PUC

ISSN 0103-9741

Monografias em Ciência da Computação
n° 18/11

Semiotic Relations and Proof Methods

Antonio L. Furtado

Departamento de Informática

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO

RUA MARQUÊS DE SÃO VICENTE, 225 - CEP 22453-900

RIO DE JANEIRO - BRASIL

Monografias em Ciência da Computação, No. 18/11 ISSN 0103-9741
Editor: Prof. Carlos José Pereira de Lucena Decemberr, 2011

Semiotic Relations and Proof Methods

Antonio L. Furtado

furtado@inf.puc-rio.br

Abstract: When a direct proof of a statement S seems hard or even impossible to obtain, there may exist another statement (or set of statements) S*, somehow related to S, on the basis of which S can be proved. In order to investigate what options can be used to move from S to S*, four kinds of semiotic relations inspired on the four master tropes of semiotic research are briefly reviewed. Specifically, our syntagmatic, paradigmatic, antithetic and meronymic relations correspond, respectively, to metonymy, metaphor, irony and synecdoche. It is suggested that these four semiotic relations determine the options to move from S to S*, leading to proof by inference, proof by analogy, proof by contradiction, and proof by cases.

Keywords: Semiotic Relations, Rhetorical Tropes, Proof Methods.

Resumo: Quando uma prova direta de uma afirmação S parece difícil, senão impossível de obter, pode existir outra afirmação (ou conjunto de afirmações) S*, de algum modo relacionada com S, com base na qual S pode ser provada. Afim de investigar quais opções podem ser usadas para passar de S a S*, quatro tipos de relações semióticas inspiradas nos quatro tropos mestres pesquisados em semiótica são brevemente revistos. Especificamente, nossas relações sintagmáticas, paradigmáticas, antitéticas e meronímicas correspondem, respectivamente, a metonímia, metáfora, ironia e sinédoque. Sugere-se que estas quatro relações semióticas determinam as opções para a passagem de S a S*, levando a prova por inferência, prova por analogia, prova por contradição, e prova por casos.

Palavras-chave: Relações Semióticas, Tropos Retóricos, Métodos de Prova.

In charge of publications

Rosane Teles Lins Castilho
Assessoria de Biblioteca, Documentação e Informação
PUC-Rio Departamento de Informática
Rua Marquês de São Vicente, 225 - Gávea
22451-900 Rio de Janeiro RJ Brasil
Tel. +55 21 3527-1516 Fax: +55 21 3527-1530
E-mail: bib-di@inf.puc-rio.br

veritas est adæquatio rei et intellectus
St. Thomas Aquinas quoting Isaac Israeli,
Summa Theologica, I, q. 16; a. 2, ad 2.

μηδείς αγεωμέτρητος εισίτω
written over the entrance of Plato's Academy.

1. Introduction

The objective of this paper is to investigate what options one has to move from a statement S that does not seem to be directly provable to some related statement (or set of statements) S*, which could be shown to be true and to imply that S itself must be true. We suggest that there are four basic ways to *move* from S to S*, enabled by what we have categorized as *semiotic relations*. These relations have been drawn from the so-called *four master tropes*, a topic of major interest in the area of semiotic research [Chandler]. It is no coincidence that 'trope' comes from the Greek 'τροποσ' from 'τρεπειν', 'to turn', akin to the notion of *moving* that underlies the present discussion.

Our four semiotic relations, together with their intuitive meaning, associated logical connectives, and corresponding tropes are listed below:

relation	**meaning**	**connective**	**trope**
syntagmatic	contiguity, sequence	and	metonymy
paradigmatic	similarity, alternatives	or	metaphor
antithetic	opposition, negation	not	irony
meronymic	hierarchy, details	part-of	synecdoche

These four tropes were characterized as fundamental, among the numerous rhetorical tropes popular in Greco-Roman antiquity [Quintilian], first in the XVIth century [Ramus] and again in the XVIIIth century [Vico]. In modern times they were revived in a seminal study [Burke]. Their universality has been repeatedly emphasized, with the indication that they may constitute "a system, indeed *the* system, by which the mind comes to grasp the world conceptually in language" [Culler]. Applications to several topics have been reported, for instance to worldviews and ideologies [White] and, in our own work, to digital interactive composition of story-plots [Ciarlini-2].

With respect to the names we assigned to the proposed semiotic relations, the terms 'syntagmatic' and 'paradigmatic' correspond to the two *linguistic axes* of [Saussure]. The term 'antithetic' reflects the fact that, according to [Burke], the perspective induced by the irony trope is associated with *dialectic*, which features *antithesis* as a key concept expressing negation. Finally, in [Winston], wherein six types of part-of links are distinguished, one reads: "We will refer to relationships that can be expressed with the term 'part' in the above frames as 'meronymic' relations after the Greek 'meros' for part".

Informally speaking, the preferred strategy to apply when S is not directly provable is to look for other statements, in the same domain, from which S could be deduced. If no clues are offered by the original domain, one may try to locate an analogue to S in another domain, which may be more amenable to a successful treatment. Especially when S is an assertion that something cannot hold, an often convenient option is to assume the contrary

and then show that the assumption leads to an inconsistency. Finally, if a general proof of S is unfeasible, one may break down the problem into an exhaustive list of cases, to be handled separately one by one. The main thrust of this paper is that these four options to prove a statement S in connection with a statement (or set of statements) S* – namely proof by inference, proof by analogy, proof by contradiction, and proof by cases – are determined by the four semiotic relations mentioned before.

The paper is organized as follows. Section 2 deals with the application of the four proof methods, relying on examples to illustrate the connection of each method with the respective enabling semiotic relation. Sections 3 and 4 discuss a few problems arising from the complementary processes of finding a proof and expressing it convincingly. Section 5 contains concluding remarks.

2. Applying the semiotic relations

Certain statements are obviously true by definition, or are verifiable through a simple inspection. Direct proof that something exists merely requires to exhibit an instance, even though some work may be required to *construct* it, as with the statement that there exist irrational numbers a and b such that a^b is rational — which is usually evidenced by producing some series of equalities (which, curiously, can only be checked symbolically since the first two cannot be computed over the domain Q of rational numbers):

$$a = \sqrt{2}\,,\ b = \log_2 9,\ a^b = 3$$

but it often happens that no such direct proof is feasible.

To prove a statement S in such circumstances, we can move to some other statement (or set of statements) S*, which must be preliminarily shown to be linked to S by a semantic relation, and then try, recursively, to prove S*. There are (at least) four such "moves", each of them corresponding to one of the rhetorical master tropes.

We say that a *syntagmatic relation* holds between S and S* if S is a logical consequence of S*. The associated trope is *metonymy*. The resulting method is *proof by inference*.

A *paradigmatic relation* holds between S and S* if after suitable mappings the relevant features of S can be converted into features of S*. The associated trope is *metaphor*. The resulting method is *proof by analogy*.

An *antithetic relation* holds between S and S* if S* could be shown to be inconsistent if ~S were true. The associated trope is *irony*. The resulting method is *proof by contradiction* (also called *reductio ad absurdum*).

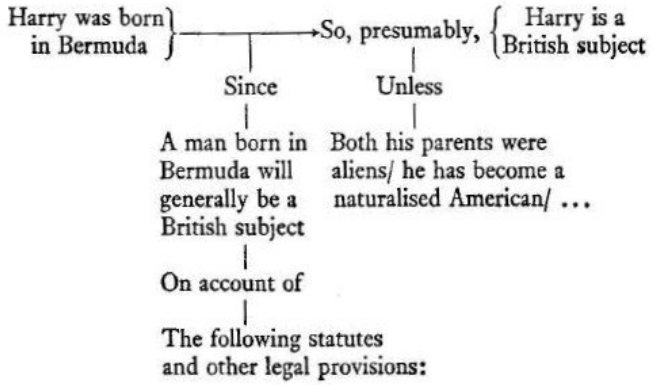
A *meronymic relation* holds between S and S* if S* is a set of statements into which S can be decomposed exhaustively. The associated trope is *synecdoche*. The resulting method is *proof by cases*.

2.1. Proof by inference

Example 1: "Socrates is mortal". This time-honoured example recognizes that mortality is a human condition, as expressed by the rule: $\forall x\ (\text{human}(x) \rightarrow \text{mortal}(x))$. Since Socrates is known as a human being, the rule applies and the statement follows as a consequence.

Example 2: "Harry, who was born in Bermuda, is a British subject". Stephen Toulmin has argued convincingly that the conventional syllogism structure must be expanded to deal

with reasoning in the domain of justice [Toulmin]. So it is not enough to consider what he calls the *data* (Harry was born in Bermuda), the *claim* (Harry is a British subject) and the *warrant* (a man born in Bermuda is a British subject). To these three elements he adds a modality or, to use his own terms, a *qualifier* (presumably), given that the rule admits exceptions that constitute a possible *rebuttal* (unless both his parents were aliens, or he has become an American citizen, or ...). But, even more characteristic of legal argument, is the *warrant* (statutes and other legal provisions); indeed the judicial system is governed by positive law (as opposed to natural law), which must have been officially established, and which may differ for different countries (e.g. notice among the exceptions the prevalence of *ius sanguinis* over *ius soli*, in contrast to Brazilian norms). Toulmin's scheme can best be comprehended under the form of a diagram:



To Toulmin's remarks one must add that the existence of what he calls the 'data' may not be recognized in justice if not officially registered as well (e.g. via a birth certificate). In database terminology this corresponds to the 'closed world assumption' [Casanova]. Also recall the assumption in criminal law that a defendant is judged 'not guilty' (thus avoiding the term 'innocent') unless proved responsible for the alleged offense, which in turn must have been exactly specified by a previous law (*nullum crimen sine prævia lege pœnale*). All these considerations bring to mind the principle of 'negation as finite failure', also explained in [Casanova] — ~S holds whenever S neither resides in the database nor can be derived from the stored data and the rules that have been explicitly defined.

2.2. Proof by analogy

Example 3: "There can be no efficient algorithm to determine the minimum number of schedules for tests of a group of students, so that no student will miss a test because its schedule coincides with that of some other course in which the student is enrolled". Establishing non-conflicting schedules has an analogue in graph theory, if courses are mapped into nodes, and the fact that two courses c_1 and c_2 have one or more students in common is mapped into an edge connecting the nodes labeled c_1 and c_2. Then the original problem is converted into the problem of finding the chromatic number of a graph, which has been shown to be np-complete (and hence of intractable computational complexity) [Karp].

Example 4: "A Buddhist monk begins at dawn one day walking up a mountain, reaches the top at sunset, meditates at the top overnight until, at dawn, he begins to walk back to the

foot of the mountain, which he reaches at sunset. Make no assumptions about his starting or stopping or about his pace during the trips. Is there a place on the path which the monk occupies at the same hour of the day on the two trips?" The solution given in [Turner] involves a close analogue for which, rather surprisingly, no mathematical treatment is required, and in fact the answer is immediately evident. The mappings involve *blending* the scene of the monk climbing with that of his return. The action takes place in a single day, with the monk and his double walking in opposite directions – and so inevitably meeting himself at some intermediate place.

2.3. Proof by contradiction

Example 5: "There exists an infinity of prime numbers". Assume, on the contrary, that the primes form a finite set L = $\{p_1, p_2, ..., p_n\}$. The proof dates from ancient times [Euclid]. Taking all the primes in L, one can obtain: $P = p_1 1 \times p_2 \times ... \times p_n + 1$. The number P calculated in this way is either a new prime, in which case we already have a contradiction, or a multiple decomposable into prime factors: $P = q_1 \times q_2 \times ... \times q_m$. But the q_i should be different from the prime numbers in L, since P is not divisible by any of them (the division would always yield 1 as remainder). So the q_i would be new primes, again contradicting the ~S assumption.

2.4. Proof by cases

Example 6: "The absolute value of the sum of two non-zero numbers is less than or equal to the sum of their absolute values". In formal notation: $|a + b| \leq |a| + |b|$. There seem two be four cases, which can be easily treated by elementary arithmetic:
case 1. if a and b are positive, the left side is equal to the right side;
case 2. if a is positive and b negative, the left side is less than the right side;
case 3. if a is negative and b positive, the left side is less than the right side;
case 4. if both a and b are negative, the left side is equal to the right side.

Actually the four cases are reducible to three, by collapsing cases 2 and 3 in view of the commutative property of addition.

Example 7: "The sum of all natural numbers from 0 to n is equal to $n \times (n + 1) / 2$". To show case by case that this holds for any value of n would lead to an infinite process. Fortunately, thanks to a technique known as finite induction, the problem can be reduced to the following cases:
case 1. for $n = 0$, the result of computing the formula is 0, which is obviously correct;
case 2. assume that for $n = i$ the formula works correctly, i.e.: $0 + 1 + ... i = i \times (i + 1) / 2$;
case 3. for $n = i + 1$, it must be shown that the formula yields $(i + 1) \times ((i + 1) + 1)/2$. This last case, called the induction step, can be established by using the assumption for $n = i$ and then performing a series of simple algebraic transformations: $(0 + 1 + ... + i) + (i + 1) = i \times (i + 1) / 2 + (i + 1) = (i \times (i + 1) + 2 \times (i + 1))/2 = (i + 1) \times (i = 2) / 2 = (i + 1) \times ((i + 1) + 1)/2$.

Example 8: "Four colours are enough to colour a geographical map so that no two adjacent political units have the same colour". This is the so-called four colours conjecture, which defeated the attempts of many researchers for a long time, until being finally established as a proven theorem by two researchers working together in 1976 [Appel]. They first managed to identify an exhaustive list of cases, corresponding to 1936 "irreducible

configurations". To handle such an overwhelming number of cases, they were forced to appeal to computer support. Subsequent efforts were made to reduce this number, but to our knowledge it still remains quite large.

3. A preliminary step

Finding the proof to a statement S and expressing the proof are more often than not two sharply different processes. In particular, to find a proof by inference, a person must start in a backward direction by applying a reasoning strategy called *abduction* [Peirce]. Its purpose is to search some *hypothesis* S* that may be used next to justify S. To perform abduction, one assumes that S holds and then looks for some existing rule of the form S* → S relating S and S*. In a sense, abduction involves traversing the rule in a right-to-left direction, inversely therefore to how we handle *deduction*, on which the process of expressing a proof by inference is based. Recall that medical doctors are relying on abduction while they try to trace back the observed symptoms to diseases that may have caused them, and that differential diagnosis becomes necessary if more than one disease is hypothesized.

The rules themselves should have been formulated beforehand, typically by *induction*, i.e. by observing that S occurs whenever S* does, and that this can be attributed to logical implication or at the very least to probabilistic evidence, rather than to fortuitous coincidence (the *post hoc ergo propter hoc* fallacy). After the advent of computers, *data mining* runs [Han] (involving statistical correlation and several other techniques) began to be routinely performed over large data repositories to discover such useful rules.

For proof by analogy, the preliminary search is even trickier. One must be able to look for analogues in domains other than that of the statement on hand, and abstract the essentials from knowledge expressed in a widely distinct formalism. Perhaps the required competence hinges on the access to a repertoire of well-structured and well-indexed mental *forms*, either characterized as ideas [Plato], or archetypes [Jung], or basic metaphors [Lakoff], or scripts [Schank], etc. Whether they are inborn or acquired is the topic of endless debate.

Children are very early stimulated in school to answer analogy questions in the form "A is to B as C is to *what*?". Indeed proportionality is a helpful criterion to formulate the mappings between the features of the original statement and the candidate analogue. A modern discipline, *case-based reasoning* [Kolodner], attempts to automate the search for analogues, ideally working on some rich computer-accessible library. One technique to construct such libraries involves extracting patterns from the observed detailed descriptions through *most specific generalization* [Ciarlini-1, Furtado].

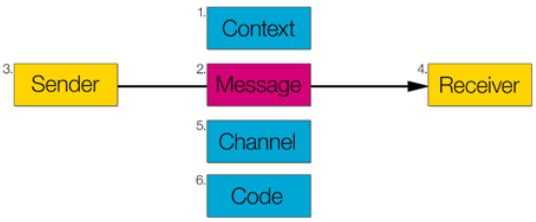
For proof by contradiction, determining S* can sometimes be almost immediate. In example 5, in opposition to the notion of an infinity of numbers with the property of being prime, one promptly perceives, without leaving the original domain, that a contrary notion is that the existing primes form a finite set – and from that follows the idea of using the members of this set to construct the statement that will lead to a contradiction. But other problems are not so simple. We shall look at the famous Fermat's Last Theorem (proposed in 1637, just before his death), which was expressed by a simple algebraic equation, but was proved by contradiction much later [Wiles], using a rather advanced geometry result about the modularity of elliptic curves. So it combines analogy with contradiction (plus long series of inferences) and, on top of all that, it illustrates how crucial it is to *restrict* the

cases to be covered in a proof by cases to precisely what is required to prove the statement – it became eventually clear that it suffices to consider *semistable* elliptic curves. Once again as in example 8, I shall only provide a very brief and very informal note, due to my absolute lack of familiarity with this level of mathematics.

Example 9: "No three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than two". Thanks to the effort of a number of researchers from 1637 to 1995 (when Wiles's paper was published), it was proved, case by case, that any solution to this deceptively simple equation could be used to generate a non-modular semistable elliptic curve, whereas it was also proved that all such elliptic curves had to be modular – a contradiction that implies that there can be no solutions to the equation, thus finally transforming the conjecture into a theorem.

4. Choosing how to express a proof

Let us now turn to the second process mentioned at the beginning of the previous section, namely, having succeeded in proving that a sentence is true by a judicious application of methods such as those exemplified in section 2, how to suitably express the demonstration to other people. To realize what is involved it is convenient to view this as a *communication process*, requiring our attention to at least the six items contained in the diagram below [Jakobson]:



In words: the researcher (sender) who devised the proof formulates the demonstration (message) in some formal or informal language (code) and passes it through some medium (channel) to an interested person (receiver) who should be able to understand it. The cultural environment prevailing at a given place and time (context) imposes conditions that may exert a favourable or unfavourable influence on the outcome of the process.

Of course the sender must make sure that the proof is correct with respect to both contents and form, but the effort can ultimately succeed only if the receiver can decode the demonstration to the point of effectively learning it and taking maximum advantage from the new knowledge thus acquired. The choice of a formalism is sometimes crucial to this end. For instance, the use of finite induction for example 7 above is considered in [Chateaubriand] as inappropriate for teaching to beginning students. Even if the algebraic manipulations can be followed by them, the stepwise argument would not "relate meaningfully" to the students, whereas a more intuitive presentation relying on a pictorial sketch would have a better chance of eliciting a reaction of "dawning understanding".

More generally, the correct connection from sender to message in Jakobson's communication scheme is just one prerequisite of the process. It corresponds to the adequacy of the *signifier* to the *signified* in [Saussure]. But communication must reach its

final destination, the receiver, bringing to mind the three-element view – *object*, *representamen*, *interpretant* – advocated in [Peirce]. It is through this path that the human intellect can, although incompletely and imperfectly, grasp a glimpse of the real, as in the epigraph that opens this paper.

Let us examine two kinds of misunderstanding that may result from an undue application of a simple principle: "if a statement S involving a is true and a = b, the substitution of b for a yields a statement that is also true".

First, take the true statement "the expression 3 + 1 + 2 contains three terms", and note that 3 + 1 + 2 = 5 + 1. By substitution, "the expression 5 + 1 contains three terms" should be true, but it is patently false. Clearly the substitution could not have been done, since this particular statement is an argument *de dicto*, whereas the value equality is a *de re* consideration. Or we might say, perhaps, that the statement referred to a signifier and the comparison to a signified, in Saussure's terminology.

The second case is a little less trivial. Suppose the statement "Gottlob believes that Venus is a planet" is true, and consider the relatively well-known equality Venus = Evening Star. The substitution, giving "Gottlob believes that the Evening Star is a planet" is not necessarily true, however. Even if Gottlob is aware of the equality, he may have never taken the trouble to perform the substitution, and therefore the maximum that we could say in this case, introducing a modality, is that "Gottlob *possibly* believes that the Evening Star is a planet". The full-fledged substitution would only be warranted if both the equality and the substitution took place in Gottlob's head, i.e. at the level of Peirce's interpretant.

5. Concluding remarks

It must be stressed that the over-simplified semiotic-based model proposed in this paper is far from complete, as all models are by definition. Much work remains to be done, which should equally be said about heuristics to present demonstrations with enough intuitive appeal and clarity. Theorems such as the four-colours theorem (mentioned in example 8) and Fermat's last theorem (example 9) still come in extremely lengthy reports and require proficiency in a variety of domains.

In our times many such examples can be listed in which we are compelled to accept some results on the authority of a few top specialists. Occasionally they try, albeit with doubtful results, to enlighten the non-initiated. If you want to understand Fermat's Last Theorem, have a look at the honest attempt in [Faltings], who a little bit optimistically declares: "I have tried to present the basic ideas to a wider mathematical audience, and in the process I have skipped over certain details, which are in my opinion not so much of interest to the nonspecialist".

In conclusion, it is the present author's duty to confess his own perplexity vis-a-vis the arcanes of logical and mathematical formalisms, and, above all, the apparently unsystematic flashes of intuition that guide researchers to see how to solve what would have seemed unsolvable. Obedient to the lemma in epigraph, he must humbly stand by the entrance of Plato's Academy.

References

[Appel] K. Appel, W. Haken. "Every planar map is four-colorable". *Bulletin of the American Mathematical Society*, 82, 5, 1976.

[Burke] K. Burke. *A Grammar of Motives*. Berkeley: University of California Press, 1969.

[Casanova] M.A. Casanova, F.A.C. Giorno, A.L. Furtado. *Programação em Lógica e a Linguagem Prolog*. São Paulo: Edgard Blücher, 1987.

[Ciarlini-1] A.E.M. Ciarlini, A.L. Furtado. "Constructing libraries of typical plans". *Proc. 13th Conference on Advanced Information Systems Engineering*, 2001.

[Ciarlini-2] A.E.M. Ciarlini, S.D.J. Barbosa, M.A. Casanova, A.L. Furtado. "Event relations in plan-based plot composition". *Computers in Entertainment*, 7, 4, 2009.

[Chandler] D. Chandler. *Semiotics: the Basics*. London: Routledge, 2002.

[Chateaubriand] O. Chateaubriand Filho. *Logical Forms*. Campinas: UNICAMP, 2001.

[Culler] J. Culler. *The Pursuit of Signs: Semiotics, Literature, Deconstruction*. London: Routledge, 1981.

[Euclid] Euclid. T*he Thirteen Books of the Elements*. T.L. Heath (trans.). Mineola: Dover Publications, 1956.

[Faltings] G. Faltings. "The Proof of Fermat's Last Theorem by R. Taylor and A.Wiles". *Notices of the American Mathematical Society*, 42, 7, 1995.

[Furtado] A.L. Furtado. "Analogy by generalization and the quest of the grail**"**. *ACM Sigplan Notices*, 27, 1, 1992.

[Han] J. Han, M. Kamber, J. Pei. *Data Mining: Concepts and Techniques*. San Mateo: Morgan Kaufmann Publishers, 2011.

[Jakobson] R. Jakobson. *Selected Writings*. Amsterdam: Mouton de Gruyter, 1982.

[Jung] C.G. Jung. *The Archetypes and the Collective Unconscious*. R.F.C. Hull (trans.). Princeton: Princeton University Press, 1981.

[Karp] R.M. Karp. "Reducibility Among Combinatorial Problems". In R. E. Miller and J. W. Thatcher (eds.). *Complexity of Computer Computations*. New York: Plenum, 1972.

[Kolodner] Kolodner, J.L. *Case-based Reasoning*. San Mateo: Morgan Kaufmann Publishers, 1993.

[Lakoff] G. Lakoff, M. Johnson. *Metaphors We Live By*. Chicago: University of Chicago Press, 2003.

[Peirce] C.S. Peirce. *Writings of Charles S. Peirce: a Chronological Edition*. N. Houser (ed.). Bloomington: Indiana University Press, 1998.

[Plato] Plato. *Cratylus, Parmenides, Greater Hippias, Lesser Hippias*. H.N. Fowler (trans.). Loeb Classical Library. Cambridge: Harvard University Press, 1926.

[Ramus] P. Ramus. *Rhetoricae Distinctiones in Quintilianum*. J.J. Murphy (ed.), C. Newlands (trans.). Carbondale: Southern Illinois University, 2010.

[Saussure] F. Saussure. *Cours de Linguistique Générale*. C. Bally, A. Sechehaye, A. Riedlinger (eds.). Paris: Payot, 1995.

[Schank] R.C. Schank, R.P. Abelson. *Scripts, Plans Goals, and Understanding*. New York: Psychology Press, 1977.

[Toulmin] S. Toulmin. *The Uses of Argument*. Cambridge: Cambrige University Press, 2003.

[Turner] M. Turner. *Blending and Conceptual Integration - the Riddle of the Buddhist Mon*k. http://markturner.org/blending.html.

[Vico] G. Vico. *The New Science*. T.G. Bergin, M.H. Finch (trans.). Ithaca: Cornell University Press, 1968.

[White] H. White. *Metahistory: the Historical Imagination in Nineteenth-Century Europe*. Baltimore: John Hopkins University Press, 1973.

[Wiles] A. Wiles. "Modular elliptic curves and Fermat's Last Theorem". A*nnals of Mathematics,* 142, 1995.

[Winston] M.E. Winston, R. Chaffin., D. Herrmann. (1987). "A taxonomy of part-whole relations". *Cognitive Science*, 11, 4, 1987.