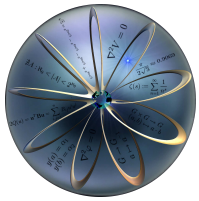


planetmath.org

Math for the people, by the people.

diamond lemma

Canonical name	DiamondLemma
Date of creation	2013-03-22 15:23:51
Last modified on	2013-03-22 15:23:51
Owner	CWoo (3771)
Last modified by	CWoo (3771)
Numerical id	9
Author	CWoo (3771)
Entry type	Topic
Classification	msc 68Q42
Classification	msc 03C05
Related topic	TerminatingReduction
Related topic	NormalizingReduction
Defines	reduction

The diamond lemmas constitute a of results about the existence of a unique normal form. Diamond lemmas exist in many diverse areas of mathematics, and as a result their technical contents can be quite different, but they are easily recognisable from their overall and basic idea — the "diamond" condition from which they inherit their name.

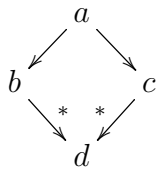
1 Newman's Diamond Lemma

The basic diamond lemma, that of Newman [**?**], is today most easily presented in of binary relations.

Theorem 1. *Let X be a set and let $\to$ be a binary relation on X. If $\to$ is terminating, then the following conditions are equivalent:*

1. *For all $a, b, c \in X$ such that $a \to b$ and $a \to c$, then b and c are joinable.*
2. *Every $a \in X$ has a unique normal form.*

Condition **??** can be graphically drawn as



where $\overset{*}{\to}$ denotes the reflexive transitive closure of $\to$. This is the "diamond" from which the result derives its name — not crystallised carbon, but merely a square standing on one corner. In relation to this picture, what the condition says is that whenever one has $a, b, c \in X$ forming the top two sides of such a diagram, there is a fourth corner $d \in X$ which completes the diamond.

The typical case to which one applies this theorem is that X is a set of formal terms on which one wishes to define an equivalence relation $\sim$. The $\to$ relation encodes a set of "elementary" equivalences — an example in standard algebra of such an elementary equivalence might be the instance $a(b{+}c) \to ab{+}ac$ of the distributivity axiom — that generate the wanted $\sim$. It is techincally possible to define the equivalence $\sim$ as the reflexive–transitive–symmetric closure of $\to$, but since X is typically infinite that definition does not lead to an effective method for determining whether $x \sim y$. However

when the relation $\to$ satisfies the conditions in Theorem **??**, there does exist an algorithm which given $\to$ determines whether two arbitrary elements are related by $\sim$.

In a computational setting, the interpretation of $x \to y$ is usually that there exists a "one-step simplification" that converts the expression x to the expression y. The corresponding interpretation of $x \xrightarrow{*} y$ is thus that there exists a finite sequence of "simplifications" that converts x to y. The formal term used for "simplifications" in this sense is *reductions*, so $x \xrightarrow{*} y$ is read as "x reduces to y" or "x can be reduced to y".

The theorem has several immediate applications — first of all that there is a unique function $N\colon X \longrightarrow X$ which sends arbitrary elements of X to their normal forms — and this leads to a test for whether arbitrary elements are equivalent.

Lemma 1. *Let X be a set and $\to$ a binary relation on X such that all elements of X has a unique normal form with respect to $\to$. Denote by $\sim$ the reflexive transitive symmetric closure of $\to$ and denote by N the function $X \longrightarrow X$ which sends every element to its normal form with respect to $\to$. Then for all $x, y \in X$,*

$$x \sim y \quad \textit{if and only if} \quad N(x) = N(y). \tag{1}$$

Proof. Denote by $\xrightarrow{*}$ the reflexive–transitive closure of $\to$ and denote by $\leftrightarrow$ the symmetrisation of $\to$. If $N(x) = N(y)$ then obviously $x \xrightarrow{*} N(x) = N(y) \xleftarrow{*} y$ and thus $x \sim N(x) \sim y$ as claimed. If conversely $x \sim y$ then there must exist some sequence

$$z_0 \leftrightarrow z_1 \leftrightarrow \cdots \leftrightarrow z_{n-1} \leftrightarrow z_n$$

where $z_0, \ldots, z_n \in X$, $z_0 = x$, and $z_n = y$. For every z_k one of $z_k \to z_{k+1}$ and $z_k \leftarrow z_{k+1}$ must hold. In the former case $z_k \xrightarrow{*} z_{k+1} \xrightarrow{*} N(z_{k+1})$ and thus by transitivity $z_k \xrightarrow{*} N(z_{k+1})$, but this means $N(z_{k+1})$ is a normal form also of z_k. In the latter case one similarly shows that $N(z_k)$ is a normal form of z_{k+1}. Either way it follows from the uniqueness of the normal form that $N(z_k) = N(z_{k+1})$. Thus $N(z_0) = N(z_1) = \cdots = N(z_{n-1}) = N(z_n)$ and hence $N(x) = N(y)$ as claimed. □

Another application of normal forms is to serve as representatives of the equivalence classes of X. Many mathematical constructions of algebraic

structures (e.g. that of a quotient of a group) end up producing a set $X/\!\sim$ of equivalence classes of some given set X, but these are as a rule unfeasible for computational purposes. What one can do instead is to choose an element from each equivalence class and use these as representatives of their equivalence classes. When normal forms are known to be unique, there trivially exists a bijection from

$$X_{\mathrm{nf}} = \{\, x \in X \mid x \text{ is on normal form} \,\}$$

to $X/\!\sim$ given by $x \mapsto [x]_\sim$, and its inverse can thanks to Lemma **??** be defined in terms of the normal form map N as $[x]_\sim \mapsto N(x)$.

How does one know that the normal form map N is effective, though? This is because of the terminating property on the binary relation in Theorem **??**.

The primary consequence of being terminating is that $\overset{*}{\to}$ is well-founded, and it is no surprise that Theorem **??** is proved using well-founded induction. Being terminating is also what guarantees that the following algorithm "terminates".

Algorithm 1 (Normal form)**.** *Let X be a set and $\to$ a strict binary relation on X which satisfies the descending chain condition.*

Input *An element $x \in X$.*

Output *A normal form of x.*

Procedure *If x is on normal form with respect to $\to$ then return x. Otherwise there is some $y \in X$ such that $x \to y$; pick one such y. Set $x := y$ and repeat the procedure from start.*

For $\to$ which the descending chain condition and have unique normal forms, Algorithm **??** and Lemma **??** combine to an algorithm for deciding the relation $\sim$. A typical problem is however that uniqueness of the normal form is a global condition that is very hard to establish using elementary methods. *Theorem* **??** *offers an equivalent local condition that often is straightforward to verify in each particular case by explicit calculations.*

2 Diamond lemmas for algebraic structures

One disadvantage of the basic diamond lemma (Theorem **??**) is that it requires all reductions to be explicit, whereas the mathematician probably

expects it to handle reduction schemas transparently. To illustate the , consider again the reduction $a(b + c) \to ab + ac$. This does *not* imply $(d + e)(b + c) \to (d + e)b + (d + e)c$, or even $2(b + c) \to 2b + 2c$, because all three left hand are distinct as formulae (i.e., as elements of X). In to let a, b, and c be arbitrary, one need to explicitly state that e.g. "$a(b+c) \to ab+ac$ for all well-formed formulae a, b, and c". Even this may be less than what was intended, since it is often the case that one wants it to follow from $a(b + c) \to ab + ac$ also that $f\big(a(b + c)\big) \to f(ab + ac)$ for arbitrary functionalised expressions f. Theorem **??** requires its user to take care of such details explicitly.

Moreover, the conditions in Theorem **??** are stated about arbitrary elements of X, so even if one employs schemas in the definition of $\to$, it is necessary to verify that condition **??** holds for every concrete triple (a, b, c) of elements of X such that $b \leftarrow a \to c$. This too can be done collectively using proof schemas, but the situation is complicated enough that it is often far from clear whether all cases have been checked. It is furthermore common that trivial verifications of a syntactic origin outnumber the verifications that have interesting mathematical content. This makes it less likely that mathematicians will actually bother to produce a proof, and more likely that they will skip it altogether by resorting to the notorious "It is easy to see that ..."

Finally, it is not always the case than one just wants an equivalence relation. When the set X has an established structure one typically rather wants $\sim$ to be a congruence relation, but the basic diamond lemma can of course not take such sophistications into account. Therefore *there exist also a number of specialised diamond lemmas which are tailored to particular* and can make do with verifications of significantly fewer cases than the basic diamond lemma.

The most familiar such result is probably the *diamond lemma for ring theory* of Bergman [**?**], also known as the *composition lemma for associative algebras* [**?**].

[Give full statement of theorem? It's quite a mouthful.]

[Write about relation to Gröbner basis theory.]

References

[1] G. M. Bergman: The Diamond Lemma for Ring Theory, *Adv. Math.* **29** (1978), 178–218.

[2] L. A. Bokut′: Embeddings into simple associative algebras (Russian), *Algebra i Logika* **15**, no. 2 (1976), pp. 117–142 and 245. English translation in *Algebra and Logic*, pp. 73–90.

[3] M. H. A. Newman: On theories with a combinatorial definition of "equivalence", *Ann. of Math.* **43** (1942), 223–243.