File 20101203.0708: Weekly activity report 0165:

weekly activity report 165 (loughry)
Joe Loughry
Sent: 03 December 2010 07:08
To: Niki Trigoni; Andrew Martin; Joanna Ashbourn
Cc: otaschner@aol.com; anniecruz13@gmail.com; andrea@hpwtdogmom.org;
chip.w.auten@lmco.com; edloughry@aol.com; diane@dldrncs.com;
Joe Loughry; mmcauliffesl@comcast.net; tom.a.marso@lmco.com

Weekly activity report no. 20101202.2028 (GMT-7) sequence no. 0165, week 8 MT

I have begun working again at the Simulink level in MATLAB after giving up on Simscape as a lost cause. The Simscape product is a new and expensive tool; the vendor will not licence it to work with student versions of MATLAB and Simulink, which are what OUCS site-licences through the university. After spending time on the phone with technical support at both mathworks.com and mathworks.co.uk, what transpires is that Simscape only works with the full commercial version of MATLAB and it would cost 900 to get it running, not the advertised 150 for an academic licence. That would have used up my entire 2011 travel budget; I cannot afford the expense right now. The trade-off is additional time required to implement a simulation the hard way (as a set of control laws in Simulink) and not having pretty animated diagrams to show off, vs probably ending up with a deeper understanding of the underlying mechanism if I do it the hard way. I am willing to accept the trade-off and am moving ahead with a more complicated implementation at a lower level of abstraction. I am building it up from a 1-D dynamics problem of a simple harmonic oscillator that I plan to generalise to n dimensions by basis vector analysis. The cheaper method is fully generalisable, an advantage over the Simscape product which would have been unable to go beyond 3-D. The method of working in Simulink takes some getting used to; it emulates continuous functions, a significant departure from the discrete time simulations I wrote before (my favourite being $F=G\frac{m_1\cdot m_2}{r^2}$ with more than two bodies). In those simulations, the time interval had to fluctuate continually in order to avoid losing precision in the acceleration calculation, else the simulation would inevitably run away after the first few close approaches. I solved that problem efficiently by varying the precision of the force calculation according to the second derivative of position. In a real-time animation, the effect of the varying precision was unnoticeable except for the fact that the total energy of the system no longer increased without bound. Using the present tool, I no longer have control over that parameter, but further the whole way of looking at the problem is reversed. Instead of taking derivatives of position to get velocity and acceleration, it is recommended to integrate forces over time to get velocity and position, an approach that works well with my model, but requires an adjustment in thinking. The manual recommends using a single second-order integrator because it is more efficient than two first-order integrators, but I want the visibility in between so that I can plot the intermediate values and selectively apply friction and damping feedback to the system. (In my model, some elements are frictionless, massless and infinitesimally small, not realistic assumptions in a mechanical system. But I have to keep in mind that the model represents accreditor behaviour and risk mitigations, not actual physical forces, mass and acceleration. I am trying to predict the actions of people, not linkages.) Once I have the thing yielding reasonable results for a textbook oscillator, I will abstract out the functional blocks and duplicate them for a set of basis vectors. After I have that producing reasonable-looking phase space plots, I will apply interpretations to map positions and motions to accreditation events, determine the right scale values to bring it into agreement with observation, and finally print out some nice plots to show the assessors and to begin to talk about interpretation and predictive value. I claim that the trajectory of a risk in phase space is an attractor to an optimum path from risk to mitigation that reflects the intention of an accreditor in a multi-lateral ST&E. With one accreditor who never changes his mind, the trajectory degenerates to a straight line. With two or---maybe it has similarities to the three-body problem!---more accreditors, or equivalently (as I currently think) involving accreditors who change their minds in mid-ST&E, the time evolution of the system is much more complicated, possibly chaotic. It still has a stable attractor, though, because my model is tied to a physical system and thermodynamics rules. The attractor, if you wait long enough, is always a unique set of fixed points for a given initial configuration. I will have plots showing this for the assessors in a couple of weeks. Thinking about using a heat map to show the dwell time. Not sure if it means anything, but a plot might be suggestive.

My confirmation viva is now scheduled for 10am on Thursday, 16th December. Unless it snows, I should arrive in time to get at least a little sleep before the viva. I am meeting with Dr Ashbourn on Friday and flying out on Monday morning. Dr Martin is on travel this month and our itineraries do not overlap, but I asked for a meeting early next week via Skype when he is in Australia.

The Security Reading Group met this week to discuss the article by Christian Collberg and Stephen Kobourov, 'Self-Plagiarism in Computer Science' (Comm. ACM 48(4), pp. 88--94, April 2005). Present on the Skype call were Wattana, Shamal, John, and Joe. I brought this article to the attention of the reading group not because I thought it was a good article but because I thought it was especially poor and I disagreed strongly with some of the authors' conclusions. It has a flawed methodology, bad statistics, it is not well written and should really have been presented as a letter to the editor instead of an article. (We can see the probable reason for it to have been promoted to an article later.) Nevertheless, flawed as it is, the paper raises some important points and I thought it could serve as a jumping-off point for a discussion that would be relevant for the cohort. It did. The paper is a polemic, but I like polemics. We looked at it from the point of view of quality control; our job as DPhil students is to produce high-quality research, and part of that responsibility is to do so in the environment of computer science as it exists today. The field has some idiosyncratic conventions that differ from, for example, high-energy physics, literature or molecular biology. Computer science suffers from a lack of quick-turnaround journals like the ones that litter chemistry and physics; even the highest profile journals like Nature can publish a paper in two weeks if they have to---something that came around to bite them in the heyday of Jan Hendrik Schn---but computer science has no journals of that ilk. John pointed out the counterexample that there are a couple of computer security journals that are able to publish new results very quickly, but they are definitely the exception. Consequently, computer science depends primarily for distribution of new results on conferences, especially the big international conferences, and even those have long lead times because of the trouble of long distance travel. Interestingly, computer scientists make almost no use of the arXiv, and no one can explain why. Even the traditional progression from technical report to conference paper to archival journal article is short-circuited in computer science, at least in our part of the field today, because all the important conferences are treated almost like archival journals---which is the function that they seem to fulfil---especially in security, where the half-life of ideas tends to be short. I am not as familiar with the journal behaviour of, for example, programming language research, where the situation might be reversed and closer to the traditional model.

The authors of this article appear to be characterising as a liability some of the quirks of computer science publishing that I think are of academic interest. The reason I give is that the field requires a different class of productivity, even if the results are not exactly aligned across all sciences. We got into a good discussion of this topic beginning from the idea of ‘salami slicing’, also known as Least Publishable Unit, presented in the article as if it were a novel idea and not the same problem I have seen described a dozen times or more in books on scientific writing, none of which appear in this article’s reference list. That list is interesting in itself: a completely inadequate survey of the field of scientific writing---of the books I remember, nearly all of them pre-date this paper by a decade or more. Shamal related his own experience with a paper that was first rejected by one conference, then extended to address the referees’ concerns, but it acquired more sections along the way and was ultimately divided into three papers because it contained several different contributions. It mirrors my own experience with a paper that was rejected by two conferences, extended to include a newly developed solution to the problem it gave originally, and then was broken up into two papers so as not to obscure the different contributions. Another writing sin the authors decry is reusing the perfect introduction, something that several of us agreed is not only desirable but necessary in cases where you are presenting an idea for the first time to an audience that has never heard of your topic before. The introduction of the paper I am writing currently gets closer to perfect every time I rewrite it, more concise and more able to stand on its own. I consider it a process of tuning the presentation and not, as the authors would have it, ‘blatant reuse’ (p. 91). John told of running into the same thing with the topic of trusted computing when presenting before an audience unfamiliar with the idea. In my case, there are no natural venues for research on cross domain certification and accreditation, so I am constantly beginning talks and papers with an overview of the problem and the same or similar motivating examples before I can even begin to describe a contribution.

Other problems with this article are apparent in section 2 where the authors use inappropriate humour in two places to shore up their examples: one of the examples is OK and the other is terrible. The authors’ use of sarcasm and scare quotes is out of place in a technical journal article. The authors’ comparison of IEEE and ACM reuse policies is useful, although out of date now, after IEEE changed their policy in response to serious scientific misconduct episodes that took place within the past five years. The definitions on page 91 were the first useful bit in the whole article, I thought, building on definitions first published in 2000. I prefer it when people publish useful definitions or new frameworks where there existed none before because there is always the chance that future authors will pick up those definitions and begin to use them consistently. The term ‘advocacy reuse’ in particular I think is a useful new definition, one that I hope gains wider currency in future. Related to the concept of advocacy reuse, John mentioned something interesting about the writing of Bruce Schneier and Ross Anderson; how they write a lot of articles on a narrow range of topics (the economics of information security in the case of Prof. Anderson; as Shamal said, he can write anything at all about economics and it automatically gets published), repeating themselves quite a bit across different audiences if you read a lot of what they write. This is related to the distinction posed in the article between horizontal and vertical reuse and academic credit.

On page 92 we discover the real reason this article got written, which was to advertise the authors' tool, SPlaT. Wattana looked up their original technical report on the tool, although the Skype connection went down before we could get into a discussion of what he found. The sentence in the section that follows, about statistical significance, to my eye appears to be in response to a referee's complaint: given the size of their population and their sample size reported it is just about possible to figure the confidence interval---the text is missing one necessary piece of information so I can't calculate it exactly---but the significance is below 0.25 given any set of reasonable assumptions.

In the middle of the discussion about statistical significance, the network connection failed and Skype lost video, and then audio. We were able to get a few text messages through before the connection dropped permanently. It was a good session, unfortunately cut short by technical problems. Some further discussion took place via email afterwards.

At Lockheed, the project manager for my other research project met with the sponsor in Rome, New York last week; the sponsor is happy with our progress at the end of Phase II and gave us some direction for development in Phase III. Funding runs out nine months from now, as planned. We need a better storyboard and demo to show off; our progress reports to date have been filled with technical detail and research results, but what came out of this UCDMO get-together was that other research groups came prepared with slick presentations and slides to show off. Our system is about to get a GUI that will make for a better demo soon; in this phase we have more funding for development and can afford to hire another person.

My current task list (in priority order, most urgent first; work on tasks in this order):

1. Working on getting the low-level simulation working in Simulink now for a demo to the assessors in two weeks.

2. Prepare an overview talk for viva: history, motivating examples, thesis, preliminary results, rejected alternatives, detailed plan for finishing, and contingency planning.

3. Crosstalk article is now going to wait until after I present to the assessors. In the outline, I have that R-prime was evaluated under CC v3.0, but I recalled recently that there was an earlier version of the system (call it R_0) for the E project that was supposed to be 'evaluatable' under CCv2.3. R-double-prime was certified under DIACAP as the first test case to replace DCID 6/3, but it looks now like DoD and IC will be put together under the tent by UCDMO soon, as soon as they obtain full control of DSAWG. That is expected to occur in the first week of January. It affects the whole structure of the Crosstalk article, so best work on the implementation of the model until an announcement is made.

4. Thinking about what the definition of 'succeed' and 'fail' are in the context of CC evaluation; 'did not complete validation', 'abandoned before the end of validation', 'failed to receive certification', 'abandoned before the end of evaluation' and 'not submitted for evaluation' are all different and significant events.

5. The lower-level control-law model in Simulink will be able to cut-and-paste extend to 4 systems in parallel with the same set of fixed points easily, I think. To do: implement Prof. Polak's equilibrium acid test from Yale and the double alarm clock option model (not as easy to do without the timed elements available in Simscape, but should be possible with discrete Simulink elements;

have to model it as a discontinuity).

6. Background reading: Pennock and Wellman (2004) on uncertainty markets, Levitt and Dubner (2009) on asymmetric information, Bernstein (1996) on risk assessment (on hold), Karp (2009) on research methods, and Achdou & Pironneua on option pricing.

7. Ping the following people: Paul Ozura [BAH], Dennis Bowden [San Diego], [Patti Spicer, Charles Nightingale, Hal Forsberg] at CSC. Waiting to hear back from Dr Kladko on the CC lab visit; I let him know when I would be on travel.

8. Small tasks (get these done before viva): update first case study chart with changes from last conference; draw fault-tree diagrams for R-prime, R-double-prime and S-star; draw up organisation charts for R, R-prime, S-star, R-double-prime, N, L and G; update documentation of the current set of anonymisation codes.

Joe Loughry
Doctoral student in the Computing Laboratory,
St Cross College, Oxford

End of WAR 0165.

References