MACHAZINE

Wiskunde
Informatica
Studievereniging

'Christiaan Huygens'

OTTO VISSER

Over 900! (well almost)

IT'S HACKENING!

HackDelft 2019

HISTORICAL PERSON

Sophie Germain

CONTAINING:

CURRENT AFFAIRS | ASSOCIATION | COMPUTER SCIENCE | MATHEMATICS | MISCELLANEOUS

Advertiser index

Louise Leibbrandt

The second quarter has brought us a cold winter with strong winds and unbearable biking conditions. The halls of EWI are filled with freezing hands and red noses. Luckily the CH room provides a warm and comfy refuge from these dark months. As the almost overwhelming amount of Christmas lights twinkle in this warm space, most students are busy hiding CH mugs as the demand for warm drinks has exploded. The atmosphere is comforting and students of all ages come here to enjoy a cup of hot cocoa together. It is nice to see that even some of the new first year international students have adopted the habit of coming here to share a drink and a chat. Many of us native Dutch students sympathize with these new students as they adjust to the unknown Dutch weather conditions and as they settle into the new Computer Science (CS) curriculum.

It is no secret that the first year CS students are struggling, with 800 they have just completed their first three courses and now face 3 new challenging ones. As a second year CS student I can attest that it is no easy feat to keep a cool head whilst taking on this difficult curriculum. The life of such a student is filled with programming, studying slides and asking many questions to those students who seem to understand the material just a bit better than the rest. We are very pleased as active CH members that many of these overworked students find the time to attend the many activities and parties hosted by the study association and to see them thrive within the many first year committees. As the committee kickoff has just happened and as the old member committee drinks are taking place in the /Pub, we get to enjoy the enthusiasm and warm personalities of these freshman.

It is not only at CH where students can find an escape from the blues these weeks always seem to bring. Christmas fills the streets of Delft and lights align every street and canal in our cosy small town. The infamous 'Lichtjesavond' or evening of light took place in the December within the heart of Delft. Stalls fill the streets selling delicious Dutch delicacies and people come together to watch the lighting of the Christmas tree in the town square. The night is also filled with music as many Christmas carolers and small bands come to perform. If you missed 'Lichtjesavond' this year or have yet to go, I would definitely recommend going next year!

By the time this issue is published, Christmas break will be long gone and finals will be upon us. Therefore, I wish all students reading this good luck with their exams. If you happen to be a professor reading this, I hope this vacation has filled you with enough Christmas spirit to go easy on the students this exam period and bump the grading curve up :). And finally to all readers, enjoy reading this issue of the MaCHazine! As always, if you have an idea for an article or any suggestions for improvements, don't hesitate to contact us at machazine@ch.tudelft.nl.

Table of Contents

Current Affairs

Association

Computer Science

Mathematics

Miscellaneous

MACHAZINE

From the Board

Jeroen Nelen

Career Affairs

My position inside the board is Career Affairs. This means that my main goal is to enlarge our social network and to bridge the gap between the theoretical knowledge that you gain on the university and the practical skills required in a company or business. It is a relatively new function inside our board and I really appreciate the freedom that comes with this function. As part of my position, I organize Career Colleges, which are workshops and lectures meant to bridge that gap. Additionally, I try to expand our network by use of our alumni and our ambassadors. Ambassadors are people with a large network that want to help us grow. They give input and try to help us whenever they can.

Overall, my experience of being part of the board is very positive. You get to learn new people, new skills, the history of the association but you also learn about yourself: about your personality, work preferences and more. For me, this year is all about seven people that want to improve the association together which we do by choosing a few issues that we would like to address and fix during the year. In August, during the preparations, we wrote a policy on what we wanted to improve. One of our policy issues was merchandise and we have more merchandise now! (Read on and you will see what kind of merchandise there is.) It is very cool to see the abstract concept now in real life and it makes this experience very charming and pleasant.

To conclude, I came to a realization that three or four months ago, I only saw what was above the waterline. This visible part already appealed to me, but now that I am seeing more, I like the association even more. While there are of course some unpleasant things that you need to do, like descaling the tea machine, this really weighs up against the positive sides. The people and things you learn during this year make it a cool experience and I am proud to be part of this team. Together, we hopefully make Christiaan Huygens a little bit better every year.

Huygsche!

Dear reader,

I want to start off by talking about the iceberg principle. The iceberg principle simply states that only 10% of the information is easily visible and is "above the waterline," while the other 90% is hidden beneath the surface. And this describes quite accurately how I feel right now about being part of the board.

Let me explain this. It's a calm evening and I am still in the CH room. It is 9 o'clock and while I am writing this From the board article, I am also cleaning and descaling the tea machine. This made me think about this principle just a little bit longer. At CH we serve free coffee and tea for our members and I really love it that we serve this. Not only because I enjoy drinking coffee, but also because it makes our members connect and relax together while enjoying a hot coffee or tea. During the break, students come inside our room, grab a coffee and have a talk with each other or with us. It is a small but pleasant concept.

Coffee is a great example of this iceberg principle because as a member, you only grab a mug, grab some coffee or tea and then leave the CH room again. Which is of course perfectly fine, I did that last year as well. But during these last three months, I realized how much I underestimated how much more there is to it. Because there needs to be a budget to buy a specific brand of coffee, coffee filters, tea, sticks, creamer and sugar. Then these things need to be bought and stored somewhere inside one of our CH storage rooms. Every day, the mugs are cleaned. And twice every year, the coffee and tea machine need to be cleaned and descaled with very specific cleaning products and procedures. This made me realize how much more there is to such a small thing like this. Don't worry, this is not a lecture or speech to convince you how much work the board does, but rather an example of how I feel about being a part of the board.

Current Affairs

TU Delft news

Wouter Versteegh

The Delft University of Technology is the biggest and oldest public technical university in The Netherlands, established by King Willem II on January 8th, 1842. But what is currently happening in and around the TU Delft? This article will list the most important events of the recent months.

First books published in TU Delft Open Textbook project

Online books are very useful for students as they are free and can be accessed everywhere if you have your phone or laptop with you. For myself at least, I first look if the book I need is available online before buying a hardcopy and surely I am not the only one. Downside of this is that you often find outdated books. As a part of the TU Delft's principle of transparency in education, the TU Delft Library now supports teachers with their process to publish their book online under open license. This means that you can get certain books for free! The teachers are also able to adjust or add to the material so the book is a lot more up to date than if you would wait for the next version to come out.

As project manager Michiel de Jong states: "We want to create an online community around open textbooks. Not only students but also fellow researchers all around the world can read the books and reuse the material, as long as they respect the Creative Commons conditions".
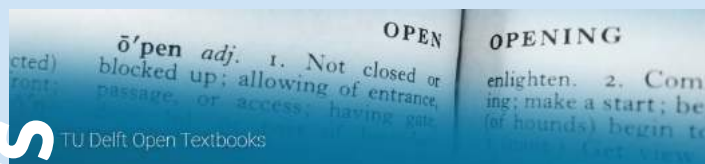
This Open Textbook project is fairly new so not many books are yet available but as time progresses you can expect more books to be available. You can find the books on https://textbooks.open.tudelft.nl/index.php/textbooks.

Exhibition The Age of Standards

From the 29th of November to the 1st of March, an exhibition on The Age of Standards will be held in the TU Delft Conference Centre. Based on the academic heritage of the TU Delft, the exhibition aims to show the confusing world behind the daily use of standards. As you know we use the metric system, which uses meters for distance and such, but ever wondered why we use meters? And why we sometimes use kilograms to measure weight? A look into the origin of the SI-units shows that the definition of a kilogram has changed a lot over the previous centuries, even though it feels like second nature to us.

One of the first definitions of a kilogram was "Prototype found in French Academy for Sciences" which was a "1 kilogram" solid metal weight . The most recent is actually in the works now, and it determined by "1 kg $\approx$ 1.4755214 * 10^{40} f/c^2 ", with f the frequency of a photon with a certain frequency. As you can imagine, it can be quite hard to define such seemingly standard units. The exhibition looks back on the invention and introduction of the metric system and the current works on it. It describes the shift from physical prototypes to constant based physics. If you are interested in our metric system, I would recommend you to visit this exhibition.

Ransomware does not stand a chance at TU Delft

A research done by Fox-IT says that dozens of Dutch companies may have been affected by a ransomware called SamSam over the last few months. This ransomware uses configuration mistakes in the IT of the company and blocks computer systems. To release these, the companies have to pay ransom, often in bitcoin. This raises questions about the cyber security here at the TU Delft.

It was tested extensively and luckily the TU Delft is very well protected. If you want to avoid installing ransomware here are some tips:

- Back-up! Back-up!
- Make sure that the back-up is in a secure location and not connected to your computer
- Use good anti-virus software
- Make sure to update all software on your computer. If a new version is released you should update it immediately
- Be watchful for phishing emails
- If you come across something suspicious, disconnect from the internet immediately

Over 900! (well, almost)

Otto Visser

The bachelor Computer Science & Engineering has seen rapid growth in the past few years. This year especially the growth is immense: the amount of first year students has roughly doubled.

The staff was already getting a bit nervous somewhere around March this year. This is the time we get the first numbers on how many students are enrolling for our programme. The magic number was 191 % growth. Reactions went from "Look at us being popular!" to very quickly: "how are we going to deal with this?". In the weeks and months after, a crisis team was formed to think about possible solutions to what some called: the tsunami. Are we really going to grow by that much? And: why? Can we still stop this? Recruitment for additional staff started and we also began to rethink our own courses.

The problem is that by the time you really know how many students are in the first year, you have already had the first exam. Until then every enrolled student is a bit like Schrödinger's cat. He/she could be in the lecture hall, but the student might just as well be in Utrecht to become a vet. Or just at home, playing Fortnite and binge-watching Netflix. Not every student has a mother that knows the schedule and kicks her kid into the lecture hall after all.
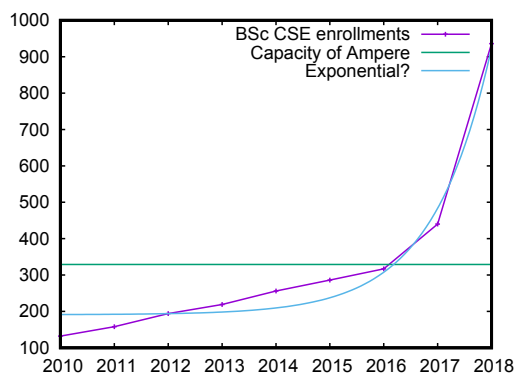

Figure 1: No need to worry: next year we have a numerus fixus.

I have been involved with the Computer Organisation (CO) course for a while now. It is a first year, first quarter course so we get all of the students. It is a gamified course which means students have a whole buffet of bonuses to choose from. TAs handle most of the checking and I do the administrative part. Thankfully all the systems used for this agreed on one convenient file format for exchanging information: CSV. CSV is an abbreviation for Comma Separated Values. To import grades into Osiris you provide a file with student numbers and grades separated by a **tab**. And for Brightspace you need the comma, but you also need to make sure the line endings are correct. As some of you might know, Unix-like operating systems use a newline (\n), Windows decided that we also still need to do carriage return so they use \r\n. Brightspace decided differently. They invented a new line ending: #

CO this year was different. Let me provide some numbers. Per week we had 6 lectures (3 groups times two lectures a week) and 6 tutorials (once a week in groups of "only" 128). For the shared lab (the lab is organised together with the other 2 courses in the first quarter) we needed TAs. A lot of TAs. We had roughly 64 TAs for the shared lab out of which approximately 32 could handle CO questions and handle the load of the 866 people that tried to get the (dis?)approval of their assembly code. I used to make the joke to the students that if I know your name, you are either a very good or a very bad student. This year I could start doing that with my TAs and I gave up on even trying to memorise student names (except ████, ████████ and ████: I know your name!). I received well over 800 mails for just this course edition (if you happen to be one of those mail senders: I apologise if it took a bit longer to get a reply!).

And then there were the exams. 42 kg of exams. Thankfully we only got 8 kg back: the answer forms. To prevent new back injuries and overdoses of Oxycodon we actually bought a cargo bike. 841 students had enrolled for part 1 and 887 had enrolled for part 2. Typically we lose students half way, but not this year. Also note how none of the numbers I mentioned so far matches the 936 students that the course has on Brightspace. So if anyone ever asks how many students I had in the course, the only correct answer is: I do not know.

Figure 2: No problem, they still fit in one small classroom.

The course has ended and I think we managed to deliver (a big thank you to all of the TAs that helped!) even though sometimes a bit late. But can we really say that we can handle this many students? It is safe to say that if every quarter I had a course like this I would soon no longer have a wife at home. I am home one day a week with my kids, but I regretfully have to admit that they watched a bit more YouTube and Netflix than I wanted them to. And this cohort still has to progress to year 2 and 3. In the third year we are going to make other faculties happy with a lot of minor students (finally: a break for us!) and then at the end: an individual bachelor research project. Student numbers might have doubled, but so far staff numbers for sure did not. CHallenge accepted?

Current Affairs

Faculty Student Council

Bram Dikker and Arian Joyandeh

The new academic year has been on its way for some months now and the new Faculty Student Council (FSC) members are setting up shop. We even have a member from abroad! Here is a short introduction on what the FSC is, does and how you could potentially join.

What is the FSC?

The FSC or Faculty Student Council is a student representative council within our faculty EEMCS. In practice the FSC will try to improve the faculty on behalf of the students by giving advice and participating in important meetings and discussions within the faculty. We have a weekly meeting to discuss problems within the faculty. Then we can discuss these problems with the board of EEMCS in another monthly meeting. We also attend the budget meetings within EEMCS where we have a say in how the faculty spends its millions. On top of that we also discuss university-wide issues through meetings with all other FSCs and the Student Council of the university. The FSC has the right to advise and the right of initiative regarding anything relevant to the students of EEMCS. This allows us to really make a difference at the faculty!

The elections

The FSC is chosen every year by elections. Everyone could sign up for the elections, this makes the FSC very diverse. We have a freshman, master students and internationals within the FSC. Then, depending on your number of votes, you could get a seat in the FSC. Within the FSC there are different "chambers", with each chamber representing a program within EEMCS. Depending on our program we could only run for a seat at our own chamber. There are 4 seats available in the Electrical Engineering chamber, 4 in the Computer Science chamber, 3 in the Mathematics chamber and 1 in the SET chamber. This last chamber might be unknown for some students. SET (Sustainable Energy Technology) is a relatively new MSc programme and was initially represented in the Applied Physics Council. Last year, they became part of the EEMCS council. Everyone is new so we have a fresh insight on all faculty matters. We have very capable people, all having experience in all fields of life. These experiences will help the faculty and you greatly. We have had numerous meetings about subjects ranging from alpacas to plates. We will introduce the members of the new FSC here:

Electrical Engineering chamber:
Erné Bronkhorst   (CHairman)
Joey van Rijn   (Secretary)
Thomas Roos
Gabriela Zacca

Computer Science chamber:
Bram Dikker
Sterre Noorthoek   (Treasurer)

Francis Behnen
Cas Buijs

Applied Mathematics chamber:
Arian Joyandeh
Emiel Hhoefkens
Jorino van Rhijn

Sustainable Energy Technology chamber:
Thomas Spruit   (Secretary)

What we're doing now

The new FSC is currently in full effect. We have subdivided into smaller focus groups in which we discuss matters such as the current capacity, sustainability and internationalization. We have had a training with all the FSC's from the TU Delft where we have already learned a lot. We are also picking up where the old FSC left off. There are also meetings with all the faculties. We will continue their work on the improvement of Collegerama and we will make EEMCS great again.

We want your input!

We are still thinking of subjects we want to improve this year. For that we will also need your help. Every quarter we will organize a coffee moment to talk to students. You can then find us in the hall of EEMCS with free coffee, ready to hear your stories about studying at EEMCS. We would be pleased to hear about all the problems you encounter throughout the faculty or any ideas you might have for improving the education at EEMCS, big or small. If you cannot wait for the next coffee moment, you can always send us an email at: fsc@ch.tudelft.nl.

Riots in France, Belgium and The Netherlands?

Fred Vermolen

In November 2018, demonstrations and riots started in France. Later on, Brussels followed and on December 1st demonstrations, on a very, very modest scale started in The Hague. Where do the protests lead to?

November 2018, the 'Gilets Jaunes', or yellow vests, started demonstrating in Paris. The reason why they started demonstrating was the increase of fuel prices. The rural areas in France lack a well-functioning system of public transport, and therefore, peasants and commoners are bound to use their own means of transport. Since many of these people are already struggling with a modest income, the increase of the fuel prices –predominantly via taxes raised by the government to meet the requirements in the Paris Climate Treaty– will decrease their relatively modest purchasing power even further. These people are mad and this is understandable. The French President, Mr Macron, married to a woman of the same age as his mother, used to be a banker and many people look upon him as a friend of the extremely wealthy people in France. Despite their voting for him as a president, they despise him. One might wonder why on Earth did the French people elect Mr Macron as the president of France? The reason is plain. The alternative was Madame Marine Le Pen. Marine Le Pen is a populist like Mr Geert Wilders in The Netherlands. In fact, the French have chosen the lesser evil of the two candidates. C'est incroyable (it's incredible)!, the French would say. I do not think that Mr Macron will have a second term. The French really do not like him to put it mildly.

It seems that Mr Macron does not want to discuss his policy with the common French people, nor is he prepared to revise his announced increases of the fuel prices. It is not only the fuel prices in France that will be increased by the government, it is also the property taxes that have been abolished by Mr Macron. This measure was warmly welcomed by the richest French people. But abolishing such taxes, and upon maintaining a social system where the salaries of employees who are ill are not paid by their companies, but by the state, immediately implies that ordinary people have to pay more taxes to sustain this social system. This is what has happened in France. The real estate taxes increased by almost fifty percent. Further, as a Roi Soleil (Sun King), referring to king Louis Quatorze (Louis Fourteen), 1638-1715, Mr Macron instructed to spend seven million Euros to buy tableware (can you believe it?) for the Elysee (the Presidential Palace). Furthermore, he gave his wife a salary of 450,000 euros a year (not including expenses, assistants, and drivers). The French are angry. They are protesting right now in Paris, but also in other parts of the country. Next to all these ridiculous expenses, the French are faced with violence in the suburbs (banlieux) of their big cities like Paris, Saint-Etienne, Lyon, Marseille etc. The French have the right to be angry. The French protesters were recognizable by wearing yellow vests (gilets jaunes).

In the course of the month, the riots moved up North and arrived in Belgium, where Brussels witnessed violence on November 30 and December 1. Today, December 2, and yesterday, Paris has changed into a complete war zone. Bombs are detonated near the Arc de Triomphe and the police are using tear gas and even snipers in their efforts to calm down the angry crowds. So far, it is all in vain. Mr Macron is in Argentina now for the G20 summit, and he is condemning the violence. He is choosing a harsh policy. Whether this choice is wise, time

will tell. The French have a history of revolutions (1789-1799), where the guillotine was used extensively. Personally, I think that this movement could be the onset of a new French revolution.

Later, December 1st, anti-government protests started in The Netherlands on a very small scale in The Hague, Leeuwarden, Maastricht and Nijmegen. The protesters are also wearing yellow vests, and they insist on protesting without any form of violence. The reason for their protests is that they are against the policy of the Dutch Prime Minister, Mr Rutte. I was in The Hague. The reasons for my presence were the following: loan system that was introduced for students (young graduates will have a debt and have trouble buying a house), Marrakesh Treaty (this will result into an extremely large inflow of immigrants from Africa and the Middle East, I wonder whether a small country like the Netherlands is able to accomodate all these people), increase of taxes on fuels (fuel prices are extremely taxed in the Netherlands, which was supposed to be a temporary measure, but the taxes have never been reduced), ambiguity in Law verdicts, transition of more and more legislation from the Netherlands to the European Union, transition from gas to electric heating systems (the government wants people to buy expensive heat pumps despite the fact that gas is a very clean means for heating, countries like Israel and Portugal are changing towards gas because of its cleanness) and the degradation of the social system despite increase of taxes. I strictly emphasize that I only believe in peaceful participation.

We were walking in the centre of The Hague with about two hundred people. Nobody was violent and even litter was cleaned by the crowd. I was somewhat astonished by the low number of people, and in particular, I was surprised by the lack of young people. They were not there, whereas the only reason that I participated was that I did this for the younger generations: the students, but also for my own children. Furthermore, the police were very intimidating, with their massive presence, arrest vehicles and horses. We were denied our right to demonstrate next to the Binnenhof. We had to move to the Malieveld. At a certain point, we were confined and circled by police vehicles and horses. We could not leave the circle. The police walked on horseback through the crowd, pushing away people who were standing. People were just standing and singing a well-known song (vijftien miljoen mensen). There was no aggression at all. At a certain moment, we had to pull off our yellow vests and to walk away, otherwise we would be arrested. The crowd was only taking a walk. This clearly demonstrated the fear of people who work for the government. Of course, they were afraid that the same violence as in France would arise. This is not to be expected from a crowd of people who are predominantly in their forties and fifties. The younger generations were simply not there. They do not seem to bother, so why should they be protesting? They have better things to do.

The protests showed the very ugly face of the Dutch authorities, and the lack of democracy. However, of course, you do not bother, why would you, as long as we still have enough to eat, and as long as you can still have your beers and city trips. I guess that this movement will gradually disappear, since the Dutch do not bother. I am not so sure about what will happen in France. Possibly, when this column is issued, more will be known about the situation in France.

Well, I have bored you with all this. It is time for a couple of pints.   *Skål!*

Association

Committee Kick-Off

Alves Marinov

As tradition commands, this year not only the board of CH changes but also the committees are reassembling with new blood. And one of the many wonderful committees in our association is the CHoCo. Represented by Dutch and international members we are responsible for organizing a freshmen dinner and the parent's day. So, to get to know each other before the hard work begins we were invited to the Committee Kick-Off.

We started this event on the 14th of November at the famous Bastiaansplein. At 18:00 the fun began. There were exactly 62 activities (or you could call them challenges) prepared for us and the other committees to do. The first thing we realized is that we were with too many people for one group, so we had to split in two. After that both groups went their separate ways to complete whatever challenges were ahead of them.

We began by going to the square in front of the " new church". There we officially started with the challenges. Our first task was to form a human pyramid as all great teams do, of course. Then it was time to say hi to the cheese shop and take some selfies with the products there.

After the photo session there was a small exchange of clothes as per one of the challenges. Speeches were made, songs were sung, there was also a dance-off and of course we didn't miss the opportunity to go to Alev.

Unfortunately the time for fooling around was soon over but the fun was not yet. After finishing off as many challenges as possible we headed to Gasterij 't Karrewiel - a wonderful restaurant, where we 'gourmetted'. And all of it just for us.

There we were greeted warmly. The atmosphere was wonderful and cozy. The food was delicious. All the way from the elaborate bacon wrapped sausages that you get to cook yourself, and on a stone plate nonetheless, to the bread itself - everything. For dessert we had the opportunity to make ourselves some pancakes - simply perfect. At the end of the dinner the winners of the challenges were announced, a speech was held to welcome the new committee members and to wish them good luck, all committees were mentioned of course. After some more joyful talking we had to depart from the restaurant because as it turned out it was pretty late. Time flies when you're having so much fun. And it seemed like everyone was having a good time.

Overall the Committee Kick-Off is something you cannot experience every day. It is definitely something special. It has a serious intent but does it in a very fun way. It is a very social experience. You get to meet new people, have fun with them and in the end even share a meal or two with them. It also helps with the bonding within the committees themselves. You become closer to people with whom you'll be spending the academic year working together on all the wonderful activities and events that are to come. And that is what the committees and CH is about.

Association

Time for AkCie

Ardy Zwanenburg

This year AkCie presents: BadpAkCie. The activities committee of the year 2018-2019 has the following twelve members: Ardy (Chairman), Andy (Secretary), Gancho (Treasurer), Charlotte and Carlotta (Promotional Affairs), Noortje and Janne (Decorations Affairs), Jeroen and Lola (Purchase Affairs), Niels (Ice Affairs), Tuhin (Music Affairs) and last but not least Ricardo (Peer Pressure Affairs). Maybe I should also mention our two QQ'ers Jari and Jeroen. They are here to help us with our journey this year.

Our job as a committee is to organize a number of activities throughout the year, with the goal of having fun with fellow students outside of the lectures at the university. These activities, amongst others, include member lunches and having drinks. So far we have already organized two activities: the ADSL drinks and the Sinterklaas member lunch.

The Start

During one of our lectures a board member of CH stopped by and told us about the first year committees. We were told what each committee does and how we could become a member of one. We also had the chance to fill in the interest form. After that we didn't hear anything about it until a month later. We all got an email that we had to come up to the 20th floor of EWI and shouldn't tell anyone. There we were asked if we wanted to join AkCie. A week later we had our first meeting.

The first meeting was a lot of fun. We are a committee with members from three different studies: Computer Science and Engineering, Applied Mathematics and Applied Mathematics and Applied Physics. We sorted out most tasks pretty quickly. Only the Treasurer and Chairman positions were a bit of a discussion.

Of course we had to come up with a theme and a color for our committee. After some ideas we decided to go with BadpAkCie. And what color fits better with this theme than Bondi Beach Red? So that became our color.

ADSL

ADSL stands for the Algemene Docenten Studenten Lounge, which could be translated to the General Teachers Students lounge. This is an event for students to get to know their teachers better. The teachers can order free beers and the students can't. So if they wanted a free beer they had to chat with the teachers, get to know them and get beer from them. However, what happened was that Otto bought a big pull of beer and just went to students and had a talk with them. There were different teachers from Computer Science and Mathematics. Overall, it was really fun to participate and organize this event.

Sinterklaas member lunch

During a lunchbreak we organized a member lunch for the Dutch tradition Sinterklaas. It was really fun! We had our own home made smoothie, which were of course as red as Bondi Beach red :-). After everyone started eating their lunch, Sinterklaas came in with his favorite Piet: Mint green Piet. Some "children" were even allowed to come on stage and sit on Sinterklaas his lap. After that, Sinterklaas told something about them and of course he gave them a gift.

Now and the future

At this moment we have a small break. We have had two activities and still have one left to organize. Now we are busy with studying and a bit with the AkCie. We are thinking about our last activity and how to organize it. We don't know what it is yet, but as soon as you see a poster with `BadpAkCie presents…', you should already have bought your tickets. Hope to see you there!

Association

HackDelft: It's hackening!

Raoul Bruens

Hackathons have become increasingly popular, among both students and companies, as the skills that are showcased during such events are desirable traits in a business environment. Students get a chance to get their hands on data sets that are representative of the problems that businesses have to solve. Because of this hackathons are a very fun way to get to know, develop and apply the skills that are required for efficient problem solving.

The annual HackDelft Hackathon is the only large hacking event in Delft that is organized by students for students. The event will be held in the Sports & Culture center, at which you will have 24 hours to work on all kinds of problems in groups of four students. Companies will provide sample problems for you, along with their own data sets. This year, the companies will be Optiver, PWC, CGI and Sogeti. Based on these provided data sets you can also come up with your own problem to solve. Nothing is too crazy, you can be as creative as you want!

At this event you will have the chance to apply your skills and knowledge to tackle your chosen problems, with your preferred IDE or editorial software. At the event, there will be all kinds of hardware tools and gadgets provided to you so that you can have all the options available to come up with your preferred take on the solution. The most creative, innovative and well-worked out solution of the hackathon will win the grand prize, but there will also be a categorical price for the best solutions of each data set.

Because of the freedom within a hackathon there is something to do for every skill level. People who are not familiar with hackathons may have noticed so far that I have not mentioned breaking into systems and software security at all. They might think that a hackathon is about hacking into things. When you think about it, it is not all that surprising given that the term hacking is often used by the modern media as meaning 'using a computer to gain unauthorized access to data in a system' or plainly as 'hacking into something'. However, the broader definition entails 'a piece of computer code providing a quick and

elegant solution to a particular problem'. Thus, every creative contribution during a hackathon that tries to solve a particular problem is justified as hacking (so also when your problem is breaking into a system). Thus, every innovative contribution is appreciated! Even if you're not that familiar with coding, you can still work on anything that substitutes a solution. Think of creating mathematical formulas, user interfaces or even composing a soundtrack! The options are endless, so if you're in doubt, just attend the hackathon and make it a fun new experience .

Of course, aside from all the hacking, there will be team bonding activities throughout the day. Previous year, there was a change to do cup stacking and there was capture the flag game. These games are a good, fun way to get to know your fellow hackathon attendants!

If you're interested in joining, keep an eye on our website which will be live soon. The event will have a dedicated sleeping area if you want to take a rest from hacking during the night, though a lot of students will try to hack throughout the night. Diner, breakfast, lunch, drinks and snacks will also be provided. I hope to see you at our next HackDelft Hackathon; it's Hackening!

GET THE LOOK

You may have noticed it around campus - CH has new merchandise! Find out here how you can represent your love for mathematics, computer science and owls in style. All items shown are available at the CH board.

SUNGLASSES - €4,00

No matter the occasion - ski trip, summer holiday, festival or simply your bike ride to EWI - you can protect your eyes in style with the new CH sunglasses!

TOTE BAG - FREE

Never have enough space in your backpack for all your new books? The new CH tote bag is the answer to all your problems! Get one for free at the CH book sale.

CHappy SOCKS - €4,50

Stay happy with the new CHappy socks, which bring together mathematics and computer science with a fun print! The perfect gift for family, friends, and of course, yourself.

AREA FiftyLAN - Gaming Event

Wouter Versteegh

You might have already seen the huge banner in front of CH which could only mean one thing: Area FiftyLAN is coming soon! If you study computer science, chances are you play, or you have seen someone play Hearthstone during many first year computer science lectures. It comes as no surprise that the study association organizes one of the biggest gaming events for all students in Delft: Area FiftyLAN.

Since the first time it was organized, Area FiftyLAN has grown to be an event where 220 students from the TU Delft are able to play and watch video games, chill out, party and socialize all they want. People can participate in official tournaments for games like League of Legends, Rocket League and CS:GO. For all these tournaments the LANcie will arrange very nice prizes.

Of course, participating in these tournaments is not the only thing that you can do. For the more casual gamer, or just anyone in general, there is plenty of other stuff to do. A whole corner is furnished to make sure that you can play casual party games like Mario Kart, Super Smash Bros, Just Dance and more, while enjoying a nice drink you can get at the bar. All you need to do is enjoy, because everything else will be taken care of. All meals during the weekend are provided and there is a separate hall where you can sleep.

This whole event is organized by the five of us, under the highly valued supervision of Tom Heijnders, our Qualitate Qua. Since the beginning of September the committee has been working to make this event an event you will never forget!
We are currently promoting the event as much as possible as most of the basics have been taken care of. The event will be held at X (formerly Sports and Culture) on the TU Delft Campus in the weekend of the 1st, 2nd and 3rd of March. If you are in for a unique and fun weekend where you can enjoy all the wonders of gaming, or just chill out a lot, then we would love to see you at our event!

If you have a question or other ideas for our event, feel free to approach the LANcie, ask the Board, check our website https://areafiftylan.nl/ or email us as at areafiftylan@ch.tudelft.nl. Disclaimer: favorite games can be quite subjective. We cannot guarantee that your idea will be accounted for at the event.
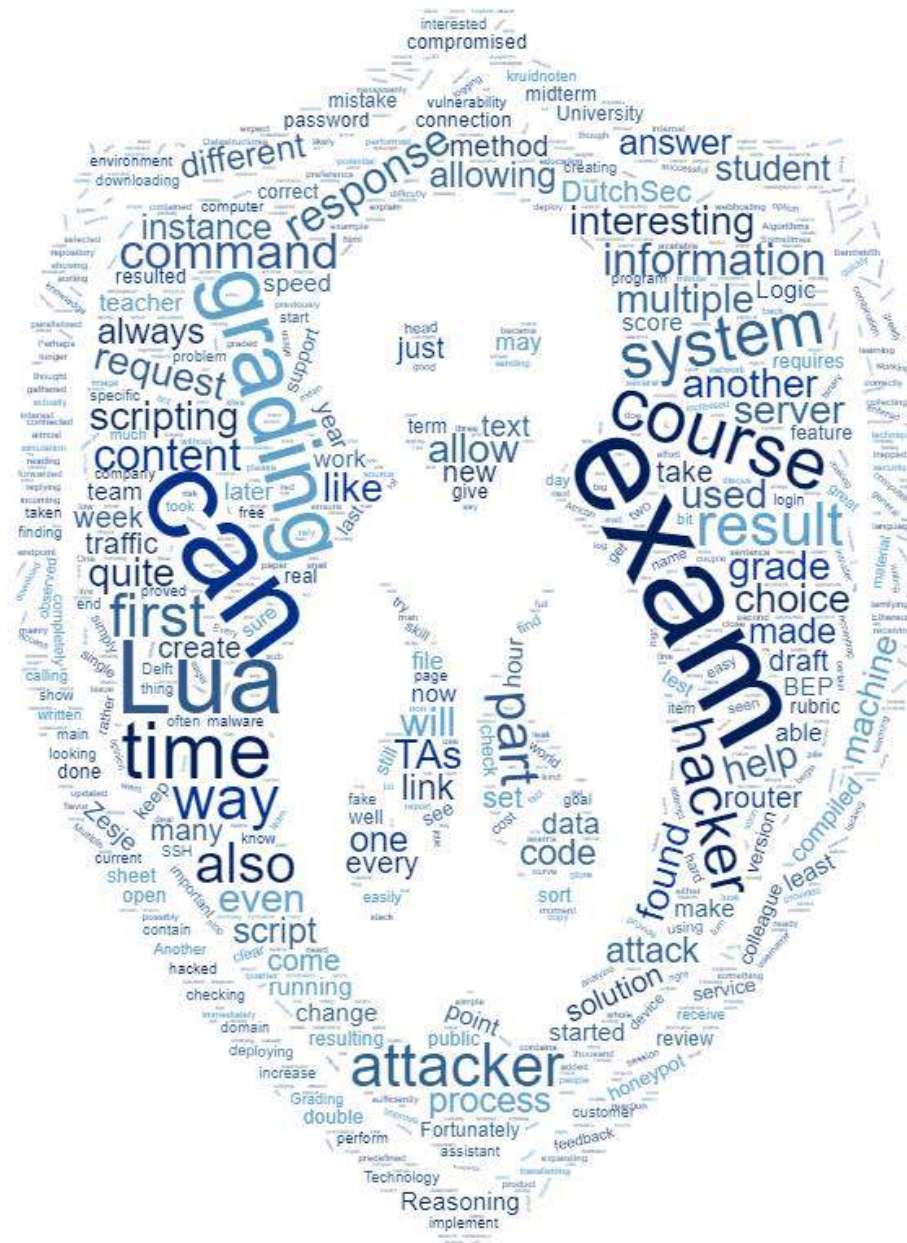
See you all at the 5th edition of the Area FiftyLAN,
The LANcie,

Timo, Chris, Erik, Tim, Tom and Wouter

Association

14

Computer Science

On the creation of exams and the nightmares of grading them

Stefan Hugtenburg

Out of all jobs I perform as a teacher, grading is one of those that has an remarkable interest curve. From very interesting in the first two hours, to tedious and boring quickly after. Why does this curve have this form and what can we do to make grading more interesting?

It took 5 kg of 'chocolade kruidnoten', 3 kg of regular 'kruidnoten', 36 stroopwafels, 24 pizza's, and countless cups of coffee, tea and hot chocolate. We spent about 300 (wo)man-hours on this Herculean task. But we finished grading the 884 midterms students handed in for Reasoning & Logic, a first year first quarter course. Unfortunately that was only week 5 of the first quarter. Since then me, my colleagues, and a great team of teaching assistants have graded over 800 end terms for both Reasoning & Logic and Object-Oriented Programming, 400 resits of the midterm for Reasoning & Logic, and as I am writing this I should be finishing the grading of another 800 midterms for Algorithms & Datastructures. Just this grading has taken well over 1000 (wo)man-hours of teaching assistants and at least 200 of myself and my colleagues.

Throughout these different grading sessions, I found that I always go through the same cycle. Grading the first 20 or so exams is fine. I enjoy it. It is a great way to discover what parts of my lectures were clear to the students and what parts were not. Unfortunately after let's say 80 exams, you have seen most of the common mistakes. There are always some interesting answers that mix things up a bit, but most of it is simply reading a bunch of text that you have read over 80 times before, and scribbling some scores down. Fortunately the teaching assistants (TAs) are eager to help us out! As a team we set to work and struggle through the stacks and stacks of paper, making sure to take some breaks and discuss the interesting answers, eat home-made pasta, and learn about the maintenance required in taking care of an African land snail. I am pleased to report that after spending 2 weeks with the same team of teaching assistants I am now quite knowledgeable about the requirements of having one of these magnificent creatures as a pet.

Unfortunately the snail also provides an accurate mascot for the grading. So what can we do to increase the sluggish pace of grading? In this article I will open the curtains a bit on the backstage area of running a course. How do we (or maybe this is just me) go about creating and grading exams? What can we improve? And what are we doing right now to try and improve on that?

Writing Exams: from the teacher perspective

It is probably not controversial to say that exams are a big deal to students. Having studied the material of a course for 10 weeks, they have a 3-hour window to prove their understanding. A stressful affair to be sure. Perhaps it is a little more surprising to learn that as a teacher, I too am quite stressed about exams. I need to make sure the exam covers the material, is not too hard or too easy, is easily gradable, etc. To start this whole process, I can, fortunately, rely on the training from the UTQ (University Teaching Qualification).

First thing I do, is compile a list of learning objectives for the course and think about how many questions (or points) I want to allocate to that learning objective. If I have a distribution that satisfies me, I then draft ideas for

Figure 1: After learning all about them, a live specimen of the African land snail joined us in grading one day.

questions. They can be single-sentence drafts, like: 'MC-question: compute rec fun'. Usually this is the part that is still relatively easy. For an exam with 20 Multiple Choice questions and 5 open questions this part takes about an hour. Then comes the hard part, actually creating the questions. Something that can at least be parallelised over teachers, and for some courses even TAs. As those of you who have taken my exams know, I like to take inspiration from books, movies, and video games. Lawyers by the name of Phoenix, girls by the name of Lyra, and the detective duo of Sean and Michelle often feature in my exams. In the future you can expect a certain shelled animal to pop up. Did you know for instance that they require calcium to grow their shells? I find it easier to create these questions if they have a story that I am telling with them. When writing the first draft of my questions, they often contain flavor text to introduce a problem. Unfortunately this flavor text usually adds little to the exam and parsing this text can be cumbersome and waste the students' time during the exam. A lot of this flavor text therefore ends up on the cutting board in the second draft. For some questions it survives however, as questions in the real-world are not always clean and formally stated either. When creating the questions, I also create drafts of the answer model. Not only does this help ensure the question can be solved, it also provides insight into the difficulty of the question. If a multiple-choice question requires 10 sentences to explain the answer, it may be more difficult than a question, whose answer requires only 1 sentence of explanation.

The second draft of the exam contains a mixture of my questions and those of the other creators and this is the moment where the polishing begins. I ask the head-TAs to do the exam and give feedback. They always find mistakes, difficulty spikes, and propose new phrasings or even completely new questions. Another important data point they provide is the amount of time they spent on solving the exam. To gauge the length of the exam, I always try to design them in such away that my head-TAs can solve them in half the time of the exam, and me and my co-teachers can do it in a third of the set time.

When we are satisfied, the most terrifying moment in the whole process takes place: sending the exams to the printer. I, Making sure that I compiled the

document properly, am sending the latest version, have excluded the answers, and am requesting sufficiently many to be printed. I am very glad with the excellent support from the secretarial staff with the rest of this process.

Although printing them is terrifying, I am most nervous when the exam is about to start. It takes roughly the first 30 minutes of the exam for me to settle down again. If no major mistakes have been found in the first 30 minutes, then at least the first part of the exam seems to have been in order. Fortunately I can always rely on my head-TAs to also be present and help with answering questions while my nerves settle. Another three hours later (as a teacher I always need to wait for the extra time to end as well of course), me and the TAs leave the rooms, carrying our work for the next week(s).

Grading exams: a shortage of red pens

And with that, grading can begin. I communicate several time slots to the TAs and ask them to indicate when they can come over to help me out. Gathering the red pens I have collected over the last year, after many trips to the office of our secretaries, some kruidnoten and cookies, we can get started.

I instruct the TAs on how we will be grading. Every TA becomes part of a small team (4 TAs at most), where every team is assigned one (sub)question. We go through the grading rubric that I prepared in advance and then the team goes to work. I encourage them to discuss any cases that do not match the rubric and take careful notes of how they decided to grade them. As a result we end up with a much larger and more extensive rubric than we started with. After all questions have been graded it is time to digitise our grading efforts.

To help us during the exam reviews, we first sort all of the exams alphabetically by last name. Fortunately we teach many different sorting algorithms in Algorithms & Datastructures, so we have plenty of options to choose from. Unfortunately, it turns out that sorting methods optimised for a computer (e.g. Merge-Sort) do not necessarily work well for humans with large stacks in paper in front of them. But this is not even close to the worst part of it. After this, it is time to copy all of the scores for every (sub)question into an Excel-sheet. This can be parallelised of course, but even with 6 people it feels we are slugging through the pile.

Having entered all of them, we are almost done. To ensure we have made no mistake in transferring the scores, we go through all of them once more double-checking whether the score is correct in the sheet. We also check that we have sorted the exams correctly at this time.

Having done all this, we can finally move on to the last part of grading. We make a selection of exams to double check. It depends on the course how a selection for double checking is made, for instance for the midterm of Reasoning & Logic we took another look at everyone with a grade between 4.5 and 4.9 (as a 5.0 was the minimum grade to pass the course), as well as some exams randomly selected from the pile. The main goal is not necessarily to double-check if the grades are correct (though this is why these exams are selected, as these students are most likely to show up at the exam review anyway), but mostly to find out if there are questions that should be completely regraded. Sometimes for instance, we find that one question was graded too strictly or too lenient after all and we go through all exams again.

To give you some idea of how much time all of this costs, for a first-year exam this year it took us 300 hours to grade the exam, but another 30 to digitise the results, sort them, and double check about 5% of the exams.

Why multiple choice is not the solution

I realise that with the heading I have just written, I may have upset some of my colleagues. It may even be taken as criticism of the way they handle their exams. But please know that I do not mean it that way, so allow me to explain this claim. There are many courses in which multiple choice can test most, if not all, of the material just fine. Combine that with some lab work that tests the remainder of the skills and you are all set. Unfortunately,

some other courses cannot be tested in such a way in my opinion. Of course there are huge costs in terms of time spent grading (which scales very poorly with the number of students) and restrictions in terms of TA-availability and the three week limit on grading exam. This trade-off is one that me and my colleagues all balance in their own way.

For a course like Reasoning & Logic, in which proofs are a fundamental skill, multiple choice simply cannot test the creativity and structured way of working required for this course. Or so I think. Perhaps it is me lacking the skill to come up with sufficiently good multiple choice questions, but at least for proofs (and also automata) my colleagues seem to agree with me.

For computation-based questions, such as those found in mathematics, I can see how multiple choice questions can be used effectively, but I would still not be in favor of them. It puts, in my opinion, too much reward on the outcome of a set of computations, rather than the process. It is an interesting discussion and if you disagree then by all means please come by and have a chat. I am happy to be taught how to do more with multiple choice!

But for now it seems, that I should instead look into updating the way I grade exams, rather than how I create them.

Zesje: the solution?

As a computer scientist, the first thing I consider when it comes to speeding up something is, of course, my computer. How can this machine help me reduce the workload? It turns out that a physicist at our university thought the same thing some years ago. The result is *Zesje*, a system that allows you to scan the answers sheets of your exams and grade them digitally.

For every question you create a set of rubric items that together form the score. Every item can have a description, providing feedback to the students on what they did (in)correctly when answering the question. Multiple graders can set to work and (as soon as my merge request for it is done) can get a random exam to grade. With some JavaScript additions made by one of the TAs, we could soon grade the exams using only some keyboard shortcuts! No need to sort exams or spend hours transferring scores to an Excel-sheet. Even regrading a question was easy (One SQL-query later and we only had to regrade those exams that did not have a certain item marked). I would estimate that using Zesje easily cut 20% of our grading time (despite some start-up issues).
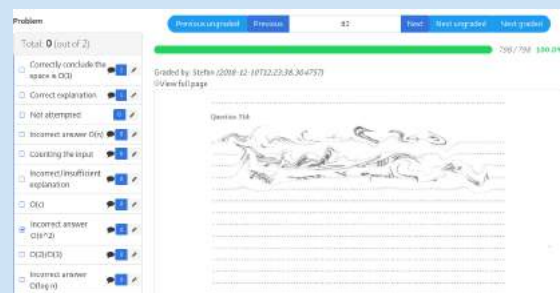
Figure 2: Grading in Zesje: the exam on the right, and the rubric on the left. The exam has been blurred on purpose, though even now it is more readable than some of the handwriting seen on exams.

So for me at least, Zesje is the way out. Due to its e-mail feature that sends all students a copy of their exam with the grading feedback attached, it makes sure a little of the effort that goes into grading actually helps the students, rather than just judging them. But of course, Zesje is not perfect either. Fortunately, it is open source[1]. So to all of you reading this, interested in helping us improve education (or specifically, grading exams), why not check it out and see if you can help close some issues?

---

[1] https://gitlab.kwant-project.org/zesje/zesje/

Improve reaction speeds on hacking attempts to provide greater insight in techniques and vulnerabilities used

Martijn Janssen

When finalizing your bachelor's degree at the Delft University of Technology, the final quarter contains the Bachelor End Project (BEP). The BEP is aimed at applying your accumulated knowledge about Computer Science on developing or expanding a real-world application in a collaborative setting.

Introduction

This BEP was carried out in collaboration with Nordin van Nes, Thomas Oomens and DutchSec. DutchSec is a company that specializes in security and has developed some very interesting products. In this day and age, more and more companies have exposed parts of their business to the internet, increasing the risk of being compromised. DutchSec aims to increase their knowledge about these attacks and provide more insight into the inner workings of these hacks and exploits. This is all used to keep data secure and make the world-wide-web a safer place.

When placing any device with a direct connection to the internet on a network, it being a server, an IP-camera or something else with an outside connection, it will receive thousands of hacking attempts every day. This is unavoidable, but for this reason protection is needed to keep these devices out of the hands of intruders. This can be done by finding the security leaks in these devices and patching these leaks to keep them updated.

The tool that DutchSec uses to achieve this goal is Honeytrap. Honeytrap is a fully open-source honeypot solution written in Go, which is able to deploy fake environments to trap hackers. These fake environments simulate a real server, tricking the hacker into thinking he is connected with a real server. When a hacker is trapped, all the activity is logged and stored for review and analysis at a later point. One of the main strengths of Honeytrap is the ability to use a single solution for multiple problems. Whereas all other honeypot implementations only work for one service (SSH or HTTP or PostgreSQL), Honeytrap is able to implement all of these in a single program and be extendable. If a new service is built like Ethereum, the feature to support Ethereum simulation can simply be added to Honeytrap by writing this service, while still being able to support all the other previously supported services.

Everywhere in this text where the term 'hacker' or 'attacker' is used, this can be a literal hacker, or some program that is running on another (compromised) system. This program is trying to recruit other systems in it's network, forming a botnet of hundreds, thousands or even millions of systems.

An example: When a hacker connects with SSH to the Honeytrap instance, Honeytrap acts like a server, showing all the correct information to the intruder and allowing every or some username password combinations to result in a successful login. From there, the attacker will see a commandline where commands can be entered, just like on a normal server. For some commands there will be a predefined response, and some commands will give the response that it is not found. When returning less **command not found** responses, it will be more likely that the hacker will continue to try and compromise the system. Most of the time the hacker will stop when a specific command is not found. This directly results in collecting less data about attack vectors.

Problem definition

The main problem with the current implementation of Honeytrap is the reaction speed on changes in the attack methods. Since there are so many rapid changes to the ways hackers are able to attack a system, it's hard to keep up. Currently, every change to Honeytrap, how small or big, requires the maintainers to create a Pull Request and go through the review process, release a new version of Honeytrap and deploy this to all the running Honeytrap instances. Deploying it to these instances requires a reboot of Honeytrap, causing downtime and possibly missing critical information.

This is not a process that customers and DutchSec themselves like, when the hacker comes across a command that is unrecognized, the hacker quite possibly stops attacking that system. The goal is to be able to react immediately to the changes in the attack, allowing a next attacker to receive the correct response. It should also allow for the writers of the Lua scripts to track attackers over different sessions, store information in the scripts may the attacker revisit the honeypot or to exchange information between the Lua and Go code.

The last request that was made was to make the Lua scripting expandable, suitable for some sort of app-store or in some way shareable. This would allow DutchSec to cater to the wishes of their enterprise customers, allow for a more orchestrated way of deploying Honeytrap.

Solution

To speed up the process of deploying new code, we are mainly looking at the usage of non-compiled solutions. If we were looking at compiled solutions, we would still have to wait for the amended code to be compiled and be available for usage by Honeytrap. Looking at the available options to implement this, we had 2 choices: Lua and Javascript. This was mainly due to the fact that these were the only non-compiled languages that had decent or good support in Go. The customer had a slight preference to Lua, and it also aligns with the vision of Lua itself: "Lua is a powerful, efficient, lightweight, embeddable scripting language".

The first version of Lua scripting in Honeytrap was ready quite quickly, allowing us to test in a live environment. We already had a Honeytrap instance deployed on a public ip, and another connected with a domain collecting traffic to create a general impression of the data we could expect to receive. After deploying the updated version of Honeytrap with Lua scripting, containing

a simple script replying to a request that was made quite often, the traffic was observed. After replying to these requests, traffic gradually increased for the server, receiving some different requests than before the script was running. The speed at which we could change the contents of the responses and how Honeytrap handled them made it very easy to tailor our responses to the incoming messages.

After the initial code was expanded to allow importing different Lua files, methods and allow for calling Lua methods from Go and vice versa, general http handling code was constructed. Around this time, several requests were popping up, calling the **/GponForm/diag_Form?images/** endpoint on our Honeytrap. After some searching, it became clear that this was some kind of router vulnerability, allowing the attacker to execute commands on the router without permissions, resulting in remote code execution. A diagnostic endpoint **/diag.html?images/** on this same piece of software contained another vulnerability, allowing the attacker to see the result of his command. These two combined, result in a very easily hackable system. These two vulnerabilities resulted in a handful of binaries, scripts and compromised ip's (mostly resulting from other hacked routers), which proved the increased effectivity of such a system.

Expanding the system

After seeing these results, we were eager to implement other parts of Lua scripting. Allowing storage of variables in the Lua scripts, storing the Lua state over connections to allow the attacker to come back later and have the same data, makes the simulation less random. Another quite important feature that was added at this point is calling Go methods from Lua and Lua methods from Go, making our logging solution better and perform actions like downloading malware or checking page-contents.

Now downloading malware resulted in some very unexpected results. Before, we thought that some malware was just old or no longer used. A portion of the links in our logs were no longer up at the time we checked them, there were no files of binaries. After having the file download ready, some of these links that previously contained no content, now were immediately downloaded. Some time after downloading the link went down again, resulting in the original situation of having no content to download manually. The most important observation here is that these links may not be up or contain content all the time. These links sometimes only contain content when the actual attack is being performed. Sometimes the link was only up for a duration shorter than 5 minutes, reducing the chance that the contents of the link is found.

Experimenting further by supplying potential login information in a simple **passwords.txt** file on a 'fake filesystem' when simulating command line access on the server also proved quite successful. The **passwords.txt** file would contain some sample `username:password` combinations which could be used to log in with SSH. From the traffic, the conclusion could be drawn that some attackers have a quite sophisticated technique. A couple of servers are scouting for new information on public machines, while another machine acts on the found information by logging into Honeytrap after some time and executing malicious commands, having made no previous (incorrect) login attempts on Honeytrap.

While some attackers were trapped in Honeytrap and thought they gained access to our systems, they started performing speedtests using a free public speedtesting provider. Probably filtering out the high-speed systems, identifying high-bandwidth machines to be used at a later point for DDOS attacks. Possibly this could be used to discard the low-bandwidth machines, minimizing the risk of being caught.

Upon suggestion of our supervisor at the Delft University of Technology, we started looking at a bit more data collection. It's very interesting to see what happens when different results are given for the same request. Putting our Lua scripter to the test, an AB-Tester was written completely in Lua, allowing us to select a different response for all the incoming connections from a list of predefined responses. This resulted in a clustering in the responses and reactions received, showing the attackers' preferences for specific machines. Some machines peaked their interest, but some others resulted in traffic dropping to almost zero.

Running a Lua script that simulates an infection flow can result in cool results: after a couple of weeks, our Honeytrap started receiving forwarded requests from another URL. Combined with the fact that we observed some hacked routers serving html content when visited, it became clear that attackers are using compromised systems to perform illegal webhosting. To give an example: the hacker is in possession of some domain that is not his and has obtained a hacked router. This domain can be forwarded to the router to be used to host phishing pages, ads and scams (win a free iPhone). This is a great way to get reliable low-traffic webhosting, without costs or the hassle of having to deal with hosting companies which obviously don't allow these kinds of websites on their platforms.

Conclusion

From all our findings, the information gathered and behavior observed, we can safely conclude that Lua scripting is the way for Honeytrap to Go. It greatly reduces the speed at which deployments can be performed, but at the same time allowing for more ease of use, resulting in more information gathered. It also shows that all the current honeypot implementations are lacking, not even approaching a part of their full potential. All these specific techniques seen in our analysis show that the current Honeytrap implementation can be improved significantly. Our BEP has proved that Lua scripting is the direction to take for Honeytrap, and that it also greatly increases the output of Honeytrap, finding more interesting content.

This BEP has allowed us to learn a lot about a field that we were very interested in, while working on a great project, collaborate with smart people, expanding a product and giving back to the open-source community. If you are interested in running Honeytrap yourself, feel free to do so, all code is public and hosted at 'github.com/honeytrap/honeytrap'.

If you want to read our full report, visit the Delft University of Technology repository and search for "Extending Honeytrap with Lua scripting" in the education repository, or visiting this page: 'https://repository.tudelft.nl/islandora/object/uuid%3Aae1c32d9-662a-4f42-b920-f68c9d5b9771'. If you have questions, feel free to contact me: martijngajanssen@gmail.com.

De Delftse Bedrijvendagen

What does your future look like?

'De Delftse Bedrijvendagen' offers you a great opportunity to kick start your career. 'De Delftse Bedrijvendagen' is the largest technical career fair in the Benelux and takes place at the Aula conference centre of the Delft University of Technology. Four events organized in February, March, April and May will give you an excellent preparation for your future career. The four events form building blocks to connect you to your dream job. Use our event to find an internship, graduation assignment or a starters position. Not sure what direction you want to go? The 'Delftse Bedrijvendagen' has 150 companies ready to meet you.

Building blocks

1. Get ready at the Application trainings by following workshops from top companies.
2. Orientate yourself at the largest technical career fair of the Benelux by visiting the Presentation Days.
3. Get an on-site impression of a company by joining an in-house day.
4. Talk to a recruiter of a company of your choice during the Interview days.

How to join

Past year over 3300 students visited the 'De Delftse Bedrijvendagen', want to join this edition? Subscribe for the 2019 edition! The application opens on the 7th of January. By subscribing you can attend all events, but all events can also be attended separately.

You can subscribe at the website ddb.tudelft.nl or on 22, 23, or 24 January at the desk in the Aula. Up until the 25th of January subscription is available at a reduced price. The subscription closes the 22nd of February.*

*All personal information will be handled with care as our privacy policy rescribes

Contact
'De Delftse Bedrijvendagen' is organized by
Vereniging voor Technische Physica Applied Physics
Gezelschap Leeghwater Mechanical Engineering
Technologisch Gezelschap Chemical Engineering
VSV 'Leonardo da Vinci' Aerospace Engineering
W.I.S.V. 'Christiaan Huygens' Applied Mathematics
and Computer Science

De Delftse Bedrijvendagen secretariat
Mekelweg 2, 2628 CD Delft

Tel: +31 (0)15 278 1900
Email: ddb@ddb.tudelft.nl
ddb.tudelft.nl

Events

👔 Application Days

A good preparation is half the battle. At the application days recruiters from high ranked companies will provide trainings for job application. Refresh your LinkedIn profile picture with a photo taken by a professional photographer and get your resume checked by an expert.

📈 Presentation Days

Meet 150 national and international companies at the career fair. Companies, ranging from consultancy to engineering, come to the Aula conference centre. At the presentation days you can orientate yourself by attending presentations or visiting info stands.

🏢 In-house Days

In-house Days offer an opportunity to form a better, more complete idea of the companies you are interested in. Your resume will be forwarded to the companies of your choice. Based on the resumes the companies will select the participants. You can sign up for the In-house Days until the 24th of February, the Sunday after the Presentation Days.

💬 Interview Days

At the one-one-one interviews there is an opportunity to have an orientating talk or have the first interview of an application process. Your resume will be sent to companies you are interested in. You will receive an overview of which companies are interested in meeting you, and from these you can make a selection.

Important Dates

7 January
Registration open

25 January
Deadline reduced
(entree fee)

12, 13 & 14 February
Application Trainings

18,19 & 20 February
Presentation Days

22 February
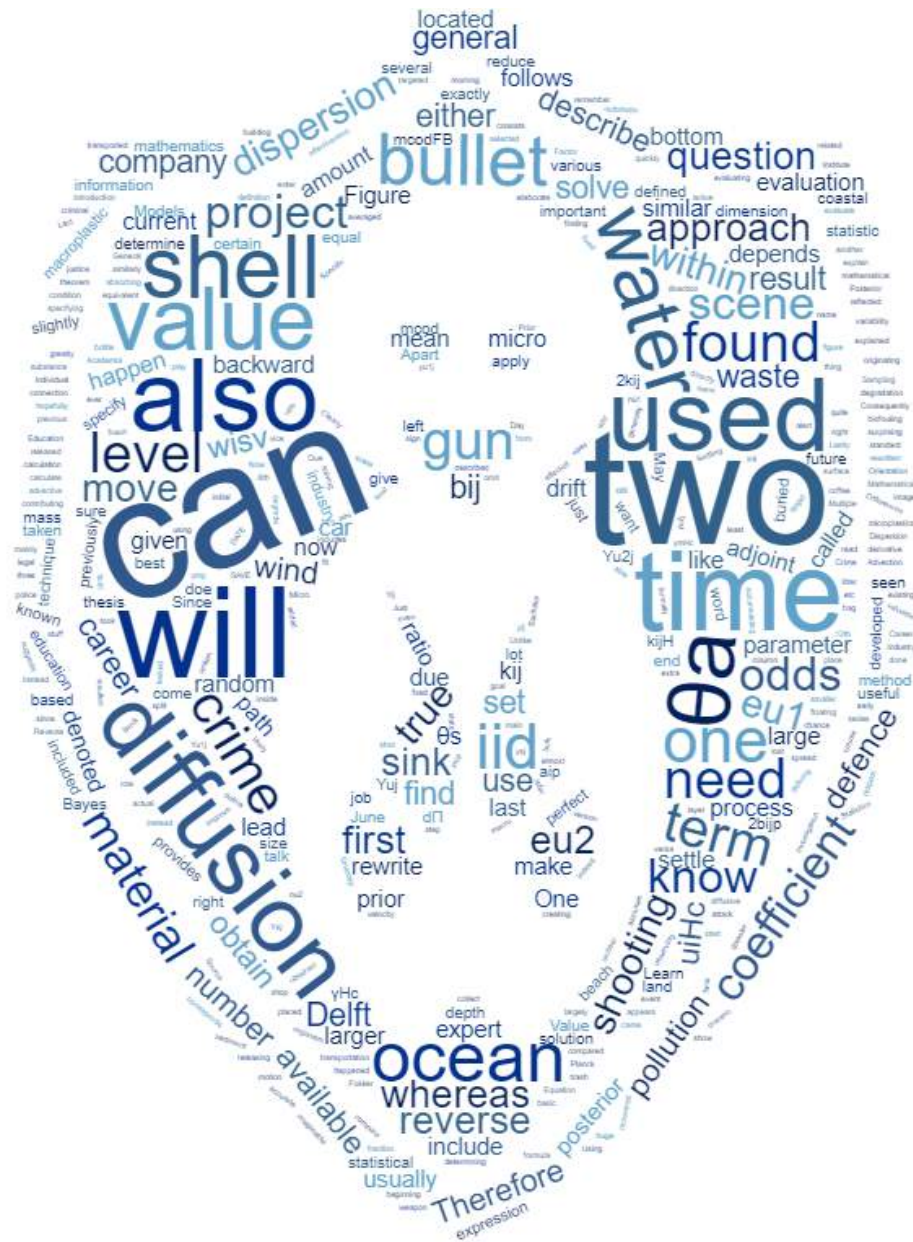Subscription closes

18 - 29 March
In-House Days

13 - 24 May
Interview Days

Mathematics

Statistical Modelling of Forensic Evidence

Inoni van Dorp

May 8th, 2018. Multiple shots are fired at the Peperstraat in Delft with an automatic firearm. The forensic experts arrive at the crime scene quickly and are able to collect several bullet shells, which are then transported to the Netherlands Forensic Institute for further investigation.

Statistics plays an important role in the evaluation of forensic evidence. The shooting that was mentioned in the introduction was targeted at one of the coffee shops located in Delft. This was just the beginning of a series of criminal events last May and June. In the early morning of June 12th, another shooting took place at the Molslaan in Delft, but this time it was unclear what the target of the attack was.

Figure 1: Crime scenes after the shooting in the Peperstraat (left) and the Molslaan (right). Source: In de buurt Delft

Both shootings can be used to explain the two possible forensic identification of source questions usually considered in the evaluation of forensic evidence. One of the possible questions of interest might be if the bullet shells found at the two crime scenes come from the same unknown gun, or in other words, if the two crimes are related. This will be called an *identification of common source problem*.

In the night after the shooting at the Molslaan, three suspects were arrested by the police. In their car, several weapons were found. The possible question of interest might then be if the bullet shells from one of the crime scenes came from the gun found in the car of the suspects. This is called an *identification of specific source problem*, since we want to know if the bullet shells come from a specific, known gun.

To specify the statistical models corresponding to the two identification of source questions, we need two sets of evidence to evaluate and a set of background material to compare the evidence with. Then two competing hypotheses need to be formulated: the hypothesis H_p will be presented by the prosecutor, whereas the hypothesis H_d corresponds to the defence. Lastly, we need to define sampling models corresponding to the prosecutor's and defence's hypothesis. These will specify the statistical models corresponding to each hypothesis.

Common source problem

In the common source problem, the available evidence is denoted by $e = \{e_{u_1}, e_{u_2}, e_a\}$, where e_{u_1} denotes the first unknown source evidence, for example the bullet shells found at the Peperstraat; e_{u_2} denotes the second unknown source of evidence, for example the shells from the Molslaan; and e_a denotes the available background material. The hypotheses for the common source problem are usually formulated as follows:

H_p : The two sets of unknown source evidence (e_{u_1} and e_{u_2}) both originate from the same unknown source.

H_d : The two sets of unknown source evidence (e_{u_1} and e_{u_2}) originate from two different unknown sources.

Specific source problem

In the specific source problem, the available forensic evidence now consists of $e = \{e_u, e_s, e_a\}$. Here, e_u denotes the unknown source evidence, for example the bullet shells found at the Peperstraat or the Molslaan; e_s denotes the specific source evidence, for example bullet shells from the gun found in the car of the suspects; and again e_a denotes the available background material. The hypotheses for the specific source problem are usually formulated as follows:

H_p : The unknown source evidence e_u and the specific source evidence e_s both originate from the specific source.

H_d : The unknown source evidence e_u does not originate from the specific source, but from some other unknown source.

General two-level model

Before specifying the sampling models for the common and specific source problem, the general two-level model used in forensic statistics needs to be explained. This model assumes two levels of variation in the generation of forensic evidence. The first level is the between-source variation, which will be denoted by the distribution $G(\cdot|\theta_a)$. Suppose that we want to know how the bullet shells found at the crime scene are generated. Then the between-source variation models the variability between all possible guns that might have been used at the crime scene.
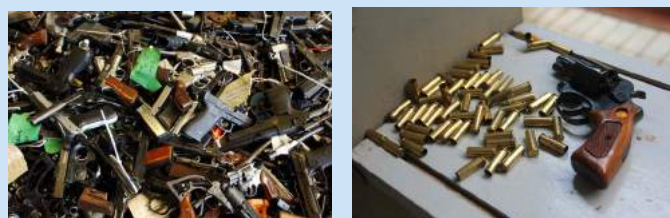
Figure 2: An example of between-source variation (left) and within-source variation (right).

The second level is the within-source variation, which is denoted by the distribution $F_a(\cdot|\theta_a, a_i)$, where a_i denotes the source we condition on. Suppose that a gun is selected from the between-source distribution. Then the bullet shells originating from that gun will not be exactly similar, and this is modelled by the within-source variation. This general two-level model will be used frequently in defining the common source and specific source sampling models.

Sampling models

The common source sampling models are formally defined as follows: the background material $e_a = (y_{ij}, 1 \leq i \leq n_a, 1 \leq j \leq n_i)$ is assumed to be generated according to the general two-level model

$$A_i \overset{\text{iid}}{\sim} G(\cdot|\theta_a) \quad \text{and} \quad Y_{ij}|A_i = a_i \overset{\text{iid}}{\sim} F_a(\cdot|a_i, \theta_a).$$

The first unknown source evidence $e_{u_1} = (y_{u_1 j}, 1 \leq j \leq n_{u_1})$ is assumed to be generated similarly

$$P \sim G(\cdot|\theta_a) \quad \text{and} \quad Y_{u_1 j}|P = p \overset{\text{iid}}{\sim} F_a(\cdot|p, \theta_a).$$

However, the generation of the second unknown source evidence $e_{u_2} = (y_{u_2 j}, 1 \leq j \leq n_{u_2})$ depends on which hypothesis is assumed to be true. According to the prosecution, we have

$$Y_{u_2 j}|P = p \overset{\text{iid}}{\sim} F_a(\cdot|p, \theta_a),$$

whereas the defense will state that

$$D \sim G(\cdot|\theta_a) \quad \text{and} \quad Y_{u_2 j}|D = d \overset{\text{iid}}{\sim} F_a(\cdot|d, \theta_a).$$

In the specific source problem, the sampling model of the background material is exactly similar to the common source background sampling model. However, the specific source evidence $e_s = (y_{sj}, 1 \leq j \leq n_s)$ is assumed to be generated by

$$Y_{sj} \overset{\text{iid}}{\sim} F_s(\cdot|\theta_s),$$

where $F_s(\cdot|\theta_s)$ can be seen as the within-specific-source distribution. This means that there is no between-source variation for the specific source evidence! The generation of the unknown source evidence $e_u = (y_{uj}, 1 \leq j \leq n_u)$ depends on which hypothesis is assumed to be true. Under the prosecution model, we have

$$Y_{uj} \overset{\text{iid}}{\sim} F_s(\cdot|\theta_s),$$

whereas under the defense model

$$D \sim G(\cdot|\theta_a) \quad \text{and} \quad Y_{uj}|D = d \overset{\text{iid}}{\sim} F_a(\cdot|d, \theta_a).$$

If you are lost due to all the mathematical formulas above, just remember that the most important difference between the common source and specific source problem is that in the common source problem all sources are assumed to be *unknown*, whereas in the specific source problem one of the sources is *known*.

Value of evidence

The sampling models are our building blocks for the value of evidence, but the actual question of interest is which hypothesis is most probable after observing all evidence. This is reflected by the posterior odds

$$\frac{\mathbb{P}(H_p|e)}{\mathbb{P}(H_d|e)}.$$

If the posterior odds are larger than one, the prosecutor's hypothesis is more probable than the defence hypothesis after evaluating all evidence. Since the posterior odds cannot be determined directly, we can use Bayes' theorem to split it into two fractions:

$$\frac{\mathbb{P}(H_p|e)}{\mathbb{P}(H_d|e)} = \frac{\mathbb{P}(e|H_p)}{\mathbb{P}(e|H_d)} \cdot \frac{\mathbb{P}(H_p)}{\mathbb{P}(H_d)},$$

or in words,

$$\text{Posterior odds} = \text{Value of evidence} \times \text{Prior odds}.$$

In the evaluation of evidence, the forensic experts are tasked with determining the value of evidence, whereas legal experts have to determine the probability of occurrence of the two hypotheses without considering the recovered evidence, i.e. the prior odds.

There are two approaches to determine the value of evidence. According to the frequentist approach, the value of evidence is given by the likelihood ratio

$$LR(\theta; e_u) = \frac{f(e_u|\theta, H_p)}{f(e_u|\theta, H_d)}.$$

This is, as the name suggests, the ratio of two likelihoods, where either the prosecutor's hypothesis or the defence hypothesis is assumed to be true. The likelihood ratio depends on the parameter θ, which has a fixed but unknown true value. Therefore, the best a frequentist can do is to estimate the true value of θ based on the background material.

However, according to the Bayesian approach, the value of evidence is given by the Bayes Factor

$$BF(e) = \frac{\int f(e|\theta, H_p) \, d\Pi(\theta|H_p)}{\int f(e|\theta, H_d) \, d\Pi(\theta|H_d)}.$$

The parameter Θ is now seen as a random variable itself, which has a prior distribution. Therefore, the likelihoods need to be integrated over all possible values of Θ with respect to this prior distribution.

Closure

If you have understood most of the aforementioned, I can congratulate you: you are now familiar with the basics of forensic statistics! There is a lot more interesting stuff to read about. For example, in my thesis I considered two frequently used combinations of within- and between-source distributions, corresponding to continuous or discrete evidence. Using these models the difference between the value of evidence resulting from the common source problem and the specific source problem was evaluated. Spoiler alert: in most situations the common source problem gives more conservative values of evidence than the specific source problem. So, if you ever have to face justice, make sure you can convince them that the crime fits best in the common source framework :-)

References
[1] Ommen, D.M., *Approximate Statistical Solutions to the Forensic Identification of Source Problem*, PhD thesis, 2017

[2] van Dorp, I.N., *Statistical modelling of forensic evidence*, Master's thesis, Delft University of Technology, The Netherlands, 2018

Mathematics

Reverse time moving and settling of plastic in coastal waters

Elsje Burgers

The plastic pollution in our oceans is an environmental disaster. To reduce the amount of plastic, it is useful to know how the plastic moves, degrades and sinks. Models are being developed that describe the behaviour of this plastic pollution.

Plastic pollution is worldwide a huge problem. The use of plastic has greatly increased over the last decades and is expected to increase even more in the future. As a result, there is an increasing amount of plastic that ends up in our oceans. Unfortunately, this does a lot of harm to the oceanic ecosystems. There is an increasing number of projects that aim to reduce the amount of plastic waste in our oceans. This can either be done by making sure there is less plastic waste entering the ocean or by cleaning up the waste that is already there. To optimize the effectiveness of plastic waste removal it is necessary to know how the plastic litter moves, degrades and sinks.

Models are being developed that can describe what happens with plastic particles in the ocean but unfortunately this is quite complex. There is a large number of processes and parameters that need to be taken into account to make an accurate model. I based my project mainly on the model of K. Critchell and J. Lambrechts [1], which is visualized in figure 1.
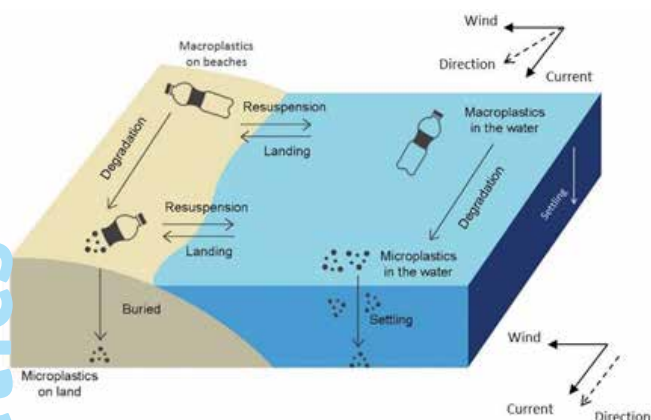

Figure 1: This image shows what can happen to plastic particles when they are located in coastal waters. [1]

This model starts with macroplastics that enter the coastal water. macroplastics are defined as plastic particles with a size larger than 5 mm, which means that macroplastics could be almost all the plastic trash imaginable (bottles, bags, packaging, etc.). In general the macroplastics will float on the water. Over time a few things can happen with a macroplastic. Of course the macroplastic will move due to processes like wind, current and dispersion. The macroplastics could then land on the beach and there either be buried or resuspended in the ocean. Apart from moving, the macroplastics could also sink and settle on the bottom of the ocean. Once settled, it is assumed a particle

stops moving. Last but not least, the macroplastics can also degrade, creating micro-plastics, which are plastic particles with a size smaller than 5 mm.

Unlike macroplastics, micro-plastics are assumed to be spread through the water column instead of floating on the water. This means that when they move, they will not be affected by the wind. Just like macroplastics, they also have a chance to sink and settle on the bottom of the ocean. Micro-plastics can also land on the beach and there again either be buried or resuspended. The main goal of my Bachelor thesis was to include the settling of particles in both the forward and reverse time equations that describe the movement of plastic particles in the water.

Advection-diffusion equation

To understand how the settling can be included, we first have to understand how the plastic particles move. The movement of macro and microplastics is similar. The particle's movement is largely determined by bulk movements like the wind and the current. However, there is also a random movement contributing to the transportation. This is called dispersion. Dispersion can be compared with diffusion but on a larger scale. Since there is both advective and diffusive transport, the advection-diffusion equation can be used to describe the movement of plastic particles in the water. For two dimensions this is the following equation:

$$\frac{\partial Hc}{\partial t} = \sum_{i=1}^{2} -\frac{\partial u_i Hc}{\partial x_i} + \sum_{i=1}^{2}\sum_{j=1}^{2} \frac{\partial}{\partial x_i}\left(k_{ij}H\frac{\partial c}{\partial x_j}\right). \tag{1}$$

Here H is the water depth, c is the depth-averaged concentration of plastic particles, u_i is the velocity of the plastic particles due to current and wind in the x_i direction and k_{ij} is the dispersion coefficient. There are various methods to solve the advection-diffusion equation. In my project I used a Lagrangian approach. I modelled the motion of a large number of individual particles to obtain a value for the concentration.

Kolmogorov forward equation

Due to the random movement of the plastic particles in water, their position can also be described by a probability distribution. This probability distribution is different for each timestep. The probability distribution of for a particle can be obtained by solving the Kolmogorov forward equation, also know as the Fokker-Planck equation.

If at a time s a particle is at position y, the Kolmogorov forward equation will give the probability distribution for the position of that particle at a future time $t > s$. This provides valuable information, for example where the particle will be likely to end up and what will be possible paths taken by this particle. The Kolmogorov forward equation for two dimensions can be written as:

$$\frac{\partial p}{\partial t} = -\sum_{i=1}^{2}\frac{\partial a_i p}{\partial x_i} + \sum_{i=1}^{2}\sum_{j=1}^{2}\frac{\partial^2 b_{ij}p}{\partial x_i \partial x_j}. \tag{2}$$

Here p is the probability distribution for a certain time, given the initial time and position of a particle, a_i is the drift coefficient and b_{ij} is the dispersion coefficient.

It might not be surprising that there is a connection between the advection-diffusion equation and the Kolmogorov forward equation. The concentration distribution of the advection-diffusion equation is equivalent to the result you would obtain by releasing a large number of particles with the probability distribution of the Kolmogorov forward equation. Therefore, it is easy to rewrite the advection-diffusion equation into the Kolmogorov forward equation by using the transformation $c = \frac{p}{H}$ and a slightly different definition of the drift coefficient [2]. Consequently, the solution for the advection-diffusion equation also provides a solution for the Kolmogorov forward equation and vice versa.

Settling

As previously mentioned, it is possible that particles sink and settle on the bottom of the ocean. There are various processes that can lead to settling, for example degradation, absorbing water or other substances and biofouling (a layer of micro-organisms accumulating on the surface). The settling of particles is generally not included in transport models. In my project I have used techniques that were previously used for the settling of sediment to add the settling to the transport equations. This resulted in the following expression for the Kolmogorov forward equation:

$$\frac{\partial p}{\partial t} = -\sum_{i=1}^{2} \frac{\partial a_i p}{\partial x_i} + \sum_{i=1}^{2}\sum_{j=1}^{2} \frac{\partial^2 b_{ij} p}{\partial x_i \partial x_j} + \frac{\partial \gamma m p}{\partial m}. \qquad (3)$$

The last term is the 'settling term', γ is the settling rate which is depending on the time and position of the particle and m is the mass of the particles. Now p is a slightly different probability distribution. Apart from the time and position, p is also depending on the mass of the particles. Equation 3 can be rewritten into this advection-diffusion equation that includes a settling term:

$$\frac{\partial Hc}{\partial t} = \sum_{i=1}^{2} -\frac{\partial u_i Hc}{\partial x_i} + \sum_{i=1}^{2}\sum_{j=1}^{2} \left(\frac{\partial}{\partial x_i} \left(k_{ij} H \frac{\partial c}{\partial x_j} \right) \right) - \gamma Hc. \qquad (4)$$

I will not elaborate on the methods used to obtain these results but for more information I refer to [3] and [4].

Reverse time

Instead of finding out what will happen to a particle when it is released, it can also be useful to know what has happened with a particle before it was located at a certain position. This could be used to find for example the source of pollution. In reverse time, we can use the Kolmogorov backward equation, which is equal to:

$$\frac{\partial p}{\partial s} = \sum_{i=1}^{2} a_i \frac{\partial p}{\partial y_i} + \sum_{i=1}^{2}\sum_{j=1}^{2} b_{ij} \frac{\partial^2 p}{\partial y_i \partial y_j}. \qquad (5)$$

This is the adjoint of the Kolmogorov forward equation [2]. Differences with equation 2 are the sign of the first term and the position of the coefficients a_i and b_{ij}.

To find a reverse time advection-diffusion equation, we have to rewrite the Kolmogorov backward equation. This leads to the following expression for the reverse time advection-diffusion equation:

$$\frac{\partial Hc}{\partial s} = \sum_{i=1}^{2} \frac{\partial u_i Hc}{\partial y_i} + \sum_{i=1}^{2}\sum_{j=1}^{2} \left(-\frac{\partial}{\partial y_i} \left(k_{ij} \frac{\partial Hc}{\partial y_j} \right) + Hc \frac{\partial^2 k_{ij}}{\partial y_i \partial y_j} \right). \qquad (6)$$

An extra term appears because the drift and dispersion coefficients are placed inside the derivative again. This makes is possible to use the same techniques that were used on equation 1 to solve this equation.

To include the settling of the particles in the reverse time equations, we also need to calculate the adjoint of the settling term $\frac{\partial \gamma(x,t) m p}{\partial m}$. I will omit the calculations but the adjoint of the settling term is equal to

$$-\gamma(x,t) m \frac{\partial p}{\partial m}. \qquad (7)$$

This is added to the Kolmogorov backward equation to obtain the following result:

$$\frac{\partial p}{\partial s} = \sum_{i=1}^{2} a_i \frac{\partial p}{\partial y_i} + \sum_{i=1}^{2}\sum_{j=1}^{2} b_{ij} \frac{\partial^2 p}{\partial y_i \partial y_j} - \gamma(x,t) m \frac{\partial p}{\partial m}. \qquad (8)$$

As a final step, we rewrite equation 8 into the form of the advection-diffusion equation. This lead to this equation:

$$\frac{\partial Hc}{\partial s} = \sum_{i=1}^{2} \frac{\partial u_i Hc}{\partial y_i} + \sum_{i=1}^{2}\sum_{j=1}^{2} \left(-\frac{\partial}{\partial y_i} \left(k_{ij} \frac{\partial Hc}{\partial y_j} \right) + Hc \frac{\partial^2 k_{ij}}{\partial y_i \partial y_j} \right)$$
$$\frac{\partial \gamma m Hc}{\partial m} + \gamma Hc. \qquad (9)$$

Clearly, equation 9 is more complex to solve than the previous versions of the advection-diffusion equation. However, it is still possible to solve this equation with a Lagrangian approach. Therefore, this equation can indeed be used to include the settling of particles to the standard transport model for plastic particles and hopefully this could improve the existing models.

References

[1] K. Critchell and J.Lambrechts. *Modelling accumulation of marine plastics in the coastal zone; what are dominant physical processes*. Estuarine, Coastal and Shelf Science, 171:111-122, 2016.

[2] Syed Hyder Ali Muttaqi Shah. *Lagrangian modelling of transport processes in the ocean*. PhD Thesis, TU Delft, September 2015.

[3] Wilson Mahera Charles. *Transport modelling in coastal waters using stochastic differential equations*. PhD Thesis, TU Delft, March 2007.

[4] H.F.P. van den Boogaard, M.J.J. Hoogkamer and A.W. Heemink. *Parameter identification in particle models*. Stochastic Hydrology and Hydraulics, 7:109-130, 1993.

Mathematics

Mathematical Career Orientation Day

Industry | Academia | Education

SAVE
THE DATE

➤ **April 3rd 2019** ◄

One–on–one talks with companies

Learn about the career paths of other alumni of Mathematics and how they apply mathematics in their industry. This is also the perfect opportunity to find a job, internship or graduation project at one of the participating companies!

Presentations about a career in academia or education

🌐

wisv.ch/mcodFB

wisv.ch/mcod

Wiskunde Informatica Studievereniging 'Christiaan Huygens'

Miscellaneous

Historical Person: Sophie Germain

Eva Slingerland

Every edition of the MaCHazine discusses a historical person. For this number, we will tell you about the life and career of Sophie Germain, a female mathematician who played an important role in Number Theory.

Soeur GERMAIN (portrait de), à l'âge de 11 ans.

Early life

Born on April 1st in 1776, Marie-Sophie Germain grew up in a family with two sisters in Paris. She was a withdrawn child that turned to her father's library for entertainment. There she read about Archimedes and learned herself Latin and Greek to read the works of Sir Isaac Newton and Leonhard Euler. Unfortunately, her parents didn't approve of this interest in mathematics, because they felt it was inappropriate for a woman. Therefore, they denied her warm clothes and a fire to keep her from studying. Sophie studied during the nights anyway, by using the light of candles and warmth of blankets.

When she was 18 years old, the École Polytechnique opened. As a woman she wasn't allowed to attend, so she used the name Monsieur Antoine-August LeBlanc, a former student, when sending in work. She most likely received the lecture notes from her friends. However, when Lagrange saw the intelligence of this M. LeBlanc, he set up a meeting and therefore Sophie was forced to reveal her true identity. Lagrange luckily did not mind all this and became her mentor to help her with her work.

She used the same name when she wrote a letter to Carl Friedrich Gauss. He also ended up finding out about her true identity, to which he replied: *'But how can I describe my astonishment and admiration on seeing my esteemed correspondent Monsieur LeBlanc metamorphosed into this celebrated person, yielding a copy so brilliant it is hard to believe? ... But when a woman, because of her sex, our customs and prejudices, encounters infinitely more obstacles than men, in familiarizing herself with [number theory's] knotty problems, yet overcomes these fetters and penetrates that which is most hidden, she doubtless has the most noble courage, extraordinary talent, and superior genius.'* Sophie's correspondences with Lagrange and Gauss continued throughout her life.

Contributions to science

Next to mathematics, Sophie was also interested in philosophy and physics. This explains how her work shifted from number theory to more applied mathematics. In 1816, after two attempts, she finally won the grand prize from the Paris Academy of Sciences for her essay on an experiment concerning vibrating metal plates. She was the first woman ever to win a prize from this academy. She continued to work on elasticity theory, but her interest for number theory was renewed. Her most significant result in this area was her contribution to the proof of Fermat's Last Theorem, which states that there are no three positive integers x, y, z that satisfy the equation $x^n + y^n = z^n$ for any integer n greater than 2. We can identify two cases here:

1. n doesn't divide any of x, y or z
2. n divides at least one of x, y or z

Sophie Germain's theorem states the following on case 1: Let p be an odd prime. If there exists an auxiliary prime $q = 2Np + 1$, where N is any positive integer not divisible by 3 such that:

1. if $x^p + y^p + z^p = 0 \ (\mod q)$ then q divides xyz and
2. p is not a pth power residue $(\mod q)$

Then case 1 of Fermat's Last Theorem holds true for p. Legendre used this result for the case $p = 5$ in his complete proof of the theorem. Furthermore, she also set up the principle of Sophie Germain prime numbers, or safe primes. A number p is a Sophie Germain prime number if p is prime and $2p + 1$ is also prime. These numbers are useful for applications in public key cryptography and primality testing.

Death and commemoration

On the 27th of June in 1831, Germain died due to breast cancer. Unfortunately, due to prejudices against her sex, she was never able to make a career out of her interest for mathematics, physics and philosophy. So despite her intellectual achievements, her death certificate listed her as a property holder, and not as a mathematician. When the matter of honorary degrees came up at the university of Göttingen in 1937, Gauss recommended to award her with honorary degree: 'she [Germain] proved to the world that even a woman can accomplish something worthwhile in the most rigorous and abstract of the sciences and for that reason would well have deserved an honorary degree.' Since 2003, the Sophie Germain Prize is awarded to honor French mathematicians for research in the foundations of mathematics.

References
[1]   ttps://www.sdsc.edu/ScienceWomen/germain.html

[2]   ttps://www.britannica.com/biography/Sophie-Germain

[3]   ttps://blogs.scientificamerican.com/roots-of-unity/gauss-and-germain-on-pleasure-and-passion/

Miscellaneous

Mathematical Puzzles

Kilian Buis

Problem 1

Suppose you have an engine that needs two batteries to work. You have 8 available batteries; 4 working ones and 4 broken ones. You do not know which ones are working and which are not. You could of course try all $\binom{8}{2} = \frac{8 \cdot 7}{2} =$ 28 possiblities, but you can do it a lot quicker.

How can you test the batteries so that you are guarenteed to get a working pair in 7 tries or less?

Problem 2

The rectangle ABCD is divided into squares. The length of side AB is 16. What is the length of side AD?
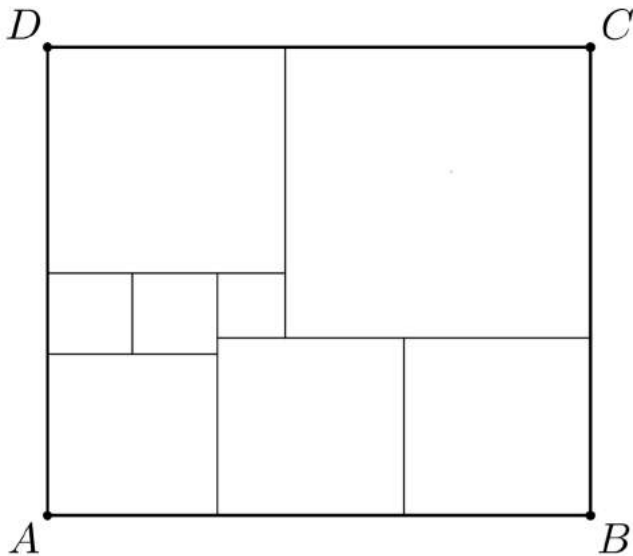
Solutions for last issue

Problem 1

Important is that the pirates all know each other to be top-notch logicians. So when each one votes, they will not just be thinking about the current proposal, but about all possible outcomes down the line. And because the rank order is known in advance, each can accurately predict how the others would vote in any situation and adjust their own votes accordingly.

Because Pirate E is last, he has the most outcomes to consider, so start by following his thought process. He would reason this out by working backwards from the last possible scenario with only him and Pirate D remaining. Pirate D would obviously propose to keep all the gold and Pirate E's one vote would not be enough to override him, so Pirate E wants to avoid this situation at all costs.

Now we move to the previous decision point with three pirates left and Pirate C making the proposal. Everyone knowns that if Pirate C is outvoted, the decision moves to Pirate D, who will then get all the gold, while Pirate E gets nothing. So to secure Pirate E's vote Pirate C only needs to offer Pirate E slightly more than nothing, one coin. Since this ensures Pirates E's support, Pirate C does not need to offer Pirate D anything at all.

What if there are four pirates? As captain, Pirate B would still only need one other vote for his plan to pass. He knows that Pirate D does not want the decision to pass to Pirate C, so Pirate B would offer Pirate D one coin for his support with nothing for Pirate C or E.

Now we are back at the initial vote with all five pirates standing. Having considered all the other scenarios, Pirate A knows that if he goes overboard, the decision comes down to Pirate B, which would be bad news for Pirate C and E. So Pirate A offers Pirate C and E one coin each, keeping 98 coins for himself. Pirate B and D vote no, but Pirate C and E grudgingly vote yes, knowing that the alternative would be worse for them.

Problem 2
$A = 1, B = 4, C = 5.$

Miscellaneous

Computer Science puzzle

Louise Leibbrandt

Cryptogram

The following message about Ada Lovelace as a child is in code. Crack the cypher and decode the message. Each letter of the alphabet is given a distinct number. Not all letters appear in the message.

Message

| 6 | 25 | 24 |

| 20 | 8 | 9 | 5 | 21 |

| 7 | 2 | 7 |

| 2 | 23 | 24 | 7 | 3 | 6 |

| 8 | 19 |

| 10 | 24 | 12 | 5 | 21 |

| 7 | 10 | 16 | 24 |

| 6 | 8 |

| 19 | 16 | 20 |

| 7 | 5 | 2 |

| 7 | 22 | 22 | 23 | 8 | 7 | 17 | 25 | 24 | 2 |

| 6 | 25 | 24 |

| 22 | 23 | 8 | 10 | 16 | 24 | 3 |

| 8 | 19 |

| 25 | 24 | 23 |

| 24 | 7 | 23 | 6 | 25 |

| 10 | 8 | 9 | 5 | 2 |

| 13 | 6 | 7 | 6 | 24 |

| 18 | 12 | 6 | 25 |

| 6 | 20 | 22 | 12 | 17 | 7 | 16 |

| 21 | 9 | 13 | 6 | 8 |

| 7 | 5 | 2 |

| 7 |

| 13 | 17 | 12 | 24 | 5 | 6 | 12 | 19 | 12 | 17 |

| 24 | 20 | 24 |

Miscellaneous

Fill in the following key to solve the puzzle

1	2	3	4	5	6	7	8	9	10	11	12	13
14	15	16	17	18	19	20	21	22	23	24	25	26

Solution to last issue's puzzle

The best way to solve this kind of problem is to turn the offending field from a blank final into an ordinary final, replacing the static initializer block with a static field initializer. This is best done by refactoring the code in the static block into a helper method:

```
public class UnwelcomeGuest {
    public static final long GUEST_USER_ID = -1;
    private static final long USER_ID = getUserIdOrGuest();
    private static long getUserIdOrGuest() {
        try {
            return getUserIdFromEnvironment();
        } catch (IdUnavailableException e) {
            System.out.println("Logging in as guest");
            return GUEST_USER_ID;
        }
    }
    ... // The rest of the program is unchanged
}
```

This version of the program is clearly correct and is more readable than the original because it adds a descriptive name for the field value computation, where the original version had only an anonymous static initializer block. With this change to the program, it works as expected.

In summary, most programmers do not need to learn the details of the definite assignment rules. Usually the rules just do the right thing. If you must refactor a program to eliminate a compilation error caused by the definite assignment rules, consider adding a new method. Besides solving the definite assignment problem, it may offer an opportunity to make the program more readable.

Miscellaneous

Science Trends

Willemijn Tutuarima

On this page you will find some brief information on recent scientific breakthroughs or interesting news. Whether they're big or small, if we think they might interest you, we will mention them here! Do you miss a certain trend or want to inform your fellow readers of an interesting innovation? Feel free to contact us.

A voice in restriction

Many of us don't realize that freedom of speech is not always a given. In some countries you need to stay anonymous during communication to avoid prosecution while also needing a trustworthy identity while communicating with others. A group of researchers at UC Santa Barbara have designed an application to make communication for people in such countries safer. With this app the users stay completely anonymous and they are sure that the messages they get can be trusted. The app is called SecurePost and allows users to create secure groups on social media such as Twitter and Facebook, which enables them to build up trust with their readers. Even if the application would be hacked or infiltrated, all the users will be protected and anonymous. The way the team made the application safe to share is by QR codes which can be shared in person or over a trusted connection. This ensures security even if a third party would witness the exchange. SecurePost also attaches a cryptographic signature to the post which verifies the authenticity of all messages. This way, messages by impostors can be flagged and removed. This application is an example of how technology can help others and how it will be a beginning of many more innovations. [1]

Pacemaker for the brain

At the University of California, Berkeley, engineers have developed a new neurostimulator that can listen to and stimulate electric current in the brain and at the same time, potentially deliver fine-tuned treatments to patients with diseases like epilepsy and Parkinson's. The device is named WAND, which stands for Wireless Artifact-free Neuromodulation Device, and is both wireless and autonomous, meaning that once it learns to recognize the signs of tremor or seizure, it can adjust the stimulation parameters on its own to prevent the unwanted movements. The WAND works like a pacemaker for the brain, monitoring the brain's electrical activity and delivering electrical stimulation if it detects something wrong. The device is meant to lower both the cost and duration of finding the right therapy for a patient and is meant to be accessible and have improved outcomes from current methods used to diagnose patients. Although the progress made with this device is remarkable, the device still needs a lot of work before it can give optimal treatment. However, when it does, the device can be extremely effective at preventing debilitating tremors or seizures in patients with a variety of neurological conditions. [2]

Flying cars for sale.

The company Pal-V from the town of Raamsdonksveer has published an announcement that they will be selling the first flying cars in the Netherlands by the end of the year. The first model is called the liberty Pioneer and will cost €500.000 of which there will be 90 samples. The second model, called the Liberty sport will be €300.000 and will arrive shortly after the first model. The car will have both a steering wheel and all the handles to be able to fly with it. The capacity is 2 persons and the maximum endurance will be around 4 hours. You might think a city would get really crowded with cars flying and landing everywhere, but this is not how the new flying car will work. The car is supposed to be used as a regular car in the cities, so for short distance, and used as a plane for longer distance, for example in between towns. The only big problem for now is space to land because in the Netherlands the amount of small airports where the cars would be able to land is very small. This is also why not everyone will have one of these cars in the next 5 years, but maybe in the further future this will be one of the main ways of transportation in the Netherlands. [3]

References

[1] https://www.sciencedaily.com/releases/2019/01/190115121106.htm

[2] https://www.sciencedaily.com/releases/2019/01/190101094517.htm

[3] https://www.omroepbrabant.nl/nieuws/2811519/Eerste-vliegende-auto-rolt-eind-dit-jaar-uit-fabriek-Pal-V-Liberty-Pioneer-kost-half-miljoen-euro

Miscellaneous

We push
technology further

to print microchip features
that are finer

to make the
energy use of
a battery more
efficient

to make electric
cars the standard

Do you dream of changing the world of innovation? Do complex technological challenges
appeal to your imagination? We are looking for you. ASML always wants to get in touch
with eager and curious students.

Join us at workingatasml.com/students

ASML

Be part of progress

De Delftse Bedrijvendagen

'De Delftse Bedrijvendagen' (DDB) will have both their solicitation workshops as well as the presentation days this month. 150 companies will present themselves here at the largest technology oriented career event in the Benelux. For more information, go to ddb.tudelft.nl

Dies Natalis week

During this week full of activities, we celebrate the birthday of the study association.
Activities like a diner, special lunch lecture and a lot more!

Mathematical Career Orientation Day

During the Mathematical Career Orientation Day, you will get the opportunity to have one-on-one conversations with Mathematics alumni from the participating companies. You will get the opportunity to ask all questions that you want to know!

Februari

3.1 - 3.2	Department Symposium
13	MeisCie activity; Wine tasting
12-14	DDB application trainings
18-20	DDB Presentation Days
20	SjaarCie Party
25	MaPhyA pre-Activity
26	T.U.E.S.Day Lecture: Sioux
27	MatCH activity
28	Career College 3.1 - Graduation Panel

March

1-3	Area FiftyLAN - LAN Party
4	General Assembly
5	T.U.E.S.Day Lecture: Mathematics
6	ICom interest lunch
7	International Food Festival
18-22	Dies Natalis week
18-29	DDB In-House Days
26	T.U.E.S.Day Lecture: ASR
28	Career College 3.2 - Personal Development

April

2	T.U.E.S.day Lecture: Computer Science
2	MaPhyA activity
3	Mathematical Career Orientation Day
6	Parents' day
13-24	Interview Days
23	T.U.E.S.Day lecture: ORTEC
25	Career College 4.1: Personal Development
30	T.U.E.S.Day Lecture: AIVD