Mutual independence, pairwise independence and k-wise independence: Events versus random variables

Amitabha Bagchi
Department of CS&E, IIT Delhi

September 30, 2017

1 Independence of collections of events

When we talk of independence of collections of events two definitions act as bookends, being the strongest and weakest of definitions: *mutual independence* and *pairwise independence*. Let us see what these are:

Definition 1. *Given a finite or countable index set I, a collection of events, $\mathcal{C} = \{A_i : i \in I\}$, is called* mutually independent *if for every $J \subseteq I$,*

$$P\left\{\bigcap_{i \in J} A_i\right\} = \prod_{i \in J} P\{A_i\}.$$

Definition 2. *Given a finite index set I, a collection of events, $\mathcal{C} = \{A_i : i \in I\}$, is called* pairwise independent *if for every $i, j \in I$,*

$$P\{A_i \cap A_j\} = P\{A_i\}P\{A_j\}.$$

Mutual independence is clearly the stronger definition since it implies pairwise independence. It is easy to constuct an example that shows that a collection can be pairwise independent but not mutually independence.

Example 1 ([1])**.** *Toss three fair coins independently. Define events A_{ij}: Coins i and j match ($i, j \in \{1, 2, 3\}, i \neq j$). $P\{A_{ij}\} = 1/2, i \neq j$, and if we take $i \neq j \neq k$, then*

$$P\{A_{ij} \cap A_{jk}\} = P\{\textit{All three coins match}\} = \frac{1}{4}.$$

This shows that the collection is pairwise independent.

But $P\{A_{12} \cap A_{23} \cap A_{13}\}$ is also equal to $P\{$All three coins match$\}$. However, the product of the probabilities of the three events is 1/8 which is less than 1/4, so mutual independence does not hold.

If we want to interpolate between the definitions of mutual independence and pairwise independence, we get the following definition of k-wise independence, for $k \geq 2$.

Definition 3. *Given a finite or countable index set I, and an integer $k \geq 2$, a collection of events, $\mathcal{C} = \{A_i : i \in I\}$, is called k-*wise independent *if for every $J \subseteq I$, $|J| \leq k$,*

$$P\left\{\bigcap_{i \in J} A_i\right\} = \prod_{i \in J} P\{A_i\}.$$

Note that setting $k = 2$ gives us pairwise independence and making k as large as required when I is finite gives us mutual independence.

Remark 1. There is a question here: Why did we require $|J| \leq k$ and not just leave it at the weaker condition $|J| = k$? To answer this let us look at the following example:

Example 2. *Consider two events A and B such that $P\{A \cap B\} \neq P\{A\}P\{B\}$, i.e., they are dependent events. Now consider a third event $C = \emptyset$. $P\{A \cap B \cap C\}$ is 0 since $C = \emptyset$, and for is $P\{A\}P\{B\}P\{C\}$ since $P\{C\} = 0$. So although every set of three events in this collection (there is only one set of three events) has the independence property, this collection is not pairwise independent.*

What this example tells us is that if we had fixed $|J| = k$ in the definition of k-wise independence then we cannot reach the definition of mutual independence even if we set k to be large enough.

2 Independence of collections of collections of events

The definition of independence and the three definitions for independence of collections can be generalised to collections of collections of events.

Definition 4. *Two collections of events, $\mathcal{C}_1$ and $\mathcal{C}_2$, are said to be* independent *if*

$$P\{A \cap B\} = P\{A\}P\{B\},$$

whenever $A \in \mathcal{C}_1$ and $B \in \mathcal{C}_2$.

Suppose we are given a collection $\mathfrak{C} = \{\mathcal{C}_i : i \geq 0\}$ where each $\mathcal{C}_i = \{A_{ij} : j \geq 0\}$ is a collection of events, let us make up a term and say that $\mathcal{A} = \{A_i : i \geq 0\}$ is a *representative* collection of $\mathfrak{C}$ if $A_i \in \mathcal{C}_i, i \geq 0$.

With this term, we can simply group the three definitions given above in one as follows:

Definition 5. *A collection $\mathfrak{C} = \{\mathcal{C}_i : i \geq 0\}$ where each $\mathcal{C}_i = \{A_{ij} : j \geq 0\}$ is a collection of events, is said to be mutually independent, pairwise independent, or, respectively, k-wise independent, if* every *representative collection of $\mathfrak{C}$, i.e., every collection $\{A_i : A_i \in \mathcal{C}_i, i \geq 0\}$, is mutually independent, pairwise independent, or, respectively, k-wise independent.*

3 Independence of collections of random variables

We approach notions of independence of random variables by viewing random variables as collections of events from the probability space. This means that collections of random variables can be viewed as collections of collections of events. This allows us to use the notions of independence for collections of collections of events to describe notions of independence for collections of random variables.

Without going into the technicalities of measure spaces, let us note that if we are given an outcome space Ω and we have a random variable X, i.e., a total function, $X : \Omega \to A$, that maps Ω to some set A, then X may also be viewed as a collection of events. For $a \in A$, define the set

$$B_{X,a} = \{\omega \in \Omega : X(\omega) = a\}.$$

Then the collection of events associated with X is:

$$\mathcal{C}_X = \{B_{X,a} : a \in A\}.$$

Now, recall how independence is defined for two random variables:

Definition 6. *Two random variables* $X_1 : \Omega \to A_1$ *and* $X_2 : \Omega \to A_2$ *defined on the same space* Ω *are said to be independent if*

$$P\{X_1 = a_1 \cap X_2 = a_2\} = P\{X_1 = a_1\}P\{X_2 = a_2\},$$

for all $a_1 \in A_1, a_2 \in A_2$.

Note that this is exactly equivalent to Definition 4 applied to the two collections $\mathcal{C}_{X_1}$ and $\mathcal{C}_{X_2}$.

So, now we can use Definition 5 to write an omnibus definition for collections of random variables.

Definition 7. *A collection of random variables* $\{X_i : i \geq 0\}$*, where* X_i *maps* Ω *to* A_i*, is said to be mutually independent, pairwise independent, or, respectively,* k*-wise independent, if the collection of collection of events* $\{C_{X_i} : i \geq 0\}$ *is mutually independent, pairwise independent, or, respectively,* k*-wise independent.*

Remark on k**-wise independence of random variables.** We observe a special property of the the collection of collection of random variable $\{C_{X_i} : i \geq 0\}$. Suppose we are given that this collection has the property that if we select *exactly* k random variables, then every representative collection has the independence property then we can show that every set of $k-1$ random variables also has the independence property. Consider the random variables $X_1, \ldots, X_{k-1}$ and $a_i \in A_i, 1 \leq i \leq k-1$. Choose another r.v. from the rest of the collection, let's say X_k. We know that for any event A,

$$\sum_{a \in A_K} \mathrm{P}\{A \cap X_k = a\} = \mathrm{P}\{A\}.$$

So, we can say that

$$\mathrm{P}\left\{\bigcap_{i=1}^{k-1}\{X_i = a_i\}\right\} = \sum_{a \in A_K} \mathrm{P}\left\{\{X_k = a\}\bigcap_{i=1}^{k-1}\{X_i = a_i\}\right\}.$$

By the exactly k-wise independence property the RHS is equal to

$$\sum_{a \in A_k} \mathrm{P}\{X_k = a\} \prod_{i=1}^{k-1} \mathrm{P}\{X_i = a_i\},$$

which is equal to $\prod_{i=1}^{k-1} \mathrm{P}\{X_i = a_i\}$ since $\sum_{a \in A_k} \mathrm{P}\{X_k = a\} = 1$. Thus we see that the collections of collections of events induced by random variables have a special property that, it is not hard to see, general collections of collections of events may not necessarily have. So, we conclude that the care we had to take in the definition of k-wise independence (as discussed in Remark 1) is required when we talk about collections of events but not required in the case of collections of random variables.

References

[1] E. Lehman, F. T. Leighton, and A. R. Meyer Mathematics for Computer Science. Lecture notes from Fall 2010, MIT Open Courseware. Retrieved September 2017.