Problem. Suppose that in a sample space there are n mutually independent events $A_1, \ldots, A_n$ of probabilities $p_i = P(A_i)$ distinct from 1 and 0. Show that there are at least 2^n outcomes in the sample space.

It is hard to write down intersections of multiple sets, so we need a convenient notation. For any subset I of $\{1, \ldots, n\}$, let A_I denote the intersection of all events A_i with index i in I, and all events $\tilde{A}_j$ with index j not in I. For example, $A_{\{1,2\}} = A_1 \cap A_2 \cap \widetilde{A_3} \cap \ldots \cap \widetilde{A_n}$.

Solution. The index I runs over all subsets of the set $\{1, \ldots, n\}$, so there are 2^n different indexes I. Furthermore, the sets A_I and A_J with different indexes are disjoint. Indeed, if the indexes I and J are different, then they differ at least in one element; say, some number i is in I but not in J. Well, then $A_I \subset A_i$ and $A_J \subset \tilde{A}_i$, so A_I and A_J can not have common outcomes. Now, if we show that all intersection events A_I are non-empty, then we get at least 2^n outcomes (at least one outcome in each of the 2^n intersection events A_I).

Let us show that each A_I is non-empty. The event A_I is the intersection of events A_i indexed with $i \in I$ and events $\tilde{A}_j$ indexed with $j \notin I$. Since the n events A_i and $\tilde{A}_j$ are mutually independent, the probability $P(A_I)$ is the product of non-zero probabilities $p_i = P(A_i)$ and $1 - p_j = P\left(\tilde{A}_j\right)$. Since $P(A_I) \neq 0$, the event A_I is non-empty. End of proof.

Intuitively it is clear that if some events $B_1, \ldots, B_{k+1}$ are mutually independent, then the events $B_1, \ldots, B_k, \tilde{B}_{k+1}$ are also mutually independent. However, we need to formally prove it. Fortunately, it is not hard! Note also that if we can replace one set (say B_{k+1}) with its complement without losing mutual independence, then we can repeat the operation and replace another set (say B_5) with its complement. In other words, if we know that replacing one event in $B_1, \ldots, B_{k+1}$ with its complement does not result in a loss of independence, then replacing any number of events with their complements does not result in a loss of independence. I used this fact when I claimed that the n events A_i and $\tilde{A}_j$ are mutually independent.

Statement. If some events $B_1, \dots, B_{k+1}$ are mutually independent, then the events $B_1, \dots, B_k, \tilde{B}_{k+1}$ are also mutually independent.

Proof. Let I denote a subset $\{i_1, .., i_k\}$ of $\{1, \dots, k\}$ and J denote the set $\{i_1, .., i_k, k+1\}$, and $p_i = P(B_i)$. Then

$$P(B_I \cup B_J) = P(B_I) + P(B_J)$$

$$p_{i_i} * \dots * p_{i_k} = P(B_I) + \; p_1 * \dots * p_{i_k} * p_{k+1}$$

$$p_{i_1} * \dots * p_{i_k} * (1 - p_{k+1}) = P(B_I)$$

$$P(B_{i_1}) * \dots * P(B_{i_k}) * P(\tilde{B}_{k+1}) = P(B_I).$$

Thus, the probability of the intersection $B_{i_1} \cap \dots \cap B_{i_k} \cap \tilde{B}_{k+1}$ is the product of the corresponding probabilities. We also know that the probability of $B_{i_1} \cap \dots \cap B_{i_k}$ is the product of probabilities (since $B_1, \dots, B_{k+1}$ are mutually independent). So, $B_1, \dots, B_k, \tilde{B}_{k+1}$ are mutually independent.