# Six-year journey leads to proof of Feit-Thompson Theorem

October 12 2012, by Rob Knies

Georges Gonthier.

At 5:46 p.m. on Sept. 20, Georges Gonthier, principal researcher at Microsoft Research Cambridge, sent a brief email to his colleagues at the Microsoft Research-Inria Joint Centre in Paris. It read, in full: "This is really the End."

Those five innocuous words heralded the culmination of a project that had consumed more than six years and resulted in the formal proof of the Feit-Thompson Theorem, the first major step of the classification of finite simple groups.

The theorem, first proved by Walter Feit and John Griggs Thompson in

1963 and also known as the Odd-Order Theorem, states that in mathematical group theory, every finite group of odd order is solvable.

That might seem a deceptively simple definition to non-mathematicians, but Gonthier and his collaborators on the Mathematical Components project at the Microsoft Research-INRIA Joint Centre are anything but. Their achievement in completing a computer-assisted proof by the Coq proof assistant, developed at Inria, the French National Research Institute for Computer Science and Applied Mathematics, was acclaimed widely as news spread.

Michel Cosnard, Inria chairman of the board and CEO, was quick to commend the development.

"My deepest congratulations for this beautiful and amazing piece of work," he wrote. "Of course, Georges Gonthier and his team deserve our full consideration. But I would also underline the quality of the Microsoft Research-Inria partnership, which gave to them the absolutely necessary conditions for climbing this Everest."

Andrew Blake, laboratory director at Microsoft Research Cambridge, provided further detail:

- "Georges and his team at Inria have been working on this proof of the Feit-Thompson or Odd-Order Theorem for six years or so, since he completed his proof of the Four-Color Theorem. That might seem a long time for one theorem, but in fact:
- "It is a big theorem—the proof runs to two volumes. This is a large body of material to verify by eye—how much confidence can one have in that? Now the verification is substantially automated through the use of Coq.
- "Along the way, a good deal of the structure of finite-group

theory—textbooks of standard results—have been coded and verified.
- "All of this has also stressed the Coq proof environment and strengthened it, and Coq is also used for a multitude of verification tasks in security-critical code.

"One may anticipate that this could affect profoundly both computer science and mathematics."

As Blake mentioned, Gonthier, winner of the 2011 EADS Foundation Grand Prize in Computer Science, is no stranger to this sort of achievement. In 2005, he and Benjamin Werner completed a formal proof of the "Four-Color Theorem", the first longstanding mathematical problem to be resolved using a computer program. "In Formal Proof—The Four Color Theorem," published in December 2008 in *Notices of the American Mathematical Society,* Gonthier explained what was at stake.

"For some 30 years," he wrote, "computer science has been working out a solution to this problem: formal program proofs. The idea is to write code that describes not only what the machine should do, but also why it should be doing it—a formal proof of correctness. The validity of the proof is an objective mathematical fact that can be checked by a different program, whose own validity can be ascertained empirically because it does run on many inputs.

"The main technical difficulty is that formal proofs are very difficult to produce, even with a language rich enough to express all mathematics."

Now that he and his team have achieved a second mathematical theorem completely proved in Coq, he explains the background behind the six-year effort.

"Groups are very important objects in mathematics," Gonthier says. "They describe sets of symmetries, or reversible operations, and they have been used to explain the structure of nature, specifically how atomic particles combine and fall into various classes. They're also well-known in computer science, because group theory is the base for most cryptography schemes."

To illustrate the concept of "group," he refers to a common but challenging brainteaser.

"Think about a Rubik's Cube," Gonthier says. "It is a puzzle based on group theory, because the various operations you do when you turn the cubes around can all be reversed. If you do a couple of them, it all seems mixed up. But if you know a little group theory, you understand how to solve the cube.

"The Odd-Order Theorem precisely says that groups that have an odd number of elements are solvable. Finite groups can be factored somewhat like integers, though for a more complicated multiplication. The basic group factors, called simple groups, also come in many more shapes than the basic integer factors, the prime numbers. Solvable groups, however, can be factored down to primes, like integers. They're called this because they correspond to solvable polynomial equations."

## Innovation at Length

The proof by Feit and Thompson showed that groups with an odd number of elements are always solvable. It was shocking to the mathematical community at the time, because the proof lasted for 255 pages, a gargantuan effort that has proved to be quite mathematically innovative.

Now with the formal, computer-checked proof of the Feit-Thompson

Theorem, Gonthier and collaborators, most notably Laurent Théry and Assia Mahboubi of Inria, have extended the utility of the theorem.

"Because the formal proof can be computer-processed," Gonthier says, "we can get more information out of it. We can know that it's absolutely correct."

Gonthier describes his initial emotion upon completing the formal proof as "elation" and reports that he immediately began to contemplate a full night's sleep, which had proved difficult to obtain as the effort grew to a close. But clearly, it was a passionate pursuit.

"The work is about developing the use of computers as tools for doing mathematics for processing mathematical knowledge," he says. "Mathematics is one of the last great romantic disciplines, where basically one genius has to hold everything in his head and understand everything all at once.

"Computers have been gaining in math, but mostly to solve ancillary problems such as type setting, or carrying out numerical or symbolic calculation, or enumerating various categories of common natural objects, like polyhedra of various shapes. They're not used to process the actual mathematical knowledge: the theories, the definitions, the theorems, and the proofs of those theorems."

The possibility of doing so has been tantalizing but elusive.

"My work has been to try to break this barrier and make computers into effective tools," Gonthier states. "That is mostly about finding ways of expressing mathematical knowledge so that it can be processed by software."

The focus of the project was on developing tools for expressing

mathematics.

## One Step at a Time

"Ultimately, there were a number of intermediate goals in developing a good theory," Gonthier says, "first of all, observing pen-and-paper mathematics. I had much of that done by the time I'd completed the proof of the Four-Color Theorem. Then it was basic group theory, then algebra, then more advanced group theory, then character theory, and so on. There were lots of intermediate objectives, and we'd just move from one target to the next."

When Gonthier first suggested a formal Feit-Thompson Theorem proof, his fellow members of the Mathematical Components team at Inria could hardly believe their ears.

"The reaction of the team the first time we had a meeting and I exposed a grand plan," he recalls ruefully, "was that I had delusions of grandeur. But the real reason of having this project was to understand how to build all these theories, how to make them fit together, and to validate all of this by carrying out a proof that was clearly deemed to be out of reach at the time we started the project."

Along the way, he learned a few things—about formal proofs in group theory and about himself.

"Stubbornness pays off," he laughs, before reflecting on how the latest proof differed from his work on the Four-Color Theorem.

"The Four-Color Theorem proof I basically did on my own," Gonthier says. "Here, I worked with a team in more of a leadership role, and motivating the team was a new challenge for me."

Apparently, he proved sufficiently motivating. A couple of hours after Gonthier sent his original mail, Théry sent his own, providing a few facts about the project:

"Number of lines—170,000," he wrote. "Number of definitions—15,000. Number of theorems—4,300. Fun—enormous!"

Initial enthusiasm aside, though, the hope is that the formal proof of the Feit-Thompson Theorem could lead to similarly big results in proofs of programs.

"The Feit-Thompson Theorem," Gonthier says, "is the first steppingstone in a much larger result, the classification of finite simple groups, which is known as the 'monster theorem' because it's one of those theorems where belief in it resides in the belief of a few selected people who have understanding of it."

Source: Microsoft