Perio Interview
with Arthemy Kiselev

Zero-Knowledge Proofs,
by Time Travel
Bart Marinissen

Periodiek

Recurring Magazine | Issue 2019-1

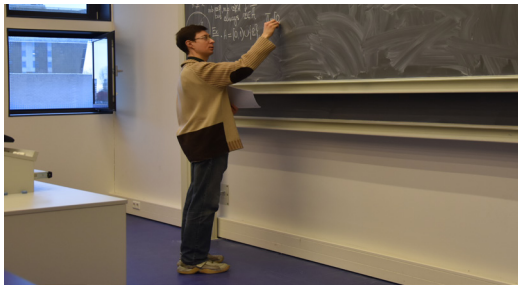
Event Horizon Telescope

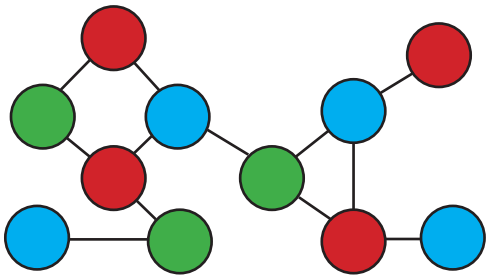
In the News:
Black Hole Picture

FMF

8 - Interview with Arthemy Kiselev

In this edition, Arthemy Kiselev is the participant for the Perio Interview. It turns out that the frequently seen lecturer likes making (and repairing) ovens and off-road driving. Find out where Kiselev grew up, what his scientific and personal interests are, and more.



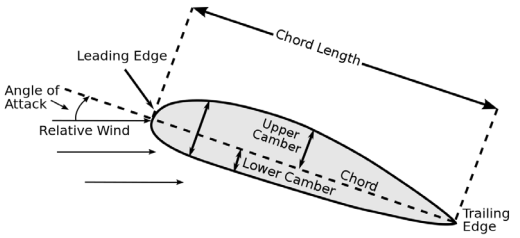


14 - Zero-Knowledge Proofs by Time Travel

How do you let someone know you know a secret without revealing *anything* about that secret? This is what is done in Zero-Knowledge Proofs. In collaboration with TNO we present you this fascinating article by Bart Marinissen.

18 - Study of the Joukowski Transformation for Medial Imaging Application

Valvular heart disease is still a big problem in industrialized countries. The geometry of the aortic valves cannot be described accurately by current methods, so new ways of diagnosing are being searched for.



In this Periodiek

Editors
Robert van der Meer,
Jonah Stalknecht,
Gerrit van Tilburg,
Jasper Somsen,
Robert Mol

Authors
Robert van der Meer,
Robbert Scholtens,
Samuel Galanakis,
Jonah Stalknecht,
Eva Ruitenberg,
Jasper Somsen,
Bart Marinissen,
Alden Waters,
Robert Mol,
Teke Xu

Advertisers
KxA (p.6),
ASML (p.12)
TNO (p.21)
Schut (p.28)

Advertise? Contact us at bestuur@fmf.nl.

Print run 1000 pieces

Press Drukbedrijf.nl

ISSN 1875-4546

The Periodiek
is a magazine from the Fysisch-Mathematische Faculteitsvereniging and appears three times per year. Previous issues can be found at perio.fmf.nl. The board of editors can be reached at perio@fmf.nl.

From the Editor in Chief

Regular visitors of the FMF throughout the past years will have noticed a difference between this year and the previous years: our beloved Bart is no longer present on a daily basis. Bart has started working for TNO. This Perio, in cooperation with TNO, we offer an especially long article by Bart for you to enjoy.

Personally, I am also very excited about this edition's Perio Interview. Professor Kiselev is one of my personal favourite professors at this faculty. His intriguing personality made me look forward to this interview. I hope you will enjoy it.

Jonah Stalknecht

In the News: Black Hole Picture

Event Horizon Telescope

On April 10th 2019 the Event Horizon Telescope collaboration released the first ever picture of a black hole.You have probably seen the picture by now, it has been all over the news and the internet since then. The black hole photographed lives at the center of the Messier 87 galaxy in the nearby Virgo cluster an approximate 55 million light years away, and has a staggering mass 6.5 billion times that of our Sun.

How the Picture Was Taken

Black holes are —as the name suggests— black, and are therefore quite difficult to photograph. Apart from the difficulty that there is not a lot of light coming from a black hole, this particular black hole only takes up only about 42 microarcseconds of the nights sky (which is about 10^{-8} degrees), which sounds absolutely tiny when compared to the 50.000 miliarcsecond resolution of the Hubble telescope. It took a team of over 200 scientists and eight telescopes in/on Antarctica, Arizona, Chili, Hawai, Mexico and Spain to achieve this milestone. All telescopes combined power in June 2017 to create one giant observatory which has astounding precision. In essence, using a technique called 'Very-Long-Baseline Interferometry', this setup can be thought of as a single virtual microwave disk, with a diameter spanning from Spain to Antarctica. VLBI is a method in which they measure the time difference between the detection of signals at every telescope using hydrogen masers atomic clocks, and then later recombining the data to create a coherent picture.

How the Data Was Processed

The telescopes recorded about 64 gigabits worth of data every second for a total of 5 petabytes of raw data. This was too much to transfer over the internet, so instead all the data was stored on hard

drives and these were physically transferred by plane to MIT Haystack Observatory and the Max Planck Institute for Radio Astronomy in Born. It took two years to process all this data, using an algorithm called 'CHIRP' (Continuous High-resolution Image Reconstruction using Patch priors). This algorithm was for a large part developed at MIT by the now famous Katie Bouman, who has become the face of the black hole picture.

"We have now seen the unseeable." —Avery Broderick

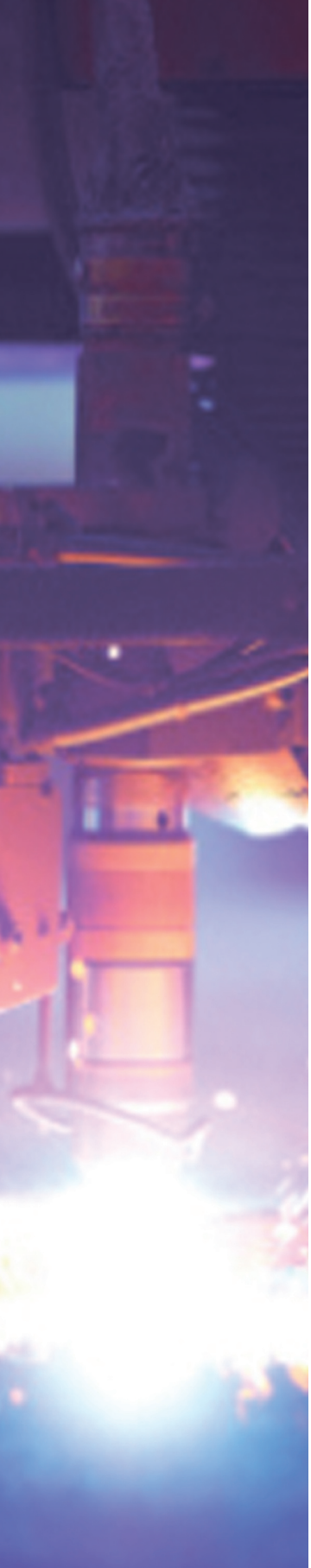
What We Really See

The black hole itself is not directly visible in the picture, since a black hole doesn't emit light. Rather, we see a ring of very hot gas that rotates around the black hole. Due to its enormous mass, spacetime is significantly warped around the black hole. As a consequence of this, light no longer moves in straight lines, but rather curves around the black hole. This means that we don't only see the front side of (the hot gas around) the black hole, but we can also see the back side, the top, the bottom and everything in between. The reason that one side of the picture is a lot brighter than the other side can be explained using the Doppler effect. Since the gas is rotating around the black hole, one side is rotating towards us, and the other side is rotating away from us. The side that is moving towards us, will have its light blue shifted, resulting in a higher intensity, while the side that is moving away from us has its light redshifted, which makes it dimmer.

What We Can Expect Next

We can expect more photos of black holes from the EHT. The black hole in the center of the Milky Way, Sagittarius A*, has also been a target of the EHT and we may see a picture of it in the near future. Though Sagittarius A* is 1000 times smaller than the black hole at the center of M87, it also about 1000 times closer, making it comparable in resolution. In April 2018 they already added a new telescope in Greenland to significantly improve the resolution power, and there are already two new telescopes that are waiting to join the collaboration. There is even talk of putting a radio telescope into space to help improve the resolution power even further.

NRAO/AUI/NSF



Creatieve software engineer?

Hou jij van afwisseling?

Zou je je willen specialiseren in Big data toepassingen?

Geïnteresseerd in de industrie, verkeer of zorg sector?

Ben je goed in programmeren liefst in c++?

Achtergrond in Natuurkunde, Informatica of AI?

Wij hebben vacatures voor zowel ervaren engineers als trainees.

KxA datasolutions is een innovatief bedrijf voortgekomen uit de astronomie, gespecialiseerd in data toepassingen en gevestigd op de grens van Groningen en Friesland. We werken aan veel verschillende dataprojecten. De ene keer houden we ons bezig met slimme datatoepassingen voor het verkeer de andere keer zijn we bezig met de optimalisatie van een fabriek of helpen we mee aan de ontwikkeling van een innovatieve windmolen of analyseren we onverwachte uitval in een fabriek.

Geïnteresseerd? Kom dan eens kennismaken.
Geen auto? Wij kunnen zorgen voor vervoer.

Geintereseerd? Bel of mail!

Wilma Mulder
mulder@kxa.nl
tel. 06 15347819

{kxa}
DataSolutions

From the Board

Commissioner of Education

AUTHOR: **ROBBERT SCHOLTENS**

Hello! I'm Robbert, the FMF's commissioner of education ("the education") for the academic year 2018-2019. Most of you will have probably seen me around, but probably don't have much of an idea of what I actually *do* for the association. With this piece, I hope I can shed some light on my jobs and responsibilities.

In a nutshell, I would define being the education means, for one, that I maintain the contact between the university/degree programs and the association. This includes attending meetings and thinking with them about how to improve the education. And secondly, I make sure there is sufficient study-oriented activities/facilities hosted within the association. Stating it like this, though, makes it a little vague; I'll concretize a little next.

For instance, for the first time this year the commissioner of education maintains the FMF's database of exams and has responsibility for the FMF's collective purchasing of study books. Both of these greatly improve the study-related character of the association; between mountains of material to study before an exam, and saving you money for other expenses you have.

Another thing I do is organize the catch-up sessions, which's usefulness you'll have encountered if you've attended one. In short, it's a lecture-styled talk in which a TA explains the material that's been treated in the previous five or six weeks of the course, so the student gets a good overview of what's the most important material. Although the planning is a challenge, the usefulness for the general student cannot be overstated.

And finally, I act as the liaison between the university and the association. Whenever they require the assistance of the association(s), I am the one who is emailed and asked to sit in on a meeting. During such meetings, I get to voice my opinion and constructively contribute to the issue at hand. These can range from discussing the potentiality of the kick-off week, to the Bachelor's project fair – which I then also (in part) host.

Despite all of these "main" tasks I have as education though, I want to stress there is a lot of opportunity for you to develop your own initiatives – more so than in any other board position, I would claim (with caution). There is a lot of room for initiatives, both with regards to the university and the assocation. In my experience, both are very open to any idea for improvement you can offer, and this makes for a very stimulating environment.

In short, I think that doing board of the FMF as the education has been a great boon for me, due to the contacts I've obtained within the university and the gained experience in organising a variety of events. It's a position with a lot of variation, and that's what I like.

And, of course you can end the day on the couch with a beer, as the education does.

Have a great time!•

FIGURE 1: Robbert having a great time.

Perio Interview: Arthemy Kiselev

The participant in this edition of the Perio Interview is Dr. Arthemy Kiselev. Kiselev is well known among students for teaching both mathematics and physics courses. Continue reading to discover where Kiselev grew up, what his scientific and personal interests are and more. An even more elaborated version of the interview can be found here!

Where did you grow up?

I was born and grew up in Ivanovo, an academic city in Russia counting seven universities. This city is located approximately 300 kilometers from Moscow. After graduating school when I was seventeen, I went to Moscow to study at university level.

I grew up in a big and friendly family of classical intelligentsia. Such people, be they university professors, hospital doctors, high-skilled engineers, or writers and filmmakers, set a life goal to create, preserve, and disseminate fundamental and cultural knowledge about Nature and mankind. In the family, I belong to the third generation of this tradition: everyone got a university education, and almost all hold a PhD degree (or PhD + Dr.Sc.) and other professional titles.

Which universities did you attend to?

In Moscow in the mid-1990s, I did my studies at two universities in parallel. I had also passed cruel entrance exams & interview to the theoretical physics track at the renowned FOPF faculty of FizTech (where, by the way, students join research labs already in the second year of study), yet I chose mathematical physics at Lomonosov Moscow State University and pure mathematics at the Independent University of Moscow. At the Moscow State University, most of the classes had to be attended. Classes were given between 9:00 and 16:35 (also on Saturdays). In the evening hours, I studied at the Independent University of Moscow. Here the classes started at 17:30 and finished at 21:05. Attendance here was voluntarily. Combining these two studies was rare and a unique experience, with a 'red-cover' diploma[1] at MSU. In three years (2001-4), I then wrote and defended the PhD dissertation on geometry of nonlinear PDE.

And at which universities did you work?

Just have a look in my CV. Brock, Montreal, METU Ankara, Utrecht, all of them with assistant, then associate professorship at ISPU (Ivanovo, Russia) at the background. Good to know: ISPU is formerly the Riga Polytechnical — until July 1917, when the city was ceded to the Kaiser during WWI.

Besides universities, there are research institutes. You may go there after a PhD defence, for example. Such are the Max Planck Institutes in Germany, CRM (Montreal), SISSA (Trieste), and Institut des Hautes Études Scientifiques, which is a European analogue of IAS in Princeton. Visitor grants from MPIM Bonn and IHES in Bures-sur-Yvette are extremely competitive. Staying there teaches you a lot; in both 2016 and 2017, I was the only visitor invited to the IHES from the Netherlands.

[1] *Red-cover diploma* means that all grades were 9.5 or 10, so it is equivalent to receiving a summa cum laude diploma at the RuG today.

What do you consider to be your field of research?

The mathematics of physics. Specifically, design and development of geometric and algebraic tools for the study of models for the quantum world. For the past 12 years or so, I have been working on a set of problems posed by Maxim Kontsevich (Fields medal 1998) at the IHES. Much of what I do goes in cooperation with my students.

What is your favourite equation?

In fact, two: $E = mc^2$ and $e^{i\pi} + 1 = 0$.

Did you have any dream jobs as a kid?

It was in 1984, I presume. At that time, the administrative paranoia was not about running bankrupt, hence losing daily comforts, but about being attacked suddenly by enemies. Growing into a leader who guides and inspires mob in a casino was not yet actual. I was in kindergarten and we were lined up as a queue of boys. An animatrice asked everyone: "Who do you want to be in the future?". The compulsory responses were: "I want to be a fighter pilot." or "I want to be a tank driver." Some less loyal ones responded they wanted to be artillery officers. I perhaps spoilt the statistics by saying that in the present circumstances, I wanted to be a retired person.

Do you think a theory of everything can be established?

Young Max Planck came to Philipp von Jolly, his advisor, and informed the maitre that he wanted to specialise in theoretical physics. 'Why would you spoil your life?' replied the professor. 'In this field, almost everything is already discovered, and all that remains is to fill a few unimportant gaps.'

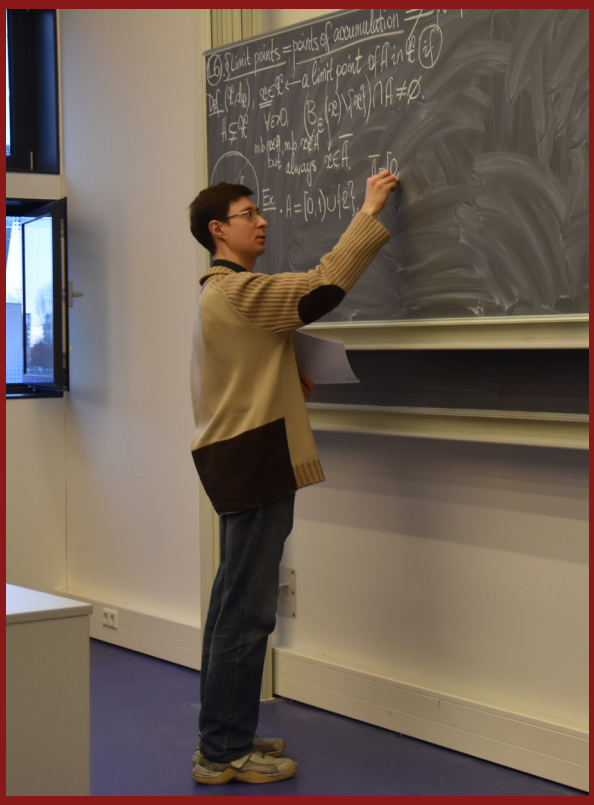


FIGURE 1: A.V. Kiselev lecturing in the course Metric Spaces.

In which field do you think a theory of everything would come from?

If it did. Nevertheless,

"A biologist thinks she is a biochemist.

A biochemist thinks he is a chemist.

A chemist thinks she is a chemical physicist.

A chemical physicist thinks he is a physicist.

A physicist thinks she is Almighty God.

God thinks He is a mathematician."

(quoted from the rector of Bonn University)

What is the most interesting recent scientific development according to you?

Your own one! The discovery which you achieved either entirely by yourself or in collaboration with colleagues (perhaps senior). Please do not hesitate to share your experience and achievement at colloquia or conferences.

It is amazing how, through communication between people and disciplines, seemingly distant topics get interconnected. For example, my PhD student has been working on the expansion $\star \bmod \bar{o}(\hbar^4)$ of the Kontsevich star-product. He communicated a gigantic list of relations between the coefficients arising at $\hbar^5$ and $\hbar^6$ to a team in Oxford, and on 31 December 2018, our colleagues not only announced the next, higher order formula but also related the values of sought-for integrals to polylogarithms and multiple zeta values. Who could foresee? Indeed, where is deformation quantization and where the Riemann ζ!

The reverse side of your question is that, we learn, certain fashionable theories did not work. Literally billions were spent, still under the nearest lantern no purse was found. Such 'scientific closures' are very interesting developments. Circular inertial motion and epicycles give you fantastic precision for celestial mechanics. There is no phlogiston, still there are the Watt and Stirling engines. Maxwell derived the equations for vortices of aether, which there isn't. Likewise, Kelvin viewed the periodic table as classification of knots. You could name a concept or two. This is the pace of science: we try and discard many models before one of them pays off.

What makes a good lecture?

Severe selection and time-planning before, dialogue during, and bright ideas after.

What do you think that are three books that everyone should read? And why?

Books that 'everyone should read' are likely the ones which we adults keep reading to a child. "Winnie-the-Pooh" and "The House at Pooh Corner" by Milne. "Moomintroll" by Tove Jansson and "Karlsson-on-the-Roof" by Astrid Lindgren. "Brother Rabbit" by Joel Harris. The true love of quantum field theorists, Snark and Alice.

If you do read for your own pleasure and thinking, great! I often re-read Bulgakov's "Master and Margarita", "The good soldier Švejk" by Hašek, and "The snail on the slope" by Arkady and Boris Strugatsky. To a scientist, "Summa technologiae" by Stanislaw Lem would be inspiring.

'Why?' is a very important question. A while ago, a grant agency asked me why certain scientific results are more important than others, and how that agency could decide at once — what is the indicator; where to look at? Their provisional idea was the sum of money promised as a prize for achieving a particular result. I argued that the significance is expressed quantitatively, i.e. the way they sought, by the number of years a result is remembered and considered significant. Same it is with books: what makes a masterpiece eternal? Recite Orwell, Kafka, Solzhenitsyn.

"One hobby of mine is making and repairing ovens, another one is off-road driving"

What are your hobbies or interests?

One of my hobbies is ceramic brick masonry, especially making ovens. It is my hobby to build and repair these ovens in Russia. I started repairing brick ovens when I was about 12 years old and now I own one (picture). In Russia, there are two common types of ovens. The so-called Dutch oven and the Russian ovens. A Dutch oven is smaller in size and purely for heating. A Russian oven is quite big in construction — one of the ovens I made consists of 2000 yellow, heat resistant bricks — and could be used for both cooking and heating. Also, a platform on top of it could be used to sleep on. Heated bricks have a temperature between 60 and 90 degrees. Laying down on them has a healing effect because of the warmth, which is for example good for people with Rheumatism.

Another hobby of mine is off-road driving, on roads like in the figures. I own a four-wheel drive and a city car. I drive on roads which are damaged by wood transport from the forest. These roads are designated on maps, therefore very strictly speaking it is not off-road driving. If the car get stuck I use a handcraft to

FIGURE 2: Off-road driving is one of the hobbies of Dr. Kiselev. ''There is more than one way towards a solution of the problem.''

FIGURE 3: Another hobby of Dr. Kiselev is making and repairing ceramic ovens. ''Renewable, sustainable bio-energy is guaranteed at efficiency 98-99% by the on-the-edge (of extinction) technology.''

pull it out of the mud. A metal cable can be attached to the nearest tree and you also need to cut a tree and put pieces of wood under the tires of the car.

Equally am I interested in reading and cinema: at the IHES (or as it was done in Utrecht, when I was a VENI postdoc), we regularly watch and discuss Buñuel, Tarkovsky, Kurosawa, or for instance "The third man", "Subway", and "Le manuscrit trouvé à Saragosse" from the 7th Art by Wojciech Has, etc. There is an inner and social request for culture, you see?

What kind of music do you like?

Applied classics: for mobile phones (Vivaldi, Mozart), for large squares and volumes (Bach, Beethoven, J.-M. Jarre), for off-road car control (Strauss), for elevators (Louis Armstrong, Ben Webster), or student lullabies (The Beatles, Nautilus Pompilius, Vangelis). As well as the vocalists: Bulat Okudzhava, Yuliy Kim, Mikhail Shcherbakov.

What did you have for breakfast?

I start with a good breakfast, have a good lunch and small diner. For breakfast I had a glass of carrot juice, two soft-boiled eggs, a slice of crude rye bread, two pieces of bitter chocolate, a walnut, two apricots, a kiwi, and a handful of rowan berries (Sorbus Aucuparia).
This is not my everyday breakfast. One has to change, using e.g. a four- or five cycle.

If you would have to choose between 'during every lecture a person is cutting a kilogram of onions on the first row' or 'every lecture has to be given in front of a whiteboard with a marker that does not work entirely well', what would you choose?

In fact, I am very grateful to this university, which helped me to find experimentally an answer to this question. Several years ago I was reading one of my courses where exactly this — although not with onions — situation did occur with somebody who was sitting on the front row. That student had his lunch during my lecture. It was a full meal: a soup, some dishes with potatoes, meat and vegetables, a bottle of soft drink and a cake. That all happened at the moment when everybody in the audience was hungry.
My duty as a lecturer is that something remains in the heads of the students. So if quite some time passes, then it would not matter that there were onions in the room. It matters that the presentation was accessible and that there was a good blackboard I suppose. Also, people far away from those onions could still survive. Note that markers are also stinking. So if I had to choose between stinking markers which are synthetic and stinking onions, which are natural, well, nobody has yet died from the smell of onions.

ASML: Knowing how to code is not enough for career success

ADVERTORIAL BY ASML

Software development skills are in demand, as any quick scan of online job boards will confirm. But the people doing the hiring have an important piece of advice: knowing how to code isn't enough for long-term career success. The developer skill set is changing.

"Software engineering is about abstraction and structure," says Jan Friso Groote, professor in Computer Science at the Eindhoven University of Technology (TU/e). "The real problem of software is that it is so immensely complex that if it is not well structured, it becomes unmaintainable." As a result, the most important skill of a software developer isn't writing code and testing it until the bugs are quashed. It is understanding the essence of a problem and building a structured, reliable, extendable and maintainable approach for solving it.

For development teams who have taken this approach to its logical conclusion, it means that software engineers write very little traditional code. They spend most of their time working in abstract modelling languages, specifying the behavior of a system. Formal verification tools allow those teams to be confident

that their solution is complete and error-free, and the code itself is then automatically generated.

With such a model-driven engineering (MDE) approach, a team at ASML recently replaced half a million lines of code that had been built the conventional way. “When we made this change to our software, it was a challenging period and a lot of energy was needed from our software engineers,” said David van Beek, who leads a group of software engineers at ASML. “We really grew as a group and as a department. We continue to grow now, and we need developers with this energy and drive to ensure we continue to produce a clean and extendable design in the years ahead.”

It’s not surprising that companies like ASML are embracing model-driven software development. ASML makes equipment for chip manufacturing. All of the world’s leading makers of processors and memory chips are using ASML’s lithography systems to create the nanometer-sized electric circuits found on modern chips. These are some of the most sophisticated machines ever built, so the demands for the software that runs them are high.

Rogier Wester, manager of the Lithography Systems Software Architecture group at ASML, said he looks for candidates who demonstrate abstraction skills, who understand the essence of the problem and are still able to create simple solutions. This is because complex solutions do not usually work and even if issues do not crop up immediately, bugs will still appear when customers start to use the product.

This requires developers to think in a very different way. “Think about what will go wrong. Divide and conquer. Use models for abstraction and conciseness. Use appropriate tools, that allow you to refactor and change with confidence,” Wester said. “We need very skilled software designers and, in my honest opinion, we see the challenge for the universities to offer an integral computer science education on software architecture and design, abstract modeling, and formal specification and verification,” he added.

Know more about Software at ASML: workingatasml.com•

Zero-Knowledge Proofs, by Time Travel

AUTHOR: **B MARINISSEN**

One of the more exciting developments in cryptography is the creation of practical 'Zero-Knowledge Proofs of Knowledge' (ZKPoK). These allow you to convince someone you know a secret, without revealing anything about that secret. They are used in practice by systems that need to verify personal information, but want to keep it private. Examples would be a system for logging in without revealing your password or username.

Former member and known face within the association Bart Marinissnen wrote an article relating to his work at TNO: An introductory explanation of Zero-Knowledge Proofs.

Another example is the crypto-currency Zcash, which uses these proofs to hide the value, sender and recipient of a transaction, whilst still verifying the sender owns what he is sending, and no value is destroyed or created. However, it is hard to find a good introduction to Zero-Knowledge Proofs of Knowledge[1]. The subject does not require much technical knowledge. We will only need a very brief incursion into complexity theory. However, there are some tricky 'time reverting' arguments. These don't require special knowledge, but they are hard to get your head around. Moreover, we have a paradox to deal with: we need to prove we know something without revealing anything.

To start with, we will give a practical example of a ZKPoK, with an outline of why it should work. That'll include a first look at the time reversing arguments. Then, we want to generalize this to ZKPoKs in general. To do this, we need an answer to the questions "What is knowledge?"[2] and "What is a secret?". We will answer these with a quick foray into complexity theory[3]. With these answers, we can then say what it means to 'prove knowledge' without 'leaking knowledge'. We end with another example of a ZKPoK. Showing it really is a ZKPoK is left as an exercise to the reader.

[1] A good one is the blog post by Matthew Green: 'Zero Knowledge Proofs: An illustrated primer' which forms the basis of this article. Notably, our example is directly adapted from that blog post.

[2] Apologies in advance to the field of epistemology, which we have completely swept aside here. Please do note that it is only *a* definition, not *the* definition.

[3] Apologies in advance also to anyone familiar with complexity theory, we will *not* give an introduction to the field, just borrow some notions.

Paperclips and radio towers

Our example starts with the company 'Paperclips inc.'

They have a network of radio-towers with overlapping range. They don't want two towers with overlapping range to interfere with each other, so they decided to use 3 different frequencies. Figuring out a way to assign these frequencies is hard.

Paperclips inc. have hired us to solve this. For our sake, we will assume that this is a solvable problem, and that we have found such a solution. All that is left is to complete the transaction. However, 'Paperclips inc.' does not want to pay us unless they are sure we have a solution. But, as a matter of principle, we do not deliver until we have been paid. This seems to leave us at an impasse. (For the sake of this article, we will ignore the option of a trusted third-party.) Luckily, we can solve this with a ZKPoK (and a whole lot of paper and crayons).

FIGURE 2: The product of Paperclips inc.

"We need to prove we know something without revealing anything."

First, we transform this into a graph-theory problem. Let each tower be a node in a graph. If two towers have overlapping range, place an edge between those nodes. We represent the frequency of a tower by a color of the corresponding node. Then, two towers interfere if an edge has the same color at both ends. Thus, we have to find a coloring of the graph where this does not happen, whilst only using 3 colors. This is called the 3-coloring problem.

In general a ZKPoK is a protocol with two roles a Prover (us) and a Verifier (Paperclips inc.). The protocol consists of rounds of the following three steps:

- The Prover (us) sends a randomly chosen *commitment* to the Verifier.
- The Verifier (Paperclips inc.) sends a randomly chosen *challenge* to the Prover.
- The Prover gives a *response* to this challenge, which the Verifier can check.

We say someone is a 'True Prover' if they can always give a correct response to the challenge. As we will see, it is paramount that the commitment is made *before* the challenge is chosen.

The idea is to have as many rounds as needed to convince the Verifier. All the while, we don't want to leak the secret.

Our first attempt uses permutations of the colors to hide the real solution. In a permutation we swap the colors around.

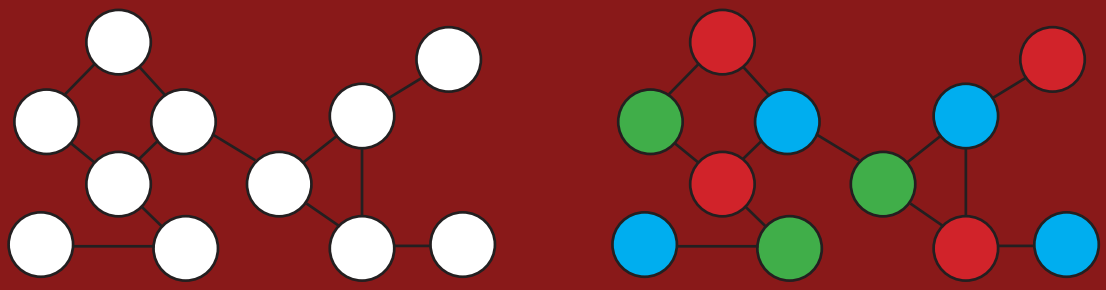
For example, we might color all red nodes green, green nodes red, and leave blue nodes blue. The idea is that you cannot trivially combine two partial views of the graph if they used a different permutation of colors.

The protocol would be as follows:

- We pick a random permutation, apply it to our solution, and color in the entire graph on paper. Then, we cover each node with a lid, and let Paperclips. inc into the room.
- Paperclips inc. get to choose 10% of the edges in the graph.
- We reveal the nodes at the end of those edges.

In any round, Paperclips inc. gets to see whether our coloring works for the edges they chose. Note that our commitment is *binding*. If we try to change the colors after Paperclips inc. walks in, they will spot us. This prevents us from changing the colors after we know their challenge. This protocol actually does leak information about the solution, but we will get to that later.

FIGURE 3: An example of a graph (left) and a valid 3-coloring (right).



For know, lets see why this is a Proof of knowledge. That is, lets show that Paperclips inc. should be convinced after enough rounds. For this, we will use a 'time reversing' argument. Specifically, we will build an *Extractor*. This is a method for extracting the secret from any true Prover. All this method needs is the ability to 'reverse time' for the Prover.

The method works as follows:

- Let us color in the graph.
- Ask to see 10% of the graph.
- Roll back time to after we colored in the graph.
- Ask to see another 10%.
- Repeat 10 times.

Since you cannot extract knowledge that is not there, this shows we must really know the secret. At first glance, this is undermined by the impossibility of time travel.

However, we can run this Extractor on ourselves without time travel. Rolling back to a point is just a matter of pretending things after that point did not happen. This means any true Prover is able to extract the coloring from themselves. Hence, they must know the coloring.

This is is very convincing to us, but why would Paperclips inc. be convinced? The trick is that every round, they get to test whether we are a true Prover. At best, a trickster has a 9 in 10 chance to pass this test (presuming they can make a coloring with only a single random wrong edge). Hence, for 99% confidence, Paperclips inc. will demand 44 rounds ($0.9^{44} \approx 0.01$).

Besides the massive waste of paper and crayons, this protocol is not perfect. Paperclips inc. can extract the coloring without needing a time machines. They can reverse engineer our permutation by asking for the same edge in different rounds. If at first you saw a red and green node on the edge, and you saw a blue and red node after, you can determine the whole permutation. So, if they pick a special edge and ask for it in every round, they can combine all our answers.

We can fix this leak with the following insight: In order to learn the permutation used, the attacker needs to see an edge he already saw. But until he sees *another* node that round, he does not learn anything new about the coloring. So, we will only let Paperclips inc. query a single edge per round. This leaves them two options in a round: query an edge they saw before and learn about the permutation used, or query a new edge, but without knowing the permutation that was used. Neither option will help them find a correct coloring.

So our new protocol is:

- We choose a random permutation, apply it and color in the graph.
- They pick a single edge.
- We reveal the colored-in nodes at the end of that edge.

The same Extractor still works, you just need to

roll back time once per edge rather than 10 times. Remember though, time travel is not possible. Thus, a Prover does not need to worry the Verifier will use an Extractor on him.

Note that the chances of catching a cheater in a single round went down. Given N edges, the chance of getting caught is $1/N$. For a 99% certainty, this means we need roughly $4.605 \times N$ rounds (we use $4.605 \approx \ln(100)$ and $\ln(1 - 1/N) \approx -1/N$). This is bad news for trees, and whatever crayons are made off. But, at least our secret will be safe. To see that indeed, this does not leak any info, we use another time reversing argument. We will build a Simulator, that gets the ability to reverse time for a Verifier. This Simulator will generate a Prover-Verifier interaction that is indistinguishable from the real thing (from the point of view of the Verifier).

The Simulator works as follows:

- Make a commitment randomly (just assign a random color to each node).
- Let the Verifier make a challenge.
- If we happened to randomly assign different colors to the ends of that edge, great.
- Otherwise, reverse back time until before the commitment and try again.

Note that this gets around the requirement that a commitment must be made *before* the challenge is decided. This is how it is possible to make a Simulator without knowing the secret.

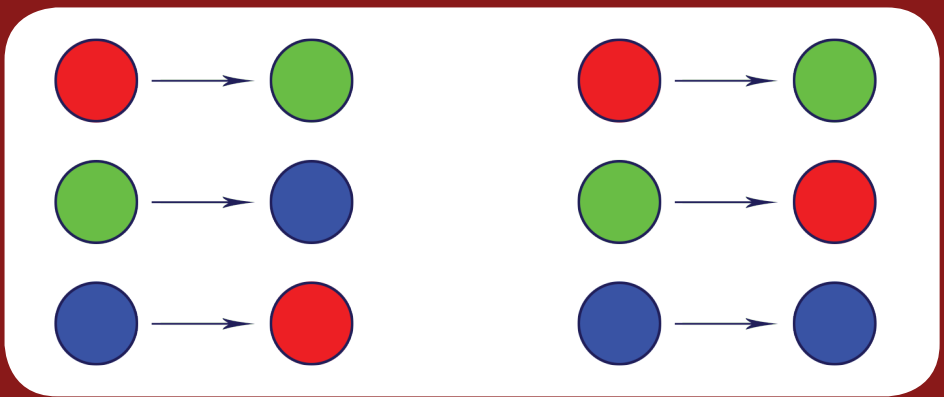
From the perspective of a Verifier, this looks totally convincing. Now, it is obvious a Verifier could not learn about the coloring from this interaction. After all, the Simulator does not know the coloring either. In some sense, this means a Verifier does not learn about the coloring from a real interaction either. After all, the interaction with a Simulator is indistinguishable.

Still, time travel taints the above argument. However, just like before, a Simulator is useful without time travel. Anyone could take the role of Verifier, and use the Simulator on themselves. Again, rolling back time for yourself is a matter of pretending to forget. The interaction we generated here is indistinguishable of a true interaction. However, we generated this interaction without any knowledge of the coloring. Thus, neither the generated interaction, nor the real interaction can contain any information about the coloring.

This also means that anyone watching a Prover and Verifier interact is not convinced the Prover knows a valid coloring. After all, they could have colluded before-hand, generated a fake transcript with the Simulator, and are now just replaying this transcript. Still, participating in the interaction with a real Prover *does* convince a Verifier the Prover knows the secret. This goes back to the requirement of committing *before* the challenge is made. The Verifier, who makes the challenge, knows it was made *after* the commitment. Anyone watching does not.

Now, we want to generalize these concepts of a Simulator an Extractor. Before we do that, we need a more precise definition of 'Knowledge'.

FIGURE 4: Color permutations



What is Knowledge, and Other Million-Dollar Questions

We have now seen an outline of the arguments for why a protocol might be a Zero-Knowledge Proof of Knowledge. To flesh out those arguments, we need to get a better idea of what it means to have or gain knowledge. Or rather, we need to come up with some kind of definition of having and gaining knowledge. We will do this based on the famous million dollar question of P vs NP from complexity theory. Now, this will not be an introduction the field of complexity theory. We are just going to quickly borrow some concepts. For a true introduction, the Wikipedia page on P vs NP is pretty good.

A naive definition of complete knowledge of some secret might be: having access to the secret on some kind of storage. It might be on a USB stick, in your memory, or written on a piece of paper. This is not sufficient though. It might be possible to have enough information to compute the secret, but not have the actual value stored. We still consider this knowledge. For example, if I tell you I have a secret number that it is even, and prime, you essentially know my secret number, but you don't have it stored anywhere.

As a fix, we might say the knowledge is 'being able' to compute a certain value. This matches with the definition of an Extractor. We would then say gaining knowledge is making it 'easier' to feasibly compute a certain value.

"If I tell you I have a secret number that it is even, and prime, you essentially know my secret number, but you don't have it stored anywhere."

One issue though, is that we want 'able to compute' to be practical. In fact, in our example of graph coloring, Paperclips inc. is technically 'able' to compute a solution themselves. All they need to do is try all 3^N possible colorings (N being the number of nodes in the graph) and see if one is valid. However, for 100 nodes, this is already totally and completely infeasible. Thus, we want to say something like: "knowledge of a secret is 'feasibly' being able to compute it".

This is where complexity theory comes in. It gives us a rigid framework for defining 'feasible' computation.

Simple complexity theory deals with *decision problems*. These are simple yes/no questions about an input. Generally, they ask whether an input meets certain criteria.

Some examples would be:

- Is this number prime?
- For this triple a, b, c does $a + b = c$?
- Is this a valid 3-coloring of a given graph G?
- Does this graph have a valid 3-coloring?
- Is this logical proof correct?

We can then classify decision problems by how easy they are to check. In complexity theory, we have the class of decision problems P. This stands for 'Polynomial time', rather than explaining what this is, suffice it to say that 'Polynomial time' problems are considered feasible to compute.
Some examples would be:

- For this triple a, b, c does $a + b = c$?
- Is this a valid 3-coloring of a given graph G?
- Is this path from a to b the shortest path in graph G?
- For this triple a, b, g is g the greatest common divisor of a and b?

Next, we need the class of NP decision problems. This does not mean non-polynomial time. Instead, it means 'Non-deterministic Polynomial time'. That name comes from the original definition of NP. We will use a different (but equivalent) definition. We characterize NP problems as 'existence' problems that are feasible to *verify*. More precisely: these are decision problems, where every input X maps into a new decision problem I_X called an instance of the problem. We demand that the instance is a P problem. Any input y accepted by the instance I_X is called a 'witness' to the instance, The over-arching problem only accepts an input X if a witness for the corresponding instance I_X exists. This is where the term 'witness' comes from. By producing a witness, you 'testify' that X should be accepted.

The requirement that I_X is a problem from P is why we say these are 'easy to verify' problems. Checking a witness is easy to do.

Some examples for NP problems would be:

- Does the graph X have a valid 3-coloring?
  - A witness would be a valid three-coloring
- Are the graphs $X = (G, H)$ isomorphic?
  - A witness would be an isomorphism.
- Is this number X not prime?
  - A witness would be a factorization of X.

Every problem in P also lies in NP by definition of NP. (For a problem A in P, and any input X needs to decide on, set $I_X = A$) Whether every problem in NP also lies in P is an open question, called P vs NP. It is one of the millenium problems. As such, solving it will net you $1 000 000.

Lucky for us, it is widely assumed that $P \neq NP$. The problems that lie in NP but not in P are easy to compute, but hard to verify. Our definition for knowledge of a secret will only work for these problems.

"Solving it will net you $1 000 000."

We presume there is some instance of an NP problem that is known to all parties. The 'secret' a Prover knows is the witness to this instance. By knowledge of a secret, we mean the ability to feasibly compute it. That is, we want the secret to be computable in Polynomial time. This is related to the complexity class P, but not a decision problem.

Zero-Knowledge Proofs of Knowledge in General

First, let us set the stage. There is a Prover, who knows a secret. Specifically he knows a witness for a certain instance of an NP problem. There is also a Verifier, who knows about the instance of the NP problem. The Prover wants to convince the Verifier he really does know a witness, but he does not want the Verifier to gain any knowledge about the witness.

We will do this with a Zero-Knowledge Proof of Knowledge. This is a protocol that has 3 properties: completeness, existence of an Extractor, and existence of a Simulator.

The completeness requirement has been implicit so far. It means that no matter what witness a Prover knows, he will always be able to convince a Verifier. That is, the set of things you can prove completely covers all things you might want to prove.

Moreover, there must exist an Extractor algorithm. This is a feasible (i.e. polynomial time) algorithm that should produce the 'secret' witness. In order to do this, it is allowed to interact with and 'roll back' a Prover. Completeness, and the existence of an Extractor together make a protocol a Proof of Knowledge.

Finally, there must exist a Simulator algorithm. This is an efficient (i.e. polynomial time) algorithm that is allowed to interact with and 'roll back' a Verifier. The requirement for a Simulator algorithm is to be statically indistinguishable from the point of view of the Verifier[4].

Both the Extractor and Simulator have this strange 'rolling back time' ability. The idea is that a true Prover can use an Extractor on himself without needing time travel. Similarly, anyone can take the role of Verifier and use a Simulator on themselves without time travel. All that is needed to roll back yourself to some moment is to ignore anything that happened since that moment.

Now, if a true Prover runs the Extractor on themselves, they have computed the witness. Hence, by definition, a true Prover knows the witness.

Similarly, if anyone uses the Simulator on themselves, they generate an interaction that is indistinguishable from the interaction with a true Prover. So, suppose we can use the interaction with a real Prover to

[4] A correct Verifier or any possible machine? This gives the difference between 'honest verifier' and 'perfect' zero-knowledge. An important difference we don't have the time to get into. Rest assured that our example is perfect zero-knowledge.

'help' compute the witness. We could duplicate this improvement by simply generating a fake interaction through a Simulator. After, all, that creates an indistinguishable interaction. But then, we could have gotten the same improvement without the real interaction. Thus, we don't gain any knowledge from the real interaction.

Meanwhile, if you are a Prover, you don't need to worry about the Verifier using an Extractor on you, unless he has a time machine. At the same time, a Verifier is sure he is talking to a real Prover, because he *knows* he made his challenges *after* the commitment. All that is needed are enough rounds for this confidence to become high enough.

Wrapping it up

After all this, we should have a decent understanding of how and why Zero-Knowledge Proofs of Knowledge work. Moreover, we have seen an example of such a system. Interestingly, it turns out our system is actually universal. That is, our system could be used for any instance of an NP problem, not just the three-coloring problem. This is a consequence of three-coloring being a so called 'NP-complete' problem. This means any instance of an NP problem can be (efficiently) translated into an instance of the three-coloring problem. Our system was not very efficient though, requiring 4.605 times as many rounds as there are edges in the graph. Moreover, our system is rather physical. We need actual paper, crayons and lids for the commitment. Notably, there are cryptographic techniques that are able to make this commitment in a digital manner.

It should be noted that, by our definition of Simulators and Extractors, a ZKPoK must be interactive. Moreover, an interaction was not convincing to any onlookers, since they cannot confirm the commitments were made *before* the challenges. In practice, it would be nice to have non-interactive Zero-Knowledge Proofs. You could just publish these, and let it be known to the world you know some secret, without revealing what this secret is. For this, we have the Fiat-Shamir transform at our disposal. Here we take an interactive Zero-Knowledge Proof (where challenges are made *uniformly* at random) and make it into a non interactive one. This is what is meant when people talk about non-interactive Zero-Knowledge Proofs. In short, this works by making all commitments in advance, and using a hash-function to derive the challenges from the commitments.

Our example is a nice illustration, but is not very efficient. More practical schemes do exists. Most notable are ZK-SNARKS, ZK-STARKS, and Bulletproofs. These are very efficient non-interactive ZKPoKs. The classic example of a ZKPoK is Schnorr's protocol. Schnorr-signatures are essentially the non-interactive version of that.

Another example

Finally, I leave you with another ZKPoK. This is for the NP problem of graph isomorphism. That is, we have the question "Is this pair of graphs G, H isomorphic?" A witness would be an isomorphism between G and H.

The protocol proceeds in rounds of the following:

Commitment:
> Generate a new graph A by randomly relabeling the nodes of G or H.

Challenge:
> Verifier picks either G or H

Response:
> Show the isomorphism between A and G or H as chosen by the Verifier.

Proving it really is a ZKPoK is left as an exercise to the reader. Remember, you need to show completeness, and construct an Extractor and a Simulator.

INNOVATION NEEDS VARIATION

At TNO countless specialists from so many different fields join forces in the most diverse projects, each of which has an impact on our society.

WHERE DOES YOUR CHALLENGE LIE AT TNO?

LET'S FIND OUT

THYMEN WABEKE

Innovator

"Each project is different, and there is so much choice. At TNO you never do the same thing twice."

TNO innovation for life

CHECK TNO.NL/CAREER FOR CURRENT VACANCIES

Follow us on:

tno_talent
TNOresearch
company/tno
tno_research

Study of the Joukowski Transformation for Medical Imaging Application

AUTHORS: **T. XU, S. GALANAKIS** AND **A. WATERS**

The aortic valve in the human heart is a valve which regulates the blood flow through the heart. In spite of current advanced medical techniques, valvular heart disease still remains common in industrialised countries, because of the prevalence of rheumatic heart disease and degenerative valve diseases [3]. Current methods available such as echocardiogram and MRI can not precisely describe the geometry of the aortic valves [4]. Therefore we are aiming to find a new way of diagnosis that has harmless, accurate and efficient properties.

Status of the Research

We currently have achieved serious progress in 2-dimensions of the modeling of aortic valve geometry. The mathematics developed jointly by Dr. Alden Waters and Dr. Cristobal Bertolgio indicates that current numerical models can be greatly sped up by using energy functionals [2]. In addition, developing 3D models by ultrasound technology and back projections using the Radon transformation is a feasible goal. In this article, we are going to discuss some early results on research in the 2D model.

Inverse Boundary Value Problem

Given a rigid object immersed in a viscous liquid within a bounded domain, we can determine the location and the form of the object, solely using the measurements on its boundary. This is known as an Inverse Boundary Value Problem (IBVP), when we seek to determine properties of a medium through measurements made exclusively on the boundary. The laws that govern the medium are usually expressed in the form of a system of partial differential equations. The problem is then the determination of the coefficients corresponding to the partial differential equations, given measurements at certain points on the enclosing boundary.

Theorem 1. *Let D be a smooth object immersed in a viscous liquid flowing through a bounded domain (Ω). D is then uniquely identifiable by measurements of the of fluid velocity on the boundary, provided the boundary is locally Lipschitz.*

The theorem above can be derived from the main result of [6]. The result is proven by using fluid mechanics to reduce it to the study of IBVP's of harmonic functions, namely those for which $\Delta u = 0$. A possible application of the above results, in the context of medical imaging is to the valves of the heart, which regulate the passage of blood between its chambers. These valves consist of two or three valve flaps/leaflets (as depicted in Figure 1) and prevent the backward flow of blood. In this case the rigid objects in question are the valve flaps, which the viscous liquid (blood) flows around. The role of the boundary is played by the surrounding heart tissue and the enclosed area comprises the domain.

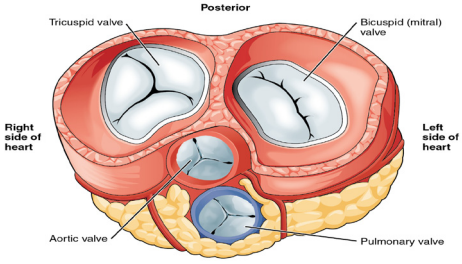


FIGURE 1: Valves of the heart. Sourced from [10].

In order to apply the theory to this case, several simplications and approximations are made. A two dimensional model is used, the valves are approximated by aerofoils and the boundary by a distorted rectangle. An aerofoil is a winglike curved shape used in many applications due to its aerodynamic properties.

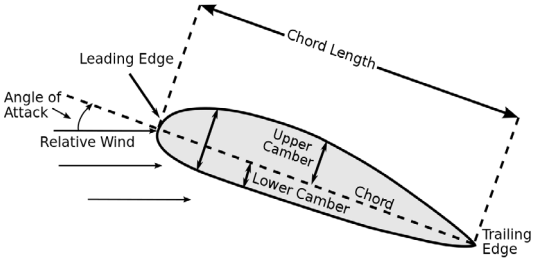


FIGURE 2: Diagram of an aerofoil exhibiting angle of attack. Sourced from[14].

Joukowski Transformation

The computation of the fluid flow around aerofoils can be cumbersome due to its often complex and asymmetric geometry. To avoid this issue, a conformal mapping technique is used. As such, we introduce a Joukowski map which is conformal. The Joukowski map and its inverse form is shown as follows, with parameter $\lambda > 0$ and $z \in \mathbb{C} \setminus \{0\}$.

$$J(z) = z + \frac{\lambda^2}{z}$$
$$J^{-1}(z) = z + \sqrt{z^2 + 4\lambda^2}$$

Conformal maps are complex maps that are locally angle preserving (and as such preserve the Laplacian, $\Delta u = 0$). The reason that we choose Joukowski map in our research model is that, under specific conditions, this complex map transforms circles into aerofoils, fittingly named Joukowski aerofoils. This property of the Joukowski map has historically been used in the field of aerodynamics in order to understand the design of aerofoils.

Using the Joukowski map, we can firstly compute the fluid flow around a simpler object, such as a circle, and then map it to the original target.

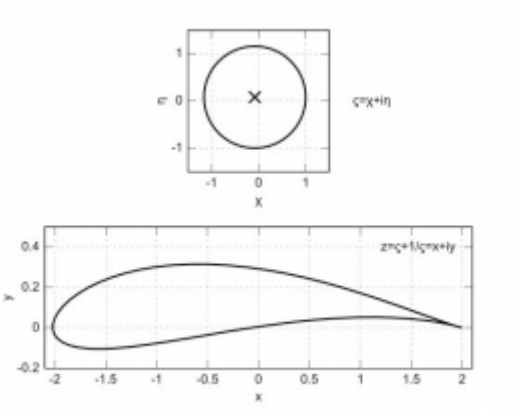


FIGURE 3: Circle with a slightly offset center and corresponding Joukowski aerofoil. Sourced from [15].

An Example of Producing the Model of the Heart Valve

The model consists of one aerofoil representing a valve flap, tangent to the boundary which represents the surrounding tissue and is a distorted rectangle. Here is a simple case of a fixed circle within a rectangular domain.

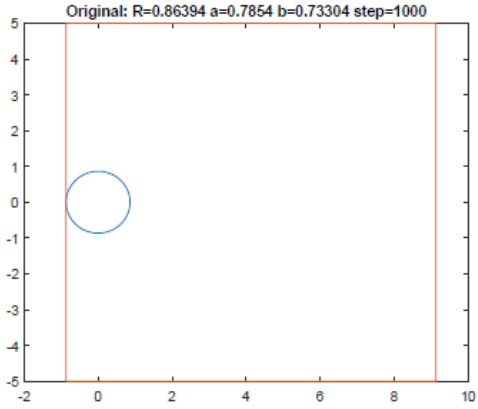


FIGURE 4: Original picture with circle at origin and tangent to left hand side of rectangular boundary.

To get a properly transformed Joukowski map, we need to move the circle and the rectangle a bit and make some rotation to the original plot. As the location, angles of the circle will impact on the shape of Joukowski transformed aerofoil. The process adapted from [7] can be perfectly modeling the valve flaps:

$$z = J(z_0 e^{i\alpha} + c)$$

In the transformation above, we define the parameters α, β, R, c as $c = \alpha - Re^{-i\beta}$. α is the angle of the rotation, R is the radius. In fact, varing those parameters allows us to control the thickness and camber of the aerofoils. Specifically, $\frac{R}{a} > 1$ determines the thickness (increases as $\frac{R}{a} \to 1$), β determines the camber and the tangent at the cusp makes an angle 2β with the real axis. After the relocation and the rotation of the original circle, we get a new plot as follows,

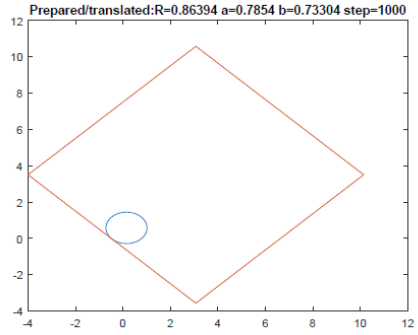


FIGURE 5: Result of applying the first two steps.

After applying the Joukowski transformation to the relocated plot, we get what resembles an aerofoil. Thus, the 2D modeling is initially completed:

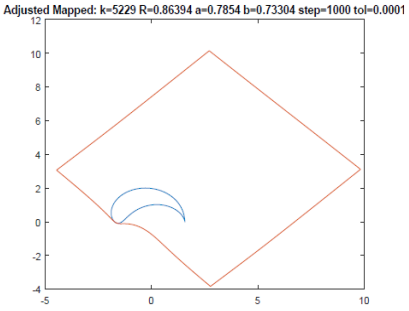


FIGURE 6: Final result after applying Joukowski map to the adjusted original.

Note: To use the Joukowski transformation, we need to make sure that the rectangle has Lipschitz boundaries, which means that the boundary of the domain needs to be locally Lipschitz continuous. This property of Joukowski map has been proven in [1].

Conclusion and Future Work

As we stated in the beginning, the article is about the early results of the research, and the overall goal of our study is the identification of defective heart valves by comparison with known data set. The conformal mapping method with the Joukowski map was employed in conjunction with results from previous research in order to reduce data measurements needed. At this point, we have successfully achieved the building of one of the valve flaps in the 2D model. In the future, we are aiming to get a full picture of two or three valve flaps by other techniques. For example, two pictures can be sewn together by using advanced fluid mechanics to get a 2D model of two valves.
In addition, [2] has provided a method to measure the boundary for the 2 valves, the implicit valve model. We can measure 2 slices of flows in the aortic root to form a picture of 2 valves.

References

[1] S. J. Galanakis, Study of the Jowkowski transformation for medical imaging application, 2018.
[2] L. Sok, Estimation of the aortic valve geometry by solving an inverse problem in Fenics, 2018.
[3] J. Soler-Soler and E. Galve, Worldwide perspective of valve disease Heart, 81:721-725, 2000.
[4] D. J. Pennell, Cardiovascular Magnetic Resonance
[5] C. Alvarez, C. Conca, L. Friz, O. Kavian and J. H. Ortega. Identification of immersed obstacles via boundary measurements. Inverse Problems, 21(5):1531, 2005.
[6] C. E. Brennen, An internet book on fluid dynamics: joukowski airfoils, 2004.
[7] O. College, Heart valves, illustration from anatomy and physiology, connexions website, 2013.
[8] W.c. User: Antilived. Diagram of an aerofoil exhibiting angle of attack, with labels, 2006.
[9] W.c. User: Krishnavedala. An example of joukowski transform of a circle into an aerofoil. The circle in complex plane is centered at (-0.08, 0.08) and has a radius
of 1.08, 2015.

Previous Brainwork

AUTHOR: **R. MOL**

Previous edition's Brainwork was a difficult one. If you solved the nonogram, the result would be a QR code. Should you scan that correctly, it would redirect you to www.periopuzzel.fmf.nl which would give you the image below.

Go to

?v=(8-1)(-)[_ager][-](8+1)
(9.81m/s^2) [{p/q}] ( )[{0,1,2,...}] (a+bi) [_ol]

Filling in the symbols; lowercase letters and numbers on the round brackets and capital letters in the square brackets. The result will be 'watch?v=7-JE9gQaNzM'. Pasting this into a youtube link gives https://www.youtube.com/watch?v=7-JE9gQaNzM.
In this video, a non-uniquely solvable sudoku is displayed. Using the hint given in the discription, if you use the given numbers as coordinates you should head southwest (per channel name) and use the 'map' given as channel image to know which turns to take. A bar on the left means you should go straight when presented with a left turn or take a right when presented with a right turn.
Doing this, you should end up in the Noorderplantsoen, at the restaurant called 'Zondag'.
As such, the answer to the puzzle is Sunday.

This was correctly solved by: Bart Dopheide and Bas Wijnen. The raffle was won by Bas! He can come pick up his prize at the FMF!

Chili Sin Carne

AUTHOR: **E. RUITENBERG**

Despite winter really being over, it is never too summery for comfort food. A tasty, vegan chili is always good. Nice to have with a desperado in the sun. Also very suitable in a taco or burrito.

Ingredients:

3 bell peppers
1 cup bulgur
500 grams of black beans
500 ml passata
400 gram tomatoes
3 teaspoons of chilli powder
2 teaspoons of dried oregano
2 teaspoons of cumin powder
1/2 teaspoons of nutmeg
A bit of cayenne powder
2 teaspoons of olive oil
4 garlic cloves
1 large red onion
2 cups of water

Cut the bell peppers in large pieces (1.5 x 1.5 cm) and cut the onion and garlic into small pieces. Wash the black beans. Heat a layer of olive oil in a deep pan, with a lid, on high heat. Sweat the garlic and onuin, then add the bell peppers and stir until the bell peppers are soft (approximately 3 minutes). Add the spices and stir until it smells good. After this, add all remaining ingredients , except the black beans. Let it simmer for 10 minutes with the lid on, stir occasionally. Add the beans and let it simmer for 15 more minutes or until you attain the thickness you want.

Possible garnishes:
- Avocado
- Cheddar
- Sour Cream

Brainwork: 7 Pictures

AUTHOR: **JASPER SOMSEN**

Finding the answer to the previous brainwork involved quite some different types of knowledge. And maybe even going outside was necessary to find out the day of the week as a final answer. I thought it was Saturday, but maybe that was incorrect.

This time, one of the editors looked up some older perios to find inspiration for a good puzzle. In some previous brainworks (back when we sent them in the mail, which we still do anyway), the fotocie challenged the readers to find photographed places. In a similar way, I challenge you to not only find these locations, but also the question that is given in bold.
Good luck!

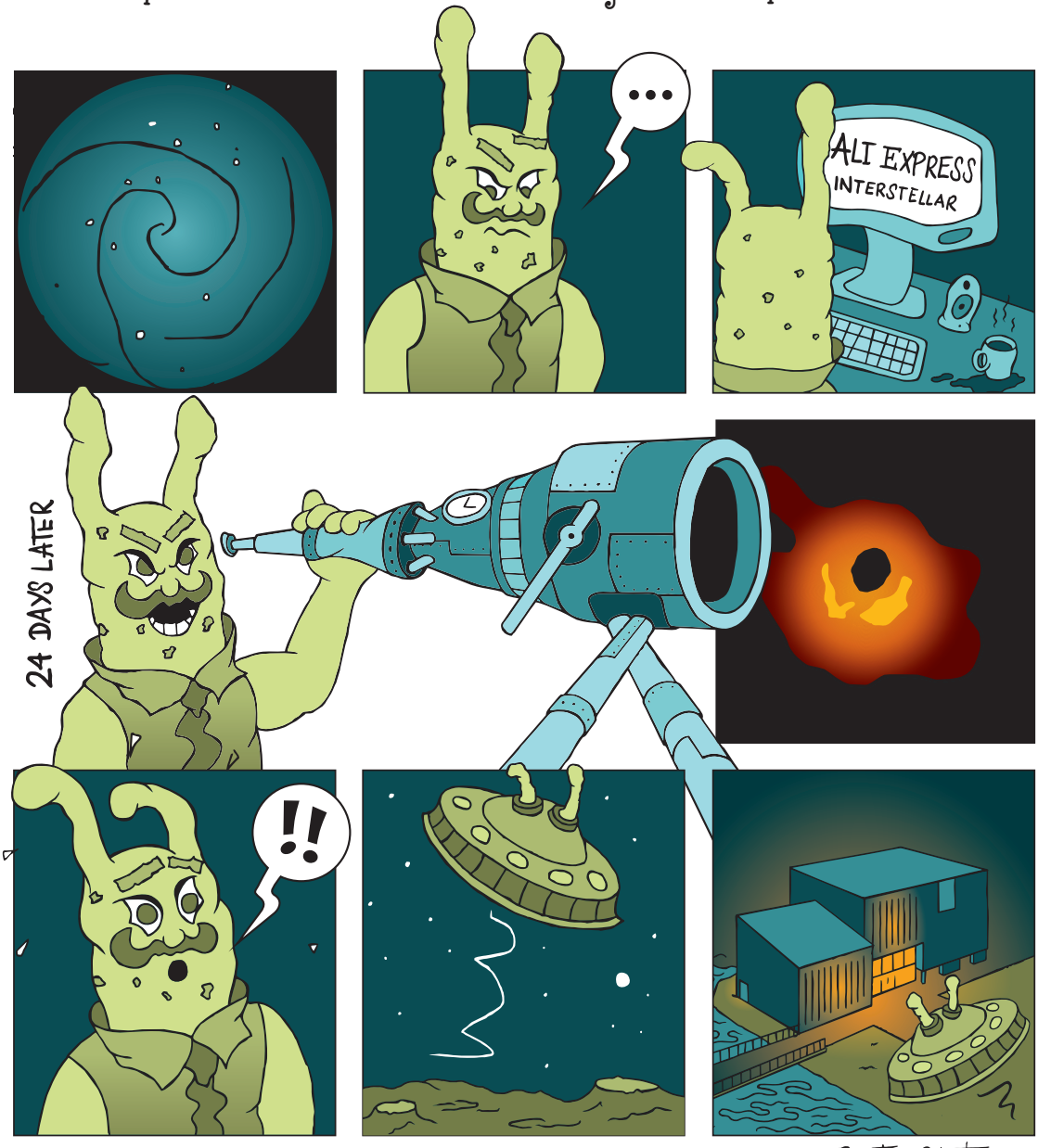
Below, you will find seven pictures of places in and around Groningen (at least within the municipality). Important about these pictures is the location where the photographer must have been standing. It doesn't have to be very exact for 2, 3 and 6.

The actual assignment is to **find a pop music artist connected to picture number 7**. The other pictures are there to establish some kind of pattern (in order). The final answer should have something to do whith "LSAL". This will not help you along the way.

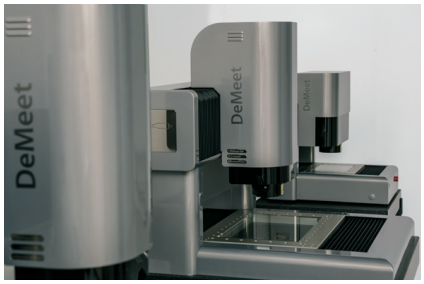
If you find the answer, send it to perio@fmf.nl. We will raffle a mystery prize among the people who send in the correct solution•

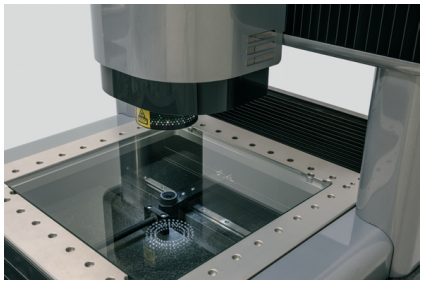
Dr. Peri

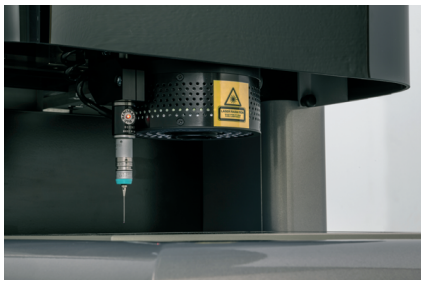
The existence of a sink in which all students' knowledge is lost has been known for a long time, however, it has never been captured by anyone known. Dr. Peri seeks to conquer this sink in order to drain all knowledge of His home planet NSFW0053.

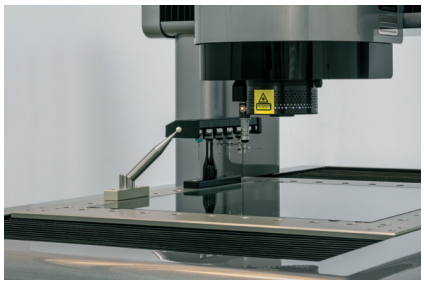


Robert & Robert 2019









Schut Geometrische Meettechniek is een internationale organisatie met vijf vestigingen in Europa en de hoofdvestiging in Groningen. Het bedrijf is ISO 9001 gecertificeerd en gespecialiseerd in de ontwikkeling, productie, verkoop en service van precisie meetinstrumenten en -systemen.

Aangezien we onze activiteiten uitbreiden, zijn we continu op zoek naar enthousiaste medewerkers om ons team te versterken. Als jij wilt werken in een bedrijf dat mensen met ideeën en initiatief waardeert, dan is Schut Geometrische Meettechniek de plaats. De bedrijfsstructuur is overzichtelijk en de sfeer is informeel met een “no nonsense” karakter.

Op onze afdelingen voor de technische verkoop, software support en ontwikkeling van onze 3D meetmachines werken mensen met een academische achtergrond. Hierbij gaat het om functies zoals ***Sales Engineer***, ***Software Support Engineer***, ***Software Developer (C++)***, ***Electronics Developer*** en ***Mechanical Engineer***.

Je bent bij ons van harte welkom voor een oriënterend gesprek of een open sollicitatiegesprek of overleg over de mogelijkheden van een **stage-** of **afstudeerproject**. Wij raken graag in contact met gemotiveerde en talentvolle studenten.

Voor meer informatie kijk op **www.Schut.com** en **Vacatures.Schut.com**, of stuur een e-mail naar **Sollicitatie@Schut.com**.

APPROVE for DeMeet

DeMeet

SCHUT.COM

Schut