ISSN 2250-0987
Gennaro Auletta, UNIASCIT, Vol 2 (2), 2012, 216-221

INFERENCES WITH INFORMATION

Gennaro Auletta[#1]

[#]*University of Cassino. Philosophy Department*

***Abstract*— This paper develops a connection between logical inferences and information transmission/sharing. It can turn out to be very helpful when our problem is to do the best guess about the meaning of a message.**

***Keywords*— Equivocation, Venn diagram, premises, conclusion, inference.**

Information deals with continuous quantities (when integrals of probabilities are used) or in many cases with infinite countable sets (when sums are considered). Logic, on the contrary, deals with propositions or statements that can only assume two "values", truth or falsity. Nevertheless, a connection between logic and information can be very helpful when dealing with situations in which we actually perform inferences or guesses about information, e.g. when we would like to infer the correct meaning of a message.

In order to build a fruitful and robust connection between logic and information theory, we must ask about the general significance of some logical expressions and how they could be interpreted in terms of information transmission (the most basic form of dealing with information). A traditional way to write the main statements involved in logic calculations is:

$(\forall t)(Xt \rightarrow Yt)$, $(\forall t)(Xt \rightarrow \neg Yt)$,

$(\exists t)(Xt \wedge Yt)$, $(\exists t)(Xt \wedge \neg Yt)$,

The reason why I am considering the above expressions and not forms taken form the basic propositional logic is that they allow a direct use of Venn diagrams that are very helpful for solving our problem. However, for the sake of simplicity here and in the following I avoid to make use of quantifiers. Then, for practical purposes I take the terms (each of which stands for some subject or some predicate) X, Y, and Z to be kinds of propositions meaning: "The object t is member of the class X", "The object t is member of the class Y", or "The object t is member of the class Z", and reformulate the above statements as

$X \rightarrow Y$, $X \rightarrow \neg Y$, $X \wedge Y$, $X \wedge \neg Y$.

Therefore, each logical term is referred to some class and for this reason I shall also use X, Y or Z as a shorthand for denoting the relative class (and therefore it has to be taken as a logical term). When in some situations ambiguities arise one can make use more specific distinctions, for instance introducing an indices like X1 and X2.

When we say that $X \rightarrow Y$, we mean that X is sufficient condition of Y. This tells that if Y is true we cannot say nothing about X, which can be either true or false. Then, the implication $X \rightarrow Y$ can be represented in information theory with the concept of equivocation (conditional entropy): $H(X|Y)$, which expresses the incertitude or randomness of the output X relative to the input Y. Similar formulations are true for all other implications, some of which I resume here:

$X \rightarrow Y$	$H(X\|Y)$
$Y \rightarrow X$	$H(Y\|X)$
$Z \rightarrow Y$	$H(Z\|Y)$
$Z \rightarrow X$	$H(Z\|X)$.

This clearly shows that it is not information that is "transmitted" during a process of information exchange but at most equivocation. Information makes only sense from the perspective of a potential receiver (from the point of view of the code X relative to an input Y). As far as we do not consider such a situation, what we actually transmit (from the point of view of the sender or of the source) is only a physical signal that can eventually acquire an informational value only when it is considered (and foremost codified) from the point of view of the receiver. This is also clear when we consider the fact that during any process of information exchange there is always information dispersion and therefore growth of entropy, what shows that we cannot say in any sense that is information to be transmitted. At the opposite, it is equivocation to be "transmitted" to the extent to which it never decreases (generally, it increases across some communicative steps).

To express this more accurately, I can say that equivocation is present in any information transmission or exchange so that the conditional entropies above are a good expression of such a process. On the contrary, when information is only shared, equivocation does not necessarily occur (apart from degradation processes due to physical-thermodynamic factors). Another form to say this is the following: apart from the information that is already shared (which however in itself does not add new knowledge) all the rest in any information exchange is necessarily equivocation (since it falls outside the information that we share). It is clear that we can in fact get new information during some information exchange. However, what happens is that we are able to expand the information that we share with the sender thanks either to a new communication or to some additional information that we share with a third party that allows us to reduce the equivocation present in the first message. In other words, any information exchange is ultimately a kind of error correction.

Unfortunately, a causal-mechanical understanding of information exchange has misunderstood this basic point by assuming that information somehow "propagates" from a source to a receiver. In very elementary and limiting cases we can say this only in a figurative sense, but to assume that this describes communication is certainly wrong.

A totally different treatment deserves the implication $X \rightarrow \neg Y$. Indeed, such an implication when translated in the language of information theory expresses a certitude about the relation between input Y and output X. Indeed, suppose that Y is logically true. This determines that X is false. Translated in terms of information, we have that the variability of the output X is univocally correlated with the variability of the input Y or that the variability of X is without equivocation. Then, the above implication $X \rightarrow \neg Y$ can be expressed as the information that X and Y share, or their mutual information:

$$X \rightarrow \neg Y \qquad I(X:Y)$$
$$Y \rightarrow \neg X \qquad I(X:Y)$$
$$Z \rightarrow \neg Y \qquad I(Z:Y)$$
$$Z \rightarrow \neg X \qquad I(Z:X).$$

I recall that

$$I(X:Y) = H(X,Y) - H(X) - H(Y)$$

or

$$H(X) = H(X|Y) + I(X:Y).$$

All that means that the quantity H(X) can be associated to the logical form $\neg X$ since it expresses the variability of X, and the same is true for H(Y) and H(Z). Indeed, if X represents a truth is fully deprived of potential informational value (in other words, the negation tells that the message has been already univocally determined).

The joint entropy of X and Y:

$$H(X,Y) = H(X) + H(Y) - I(X:Y)$$
$$= H(Y) + H(X|Y)$$
$$= H(X|Y) + H(Y|X) + I(X:Y)$$

can be put in relation with the logical expression

$$\neg X \wedge \neg Y,$$

since it expresses the incertitude of both X and Y.

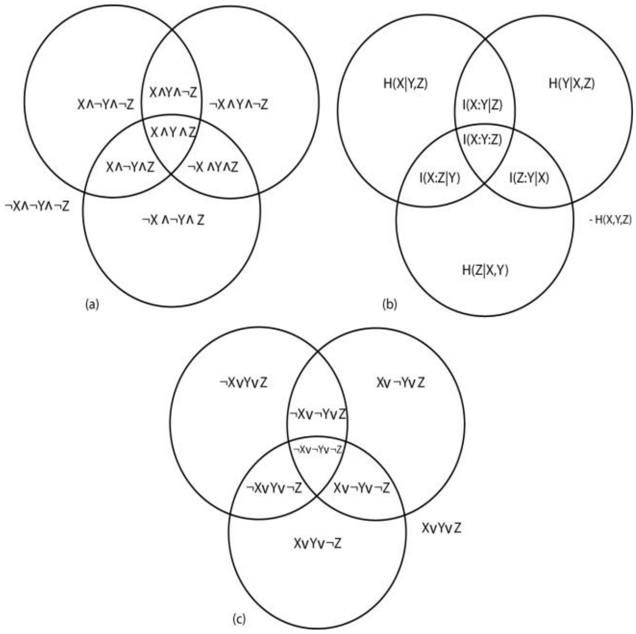

Fig. 1 A comparison of the logical and information-theory Venn's diagrams. (a) Traditional logical expressions with their relative Venn-diagram representation. (b) Traditional information-theory expressions. (c) Logical counterpart of the information-theory expressions. It is clear that the latter are contradictory relative to the traditional logical expression. For this reason, what in insert (a) is sum of subsets here is intersection and vice versa. I stress that what does matter here is the established correspondence between expressions and not areas: e.g. H(X|Y) corresponds to $X \rightarrow Y$ and not to $X \wedge \neg Y$.

The expressions involving three terms or sets are always a little more cumbersome but can be computed in a recursive way (see Fig. 1):

$$H(X,Y,Z) = [H(X) - I(X:Y)] + [H(Y) - I(Y:Z)] + [H(Z) - I(X:Z)] = H(X,Y) + H(Z|X,Y).$$

This allows us to write the following expression:

$$H(Z|X,Y) - H(X,Y,Z) = - H(X,Y),$$

which corresponds to the logical expression $X \vee Y$. This expression tells that nothing can be said about the relations between X and Y (neither whether or not a signal was sent). We can build similar forms

$$- H(Z,X) = H(Y|Z,X) - H(X,Y,Z)$$
$$- H(Z,Y) = H(X|Z,Y) - H(X,Y,Z).$$

Another interesting expression is

$$d(X,Y) = H(X|Y) + H(Y|X),$$

which is known as variation of information and helps us to build the counterpart of the logical form $X \wedge Y$:

$$d(X,Y) - H(X,Y) = - I(X:Y).$$

This expression tells us that there is no joint variability of X and Y or that both X and Y are deprived of potential informational value (which corresponds to a logical certitude). Moreover,

$$H(Y) - H(X,Y) = - H(X|Y)$$

corresponds to the logical form $X \wedge \neg Y$. Similarly,

$$- H(Z|X) = H(X) - H(X,Y)$$
$$- H(Z|Y) = H(Y) - H(X,Y).$$

Consider also the following relation:

$$H(X|Y,Z) + I(Z:X|Y) = H(X|Y),$$

which corresponds to

$$(\neg X \vee \neg Y \vee Z) \wedge (\neg X \vee Y \vee \neg Z) = \neg X \vee Y.$$

Similarly,

$$H(Z|X,Y) + I(Y:Z|X) = H(Z|X),$$
$$H(Z|X,Y) + I(Z:X|Y) = H(Z|Y).$$

It is also interesting to observe that

$$I(X:Y|Z) + I(X:Y:Z) = I(X:Y),$$
$$I(X:Z|Y) + I(X:Y:Z) = I(X:Z),$$
$$I(Z:Y|X) + I(X:Y:Z) = I(Z:Y).$$

Let us also remark that:

$$I(X:Y:Z) = I(X:Y) - I(X:Y|Z),$$

and similarly for I(Z:X) and I(Z:Y).

I have already said that actual information transmission goes always with equivocation together. On the contrary, when there is mutual information we can only say that the conditions have been established (essentially we have built a channel) allowing to have such a communication. Therefore, to have a channel is a weaker condition that to actually transmit information (which requires a channel). However, it is a necessary condition for having such transmission. On the other hand, to deny that there is a channel is stronger statement than to deny that there information transmission.

With these tools let us now try to express in information terms the inference:

If $X \rightarrow Y$ and $Z \rightarrow X$, then $Z \rightarrow Y$.

In other words, what we would like to see is whether also in the conditional entropies involved in information transmission there is the same transitivity that we have in implications. Now, we see how fruitful was the assumption that the implication expresses equivocation. Indeed, faithful transmission or mutual information is not preserved across several communication steps, since, as mentioned, each transmission of information is subject to dispersion and noise that is always a kind of information loss. So, we cannot say that if Y is faithfully connected to X and X to Z, also Y is to Z. On the contrary, we can certainly say that if X represents the equivocation about the input Y and Z represents the equivocation about the input X, then Z equivocates Y at least for the amount given by the sum of the two previous equivocations but not less. Then, we are intuitively justified in affirming that

If H(Z|X) and H(X|Y), then H(Z|Y).

Let us combine the premises:

$$H(X|Y) + H(Z|X) = H(Z|Y,X) + I(X:Z|Y) + H(Z|X,Y) + I(Z:Y|X).$$

Let us consider the second and third elements in the RHS of the previous expression. Their sum is

$$I(X:Z|Y) + H(Z|X,Y) = H(Z|Y),$$

which is the desired result. Since we can write

$$H(X|Y) + H(Z|X) = H(Z|Y) + H(Z|X),$$

it is clear that the conclusion plus one of the premises is equivalent to the sum of the premises, which justifies the inference. The interpretation of the above inference is quite straightforward: If there is information transmission from Y to X and from X to Z, we

ISSN 2250-0987
Gennaro Auletta, UNIASCIT, Vol 2 (2), 2012, 216-221

can say that there is also information transmission from Y to Z. We can express this by writing the inference in terms of the following inequality:

$$H(Z|X) + H(X|Y) \geq H(Z|Y),$$

as it is also clear by having a look at Fig. 2.

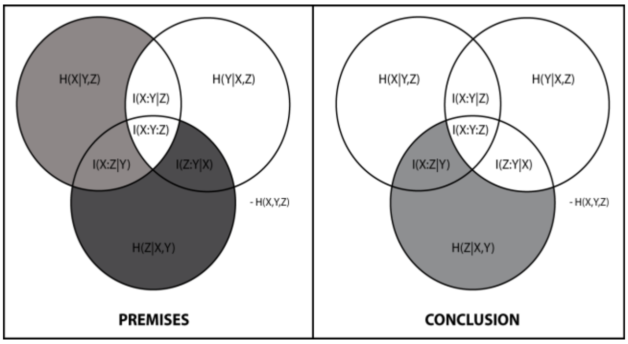

Fig. 2: The inference H(Z|X) + H(X|Y) ≥ H(Z|Y).

Let us now consider the following classical inference:

If $X \rightarrow \neg Y$ and $Z \rightarrow X$, then $Z \rightarrow \neg Y$.

We expect that if X and Y share information, that is, I(X:Y), and there is some equivocation Z relative to X (H(Z|X)), also Z and Y will share some information. Let us reformulate the two premises as:

$$I(X:Y) + H(Z|X) = I(X:Y|Z) + I(X:Y:Z) + H(Z|X,Y) + I(Z:Y|X).$$

Now we can remark that the sum of the second and last elements gives:

$$I(X:Y:Z) + I(Z:Y|X) = I(Z:Y),$$

which is the desired result. Now, we can write the premises as:

$$H(X,Z) - H(X|Y) = I(X:Y|Z) + H(Z|X,Y) + I(Z:Y).$$

This identity shows that the RHS of the top line is again an alternative way to consider the dealing with information represented by the premises. Indeed, we can say that to have both X and Y that share information and Z that equivocates X is equivalent to say that Z that shares information with Y, that X and Y share information but not with Z, and that Z equivocates both X and Y. An alternative way to say this is that to have both X and Y that share information and Z that equivocates X is equivalent to affirm that Z equivocates both X and Y and Z and X jointly share information with Y:

$$I(X:Y) + H(Z|X) = I(X,Z:Y) + H(Z|X,Y),$$

where

$$I(X,Z:Y) = I(X:Y) + I(Z:Y) - I(X:Y:Z).$$

Note that we have succeeded in writing an equivalence between the sum of the two premises and the sum of other two terms that bear some structural similarity to them. The general significance of the above inference in terms of information theory is the following: if X shares information with Y and X transmits information to Z, then we can say that Z shares information with Y. As remarked, to share information is weaker than to actually transmit information (nothing ensures that the two partner will ever communicate). However, why we cannot say that to have a channel between X and Y as well as between Z and X implies that there is also a channel between X and Y? The fact that nothing ensures that the first two channels are really "lined up". It is a fallacy comparable with that occurring in logic when trying to derive a conclusion only from particular premises. In other words, in order to formulate any statement about information sharing or exchanging we need an actual information transmission or exchange, and the same is true when we correct some equivocation. Also here we can write the inference as an inequality (see Fig. 3).

$$I(X:Y) + H(Z|X) \geq I(Z:Y).$$

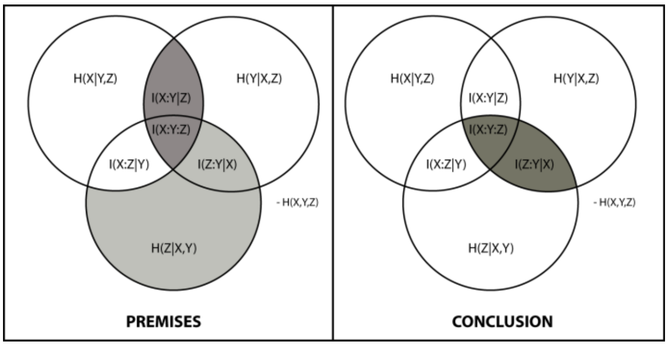

Fig. 3: The inference I(X:Y) + H(Z|X) ≥ I(Z:Y).

More difficult to interpret is the equivalent of the classical inference:

If $X \rightarrow Y$ and $Z \wedge X$, then $Z \wedge Y$.

Our aim is to derive – I(Z:Y) from premises H(X|Y) and – I(Z:X). To this purpose, let us write:

$$\begin{aligned} H(X|Y) - I(Z:X) &= H(X|Y) + H(X|Z) + H(Z|X) - H(X,Z) \\ &= H(X|Z,Y) + I(Z:X|Y) + H(X|Y,Z) + I(X:Y|Z) + H(Z|X,Y) + I(Z:Y|X) \end{aligned}$$

$$-H(X,Z).$$

Now, I remark that

$$H(X|Z,Y) - H(X,Z) = H(Y|X,Z) - H(Z,Y),$$

which allows us to write

$$H(X|Y) - I(Z:X) = H(X|Z,Y) + I(Z:X|Y) + H(Y|X,Z) + I(X:Y|Z) + H(Z|X,Y) + I(Z:Y|X) - H(Z,Y).$$

Since the expected conclusion can be written as

$$-I(Z:Y) = -H(Z,Y) + H(Z|Y) + H(Y|Z),$$

we can reformulate the RHS of the previous equation:

$$H(X|Y) - I(Z:X) = H(X|Z,Y) + I(Z:Y|X) - I(Z:Y).$$

The significance of this equation could be: To say that there is the equivocation X relative to Y and Z and X do not show correlated variability is equivalent to affirm that also Z and Y do not show correlated variability, X shows equivocation on both Z an Y and the latter two share information but not with X. A simpler way to say this is

$$H(X|Y) - I(Z:X) = H(X|Z,Y) - I(X:Y:Z).$$

In other words, the RHS tells us that there is equivocation of X on both Z and Y and X,Y,Z have no common information. Indeed, to affirm that there is information transmission from Y to X but no mutual information between Z and X implies that there is also no mutual information between Z and Y. Again, we can rewrite this inference as an inequality (see Fig. 4).

$$H(X|Y) - I(Z:X) \geq -I(Z:Y).$$

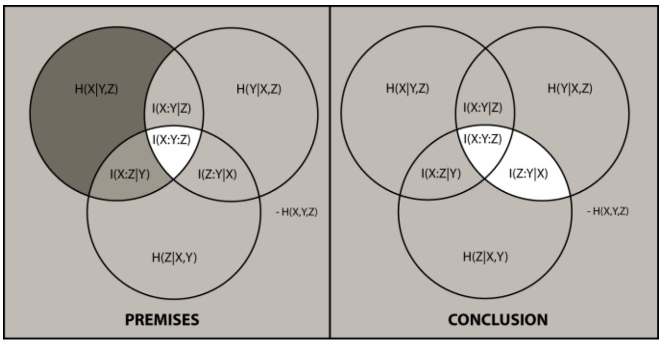

Fig. 4 The inference $H(X|Y) - I(Z:X) \geq -I(Z:Y)$. Note that the region $H(X|Y,Z)$ is counted two times in the premises.

Another classical inference is:

$$\text{If } X \rightarrow \neg Y \text{ and } Z \rightarrow X, \text{ then } Z \rightarrow \neg Y.$$

In this case, we like to obtain the conclusion $-H(Z|Y)$ from the premises $I(X:Y)$ and $-I(Z:X)$. Let us again sum the two premises:

$$I(X:Y) - I(Z:X) = H(X) - H(X|Y) - H(X) + H(X|Z)$$
$$= -H(X|Y) + H(X|Z)$$
$$= -H(X|Y) + H(X,Y) - H(Z|X) - I(X:Y)$$
$$= -I(X:Y) - H(Z|X) + H(Y).$$

Now, since

$$H(Y) = H(Z,Y) - H(Z|Y)$$

and

$$H(Z,Y) = H(Z|X) + I(Z:X) + H(Y|Z),$$

we can write:

$$I(X:Y) - I(Z:X) = -I(X:Y) - H(Z|X) + H(Z|X) + I(Z:X) + H(Y|Z) - H(Z|Y)$$
$$= -I(X:Y) + I(Z:X) + H(Y|Z) - H(Z|Y)$$
$$= -I(X:Y|Z) - I(X:Y:Z) + I(Z:X|Y) + I(X:Y:Z) + H(Y|X,Z) + I(X:Y|Z) - H(Z|Y)$$
$$= I(Z:X|Y) + H(Y|X,Z) - H(Z|Y).$$

The significance of this equation could be: To say that X and Y share information but Z and X do not is equivalent to say that there is no equivocation of Z on Y and both Z and X share information but not with Y and that there is equivocation of Y on both X and Z. The general significance of the derivation is quite simple: To say that there is a mutual information between X and Y but no mutual information between Z and X amounts to say that there can be no information transmission from Y to Z. We can express also this inference as an inequality (see Fig. 5):

$$I(X:Y) - I(Z:X) \geq -H(Z|Y).$$

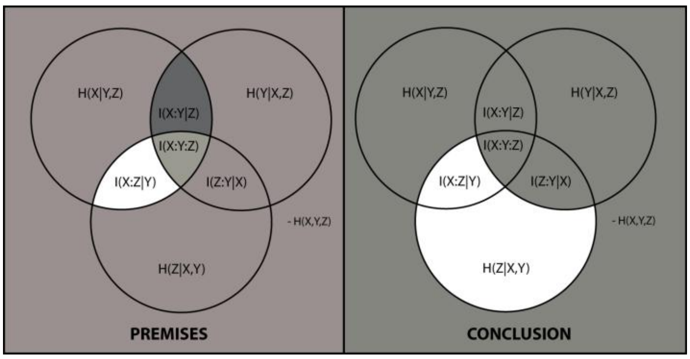

Fig. 5 The inference $I(X:Y) - I(Z:X) \geq -H(Z|Y)$. Note that the region $I(X:Y|Z)$ is counted two times in the premises.

Finally I only briefly present the informational analogue of inference

If X → Y and Z ∧ X, then Z ∧ Y,

which is:

If H(X|Y) and – H(Z|Y) then we have also – H(Z|X).

This inference says that if there is information transmission from Y to X but no transmission from Y to Z, then there is also no information transmission from X to Z (see also Fig. 6).

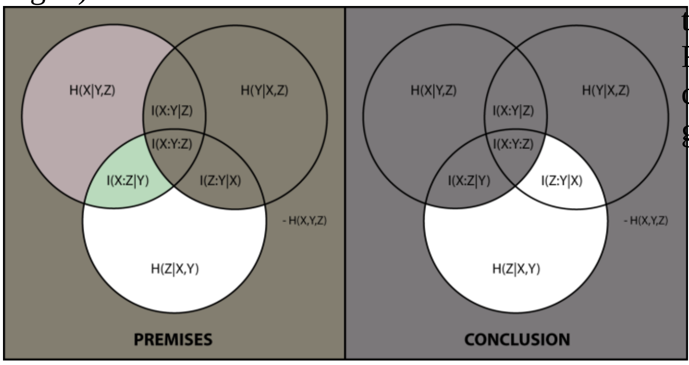

Fig. 6 The inference H(Z|X) – H(Z|Y) ≥ – H(X|Y). Note that the region H(X|Y,Z) is counted two times in the premises.

The general lesson is that if one of the premises is the affirmation or the denial of the existence of shared information, also the conclusion will consist in the affirmation or denial of the existence of shared information. If one of the premises affirms the existence of shared information and the other one denies the existence of another kind of shared information, the conclusion will deny that there information transmission at all. A very easy rule for expressing this generalization is the following. Apart from the first inference and some few which can be derived from it, all other ones involve two times a shared information and one time a conditional entropy, it does not matter whether in the premises or in the conclusion. Let us take the second inference, i.e.

I(X:Y) + H(Z|X) ≥ I(Z:Y)

as paradigmatic. Then we can generated any other kind of inference by moving one of the terms on the LHS or the RHS into the opposite side according to the ordinary rules of inequalities. For instance, by moving the two mutual-information terms we obtain:

H(X|Y) – I(Z:Y) ≥ – I(Z:X),

which is the third inference apart from a substitution of variables. Anyway, also this form is absolutely correct. By moving the conclusion and conditional-entropy term we obtain the fourth inference:

I(X:Y) – I(Z:Y) ≥ – H(Z|X),

apart from a change of variables which however does not affect the soundness of the derivation.

As I have mentioned, the first inference and those derived from it have a different structure. Remark that the change of sign of two conditional-entropy of the first inference generates the fifth inference:

H(X|Y) – H(Z|Y) ≥ – H(Z|X).

We could also write:

H(Z|X) – H(Z|Y) ≥ – H(X|Y),

which is again fully correct.