebraic geometry and related algebra*. Amer. Math. Monthly **83** (1976), 409-448.
[AL94] W. ADAMS - P. LOUSTAUNAU, *An introduction to Gröbner bases*, Graduate Studies in Math. **3**, Amer. Math. Soc., Providence, 1994.
[BW93] T. BECKER - V. WEISPFENNING, *Gröbner bases*, Springer, New York, 1993.
[CLS92] D. Cox - J. LITTLE - D. O'SHEA, *Ideals, varieties, and algorithms*, Springer, New York, 1992.
[CLS04] D. COX - J. LITTLE - D. O'SHEA, *Using algebraic geometry*, second ed., Springer, New York, 2004.
[Ch88] S.-C. CHOU, *Mechanical geometry theorem proving*, Math. and Its Appl. **41**, D. Reidel Publ. Comp., Dordrecht, 1988.
[DE05] A. DICKENSTEIN - I. EMIRIS (eds.), *Solving polynomial equations: foundations, algorithms and applications*, Springer, Berlin, 2005.
[GG03] J. VON ZUR GATHEN - J. GERHARD, *Modern computer algebra*, second ed., Cambridge Univ. Press, Cambridge, 2003.
[GKW03] J. GRABMEIER - E. KALTOFEN - V. WEISPFENNING (eds.), *Computer algebra handbook*, Springer, Heidelberg, 2003.
[GP02] G.-M. GREUEL - G. PFISTER, *A Singular introduction to commutative algebra*, Springer, Berlin, 2002.
[KR00] M. KREUZER - L. ROBBIANO, *Computational Commutative Algebra 1*, Springer, 2000.
[KR05] M. KREUZER - L. ROBBIANO, *Computational Commutative Algebra 2*, Springer, 2005, to appear.
[Ste04] H. STETTER, *Numerical polynomial algebra*, SIAM, Philadelphia, 2004.
[Stu96] B. STURMFELS, *Gröbner bases and convex polytopes*, University Lect. Ser. 8, Amer. Math. Soc., Providence, 1996.

[Stu02] B. STURMFELS, *Solving systems of polynomial equations*, CBMS Regional Conference Series in Math. **97**, Amer. Math. Soc., Providence, 2002.

[Wu94] W.T. WU, *Mechanical theorem proving in geometries*, Texts and Monographs in Symb. Comput., Springer, Berlin, 1994.

Lorenzo Robbiano: Dipartimento di Matematica,
Via Dodecaneso 35, 16146 Genova
e-mail: robbiano@dima.unige.it
http://www.dima.unige.it/robbiano
http://cocoa.dima.unige.it