Automi cellulari e crittografia

Daniele & Luca Volonterio

Breve storia degli automi cellulari

Concetto proposto da Von Neumann negli anni '40: modello formale di organismi viventi in grado di riprodursi

Composto da:

- Un reticolo di celle
- Un insieme finito di stati che può assumere una cella
- Per ogni cella, un intorno di celle con cui interagisce
- Una regola che descrive lo stato di una cella al tempo t+1, in funzione dello stato al tempo t della cella e del suo intorno

Necessità di costruire sistemi Turing-completi per eliminare casi banali

(immagine di CA 1d banale, una cella che si riproduce a sinistra e a destra)

Automi cellulari elementari (ECA)

" rule 18 " rule 86

- Reticolo 1d
- Stati binari
- Intorno: cellule immediatamente adiacenti
- 3 input binari -> 1 output binario: 256 regole
- Si riducono a 88 ammettendo riflessioni sinistra-destra e inversioni 0-1

Turing-completezza: Rule 110

- Classe 1: l'evoluzione conduce ad uno stato omogeneo
  - Esempio: Rule 160
- Classe 2: l'evoluzione conduce ad un insieme di strutture semplici stabili o periodiche separate tra di loro
  - Esempio: Rule 32
- Classe 3: l'evoluzione conduce ad un pattern caotico
  - Esempio: Rule 30
- Classe 4: l'evoluzione conduce a strutture complesse localizzate nello spazio, a volte longeve. Si ritiene che questa classe di automi sia capace di computazione universale