ПРОСТОТА КАК КРИТЕРИЙ УБЕДИТЕЛЬНОСТИ ДОКАЗАТЕЛЬСТВА

Е.М. Черепанов

Рассматриваются понятия структурной и прагматической сложности доказательства в счислении предикатов первого порядка. Рассмотрены возможные способы измерения сложности доказательства формул. На базе такого способа измерения сложности доказательств сформулирован алгоритм компьютерного поиска простейшего доказательства за заданное количество шагов. Предложенный метод поиска простейшего доказательства позволяет обосновывать убедительность как «ручного», так и «машинного» доказательства теорем. Показана «упрощающая» роль дефинициальных расширений теории в поиске простейшего доказательства.

Keywords: simplicity, complexity, proving, algorithm

Математическое доказательство занимает важное место в философских аргументах относительно природы человеческого знания. Во-первых, доказательство есть аргумент, а различные теории правильности аргумента долгое время рассматривались в качестве части философии. До сих пор логика многими исследователями считается не частью математики под названием «математическая логика», а вполне актуальной философской проблематикой. Во-вторых, математическое доказательство инспирировало влиятельнейшие теории о природе идей и человеческого ума. Так, понятие априорного мышления, игравшее важнейшую роль в истории философии и продолжающее играть ее и сегодня, сопряжено прежде всего с пониманием того, что представляет собой постижение математического доказательства. Математика связана с философией множеством тем и понятий, и повсюду мы сталкиваемся с тем, что при этом понятие математического доказательства часто выходит на передний план.

Главной характеристикой традиционной концепции доказательства является *убедительность доказательства*. Доказательство есть аргумент нашей веры в истинность утверждения, а аргумент должен быть убедительным и поэтому при обсуждении доказательства неизбежно возникает тема самого рационального мышления. Факторы, влияющие на убедительность доказательства, подробно рассмотрены в книге В.В. Целищева «Эпистемология математического доказательства» [1]. В рамках настоящей статьи мы остановимся на одном из важнейших факторов, влияющих на убедительность доказательства, а именно, на критерии простоты.

ã Черепанов Е.М., 2010

Роль критерия простоты в доказательстве утверждений в рамках теории многозначна. Если доказательство есть последовательность утверждений, в которой переход от одного утверждения к другому представляется необходимым, то возникает вопрос о том, почему математическая практика в значительной степени состоит из «передоказывания» теорем, поиска новых, все более простых доказательств. В этом смысле данную практику можно рассматривать как движение от формализованного доказательства к интуитивному. Таким образом, мы имеем две тенденции в доказывании теорем. С одной стороны, теоремы, в доказательстве которых используются интуитивные соображения, передоказываются в соответствии с пересмотром критериев строгости математического доказательства. С другой стороны, строго доказанные теоремы передоказываются для того, чтобы достичь понимания доказательства (здесь «понимание» доказательства является одним из критериев его убедительности). Этот процесс понимания и проявляется в серии новых, все более простых доказательств. Понятие простоты доказательства выступает не просто психологическим критерием, а одним из основных требований к доказательству, так как более простое доказательство является и более информативным.

Так как доказательство есть упорядоченная последовательность формул, перед тем как предложить способы измерения структурной сложности математического доказательства, определим способ измерения структурной сложности формулы через значение сложности входящих в нее терминов.

Пожалуй, самыми значимыми в области исследования структурной сложности терминов стали работы Н. Гудмена. В 1961 г. в книге «The structure of appearance» [2] публикуется окончательная версия его подхода к измерению простоты внелогических терминов первопорядковых теорий. В более ранней статье «The test of simplicity» [3] Гудмен подчеркивает: «…Мы должны начать, ограничившись очень малой частью проблемы привлекающей внимание. Теория есть система утверждений. Я буду касаться здесь исключительно проблемы простоты множества понятий (словаря системы), используемых в этих утверждениях» [4].

Определяя понятие структурной характеристики внелогичеких терминов, к которым Гудмен относит местность каждого термина, некоторые возможные специальные свойства каждого из терминов (различные виды рефлексивности, симметричности и сильной транзитивности) – он называет эти характеристики *релевантными*, – Гудмен предлагает числовую функцию, описывающую эти структурные характеристики, которые и можно считать эталонами измерения простоты/сложности для внелоги-

ческих терминов теории. Сложность «словаря системы» Гудмен определяет с помощью созданных им «эталонов» измерения.

Понятие «более» является ключевым во многих подходах к измерению простоты/сложности объектов и процессов. Такой же принцип главенствует и в теории простоты Гудмена. Самым простым термином считается одноместный предикат. Двухместный предикат в общем случае является структурно более сложным, чем одноместный, трехместный – более сложным, чем двухместный, и т.д. Кроме того, полагается, что если некоторое фиксированное множество предикатов может быть определимо из другого фиксированного множества предикатов, то сложность исходного множества предикатов не больше, чем сложность второго. Последний принцип играет ключевую роль в предложенном Гудменом подходе, так как позволяет в некоторых случаях определять сложные термины через более простые. С каждым из терминов теории Гудмен соотносит класс его интерпретаций (или класс моделей этого термина) и определяет способ измерения сложности терминов, имеющих релевантную спецификацию. Каждому термину, имеющему релевантную спецификацию, в теории Гудмена приписывается целое число, характеризующее сложность класса интерпретаций этого термина. Технические подробности, касающиеся способа задания числовой функции на множестве релевантных классов, можно найти в упомянутой работе Гудмена «The structure of appearance».

Таким образом, значения сложности терминов, имеющих релевантную спецификацию, являются эталонами измерения, а значение сложности произвольного термина, а следовательно, и класса его интерпретаций определяется через значение сложности созданных эталонов измерения. Значение сложности произвольного термина определяется через значение минимального по значению сложности термина релевантного вида, из которого этот термин определим. Определение числовой функции, позволяющей приписать числовое значение сложности произвольному термину теории, приведено автором ранее [5].

Далее, будем писать $v_G(P)$, подразумевая, что речь идет о значении сложности класса интерпретаций термина *P*.

Если L – язык первого порядка конечной сигнатуры $\Omega =< P_1^{m_1}, ..., P_n^{m_n} >$, где m_i есть местность каждого термина, то значение сложности множества внелогических терминов этого языка определяется в теории Гудмена следующим образом:

$$\nu_G(\mathrm{Mod}(L) = \sum_{i=1}^{n} \nu_G(P_i^{m_i}).$$

Аналогичным образом можно подойти и к структурной сложности формул языка первого порядка L заданной конечной сигнатуры Ω. Здесь будем руководствоваться довольно естественным принципом, согласно которому сложность любого предложения в языке определяется количеством слов в нем и сложностью используемых слов.

Следуя этому, к структурным характеристикам формулы будем относить количество вхождений в эту формулу предикатов (под количеством вхождений предикатов в формулу здесь будем понимать возможное количество использований каждого предиката), а также структурные характеристики каждого из этих предикатов.

Самым простым и наиболее естественным способом приписать значение структурной сложности формуле этого языка является способ, аналогичный оценке сложности класса интерпретаций множества внелогических терминов по Гудмену. Согласно этому способу мы получим, что если $\{P_{i_1}^{j_1}, ..., P_{i_m}^{j_m}\}$ есть множество всех вхождений предикатов в формулу φ, то значение структурной сложности формулы φ можно определить следующим образом: $\nu_f(\varphi) = \sum_{k=1}^{m} \nu_G(P_{i_k}^{j_k})$, где $\nu_G(P_{i_k}^{j_k})$ есть значение сложности класса интерпретаций этого термина.

Предложенный способ измерения структурной сложности формул языка L позволит нам различать, в частности, и структурную сложность логически эквивалентных формул. То есть из двух формул φ и ψ, таких что $\forall x(\varphi \leftrightarrow \psi)$ мы всегда сможем выбрать наименее структурно сложную формулу. Возможность различения структурной сложности логически эквивалентных формул позволяет нам вести речь о *прагматической сложности*, так что здесь уместно будет говорить об удобстве использования и легкости восприятия наименее структурно сложной из двух логически эквивалентных формул, но об этом речь пойдет далее.

Различение формул по значению их структурной сложности дает нам возможность различения структурной сложности различных доказательств одной и той же формулы. Напомним, что *доказательством формулы* φ в фиксированном исчислении *IP* первого порядка заданной конечной сигнатуры Ω называется последовательность формул $\{\varphi_1, \ldots, \varphi_{n+1}\}$, такая что

$\varphi_{n+1} = \varphi$ и для каждого $i \le n+1$ каждая формула φ_i удовлетворяет одному из следующих условий:

i) φ_i является аксиомой *IP*;
ii) φ_i получается из φ_j, где $j < i$, по одному из правил вывода.

В классическом исчислении логики первого порядка основными правилами вывода являются следующие:

а) $\dfrac{\Phi, \Phi \to \Psi}{\Psi}$ (modus ponens);

б) $\dfrac{\Phi \to \Psi}{\Phi \to \forall x \Psi}$;

в) $\dfrac{\Phi \to \Psi}{\exists x \Phi \to \Psi}$.

Выводом в исчислении *IP* формулы φ из множества формул Г называется последовательность формул $\{\varphi_1, \ldots, \varphi_{n+1}\}$ такая, что $\varphi_{n+1} = \varphi$ и для каждого $i \le n+1$ каждая формула φ_1 удовлетворяет одному из следующих условий:

i) φ_i доказуема в исчислении *IP*;
ii) φ_i принадлежит множеству формул Г;
iii) φ_i получается из φ_j, где $j < i$, по одному из правил вывода (а) – (в), причем при применении правил (б) и (в) переменная x не должна входить ни в одну из формул Г свободно.

На множестве всех доказательств исчисления *IP* определим числовую функцию, характеризующую сложность этого доказательства. Аналогичным образом к структурным характеристикам доказательства будем относить количество формул в последовательности формул, структурные характеристики каждой формулы в этой последовательности и структурные характеристики входящих в эти формулы терминов.

Численной функцией, характеризующей *структурную сложность* доказательства, будем считать следующую функцию. Если через v_{pr} обозначить численное значение структурной сложности доказательства формулы φ последовательностью формул $\{\varphi_1, \ldots, \varphi_{n+1}\}$, то определим численное значение структурной сложности этого доказательства следующим образом:

$$v_{pr}\{\varphi_1, ..., \varphi_{n+1}\} = v_f(\varphi_1) + ... + v_f(\varphi_{n+1})$$

Покажем утилитарную приемлемость такого подхода для измерения структурной сложности доказательств утверждений. В научной практике все большее распространение получают методы компьютерного доказательства теорем. Компьютерное доказательство может служить как способом проверки «ручного» доказательства, так и способом поиска доказательства еще не доказанных утверждений.

Пусть методы машинного доказательства таковы, что позволяют нам находить все конечные цепочки доказательства заданной длины. Допустим, что доказана некоторая формула φ и это доказательство осуществлено за n шагов, то есть доказательством этой формулы является последовательность формул $\{\varphi_1, \ldots, \varphi_{n+1}\}$ и $\varphi_{n+1} = \varphi$. Каким образом найти более простое доказательство? Рассмотрим все последовательности формул доказательства формулы φ длины не более n. Количество такого рода последовательностей, построенное по вышеуказанным правилам вывода будет конечно и пусть это число равно k. Пусть D есть множество такого рода последовательностей длины не более n.

Рассмотрим последовательность $d_i \in D$. Значение сложности этой последовательности формул определяется указанным образом:

$$v_{pr}(d_i) = v_f(\varphi_{i_1}) + ... + v_f(\varphi_{i_n})$$

Разобьем множество последовательностей формул D на классы эквивалентности по степени сложности элементов этого множества. Пусть это будет фактор-множество D_v. Упорядочим элементы множества по степени их сложности. Пусть $D_v = \{K_1, ..., K_l\}$, причем значение сложности элементов произвольного класса этого множества больше значения сложности предыдущего класса и меньше сложности последующего.

Остается теперь только рассмотреть все последовательности доказательств меньшей сложности, чем сложность уже полученного доказательства. Если доказанная формула φ принадлежит классу K_1, то это и есть простейшее доказательство указанной длины.

Допустим, что доказанная формула принадлежит классу K_j, тогда рассматриваем классы $\{K_1, ..., K_{j-1}\}$ по порядку начиная с первого и выбираем первую попавшуюся последовательность, заканчивающуюся формулой φ, – это и будет простейшим доказательством.

Ровно так же будет выглядеть процесс поиска простейшего доказательства формулы φ при отсутствии предварительного (возможно, «ручного») доказательства этой формулы. В этом случае, если нас интересует доказательство длины, определяемое заданным числом шагов *n*, мы будем рассматривать множество классов эквивалентности $D_v = \{K_1, ..., K_l\}$ начиная с первого класса. Если такого доказательства не находится, то в рассматриваемых условиях доказательства указанной длины не существует.

В математической практике при поиске доказательства того или иного утверждения значительную роль играет «подходящее» (облегчающее поиск такого доказательства) консервативное расширение исходной теории. Покажем, что дефинициальное расширение теории способствует «упрощению» доказательств исходной теории.

Для ясности изложения приведем необходимые определения относительно определимости терминов. Детально различные виды определимости рассмотрены в книге В.А. Смирнова «Различные методы анализа научного знания» [6].

На основе результатов, касающихся определимости предикатных терминов в первопорядковых теориях, можно рассмотреть и некоторые аспекты учения об определениях. Ограничимся пока только определениями предикатных терминов в первопорядковых теориях. Целесообразно выделить три подхода к определениям, или три точки зрения на определения.

Во-первых, определения рассматриваются как процедуры, вводящие новый термин. Во-вторых, они понимаются как процедуры установления значения уже имеющегося термина через другие термины. В-третьих, определения понимаются как процедуры перевода (Л. Витгенштейн «Определения суть правила перевода с одного языка на другой») [7].

Так, если имеется теория T_1, словарь которой не содержит термина *P*, и теория T_2, которая дополнительно к словарю теории T_1 содержит термин *P*, то определение при третьем подходе трактуется как перевод выражений теории T_2, содержащих термин *P*, в выражения теории T_1.

Первый подход. Пусть имеется теория *T* и ее словарь [*T*] не содержит термина *P*. Пусть множество предложений сформулировано в терминах словаря $[T] \cup P$. Множество предложений Δ *играет роль определения* *n*-местного термина *P* в теории *T* тогда и только тогда, когда существует формула ψ, сформированная в терминах не содержащих *P*, ровно с *n* различными свободными переменными, такая что $Th(T \cup \Delta) = Th(T \cup \{\forall x(P(x) \leftrightarrow \psi)\})$.

Очевидно, что $Th(T \cup \Delta)$ есть консервативное расширение теории T, так как оно не содержит новых теорем по сравнению с теорией T. Легко видеть, что из определимости термина P в $Th(T \cup \Delta)$ следует, что Δ удовлетворяет условию переводимости.

Второй подход. Мы будем считать, что термин P задан только на объектах, удовлетворяющих условию φ, а на остальных не задан. С формальной точки зрения при рассмотрении условных определений удобно использовать технику ограниченных кванторов, в частности вместо $\forall x(\varphi(x) \to (P(x) \to \psi(x)))$ писать $\forall x_{j(x)}(P(x) \to \psi(x))$.

Таким образом, n-местный термин P явно условно определим в терминах предложений Δ тогда и только тогда, когда существуют условие φ и формула ψ, содержащая ровно n различных свободных переменных и не содержащая термина P такая, что $\Delta \vdash \forall x_{\varphi(x)}(P(x) \leftrightarrow \psi(x))$.

Покажем теперь прагматическую важность консервативных расширений, упрощающих поиск простейшего доказательства. Следует отметить, что в поиске и построении эквивалентных доказательств (эквивалентных в смысле доказательства одной и той же формулы) огромную роль играют такие прагматические аспекты простоты, как удобство использования и легкость восприятия.

Автором предложен метод измерения такого вида прагматической простоты [8], и состоит он в следующем. Всякая формула или последовательность формул рассматривается как «цельный» объект. Так, в математической практике удобнее и проще рассматривать аксиоматику теории как список небольших и обозримых формул, хотя при этом можно рассматривать этот список и как конъюнкцию этих формул. Поэтому каждой формуле (или списку формул) сопоставляется атомарная формула, образованная конкатенацией мест входящих в такого рода объект предикатов. Построение такой атомарной формулы и определение такого рода простоты осуществляются следующим образом.

Построим отображение f, которое для всякой формулы φ языка L ставит в соответствие формулу языка L_φ, единственный предикатный символ в сигнатуре которого и местность которого определяются суммой мест, входящих в формулу φ предикатов. Это сопоставление будем осуществлять по следующему правилу:

а) если φ есть формула вида $P(x_1, ..., x_n)$, то $f(\varphi) = \varphi$;

б) если φ есть формула вида $\neg P(x_1, ..., x_n)$, то $f(\varphi) = \varphi$;

в) если φ есть формула вида $P_1(x_1, ..., x_n) \Delta P_2(y_1, ..., y_m)$, где $\Delta \in \{\&, \vee, \rightarrow\}$, то $f(\varphi) = R(x_1, ..., x_n, y_1, ..., y_m)$;

г) если φ есть формула вида $Qx\psi(x)$, где $Q \in \{\forall, \exists\}$, то $f(\varphi) = f(\psi)$;

д) если φ есть формула вида $\psi_1 \Delta \psi_2$, то $f(\varphi) = f(f(\psi_1) \Delta f(\psi_2))$;

Таким образом, если каждой формуле φ языка L отображение f ставит в соответствие атомарную формулу $R(x_1, ..., x_k) = f(\varphi)$ то, обозначив через $\nu_p(\varphi)$ численное значение прагматической сложности формулы φ, а через $\nu_G(R)$ значение сложности класса интерпретаций термина R по Гудмену, определим прагматическую сложность формулы φ следующим образом:

$$\nu_p(\varphi) = \nu_G(f(\varphi)) = \nu_G(R).$$

Аналогичным образом каждой последовательности формул, являющейся доказательством формулы φ, с помощью отображения f будем ставить в соответствие формулу R и *прагматическое* значение сложности этого доказательства будем определять аналогичным же образом:

$$\nu_p(\{\varphi_1, ..., \varphi_{n+1}\}) = \nu_G(f(\{\varphi_1, ..., \varphi_{n+1}\}) = \nu_G(f(\varphi_1 \Delta ... \Delta \varphi_{n+1})) = \nu_G(R)$$

Пусть последовательность формул $\{\varphi_1, ..., \varphi_{n+1}\}$ есть доказательство формулы φ ($\varphi_{n+1} = \varphi$) в теории T сигнатуры Ω и пусть T^* есть дефинициальное расширение теории T, образованное добавлением нового сигнатурного термина Q посредством следующего определения:

$$\forall x_1 ... x_n (Q(x_1, ..., x_n) \leftrightarrow \psi(x_1, ..., x_n)),$$

где в формулу ψ входят лишь термины теории T. Автором показано [9], что

$$\nu_p(Q(x_1, ..., x_n)) \leq \nu_p(\psi(x_1, ..., x_n))$$

Тогда если в теории T^* в последовательности формул, являющейся доказательством формулы φ, встречается определяемый термин, то согласно определению прагматической сложности доказательство формулы φ в теории T^* будет проще в силу приведенного выше соотношения. То есть если $\{\varphi_1, ..., \varphi_{n+1}\}$ есть доказательство формулы φ ($\varphi_{n+1} = \varphi$) в теории T, а есть доказательство формулы φ ($\varphi = \psi_{k+1}$) в теории T^*, то

$$\nu_p(\{\psi_1, ..., \psi_{k+1}\}) \le \nu_p(\{\varphi_1, ..., \varphi_{n+1}\})$$

Отметим тут же одно немаловажное обстоятельство, касающееся такого рода определений структурной и прагматической сложности доказательства. Можно сформулировать следующее утверждение.

Утверждение. Пусть по-прежнему ν_{pr} есть обозначение структурной сложности доказательства, а ν_p – прагматической сложности и пусть доказательством формулы φ является последовательности формул $\{\varphi_1, ..., \varphi_{n+1}\}$ тогда $\nu_{pr}(\{\varphi_1, ..., \varphi_{n+1}\}) \le \nu_p(\{\varphi_1, ..., \varphi_{n+1}\})$.

Доказательство. Доказательство этого утверждения вытекает из определения структурной и прагматической сложности формул и одного из основных свойств метода измерения сложности предикатных терминов по Гудмену, согласно которому если $n = k + m$, то $\nu_G(P^n) \ge \nu_G(R^k) + \nu_G(G^m)$.

Рассмотрим две последовательности доказательства формулы φ: $\{\varphi_1, ..., \varphi_{n+1}\}$ и $\{\psi_1, ..., \psi_{k+1}\}$. Возникает естественный вопрос: если $\nu_p(\{\varphi_1, ..., \varphi_{n+1}\}) \le \nu_{pr}(\{\psi_1, ..., \psi_{k+1}\})$, то следует ли из этого, что $\nu_p\{\varphi_1, ..., \varphi_{n+1}\}) \le \nu_p(\{\psi_1, ..., \psi_{k+1}\})$? То, что в общем случае это не так, показывает приводимый ниже пример.

Пусть $d_1 = \{P_1(x_1, x_2), ..., P_4(x_7, x_8), P_5(x_9)\}$ и $d_2 = \{R(y_1, ..., y_4), R_2(z_1, ..., z_4)\}$ суть две последовательности атомарных формул и пусть для простоты все предикаты $\{P_1, ..., P_4, R_1, R_2\}$ есть иррефлексивные предикаты [10]. Теория Гудмена определяет значение сложности произвольного n-местного иррефлексивного предиката по формуле $2n - 1$. Согласно определению прагматической сложности и определению сложности предикатов по Гудмену $\nu_p(d_1) > \nu_p(d_2)$. Значения структурной сложности для этих последовательностей будут следующими: $\nu_p(d_1) = \nu_G(P_1) + \ldots + \nu_G(P_5) = 3 + 3 + 3 + 3 + 1 = 13$, а $\nu_{pr}(d_2) = \nu_G(R_1) + \nu_G(R_2) = 7 + 7 = 14$, т.е. $\nu_{pr}(d_1) < \nu_{pr}(d_2)$.

Этот пример показывает, что если с помощью введения определяемого термина мы достигаем прагматического упрощения теории, то при поиске простейшего доказательства целесообразно опираться на понятие структурной простоты доказательства.

В настоящей работе предложены методы измерения структурной и прагматической сложности доказательств в исчислении первого порядка. Показана прагматическая обоснованность такого метода измерения сложности доказательств. Продемонстрировано соотношение структурного

и прагматического стандартов простоты. Поиск в какой-либо теории простейшего доказательства имеет важное значение, так как простое доказательство легче проверить, т.е. убедиться как в истинности доказанного утверждения, так и в возможности опровергнуть его. И здесь можно увидеть, что истинность и простота тесно связаны между собой. Любое доказательство требует верификации, но не всегда это сделать легко, когда речь идет о сложном доказательстве, которое характеризуется большой длиной и сложными конструкциями формул. В этом случае достаточно затруднительно убедиться в валидности приведенного доказательства по сравнению с простым доказательством. Таким образом, более простое доказательство является и более убедительным.

Примечания

1. См.: *Целищев В.В.* Эпистемология математического доказательства. – Новосибирск: Параллель, 2006.

2. См.: *Goodman N.* The structure of appearance. – Harvard Univ. Press, 1961.

3. См.: *Goodman N.* The test of simplicity // Science. – 1958. – V. 128, No. 3331. – P. 1064–1069.

4. Ibid. – P. 1067.

5. См.: *Черепанов Е.М.* Сложность «экстралогического базиса системы» по Гудмену и ложность научной теории // Вычислительные системы. – Новосибирск, 2001. – Вып. 168.

6. См.: *Смирнов В.А.* Логические методы анализа научного знания. – М.: Наука, 1987.

7. *Витгенштейн Л.* Логико-философский трактат. – М., 1958. – С. 43.

8. См.: *Черепанов Е.М.* Содержательность, информативность, простота // Философия науки. – 2006. – № 2 (29). – С. 52–64.

9. Там же.

10. n-местный предикат называется иррефлексивным, если $\forall x_1 \ldots x_n (P(x_1, \ldots, x_n) \leftrightarrow (x \neq x_2 \neq \ldots \neq x_n))$.

Дата поступления 04.04.2009

Институт математики СО РАН,
г. Новосибирск
E-mail: emcher@math.nsc.ru

Cherepanov, E.M. **Simplicity as a criterion of proving validity**

The paper discusses the conceptions of structural complexity of proving and pragmatic one in calculus of first order predicates. Possible ways to measure complexity of formula proving are presented. On the basis of such a way of measuring complexity of proving, an algorithm of computer search of the most simple proving within a given number of iterations is introduced. This method of search of the most simple proving enables to vindicate validity of both "manual" and "machine" proving of theorems. A "simplifying" role of definitional extensions of a theory in a search of the most simple proving is shown.

Keywords: simplicity, complexity, proving, algorithm