Il gruppo delle trecce

di ESTER DALVIT

Nel numero 34 di XlaTangente*, alle pagine 26-29, abbiamo parlato di trecce, iniziando a formalizzarle come oggetti matematici. Finora non abbiamo però parlato della caratteristica più importante dell'insieme delle trecce: esso può essere dotato di una struttura matematica, quella di "gruppo", che ci permette non solo di "fare dei conti" con le trecce, ma anche di utilizzarle in maniera concreta, ad esempio in crittografia!*

Ripensiamo a come si costruisce una treccia: si prendono alcuni fili e si fissano a un'estremità (le ciocche di capelli sono già fissate in testa!). Si scelgono due fili e se ne fa passare uno davanti all'altro; poi se ne scelgono altri due (o gli stessi) e se ne fa passare di nuovo uno davanti all'altro, e così via. Se consideriamo ogni pezzo come una treccia a sé stante, l'operazione che stiamo compiendo consiste nel "fondere" tante trecce, tutte con lo stesso numero di fili, una dopo l'altra. In altre parole, incolliamo una treccia sotto l'altra, in modo da far combaciare le estremità dei fili. Diamo un nome a questa operazione, che si rivelerà fondamentale: la chiameremo composizione.
Più precisamente, possiamo definire la composizione come un'operazione binaria, cioè una "scatola nera" che prende come *input* due trecce T e S (con lo stesso numero di fili) e dà come *output* la treccia composta T*S, che indicheremo con TS, costruita intrecciando prima T e poi S.

Naturalmente, la composizione è associativa: se componiamo tre trecce T, S e R in quest'ordine, ognuno dei due modi

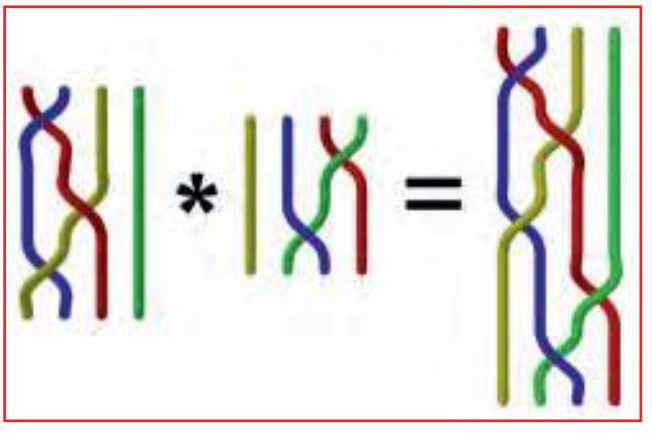

Figura 1. Composizione di due trecce

di eseguire l'operazione, (TS)R e T(SR), dà lo stesso risultato. In altre parole intrecciare T, quindi S e quindi R è come intrecciare T con la treccia ottenuta dalla composizione di S con R. Per questo non scriveremo più le parentesi tra le diverse trecce che vengono composte.
Pensandoci bene, abbiamo già usato questa proprietà nello scorso numero di *XlaTangente*: per descrivere una treccia, l'abbiamo decomposta in trecce elementari, che abbiamo chiamato σ_i e σ_i^{-1}. Una treccia veniva allora indicata con una "parola", cioè una sequenza di "lettere", o trecce elementari, ad esempio $\sigma_3\sigma_1^{-1}\sigma_2\sigma_3^{-1}$. In questo senso descriviamo la treccia come la composizione delle trecce elementari indicate nella sequenza, specificando l'ordine in cui si prendono le trecce, ma senza specificare quale composizione andasse fatta prima e quale dopo.
La treccia più semplice che possiamo pensare è quella in cui tutti i fili sono paralleli, cioè la treccia senza incroci, che possiamo indicare con il simbolo 1. Anche se sembra una treccia banale (e, infatti, a volte viene chiamata proprio «treccia banale»), essa gioca un ruolo fondamentale: è infatti l'elemento neutro per la composizione. Ciò significa che se componiamo qualsiasi treccia T con la treccia 1, a destra o a sinistra, il risultato è sempre T. In simboli possiamo scrivere T*1 = 1*T = T.

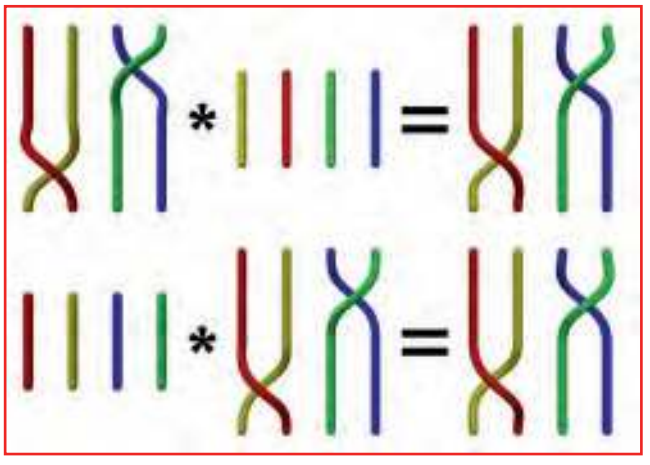

Figura 2. Elemento neutro

Ci possiamo ora chiedere: data una treccia T, esiste una treccia S che, intrecciata prima, o dopo T, faccia in modo che il risultato sia la treccia banale? In altre parole, data comunque una treccia T, esiste sempre la treccia inversa?
Se consideriamo una delle trecce elementari σ_i, trovare la sua inversa è facile: essa sarà σ_i^{-1}, come abbiamo già visto nello scorso numero.
Ma anche per trecce più complicate non è difficile trovare l'inversa: basta guardare la treccia T in uno specchio messo in modo perpendicolare rispetto alla "direzione" della treccia stessa! Infatti in questo modo otteniamo una treccia T' che è quella di partenza letta al contrario e con tutti gli incroci invertiti. Si possono allora considerare i due incroci centrali nella treccia composta TT' (o T'T): essi sono uno l'inverso dell'altro, e possono quindi essere cancellati. Ripetendo questa semplificazione per ogni coppia di incroci, alla fine otteniamo la treccia banale.
Facciamo un esempio: per ottenere l'inversa della treccia $\sigma_2\sigma_1^{-1}\sigma_3$ basta leggere le sue lettere da destra a sinistra, cambiandone gli esponenti. Avremo quindi la treccia $\sigma_3^{-1}\sigma_1\sigma_2^{-1}$.

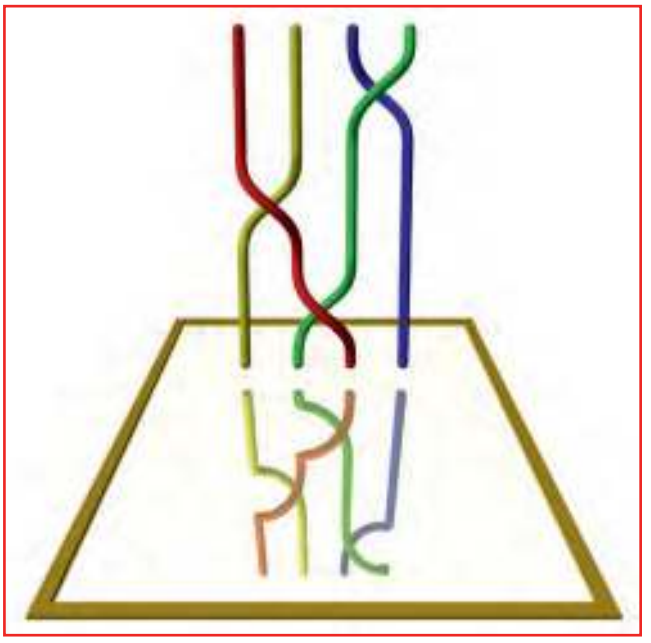

Figura 3. Inversa

Riassumendo, abbiamo scoperto che nell'insieme delle trecce con un numero fissato di fili possiamo definire un'operazione binaria associativa, che funge da composizione; che esiste un elemento neutro, la treccia banale, e che per ogni treccia esiste l'inversa. Un insieme con un'operazione con queste proprietà si chiama *gruppo*.
Quindi, per ogni intero positivo *n*, abbiamo trovato il gruppo delle trecce a *n* fili.

La struttura di gruppo è un concetto centrale in matematica: ad esempio, sono dei gruppi i numeri interi con l'operazione di somma, i reali senza lo 0 con l'operazione di moltiplicazione, ma anche le isometrie del piano o le permutazioni di *n* elementi con l'operazione di composizione.

Uno degli aspetti interessanti dei gruppi delle trecce è la non commutatività. Quando componiamo due trecce T e S dobbiamo fare attenzione al loro ordine: non sempre TS = ST, anzi, questo succede molto raramente!
Facciamo un esempio: componiamo σ_1 e σ_2, nei due modi possibili (come nella figura 4): $\sigma_1\sigma_2$ non è uguale a $\sigma_2\sigma_1$.

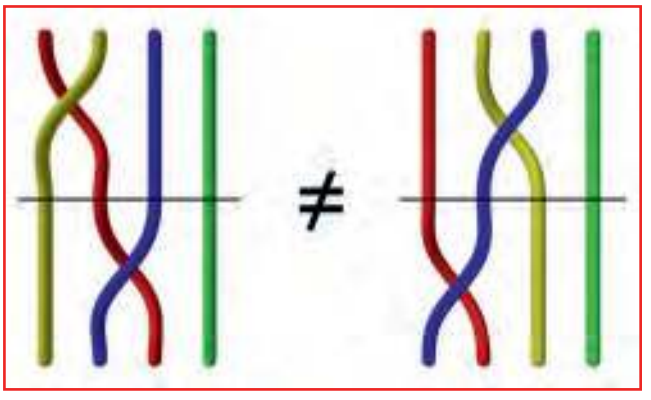

Figura 4. Non commutatività: σ_1 e σ_2

TRECCE E NODI

Nello scorso numero abbiamo descritto un modo per ottenere altri oggetti matematici, i nodi, a partire dalle trecce: la chiusura. Chiudere una treccia significa collegare il capo superiore di ogni filo con il capo inferiore del filo nella posizione corrispondente, usando delle nuove cordicelle che non si intrecciano.
Una prima domanda che ci possiamo porre è: dato un nodo qualsiasi, possiamo ottenerlo come chiusura di una treccia? E se sì, di quale, o quali, trecce?
Alla prima domanda ha risposto per primo il matematico americano Alexander (1888-1971), negli anni '20 del secolo scorso, proponendo un algoritmo che permette di mettere un nodo qualsiasi nella forma di una treccia chiusa. Il procedimento è basato sull'idea di fare del nodo una specie di matassa, che si avvolga attorno a un asse, girando sempre nello stesso verso. Infatti, se guardiamo il disegno di una treccia chiusa, ci accorgiamo che ogni filo della treccia continua nella chiusura, girando in senso antiorario attorno a un asse, immaginato perpendicolare al piano del disegno, fino a tornare all'inizio di un filo (quello di partenza o un altro).

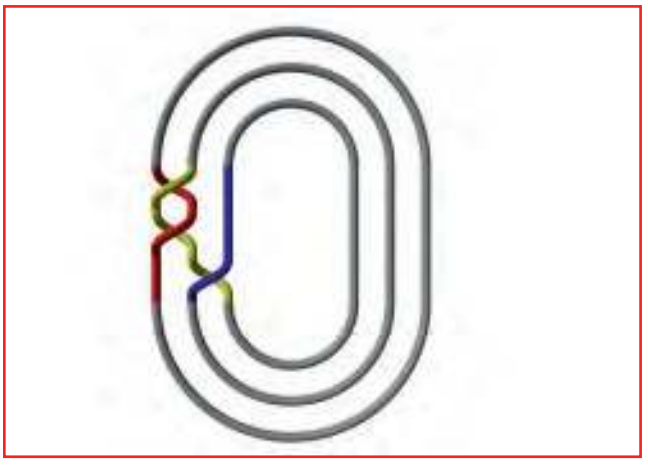

Figura 5. Una treccia chiusa con 3 fili e 2 componenti

Alexander è riuscito a dimostrare che tutti i nodi possono essere messi in una forma di questo tipo. Senza entrare nei dettagli, i passaggi fondamentali sono questi: scegliere un asse (rappresentato con un punto in figura 6bis), scegliere un punto di partenza sul nodo, cominciare a percorrere il nodo girando in senso antiorario attorno all'asse e colorare tutte le parti del nodo in cui, viceversa, ci si trova a dover girare in senso orario (vedi figura 6bis); e, infine, muovere le parti colorate in rosso una alla volta "dall'altra parte" dell'asse. Ad esempio possiamo deformare il nodo della figura 6a nella forma della figura 6b, seguendo le «istantanee» c, d, e, f in figura 6bis.
Per avere un'idea più chiara delle operazioni da compiere, si può guardare il filmato:
http://www.youtube.com/watch?v=h5IErq3m1ns

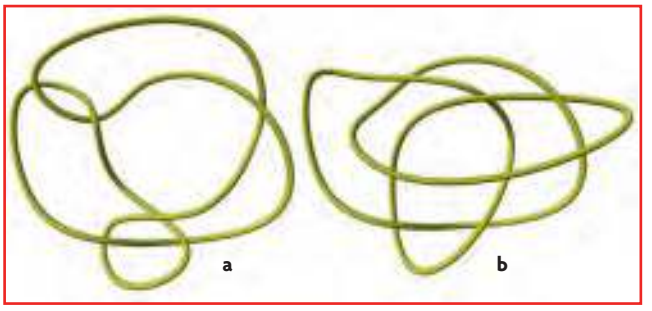

Figura 6. a) nodo b) matassa

Ora il nodo "gira" sempre nello stesso verso attorno all'asse. In altre parole, qualsiasi semipiano che abbia l'asse come bordo, interseca il nodo sempre nello stesso numero di punti, tre nell'esempio che stiamo considerando (vedi figura 7).

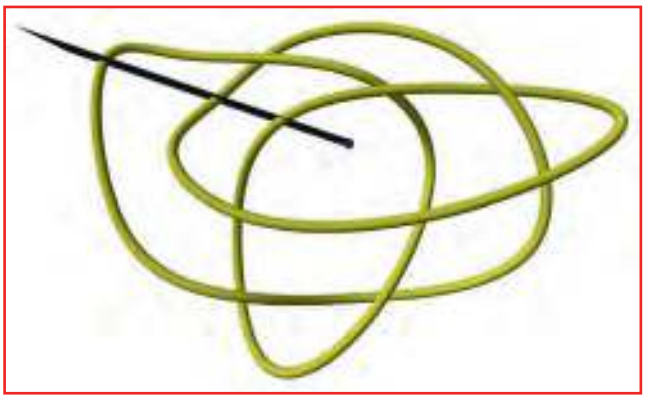

Figura 7. Semipiano che taglia nodo

A questo punto basta scegliere uno dei semipiani e tagliare il nodo lungo esso. Nel nostro esempio otteniamo tre cordicelle. Possiamo quindi allontanare gli estremi delle cordicelle, mantenendoli su due piani che spostiamo sino a farli diventare paralleli. Durante questo procedimento, le cordicelle non si devono mai intersecare (figura 8).

Otteniamo così una treccia. Se volessimo richiuderla, otterremmo lo stesso nodo da cui siamo partiti: infatti, i nuovi fili aggiunti con la chiusura non si intersecano, e possiamo immaginare di procedere a ritroso nella successione appena descritta, accorciando i fili aggiunti fino a farli sparire.

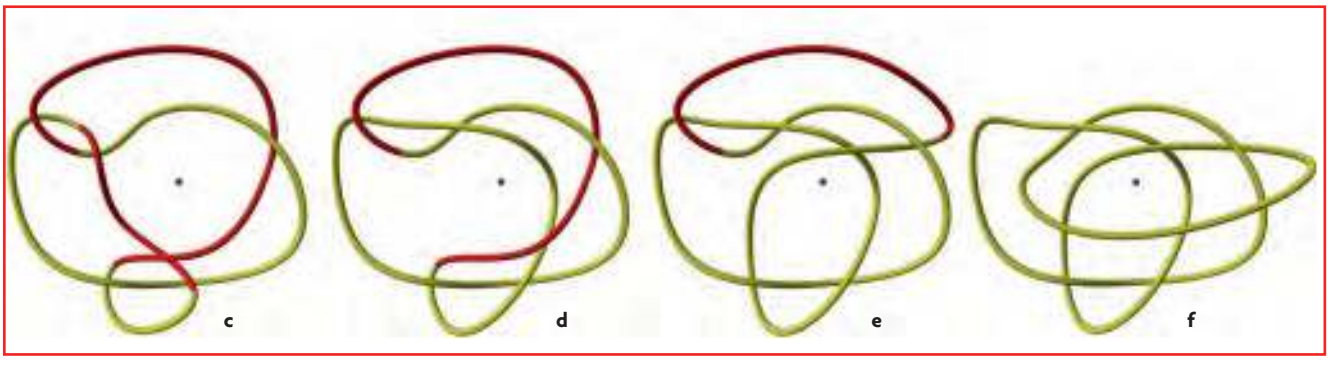

Figura 6bis. c) d) e) f) deformazioni «continue» del nodo

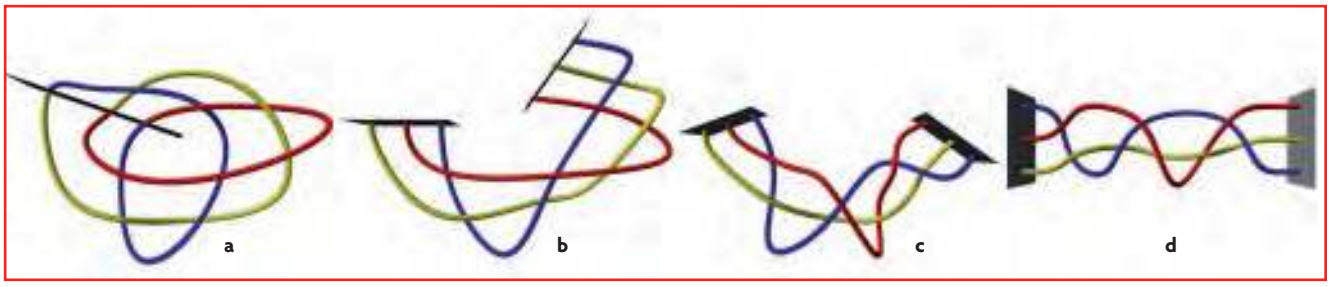

Figura 8. a) b) c) d) aprire la matassa

L'algoritmo descritto può però dare trecce diverse, a seconda dell'asse scelto, delle mosse utilizzate per trasformare il nodo iniziale in una matassa e del semipiano lungo il quale tagliamo il nodo. Quindi ci sono trecce diverse che, tramite la chiusura, danno lo stesso nodo.
Come possiamo capire quando questo accade? Quali trecce danno origine allo stesso nodo?
Per affrontare il problema possiamo fissare una treccia e cercare di capire quali mosse la cambiano senza modificarne la chiusura.

Ad esempio, chiudendo la treccia con due fili σ_1^3 otteniamo un nodo trifoglio. Ma anche chiudendo la treccia con tre fili $\sigma_1^3\sigma_2$ otteniamo lo stesso nodo: infatti, una volta chiusa la seconda treccia, c'è un ricciolo all'interno che può venir tolto, e si ottiene la chiusura della prima treccia. Con lo stesso procedimento, ma girando il ricciolo nell'altro senso, si può vedere che anche $\sigma_1^3\sigma_2^{-1}$ dà sempre un nodo trifoglio.
In generale, se partiamo da una qualsiasi treccia a n fili e aggiungiamo un nuovo filo a destra e un solo incrocio tra esso e il filo immediatamente alla sua sinistra, otteniamo una nuova treccia, che, una volta chiusa, dà lo stesso nodo della treccia di partenza.
Più brevemente, possiamo scrivere: data una treccia T a n fili (e che coinvolge quindi solo gli scambi σ_1, ..., σ_{n-1}), la chiusura di T dà lo stesso nodo della chiusura di $T\sigma_n$ e di $T\sigma_n^{-1}$, che sono trecce con n+1 fili.
Questa mossa sulle trecce è chiamata *stabilizzazione* ed è uno dei due modi fondamentali per trasformare una treccia senza cambiare il nodo ottenuto dalla sua chiusura.

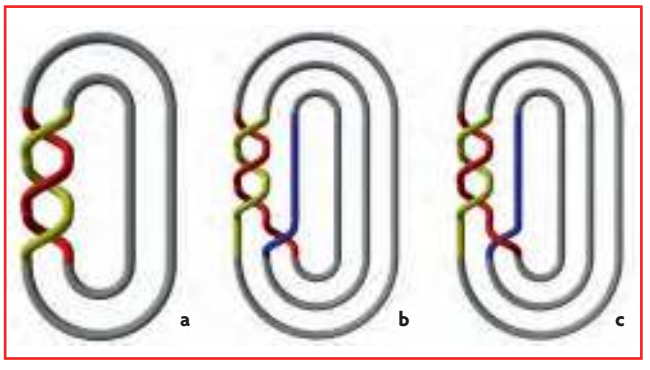

Figura 9. a) b) c) stabilizzazione: trifogli σ_1^3, $\sigma_1^3\sigma_2$ e $\sigma_1^3\sigma_2^{-1}$

L'altro modo è chiamato *coniugio*: questa mossa consiste nel comporre la treccia di partenza, T, con una treccia S da una parte e la treccia inversa S^{-1} dall'altra, ottenendo quindi la treccia $S^{-1}TS$. Questa è detta una treccia coniugata di T.
Se chiudiamo la treccia $S^{-1}TS$, possiamo far scivolare la (sotto)treccia S lungo i fili della chiusura, fino a portarla a contatto con S^{-1}. A questo punto possiamo semplificare S con S^{-1}, dato che sono adiacenti e sono una l'inversa dell'altra. Dunque la chiusura di $S^{-1}TS$ darà lo stesso nodo ottenuto chiudendo T.

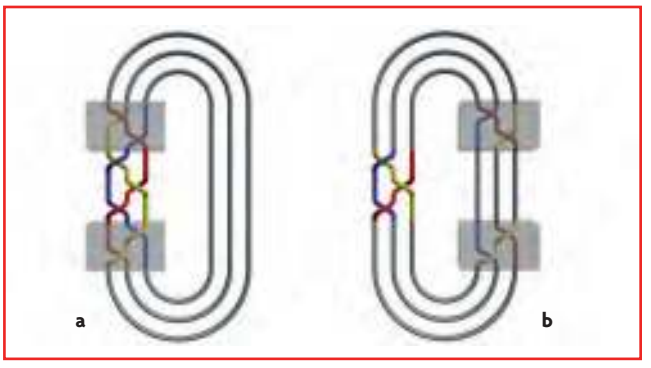

Figura 10. a) coniugio b) semplificazione

Si può dimostrare che, usando solo queste due mosse (e le relazioni nei gruppi delle trecce, descritte nel box a p. 31) è possibile ottenere, a partire da una data treccia, tutte le trecce che danno lo stesso nodo tramite la chiusura.
Questo risultato è noto come teorema di Markov, ma non è chiaro se sia stato il matematico russo o un suo studente a dimostrarlo per primo, a metà del secolo scorso.
Noi abbiamo descritto la parte facile: abbiamo notato che queste due mosse non cambiano il nodo che è chiusura della treccia. La parte difficile è l'altra, cioè dimostrare che le due mosse sono sufficienti per passare da una treccia a tutte quelle che, una volta chiuse, danno lo stesso nodo.

Trecce, nodi e... crittografia

Nel teorema di Markov una delle mosse fondamentali è il coniugio. Ma come si fa a capire se due trecce sono coniugate oppure no? Il problema è abbastanza complesso, ed è stato risolto da Garside, in un articolo pubblicato nel 1969.
Una variante, chiamata "problema della ricerca dei coniugati", consiste non solo nel capire se due trecce T e T' sono coniugate, ma anche – se lo sono – nel trovare una treccia S "coniugante", cioè tale che $S^{-1}TS = T'$.
Naturalmente il problema opposto è molto facile e consiste solo in un calcolo: date T ed S, è immediato trovare T'.
Problemi e funzioni di questo tipo sono chiamati *one-way* o unidirezionali: affrontandoli da un lato è facile calcolare il risultato, ma se si inverte il problema (o si vuole calcolare la funzione inversa), la ricerca del risultato diventa molto complicata. Le funzioni *one-way* sono molto ricercate dalla crittografia, che le sfrutta per cifrare messaggi e dati che devono rimanere riservati. Infatti, per cifrare un messaggio basta andare nella direzione "semplice" del problema, mentre un eventuale ascoltatore che intercettasse il messaggio

e volesse decifrarlo, dovrebbe affrontare il problema nella direzione opposta, quella che lo rende difficile.
Negli ultimi anni sono stati proposti alcuni schemi crittografici, cioè procedimenti da seguire per cifrare e decifrare messaggi, basati sui gruppi delle trecce: il messaggio da cifrare viene interpretato come una treccia e si sfrutta la complessità del problema del coniugio per renderlo non interpretabile da persone diverse dal destinatario. Ne abbiamo parlato anche nel numero 32 di *XlaTangente* alle pp. 23-28.
In realtà questi schemi non sono (ancora) usati in pratica, perché non sono ritenuti abbastanza sicuri. I ricercatori stanno sviluppando metodi sempre più efficaci e veloci per risolvere la direzione "difficile" del problema, il che renderebbe il problema non più *one-way* e farebbe crollare la sicurezza degli schemi basati su di esso. Gli studi a venire ci diranno se un giorno potremo usare la crittografia basata sulle trecce per le nostre carte di credito o se dovremo trovare nuovi gruppi e nuovi problemi da poter sfruttare in questo ambito.

Ester Dalvit
Laureata in Matematica presso l'Università degli Studi di Trento e quella di Tuebingen in Germania, con un progetto di doppia laurea. Nel 2011, ha conseguito il titolo di dottore di ricerca Matematica con indirizzo in Comunicazione e Didattica, e attualmente lavora presso il Laboratorio di Didattica e Comunicazione della Matematica dell'Università degli Studi di Trento.
dalvit@science.unitn.it

Una descrizione del gruppo delle trecce

Non è facile capire "come sono fatti" i gruppi delle trecce: possiamo sicuramente scrivere tutti i loro elementi usando le parole che si possono formare con le lettere σ_i e σ_i^{-1}, ma parole diverse possono indicare lo stesso elemento del gruppo. Ad esempio, la treccia banale 1 si può scrivere anche come $\sigma_1\ \sigma_1^{-1}$, o con espressioni più complicate, come $\sigma_1\sigma_2\sigma_1\sigma_1^{-1}\sigma_2^{-1}\sigma_1^{-1}$, o con un'infinità di altre parole diverse.

Ci sono sostanzialmente tre modi per trovare nuove parole che designano la stessa treccia, assegnata anch'essa attraverso una parola: il più semplice consiste nell'aggiungere (o togliere) due lettere adiacenti del tipo $\sigma_i\ \sigma_i^{-1}$ oppure $\sigma_i^{-1}\sigma_i$. Ad esempio la treccia $\sigma_1\sigma_3$ sarà la stessa di $\sigma_1\sigma_2^{-1}\sigma_2\sigma_3$ oppure di $\sigma_1\sigma_3\sigma_2\sigma_2^{-1}$, e così via. Queste "mosse" sulle parole vengono chiamate *riduzioni libere*, e si possono fare in ogni gruppo, perché ogni elemento ha il suo inverso (Figura 11).

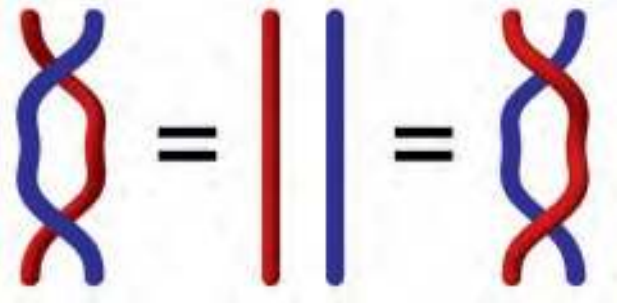

Figura 11. Riduzione libera

Un secondo modo consiste nello scambiare due lettere vicine, se i loro indici non sono due numeri consecutivi. Ad esempio, la parola $\sigma_1\sigma_3$ può essere cambiata in $\sigma_3\sigma_1$ senza cambiare la treccia rappresentata. Invece, $\sigma_1\sigma_2$ non indica la stessa treccia di $\sigma_2\sigma_1$, perché gli indici sono consecutivi (vedi figura 4).
Questa mossa corrisponde a un movimento nella treccia: fa scivolare due incroci vicini, che interessano diverse coppie di fili, uno dall'alto verso il basso e l'altro dal basso verso l'alto, fino a scambiarli di posto (Figura 12).

Anche l'ultimo modo si vede più facilmente come movimento dei fili nella treccia: in una situazione come quella nella figura 13, possiamo far scivolare il filo giallo tra

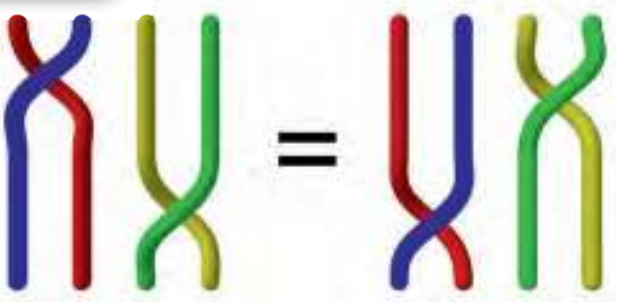

Figura 12. Relazione 1

l'incrocio formato dai fili rosso e blu. In simboli, otteniamo che la treccia descritta da $\sigma_1\sigma_2\sigma_1$ è indicata anche dalla parola $\sigma_2\sigma_1\sigma_2$. In generale questa mossa si scrive come $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$. Ciò significa che la parola a destra può essere sostituita da quella a sinistra (e viceversa), ogni volta che la troviamo come parte di una treccia. Ad esempio $\sigma_3\sigma_2\sigma_3\sigma_1$, può essere trasformata in $\sigma_2\sigma_3\sigma_2\sigma_1$.

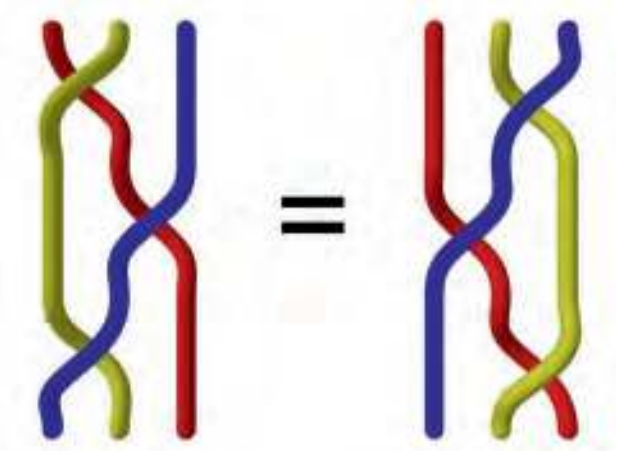

Figura 13. Relazione treccia

Si può dimostrare che queste tre mosse sono sufficienti per ottenere tutte le parole equivalenti a una parola data (cioè quelle che descrivono la stessa treccia). Questo risultato è dovuto a Emil Artin (1898-1962), il primo matematico che, circa novant'anni fa, formalizzò le trecce.