Document extract

Title of chapter/article	On the analysis of indirect proofs: Contradiction and contraposition
Author(s)	Nicolas Jourdan & Oleksiy Yevdokimov
Copyright owner	The Australian Association of Mathematics Teachers Inc.
Published in	Australian Senior Mathematics Journal vol. 30 no. 1
Year of publication	2016
Page range	55–64
ISBN/ISSN	0819-4564
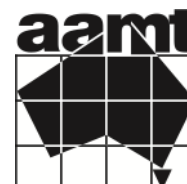
AAMT—supporting and enhancing the work of teachers

ASMJ

Contents

Refereeing procedure

All articles are subject to peer review. The following procedure is undertaken:

1. On receiving a paper, the editors decide if the paper is within the province of the journal, which is "the teaching and learning of mathematics in Years 11 and 12 of secondary school and the early years of tertiary education." The author(s) of the paper is notified and appropriately advised if not.

2. A potentially publishable paper is sent 'blind' to two referees with expertise related to the paper; the referees will usually be selected from the Editorial Panel and practising teachers and academics.

3. The Editors act in line with the referee reports in one of the following ways:
   (i) accept the paper for publishing 'as is';
   (ii) reject the paper outright, in which case the author(s) is notified;
   (iii) inform the author(s) of changes which need to be made before the paper is accepted for publication;
   (iv) make minor changes without prior reference to the author(s).

On the analysis of indirect proofs: Contradiction and contraposition

Nicolas Jourdan & Oleksiy Yevdokimov
University of Southern Queensland
nicolas.jourdan@usq.edu.au
oleksiy.yevdokimov@usq.edu.au

Proof by contradiction is a very powerful mathematical technique. Indeed, remarkable results such as the fundamental theorem of arithmetic can be proved by contradiction (e.g., Grossman, 2009, p. 248). This method of proof is also one of the oldest types of proof early Greek mathematicians developed. More than two millennia ago two of the most famous results in mathematics: The irrationality of $\sqrt{2}$ (Heath, 1921, p. 155), and the infinitude of prime numbers (Euclid, Elements IX, 20) were obtained through reasoning by contradiction. This method of proof was so well established in Greek mathematics that many of Euclid's theorems and most of Archimedes' important results were proved by contradiction.

In the 17th century, proofs by contradiction became the focus of attention of philosophers and mathematicians, and the status and dignity of this method of proof came into question (Mancosu, 1991, p. 15). The debate centred around the traditional Aristotelian position that only causality could be the base of true scientific knowledge. In particular, according to this traditional position, a mathematical proof must proceed from the cause to the effect. Starting from false assumptions a proof by contradiction could not reveal the cause. As Mancosu (1996, p. 26) writes: "There was thus a consensus on the part of these scholars that proofs by contradiction were inferior to direct proofs on account of their lack of causality."

More recently, in the 20th century, the intuitionists went further and came to regard proof by contradiction as an invalid method of reasoning. In the classical approach the existence of an object can be proved by refuting its non-existence. To the intuitionist this is not acceptable. Led by the Dutch philosopher and mathematician L. E. J. Brouwer the intuitionists reject the law of excluded middle and only accept constructive proofs as valid proofs.

Despite all its past criticism and even rejection by some members of the mathematical community, the majority of today's mathematicians would agree with Rivaltus' position: "Proofs by contradiction have the same dignity as direct proofs because, even if they do not give us the cause of why a certain

affection is to be predicated on the subject, they nonetheless give us a reason by which we know that a state of affairs holds" (cited in Mancosu, 1991, p. 34).

Nowadays, proof has been assigned a more prominent place in the mathematics curriculum at all levels. As Hanna and de Villiers (2008, p. 329) write: "The recent National Council of Teachers of Mathematics (NCTM) Principles and Standards document and several other mathematics curricular documents have elevated the status of proof in school mathematics in several educational jurisdictions around the world."

This renewed emphasis on proof and proving in mathematics education means that "mathematics educators face a significant task in getting students to understand the roles of reasoning and proving in mathematics" (Hanna & de Villiers, 2008, p. 329). More specifically, Hanna and de Villiers are challenging educators "to foster the use of proof as a method to certify not only that something is true, but also why it is true." (p. 330). The aim of the paper is to describe a general model of proof by contradiction. The misconceptions that seem to exist between proof by contradiction and proof by contraposition are clarified through the examination of their similarities and differences. More generally we shed some light on the specific details and peculiarities of the indirect proof structure, some of which are often left unattended whilst studying and practising proof techniques. We expect the paper to be of interest to undergraduate students and their university teachers as well as anyone interested in indirect proofs.

Description of a general model

We now investigate the theoretical foundations of proof by contradiction. This method of proof is an application of the rule of logical reasoning known as *modus tollens*. According to this rule, a proposition is proved by showing that its falseness leads to unacceptable consequences. Wishing to prove a statement p, one first assumes its negation $\neg p$ to be true. One then goes on to show that $\neg p$ implies q, where q is already known to be false. By this argument, $\neg p$ must be false and it follows logically that its negation, the original proposition p must be true. Goubault-Larrecq and Mackie (1997, p. 4) give a simple example to illustrate modus tollens. Suppose we know the following two facts to be true: "If it is raining then I am inside", and "I am outside". From these two facts we can readily deduce that it is not raining. More formally, modus tollens can be stated as:

1. $p \rightarrow q$ (if p then q)
2. $\neg q$ (not q)
3. $\therefore \neg p$

For completeness we briefly mention here another commonly used rule of reasoning known as *modus ponens*, which can be formally stated as:

1. $p \rightarrow q$ (if p then q)
2. p
3. $\therefore q$

Such rules of reasoning are not part of mathematics itself. Rather, they stand above the subject matter to which they are applied.

To reiterate, the aim of a proof by contradiction is essentially to contradict one of our assumptions. If the aim is achieved then, as a consequence of modus tollens, the original statement must be true. In Figure 1 below we propose a general model for proof by contradiction.
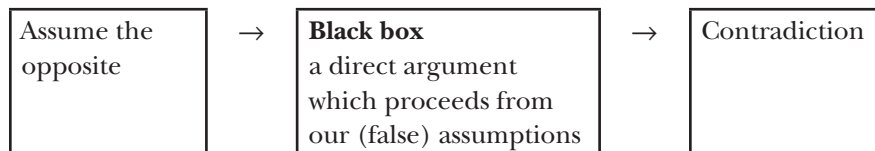
| Assume the opposite | $\rightarrow$ | **Black box**
 a direct argument which proceeds from our (false) assumptions | $\rightarrow$ | Contradiction |

Figure 1. Model for proof by contradiction.

The very first step—assuming the opposite—can, in many cases, be a stumbling block for students. In his 1979 study, Williams (cited in Thompson, 1996) presented students with a number of items dealing with indirect proof. Asked to evaluate a proof that $1 \neq 0$, many students did not view the argument as valid, owing to the fact that the initial assumption $1 = 0$ is false. Obviously this difficulty considerably hindered students' ability to use indirect proof effectively as many students appeared unwilling to argue from an hypothesis they saw as untrue (p. 478).

In general, a mathematical statement may contain any number of logical connectives—*and, or, if-then*—as well as the two quantifiers—*for all, there exists.* Many researchers (Epp, 1998; Lin et al., 2003, Thompson, 1996) report that, formulating the opposite of such statements is a difficult task for most students. As Epp (1998, p. 711) states: "One of the most serious difficulties that students have in actually constructing proofs by contradiction on their own is in supposing the wrong thing". This first step is indeed crucial. Thompson (1996, p. 476) adds, "If students have difficulty writing a negation, they have difficulties at the onset".

The 'black box' is truly the heart of the proof. It is usually a direct argument which proceeds from our (false) assumptions. What is in the box is utterly context dependent. Even for the simplest cases, the logical steps to be taken may be far from obvious to the novice and require much insight. As Barnard and Tall (1997, p. 42) explain: "Mathematical proof introduces a form of linkage different from the familiar routines of elementary arithmetic and algebra. In addition to carrying out sequential procedures in which each action cues the next, mathematical proof often requires the synthesis of several cognitive links to derive a new synthetic connection."

Their investigation into students' difficulties in proving the irrationality of the number $\sqrt{2}$ found that none of the students new to the proof were able to spontaneously link the algebraic statement $a^2 = 2b^2$ to the verbal representation "a^2 is even" (p. 44).

In a proof by contradiction, the aim is not always clear. We do want to arrive at a contradiction, but where is that contradiction to be found? Certainly, contradicting one of our assumptions will achieve the desired aim but the contradiction is not always this apparent. Indeed, rather than contradicting our assumption, the contradiction may take the form of a mathematical fact we know to be false or it may even emerge out of our own construction produced during the proof.

Proof by contradiction versus proof by contraposition

This part of the paper explores the differences and similarities that exist between proof by contraposition and proof by contradiction. The literature refers to both methods as indirect methods of proof. We will keep with this terminology in the paper. Both methods are closely related. In fact, the two methods are so closely related that they are sometime confused and so their differences and similarities are worthwhile exploring and clarifying. For example, Antonini and Mariotti (2008, p. 402) write: "In Italy, in general, mathematicians and teachers call 'proof by contradiction' … both proof by contraposition and proof by contradiction." This confused state of affairs extends well beyond Italy. In the United States, many textbooks fail to clearly distinguish between these two types of proof. Epp's *Discrete Mathematics with Applications* (2011) is an exception and she contends that proof by contraposition applies only to "a specific class of statements—those that are universal and conditional" (p. 204).

To proceed further we need to provide more details on both types of statements. A universal statement is a statement about all the elements of a given set. "All humans are mortal" is an example of a universal statement. A conditional statement is a statement of the form "if p then q", with the two propositions p and q referred to as the hypothesis and the conclusion respectively. In logic conditional statements are known as implications and may be written as "p implies q" ($p \rightarrow q$ in symbols).

Proof by contraposition

Proof by contraposition rests on the fact that an implication $p \rightarrow q$ and its contrapositive $\neg p \rightarrow \neg q$ (not q implies not p) are two logically equivalent statements. In this method of proof, there is *no contradiction to be found.* Rather our aim is to show, usually through a direct argument, that the contrapositive statement is true. By logical equivalence this automatically assures us that the implication is also true. In a proof by contraposition both the starting point and the aim are clear: assume that $\neg q$ is true and show that it logically leads to $\neg p$. To illustrate, below is an example of a proof by contraposition.

Example 1

Let x be an integer. Prove that if x^2 is even, then so is x.

Proof 1

Formally the statement can be written as

$$\forall x \in \mathbb{Z} \;\; p \to q$$

where p and q are defined as "x^2 is even" and "x is even" respectively. Negating the two propositions, the statement we want to prove has the form

$$\forall x \in \mathbb{Z} \;\; \neg p \to \neg q$$

where $\neg p$ and $\neg q$ are now "x^2 is odd" and "x is odd" respectively. Thus, we are trying to show that, given any odd integer, its square is also odd. By definition of an odd number our starting point is therefore $x = 2k + 1$, $k \in \mathbb{Z}$ and we proceed this way:

$$x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$
$$x^2 = 2n + 1,\, n \in \mathbb{Z}$$

We have proved that the square of an odd number is odd. In fact, by logical equivalence we have also proved Example 1. We note that Proof 1 can be regarded as a special case of the more general statement that the product of two odd numbers is odd.

Proof by contradiction

We now turn our attention to the other method, the proof by contradiction. As previously stated, in general, to prove a statement by contradiction, we assume that statement to be false and we show that the logical consequences of our assumptions lead to a contradiction or an impossibility. For example, to prove that there is an infinite number of primes we assume from the onset that number to be finite. Now, we are in a position to examine the main difference between the two methods of proof. In the context of implications a proof by contradiction does not simply assume the conclusion to be false. Rather it *assumes the entire statement to be false*. Negating the entire statement has two consequences:

1. The universal statement becomes an existential statement.
2. The conditional statement becomes a conjunction. In particular, the negation of $p \to q$ is the conjunction $p \wedge \neg q$ (p and not q).

The logical steps shown below provide a justification for the logical equivalence between $\neg(p \to q)$ and $p \wedge \neg q$.

$$\begin{aligned} \neg(p \to q) &\equiv \neg(\neg p \vee q) && \text{implication law} \\ &\equiv \neg\neg p \wedge \neg q && \text{de Morgan's law} \\ &\equiv p \wedge \neg q && \text{double negation law} \end{aligned}$$

To illustrate the difference between the two methods we revisit Example 1 here. We prove by contradiction that for any integer x if x^2 is even then so is x. As explained previously, Example 1 has the form

$$\forall x \in \mathbb{Z} \quad p \to q$$

where p and q are defined as "x^2 is even" and "x is even" respectively. Now we need to assume both p and $\neg q$ to be true as our starting point. This means that we assume both "x is odd" and "x^2 is even" to be true. Formally, the statement we prove can be seen as

$$\exists x \in : p \wedge \neg q \, \text{lead to a contradiction.}$$

Essentially we are trying to show that we cannot find an odd integer whose square is even and our starting point can now be any of the above two assumptions. Choosing "x is odd" we proceed along the same lines as the proof by contraposition.

$$x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$
$$x^2 = 2n + 1, \quad n \in \mathbb{Z}$$

The result "x^2 is odd" contradicts the other assumption "x^2 is even". This completes the proof. We note, whilst it may be possible to start the proof with the assumption "x^2 is even", that approach will change the proof to the direct mode, which is not considered in the paper. According to Epp (2011), "…any statement that can be proved by contraposition can be proved by contradiction. But the converse is not true. Statements such as '$\sqrt{2}$ is irrational' can be proved by contradiction but not by contraposition" (p. 204).

Indeed, "$\sqrt{2}$ is irrational" is a single proposition which cannot be written as a conditional statement since such statements require at least two propositions. Some conditional statements may be proved by contradiction but not by contraposition. This is especially the case when the hypothesis contains more than one proposition. Consider for instance the following example.

Example 2
Let a, b and c be three integers. Prove that if c divides $a + c$ but c does not divide a then c does not divide b.

Proof 2
Symbolically, the statement can be written as

$$\forall (a,b,c) \in \mathbb{Z}^3 \quad (c \mid a+b) \wedge (c \nmid a) \to c \nmid b$$

A proof by contradiction assumes the following three propositions to be true.

$$
\begin{array}{ccccc}
p_1 & & p_2 & & \neg q \\
\boxed{c \mid a+b} & \text{and} & \boxed{c \nmid a} & \text{and} & \boxed{c \mid b}
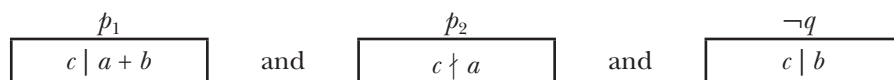\end{array}
$$

Figure 2

Schematically, the proof can be seen as

$$\exists (a,b,c) \in \mathbb{Z}^3 : p_1 \wedge p_2 \wedge \neg q \, \text{lead to a contradiction.}$$

We now show that, working from the first and third propositions, namely p_1 and $\neg q$, a few steps lead to a contradiction. Indeed, the first proposition means $a + b = k_1 c$, the third $b = k_2 c$ with $k_1, k_2 \in \mathbb{Z}$. It follows by substitution

$$a + k_2 c = k_1 c$$
$$a = (k_1 - k_2)c$$
$$a = k_3 c \text{ where } k_3 = k_1 - k_2$$

The difference of two integers is an integer thus $k_3 \in \mathbb{Z}$, and we have shown that c divides a, contradicting the second proposition p_2. The proof is complete.

In fact, an attempt at a proof by contraposition quickly leads to an impasse since we only have a single assumption to work with—namely c divides b. Knowing nothing of the divisibility of a (or $a + b$) by c, no further progress is possible.

Further examples of proof by contradiction

Besides number theory proof by contradiction may be applied in many areas including geometry, linear algebra and calculus. As previously mentioned, the contradiction we are looking for may be on our original assumption or it may arise from our own construction produced during the proof. The calculus example below falls into the latter category, where the constructed derivative function cannot be both positive and equal to zero.

Example 3
Prove that the function $f(x) = 3x^5 + 2x^3 + 2x + 1$ has exactly one root.

Proof 3
The proof is in two parts: (1) existence and (2) uniqueness.

1. To establish the existence of a root it is sufficient to show that the function crosses the x-axis. Given that f is a continuous function with $f(0) = 1$, we need to find another value of x that produces a negative value of $f(x)$. Guessing $x = -1$, we get $f(-1) = 3 \cdot (-1)5 + 2 \cdot (-1) + 1 = -3 - 2 - 2 - 1 = -6$. Thus, the *intermediate value theorem* ensures that $\exists\, c \in (-1, 0) : f(x) = 0$. Figure 3(a) below confirms the graph of f crossing the x-axis between -1 and 0.

2. The uniqueness of the root is proved by contradiction. Assuming two or more roots (say r_1 and r_2) exist, then the *mean value theorem* tells us

$$\exists\, c \in (r_1, r_2) : f'(c) = \frac{f(r_1) - f(r_2)}{r_1 - r_2} = \frac{0 - 0}{r_1 - r_2} = 0$$

In other words, there should be a horizontal tangent to the graph of $y = f(x)$ at the point $x = c$. However,

$$\frac{d}{dx} f(x) = \frac{d}{dx}\left(3x^5 + 2x^3 + 2x + 1\right) = 15x^4 + 6x^2 + 2 > 0, \ \forall x \in \mathbb{R}$$
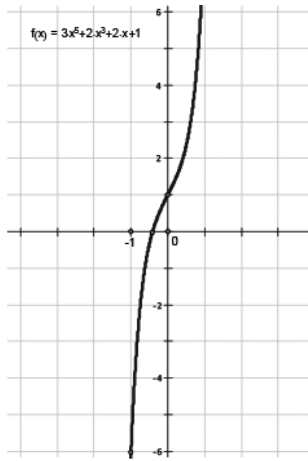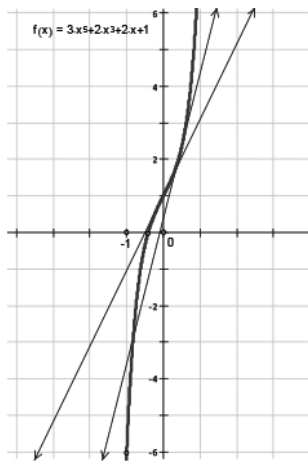
Figure 3 (a)

Figure 3 (b)

which means any tangent to the graph has a positive gradient and therefore cannot be horizontal (Figure 3(b)). Thus, we get a contradiction. This function cannot have more than one root. It is increasing everywhere, it is differentiable so its derivative is always greater than zero.

The next example is from geometry. In this example the original assumption is contradicted.

Example 4

Given a triangle ABC such that the two sides AB and BC are not equal and BD is a median, prove that BD is not perpendicular to AC.
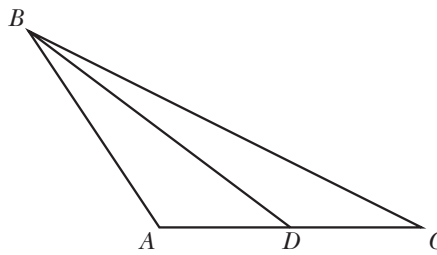

Figure 4

Proof 4

Assume BD is perpendicular to AC, that is $\angle ADB = \angle BDC = 90°$.

Now BD is a median so $AD = DC$. Therefore the two (right-angled) triangles ABD and BCD have two corresponding sides equal. It follows that the two triangles must be congruent, therefore $AB = BC$. Contradiction.

In the linear algebra example below, it is also the original assumption that is contradicted.

Example 5

Let A be an invertible matrix. Prove that A^{-1} is unique.

Proof 5

Suppose that A has two distinct inverses, namely B and C ($B \neq C$).

We have $AB = BA = I$, where the identity matrix is

$$I = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \\ 0 & & & & 1 \end{bmatrix}$$

We also have $AC = CA = I$, so it follows that $AB = AC$.

Pre-multiplying by C gives $C(AB) = C(AC)$.

By associativity, we have $(CA)B = (CA)C$. That is, $IB = IC$.

Hence, $B = C$. Contradiction. The inverse of A is unique.

Our final example shows how the given conditional statement may be proved by contradiction as well as by contraposition.

Example 6

Prove that the reciprocal of any irrational number is irrational.

Proof 6 by contraposition

The statement may be written symbolically as

$$\forall x \in \mathbb{R}, \ x \notin \mathbb{Q} \to \frac{1}{x} \notin \mathbb{Q}$$

The contrapositive statement is

$$\forall x \in \mathbb{R}, \ \frac{1}{x} \in \mathbb{Q} \to x \in \mathbb{Q}$$

Our starting point is $\frac{1}{x} \in \mathbb{Q}$.

This means that, by definition of the rational numbers,

$$\exists \ m, n \in \mathbb{Z} \ (n \neq 0) : \frac{1}{x} = \frac{m}{n}$$

That is, $x = \frac{n}{m}$, which means $x \in \mathbb{Q}$.

Proof 6 by contradiction

The negation of the original statement is

$$\exists \ x \in \mathbb{R} : \ x \notin \mathbb{Q} \wedge \frac{1}{x} \in \mathbb{Q}$$

Again, our starting point is

$$\frac{1}{x} \in \mathbb{Q}$$

and the next line of the derivation is identical to the proof by contraposition. The result $x \in \mathbb{Q}$ contradicts the assumption $x \notin \mathbb{Q}$.

Concluding remarks

The paper explored and clarified the similarities and differences that exist between proof by contradiction and proof by contraposition. The paper also focussed on the concept of contradiction mainly and a general model for this method of proof was offered.

The introduction of mathematical proof in the classroom remains a formidable challenge to students given that, at this stage of their schooling, they are used to manipulating symbols through sequential steps. There is a consensus that learners do find indirect types of proof quite difficult and do struggle with the conceptual and technical aspects of indirect proofs. As

Epp (1998, p. 711) states, "Students find proof by contradiction considerably harder to master than direct proof". Indeed, learners may struggle with understanding the concept of indirect proofs in general and of proof by contradiction in particular. To address this issue further, and for learning purposes, proof by contradiction may be considered in conjunction with other methods and didactic tools, e.g., counterexamples or the pigeon-hole principle. But, this is a topic for another investigation.

Acknowledgements

References

Antonini, S. & Mariotti M. A. (2008). Indirect proof: What is specific to this way of proving? *ZDM – The International Journal of Mathematics Education, 40*(3), 401–412.

Barnard, T. & Tall, D. (1997). Cognitive units, connections and mathematical proof. In E. Pehkonen (Ed.), *Proceedings of the 21st International Conference for the Psychology of Mathematics Education,* (Vol. 2, pp. 41–48). Lahti, Finland: University of Helsinki.

Epp, S. (1998). A unified framework for proof and disproof. *The Mathematics Teacher, 91*(8), 708–713.

Epp, S. (2011). *Discrete mathematics with applications* (4th ed.). Boston, MA: Brooks/Cole & Cengage Learning.

Euclid. (1956). *The thirteen books of Euclid's elements* (translation and commentaries by T. L. Heath). New York: Dover Publications.

Goubault-Larrecq, J. & Mackie, I. (1997). *Proof theory and automated deduction.* Dordrecht, The Netherlands: Kluwer Academic Publishers.

Grossman, P. (2009). *Discrete mathematics for computing* (3rd ed.). New York: Palgrave Macmillan.

Hanna, G. & de Villiers, M. (2008). ICMI Study 19: Proof and proving in mathematics education. *ZDM – The International Journal of Mathematics Education, 40*(2), 329–336.

Heath, T. L. (1921). *A history of Greek mathematics: From Thales to Euclid* (Vol. 1). New York: Dover Publications.

Lin, F., Lee, Y. & Wu Yu, J. (2003). Students' understanding of proof by contradiction. In N. Pateman, B. Dougherty, & J. Zilliox (Eds), *Proceedings of the Joint Meeting of PME and PMENA,* (Vol. 4, pp. 443–449). Hawaii: PME.

Mancosu, P. (1991). On the status of proofs by contradiction in the seventeenth century. *Synthese, 88*, 15–41.

Mancosu, P. (Ed.). (1996). *Philosophy of mathematical practice.* Oxford, UK: Oxford University Press.

Thompson, D. R. (1996). Learning and teaching indirect proof. *The Mathematics Teacher, 89*(6), 474–482.

Williams, E. R. (1979). *An investigation of senior high students' understanding of the nature of mathematical proof.* PhD dissertation, University of Alberta, Canada.