

En primer lloc, em trec de sobre els casos patològics. De normal, tenir dues variables  $X_k$  amb la mateixa  $k$  és nefast, ja que si  $X_k^{(1)} = C$ , aleshores  $X_k^{(2)} = C$  amb probabilitat 1 i no coincideix amb  $P(X_k = C)$ . Tot i així, si per casualitat la variable  $X_k$  és constant, llavors és automàticament independent amb tot. Aquesta mala fortuna passa només per a  $n=1$  i/o  $n=0$ , i llavors dona infinit. Dit això, assumirem a partir d'agui que  $n > 0$  i  $n > 1$ . Demostrarem ara que per a tot  $k, C_i \in \mathbb{Z}/n\mathbb{Z}$  es té

$$P(X_{k_i} = C_i) = \frac{1}{n}$$

Això és perquè podem organitzar els polinomis en sacs de posant-los al mateix sac si difereixen només en el terme independent. Dins de cada sac hi ha un únic polinomi  $p$  amb  $p(k_i) = C_i$ , així que la probabilitat és  $\frac{1}{n}$ . Per altra banda, no podem tenir  $X_{k_i} = X_{k_j}$  si  $k_i \equiv k_j \pmod{p}$ , en p és el menor primer que divideix  $n$ , ja que per a tot polinomi  $q$  es tindria  $q(k_i) \equiv q(k_j) \pmod{p}$  i  $P(X_{k_i} = 0, X_{k_j} = 1)$  seria 0 en lloc de  $\frac{1}{n^2}$ . Una altra fita superior per al nombre de variables independents és  $n$ .

Si tenim  $r$  variables independents,

veiem que  $P\left(\sum_{i=1}^r X_i = 0\right) =$

$= \frac{1}{n^r}$ . No obstant, podem fitar-ho inferiorment per  $\frac{1}{n^r}$ , que és la probabilitat d'escollir el polinomi 0, així que  $\frac{1}{n^r} \geq \frac{1}{n^m}$  i  $r \leq m$ .

Per últim, cal veure que podem escollir  $r$  variables independents sempre que  $r \leq \min\{m, p : p \mid n\}$ . Escull les variables  $X_0, X_1, \dots, X_{r-1}$

i separa els polinomis en sacs de mida  $n^r$ , on dos polinomis són al mateix sac

si només difereixen en els  $r$  termes de grau més baix. Dos polinomis  $f = \sum f_i X^i$

i  $g = \sum g_i X^i$  al mateix sac ho poden donar el mateix per a  $X = 0, 1, \dots, n^r - 1$  a que si fos

així, tindrien  $\sum_{i=0}^{r-1} f_i K^i = \sum_{i=0}^{r-1} g_i K^i$  que implica  $f_i = g_i$  perquè la matriu de



Vandermonde

$\forall K = 0, 1, \dots, n^r - 1$

és invertible (l'ús és fàcil, veu més avall el primer més petit de  $n$ ).

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & 1 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & r-2 & (r-2)^2 & (r-2)^3 & \dots & (r-2)^{r-1} \\ 1 & r-1 & (r-1)^2 & (r-1)^3 & \dots & (r-1)^{r-1} \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{r-2} \\ f_{r-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 1 & 1 & 1 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & r-2 & (r-2)^2 & (r-2)^3 & \dots & (r-2)^{r-1} \\ 1 & r-1 & (r-1)^2 & (r-1)^3 & \dots & (r-1)^{r-1} \end{pmatrix} \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{r-2} \\ g_{r-1} \end{pmatrix} \Rightarrow f_i = g_i \quad \forall i$$

ja que  $\det \begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \end{pmatrix} = \prod (i-j) = \text{coprimer amb } n \Rightarrow \text{invertible}$

Així, la resposta és:

$$\begin{cases} \infty & \text{si } n=1 \text{ o } m=0 \\ \min \{m, p: p|n\} & \text{altrement} \end{cases}$$

(820) Two Men OT & Heceta