DOI 10.26886/2520-7474.2(34)2019.6

UDC: 51-37

APPLYING AN INTERACTIVE PROGRAM-PROVER LIKE COQ CAN BECOME A NEW STANDARD FOR APPROBING OF PRACTICALLY IMPORTANT THEORETICAL WORKS

N. D. Stukach

National Aviation University, Ukraine, Kyiv

There are some theories in the world, which have great scientific and practical importance but have no approbation. In the article the theory of "widened long flip-flop" (that represents scientific and practical interests in the field of building mission-critical computing system) is used as an example to analyze reasons of such situation and ways of solving this issue. These ways appear with powerful interactive program-prover like Coq. Such prover may either prove or do not prove the theory since it depends on human prompts. But if the proof is successful, the correctness of the theory will be guaranteed.

Key words: complex theory, approbation, program-prover, Coq, arXiv.org

Стукач Н. Д. Применение интерактивной программы-прувера типа Coq может стать новым стандартом апробации практически важных теоретических работ/ Национальный авиационный университет, Украина, Киев

В мире существуют теории, имеющие важное научное и практическое значение, но не имеющие апробации. В статье на примере теории «длинного триггера» (2008 г.), представляющей научный и практический интерес в области создания mission-critical вычислительных систем, анализируются причины такой ситуации, а также возможности выхода из неё, возникающие в связи с

появлением мощных интерактивных программ-пруверов типа Coq. Прувер может доказать или не доказать теорию, многое зависит от подсказок человека. Но в случае, если доказательство удалось, корректность теории будет гарантирована.

Ключевые слова: сложная теория, апробация, программа-прувер, Coq, arXiv.org

Постановка проблемы. В мире существуют теории, имеющие важное научное и практическое значение, но не имеющие апробации. В статье на примере теории «длинного триггера» (2008 г.), представляющей научный и практический интерес* в области создания mission-critical вычислительных систем, анализируются причины такой ситуации, а также возможности выхода из неё, возникающие в связи с появлением мощных интерактивных программных пруверов типа Coq.

Основной текст. Недавно (в 2018 г.) праздновали 100-летие изобретения триггера на радиолампах – двустабильной электронной схемы, которая имела 2 входа. Подачей импульса на один вход триггер устанавливался в 1, подачей импульса на другой – сбрасывался в 0. В отсутствие импульсов триггер сохранял своё состояние, пока не отключали питание.

Этот триггер очень пригодился, когда Атанасов и Берри, признанные изобретателями электронного компьютера, строили свой компьютер ABC. Или в компьютерах Bomb и Colossus, построенных для взлома кода Энигмы. А вообще, без триггеров невозможен ни один электронный компьютер, хотя триггеры теперь строят на других электронных элементах – от одноэлектронных транзисторов до переходов Джозефсона.

Автору удалось придумать свой триггер, который является более сложным, чем двустабильный, и который не мог быть назван иначе,

чем «длинным», поскольку имеет длину (а потом оказалось, что самое интересное начинается, когда ему добавить ещё и «ширину»). Идея этого триггера пришла летом 1980 года, в период Московской олимпиады, когда автор после вступления в очную аспирантуру Киевского политехнического института и сдачи кандидатских экзаменов «растекался мыслью по древу» в поисках идеи, на которой можно было бы защититься (та, с которой поступал, не очень-то нравилась). Как сейчас он помнит, что это произошло вечером, идея была сверхпростая, но автор сразу ощутил её ценность, испытав отчётливый щелчок где-то внутри мозга. (Впоследствии такой щелчок автор ощутил ещё только один раз, не так давно, и над появившейся идеей сейчас работает.) Ночь автор не спал, а последующие 28 лет (с большими перерывами!), помня о щелчке, доводил идею до ума – 2 года в аспирантуре, потом перервался на 7 лет пока работал в СКБ киевского производственного объединения «Электронмаш», потом плодотворные 5 лет смог заниматься ею (в свободное время, разумеется) в киевском Институте кибернетики, где была подходящая интеллектуальная атмосфера, потом очень долго пришлось заниматься исключительно выживанием семьи, потом за 3 месяца нашлось время чтобы дописать и разместить в arXiv.org статью [1]**.

Упомянутые 28 лет занятия теорией «длинного триггера» не пошли автору на пользу в материальном отношении (это было как хобби – а какую пользу нужно ждать от хобби?), но очень улучшили саму работу, он довёл её до логического завершения и много поработал над стилем изложения (автор кардинально менял его минимум 6 раз, заодно исправляя ошибки и осваивая необходимые компьютерные технологии, без которых ничего бы не получилось: CorelDRAW, Perl, DreamWeaver, JavaScript, HTML, CSS, Adobe Acrobat, ABBYY Lingvo***). Сейчас стиль изложения автор считает

безупречным, ну разве с небольшими оговорками. Самое важное в [1] – это 2 леммы и 3 теоремы вместе с их доказательствами, которые были созданы ещё в 1995 году и которыми автор вполне доволен, поскольку перечитал их больше 4 раз, не найдя ошибок ни в 1995 г., ни годы спустя, когда перечитывал повторно в 2008 г. На этих леммах и теоремах держится теория «длинного триггера», но автору не удалось никого из людей подключить, чтобы его проверили, – как он теперь понимает, это происходило из-за банального «порочного круга» в системе рационального мышления современного человека, который привык ставить во главу угла экономию собственных усилий и инвестиций: чтобы кто-то стал разбираться в жутких и обширных дебрях чужой теории, этот кто-то должен быть уверен, что эта теория истинна, но как это установить без того, чтобы по-настоящему разобраться в её дебрях? Звучит запутанно, поэтому лучше обратимся к аналогии с «котом Шредингера»: чтобы узнать, жив кот или нет, необходимо открыть ящик. В рамках названной аналогии ситуация выглядит так: может и не хочется открывать ящик (тут – проверять теорию «длинного триггера», предпринимая сверхусилия без твёрдой уверенности в положительном результате), но нужно! В этом контексте роль прувера Coq в том, что он сводит сверхусилия к просто усилиям.)

Ввиду отсутствия желающих углубиться в дебри доказательств теории из [1], напрашивается идея поручить это компьютеру. Но только недавно (!) автор обнаружил, что подходящие для этого программы-пруверы уже есть – это Coq [2–5] и подобные.

Пруверы типа Coq используют не только (и даже не столько!) для доказательства теорем, хотя в этом отношении они очень мощные: успешными были попытки доказательства при помощи Coq задачи четырех красок, аксиоматической теории множеств Цермело-Френкеля, а также теорем из области математического анализа.

Помимо доказательства теорем, сейчас эти пруверы вовсю используют для создания сертифицированного программного обеспечения. Выглядит это (в идеале) так: сначала программист создаёт функциональную программу (встроенный в Coq язык функционального программирования называется Gallina, он похож на ML или Haskell), затем Coq доказывает её с помощью подсказок от программиста (называемых тактиками), а когда доказательство найдено, программа-робот переводит функциональную программу в императивную. Разумеется, тут от программиста требуется значительно большего таланта, чем обычно, но зато без человека как такового не обойтись (что не может не радовать в наш век тотальной роботизации!)

Имеется 7 факторов, которые предвещают удачу задаче поиска доказательства теории «длинного триггера» с помощью прувера Coq:

1) эта задача не слишком мала, чтобы её расценивать как тривиальное упражнение для студентов – за её решение, я думаю, полагается PhD****, а на поиск решения может быть запрошен научный грант или собраны средства путём краудфандинга (народного финансирования). В то же время задача не слишком масштабна, чтобы быть неподъёмной для одного человека или небольшой группы людей – в отличие, например, от задачи доказательства корректности полноценной операционной системы, которую из-за масштабности пока что не решили, хотя необходимость в подобном доказательстве назрела: продолжать использование существующих операционных систем с их ошибками и уязвимостями, от которых все страдают, становится абсурдом. Прувер Coq не позволит доказать корректность операционной системы, если в ней есть ошибки и уязвимости, а это нам подходит.

2) Теория «длинного триггера» раскрыта до мельчайших деталей,

заслуживающих внимания,

3) она полностью формализована, а также

4) она доступно и обстоятельно изложена на естественном языке.

5) Все сколько-нибудь сложные моменты доказательств выведены в форме структурной индукции, очень удобной для прувера Coq.

6) Теория переведена на английский – язык международного общения, который в совершенстве должны знать все специалисты, и

7) она доступна для свободного скачивания с репозитория препринтов arXiv.org.

К построению доказательства теории «длинного триггера» посредством программы-прувера Coq автор хотел бы привлечь энтузиастов. Почему не самому всё сделать? Аргументы такие: во-первых, он уже сделал достаточно для теории «длинного триггера»: создал её и опубликовал в виде статьи [1]. Во-вторых, за те 28 лет, в течение которых он ею занимался, он от неё, естественно, устал. В-третьих, у него есть другие проекты, требующие внимания. В-четвёртых, чтобы этим заняться самому, автору важно знать, что альтернативы этому нет (впрочем, глубокое освоение прувера Coq, необходимое для этого, любому вернётся сторицей!).

Выводы. Ранее созданная автором данной статьи теория «длинного триггера» (2008 г.) относится к построению mission-critical вычислительных систем. Несмотря на проработанность в деталях, она не имеет необходимой апробации ввиду сложности. Идея с апробацией в виде доказательства, получаемого от програмы-прувера Coq, представляется обоснованной, для этого имеются все необходимые предпосылки. Такое доказательство само по себе может заслуживать присуждения PhD, а также соответствующего гранта или краудфандинга. Приведение подобного доказательства впредь может стать стандартным требованием к апробации сложных теорий,

имеющих практически важное значение.

Примечания:

*Если говорить предельно обобщённо, то научная ценность теории «длинного триггера» в том, что удалось свести проблему проверки цифровых схем, имеющую экспоненциальную асимптотическую сложность, к константной сложности, т. е. $\mathbf{O}(\exp n) \longrightarrow \mathbf{O}(\mathrm{const})$. Кроме того, обычно «боятся» циклический графов и описываемых ими задач. Теория же «длинного триггера» не только «не боится» циклов, весь её эффект основан именно на циклах – как локальных, так и длинных. Сам по себе этот парадокс требует изучения. Практическая же ценность этой теории в том, что всегда полезно иметь в запасе возможность исчерпывающим образом проверять систему ещё одним способом, в данном случае – построив её как «расширенный длинный триггер». К сожалению, пока теория не прошла апробацию, в ней нельзя быть уверенным. Апробацией стала бы пробная реализация множества вариантов «длинного триггера» «в металле» и обширные физические испытания полученных изделий, но на это требуются немалые средства. Апробацией была бы проверка всех математических выкладок с участием классных математиков, но она не только накладна, но и не может нас по-настоящему удовлетворить теперь, когда появились программы-пруверы типа Coq: подтверждение прувером и дешевле, и надёжнее.

**Публикации в виде электронного препринта очень удобны для авторов. Особенно из-за того, что не требуется проходить процедуру «серьёзного научного рецензирования» перед публикацией. Трудно найти рецензента (в моём случае – вообще оказалось невозможно), который будет тратить своё бесценное время на то, чтобы углубляться в сложный объект рецензирования. Рецензенту проще придумать отписку и не рекомендовать к публикации, за это он ответственности

фактически не несёт. По крайней мере, две-три статьи автора были отклонены таким образом. Вспомним, что математик Григорий Перельман опубликовал своё решение проблемы Пуанкаре на сервере arXiv.org, и больше нигде. Перельман ждал проверки своего решения проблемы Пуанкаре много лет, и всё это время в серьёзных бумажных издательствах она бы лежала без движения, ожидая заключения рецензента, а рецензент мог быть случайным и дай Бог чтобы достаточно компетентным и добросовестным. В случае Григория Перельмана рецензирование было очень мощным (хотя и заняло 6 лет), поскольку он решил проблему Пуанкаре, входящую и в список Гильберта, и в список Математического института Клэя. В случае с теорией «длинного триггера» на такое внимание рассчитывать не приходится. Не будь arXiv.org... Важно и то, что arXiv.org – в отличие от бумажных издательств – не накладывает ограничений на объём статьи. Это позволяет всё изложить в деталях. Наконец, когда публикацию готовит сам автор, в ней минимум ошибок.

***Догадливый читатель поймёт, что статья [1] первоначально готовилась для публикации в виде веб-сайта. Так было проще опубликоваться, тем более – сразу на двух языках: русском и английском. И не было бы ограничений на объём материала. Для удобства читателей всё было раскрашено, таблицы и рисунки размещались в плавающих окнах, чтобы их можно было подтащить к читаемому фрагменту текста и иметь перед глазами, всё что можно было связано гиперссылками. Благодаря использованию CorelDRAW автор аккуратно подготовил довольно сложные рисунки. Чтобы упростить набор формул, он написал свой редактор формул (их дикое количество и они довольно сложные, хотя и похожи друг на друга – без своего редактора автор с этими формулами за разумное время не справился бы. Редактор представлял собой максимально заточенный

под проблему лёгкий веб-сервер под управлением Apache, серверная часть была написана на Perl, клиентская – на JavaScript. Для реализации почти всех операций в клиентской части удалось использовать активные ссылки – те, что начинаются с «javascript: ...»). Всё работало, однако следов посещения веб-сайта серьёзными читателями автор не обнаружил, по крайней мере в книге гостей за те несколько лет, пока сайт существовал, никто записей так и не оставил, кроме одного знакомого-шутника. К счастью, вскоре после создания сайта автор узнал о существовании arXiv.org и для публикации на этом репозитории препринтов за какие-то 2 дня преобразовал английский вариант статьи из веб-документа в PDF. Автор говорит это для тех, кто захочет воспользоваться его опытом создания электронных публикаций. Ещё необходимо сказать о переводе на английский язык. Автор считал, что неплохо владеет письменным английским, но когда прогнал свой перевод посредством ABBYY Lingvo на русский язык – ужаснулся: всё стало неправильно. Блестящий из-за своей простоты выход был найден: поняв, что всё связано с неоднозначностью языковых конструкций, автор перевёл всё по-новому, используя только те языковые конструкции, которые ABBYY Lingvo переводит на русский именно так, как автору нужно. Так сказать, авторский контроль backward-трансляции.

****Чтобы претендовать на PhD, Вы должны получить результат в одном из трёх вариантов: (1) при Вашей помощи Coq построил доказательство теории «длинного триггера»; (2) Вы доказали, что это доказательство построить невозможно; (3) Вы доказали, что в существующем варианте теория не может быть доказана, но если её изменить так-то и так-то, то Coq её доказывает. Вариант «я не смог её доказать» никого не интересует.

Литература:

1. Stukach, Nick (2008). Easily testable logical networks based on a «widened long flip-flop».

<https://arxiv.org/ftp/arxiv/papers/0808/0808.2602.pdf>. (2019, апрель, 08).

2. Coq (Материал из Википедии — свободной энциклопедии). <https://ru.wikipedia.org/wiki/Coq>. (2019, апрель, 08).

3. The Software Foundations. Volumes 1 to 4. <https://softwarefoundations.cis.upenn.edu/current/index.html>. (2019, апрель, 08).

4. О машинном доказательстве теорем. <https://itc.ua/articles/o_mashinnom_dokazatelstve_teorem_26341/>. (2019, апрель, 08).

5. Gonthier, Georges (2008), «Formal Proof—The Four-Color Theorem» (PDF), Notices of the American Mathematical Society, 55 (11), pp. 1382–1393, MR 2463991.

References:

1. Stukach, Nick (2008). Easily testable logical networks based on a «widened long flip-flop». Retrieved from https://arxiv.org/ftp/arxiv/papers/0808/0808.2602.pdf. (2019, April, 08).

2. Coq (From Wikipedia, the free encyclopedia). Retrieved from https://en.wikipedia.org/wiki/Coq. (2019, April, 08).

3. The Software Foundations. Volumes 1 to 4. Retrieved from https://softwarefoundations.cis.upenn.edu/current/index.html (2019, April, 08).

4. O mashinnom dokazatelstve teorem [On machine proving of theorems]. Retrieved from https://itc.ua/articles/o_mashinnom_dokazatelstve_teorem_26341/ [in Russian]. (2019, April, 08).

5. Gonthier, Georges (2008), «Formal Proof—The Four-Color Theorem» (PDF), Notices of the American Mathematical Society, 55 (11), pp. 1382–1393, MR 2463991.