DAGSTUHL
REPORTS

Volume 1, Issue 7, July 2011

ISSN 2192-5283

Published online and open access by
Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany.
Online available at http://www.dagstuhl.de/dagrep

Publication date
November, 2011

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at `http://dnb.d-nb.de`.

Digital Object Identifier: 10.4230/DagRep.1.7.i

Aims and Scope
The periodical *Dagstuhl Reports* documents the program and the results of Dagstuhl Seminars and Dagstuhl Perspectives Workshops.
In principal, for each Dagstuhl Seminar or Dagstuhl Perspectives Workshop a report is published that contains the following:

- an executive summary of the seminar program and the fundamental results,
- an overview of the talks given during the seminar (summarized as talk abstracts), and
- summaries from working groups (if applicable).

This basic framework can be extended by suitable contributions that are related to the program of the seminar, e.g. summaries from panel discussions or open problem sessions.

Contact
Schloss Dagstuhl – Leibniz-Zentrum für Informatik
Dagstuhl Reports, Editorial Office
Oktavie-Allee, 66687 Wadern, Germany
reports@dagstuhl.de

www.dagstuhl.de/dagrep

Report from Dagstuhl Seminar 11271

Computer Science in Sport - Special emphasis: Football

Edited by

Martin Lames[1], Tim McGarry[2], Bernhard Nebel[3], and Karen Roemer[4]

1 **TU München, DE,** martin.lames@sp.tum.de
2 **University of New Brunswick, CA,** tmcgarry@unb.ca
3 **Universität Freiburg, DE,** nebel@informatik.uni-freiburg.de
4 **Michigan Technological University, US,** kroemer@mtu.edu

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 11271 "Computer Science in Sport - Special emphasis: Football". There were five sessions over the course of three days focusing on separate specific aspects on the relevance, applications and current issues pertaining to computer science in sport. The first session on the first day was about RoboCup – the history, types of games and robots used, and the current topics relevant to machine learning, tracking and planning. The second session on the first day was a miscellaneous session, which looked at broad topics ranging from hardware devices for mobile coaching, uses of positional data in football, rehabilitation methodologies and games for learning. The second day started with a session on modelling sports as dynamical systems combined with the use of neural networks in performance analysis as well as theoretical issues in human movement science. In the afternoon of the second day the session was on topics in computer science specifically relevant to coaches, in which six different people presented. The final day of the conference hosted a session on computer science "behind the scenes" of major sports broadcasters and other media. The sessions were attended by academics, graduate students, coaches, performance analysts and athletes.

Seminar 03.–06. July, 2011 – www.dagstuhl.de/11271
1998 ACM Subject Classification B.4.0 [Input/Output and Data Communications] General, D.0 [Software] General, H.2.8 Database applications, I.2.9 Robotics, I.2.0 [Artificial Intelligence] General, J.0 [Computer Applications] General
Keywords and phrases Sport, Neural networks, Dynamical systems, Robotics, Coaching
Digital Object Identifier 10.4230/DagRep.1.7.1
Edited in cooperation with Peter Lamb

1 Executive Summary

Martin Lames

The Dagstuhl Seminar 11271 "Computer Science in Sport – Special emphasis: Football" stands in a row of 3 seminars introducing the field of computer science in sports. The general aim is to bring experts from computer science together with experts from sports science to explore the options of interdisciplinary work in this exciting field.

An additional aspect was in the focus of this seminar in July, 2011. We invited not only scientists from the field of football research but also practitioners like Max Reckers (NL) who was responsible for computer science at FC Bayern München under coach Van Gaal.

This measure led to livelier discussions because the aspects “Does this work in practice?” or “Does practice really need that?” were not only discussed but also given answers from the view of practice.

Another focus was on the pros and cons of technological aids in football. Here, the discussion brought about many issues, being far apart from a totally affirmative standpoint. The reason for the outstanding position of football in European societies is basically founded in its value for entertainment. Each game broadcasted live can be seen as a drama, a ritualized conflict that will produce a result on that very evening that cannot be foreseen in any way. It is this kind of authenticity that gives football its importance. Concerning technical aids we have to be careful that they do not endanger the dramatic properties of the game. So, as in other fields also, it is not wise to do everything we can do.

Finally, the seminar proved again the benefits of the Dagstuhl seminar concept. Experts from different fields that would hardly meet in their normal business had the opportunity to exchange their ideas in many informal meetings. There was positive resonance from most of the participants stressing especially this fact. Several ideas for new projects among the participants were produced and meanwhile initiated. An application for a next seminar on computer science in sports again with an exciting focus will be prepared soon. A “Dagstuhl Manifesto” is going to be published explaining the interdisciplinary perspectives between sports science and computer science in depth.

2 Table of Contents

3 Overview of Talks

3.1 A Survey of the Mobile Coaching System

Arnold Baca (Universität Wien, AT)

Main reference Baca, A.; Kornfeind, P.; Preuschl, E.; Bichler, S.; Tampier, M.; Novatchkov, H., "A Server-Based Mobile Coaching System," Sensors 2010, 10, 10640-10662.
URL http://www.mdpi.com/1424-8220/10/12/10640/pdf

A wireless system for monitoring, transmitting and processing performance data in sports for the purpose of providing feedback has been developed. Experts are provided with remote data access, analysis and (partly automated) feedback routines. In this way, they are able to provide athletes with individual feedback from remote locations. One specific sport, the system could be utilized for, is football.

3.2 Robot Soccer: A Challenge for AI and Robotics

Sven Behnke (Universität Bonn, DE)

Robot competitions are a popular way to benchmark robotic systems. They allow for a direct comparison of different approaches to mechatronics, perception, and behavior control outside the own lab at a predefined time. Since 1997, the RoboCup Federation holds annual international competitions for soccer robots in different leagues that investigate different aspects of soccer. While in the simulation league team play and tactics are key, bipedal locomotion, perception of the game situation from a moving camera, and control of complex motions are investigated in the humanoid league.

In my talk, I introduce the humanoid soccer robots of our team NimbRo, which won the tournament multiple times and are currently holder of the Best Humanoid Award. I cover robot construction, visual perception, hierarchical reactive behavior control, and learning.

3.3 Towards Automated Football Analysis: Algorithms and Data Structures

Joachim Gudmundsson (The University of Sydney, AU)

Joint work of Gudmundsson, Joachim; Wolle, Thomas

Analysing a football match is without doubt an important task for coaches, clubs and players; and with current technologies more and more match data is collected. For instance, many companies offer the ability to track the position of each player and the ball with high accuracy and high resolution.

Analysing this position data can be very useful. Nowadays, some companies offer products that include simple analyses, such as statistics and basic queries. It is, however, a non-trivial task to perform a more advanced analysis. In our research, we assume that we are given

only the position data of all players and the ball with high accuracy and high resolution. We present several tools, for example:

1. Automatically extract (from the position data) a list of certain events that happened during the football match. These events include kick-offs, corner kicks, passes etc. In experiments we could observe that our method is very fast and reaches a high level of correctness. We also learned that errors in the event detection are hard to avoid completely, when looking at only the position data.
2. A tool that aims at analysing a single player's trajectory (the sequence of all positions during a game). More precisely, we look for movements of a player that are repeated often (so called subtrajectory clusters). For example a left wing attacker runs from the centre-line along the left side of the field towards the opponent's goal. And this attacker might repeat this type of movement very often during a game (or perhaps multiple games). Our goal is to detect this kind of frequent movements automatically. Experiments showed that this method is computationally expensive. Nevertheless, it reliably identifies subtrajectory clusters, which then could be used for further analysis.
3. A third example is a tool that evaluates a players passing ability.

This also involves the ability to decide which pass to make i.e., the players overview of the game, ability to receive a pass and to execute a pass. This is joint work with Thomas Wolle.

3.4 Introduction and Discussion of SOMs in Human Movement Science

Peter Lamb (TU München, DE)

Joint work of Lamb, P.F., Bartlett, R.M., & Robins, A.
Main reference P.F. Lamb, R.M. Bartlett, and A. Robins, "Artificial neural networks for analyzing inter-limb coordination: the golf chip shot," Human Movement Science, 2011, *(in press)*.
URL http://dx.doi.org/10.1016/j.humov.2010.12.006

Kohonen Self-Organizing Maps (SOMs)[1] are a specific type of artificial neural network which, because of the theorized non-linear, self-organizing nature of human movement, appear to represent an attractive method of analysis for such movements[2]. The output of a SOM is commonly visualized as a grid of nodes, each with an associated weight vector.

The dimensionality of the weight vectors is the same as the dimensionality of the input data set. The examples presented in the seminar represent time-series coordination of kinematic joint angles and velocities. An input represents a single time frame, or sample, of a movement pattern and is fed forward to the input layer as an input vector. The dimensionality of the input vectors (and weight vectors) is equal to the number of dependent variables. The number of SOM nodes is typically fewer than the number of inputs, thereby reducing the data and forcing them into clusters of similar data. The steps for training a SOM are summarized as:

1. *Initialization* - Map dimensions, training parameters and initial values for the weight vectors are chosen based on the principal components of the input data set.
2. *Find best-matching node* - For each input vector, the node whose weight vector has the shortest Euclidean distance to the respective input is identified and declared the 'best-matching node'.

3. *Adjust weight vectors* - The weight vectors are adjusted during an iterative training process to model the input distribution. The weight vector of the best-matching node is adjusted the most, while nodes close to the best-matching node (in Euclidean space) are adjusted less, as their proximity decreases. The neighbourhood relation determines the magnitude of these adjustments and is the feature which preserves the topology of the input data set and therefore allows the nodes to self-organize.

Finally, a method for visualizing the nodes is decided upon based on the goals of the analysis. In this case, a 2-D grid on which the nodes form a hexagonal lattice was presented. The U-matrix was demonstrated as a method for visualizing Euclidean distance between neighbouring nodes using a color scale. To enhance the visualization the Euclidean distance can also be plotted on the z-axis so that clusters in the data can be seen more clearly.

On the U-matrix the sequence of best matching nodes which may represent a complete movement pattern can be highlighted with a trajectory. This technique allows high-dimensional changes in coordination between trials and/or testing conditions to be compared.

The concept of training a second SOM using information from the first SOM was also expanded upon. The weight vectors of the consecutive best matching nodes were projected into weight space and the coordinates of the best matching nodes were used as input for the second SOM[3]. Frequently activated regions can be thought of as stable, therefore the visualization represents coordination stability. In technique analysis, the quality of the technique is often judged according to performance outcome[4]. The methods presented here may offer coaches a more objective method for the assessment of sports techniques, one which is based on the movement itself rather than the outcome.

References

1 T. Kohonen. *Self-organizing maps (3rd ed.)*. Springer-Verlag, Berlin, 2001.
2 J.A.S. Kelso. *Dynamic patterns: the self-organization of brain and behavior*. MIT Press, Cambridge, 1995.
3 P.F. Lamb, R.M. Bartlett, and A. Robins, *Artificial neural networks for analyzing inter-limb coordination: the golf chip shot*, Human Movement Science *(in press)* 2011.
4 A. Lees. *Technique analysis in sports: a critical review*, Journal of Sports Sciences **20** 2002, 813–828.

3.5 Tactical Match Analysis In Soccer: New Perspectives?

Koen A.P.M. Lemmink (University of Groningen, NL)

Joint work of Lemmink, Koen A.P.M.; Frencken, Wouter G.P.
Main reference W.G.P. Frencken, W.G.P., K. Lemminkab, N. Dellemanc, and C. Visschera, "Oscillations of centroid position and surface area of soccer teams in small-sided games," European Journal of Sports Sciences, 11(4), 215-223, 2011.
URL http://dx.doi.org/10.1080/17461391.2010.499967

Match analysis is the objective recording and examination of behavioural events of one or more players during competition or training. Notational analysis is a method to create a permanent record of the on-the-ball actions of players within a match through hand-based or computerized systems often using video technology. For the analysis of tactical behaviour, large data sets create opportunities for analysing temporal patterns (T-patterns) and network structures. Although these notational systems have improved over time, they still have

certain limitations, especially from a tactical point of view. For example, information of position of the actions lack accuracy and, due to a single camera viewpoint, only on- the-ball actions of individual players are monitored properly.

In recent years, technological innovations, such as automated tracking based on video clips and GPS-like technology, have led to new possibilities for match analysis in ball team sports. High-frequency positional player data (up to 1000 Hz) is becoming available in the context of different ball team sports, such as soccer, field hockey, basketball, rugby, and handball.

Until now, these data are typically used to calculate distance, speed and acceleration/deceleration profiles of individual players. These types of analysis do not capture the complexity of a soccer match and new approaches of the game are required.

Data with high spatial and temporal resolution of different players at the same time open up to player vs. player and team vs. team interactions. For example, on individual level it allows for the analysis of symmetry breaking processes in player dyads, whereas on team level attacking and defensive spaces or other geometrical configurations confined by the players can be investigated. It is obvious that the current theoretical frameworks for performance analysis are not suitable for the study of these spatial- temporal game dynamics.

In contrast, dynamical systems theory is a relevant framework and its analytical tools and methods are ideal because they can cope with this type of data. This approach leads to new insights into the interactions of players and teams within different ball team sports. New ideas and research findings on several geometrical configurations in small-sided games and real matches in elite soccer will be presented to expand the existing knowledge in this area.

3.6 Position Tracking as Current Challenge in Game Sports Analysis

Roland Leser (Universität Wien, AT)

About 10 to 15 years ago only top level teams used computer assisted video annotation systems to analyze sport games and training sessions. The progress in hardware and software development made it happen that nowadays this technique is used even at amateur level. Pointing to another analysis technique we have at present similar conditions than in the situation described above. Very expensive video based position tracking systems are used by few of the top teams worldwide to analyze their game play and GPS-systems are applied to analyze training sessions of outdoor sports. Radio wave based tracking systems are currently not wide spread for performance analysis but they could dominate the future. By tendency radio wave sensors become smaller and cheaper in the next years and radio wave based tracking systems are much less service intensive than other systems. Looking forward, this kind of tracking system could be a worthwhile alternative to analyze games and training sessions of game sports for many teams. This presentation gives an overlook on the preparatory work of installing an industrial radio wave based tracking system (www.ubisense.net) for game sports analyses, outlines current results and looks ahead to future works.

3.7 The Game Data Project in the Fußball Bundesliga

Daniel Link (TU München, DE)

The German Soccer League (called in German Fussball Bundesliga) is a respectable social and economic factor in Germany. The income of Fussball Bundesliga in the season 2010/11 includes more than 1 billion €from advertising and TV rights, but at the moment no commercializing of game related data takes place. To improve this situation the Game Data Project was started in order to develop a Game Data Library for storing and delivery of basic match data, tracking data (at 25 Hz) and event data. This data is used to create statistics for Fussball Bundesliga clubs, online media, TV and betting companies.

The data collection includes three basic processes. In the live process two live observers in real time within a stadium telephone are connected to two live typists, which enter the data into the database. In a near real time process two video observers who verify data are involved in a control center away from the stadium. The tracking is done by a two camera system at the stadium, where an observer is able to make manual correction to data.

The observation of events bases on a Game Data Model, which does required operational clarity. This ontology bases on object orientation and provides a data structure for the efficient processing and storing of data and the smart calculation of statistics. The challenges for the scientific discipline sport informatics in the context of the Game Data Library are to use the enormous amounts of data that will be generated in future and to develop methods and tools and to analyze it.

3.8 Performance at the FIFA Women's World Cup 2011

Keith Lyons (University of Canberra, AU)

This paper presents data from the games ($n = 16$) in the first two rounds of the 2011 FIFA Women's World Cup. Attention is drawn to patterns of goal scoring and the relationship with FIFA ranking (18 March 2011). The paper includes a profile of winning, losing and drawing in the 16 games (presented as averages). The paper is used as a stimulus paper for discussion of technical and tactical aspects of game play at this World Cup and in football generally. The presentation makes use of Prezi to share these data.

`http://prezi.com/21c82yn9orcj/winning-performance-at-the-2011-fifa-womens-world-cup/`

3.9 Human Information Processing: The Penalty Kick and Direct Free-kick in Football

Tim McGarry (University of New Brunswick, CA)

This preliminary investigation considers information processing constraints placed on the goalkeeper in football when defending a penalty kick or direct free-kick. Statistics from the 1976–2008 European Championships and 1978–2010 World Cups affirm the importance of the penalty kick, including penalty shoot-outs in knock-out competition, for determining winning outcomes. Of note, the fourth-placed penalty taker in penalty shoot-outs was reported to be much less successful, for whatever reason, than other penalty takers in the line sequence. The data yielded 0.81, 0.77, 0.79, 0.54 and 0.75 scoring probabilities for the first through fifth placed penalty takers, respectively.

These findings on penalty kicks confirm anecdotal knowledge regarding goalkeeper disadvantage, attributed primarily to unyielding time constraint for decision-making and movement execution. For a direct free-kick, the time constraint on information processing imposed on the goalkeeper is lessened because of increased time afforded by longer ball flight. The use of a defending wall of players also assists the goalkeeper. First, the wall presents an obstacle to goal for the attacking player taking the free-kick, thus reducing the chances of goal threat from the direct shot, and, second, it reduces the "open" goal area that the goalkeeper will assign priority to protecting. The suggestion offered here is that the defending wall disadvantages the goalkeeper on those times that the ball defeats (passes) the wall on way to the goal area that the wall is designed to protect. In these instances, the goalkeeper is presented with late visual information that provides insufficient time for generating an appropriate response. Statistics from the 2004 European Championship and 2002–2006 World Cups reported general scoring probabilities of 0.08 for direct free-kicks, with increased probabilities approaching 0.11 for free-kicks taken from a central location in front of goal. Moreover, similar time constraints on goalkeepers were observed in these instances as for penalty kicks, assuming the aforementioned premise of late information pick-up holds. Further research on the use of a defending wall as a means of defending direct free-kicks in football is required.

3.10 "Empirical Coaching": Guiding Principles in Enabling Coach Expertise

Stuart Morgan (Australian Institute of Sport, Bruce, AU)

Successful football coach, Bernd Schröder, once said "there is no science in football". Performance analysis and computer science in sport has made considerable progress in recent years, yet Schröder's statement remains representative of the perceptions of many coaches. Furthermore, 2008 Tour de France winner Carlos Sastre, complained about the counter-intuitive nature of his cycling power software, and said "The computer must understand me. I don't understand the computer. It is more intelligent than me…". These two quotes illustrate two of the most significant questions for computer science in sport: what are the barriers that prevent coaches from embracing sports and computer science, and, how can

data be presented in more meaningful ways such that coach expertise is enabled (rather than threatened) by science?

It is proposed that coaches develop expertise using primary modes of game feedback, such as direct visual observation, video review, basic game statistics, input from other first hand observers such as assistant coaches, and crude insights from match outcomes such as the progressive scoreline. It is from these non-empirical sources that coaches build and test decision making schemas. Certainly, it is not until much later in their careers that coaches become exposed to empirical data, often derived by specialist sports scientists, who provide the them with a potentially bewildering array of game and performance data. It may often be that coaches do not possess the knowledge frameworks to absorb or exploit these sources of information, and that empirical data presented by scientists does not therefore influence their coaching decisions. It is proposed that consideration needs to be given to the problem of data visualisation, and in particular, matching data presentation techniques to the learning styles, decision making schemas, and game perception frameworks that coaches have otherwise used throughout their careers.

This presentation aimed to open discussions about how performance analysis data can be visualised using advances in computer science in ways that enable and amplify coach expertise, rather than attempting to supplant it. An exemplar was presented in which frequent itemsets were used to scan large amounts of ball movement data in field hockey for recurring ball movement trends. Visualisation techniques were presented, for which the primary aim was to communicate a simple pattern from within large and complex datasets.

3.11 Net-based Game Analysis by Means of DyCoN and SOCCER

Jürgen Perl (Mainz, DE)

Joint work of Perl, Jürgen; Memmert, Daniel; Grunz, Andreas

Game analysis has become much easier by automatic position recording. However, the problem remains how to transfer the astronomic amount of available data to a selection of useful information. Our approach is based on two ideas: data reduction and pattern recognition.

In the first step, by means of SOCCER, the position data of the players of a team are reduced to those of tactical groups like offense or defence, followed by normalization, where the players' constellations on the playground are reduced to their geometric formations relative to their centroids - i.e. the playground-independent position patterns.

In the second step, those patterns are learned by the self-organizing neural network DyCoN, resulting in a collection of formation clusters, each containing a variety of shapes of the corresponding formation type. Based on that information, game analysis with DyCoN and SOCCER works as follows: Along the time-axis, position data of interacting tactical groups are fed to the net, which recognizes the time-dependent corresponding formation types.

A first quantitative analysis then results in frequency distributions of formation types. Recombination with the playground position information leads to a playground specific frequency distribution. And adding the time information finally allows for process and interaction oriented analyses. Moreover, SOCCER not only offers quantitative results but also qualitative ones like game animation and tactical analyses by use of additional semantic

action valuation. While DyCoN and SOCCER are developed by the author, data preparation and semantic analysis are supported by the program VisuCat, developed by Andreas Grunz [1, 4].

The project as a whole is run in co-operation with Daniel Memmert [2, 3], German Sports University Cologne, and his game analysis working group.

References

1 A. Grunz, D. Memmert, and J. Perl, *Analysis and simulation of actions in games by means of special self-organizing maps*, International Journal of Computer Science in Sport **8** 2009, 22–37.

2 D. Memmert, and J. Perl, *Game creativity analysis by means of neural networks*, Journal of Sports Sciences **27** 2009a, 139–149.

3 D. Memmert, and J. Perl, *Analysis and simulation of creativity learning by means of artificial neural networks*, Human Movement Science **28** 2009b, 262–282.

4 A. Grunz, S. Endler, D. Memmert, and J. Perl, *Netz-gestützte Konstellations-Analyse im Fußball [Net-based constellation analysis in soccer]*. Workshop on Computer Science in Sport, Darmstadt, 2011 (to appear).

3.12 Can We Measure Football Tactical Behavior by Using Dynamic Positional Data?

Jaime Sampaio (Universidade de Trás-os-Montes – Vila Real, PT)

Football can be considered as a game sport comprised of subsystems with intra and inter-dynamic interactions and that the findings of chance and chaos in the course of the game are to be expected within the framework of these dynamical (complex) systems. The present study explored how football players' positional data can be used to access tactical behavior by measuring movement patterns and inter-player coordination. A pre post-test design was used to access the effects of a 13-week constructivist teaching program by accomplishing a 6×6 football small-sided game, played on a 60×40 m outdoor natural turf pitch. Data was captured at 5Hz by GPS devices (SPI Pro, GPSports, Canberra, Australia). In addition to positional data gathered (x, y) the following dependent variables were calculated in this study: distance of player from the geometric center of the team; maximal and minimal distance of player to the geometric center of the team. All data was analyzed with non-linear signal processing methods such as Approximate Entropy and Relative Phase. Approximate entropy values were lower in post-test situations suggesting that these time series became more regular with increasing expertise in football. Relative phase post-test values showed several stability periods with a clear trend to moving in anti-phase, as measured by players' distance to the center of the team.

Players' maximal and minimal distance from the center of the team had smoother variations, but more regular values were found in post-test and decreases in distance of 0.83 m and 1.5 m, respectively. It seems possible to measure Football tactical behavior by using dynamic positional data. Advances in this topic should allow exploring different variables, different samples and also the positional relations between confronting teams, opening up new topics under the tactical scope, allowing to narrowing the gap between science and coaching.

3.13 Model-Based Optimization of Pacing Strategies for Cycling Time Trials

Dietmar Saupe (Universität Konstanz, DE)

Based on a physical model for the forces that must be applied by pedaling while cycling and a simple physiological model for the exertion of the athlete as a function of his/her accumulated power output, an optimal riding strategy for time trials on mountain ascents is computed. A combination of the two models leads to a mathematical optimization problem that can be solved numerically by discretization. The physical model depends most sensitively on an accurate estimation of the road slope on the course. For this purpose, we also present a new method that combines model-based slope estimations with noisy measurements from multiple GPS signals of differing quality. Altogether, we provide a means to analyze rider performance, to identify and quantify potential performance improvement, as well as to instruct the athlete exactly where and how to change his/her pacing strategy to achieve these gains.

3.14 Evaluation of Image Detection Systems in Football

Malte Siegle (TU München, DE)

In football there are several position detection systems providing x, y-coordinates and movement velocities of all players on the pitch (e.g. AMISCO). These data are used to analyse different aspects of football, for example the loads imposed on players or fatigue during a match. Undoubtedly, coaches as well as scientists have a huge interest and benefit of these analyses. Nevertheless, the quality, especially the accuracy of the position detection systems should be controlled. There are only a few studies analysing the accuracy of different position detection systems, but these studies show either problems in their test design, or used lighting gates, resulting in a single comparable value for each test run. The current study presents a new method of analysing accuracy of such data. Using a Laveg laser measurement device, positions of two runners were obtained by the empirical gold standard and by a two camera based position detection system. By using the Laveg device, huge numbers (150-300) of comparable values could be obtained for every single run. Different tests (Linear runs, Acceleration-Stop-Turn-Acceleration-Runs, and different distances of runners to cameras) were performed in order to detect possible error sources of the system. Main problems for the system occurred for runners further away from the cameras and for players overlapping each other. Linear runs were measured accurately. Altogether, the presented method raises the standards of controlling the accuracy of position detection systems. Future studies should focus on the separation of different error sources.

3.15 Game Interruptions in Football

Malte Siegle (TU München, DE)

The objectives of the study were to analyse game interruptions of league soccer in detail and the tactical use of game interruptions. Sixteen matches of a German first league soccer team were observed. An observational system was designed to assess interruption types, score, duration of interruption, location of interruption, time of interruption and number of occurrences. Results showed that there is an average of 108 interruptions per match. Throw-ins and free kicks were most frequent. Referee balls, penalties, and injuries occurred least often. In 38% of the total time matches were halted. The analysis showed significant differences concerning the influence of the location of interruption, score, and time of interruption on the duration of different interruption types ($p < .05$).

The results of the study showed the tactical use of game interruptions during league soccer matches, e.g. goal kicks of the leading team take longer towards the end of the match. Moreover, analysis of positional data showed that relative running distances during interrupted match intervals were reduced by 1 m/s compared to those during running match intervals. Examining game interruptions has turned out to be a valuable source of information adding to our knowledge on soccer. We have shown evidence that the durations of many interruptions serve tactical purposes, a well-known hypothesis in practice.

3.16 Working with the Austrian U17 Women's National Football Team

Johannes Uhlig (Universität Wien, AT)

The focus of the article discusses the work with the Austrian U17 women's national football team. It mainly illuminates the strategic and tactical work and game philosophy and the basic 4-4-2-system gets explained in more detail. This 4-4-2-system changes in attack in a 4-2-4-system and in the defence in a 4-5-1, whether the switching phases often decides games.

The match schedule is mentioned as a special intervention, which is geared more closely to the respective adversaries. Finally, the theoretical and practical work with the TAP (Tactical animation program) is presented.

3.17 Offside and Wembley Goal – Can Computer Science Help Overcome Erroneous Decisions in Soccer?

Josef Wiemeyer (TU Darmstadt, DE)

The field of sport practice is full of interesting phenomena that lead to uncertainties and sometimes annoyance. Sport science is able to uncover the reasons for these phenomena and

to develop solutions. Two phenomena in soccer are a persistent threat to fairness und equal chances in soccer:

1. Erroneous offside decisions (Reasons: perspective and synchronous visual perception, flash-lag effect) according to research about 20 to 25% of offside decisions are wrong!
2. Erroneous goal decisions (Reason: depth perception and stereoscopic vision)

Using these two examples the question arises if and how computer science can help to improve the situations of the referees in soccer. In the past, selected options have been suggested to solve these problems. This statement emphasizes the strong support computer science in sport can give to solve persistent issues in soccer practice. Referees and their assistants are systematically overloaded by the perceptual demands in offside and goal decision situations. Information technologies should support them to ensure a maximum level of fairness and equal chances.

4 Working Groups

4.1 Session Summary: RoboCup

Keith Lyons (University of Canberra, AU)

The second session on Day 1 of the Computer Science in Sport Conference (Special Emphasis:Football) at Schloss Dagstuhl was dedicated to Robocup. Sven Behnke (Universität Bonn) introduced the session with some historical background about Robocup competitions. Bernhard Nebel (University of Freiburg) provided further background about the origins of Robocup. He discussed sensor interpretation (inputs and outputs) and noted the importance of cooperative sensing. Bernhard explored the ways in which robots can act cooperatively:

1. Avoidance of interference
2. Task decomposition and re-allocation
3. Joint execution
4. Dynamic role re-assignment

There are four roles for each robot in 4v4 Robocup: goalkeeper (fixed), active player, supporter, and strategic. Each role has a preferred location that is situation dependent. Each player computes the utility for each outfield role and shares it with the other outfield robots.

Bernhard discussed the development of table soccer as a micro-version of large space games. There is a commercially available table. This table uses a reactive scheme but Bernhard has been looking at anticipation schemes with decision theoretic planning. Recent research has simulated games between a decision theoretic system against a reactive system.

Sven and Berhard's presentations stimulated a great deal of interest and questions. Sven concluded the session with a discussion of technical challenges in humanoid robot design and performance.

4.2 Session Summary: Miscellaneous

Keith Lyons (University of Canberra, AU)

The Computer Science in Sport Conference (Special Emphasis:Football) at Schloss Dagstuhl had a mixed group of presentations in the third session of Day 1. Malte Siegle was the first presenter in the session and discussed his work with Martin Lames on Game Interruptions in football – a neglected element for modelling the demands if the game. Malte introduced his paper with a consideration of the use of position detection systems to measure performance in football. He noted that these systems provide no data about game interruptions. In his presentation he shared an analysis of 1729 interruptions in 16 matches and discussed the time, type, location and duration these interruptions. He used Amisco System data to provide more detail about player performance in these games. Malte noted that interruptions in play were not as long as ball in play. These interruptions were located between intermittent bouts of high intensity match time (most of which were not more than a minute in length before the next interruption). He noted that:

1. There was an average of 108 interruptions per match: these ranged from 0.13% (penalties) to throw in at 39.69% of all interruptions.
2. The average duration of these interruptions ranged from a throw in at 9 seconds to injury at 82.5 seconds.

Malte then made some very important observations about how the place where the interruption takes place affects the length of interruption. He provided some interesting data comparing attacking and defending throw ins. He noted too that direct free kicks in offensive areas with a direct shot at goal opportunity take longer and can reach an average of 36.59 seconds. Malte indicated that the state of play (winning, losing, drawing) has an impact of the length of interruptions. A team winning can take up an additional 3 seconds on goal kicks and up to 5 seconds on free kicks. This tendency for winning teams to take longer over interruptions becomes even more noticeable towards the end of the game (particularly in relation to throw ins). Malte concluded his presentation with data about distance travelled in uninterrupted and interrupted games. He used Amisco data to provide detail of these distances. Malte noted that there was evidence that goalkeepers run more in interrupted play and central defenders less. Malte's final point was an invitation to consider how interruptions might be used for player recovery and that this recovery may vary within a team depending on a player's positional responsibilities. Malte's and Martin's work has received recent publicity [1, 2].

The second presentation of the session was made by Josef Wiemeyer and was titled Offside and the Wembley Goal – Or can Computer Science help overcome erroneous decisions in Soccer? In his presentation, Josef noted:

1. 20–25% offside decisions are wrong.
2. 80% of these are false alarms
3. Decisions about offside are affected by synchronous optic perception [3, 4].

Josef indicated the role training of synchronous optic perception can play in improving decision making. However there is no evidence of the longer term affects of this training (experimental trials last six weeks) and there is still the issue of dealing with moving stimuli [5] and the Hazelhoff flash lag effect [4]. Josef discussed three solutions to these problems:

training, technology, and changing the rules. Josef then extended his discussion to the arbitration of goal line technology and used examples of 'goals' from 1966 and 2010 (Germany v England). He provided details of FIFA and IFAB discussions around goal line technology. He concluded his presentation with an invitation to delegates to consider transparency, justice and fairness in decision making by officials.

Karen Roemer presented the third paper of this session and invited delegates to discuss the design options for a longitudinal study of female athletes' ACL injuries (including female football, basketball and volleyball players). Karen noted that most research into ACL injury is mostly retrospective. She is keen to plan a prospective study.

Arnold Baca (Universität Wien) followed Karen's presentation with a discussion of the development of a mobile coaching system (Mobile Coach 1.0). Arnold noted the feedback potential of this system for elite and mass participation applications. Two papers detail the development of this work [6, 7].

Josef Wiemeyer concluded the session with a discussion of Serious Games New options for learning and training in sport. He discussed the role serious games can play in health promotion and their growing use in *exergaming*. He sounded a note of caution about the energy expenditure in such games and discussed the relative small transfer of skills from games to real life sport. He concluded that "games support what they demand". He encouraged delegates to consider the role serious games can play in improving: sensory motor activity; cognition; motivation, emotion, volition; social competency; and media competency. The session concluded at 6 p.m.

References

1 M. Pangallo. *Men are 'drama queens' when it comes to football, say scientists.* `http://www.metro.co.uk/sport/oddballs/868049-men-are-drama-queens-when-it-comes-to-football-say-scientists`, 1st July, 2011.

2 Inside World Soccer. *Men footballers play act more than women do, say scientists.* `http://www.insideworldsoccer.com/2011/07/men-footballers-play-act-more-than.html`, 2nd July, 2011.

3 M. Sachsenweger. *Testing visual perception of three-dimensionally moving objects (dynamic stereoscopy).* Documenta Ophthalmologica **64** 1986, 379–385.

4 M. Baldo, R. Ranvaud, E. Morya. *Flag errors in soccer games: the flash-lag effect brought to real life.* Perception **31** 2002, 1205–1210.

5 R.R.D. Oudejans, R. Verheijen, F.C. Bakker, J.C. Gerrits, M. Steinbrückner, and P. J. Beek. *Errors in judging 'offside' in football.* Nature **404** 2000, 33.

6 A. Baca, P. Dabnichki, M. Heller, and P. Kornfeind. *Ubiquitous computing in sports: A review and analysis.* Journal of Sports Sciences **12** 2009, 1335–1346.

7 A. Baca, P. Kornfeind, E. Preuschl, S. Bichler, M. Tampier, and H. Novatchkov. *A Server-Based Mobile Coaching System.* Sensors **10** 2010, 10640–10662

4.3 Session Summary: Dynamical Systems and Neural Networks

Jürgen Perl (Mainz, DE)

The idea of the session was to demonstrate how the complex dynamics of systems - as e.g. are endurance of athletes, phases of team positions on the playground, or interactions of tactical groups - can be analyzed by means of appropriate modelling. There are mainly two

approaches that support each other but can be dealt with separately, as had been done in the session: The dynamics of a system or a team as a whole and the behavioural patterns of specific functional or tactical groups.

In the first part of the session, Dietmar Saupe from the University of Konstanz, Germany, started with an introduction to the ideas of Dynamical Systems from a mathematical point of view, where an iteratively described process moves through phase spaces and eventually finds an attracting fix-point - or is lost in the chaos of an infinitely dense set of attractors. Those system properties can be mapped to changing phases as well as to aspects of stability and instability in motions, endurance sports, or games. His example of application came from the area of endurance sports, where the biker together with the bike and the environment like road surface, altitude profile or weather conditions build a complex dynamical system, which can be modelled and analysed by means of biomechanical equations.

In the second presentation, Jaime Sampaio from the University of Vila Real, Portugal, continued with position analysis in small sided (6 vs 6) soccer, where the success of the teams depends on the relative positions of the players. Subjects of the study were dynamical systems behaviour of the group like the effect of changes in single players' positions on tactical results, stability periods and relative phase analyses. Moreover, the connection to net-based pattern recognition techniques became clear.

The third presentation was given by Koen Lemmink form the University of Groningen, Netherlands, who also dealt with small sided soccer, concentrating on phase analyses: The centroids of the players' position build abstract team positions that move over the playground and so build time-dependent dynamical patterns. Sometimes the patterns of the both teams are in phase, sometimes not. The question of those phase-oriented analyses is in which way in-phase and anti-phase behaviour contain information about the tactical orientation and success of a team.

The second part of the session started with an introduction to self-organizing neural networks, given by Peter Lamb from the Technical University of Munich, Germany, who demonstrated how those nets are organized, how neurons can learn, and how such networks can be applied to analyse time-series data. His main example dealt with motions in golf, where networks can be used for identifying changes in coordination, clustering motion patterns and visualization of stability, which is also specific to dynamical systems and so focuses on the connection between dynamical systems and neural networks.

In the last presentation, Jürgen Perl, Mainz, Germany, demonstrated how self-organizing neural networks can be used for analyzing tactical behaviour in soccer games. To this aim, the constellations of tactical groups relative to their centroids are normalized to formations, the patterns of which can be learned and clustered to specific types by means of neural networks. The time-series of those types together with the corresponding centroid information build the basis for quantitative as well as for qualitative game analysis.

4.4 Session Summary: Coaching

Stuart Morgan (Australian Institute of Sport, Bruce, AU)

Session 3 of Day 2 at the Computer Science in Sport Conference (Special Emphasis:Football) at Schloss Dagstuhl was dedicated to Coaching themes. The session was chaired by and

introduced by Dr Stuart Morgan (Australian Institute of Sport). His introduction focused on the challenges and important issues in the communication between coaches and scientists in high performance. The presentation also explored the idea that a major contribution of data analytics and computer science in sport is in addressing the "signal to noise" problem where important patterns within a dataset may be obscured within very large amounts of data. An example of this challenge was presented using ball movement data from the 2010 Champions' Trophy Tournament, and one useful solution using association mining techniques to reveal frequent pattern itemsets was presented using these data. The presentation concluded by proposing that two significant challenges were current in computer science in sport:

1. to identify the barriers that prevent coaches from embracing sports and computer science;
2. to explore new ways that data be presented such that existing coaching expertise is *enhanced* by emprically-derived information.

The next presenter was Professor Keith Lyons (University of Canberra, Australia), who used the online presentation system, Prezi, to share data from the first two rounds (n =16 games) of the 2011 FIFA Women's World Cup. Professor Lyons drew attention to patterns of goal scoring and the relationship with FIFA ranking (18 March 2011). The paper included a profile of winning, losing and drawing in the 16 games (presented as averages). The paper was used as a stimulus for a discussion of technical and tactical aspects of game play at this World Cup and in football generally.

Associate Professor Tim McGarry (University of New Brunswick, Canada) then presented a discussion paper titled: "Human Information Processing: Penalty and Free Kicks". Dr McGarry shared some descriptive data from penalty kicks and shoot outs from European Championships and World Cups from 1976 to 2010 (1976 saw introduction of penalty shoot outs). He noted that in penalty shoot outs, penalty number 4 appears to be the weakest link in a shoot-out (of 5 penalties taken). Dr McGarry posed the question about who should take this penalty? Should the most experienced (and successful) penalty taker be allocated this role? Dr McGarry discussed goalkeeper actions in penalties and considered the options available in the time frame of the penalty kick task (approximately 400 ms). Dr McGarry also discussed free kicks, and presented descriptive data from the 2002 and 2006 World Cups, and the 2004 European Championships. He discussed the optimisation of goalkeeper reaction and response, and the role of a defensive wall in these free kick situations.

Dr Joachim Gudmundsson (NICTA, Australia), was the fourth presenter in this session. He discussed extracting and making sense of information from trajectories. He discussed his work in the defence services, with animal behaviour and in sport. Dr Gudmundsson presented visualisations depicting player movements and possible ball passing options in football data.

Dr Johaness Uhlig (Universitat Wien) was the next presenter and discussed his work with the Austrian Under 17 Women's team and with his club team. He described his coaching and his tactical approach based on a basic 4-4-2 formation. Dr Uhlig emphasised three phases of play: attack, defence, switchover. He discussed the development of a tactical animation program (TAP) to support coaches and its use in practice.

In the final presentation for the session Dr Koen Lemmink (University of Groningen) on Tactical Match Analysis in Soccer: New Perspectives? For some of the ideas discussed in this paper see Frencken, Lemmink and Delleman (2010). Dr Lemmink explored three different approaches to observing and analysing performance. He provided examples of each approach. Firstly, a "Practice Model" that uses frequencies of event data and player profiles. This is coach driven and has a focus on direct feedback. Next, a "Statistics Model" that identifies

performance indicators, and notes statistical differences. This is a domain populated by mathematicians, statisticians and econometricians, with a focus on pattern analysis and recognition. Finally, a "Theory Model" that uses scientific insight to understand interactions and networks. He emphasised the possibilities of building multidisciplinary teams that had a strong focus on explanations and shared rich data on positional play.

A vibrant discussion followed the presentations, that was particularly relevant to the high performance sports domain. Max Reckers, formerly the performance analysis specialist at the Bayern Munich Football Club, provided considerable insight to the discussion, and he discussed his ideas about sharing data. This included consideration of the role of the embedded scientist in a sport setting.

4.5 Session Summary: Media and Data Acquisition

Keith Lyons (University of Canberra, AU)

The morning session discussed Media and Data Acquisition issues. The session was chaired by Daniel Link (TU München). Daniel presented first in this session. He reported on the Game Data Library Project for the Bundesliga. Daniel discussed the game observation process for the Game Data Library. This involves the acquisition of basic data that includes match information data, tracking data (at 25 Hz), event data, static video data that are used to create raw data and statistics. Daniel presented the architecture of this service to provide data flow. He discussed the Game Data Model. Daniel presented an ontology of definitions in use in this project. This ontology has a data structure for: smart calculation; efficient processing and storing of data; and object orientation and the use of Unified Modelling Language (UML). Daniel concluded his talk with a consideration of the challenges of this project for sport science. These included how to use the enormous amounts of data that will be generated and how to develop tools to analyse the data.

Roland Leser (Universitat Wien) was the second presenter in the session. His topic was Position tracking as a challenge in game sport analysis. In his talk Roland gave an excellent exposition of how to develop a position tracking system. He noted systems such as Tracab and Catapult. He discussed radio wave systems too, including Ubisense (tag) and InMotio LPM (transponder). In choosing a system for use in his research Roland identified these criteria:

1. Off the shelf availability
2. Price
3. Sensor size
4. Sampling rate
5. Accuracy
6. Robustness (hardware, signal, definition of player)
7. Application in training and game play
8. Opponent agreement within competition

Roland discussed the use of an Ubisense system. To date this system has not been used extensively in sport. He demonstrated the installation of the system in a sports hall. Ubisense has a 160 Hz facility that is not common with other Ubisense clients. The hall is calibrated

and then checked for accuracy of measurement. The system allows some for data filtering (low pass and Kalman). Roland noted the development of software tools for the system to enable data visualisation (including heat maps) and performance analysis. Roland shared an example of the recording movement with the system (small sided football).

The final presentation of the morning was by Malte Siegle. Malte looked at the accuracy of image recognition in dynamic situations. He shared the development of protocols to check the accuracy of image recognition in respect of Laveg and laser light measurement. The field tests were conducted in a soccer stadium:

1. A linear run near the cameras with constant velocity. (Image detection worked well.)
2. Acceleration, stop, reacceleration in same direction. (Image detection issues arise with up to 1 metre error.)
3. Two players move towards each other and return after 180 degrees turn. (An error of more than 1.5 metres.)
4. Circular run with constant velocity (Image detection worked well.)

Malte noted the variability in errors in these tests and discussed the impact of the player's distance from the cameras. These tests had identified the need for better static position detection and the clear differentiation of error sources (distractions). Malte did end with some very positive views about the protocols: good values were recorded and problems were identified. This research raised the possibilities of a new standard in the evaluation of image detection. Ultimately this will lead to the comparisons of different image detection systems.

Participants

- Arnold Baca
Universität Wien, AT
- Zied Bahrouni
TU München, DE
- Sven Behnke
Universität Bonn, DE
- Joachim Gudmundsson
The University of Sydney, AU
- Peter Lamb
TU München, DE
- Martin Lames
TU München, DE
- Koen A.P.M. Lemmink
University of Groningen, NL
- Roland Leser
Universität Wien, AT
- Daniel Link
TU München, DE
- Keith Lyons
University of Canberra, AU
- Tim McGarry
University of New Brunswick, CA
- Stuart Morgan
Australian Institute of Sport, Bruce, AU
- Bernhard Nebel
Universität Freiburg, DE
- Jürgen Perl
Mainz, DE
- Max Reckers
Amsterdam, NL
- Karen Roemer
Michigan Technological University, US
- Jaime Sampaio
Universidade de Trás-os-Montes – Vila Real, PT
- Dietmar Saupe
Universität Konstanz, DE
- Malte Siegle
TU München, DE
- Otto Spaniol
RWTH Aachen, DE
- Johannes Uhlig
Universität Wien, AT
- Josef Wiemeyer
TU Darmstadt, DE

Report from Dagstuhl Seminar 11272

Decision Procedures in Soft, Hard and Bio-ware (Follow Up)

Edited by

Nikolaj Bjørner[1], Robert Nieuwenhuis[2], Helmut Veith[3], and Andrei Voronkov[4]

1 **Microsoft Research - Redmond, US,** nBjørner@microsoft.com
2 **UPC - Barcelona, ES,** roberto@lsi.upc.edu
3 **TU Wien, AT,** veith@forsyte.tuwien.ac.at
4 **University of Manchester, GB,** voronkov@cs.man.ac.uk

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 11272 *Decision Procedures in Soft, Hard and Bio-ware (Follow Up)*. It was held as a follow-on for a seminar 10161, of the same title, that took place in late April 2010 during the initial eruption of Eyjafjallajökull. In spite of the travel disruptions caused by the eruption of the volcano, the original seminar received a respectable turnout by European, mainly German and Italian participants. Unfortunately, the eruption hindered participation from overseas or even more distant parts of Europe. This caused the seminar to cover only part of the original objective. The follow-on seminar focused on the remaining objectives, in particular to *bio-ware* and *constraint solving methods*.

Seminar 03.–06. July, 2011 – www.dagstuhl.de/11272
1998 ACM Subject Classification B.1.4. Microprogram Design Aids/Verification, D.2.4. Software/Program Verification, F.4.1. Mechanical theorem proving, F.4.3. Decision Problems, J.3. Biology and genetics
Keywords and phrases Hardware and Software Verification, Bio-analysis, Satisfiability Modulo Theories, Dynamic Symbolic Execution, Interpolants
Digital Object Identifier 10.4230/DagRep.1.7.23

1 Executive Summary

Nikolaj Bjørner

The main goal of the seminar *Decision Procedures in Soft, Hard and Bio-ware (Follow Up)* was to bring together renowned as well as young aspiring researchers from two groups. The first group formed by researchers who develop both theory and efficient implementations of decision procedures. The second group comprising of researchers from application areas such as program analysis and testing, crypto-analysis, hardware verification, industrial planning and scheduling, and bio-informatics, who have worked with, and contributed to, high quality decision procedures. The purpose of the seminar was to heighten awareness between tool and theory developers for decision procedures with the array of applications found in software, hardware and biological systems analysis.

The seminar fell on two and a half days in the week of July 4–6, 2011. 25 researchers from 12 countries (Germany, Austria, Italy, France, USA, United Kingdom, China, Hungary, Spain, Sweden, Czech Republic, Ireland) participated.

2 Table of Contents

3 Overview of Talks

3.1 Combined First-Order and Separation Logic Reasoning

Joshua Berdine (Microsoft Research UK – Cambridge, GB)

We describe techniques for combining first-order and separation logic reasoning used in the SLAyer verification tool. SLAyer uses separation logic to reason about memory safety properties of low-level heap-manipulating code. The Z3 SMT solver is used internally in a number of ways:

- to discharge queries that fall into the first-order fragment of separation logic;
- to reason about equality between pointer expressions, using unSat core extraction to guide sequent calculus proof search for separation logic queries; and
- to direct sequent calculus case splits by unSAT cores.

These uses employ a first-order approximation of separation logic formulas that is linear in the size of the formula and constrains the variables as strongly as the separation logic formula, but makes weaker constraints on the heap.

3.2 Open Constraint Logic Programming with SMT

Nikolaj Bjørner (Microsoft Research – Redmond, US)

Joint work of Bjørner, Nikolaj; Ethan Jackson; Wolfram Schulte
URL http://research.microsoft.com/projects/formula

I will present work in progress on open constraint logic programming using the SMT solver Z3. Similar to Datalog satisfiability, open constraint logic programming solves satisfiability of constraint programs: the input is a constraint logic program and a query, the output is a set of pairs comprising of satisfying instances to queries and additional facts that are required to satisfy the query.

The Microsoft Research FORMULA system implements open constraint logic programming and uses it for model based design.

I will describe the abstract machine that combines forward chaining and SMT solving in FORMULA and the accompanying type system that is important to constrain how additional facts can be used.

3.3 Computational Problems in Biology: Introduction and Challenges

Christoph Flamm (Universität Wien, AT)

Main reference Jakob L. Andersen, Christoph Flamm, Daniel Merkle, Peter F. Stadler, "Maximizing Output and Recognizing Autocatalysis in Chemical Reaction Networks is NP-Complete," submitted to J Sys Chem 2011.
URL http://arxiv.org/abs/1110.6051

In my presentation I will give a brief overview of computational problems in Biology with a special focus on metabolic networks. The formalization of a chemical reaction network as a stoichiometric matrix allows to derive the important concept of elementary pathways. These pathways form a convex basis which spans the space of all feasible mass flux distributions through the reaction network under steady state conditions. These flux distributions can not be measured directly but must be inferred computationally from isotope labeling experiments. The NP-hard problem of finding the chemically correct atom to atom mapping between the reaction partners in the network constitutes the core problem of all flux reconstruction algorithm. In the main part of the talk I will present our current research on a graph grammar based approach for chemical transformations which allows for an explicitly construction of the "chemical space" over a set of chemical graphs and a set of graph rewrite rules (reactions). I will clarify the notion of chemical transformation motif an will explain how chemical transformation motifs can be found in arbitrary chemical reaction networks using an integer linear programming approach. I will close my talk by posing the unsolved inverse reaction mechanism problem which seems interesting for the verification community. The challenge of the inverse reaction mechanism problem is to find a suitable set of molecules which "implement" a given abstract reaction mechanism using only chemical transformations from a pre-specified input reactions set.

3.4 Solvers for Theories of Strings

Vijay Ganesh (MIT – Cambridge, US)

Many automatic testing, analysis, and verification techniques for programs can be effectively reduced to a constraint-generation phase followed by a constraint-solving phase. This separation of concerns often leads to more effective and maintainable tools. The increasing efficiency of off-the-shelf constraint solvers makes this approach even more compelling.

However, there are few, if any, effective and sufficiently expressive off-the-shelf solvers for string constraints generated by analysis techniques for string manipulating programs. In order to fulfill this need we designed and implemented Hampi, a solver for string constraints over bounded string variables.

Hampi constraints express membership in regular languages and bounded context-free languages. Hampi constraints may contain context-free- language definitions, regular-language definitions and operations, the membership predicate and equations over string terms (word equations). String terms are constructed out of string constants, variables, concatenation and extraction functions.

Given a set of constraints, Hampi outputs a string that satisfies all the constraints, or reports that the constraints are unsatisfiable. Hampi is expressive and efficient, and can be

successfully applied to testing and analysis of real programs. Our experiments use Hampi in: static and dynamic analyses for finding SQL injection vulnerabilities in Web applications; automated bug finding in C programs using systematic testing; and compare Hampi with another string solver.

3.5 Robust Formulas over Reals and Delta-Complete Decision Procedures

Sicun Gao (Carnegie Mellon University – Pittsburgh, US)

I will present a framework for the reliable use of numerically-driven procedures for deciding nonlinear SMT problems over reals.

I will first show decidability and reasonably low complexity of decision problems in the robust fragment of SMT, which are formulas whose satisfiability remains invariant under controllable numerical perturbations, in a very rich first-order theory over reals. I will then propose the notion of delta-complete decision procedures to capture the ideal behavior of numerically-driven procedures, which should decide robust formulas correctly and also return informative answers on non-robust formulas. I argue that delta-complete decision procedures, apart from scalability, can be more suitable than the usual precise procedures for some verification problems such as bounded model checking and invariant checking of hybrid systems.

3.6 On Quantifier-free Interpolation for Arrays

Silvio Ghilardi (Università di Milano, IT)

Joint work of Bruttomesso, Roberto; Ghilardi, Silvio; Ranise, Silvio
Main reference R. Bruttomesso, S. Ghilardi, S. Ranise, "Rewriting-based Quantifier-free Interpolation for a Theory of Arrays," Proc. 22nd International Conference on Rewriting Techniques and Applications (RTA'11), pp. 171–186, LIPIcs, Vol. 10.
URL http://dx.doi.org/10.4230/LIPIcs.RTA.2011.171

The use of interpolants in model checking [4] is becoming an enabling technology to allow fast and robust verification of hardware and software. The application of encodings based on the theory of arrays, however, is limited by the impossibility of deriving quantifier-free interpolants in general [5]. In this contribution, we first show that, with a minor extension to the theory of arrays, it is possible to obtain quantifier-free interpolants [3],[1]. We prove this by designing an interpolating procedure, based on solving equations between array updates. Rewriting techniques are used in the key steps of the solver and its proof of correctness.

Arrays are usually combined with fragments of arithmetic over indexes in applications, especially those related to software verification. For example, it is known that being able to handle integer indexes with constant increment or decrement operations is important when verifying a large class of programs with loops. As a further contribution [2], we combine the above quantifier-free interpolation solver for our variant of the theory of arrays with integer difference logic over indexes.

References

1 R. Bruttomesso, S. Ghilardi, and S. Ranise. Rewriting-based Quantifier-free Interpolation for a Theory of Arrays. Technical Report RI 334-10, Dip. Scienze dell'Informazione, Univ. di Milano, 2010.

2 R. Bruttomesso, S. Ghilardi, and S. Ranise. A Combination of Rewriting and Constraint Solving for the Quantifier-free Interpolation of Arrays with Integer Difference Constraints. In *FroCoS*, 2011.

3 R. Bruttomesso, S. Ghilardi, and S. Ranise. Rewriting-based Quantifier-free Interpolation for a Theory of Arrays. In *RTA*, LIPIcs, Vol. 10, 2011.

4 T. Henzinger and K. L. McMillan R. Jhala, R. Majumdar. Abstractions from Proofs. In *POPL*, 2004.

5 D. Kapur, R. Majumdar, and C. Zarba. Interpolation for Data Structures. In *SIGSOFT'06/FSE-14*, pages 105–116, 2006.

3.7 μZ, Fixed Point Engine in Z3

Krystof Hoder (University of Manchester, GB)

Joint work of Hoder, Krystof; Nikolaj Bjørner; Leonardo de Moura
Main reference Krystof Hoder, Nikolaj Bjørner, Leonardo de Moura, "μZ – An Efficient Engine for Fixed Points with Constraints," CAV 2011: 457–462.
URL http://dx.doi.org/10.1007/978-3-642-22110-1_36

The μZ tool is a scalable, efficient engine for fixed points with constraints.

It supports high-level declarative fixed point constraints over a combination of built-in and plugin domains. The built-in domains include formulas presented to the SMT solver Z3 and domains known from abstract interpretation. We present the interface to μZ, a number of the domains, and a set of examples illustrating the use of μZ.

3.8 Modular Theorem Proving

Christopher Lynch (Clarkson University – Potsdam, US)

Joint work of Lynch, Christopher; Ralph Eric McGregor

We show how to combine theorem proving techniques. A set of first order clauses to determine satisfiability is divided into two sets S and T, not necessarily disjoint. There are two theorem provers I and J. The theorem provers must be sound and refutationally complete, and I must be able to produce an (over-approximation of) a model. I is run on S, and J is run on T. If I determines that S is satisfiable, then I passes a candidate model M to J. If J determines that M union J is unsatisfiable then J passes back a learned clause witnessing the unsatisfiability to I. The process is repeated until I reports unsatisfiability or J had nothing new to learn. The process is sound and refutationally complete.

This is an abstract results, which can be instantiated with different theorem provers, possibly more than two. SMT is an instance of this, where S contains propositional clauses, T represents a theory, I is DPLL and J is a theory solver for T. However, our results allow for

full first order and overlaps between the theories. We also show how Resolution/Superposition can construct an over-approximation of a model, and be used as the theorem prover I.

3.9 Haplotype Inference with Boolean Optimization

João Marques-Silva (University College – Dublin, IE)

Joint work of Marques-Silva, João; Lynce, Ines ; Graca, Ana ; Morgado, Antonio; Oliveira, Arlindo

Motivated by the success of Boolean Satisfiability (SAT) solvers, there has been recent work on solving combinatorial optimization problems in Bioinformatics with SAT and SMT-based solutions. This talk overviews the successful use of SAT-based approaches in solving a concrete combinatorial optimization problem in Bioinformatics, namely haplotype inference.

The talk will details the models used the haplotype inference problem, and also overviews the algorithms used for implementing SAT and SMT- based optimization.

3.10 Computing the Size of the Solution Space

Feifei Ma (Chinese Academy of Sciences, CN)

Joint work of Ma, Feifei; Liu, Sheng; Zhang, Jian
URL http://dx.doi.org/10.1007/978-3-642-02959-2_33

Most constraint solvers and decision procedures try to decide whether a given set of formulas (constraints) are satisfiable, and try to find a solution in case they are indeed satisfiable. In this talk, we discuss a different but related class of problems, i.e., how to compute the number of solutions or the size of the solution space. Such a problem can be regarded as the counting version of the decision problem. We describe the motivation for this work, a prototype tool for solving a special version of the problem (i.e., SMT instances on linear arithmetic), and application of the technique and tool to program analysis. In addition, we are also investigating optimization problems that are constrained by SMT formulas. We use similar techniques for computing the solution space size and for solving the generalized optimization problem. (The details are available in a technical report.)

References

1 Feifei Ma, Sheng Liu and Jian Zhang, Volume Computation for Boolean Combination of Linear Arithmetic Constraints. CADE 2009: 453-468.
2 Feifei Ma, Jun Yan and Jian Zhang, Solving Generalized Optimization Prolems Subject to SMT Constraints. Technical Report, ISCAS-SKLCS-11-12, 2011.

3.11 Using Bounded Model Checking to Focus Fixpoint Iteration

David Monniaux (Verimag, FR)

Joint work of Monniaux, David and Gonnord, Laure
Main reference David Monniaux und Laure Gonnord, "Using Bounded Model Checking to Focus Fixpoint Iterations", SAS 2011, pp. 369–385, LNCS Vol. 6887, Springer-Verlag.
URL http://dx.doi.org/10.1007/978-3-642-23702-7_27

Two classical sources of imprecision in static analysis by abstract interpretation are widening and merge operations. Merge operations can be done away by distinguishing paths, as in trace partitioning, at the expense of enumerating an exponential number of paths. In this talk, we describe how to avoid such systematic exploration by focusing on a single path at a time, designated by SMT-solving. Our method combines well with acceleration techniques, thus doing away with widenings as well in some cases. We illustrate it over the well-known domain of convex polyhedra.

3.12 SAT Modulo Theories and Scheduling Applications

Robert Nieuwenhuis (UPC – Barcelona, ES)

Here we first give an overview of SMT, the DPLL(T) approach to SMT (Nieuwenhuis et al, JACM, November 2006), and its implementation in our Barcelogic SMT tool.

Then we discuss current work on the development of SMT technology for hard combinatorial (optimization) problems outside the usual verification applications. The aim is to obtain the best of several worlds, combining the advantages inherited from SAT: efficiency, robustness and automation (no need for "tuning") and CP features such as rich modeling languages, special-purpose filtering algorithms (for, e.g., planning, scheduling or timetabling constraints), and sophisticated optimization techniques. We give several examples and discuss the impact of aspects such as first-fail heuristics vs. activity-based ones, realistic structured problems vs. random or handcrafted ones, and lemma learning.

3.13 SAT/SMT Techniques for Scheduling Problems with Sequence-Dependent Setup Times

Albert Oliveras (TU of Catalonia – Barcelona, ES)

The well-known success of SAT/SMT techniques in verification applications has motivated researchers to also focus on other application areas. In this talk, we will focus on scheduling problems with sequence-dependent setup times, that is, problems where a certain time is required to prepare the necessary resources to perform a given task. Since setup times are sequence-dependent, they depend both on the current task and the one immediately preceding it.

We will present two versions of this problem depending on the function to minimize: (i) makespan and (ii) earliness plus tardiness. In both cases, will explain how we can build upon SAT/SMT technology.

3.14 SAT Modulo Non-Linear Integer Arithmetic and Linear Invariant Generation

Albert Rubio (UPC – Barcelona, ES)

Joint work of Borralleras, Cristina; Larraz, Daniel; Lucas, Salvador; Oliveras, Albert; Rodríguez-Carbonell, Enric; Rubio, Albert

Polynomial constraint solving plays a prominent role in several areas of hardware and software analysis and verification. In this talk we propose a new method for solving non-linear constraints over the integers based on encoding the problem into an SMT problem considering only linear arithmetic. Unlike other existing methods, our method focuses on proving satisfiability of the constraints rather than on proving unsatisfiability, which is more relevant in several applications. In particular, we show how our solver can be used inside the so-called constraint-based invariant generation approach, first described in Colon et al. 2003, to obtain linear invariants of imperative programs automatically. Implementation issues are described and future extension addressed.

The talk is based on the work described in [1] and [2].

References

1 Cristina Borralleras Salvador Lucas Albert Oliveras Enric Rodríguez-Carbonell Albert Rubio. *SAT Modulo Linear Arithmetic for Solving Polynomial Constraints*. Journal of Automated Reasoning, 2011. DOI 10.1007/s10817-010-9196-8.

2 Daniel Larraz. *Automatic Generation of Loop Invariants*. Master Thesis, 2011. Universitat Politecnica de Catalunya.

3.15 Decidability and complexity for the verification of safety properties of reasonable linear hybrid automata

Viorica Sofronie-Stokkermans (MPI für Informatik - Saarbrücken, DE)

Joint work of Sofronie-Stokkermans, Viorica; Damm, Werner; Ihlemann, Carsten

We identify an industrially relevant class of linear hybrid automata (LHA) called reasonable LHA for which parametric verification of convex safety properties with exhaustive entry states can be verified in polynomial time and time-bounded reachability can be decided in nondeterministic polynomial time for non-parametric verification and in exponential time for parametric verification.

Properties with exhaustive entry states are restricted to runs originating in a (specified) inner envelope of some mode invariant.

Deciding whether an LHA is reasonable is shown to be decidable in polynomial time.

The results are presented in a paper published in the proceedings of HSCC 2011.

3.16 Solving Systems of Linear Inequalities by Bound Propagation.

Andrei Voronkov (University of Manchester, GB)

Joint work of Voronkov, Andrei; Korovin, Konstantin

In this talk we introduce a new method for solving systems of linear inequalities. The algorithm incorporates many state-of-the-art techniques from DPLL-style reasoning.

We prove soundness, completeness and termination of the method.

3.17 An Efficient Decision Procedure for Imperative Tree Data Structures

Thomas Wies (IST Austria – Klosterneuburg, AT)

Joint work of Wies, Thomas; Muñiz, Marco; Kuncak, Viktor
Main reference Thomas Wies, Marco Muñiz, Viktor Kuncak, "An Efficient Decision Procedure for Imperative Tree Data Structures," CADE 2011: 476–491
URL http://dx.doi.org/10.1007/978-3-642-22438-6_36

We present a new decidable logic called TREX for expressing constraints about imperative tree data structures. In particular, TREX supports a transitive closure operator that can express reachability constraints, which often appear in data structure invariants. We show that our logic is closed under weakest precondition computation, which enables its use for automated software verification. We further show that satisfiability of formulas in TREX is decidable in NP. The low complexity makes it an attractive alternative to more expensive logics such as monadic second-order logic (MSOL) over trees, which have been traditionally used for reasoning about tree data structures.

3.18 Lazy Decomposition for Distributed Decision Procedures

Christoph Wintersteiger (Microsoft Research UK – Cambridge, GB)

Joint work of Hamadi, Youssef; Marques-Silva, Joao; Wintersteiger, Christoph
Main reference Hamadi, Marques-Silva, Wintersteiger, "Lazy Decomposition for Distributed Decision Procedures," Workshop on Parallel and Distributed Methods in Verification, 2011.
URL http://dx.doi.org/10.4204/EPTCS.72.5

The increasing popularity of automated tools for software and hardware verification puts ever increasing demands on the underlying decision procedures. In this seminar talk, we present a framework for distributed decision procedures (for first-order problems) based on Craig interpolation.

Formulas are distributed in a lazy fashion, i.e., without the use of costly decomposition algorithms. Potential models which are shown to be incorrect are reconciled through the use of Craig interpolants. Experimental results on challenging propositional satisfiability problems indicate that our method is able to outperform traditional solving techniques even without the use of additional resources.

4 Working Groups

4.1 An SMT format for Strings, Sequences and Regular Languages

We arranged a discussion session around the topic of creating an interchange format for logical formulas using strings, regular expressions and grammars. This is increasingly relevant as decision procedures are being developed and used for analyzing string-manipulating programs. There are several applications. One important application area is for sanitizer programs that remove potentially malicious content from strings so that they can be safely used when performing data-base queries or used as parameters to Java-script code run inside a browser. We formed a working group on strings led by Vijay Ganesh and Nikolaj Bjørner. The discussion forum strings-smtization@googlegroups.com, which now has a few dozen subscribers. We summarize the objectives below.

4.2 Objectives

The objective is for a design for an SMT-LIB2 format for strings, regular expressions and context free grammars. The aim is to develop a set of core operations capturing the capabilities of main string solvers and the needs of main applications that use string constraints.

Strings can be viewed as an instance of the theory of monoids (sequences) where the main operations are creating the empty string, the singleton string and concatentation of strings. Unification algorithms for this theory has been subject to extensive theoretical advances over several decades. In contrast modern programming environments support libraries that contain a large set of string operations. Applications arising from programming analysis tools use the additional vocabulary available in libraries. A realistic interchange format should therefore support operations that are encountered in applications.

Note that SMT-LIB distinguishes between theories, which define sort and function symbols and their semantics, and logics which define the fragment of the language of one or more theories (see the reference document or the tutorial at http://www.smt-lib.org/) that one wants to work with.

4.3 Working Group Participants (from the seminar and afterwards)

Nikolaj Bjørner, David Cok, Vijay Ganesh, Tim Hinrichs, Pieter Hooimeijer, Ruzica Piskac, Prateek Saxena, Cesare Tinelli, Margus Veanes, Andrei Voronkov and Ting Zhang.

Participants

- Joshua Berdine
Microsoft Res. UK – Cambridge, GB
- Nikolaj Bjørner
Microsoft Res. – Redmond, US
- Christoph Flamm
Universität Wien, AT
- Vijay Ganesh
MIT – Cambridge, US
- Sicun Gao
Carnegie Mellon University – Pittsburgh, US
- Silvio Ghilardi
Università di Milano, IT
- Krystof Hoder
University of Manchester, GB
- Deepak Kapur
University of New Mexico – Albuquerque, US
- Laura Kovacs
TU Wien, AT
- Christopher Lynch
Clarkson Univ. – Potsdam, US
- Feifei Ma
Chinese Academy of Sciences, CN
- Joao Marques-Silva
University College – Dublin, IE
- David Monniaux
VERIMAG – Gières, FR
- Robert Nieuwenhuis
UPC – Barcelona, ES
- Albert Oliveras
TU of Catalonia – Barcelona, ES
- Ruzica Piskac
EPFL – Lausanne, CH
- Enric Rodriguez-Carbonell
UPC – Barcelona, ES
- Albert Rubio
UPC – Barcelona, ES
- Viorica Sofronie-Stokkermans
MPI für Informatik – Saarbrücken, DE
- Helmut Veith
TU Wien, AT
- Andrei Voronkov
University of Manchester, GB
- Thomas Wies
IST Austria – Klosterneuburg, AT
- Christoph Wintersteiger
Microsoft Research UK – Cambridge, GB
- Jian Zhang
Chinese Academy of Sciences, CN
- Ting Zhang
Iowa State Univ. – Ames, US

Report from Dagstuhl Seminar 11281

Verifiable Elections and the Public

Edited by

R. Michael Alvarez[1], Josh Benaloh[2], Alon Rosen[3], and Peter Y. A. Ryan[4]

1 **Caltech – Pasadena, US,** rma@hss.caltech.edu
2 **Microsoft Research – Redmond, US,** benaloh@microsoft.com
3 **The Interdisciplinary Center – Herzliya, IL,** alon.rosen@idc.ac.il
4 **University of Luxembourg, LU,** peter.ryan@uni.lu

Abstract

This report documents the program of Dagstuhl Seminar 11281 "Verifiable Elections and the Public". This seminar brought together leading researchers from computer and social science, policymakers, and representatives of industry to present new research, develop new interdisciplinary approaches for studying election technologies, and to determine ways to bridge the gap between research and practice.

Seminar 10.–15. July, 2011 – www.dagstuhl.de/11281
1998 ACM Subject Classification K.6.5 Security and Protection
Keywords and phrases Electronic voting, Internet voting, voter verification, verifiable elections
Digital Object Identifier 10.4230/DagRep.1.7.36

1 Executive Summary

R. Michael Alvarez
Josh Benaloh
Alon Rosen
Peter Y. A. Ryan

This seminar brought together leading researchers from computer and social science, policymakers, and representatives from industry to discuss the issue of "Verifiable Elections and the Public". The purpose was to present new research, develop new interdisciplinary approaches for studying election technologies, and to determine ways to bridge the gap between research and practice. This seminar built upon the foundation provided by an earlier Dagstuhl seminar in 2007: Frontiers of Electronic Voting, Seminar number 07311, http://www.dagstuhl.de/07311.

The initial sessions of the seminar were devoted to a conceptual discussion of verifiable voting, and to a summary of the apparent obstacles associated with implementing innovations in election technology. There was a general sense from most seminar participants that while great progress has been made in development of verifiable voting systems, there has not been as much progress towards testing, implementing, and deploying these new voting systems. Additionally, the research community would like to be more involved in policymaking and the practice of election administration. In particular, a panel discussion regarding obstacles to innovation was quite productive, outlining several reasons for this feeling that insufficient progress has been made, including politics, a lack of interest on the part of voters, legal and

regulatory confusion, a lack of sensitivity to the training and incentives of election officials, and a sense that some efforts to innovate have been overly ambitious and complex.

After a productive discussion of obstacles to innovation, seminar participants heard talks about a variety of recent evoting and Internet voting trials and projects. These included talks on developments in Australia, Brazil, India, Estonia, Switzerland, and Norway, as well as discussion of voting technology implementations in two U.S. counties: Cuyahoga, Ohio and Sarasota, Florida. These presentations provided a great deal of real-world information on technological and practical issues regarding the implementation of new voting systems throughout the world.

Substantial time was devoted to the presentation of new voting systems. Some of these presentations regarded innovative new conceptual and hardware schemes, including new protocols for elections and ideas like using smartphones as voting platforms. Other presentations focused on advancement and elaboration of existing voting systems, for example further development of voting systems like Helios, Wombat, Prêt à Voter, and Scantegrity. All of these presentations documented the significant progress that has been made in the scientific community, in terms of development and elaboration of important cryptographic and procedural protocols for voting, as well as new ideas for potential uses of technology in elections.

One of the most exciting new developments since the earlier 2007 Dagstuhl seminar has been the implementation and testing of some of the new voting systems that are under development. These include implementations of Helios and Wombat, and also a systematic usability and understandability project regarding Prêt à Voter. These efforts are providing important data that is aiding in the continued development of these and other related new voting systems.

Voting online continues to expand throughout the world, as was widely discussed during talks on projects in Estonia, Norway, and Switzerland. And many of the talks about new voting systems regarded new protocols that can be deployed online, like the extension of Scantegrity to remote online use ("Remotegrity"). Presentations about these projects came from social scientists, technologists, and policymakers.

At the same time, there continue to be important questions raised from researchers about voting online, focusing largely on concerns about the security of online voting – specifically including the challenges of making online voting coercion-resistant in a practical, convincing, and usable way. These concerns fueled much discussion during the seminar, and it is clear that more research about the voting systems being currently deployed, and those proposed for use in the near future, is needed.

Concern is growing in the research community about how to maximize the impact of the considerable body of research that has accumulated in recent years. Seminar participants raised concerns about ways to improve the science of studying election technology, as well as methods to improve connections and collaborations between the scientific and policymaking communities. These issues will continue to intensify in the near future, and we hope that the discussions at this Dagstuhl seminar will fuel progress in the development of new scientific opportunities for research and dissemination, as well as closer collaboration between scientists and policymakers.

2 Table of Contents

3 Overview of Talks

3.1 Update on U.S. Internet Voting Demo Project, Information on UOCAVA Solutions Summit

David Beirne (Federal Voting Assistance Program, Arlington, US)

URL http://www.dagstuhl.de/mat/Files/11/11281/11281.BeirneDavid1.Slides.pdf

Pursuant to the Military and Overseas Voter Empowerment Act, the United States Department of Defense through its Federal Voting Assistance Program is charged with the conduct of an internet voting demonstration project for a statistically significant population.

3.2 VeriScan

Josh Benaloh (Microsoft Research – Redmond, US)

Verified Optical Scan (or VeriScan) is a voter front end that can be used to build a fully (end-to-end) verifiable election system. It allows voters to use ordinary optical scan ballots and slightly enhanced precinct optical scanners to create a verifiable tally which augments rather than replaces the traditional optical scan tally. The design is simple and familiar to voters and ensures that any discrepancy between the two tallies immediately implicates the optical scanner as malfunctioning. The benefits of full verifiability are obtained with minimal privacy risks – even in the event of complete cryptographic failure.

3.3 Revisiting individual verifiability

Sergiu Bursuc (University of Birmingham, GB)

Joint work of Bursuc, Sergiu; Grewal, Gurchetan S.; Ryan, Mark D.;
Main reference Sergiu Bursuc, Gurchetan Grewal, Mark Ryan, "Trivitas: Voters directly verifying votes," Proceedings of the VOTE-ID conference, 2011, Springer LNCS, to appear.

Individual verifiability has emerged over the last few years as a fundamental property necessary for the public take-up of E-voting systems. Roughly, it should convince each voter that his vote has been correctly handled by the voting system: by the voting machine, by the communication network, by the bulletin board, by the talliers and by any other party involved in the election. In the end, the voter should be convinced that his vote has been counted in the final tally.

However, individual verifiability in most current E-voting systems is either incomplete (it is not end-to-end: it does not cover all the path traversed by the vote) or is indirect (it relies on trusted third parties, on complex math and/or on dedicated software). It is true that these limitations are due to a tension between individual verifiability and coercion-resistance, but is it really the case that we can not to better?

We propose the notion of audit ballots, that allow the voter to track the handling of an audit vote from the voting phase and up to the counting phase, thus providing more intuitive individual verifiability. Because an audit vote is independent from the real vote of a voter, audit ballots do not compromise coercion-resistance. We show how audit ballots can be introduced in Helios, Prêt à Voter and JCJ/Civitas, without complicating the voter experience.

3.4 Attacking and fixing privacy in Helios

Veronique Cortier (INRIA – Nancy, FR)

Joint work of Cortier, Veronique; Smyth, Ben;
Main reference Veronique Cortier, Ben Smyth, "Attacking and Fixing Helios: An Analysis of Ballot Secrecy," Proceedings of the IEEE Computer Security Foundations Symposium (CSF 2011), pages 297–311, 2011.
URL http://dx.doi.org/10.1109/CSF.2011.27

Helios 2.0 is an open-source web-based end-to-end verifiable electronic voting system, suitable for use in low-coercion environments. In this talk, we analyse ballot secrecy and discover a vulnerability which allows an adversary to compromise the privacy of voters. The vulnerability exploits the absence of ballot independence in Helios and works by replaying a voter's ballot or a variant of it, the replayed ballot influences the election outcome, introducing information that can be used to violate privacy. We demonstrated the practicality of the attack by breaking privacy in a mock election using the current Helios implementation. Moreover, the feasibility of an attack is considered in the context of French legislative elections and, based upon our findings, we believe it constitutes a real threat to ballot secrecy in such settings.

We present a fix and show that our solution satisfies a formal definition of ballot secrecy using the applied pi calculus. In addition, we discuss the relationship between independence and privacy properties.

3.5 CRAVE: A Challenge Response Application to Voting Electronically

Jeremy Epstein (SRI – Arlington, US)

Internet voting is widely promoted in the U.S. as a way to improve voter turnout, especially by military and overseas voters, but security has been the primary obstacle to adoption, especially for marked ballot return. In this presentation we describe CRAVE, a variant on code voting using commercially available low-cost challenge-response devices as a means to allow accurate marked ballot return, even in the face of malware running in the voter's browser or elsewhere on her computer. The goal of CRAVE is to explore the range of user interfaces that can be used successfully by voters that improve security in the real world; it is not intended to address the full range of voting characteristics such as those addressed by cryptographic End-to-End systems.

3.6 Validation of User Models: Should e-voting machine development be driven by Murphy's Law?

Paul Gibson (Telecom – Evry, FR)

Verifying that an e-voting system works correctly requires making assumptions about the environment in which the system is used.

In particular, one must model the users of the system and validate that this model corresponds to some reality. However, from our experience in developing a novel voting interface, we have observed that such models are particularly difficult to build and validate. Through a number of iterations and experimental observations we planned to converge towards a better user model, and - as a consequence - a better user interface.

Unfortunately, our understanding of the voting system environment has been recently compromised when we considered untrusted users: those users whose behaviour cannot be trusted to follow the assumptions that we make. It appears that no matter how much one anticipates the behaviour of untrusted users, Murphy's law for user modelling rules supreme: "If your model of user behaviour can be invalidated it will be invalidated".

3.7 Secure Internet Voting on an Untrusted Platform

Rolf Haenni (Bern University of Applied Sciences, CH)

Many different electronic voting protocols have been developed during the last two decades. Most of them assume the secure platform problem to be solved.

Applying them for voting over the Internet with voters using their PCs or notebooks is therefore problematic. Malicious software installed on these devices can easily harm the integrity and secrecy of the vote. One approach to solve the secure platform problem in this context is to distribute trusted devices to the voters. We discuss the design and the properties of such a device from a practical perspective in terms of usability, security, and cost.

3.8 Security Problems in India's Electronic Voting System

J. Alex Halderman (University of Michigan, US)

Joint work of Wolchok, Scott; Wustrow, Eric; Halderman, J. Alex; Prasad, Hari K.; Kankipati, Arun; Sakhamuri, Sai Krishna; Yagati, Vasavya; and Gonggrijp, Rop
Main reference Scott Wolchok, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, Rop Gonggrijp, "Security Analysis of India's Electronic Voting Machines," Proc. 17th ACM Conference on Computer and Communications Security (CCS'10), pp. 1–14, Chicago, IL, October 2010
URL http://indiaevm.org

India uses paperless electronic voting machines (EVMs) for its state and national elections. These machines use a simple embedded system architecture that makes them considerably

different from the complex electronic voting systems found in the U.S. and Europe (where almost all prior research has focused). Despite growing suspicions of fraud, Indian authorities have never permitted a serious, independent review of the machines' security.

Hyderabad-based engineer Hari Prasad spent a year trying to convince election officials to complete such a review, but they insisted that the government-made machines were "perfect," "infallible," and "tamperproof." Then, in February 2010, an anonymous source gave him access to one of the machines for study. E-voting researchers J. Alex Halderman from the University of Michigan and Rop Gonggrijp from the Netherlands join him in India for the study. The team discovered that, far from being tamper-proof, the machines suffer from serious weaknesses that could be exploited to alter national election results.

Months of hot debate about these findings have produced a growing consensus that India's electronic voting machines should be scrapped, as well as nascent efforts to create a better system. There have also been more disturbing developments: Prasad was arrested and jailed in August by authorities demanding to know the identity of the anonymous source.

He has since been released on bail, and received the Electronic Frontier Foundation's Pioneer Award for his work.

In this talk, Halderman will describe the design and motivations behind India's electronic voting system, the technical problems, and the implications of the machines' security weaknesses for voting technology in India and beyond. He'll also discuss some of the formidable practical challenges that India and many other democracies face in conducting elections. Designing voting systems that provide transparency and security under these constraints presents many open problems.

3.9 Digital Democratization: Suffrage Expansion and the Decline of Political Machines in Brazil

F. Daniel Hidalgo (University of California, US)

Transitions to democracy often included institutional reforms that extended the franchise and reduced the capacity of incumbent governments to fraudulently manipulate elections. While existing studies have provided substantial insight on the broad effects of institutional reforms, there is little systematic and comparable evidence on which democratizing reforms were most consequential for political representation, as well as precise comparisons of their effects. To provide such evidence, I exploit the phased adoption of electronic voting in Brazil, a reform that I find increased the effective franchise in legislative elections by about 33% and eliminated fraud in the vote counting process.

Because the reform was initially implemented in municipalities with an electorate over an arbitrary threshold, I study its effects using a "regression discontinuity" design, which ensures a high degree of internal validity. The two distinct effects of electronic voting - the enfranchisement of illiterates and other low information voters and the elimination of fraud - had consequences for the composition of the national legislature. Against the predictions of recent economic models of democratization, I find that the enfranchisement of illiterates and other low information voters caused a small increase in the vote shares of right-wing candidates. More importantly, newly enfranchised voters were dramatically more likely to cast a "party list" or partisan ballot as opposed to a personal or candidate ballot, which

benefitted Brazil's more programmatic and ideologically coherent parties. In states with hegemonic conservative parties, I find that the introduction of electronic voting induced a roughly 20 percentage point swing against "political machine" candidates, which I attribute to the elimination of fraud. In these states, new voting technology resulted in a sharp increase in political competition and harmed right-of-center candidates.

Overall, I argue that the most important consequences of the reform was the strengthening of Brazil's major parties and a weakening of dominant subnational conservative political machines.

3.10 Internet Voting in the United States

Candice Hoke (Cleveland State University, US)

Within the United States, 60% of the States have approved voting methods for overseas civilian and military voters that utilize the public internet for the return of voted (marked) ballots. While most States require voting systems to undergo independent testing of their vendors' claims of security, voter privacy, accuracy and resiliency, the States have generally not conceptualized these internet- facing systems as voting systems. The internet voting systems have thus escaped independent certification reviews.

The largely unregulated free market approach permits vendors to overstate the security, privacy and other attributes of these systems, and to conceal flaws, needed mitigations, and defense in depth security steps needed for secure operation of the systems. The Federal agency's advocacy of all-electronic elections before the technology was proven to have reached high assurance standards has played a major, regrettable role.

3.11 An Efficient Implementation of a Highly Sound Voter Verification Technique on a Smart Card and its Application to Internet Voting

Rui Joaquim (Polytechnic Institute of Lisbon/INESC-ID – Lisboa, PT)

Joint work of Joaquim, Rui; Ribeiro, Carlos; Ferreira, Paulo
Main reference Rui Joaquim, Carlos Ribeiro, Paulo Ferreira, "Towards Trustworthy Internet Elections," INESC-ID Tec. Rep. 9/2011, February 2011.
URL http://www.inesc-id.pt/ficheiros/publicacoes/7135.pdf

Uncontrolled Internet voting is the most challenging scenario for electronic voting as the voter uses an insecure/uncontrolled platform to vote. We present a solution to the insecure platform problem of Internet voting using a tamper resistant device (e.g. smart card). However, we do not just move the trust assumptions from the PC to the tamper resistant device, we have completely removed all trust assumptions on the election integrity from both the PC and the tamper resistant device by adding a highly sound voter verification technique to the vote encryption [1]. Moreover, our system also uses a code voting approach to communicate the voter's choice to the tamper resistant device, which enables the voter to vote privately even when using public computers, e.g. computers at a public library or at a cybercafé.

References

1 Rui Joaquim and Carlos Ribeiro. *An Efficient and Highly Sound Voter Verification Technique and its Implementation.* Vote-ID 2011, Tallinn, Estonia, 2011. To appear.

3.12 Encoding complex ballots

Hugo Jonker (University of Luxembourg, LU)

Various end-to-end verifiable systems have been proposed in recent years. These systems often rely on a predefined way of filling in the ballot. However, election systems vary from country to country, and sometimes from region to region. We illustrate the problem by means of two non-trivial systems (Luxembourgian general elections and German bundesland elections). In both systems, voters not only get to express multiple benefits, but can vote multiple times for the same candidate. In addition, there are shortcut options (voting for all members of one party).

We outline one approach to reconcile the existing voter experience (which may be enshrined in law) with the Prêt à Voter system.

3.13 How to Store Some Secrets

Reto Koenig (Bern University of Applied Sciences, CH)

The key idea of coercion-resistant electronic voting protocols is to allow voters to deceive the adversary with faked credentials. Keeping up the deception under all possible circumstances requires the voter to remember multiple high-entropy credentials. This obviously states a hard problem for the human brain. We introduce the concept of a secret storing system, which allows users to conveniently store multiple high-entropy credentials with low-entropy passphrases in one single storage. Both the credentials and the passphrases can be chosen freely and independently. We propose a concrete realisation of such a system using interpolation polynomials over prime fields.

3.14 Election Observation of New Voting Technologies

Robert Krimmer (OSCE – Warszaw, PL)

The use of information and communication technologies in elections has expanded considerably in recent years. This development has however not been uniform across the OSCE. A growing number of participating States have introduced New Voting Technologies (NVT) or are considering it, while others have stopped and returned to traditional voting methods. NVT have raised questions about the compliance of these new electronic systems with OSCE commitments and international obligations for democratic elections. As a result, a number of international organizations and institutions, including ODIHR, have been paying increased attention to this issue.

Transparency and observation are cornerstones of OSCE election-related commitments. They are necessary to ensure that votes are cast by secret ballot or by equivalent free voting

procedure, and that they are counted and reported honestly with the official results made public.

However, NVT poses new challenges to the traditional and broadly accepted concepts of transparency and accountability of election processes to election administrators, voters and election observers. Hence, concerns about security and secrecy of the ballot as well as the reliability of electronic voting have become the subject of public debate in a number of countries, thereby influencing public perceptions and confidence in elections in general. NVTs have so far not reached the same level of universal acceptance, trust and confidence as paper voting. But NVT can help offer additional functionalities to elections that paper ballots cannot, for instance in cases when counting is complicated due a large numbers of concurrent elections, voting for the blind, etc.

Observing elections using NVT is a challenge. Electronic events are more difficult to observe because specialized technical skills are needed. Electronic voting consists of technological components that are not readily nor easily understood by the average observer. There is a need for an ODIHR approach to NVT in a methodological framework that dovetails with ODIHR overall methodological approach to election observation. It should also support election advisers in their daily work regarding developments with regards to NVT.

3.15 Verification, Security, and Voter Understanding

Morgan Llewellyn (IMT – Lucca, IT)

Joint work of Culnane, Chris; Heather, James; Llewellyn, Morgan; Schneider, Steve; Srinivasan, Sriram; Xia, Zhe (Joson)

Currently, a variety of voting schemes seek to increase voter confidence by allowing voters to verify that their vote has been recorded. Each of these voting systems assume that the gain in confidence from verifying their vote is greater than any potential loss of confidence resulting from voter beliefs that the verification process may reveal vote choice. Why this assumption may be natural to computer scientists, it is possible that many voters do not understand event basic ballot security features. It is in this context that we test individual understanding of random candidate ordering in a Prêt à Voter style ballot form.

Individual understanding of the ballot form was done through a series of experiments conducted at the University of Surrey. The goal of the experiments was to test individual understanding of the security features provided by randomized candidate ordering. Results indicate that a clear majority of participants understand the security features of randomized candidate ordering. However, results also reveal that some individuals did not fully understand the ballot security features and highlight the potential for attacks on user confidence resulting from large N.

3.16 The Limits of Theory: Assumptions on Which We Base Voting Protocol Security

Tal Moran (Harvard University, US)

One of the contributions of computer science theory to voting security is the notion of "security reductions": the idea that we can reduce the security of a complex system to the security of simpler components. This makes practical verification of security a more tractable problem: if we can prove a security reduction, it is enough that we check the individual components to be convinced that the system as a whole is secure. At the end of the day, however, we are always left with security "axioms": basic assumptions that we cannot reduce further on which the security of the system relies.

When we evaluate and compare voting systems, in addition to looking at what they provide, we should also be thinking about the basic assumptions they rely on.

I'll describe some of the common assumptions on which we base end-to-end verifiable voting systems and discuss their relation to reality.

3.17 Running mixnet-based elections with Helios

Olivier Pereira (UC Louvain-la-Neuve, BE)

Joint work of Bulens, Philippe; Giry, Damien; Pereira, Olivier
Main reference Philippe Bulens, Damien Giry, Olivier Pereira, "Running Mixnet-Based Elections with Helios," Electronic Voting Technology Workshop/ Workshop on Trustworthy Elections (EVT/WOTE '11), 2011.
URL http://www.usenix.org/event/evtwote11/tech/

The Helios voting system is an open-audit web-based voting system that has been used by various institutions in real-stake elections during the last few years. While targeting the simplicity of the election workflow, the homomorphic tallying process used in Helios limits its suitability for many elections (large number of candidates, specific ballot filling rules, . . .).

We present a variant of Helios that allows an efficient mixnet-based tallying procedure, and document the various choices we made in terms of election workflow and algorithm selection. In particular, we propose a modified version the TDH2 scheme of Shoup and Gennaro that we found particularly suitable for the encryption of the ballots.

Our Helios variant has been tested in two multi-thousand voter elections. The lessons taken from the first of these elections motivated some changes into our procedure, which have been successfully experimented during the second election. Voter survey data are also presented.

3.18 Wombat in the wild

Ben Riva (Tel Aviv University, IL)

We present a new electronic voting system called Wombat. Wombat is designed to be similar to the current Israeli paper based elections and it combines a paper based voting system with an electronic one, in a way that both systems complete each other.

We show the highlights of the protocol, briefly describe its implementation, and talk about a pilot we ran in a student council election with over 2000 voters.

3.19 Prêt à Voter with Confirmation Codes

Peter Y. A. Ryan (University of Luxembourg, LU)

Main reference to appear in the proceedings of EVT/WOTE 2011

A scheme is presented in which a Pretty Good Democracy style confirmation code mechanism is incorporated into Prêt à Voter. The idea is to provide voters with an immediate, easy to use confirmation at the time of casting of the correct registration of their receipt on the Web Bulletin Board. As with PGD, the registration and revelation of the confirmation code is performed by a threshold set of Trustees. Verification of the registration of the vote is now part of the vote casting and therefore more immediate and convenient for the voters.

The scheme presented here is thus more convenient while maintaining the level of verifiability of conventional Prêt à Voter. It also means that we are less reliant on the diligence of voters in later performing checks on the Bulletin Board. It seems probable that this confirmation code mechanism will provide voters with greater confidence that their vote will be accurately tallied.

3.20 Focus Groups Study on Prêt à Voter

Steve Schneider (University of Surrey, GB)

Joint work of Schneider, Steve; Llewellyn, Morgan; Culnane, Chris; Heather, James; Srinivasan, Sriramkrishnan; Xia, Zhe
Main reference Steve Schneider, Morgan Llewellyn, Chris Culnane, James Heather, Sriramkrishnan Srinivasan, Zhe Xia, "Focus Groups Study on Prêt à Voter 1.0," Proceedings of RE-Vote: International Workshop on Requirements Engineering for Electronic Voting Systems Trento, Italy, 2011.
URL http://www.computing.surrey.ac.uk/personal/st/S.Schneider/papers/2011/RE-Vote11.pdf

This presentation discussed the findings of a series of four focus group sessions carried out in the UK on a variant of the original Prê tà Voter verifiable voting system prototype implementation. The aim of these sessions was to investigate users' ability to use the system, to discover any inadequacies of the system, and to gauge the participants' understanding of its security mechanisms. Participants were asked to use the system to cast a vote, to audit their ballot forms and to confirm online that their vote had been received.

The groups also discussed general issues around security in election systems.

While voters were able to cast their votes reliably, some displayed less understanding of the security procedures they were required to carry out.

3.21 Some ideas about receipt-free cast-as-intended Internet voting for preferential elections

Vanessa Teague (The University of Melbourne, AU)

We discuss whether a remote electronic voting system might provide both strong privacy properties and strong verification that the vote was cast as intended.

We speculate on some weaker alternatives to full receipt freeness and how they might be achieved. For example, it seems reasonable to expect that the voter cannot produce a proof that can be sent to a remote party who was unable to tap the voter's communications. We compare the approach with others that achieve similar objectives based on credentials or codes. Our primary motivation is the difficulty of using either the Juels- Catalano-Jakobsson method or voting codes for preferential voting.

3.22 Internet Voting in Estonia

Alexander Trechsel (European University Institute, IT)

Joint work of Trechsel, Alexander; Vassil, Kristjan

Recent years has seen an increasing interest in Internet voting from the point of view of political scientists as well as from the perspective of policy makers. Some have argued that the introduction of e-voting boosts electoral participation by bringing down the barriers hindering electoral turnout. Others have kept a more pessimistic view, claiming that e-voting affects only those few who are highly engaged in politics already. This study aims to shed light on the topics beyond this debate. In particular, our objective is to analyze the determinants that lead some citizens to opt for e-voting and others for traditional means of participation. We ask the question of who is voting online and how can we explain the choice of the voting channel? On the basis of five e-enabled elections in Estonia we demonstrate that the introduction of internet voting has a modest effect on aggregate levels of turnout. On the individual level we find that choosing to vote online is associated with trust toward e-voting system, as well as higher levels of computer literacy. Additionally we find that the language cleavage remains an important predictor of internet voting in Estonia. Interestingly, as time has passed since the first e-enabled elections we find that traditional determinants of e-voting, such as age, gender, urban residence, income, etc, gradually loose their power.

3.23 What happened in Sarasota?

Dan Wallach (Rice University, US)

URL http://www.cs.rice.edu/~dwallach/pub/sarasota07.pdf

The November 2006 race for Florida's 13th Congressional District resulted in a 369 vote margin of victory for the winning candidate with more than 18,000 undervotes recorded

on the ES&S iVotronic touch-screen voting machines used in Sarasota County. This talk summarizes what happened, what theories might explain it, and what steps were taken at the time and afterward to understand the mystery.

3.24 Swiss Elections to the National Council: First trials with e-voting in elections at federal level

Anina Weber (Federal Chancellery – Bern, CH)

Main reference Anina Weber, Geo Taglionoi, "Swiss Elections to the National Council: First trials with e-voting in elections at federal level," Dagstuhl Preprint Archive, arXiv:1109.2489v2 [cs.CY]
URL http://arxiv.org/abs/1109.2489v2

On October 23rd 2011, around 22,000 voters will be authorized to cast their votes electronically in occasion of the elections to the National Council. These are the first trials ever with e-voting in elections at federal level in Switzerland. Four cantons are going to conduct trials with this new channel. Only Swiss voters living abroad will be authorized to participate.

The Swiss Confederation pursues the long term goal of the introduction of e-voting as a third, complementary voting method in addition to voting in person at the polling station and postal voting.

3.25 Verifiable voting with everlasting privacy

Jeroen van de Graaf (Federal University of Minas Gerais, Brazil, BR)

Main reference van de Graaf, Jeroen, "Voting with unconditional privacy: CFSY for booth voting," unpublished manuscript
URL http://eprint.iacr.org/2009/574

We study the Cramer, Franklin, Schoenmaker and Yung internet voting protocol for the booth setting. In this protocol, so called Pedersen commitments are used to define an unconditionally hiding commitment scheme. Because of its homomorphic properties, they are particularly suited for voting protocols with unconditional privacy.

In fact, a survey shows that almost all these protocols use, or could benefit from, these commitments. Though not novel cryptographically speaking, the protocol presented is interesting from a voting perspective, because it is simple enough to be understood by non-cryptographers, yet has many desirable properties, such as unconditional privacy, correctness under the discrete log assumption, individual and universal verifiability, and (optionally) ballot casting assurance.

In addition, we discuss interesting relations to and/or simplifications, of several other protocols, such as the booth voting protocol of Moran and Naor, SplitBallot, MarkPledge and Scratch & Vote.

4 Panel Discussions

4.1 What are the obstacles to improving the integrity of election systems?

This panel discussion was held the first afternoon of the seminar. Moderated by Michael Alvarez, participants in the discussion were David Beirne, Candice Hoke, Robert Krimmer and Alexander Trechsel.

Participants

- Michael Alvarez
CalTech – Pasadena, US
- David Beirne
Federal Voting Assistance Programm, Arlington, US
- Jonathan Ben-Nun
Tel Aviv University, IL
- Josh Benaloh
Microsoft Res. – Redmond, US
- Sergiu Bursuc
University of Birmingham, GB
- Michel Chevallier
Republique et Canton de Genéve, CH
- Veronique Cortier
INRIA – Nancy, FR
- Christopher Culnane
University of Surrey, GB
- Stéphanie Delaune
ENS – Cachan, FR
- Jeremy Epstein
SRI – Arlington, US
- Paul Gibson
Telecom – Evry, FR
- Rop Gonggrijp
Amsterdam, NL
- Rolf Haenni
Bern University of Applied Sciences, CH
- J. Alex Halderman
University of Michigan, US
- James Heather
University of Surrey, GB
- F. Daniel Hidalgo
University of California, US
- Candice Hoke
Cleveland State University – Cleveland, US
- Rui Joaquim
Polytechnic Institute of Lisbon/INESC-ID – Lisboa, PT
- Hugo Jonker
University of Luxembourg, LU
- Reto König
Bern University of Applied Sciences, CH
- Steve Kremer
ENS – Cachan, FR
- Robert Krimmer
OSCE - Warszaw, PL
- Manuel J. Kripp
E-Voting.CC – Viennna, AT
- Miroslaw Kutylowski
Wroclaw University of Technology, PL
- Gabriele Lenzini
University of Luxembourg, LU
- Helger Lipmaa
Cybernetica AS, EE
- Morgan Llewellyn
IMT – Lucca, IT
- Symeon Meichanetzoglou
University of Luxembourg, LU
- Tal Moran
Harvard University, US
- Maina Olembo
TU Darmstadt, DE
- Olivier Pereira
UC Louvain-la-Neuve, BE
- Ben Riva
Tel Aviv University, IL
- Mark D. Ryan
University of Birmingham, GB
- Peter Y. A. Ryan
University of Luxembourg, LU
- Steve Schneider
University of Surrey, GB
- Vanessa Teague
The University of Melbourne, AU
- Jacques Traore
Orange Labs – Caen, FR
- Alexander Trechsel
European University Institute, IT
- Jeroen van de Graaf
Federal University of Minas Gerais, Brazil, BR
- Kristjan Vassil
European University Institute, IT
- Dan Wallach
Rice University, US
- Anina Weber
Federal Chancellery – Bern, CH
- Douglas Wikström
KTH Stockholm, SE
- Filip Zagórski
George Washington Univ., US
- Xia Zhe
University of Surrey, GB

Report from Dagstuhl Seminar 11291

Mathematical and Computational Foundations of Learning Theory

Edited by

Matthias Hein[1], Gabor Lugosi[2], Lorenzo Rosasco[3], and Steve Smale[4]

1 **Universität des Saarlandes, DE,** hein@cs.uni-sb.de
2 **Univ. Pompeu Fabra – Barcelona, ES,** gabor.lugosi@gmail.com
3 **MIT – Cambridge, US, and IIT, Italy,** lrosasco@mit.edu
4 **City University – Hong Kong, CN,** smale@cityu.edu.hk

Abstract

The main goal of the seminar "Mathematical and Computational Foundations of Learning Theory" was to bring together experts from computer science, mathematics and statistics to discuss the state of the art in machine learning broadly construed and identify and formulate the key challenges in learning which have to be addressed in the future. This Dagstuhl seminar was one of the first meetings to cover the full broad range of facets of modern learning theory. The meeting was very successful and all participants agreed that such a meeting should take place on a regular basis.

Seminar 17.–22. July, 2011 – www.dagstuhl.de/11291
1998 ACM Subject Classification G.1.2 Approximation, G.1.6 Optimization, G.3 Probability and Statistics, I.5 Pattern Recognition, I.2.6 Learning
Keywords and phrases learning theory, machine learning, sparsity, high-dimensional geometry, manifold learning, online learning
Digital Object Identifier 10.4230/DagRep.1.7.53

1 Executive Summary

Matthias Hein
Gabor Lugosi
Lorenzo Rosasco
Steve Smale

The study of learning is at the very core of the problem of intelligence both in humans and machines. We have witnessed an exciting success story of machine learning in recent years. Among other examples, we now have cars that detect pedestrians, and smart-phones that can be controlled simply by our voices. Indeed, aside from the increase in computational power and availability of large amount of data, the key to these successes has been the development of efficient learning algorithms based on solid theoretical foundations. As the science and engineering of learning move forward to understand and solve richer and more articulated classes of problems, broadening the mathematical and computational foundations of learning becomes essential for future achievements.

Mathematical and Computational Foundations of Learning Theory, *Dagstuhl Reports*, Vol. 1, Issue 7, pp. 53–69
Editors: Matthias Hein, Gabor Lugosi, Lorenzo Rosasco, and Steve Smale
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The main goal of our seminar was to account for the newest developments in the field of learning theory and machine learning as well as to indicate challenges for the future. This seminar was in the same spirit of two very successful conferences titled "Mathematical Foundations of Learning Theory", organized in 2004 in Barcelona and 2006 in Paris. The seminar brought together leading researchers from computer science and mathematics to discuss the state of the art in learning and generate synergy effects between the different usually disconnected communities. This Dagstuhl seminar has been the first to cover the full range of facets of modern learning theory.

The seminar has focused on three main topics, while trying to keep a broader view on all recent advances. The three main topics were: 1) the role of sparsity in learning, 2) the role of geometry in learning, and 3) sequential learning and game theory. Experts in each field gave tutorials on each topic, covering basic concepts as well as recent results.

The meeting was hold in a very informal and stimulating atmosphere. The participants all agreed that such a seminar should be come a regular meeting.

Acknowledgements. We thank Annette Beyer and Claudia Thiele for their continuous support and help in organizing this workshop. Moreover, we would like to thank the staff at Schloss Dagstuhl for making this seminar such a remarkably enjoyable event. Special thanks go to Elisabeth Chaverdian for her wonderful piano concert with excerpts from her current program of the works of Liszt.

2 Table of Contents

3 Overview of Talks

The seminar has been structured to have in the first part of the meeting three segments covering the main topics listed in the previous section. Each segment has been introduced by a tutorial on the corresponding topic. Each tutorial has been 45 minutes long while we kept other contributions to 30 minutes. The tutorials were given by Vladimir Koltchinskii (sparsity in learning), Steve Smale (geometry in learning) and Nicolo Cesa Bianchi (game theory and sequential prediction).

3.1 Toward understanding (more) complex data. Graph Laplacians on manifolds with singularities and boundaries

Misha Belkin (Ohio State University, US)

Joint work of Qichao Que, Yusu Wang and Xueyuan Zhou

In this talk I will discuss our recent work on understanding geometry of the space using graph Laplacians. In particular, I will talk about how singularities and boundaries of the space change the behavior of the limiting Laplace operator, a phenomenon somewhat reminiscent of the Gibbs effect in Fourier analysis.

3.2 New (and old) estimators for the mean

Sébastien Bubeck (Universitat Autonoma de Barcelona, ES)

In this talk we discuss the basic problem of estimating the mean of a distribution based on an i.i.d sequence of random variables from this distribution. For subgaussian distributions the empirical mean estimator has all the guarantees that one could hope for: it has exponential tails, it is easy to update with a new observation, and it does not require any parameter tuning. Unfortunately for distributions with only a finite variance, the empirical mean has heavy tails (polynomial size). We discuss here three alternatives, the truncated empirical mean, the median of means, and Catoni's estimator. These three estimators has exponential tails for distributions with finite variances, but each has different advantages and disadvantages regarding computational complexity and parameters tuning.

3.3 Context sensitive information: Model validation by information theory

Joachim M. Buhmann (ETH Zürich, CH)

Joint work of A. Busetto, M. Chehreghani, M. Frank, A. Streich

Model selection in pattern recognition requires (i) to specify a suitable cost function for the data interpretation and (ii) to control the degrees of freedom depending on the noise level in the data. We advocate an information theoretic perspective where the uncertainty in the measurements quantizes the solution space of the underlying optimization problem, thereby adaptively regularizing the cost function. A pattern recognition model, which can tolerate a higher level of fluctuations in the measurements than alternative models, is considered to be superior provided that the solution is equally informative. The optimal tradeoff between "informativeness" and "robustness" is quantified by the approximation capacity of the selected cost function.

Empirical evidence for this model selection concept is provided by cluster validation in computer security, i.e., multilabel clustering of Boolean data for role based access control, but also in high dimensional Gaussian mixture models and the analysis of microarray data. The principle also allows us to rank different spectral clustering models w.r.t. information content. Furthermore, the approximation capacity of the SVD cost function suggests an optimal cutoff value for the SVD spectrum.

3.4 Active Learning and Adaptive Sensing for Sparse Signal Estimation and Testing

Rui M. Castro (TU Eindhoven, NL)

Joint work of Jarvis Haupt and Robert Nowak

Many traditional approaches to statistical inference and machine learning are passive, in the sense that all data are passively collected prior to analysis. However, in many practical scenarios it is possible to adjust the data collection process based on information gleaned from previous observations, closing the loop between data analysis and acquisition. Inference under such scenarios is often referred to as active learning, adaptive sensing, or inference using sequential experimental designs. In this talk I'll focus in particular on estimation and testing problems when the objects of interest are sparse vectors. I'll present a simple but powerful adaptive sensing procedure - Distilled Sensing - which is highly effective for detection and estimation of high-dimensional sparse signals in noise. Large-sample analysis shows that this procedure provably outperforms the best possible inference methods based on non-adaptive data collection methods, allowing for both detection and estimation of extremely weak signals, imperceptible without adaptive sensing. Furthermore, it can be shown that this procedure is essentially optimal for a wide range of scenarios, meaning no other adaptive sensing procedure can yield a significant performance improvement.

3.5 The Game-Theoretic Approach to Machine Learning and Adaptation

Nicoló Cesa-Bianchi (Universitá di Milano, IT)

Joint work of Ohard Shamir

In the first part of the talk, we trace the roots of the game-theoretic approach in learning theory mentioning some of the key results in prediction with expert advice and online learning. In the second part, we describe the first computationally efficient online algorithm for collaborative filtering with norm-constrained matrices. The algorithm combines "random playout" and randomized rounding of loss subgradients.

3.6 On Stability and Bootstrap of Support Vector Machines

Andreas Christmann (Universität Bayreuth, DE)

Joint work of Robert Hable, Ingo Steinwart, and Arnout Van Messem

Support Vector Machines (SVMs) play an important role in statistical machine learning. The talk will focus on some recent results on SVMs: modeling heteroscedasticity by SVMs, a consistency result of SVMs for dependent data, statistical stability (=robustness) of SVMs, and stability of bootstrap estimators of SVMs.

3.7 Nonlinear Eigenproblems in Machine Learning

Matthias Hein (Universität des Saarlandes , DE)

Many problems in data analysis can be formulated as (generalized) eigenproblems. In this work I discuss nonlinear eigenproblems, which allow extended modeling freedom compared to linear eigenproblems in particular concerning robustness and sparsity. After an introduction of the framework and the discussion of an efficient generalization of the inverse power method, two examples of nonlinear eigenproblems are discussed in more detail: the tight relaxation of a large family of balanced graph cuts based on the nonlinear 1-graph Laplacian and sparse PCA.

3.8 Well localized frames, representation of function spaces, and heat kernel estimates

Gerard Kerkyacharian (University Paris-Diderot, FR)

Joint work of T. Coulhon and P.Petrushev

Since during the last twenty years, wavelet theory has proved to be a very useful tool for theoretical purposes as well as for applications, in this talk, we will revisit and provide an extension of this theory in a general geometric framework. Our object here, will be a metric space (M, ρ) equipped with a positive Radon measure, such that (M, ρ, μ) is a homogeneous space in the sense of Harmonic Analysis (there exists $d > 0$,which plays the role of a dimension, such that for all $x \in M$, and $r > 0$, $\mu(B(x, 2r)) \leq 2^d \mu(B(x, r))$).
Moreover, the geometry of the space is related to a positive self-adjoint operator L and to the associated semi-group e^{-tL}. We suppose in addition that e^{-tL} is markovian. Here is the main hypothesis : e^{-tL} is a kernel operator, and this kernel $P_t(x, y)$ has the following Gaussian estimate : for all x, y in M, $t > 0$,

$$P_t(x, y) \leq \frac{C_2\, e^{-c\,\frac{\rho^2(x,y)}{t}}}{\sqrt{\mu(B(x, \sqrt{t}))\mu(B(y, \sqrt{t}))}}.$$

It is well known that this property is verified for the Laplacian of a Riemannian manifold with non negative Ricci curvature, for Nilpotent Lie Groups, compact Lie Groups and their homogeneous spaces The Besov spaces $B^s_{p,q}$, $0 < s$, $1 \leq p \leq \infty$, $0 \leq q \leq \infty$ could be defined in several equivalent way: as spaces of approximation, or interpolations spaces. The main results are the following :

1. One can build an efficient Littlewood-Paley decomposition and give a charaterization of the Besov spaces.
2. It is possible to build localized frames in duality : $\psi_{j,\xi}, \tilde{\psi}_{j,\xi}$, $j \in \mathbb{N}$, $\xi \in A_j$
   a.
   $$\forall f \in L^p,\ 1 \leq p \leq \infty, \quad f(x) = \sum_j \sum_{\xi \in A_j} \langle f, \psi_{j,\xi} \rangle \tilde{\psi}_{j,\xi}$$
   b.
   $$\exists c > 0,\ \forall j \in \mathbb{N},\ \xi \in A_j, \qquad \psi_{j,\xi} \text{ and } \tilde{\psi}_{j,\xi} \in \Sigma_{cb^j}.$$
   c. and we have the following characterization:
   $$f \in B^s_{p,q} \Leftrightarrow \forall\, j \in \mathbb{N}, \Big(\sum_{\xi \in A_j} |\langle f, \psi_{j,\xi} \rangle|^p \|\tilde{\psi}_{j,\xi}\|_p \Big)^{\frac{1}{p}} = \alpha_j 2^{-js}, \qquad \alpha \in l_q$$
   (with the usual modification for $p = \infty$).

3.9 Classifying Clustering Schemes

Facundo Mémoli (Stanford University, US)

Many clustering schemes are defined by optimizing an objective function defined on the partitions of the underlying set of a finite metric space. In this paper, we construct a framework for studying what happens when we instead impose various structural conditions on the clustering schemes, under the general heading of functoriality. Functoriality refers to the idea that one should be able to compare the results of clustering algorithms as one varies the data set, for example by adding points or by applying functions to it. We show that within this framework, one can prove a theorem analogous to one of J. Kleinberg, in which for example one obtains an existence and uniqueness theorem instead of a non-existence result. We obtain a full classification of all clustering schemes satisfying a condition we refer to as excisiveness. The classification can be changed by varying the notion of maps of finite metric spaces. The conditions occur naturally when one considers clustering as the statistical version of the geometric notion of connected components. By varying the degree of functoriality that one requires from the schemes it is possible to construct richer families of clustering schemes that exhibit sensitivity to density.

3.10 Testing the Manifold Hypothesis

Hari Narayanan (MIT – Cambridge, US)

Increasingly, we are confronted with very high dimensional data sets in areas like computational biology and medical imaging. As a result, methods of avoiding the curse of dimensionality have come to the forefront of machine learning research. One approach, which relies on exploiting the geometry of the data, has evolved into a subfield called manifold learning.

The underlying hypothesis of this field is that data tend to lie near a low dimensional submanifold, due to constraints that limit the degrees of freedom of the process generating them. This has been empirically observed to be the case, for example, in speech and video data. Although there are many widely used algorithms which assume this hypothesis, the basic question of testing this hypothesis is poorly understood.

I will discuss forthcoming work with Charles Fefferman and Sanjoy Mitter towards developing a provably correct, efficient algorithm to test this hypothesis from random data.

3.11 Active Clustering

Rob Nowak (University of Wisconsin – Madison, US)

Joint work of Brian Eriksson, Gautam Dasarathy, and Aarti Singh

Hierarchical clustering is a common tool used in a broad range of scientific applications. However, in many problems it may be expensive to obtain or compute similarities between the items to be clustered. If we choose to randomly subsample similarities, we cannot hope to recover small clusters with size that is sublinear in the number of objects. This necessitates an active procedure that sequentially selects which similarities to obtain in an adaptive fashion. I will describe such an active clustering procedure that generates a hierarchical clustering of N objects using only N log N similarities, instead of all N(N-1)/2 similarities. The method can recover all clusters of size larger than log N, even in the presence of a limited fraction of arbitrarily corrupted or noisy similarities. I will also discuss potential applications to network tomography and genomic data analysis.

3.12 Convex relaxations for Combinatorial Penalties

Guillaume Obozinski (ENS – Paris, FR)

In structured sparsity, one attempts to estimate a function which, in a appropriate parameterization, is encoded by a sparse vector; the support (or set of non-zero elements) of this sparse vector is furthermore assumed to present a type of structure which is known a priori. A common approach to the problem is to penalize implicitly or explicitly the structure of the support of the estimated parameter vector. In this talk, I will present a generic convex relaxation for a family of functions that penalize simultaneously the structure of the support through a general set function, and the L_p norm of the parameter vector for an arbitrary fixed p.

The formulation considered allows to treat in a unified framework several a priori disconnected approaches such as block-coding and submodular functions, and extend in the latter case theoretical results obtained by Bach.

3.13 A Meta-Learning Approach to the Regularized Learning - Case Study: Blood Glucose Prediction

Sergei Pereverzev (RICAM – Linz, AT)

The motivation for this research appeared in the course of the project "DIAdvisor" funded by the European Commission with the aim to improve the diabetes therapy.

The massive increase in the incidence of diabetes is now a major global healthcare challenge, and the treatment of diabetes is one of the most difficult therapies to manage, because of the difficulty in actively predicting blood glucose levels.

From the literature we know that nowadays there are mainly two approaches to predict the future blood glucose based upon the patient's current and past blood glucose values. One of them uses the time-series methodology, while another one employes artificial neural networks techniques. But time-series predictors seem to be too sensitive to gaps in the data, which may frequently appear when available blood glucose meters are used. As to neural networks predictors, they need long training periods and much more information to be set up.

Therefore, we join the "DIAdvisor" consortium with the idea to use regularized learning algorithms in predicting blood glucose. These algorithms are well understood now, and it is known that their performance essentially depends on the choice of regularization parameters and, which is even more important, on the choice of kernels generating Reproducing Kernel Hilbert Spaces, in which the regularization is performed. As it was quickly realized, in the context of blood glucose prediction these algorithmic instances cannot be a priori fixed, but need to be adjusted to each particular prediction input. Thus, a regularized learning based predictor should learn how to learn kernels and regularization parameters from the inputs. Such a predictor is constructed as a result of a process of learning to learn, or "meta-learning". In this way we have developed the Fully Adaptive Regularized Learning (FARL) approach to the blood glucose prediction.

The developed approach allows the construction of blood glucose predictors which, as it has been demonstrated in the extensive clinical trials, outperform the state-of-art algorithms. Moreover, it turns out that in the context of the blood glucose prediction the FARL-approach is more advanced than other meta-learning technologies such as k-NN ranking.

In this talk we are going to present a theoretical justification of the FARL-approach, as well as performance assessment results from clinical trials. The approach is described in the patent application EP 11163219.6 filed jointly by Austrian Academy of Sciences and Novo Nordisk A/S (Denmark).

3.14 The computational magic of the ventral stream: towards a theory?

Tomaso Poggio (MIT – Cambridge , US)

I conjecture that the sample complexity of object recognition is mostly due to geometric image transformations and that a main goal of the ventral stream – V1, V2, V4 and IT – is to learn-and-discount image transformations. The most surprising implication of the theory emerging from these assumptions is that the computational goals and detailed properties of cells in the ventral stream follow from *symmetry properties* of the visual world through a process of unsupervised correlational learning.

From the assumption of a hierarchy of areas with receptive fields of increasing size the theory predicts that the size of the receptive fields determines which transformations are learned during development and then factored out during normal processing; that the transformation represented in each area determines the tuning of the neurons in the area, independently of the statistics of natural images; and that class-specific transformations are learned and represented at the top of the ventral stream hierarchy.

Some of the main predictions of this theory-in-fieri are:

- the type of transformation that are learned from visual experience depend on the size (measured in terms of wavelength) and thus on the area (layer in the models) – assuming that the aperture size increases with layers;
- the mix of transformations learned determine the properties of the receptive fields – oriented bars in V1+V2, radial and spiral patterns in V4 up to class specific tuning in AIT (e.g. face tuned cells);
- class-specific modules – such as faces, places and possibly body areas – should exist in IT to process images of object classes.

3.15 Learning Theory: A Minimax Analysis

Alexander Rakhlin (University of Pennsylvania, USA)

Statistical Learning Theory studies the problem of estimating (learning) an unknown function given a class of hypotheses and an i.i.d. sample of data. Classical results show that combinatorial parameters (such as Vapnik-Chervonenkis and scale-sensitive dimensions) and complexity measures (such as covering numbers, Rademacher averages) govern learnability and rates of convergence. Further, it is known that learnability is closely related to the uniform Law of Large Numbers for function classes.

In contrast to the i.i.d. case, in the online learning framework the learner is faced with a sequence of data appearing at discrete time intervals, where the data is chosen by the adversary. Unlike statistical learning, where the focus has been on complexity measures, the online learning research has been predominantly algorithm-based. That is, an algorithm with a non-trivial guarantee provides a certificate of learnability.

We develop tools for analyzing learnability in the game-theoretic setting of online learning without necessarily providing a computationally feasible algorithm. We define complexity measures which capture the difficulty of learning in a sequential manner. Among these measures are analogues of Rademacher complexity, covering numbers and fat shattering dimension from statistical learning theory. These can be seen as temporal generalizations of classical results. The complexities we define also ensure uniform convergence for non-i.i.d. data, extending the Glivenko-Cantelli type results. A further generalization beyond external regret covers a vast array of known frameworks, such as internal and Phi-regret, Blackwell's Approachability, calibration of forecasters, global non-additive notions of cumulative loss, and more

3.16 Sparse Recovery and Structured Random Matrices

Holger Rauhut (Universität Bonn, DE)

Compressive sensing (sparse recovery) is a recent paradigm in signal processing and sampling theory that predicts that sparse signals can be recovered from a small number of linear and non- adaptive measurements using convex optimization or greedy algorithms. Quite remarkably, all good constructions of the so called measurement matrix known so far are

based on randomness. While Gaussian random matrices provide optimal recovery guarantees, such unstructured matrices are of limited use in applications. Indeed, structure often allows to have fast matrix vector multiplies. This is crucial in order to speed up recovery algorithms and to deal with large scale problems. The talk discusses models of structured random matrices that are useful in certain applications, and presents corresponding recovery guarantees. An important type of structured random matrix arises in connection with sampling sparse expansions in terms of bounded orthogonal systems (such as the Fourier system). The second type of structured random matrices to be discussed are partial random circulant matrices, that is, from convolution. In particular, we present recent results with J. Romberg and J. Tropp on the restricted isometry property of such matrices. The third type of measurement matrices arises in kernel-based semisupervised learning, for which preliminary results are reported.

3.17 Nonparametric Bandits with Covariates v.2.0

Philippe Rigollet (Princeton University, US)

Joint work of Vianney Perchet (Univ. Paris 7)

We consider a multi-armed bandit problem in a setting where each arm produces a noisy reward realization which depends on an observable random covariate. As opposed to the traditional static multi-armed bandit problem, this setting allows for dynamically changing rewards that better describe applications where side information is available. We adopt a nonparametric model where the expected rewards are smooth functions of the covariate and where the hardness of the problem is captured by a margin parameter. To maximize the expected cumulative reward, we introduced in Rigollet and Zeevi (2010) a policy based on a fixed partitioning of the covariate space. While it achieved optimal regret for a certain class of "difficult" problems, it failed to adapt the the complexity of "easy" problems. In this second attempt, we rely on a dynamic, adaptive partition that is implemented in a policy called Adaptively Binned Successive Elimination (abse) . It is proved to achieve optimal bounds on the regret an reveals an interesting phenomenon: the effect of the exploration vs. exploitation dilemma is washed away by the difficulty of nonparametric estimation. To derive these bounds, we developed a modification of the Successive Elimination policy in the static framework that achieves the sharper regret bounds necessary to prove our main theorem.

3.18 Nonparametric Sparsity Based Regularization

Lorenzo Rosasco (MIT – Cambridge,US)

In this work we are interested in the problems of supervised learning and variable selection when the input-output dependence is described by a nonlinear function depending on a few variables. Our goal is to consider a sparse nonparametric model, hence avoiding linear or additive models. The key idea is to measure the importance of each variable in the model

using partial derivatives. Based on this intuition we propose and study a new regularizer and a corresponding least squares regularization scheme. Using concepts and results from the theory of reproducing kernel Hilbert spaces and proximal methods, we show that the proposed learning algorithm corresponds to a minimization problem which can be provably solved by an iterative procedure. The consistency properties of the obtained estimator are studied both in terms of prediction and selection performance.

3.19 Learnability Beyond Uniform Convergence

Shai Shalev-Shwartz (The Hebrew University of Jerusalem, IL)

The problem of characterizing learnability is the most basic question of statistical learning theory. A fundamental result is that learnability is equivalent to uniform convergence of the empirical risk to the population risk, and that if a problem is learnable, it is learnable via empirical risk minimization. The equivalence of uniform convergence and learnability was formally established only in the supervised classification and regression setting. We show that in (even slightly) more complex prediction problems learnability does not imply uniform convergence. We discuss several alternative attempts to characterize learnability.

3.20 Entire Relaxation Path for Maximum Entropy Models

Yoram Singer (Google Inc. – Mountain View, US)

We describe a relaxed and generalized notion of maximum entropy problems for multinomial distributions. By introducing a simple re-parametrization we are able to derive an efficient homotopy tracking for the entire relaxation path. The end result is an algorithm that can provide optimal probabilistic estimates for any relaxation parameter using linear space and sub-linear time. We also show that the Legendre dual of the relaxed maximum entropy problem is the task of finding the maximum-likelihood estimator for an exponential distribution with L_1 regularization. Hence, our solution can be used for problems such as language modeling with sparse parameter representation.

3.21 Robust approachability with applications to regret minimization in games with partial monitoring

Gilles Stoltz (ENS – Paris, FR)

Approachability has become a standard tool in analyzing learning algorithms in the adversarial online learning setup. We first define this notion and recall Blackwell's early characterization [1, 2]. We then develop a variant of approachability for games where there

is ambiguity in the obtained reward that belongs to a set, rather than being a single vector. Using this variant we tackle the problem of approachability in games with partial monitoring and develop simple and efficient algorithms (i.e., with constant per-step complexity) for this setup, where the characterization of approachability has been obtained by Perchet [4] but came without an efficient algorithm. This talk is based on [3].

References

1 D. Blackwell. An analog of the minimax theorem for vector payoffs. *Pacific Journal of Mathematics*, 6:1–8, 1956.

2 D. Blackwell. Controlled random walks. In *Proceedings of the International Congress of Mathematicians, 1954, Amsterdam, vol. III*, pages 336–338, 1956.

3 S. Mannor, V. Perchet, and G. Stoltz. Robust approachability with applications to regret minimization in games with partial monitoring. In *Proceedings of the Twenty-Fourth Annual Conference on Learning Theory (COLT'11)*. Omnipress, 2011.

4 V. Perchet. Internal regret with partial monitoring calibration-based optimal algorithms. *Journal of Machine Learning Research*, 12(Jun):1893–1921, 2011.

3.22 The Lasso, correlated design, and improved oracle inequalities

Sara van de Geer (ETH Zürich, CH)

We study high-dimensional linear models and the l_1-penalized least squares estimator, also known as the Lasso estimator. In literature, oracle inequalities have been derived under restricted eigenvalue or compatibility conditions. In this paper, we complement this with entropy conditions which allow one to improve the dual norm bound, and demonstrate how this leads to new oracle inequalities. The new oracle inequalities show that a smaller choice for the tuning parameter and a trade-off between l_1-norms and small compatibility constants are possible. This implies, in particular for correlated design, improved bounds for the prediction error of the Lasso estimator as compared to the methods based on restricted eigenvalue or compatibility conditions only.

3.23 Dictionary learning: theme and variations

Alessandro Verri (University of Genova, IT)

In this talk i will illustrate our recent work on dictionary learning. The motivation of our work is rooted in the typical setting of biomedical imaging in which image annotation is expensive, while unlabeled or weakly labeled data abound. Starting from a rather conventional approach i discuss several developments including a scheme in which the analysis matrix is learnt during training and a scheme in which slowness plays a role in enforcing sparsity in the encoding stage.

3.24 Phase-transition in the family of p-resistances

Ulrike von Luxburg (Universität Hamburg

We study the family of p-resistances on graphs for $p \geq 1$. This family generalizes the standard resistance distance. We prove that for any fixed graph, for $p = 1$ the p-resistance coincides with the shortest path distance, for $p = 2$ it coincides with the standard resistance distance, and for $p \to \infty$ it converges to the inverse of the minimal s-t-cut in the graph. Secondly, we consider the special case of random geometric graphs (such as k-nearest neighbor graphs) when the number n of vertices in the graph tends to infinity. We prove that an interesting phase-transition takes place. There exists a critical threshold p^* such that if $p < p^*$, then the p-resistance depends on meaningful global properties of the graph, whereas if $p > p^*$, it only depends on trivial local quantities and does not convey any useful information. We can explicitly compute the critical value: $p^* = 1 + 1/(d-1)$ where d is the dimension of the underlying space. We also relate our findings to Laplacian regularization and suggest to use q-Laplacians as regularizers, where q satisfies $1/p^* + 1/q = 1$.

3.25 Loss Functions, and Relations Between Machine Learning Problems

Robert Williamson(Australian National University – Canberra, AU)

Loss functions are central to supervised machine learning problems, but there has been little work in the recent machine learning literature in systematically understanding the effect of choice of loss functions. In this talk I will summarize some recent work starting with consideration of proper losses for classification problems (binary and multiclass). I will consider relationships to divergences (f-divergences and Bregman), surrogate regret bounds, composite losses (the composition of a proper loss with an invertible link function), existence and uniqueness results for such representations, integral representations, and characterization of mixability and convexity.

I will conclude by situating the work as part of a larger project on relating machine learning problems.

3.26 Some Learning Algorithms Producing Sparse Approximations

Ding-Xuan Zhou (City University – Hong Kong, HK)

We shall discuss two classes of kernel-based learning algorithms which produce sparse approximations for regression. The first class is of kernel projection machine type and generated by least squares regularization schemes with ℓ^q-regularizer ($0 < q \leq 1$) in a data dependent hypothesis space based on empirical features (constructed by reproducing kernels and samples). The second class is spectral algorithms associated with high-pass filter functions. Learning rates and sparsity estimations will be provided based on properties of the kernel, the regression function, and the probability measure.

Participants

- Misha Belkin
Ohio State University, US
- Robert J. Bonneau
AFOSR – Arlington, US
- Sebastien Bubeck
Princeton University, US
- Joachim Buhmann
ETH Zürich, CH
- Rui Castro
Eindhoven University of Technology, NL
- Nicoló Cesa-Bianchi
Univ. degli Stugli de Milano, IT
- Andreas Christmann
Universität Bayreuth, DE
- Matthias Hein
Saarland University, DE
- Jürgen Jost
MPI for Mathematics in the Sciences – Leipzig, DE
- Gerard Kerkyacharian
University Paris-Diderot, FR
- Vladimir Koltchinskiii
Georgia Tech, US
- Lek-Heng Lim
University of Chicago, US
- Gabor Lugosi
Pompeu Fabra University – Barcelona, ES
- Stephane Mallat
Ecole Polytechnique – Paris, FR
- Facundo Memoli
University of Adelaide, AU
- Hari Narayanan
MIT – Cambridge, US
- Robert Nowak
Univ. of Wisconsin-Madison, US
- Guillaume Obozinski
Ecole Normale Superieure – Paris, FR
- Sergei Pereverzyev
RICAM – Linz, AT
- Tomaso Poggio
MIT – Cambridge, US
- Massimiliano Pontil
University College London, UK
- Alexander Rahklin
University of Pennsylvania, US
- Philippe Rigollet
Princeton University, US
- Holger Rauhut
Universität Bonn, DE
- Lorenzo Rosasco
MIT – Cambridge, US, and IIT, IT
- Stephen Smale
City University, HK
- Bernhard Schölkopf
MPI for Intelligent Systems – Tübingen, DE
- Shai Shalev-Shwartz
Hebrew Univ. – Jerusalem, IL
- Yoram Singer
Google Research, US
- Ingo Steinwart
Universität Stuttgart, DE
- Gilles Stoltz
Ecole Normale Superieure – Paris, FR
- Alexandre Tsybakov
Université Paris VI, FR
- Sara van de Geer
ETH Zürich, CH
- Ulrike von Luxburg
Universität Hamburg, DE
- Alessandro Verri
Univ. degli Studi di Genova, IT
- Martin Wainwright
UC Berkeley, US
- Bob Williamson
ANU – Canberra, AU
- Ding-Xuan Zhou
City University, HK
- Tong Zhang
Rutgers University, US