FUNZIONI DI HASH

U universo

$$h: U \to m$$

"funzione di hash per U con m bucket"

1) h si calcoli in tempo costante
2) h sia "molto iniettiva"

$X \subseteq U \qquad |X| = m$

$U = \Sigma^{\leq 100} \qquad X \subseteq U \qquad |X| = 20$

$\forall x, y \in X \quad x \neq y$

$h(x) \neq h(y)$

D

$h: U \to m$ unif. a caso

Full randomness

$\Sigma = \{a, b, \ldots, z, A, B, \ldots, Z\}$ $|\Sigma| = 52$

$U = \Sigma^{\le 100}$

$U = \{$ Boldi, Russo, Gianfilippi, ..., Zpaklv, ZZZZA... $\}$

$$\boxed{h : U \to 100}$$

$x = x_1 \ldots x_n \in U$

w: | w_1 | w_2 | . . . . | w_{100} | $\in \{0, 1, \ldots, 99\}$

x: | x_1 | x_2 | . . . | x_n |

$$h(x) \triangleq \left(\sum_{i=1}^{n} x_i \, w_i \right) \bmod 100$$

$$\mathcal{H}_{U,m} \subseteq m^U$$

$$\forall x \in U \quad \Pr_h[h(x) = t] = \frac{1}{m} \qquad \forall t \in m$$

FUNZIONE DI HASH PERFETTA

- $h : U \to m$
  perfetta per $X \subseteq U$ sse è iniettiva su X
  (è necessario che $m \geq |X|$)
- MINIMALE se $m = |X|$

TECNICA MWHC
(Majewski, Wormald, Havaś & Czech)

RAPPRESENTAZIONE DI FUNZIONI STATICHE A r BIT

U Universo

$X \subseteq U$

$|X| = n$

$x_i \in X$

f	$\overbrace{\qquad\qquad}^{r \text{ bit}}$
x_1	0 0 1 0 1 1
x_2	0 1 0 0 1 1
$\vdots$	
x_n	1 0 1 1 0 1

1) Fissiamo un $m \geq n$

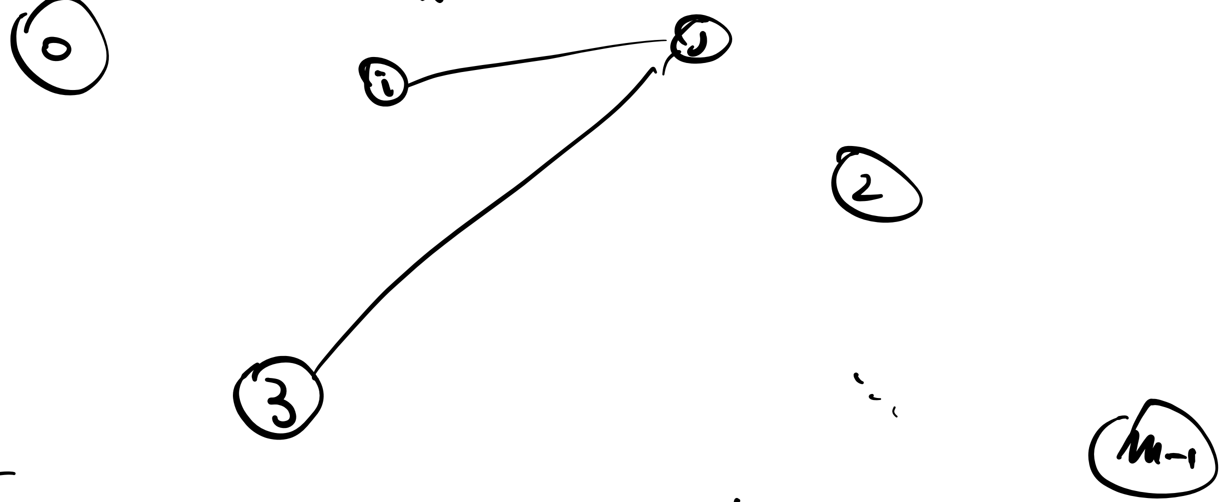
2) Scegliamo unif. a caso $h_1, h_2 : U \to m$

3) Costruiamo un grafo

$x \quad \{h_1(x), h_2(x)\} = \{i, j\}$ 1 4

$x \in X$

G m nodi e n lati



situazioni spiacevoli

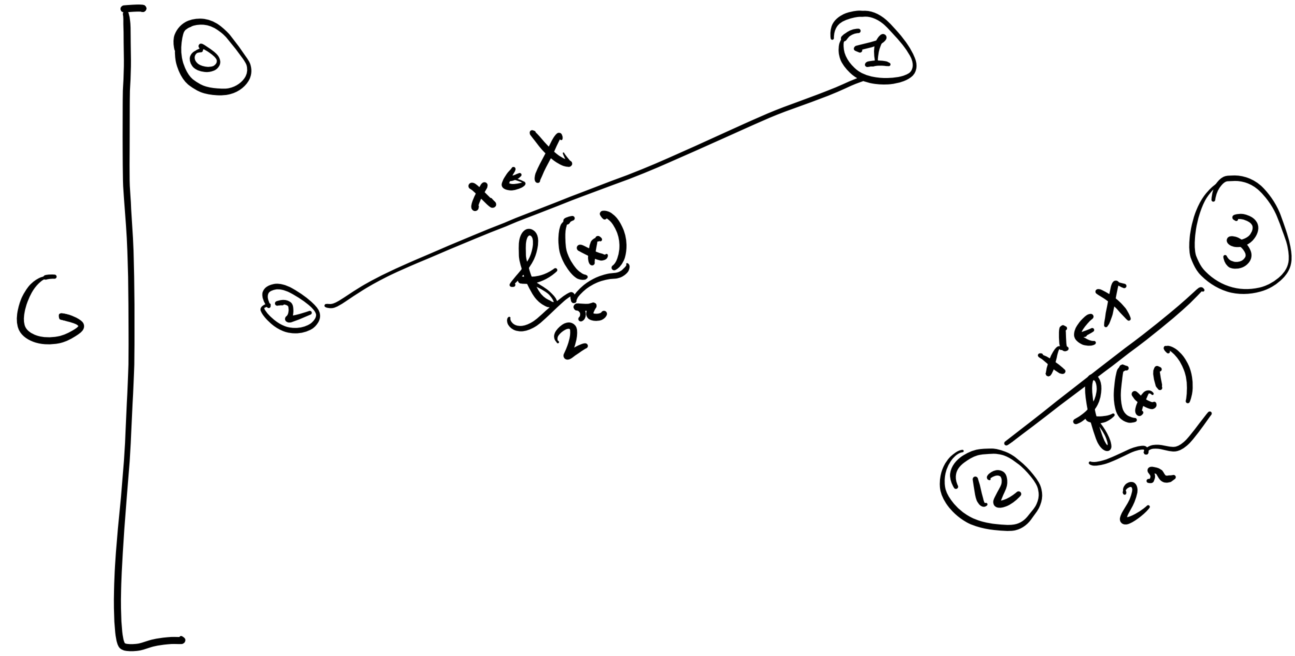
butto via h_1, h_2 e li scelgo di nuovo

1) $h_1(x) = h_2(x)$ per qualche x

2) $x, y \in X$ $\quad x \neq y$ $\quad \{h_1(x), h_2(x)\} = \{h_1(y), h_2(y)\}$

3) G ciclico

Thm: Se $m > 2.09\,n$, le funzioni h_1, h_2 hanno q.s. le proprietà desiderate (e il numero di tentativi attesi è ≈ 2)



⇓ sistema di equazioni

$A[0], A[1] \ldots, A[m-1] \in 2^r$

$\forall x \in X \quad (A[h_1(x)] + A[h_2(x)]) \bmod 2^r = f(x)$

⇒ Sistema ammette soluzioni

→ $A[0], \ldots, A[m-1]$ viene memorizzata — mr bit $= 2.09\, nr$ bit

h_1, h_2, m ← $O(1)$

$$f(\text{"Boldi"}) = (A[h_1(\text{"Boldi"})] + A[h_2(\text{"Boldi"})]) \bmod 2^r$$

ESEMPIO

$r = 3$

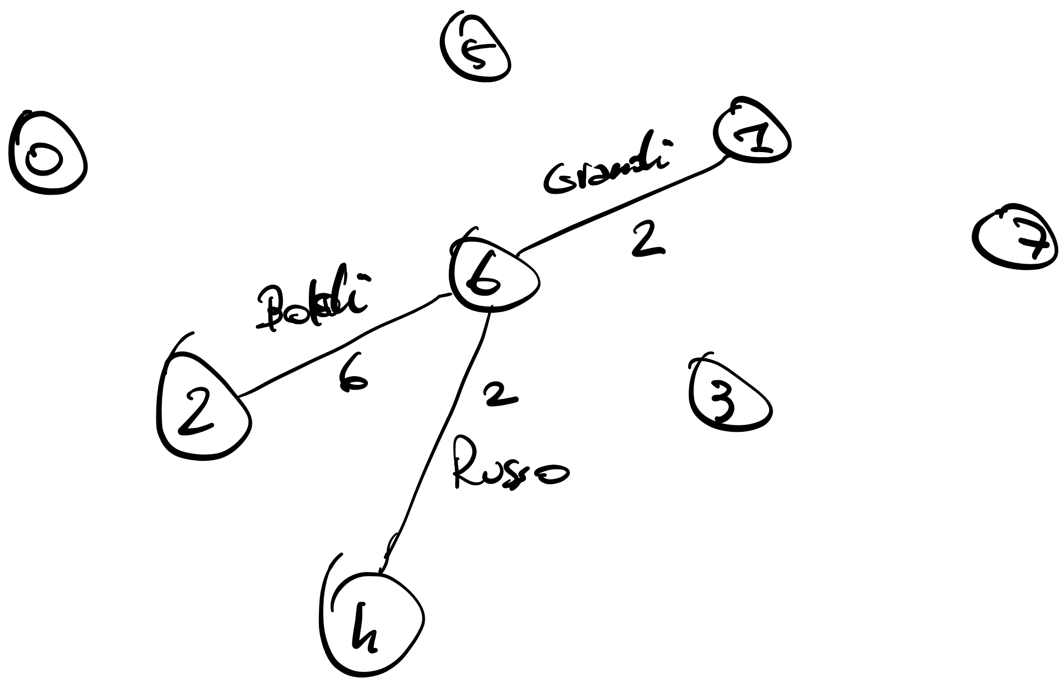
$2^r = 8$

$n = 3$

Boldi	6
Russo	2
Grandi	2

$m = 7$

$m > 2.09\, n$



x	$h_1(x)$	$h_2(x)$
Boldi	2	6
Russo	6	4
Grandi	6	1

$$\begin{cases} (A_2 + A_6) \bmod 8 = 6 \\ (A_1 + A_6) \bmod 8 = 2 \\ (A_4 + A_6) \bmod 8 = 2 \end{cases}$$

$A_2 = 6$ $\quad A_6 = 0$

$A_1 = 2$

$A_4 = 2$

A

0	1	2	3	4	5	6
0	2	6	0	2	0	0

$f(\text{"Russo"}) = 2$

CON UN 3-IPERGRAFO

Thm vale per $m > \boxed{\frac{1.23}{\gamma}} n$

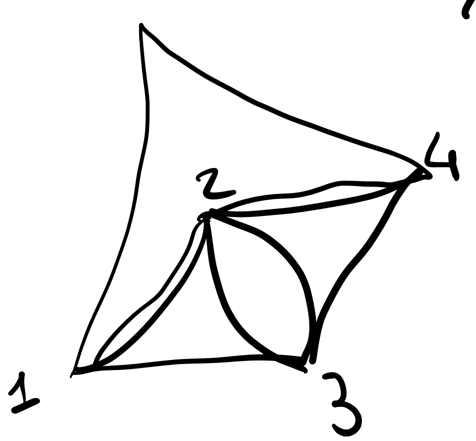
ACICLICITÀ $\longleftrightarrow$ PEELABILITY

Un ipergrafo (V, E) ammette una peeling sequence sse esiste un modo per ordinare gli iperarchi $e_1, \dots, e_n \in E$ e una sequenza di vertici $x_1, \dots, x_n \in E$ t.c.

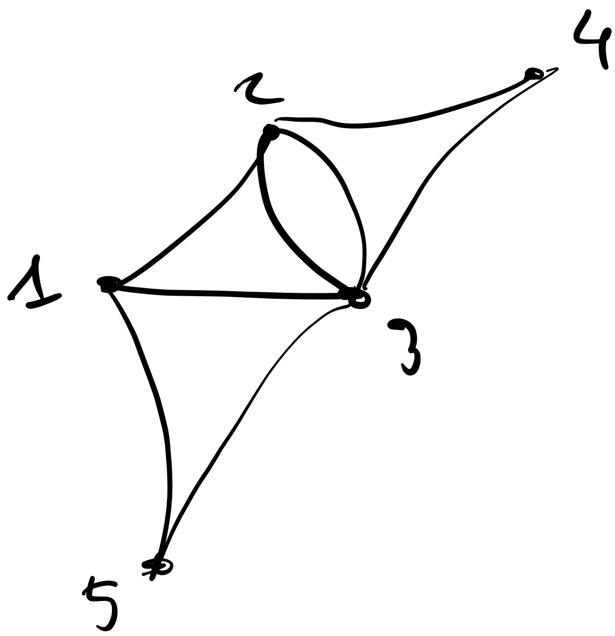
$$\left.\begin{array}{ll} x_1, & e_1 \\ x_2, & e_2 \\ \vdots & \\ x_n, & e_m \end{array}\right]$$

1) $x_i \in e_i$ (hinge)

2) $x_i \notin e_j$ $\forall j < i$



1	1, 2, 3
4	2, 3, 4
	1, 2, 4



1	1, 2, 3
4	2, 3, 4
5	1, 3, 5

$A_1 + A_2 + A_3 = \sim$

$A_2 + A_3 + A_4 = \sim$

$A_1 + A_3 + A_5 = \sim$

$\boxed{\text{SPAZIO OCCUPATO}}$

$\gamma n \overline{r}$ BIT

$nr + \gamma n + o(n)$ BIT

$nr + \gamma n < \gamma n r$

$(\gamma - 1)\cancel{n} r > \gamma \cancel{n}$ $\quad \gamma = 1.23$

$r > \frac{\gamma}{\gamma - 1}$

$r > 5$