

These notes are from <http://math.cmu.edu/~coco/teaching/discrete20/pairwise.pdf>

Let (Ω, \mathbf{Pr}) be a finite probability space and let $A_1, \dots, A_n \subseteq \Omega$ be nontrivial events. We saw in Recitation 9 that if A_1, \dots, A_n are mutually independent, then $|\Omega| \geq 2^n$. But what if A_1, \dots, A_n are only pairwise independent?

Claim 1. *If $A_1, \dots, A_n \subseteq \Omega$ are pairwise independent and nontrivial, then $|\Omega| \geq n + 1$.*

(Warning: the following proof requires linear algebra know-how)

Proof. Without loss of generality, we may suppose that $\mathbf{Pr}[\omega] \neq 0$ for all $\omega \in \Omega$. We can thus define an inner product on \mathbb{R}^Ω by

$$\langle x, y \rangle = \sum_{\omega \in \Omega} \mathbf{Pr}[\omega] \cdot x(\omega) \cdot y(\omega),$$

for any $x, y \in \mathbb{R}^\Omega$. For $i \in [n]$, define $x_i \in \mathbb{R}^\Omega$ by

$$x_i(\omega) = \mathbf{1}[\omega \in A_i] - \mathbf{Pr}[A_i].$$

Also define $x_0 \in \mathbb{R}^\Omega$ by $x_0(\omega) = 1$. Certainly $x_0 \neq 0$, and for any $i \in [n]$, $x_i \neq 0$ since A_i is nontrivial.

Now, for any $i \in [n]$, we see that

$$\begin{aligned} \langle x_0, x_i \rangle &= \sum_{\omega \in \Omega} \mathbf{Pr}[\omega] (\mathbf{1}[\omega \in A_i] - \mathbf{Pr}[A_i]) \\ &= \sum_{\omega \in A_i} \mathbf{Pr}[\omega] - \mathbf{Pr}[A_i] \sum_{\omega \in \Omega} \mathbf{Pr}[\omega] = 0. \end{aligned}$$

For any $i \neq j \in [n]$, we can compute

$$\begin{aligned} \langle x_i, x_j \rangle &= \sum_{\omega \in \Omega} \mathbf{Pr}[\omega] (\mathbf{1}[\omega \in A_i] - \mathbf{Pr}[A_i]) (\mathbf{1}[\omega \in A_j] - \mathbf{Pr}[A_j]) \\ &= \sum_{\omega \in A_i \cap A_j} \mathbf{Pr}[\omega] - \mathbf{Pr}[A_i] \sum_{\omega \in A_j} \mathbf{Pr}[\omega] - \mathbf{Pr}[A_j] \sum_{\omega \in A_i} \mathbf{Pr}[\omega] + \mathbf{Pr}[A_i] \mathbf{Pr}[A_j] \sum_{\omega \in \Omega} \mathbf{Pr}[\omega] \\ &= \mathbf{Pr}[A_i \cap A_j] - 2 \mathbf{Pr}[A_i] \mathbf{Pr}[A_j] + \mathbf{Pr}[A_i] \mathbf{Pr}[A_j] = 0, \end{aligned}$$

since A_i and A_j are independent.

Putting this together, we have shown that $x_0, \dots, x_n \in \mathbb{R}^\Omega$ are non-zero vectors which are pairwise orthogonal; thus, $|\Omega| \geq n + 1$. □

The bound in Claim 1 is tight (for infinitely many values of n). Here is one example:

Consider flipping a fair coin k times: so $\Omega = \{0, 1\}^k$ and \mathbf{Pr} is the uniform distribution. For $S \subseteq [k]$,

$$A_S = \left\{ \omega \in \Omega : \sum_{i \in S} \omega_i \equiv 0 \pmod{2} \right\}.$$

We claim that $\mathcal{A} = \{A_S : S \subseteq [k] \wedge S \neq \emptyset\}$ is pairwise independent. Indeed, we first notice that for any $S \neq \emptyset$, $\Pr[A_S] = 1/2$. We next observe that for any nonempty $S \neq T$,

$$\begin{aligned} A_S \cap A_T &= \left\{ \omega \in \Omega : \sum_{i \in S} \omega_i \equiv \sum_{i \in T} \omega_i \equiv 0 \pmod{2} \right\} \\ &= \left\{ \omega \in \Omega : \sum_{i \in S \setminus T} \omega_i \equiv \sum_{i \in T \setminus S} \omega_i \equiv \sum_{i \in S \cap T} \omega_i \pmod{2} \right\}. \end{aligned}$$

Since $S \neq T$ are nonempty, at most one of the sets $S \setminus T$, $T \setminus S$, $S \cap T$ can be empty. If all three are nonempty, then by above we see that $\Pr[A_S \cap A_T] = 2 \cdot \frac{1}{8} = \frac{1}{4} = \Pr[A_S] \Pr[A_T]$. If only two are nonempty, say $S \setminus T$ and $S \cap T$ for instance, then $\Pr[A_S \cap A_T] = \Pr[A_{S \setminus T}] \Pr[A_{S \cap T}] = \frac{1}{4} = \Pr[A_S] \Pr[A_T]$ (similarly for the other options).

Therefore, \mathcal{A} is a collection of $n = 2^k - 1$ pairwise independent and nontrivial events in Ω , which has size $|\Omega| = 2^k = n + 1$.