Independence (Probabilistic) and Independence (Logical)

David Miller
Department of Philosophy
University of Warwick
COVENTRY CV4 7AL UK
http://www.warwick.ac.uk/go/dwmiller

Popper and the Philosophy of Mathematics
Karl-Popper-Foundation, Universität Klagenfurt, 5–7 April 2018
0 Summary of lecture
1 Initial conditions
2 New definitions of probabilistic independence
3 How should logical and probabilistic independence be related?
4 Maximal logical independence and contraprobability
5 References
The first task of this lecture is to present a well known problem concerning probabilistic independence that arises whenever elements with extreme probabilities (probabilities of 0 and 1) are of serious interest, to criticize briefly a solution published in 2017 by two leading writers in this area, and to compare it with the solution offered by Karl Popper in 1994 in appendix *XX of *Logik der Forschung*.

The question inevitably arises of what job the relation of probabilistic independence should be asked to perform, in particular how it is related to logical independence. Relevant here is an extensive 1997 discussion by Georg Dorn.
It turns out that probabilistic independence, however defined, and logical independence, as usually understood, are not smoothly related. This may be of scant concern to physical interpretations of probability, but it is an unwelcome result for the logical interpretation, whose main aim is to give a metrical generalization of logical relations.

The second task of the lecture is to resolve the problem by understanding logical independence in a different (but not scandalously different) way, and by replacing logical probability by a different measure, contraprobability (which in Miller & Popper 1986 was called deductive dependence).
In the classical theory, codified in the axioms of Kolmogorov, in which absolute probability \( p(a) \) is primitive, elements \( a, b \) within the domain of the function \( p \) are defined in this way to be *probabilistically independent*:

\[
\mathcal{U}(a, b) \leftrightarrow p(ab) = p(a)p(b).
\]

The relation \( \mathcal{U} \) is symmetric. An immediate and untoward consequence is the probabilistic independence of every element \( a \) from every element \( b \) for which \( p(b) = 0 \); in particular every element \( a \) is probabilistically independent of the contradictory (or zero) element \( s \), even though \( a \), being deducible from \( s \), is logically dependent on \( s \).
It is rather less obvious that every element $b$ with probability 1 stands in the relation $\mathcal{U}$ to every element $a$. For if $p(b) = 1$, then $p(a \lor b) \leq p(b)$, whence by the addition and monotony laws $p(a) \leq p(ab) \leq p(a)$, from which it follows that $p(ab) = p(a)p(b)$. As a consequence, the tautological (or unit) element $t$ is probabilistically independent of every element $a$, even though $t$, being deducible from $a$, is logically dependent on $a$.

In response to these oddities, the classical theory admits a stronger (asymmetric) sense of independence in terms of the relative (often called conditional) probability $p(a, b)$. 
The relative (or conditional) probability $p(a, b)$ is defined, whenever $p(b) \neq 0$, by $p(a, b) = p(ab)/p(b)$.

The stronger classical definition of independence is this:

\[ DV \quad \mathcal{V}(a, b) \iff p(a, b) = p(a). \]

Since $p(a, b)p(b) = p(ab)$ for any $b$, $DV$ implies $DU$. Moreover, $\mathcal{V}(a, b)$ holds, just as $\mathcal{U}(a, b)$ does, when $p(b) = 1$. It holds too when $p(a) = 0$ and $p(b) \neq 0$. But the conclusion that any element $a$ is independent of $s$ is thwarted, since the term $\mathcal{V}(a, s)$ is ill formed. Nonetheless, $\mathcal{V}(t, b)$ and $\mathcal{V}(s, b)$ both hold when $b \neq s$. 
In the theory presented in appendices *iv and *v of *The Logic of Scientific Discovery* the term \( p(a, b) \) is well defined for all \( a, b \). Elements \( a, b \) have a conjunction \( ab \), and each \( a \) has a negation \( a' \). The disjunction \( a \lor b \), which is defined via De Morgan's laws, obeys the general addition law
\[
p(a, c) + p(b, c) = p(ab, c) + p(a \lor b, c).
\]

The self-contradictory and tautological elements \( s \) and \( t \) are defined in the usual way. The value of \( p(a, s) \) is equal to 1 for every \( a \), and so the special addition law
\[
p(a, b) + p(a', b) = 1
\]
holds if & only if \( b \) is distinct from \( s \). The absolute probability \( p(a) \) of \( a \) is identified with \( p(a, t) \).
Made aware by Dorn of the problems, noted above, in the classical definition of independence when applied to $s$ and $t$ (and to other elements with extreme probabilities), but also wanting some contingent statements with probability 1, such as ‘There exists a white raven’ and ‘There exists a golden mountain’, to count as independent of each other, Popper defined two new relations of weak independence $\mathcal{W}(a, b)$ and independence $\mathcal{I}(a, b)$:

**DW**

$$\mathcal{W}(a, b) \leftrightarrow p(a, b) = p(a, b'),$$

**DI**

$$\mathcal{I}(a, b) \leftrightarrow$$

$$\mathcal{W}(a, b) \& \mathcal{W}(a', b) \& \mathcal{W}(b, a) \& \mathcal{W}(b', a).$$
Popper showed several simple results about $\mathcal{W}$ and $\mathcal{I}$: If $\mathcal{W}(a, b)$, then $\mathcal{p}(a, b) = \mathcal{p}(a)$; that is to say, $\mathcal{V}(a, b)$. $\mathcal{I}$ is symmetric; that is, $\mathcal{I}(a, b)$ is equivalent to $\mathcal{I}(b, a)$. $\mathcal{I}(a, b)$ is equivalent to $\mathcal{I}(a, b')$; and also to $\mathcal{I}(a', b)$ (and, he could have added, equivalent to $\mathcal{I}(a', b')$ too).

Near the end of appendix *XX*, he showed directly that $\mathcal{I}(a, b)$ implies $\mathcal{U}(a, b)$, so that probabilistic independence, newly defined, ‘implies classical independence’. Indeed, $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$, and $\mathcal{I}$ are increasingly strict relations.
A recent paper by Fitelson & Hájek, published in 2017, but on line since 2014, which adopts the practice of taking relative probability as primitive, also dismisses DU for implying that ‘anything with extreme probability has the peculiar property of being probabilistically independent of itself’; this is a state of affairs that, they judge, may perhaps be acceptable for contingent events with probability 1 (§6), but is intolerable for those with probability 0 (§8).

They accordingly propose, as successors to DU, two definitions of probabilistic independence: one is DV released from the restriction that \( p(b) \neq 0 \), the other is DW.
2 The symmetry of the relation $\mathcal{I}$

It is to be regretted that Fitelson & Hájek have paid no attention to *XX of Logik der Forschung. As we shall see, the definition $\mathcal{D}_I$ is in several ways better than either $\mathcal{D}_V$ or $\mathcal{D}_W$. No element $a$ is counted by $\mathcal{D}_I$ as independent of itself or of its negation: $\neg \mathcal{I}(a, a)$ and $\neg \mathcal{I}(a, a')$.

Like $\mathcal{U}$, the relation $\mathcal{I}$ is symmetric. The two independence relations $\mathcal{V}$ and $\mathcal{W}$ that Fitelson & Hájek favour (but do not choose between) are asymmetric. They seem to regard it as a discovery that ‘on a Popperian account of independence’, as they audaciously refer to their proposals, ‘we must specify a direction of independence’ (§8).
The main theorem (*Haupttheorem*) of Popper’s appendix *XX states that neither s nor t bears the relation \( \mathcal{I} \) to any element (itself included). The proof reduces to this: by DW, \( \mathcal{W}(a, t) \) is equivalent to \( p(a) = 1 \); whence, by the addition law, at least one of \( \mathcal{W}(a, t) \) and \( \mathcal{W}(a', t) \) is false. But each follows from \( \mathcal{I}(a, t) \), so \( \mathcal{I}(a, t) \) is false. Since \( \mathcal{I}(a, b) \) and \( \mathcal{I}(a, b') \) are equivalent, \( \mathcal{I}(a, s) \) is also false. By symmetry, \( \mathcal{I}(t, a) \) and \( \mathcal{I}(s, a) \) are false.

Popper did not assert it (let alone prove it), but he would undoubtedly have been pleased that, according to DI, no element \( a \) is independent of itself, or of its negation \( a' \).
The falsity of $\mathcal{I}(a, a)$ is trivial when $0 < p(a) < 1$, since $\mathcal{I}(a, b)$ implies $\mathcal{U}(a, b)$, but it may be proved for all elements $a$. Let me offer a proof in Popper’s memory.

First of all, $\mathcal{I}(a, a)$ reduces to the conjunction of $\mathcal{W}(a, a)$ and $\mathcal{W}(a', a)$; that is, to the conjunction of $p(a, a) = p(a, a')$ and $p(a', a) = p(a', a')$. Since $p(b, b) = 1$ for any $b$, these equations imply that $p(a, a')$ and $p(a', a)$ both equal 1, so that the multiplication law, used twice, yields $p(a) = p(a') = p(aa') = 0$. The addition law precludes this, and so $\mathcal{I}(a, a)$ is false. Since $\mathcal{I}(a, b)$ and $\mathcal{I}(a, b')$ are equivalent for all $b$, $\mathcal{I}(a, a')$ too is false.
Another result that Popper envisaged, but did not prove, is the possibility that two elements with unit probability, such as two logically independent existential statements, can be probabilistically independent. To show this, let \( t \) be the closed interval \([0, 1]\), and \( a \) and \( b \) be the half-open intervals \((0, 1]\) and \([0, 1)\). Under the uniform measure:

<table>
<thead>
<tr>
<th></th>
<th>( a )</th>
<th>( a' )</th>
<th>( b )</th>
<th>( b' )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a )</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( a' )</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( b )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( b' )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

\[
p(a, b) = 1 = p(a, b') \quad W(a, b) \\
p(a', b) = 0 = p(a', b') \quad W(a', b) \\
p(b, a) = 1 = p(b, a') \quad W(b, a) \\
p(b', a) = 0 = p(b', a') \quad W(b', a)
\]
2 Logical independence of the conjuncts in $\mathcal{I}(a, b)$

The definition $DW$ offered by Popper of the weak independence $\mathcal{W}(a, b)$ of elements $a$ and $b$ is given by the equation $p(a, b) = p(a, b')$, while his definition $DI$ of (strong) independence consists of the conjunction of the four formulas $\mathcal{W}(a, b), \mathcal{W}(a', b), \mathcal{W}(b, a), \mathcal{W}(b', a)$.

Since $DW$, the less pedestrian of Fitelson & Hájek’s preferred definitions of independence, is limited to the first of these formulas, it is natural to ask what work the other three conjuncts do in the definiens of $\mathcal{I}(a, b)$. Are they all needed? Is each of them logically independent of the others? Are there any logical connections among them?
Complete independence was introduced, and exploited, by E. H. Moore (1910). It is well known to philosophers as the kind of independence enjoyed by atomic propositions in Wittgenstein’s *Tractatus*; that is, a set of statements is completely independent if all the members of any subset can be true while all the remainder are false. A completely independent set is consistent — its members can all be true together — and (simply) independent — one member can be false while all the others are true.

It turns out that the set of conjuncts in $\mathcal{I}(a, b)$ is consistent and independent, but not completely independent.
We know that if neither $p(a)$ nor $p(b)$ equals either 0 or 1, then $\mathcal{W}(a, b)$, $\mathcal{W}(a', b)$, $\mathcal{W}(b, a)$, and $\mathcal{W}(b', a)$ are logically equivalent ways of stating the probabilistic independence of $a$ and $b$ (according to DU). This means that they are all true when $a$ and $b$ are, like reports of throws of dice, independent, and all false when they are not.

It will be shown that exactly one of $\mathcal{W}(a, b)$, $\mathcal{W}(a', b)$, $\mathcal{W}(b, a)$, and $\mathcal{W}(b', a)$ can be false, and that exactly two of them can be false. But it is not possible for exactly three of them to be false. By symmetry it will be enough to investigate just one singleton, one pair, and one triple.
When two out of three conjuncts in \( I(a, b) \) are false

Suppose that \( W(a, b) \), the first conjunct of \( I(a, b) \), is true and that \( W(a', b) \), its second conjunct, is false. This supposition is equivalent, by DW, to the conjunction \( p(a, b) = p(a, b') \& p(a', b) \neq p(a', b') \), which complies with the addition law if & only if \( b \) is identical with one or other of \( s \) and \( t \). In either case \( p(a) \) equals 1.

Now suppose that \( W(b, a) \), the third conjunct of \( I(a, b) \) is false. Then by DW, \( p(b, a) \neq p(b, a') \), which is impossible if \( b = t \). It follows that \( b = s \) and therefore that \( b' = t \). But then \( W(b', a) \), the fourth conjunct of \( I(a, b) \), which says that \( p(b', a) = p(b', a') \), is true.
Given this analysis, it is straightforward to find elements $a$ and $b$, and values for the function $p$ such that, of the four conjuncts that make up $I(a, b)$, (i) only $W(a', b)$ and $W(b, a)$, the second and third conjuncts, are false, and (ii) only $W(a', b)$, the second conjunct, is false.

We obtain an example where (i) two of the conjuncts in $I(a, b)$ are true, and two are false, by identifying $b$ with $s$ and $a$ with $t$. $W(a, b)$ and $W(b', a)$ then reduce (slightly differently) to $p(t, s) = p(t, t)$; that is, to the truth $1 = 1$, while $W(a', b)$ and $W(b, a)$ both reduce to $p(s, t) = p(s, s)$; that is, to the falsehood $0 = 1$. 

© D. W. Miller 2018 Please do not cite without permission.
An example of (ii) is obtained by identifying $b$ with $t$, and $a$ with a distinct (that is, contingent) element with unit probability. Then $p(a, b) = 1 = p(a, b')$ and $p(b', a) = 0 = p(b', a')$; but $p(a', b) = 0 \neq 1 = p(a', b')$ and $p(b', a) = 0 = p(b', a')$. In short, $\mathcal{W}(a', b)$ is false, but the other three conjuncts in $\mathcal{I}(a, b)$ are all true. This example shows also that Popper’s Haupttheorem does not follow from $\mathcal{W}(a, b)$, $\mathcal{W}(b, a)$, and $\mathcal{W}(b', a)$ together.

By an appeal to the invariance of $\mathcal{I}(a, b)$ if $a$ and $b$ are interchanged, or if either is replaced by its negation, we may extend these results to any choice of conjuncts.
That the conjuncts of $\mathcal{I}(a, b)$ are not completely independent is an unexpected result, but does it have much significance? In advising us that whenever $\mathcal{W}(a, b)$ is true at least one of the other conjuncts in $\mathcal{I}(a, b)$ is true, it suggests that even if the definition $\text{DW}$ commended by Fitelson & Hájek is not relinquished in favour of Popper’s $\text{DI}$, it ought to be enriched with at least one further conjunct. This can be accomplished in seven different ways.

At several places the prospect of a range of relations of probabilistic independence (as there exists for logical independence) is equably entertained by Fitelson & Hájek.
3 Probabilistic dependence and confirmation

Not before time we must face the question of what problems a definition of probabilistic independence is designed to illuminate. I am thinking here not of physical interpretations of probability (frequency, propensity), where hypotheses of independence play a crucial role, but of what is called logical or epistemic or judgemental probability.

In various places Fitelson & Hájek adduce a link between probabilistic dependence and evidential or confirmational relevance. They ask, for example, apropos the dependence of any proposition on itself (§ 6): ‘What better support, or evidence, for X could there be than X itself?’
3 Logical and probabilistic independence

A different idea, however, is visible when they write a few lines later that ‘[w]e may well want inductive logic, understood as probability theory, to be continuous with deductive logic’. This is the suggestion that probabilistic dependence and independence may be generalizations of logical dependence and independence. The viability of this suggestion is the topic of the rest of this lecture.

The matter is not entirely simple or entirely satisfactory. But, setting aside some subtleties for the moment, we may say that complete logical independence does not imply, and is not implied by, probabilistic independence.
Let us begin with the proposal that the logical dependence of $a$ and $b$ should ensure that they are also probabilistically dependent; in other words, if any one of the four relations $a \vdash b$, $a \vdash b'$, $a' \vdash b$, and $b \vdash a$, holds, then there is no probability measure $p$ under which $a$ and $b$ turn out to be probabilistically independent, $I(a, b)$.

This is a simplified form of the strong harmony requirement of Dorn (1997), §11.6.1. If we exclude those probability measures under which some contingent elements have extreme probabilities, it is a truism. Nonetheless it is infringed, as Dorn was aware, by Popper’s definition $DI$. 

© D. W. Miller 2018

Please do not cite without permission.
Here is a simple example. Let $t$ be the closed interval $[0, 1]$, $a$ the half-open interval $(0, 1]$, and $b$ the singleton $\{1\}$. The uniform measure yields the relative probabilities given in the table below, from which the probabilistic independence $\mathcal{I}(a, b)$ of $a$ and $b$ follows. Yet $b$ implies $a$. Likewise $\mathcal{I}(a', b)$, yet $b$ contradicts $a'$. And so on.

<table>
<thead>
<tr>
<th></th>
<th>$a$</th>
<th>$a'$</th>
<th>$b$</th>
<th>$b'$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$a'$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$b$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$b'$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

$\mathcal{I}(a, b) = 1 = \mathcal{I}(a, b') = \mathcal{W}(a, b)$

$\mathcal{I}(a', b) = 0 = \mathcal{I}(a', b') = \mathcal{W}(a', b)$

$\mathcal{I}(b, a) = 0 = \mathcal{I}(b, a') = \mathcal{W}(b, a)$

$\mathcal{I}(b', a) = 1 = \mathcal{I}(b', a') = \mathcal{W}(b', a)$
Dorn wrote (*loc.cit.*): ‘in the light of the strong version of the harmony requirement, the semantics of probabilistic relations of dependence and independence is still in a mess’. I shall soon suggest a drastic way out of the mess, but first a straightforward expedient should be recorded.

This is to define \( a \) and \( b \) are probabilistically independent (with respect to \( p \)) as the conjunction of \( \mathcal{I}(a, b) \) and logical independence; and then to say that \( a \) and \( b \) are probabilistically independent simpliciter if they are so with respect to every function \( p \). It follows at once that logically dependent elements are probabilistically dependent.
This proposal may seem to be rather contrived, but it does point to something odd about Dorn’s strong harmony requirement. For in the normal run of things, it is not logical dependence that is regarded as a symptom of probabilistic dependence, but logical independence that is regarded as a symptom of probabilistic independence. (Often, it should be said, logical independence is required to be relative to a substantial background theory.)

Recall Popper’s hope that ‘There exists a white raven’ should turn out to be probabilistically independent of the logically independent ‘There exists a golden mountain’.
Even in non-extreme cases, it is a decision, not a truism, to regard logically independent elements as probabilistically independent, and it incorporates no suggestion that the latter must hold for every probability measure \( p \). The decision is a characterization of admissible probability measures, not a description of all possibilities. There are always measures under which the results of unrelated coin tosses, for example, are probabilistically dependent.

Unfortunately this way of connecting logical and probabilistic independence leads nowhere. It is firmly blocked if there exist more than two logically independent elements.
3 Complete logical independence leads to extremism

It was proved by Popper & Miller (1987) that if there exist three completely independent elements, and completely independent elements are asked to be probabilistically independent in the sense of DU (or DV, DW, or DI), then some of them have probability $0$ or probability $1$.

Proof. It is easily shown that if $\{a, b, c\}$ is a completely independent triple, then $\{ac, b\}$ and $\{ab, cb\}$ are completely independent pairs. It is implied by probabilistic independence that
\[
p(a)p(b)p(c) = p(ac)p(b) = p(abc) = p(ab)p(cb) = p(a)p(b)^2p(c),
\]
and therefore at least one of $p(a)$, $p(b)$, and $p(c)$ is $0$, or $p(b) = 1$. 

© D. W. Miller 2018

Please do not cite without permission.
There is another familiar generalization of simple logical independence. The pair \( \{a, b\} \) is said to be maximally independent if neither \( a \) nor \( b \) is a consequence of the other (simple independence) and, additionally, no (non-tautological) consequence of \( a \) or of \( b \) is a consequence of the other. Their common consequences are exactly the tautologies (which are consequences of all elements). In traditional terms \( a \) and \( b \) are independent subcontraries.

This definition can be generalized to all sets of elements. Tarski proved in 1930 that every set of elements is equivalent to a maximally independent set (it may be empty).
4 Contrasting complete and maximal independence

In short, if $a$ and $b$ are completely independent then neither provides any information about the truth value of the other, while if they maximally independent neither provides any information about the content of the other.

In §5 of ‘Carnap’s Inductive Logic’ (1967) Salmon asserted that statements $a$ and $b$ that are ‘entirely about the past’ and ‘entirely about the future’ respectively are independent in some sense, but not maximally independent. But then $a \lor b$ is entirely about both the past and the future, which implies that it is about neither, and is a tautology. This can hardly be what Salmon intended.
Theorem 1 of Popper & Miller (1987), mostly anticipated in their (1983) paper, states that, if $a$ and $b$ are maximally independent, then $p(a, b) < p(a)$, except when $p(a, b) = 1$ or $p(b) = 1$. That is, except in extreme cases, maximally independent elements are not probabilistically independent in any of the senses considered.

What is causing this impasse is not, I suggest, the unavailability of an appropriate sense of logical independence. What is missing is a way of measuring degrees of deducibility that is distinct from orthodox probability measures and in harmony with maximal independence.
The function $q(a, b)$, here to be called the contraprobability of $a$ given $b$, is defined as equal in value to $p(b', a')$. By the law of contraposition, $a'$ logically implies $b'$ if & only if $b$ logically implies $a$, and in this case both $p(a, b)$ and $q(a, b)$ take the value 1. But whereas $p(a, b) = 0$ whenever $a$ and $b$ are contraries, $q(a, b) = 0$ whenever $a$ and $b$ are subcontraries; in particular, $q(a, b) = 0$ whenever the elements $a$ and $b$ are maximally independent.

In contrast to $q(a, b)$, $p(a, b) - p(a) = 0$ whenever $a$ and $b$ are probabilistically independent (by DV, DW, DI), but not, alas, whenever they are logically independent.
Observe that the result just stated holds for all underlying probability measures $\mathfrak{p}$, so that something akin to Dorn’s harmony requirement, albeit in the opposite direction, has been rehabilitated. Dorn hoped that logical dependence might imply probabilistic dependence for every probability measure, while what is demonstrable is that maximal independence implies contraprobabilistic independence [that is, $q = 0$] for every probability measure.

Yet there are measures under which $q(a, b) = 0$ when $a$ and $b$ are not maximally independent. For $\mathfrak{p}(a'b') = 0 \neq \mathfrak{p}(b')$ is quite possible when $a \lor b$ is not a tautology.