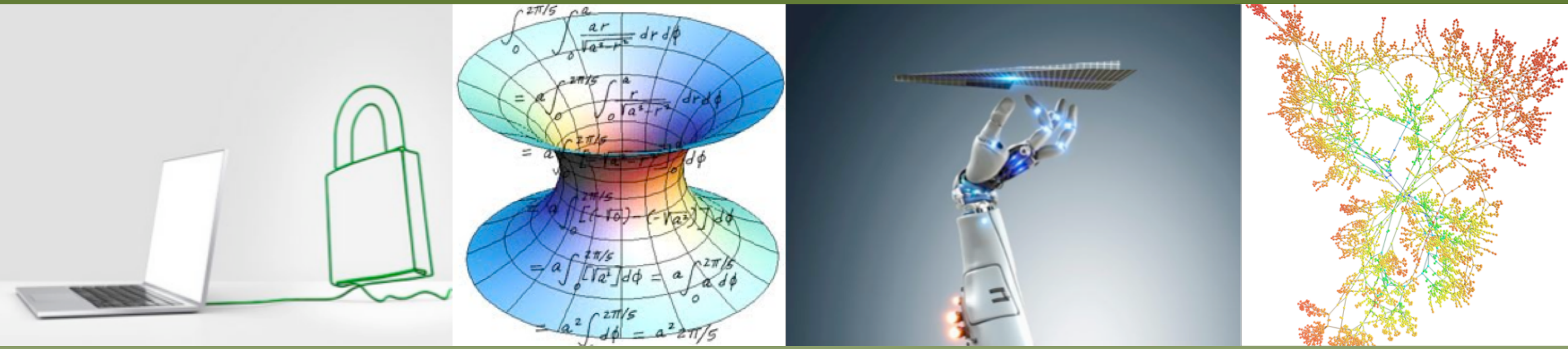
2ND URV DOCTORAL WORKSHOP IN COMPUTER SCIENCE AND MATHEMATICS

Edited by Marc Sánchez Artigas i Aïda Valls Mateu



UNIVERSITAT ROVIRA i VIRGILI

[DΣIM] Departament d'Enginyeria
Informàtica i Matemàtiques

Escola Tècnica Superior
d'Enginyeria
Universitat Rovira i Virgili

Title: 2nd URV Doctoral Workshop in Computer Science and Mathematics
Editors: Marc Sánchez Artigas i Aïda Valls Mateu
November 2015

Universitat Rovira i Virgili
C/ de l'Escorxador, s/n
43003 – Tarragona
Catalunya (Spain)

ISBN: 978-84-8424-399-1

Preface

This book of proceedings gathers the contributions presented at the *2nd URV Doctoral Workshop in Computer Science and Mathematics.* After the successful first edition in 2014, the second edition has been held in Tarragona (Catalonia, Spain) on November 13th 2015. It has been jointly organized by the research group on Architectures and Telematic Services and the Doctoral Program on Computer Science and Mathematics of Security of Universitat Rovira i Virgili (URV). The main aim of this workshop is to promote the dissemination of the ideas, methods and results that are developed in the Doctoral Thesis of the students of this doctorate program.

The workshop had two invited talks, oral presentations and posters. The first invited talk was given Dr. Pietro Michiardi, from Eurecom (France), who talked about both the algorithmic aspects and systems for Big Data analysis. The second talk was given by Mrs. Júlia Nebot from the Center of Technology Transfer of Foundation URV. She explained to the students how they can make business out of the results of a Ph.D. thesis (such as the steps for having a patent or for creating a start-up company).

In this book, the reader will find the contributions of the Ph.D. students. Each chapter presents the research topic of one student, the goals and some of the results. It is worth to note the wide coverage of this workshop, with contributions to the following main research lines: (1) Security and privacy in computer systems, (2) Artificial intelligence, robotics and vision, (3) Telematic architectures and complex networks and (4) Mathematics. All contributions present innovative proposals, methods or applications, with the aim of opening new and strategic research lines.

The editors and organizers invite you to contact the authors for more detailed explanations and we encourage you to send them your suggestions and comments that may certainly help them in the next steps of their PhD thesis. The organizing committee was formed by Dr. Marc Sánchez, Dr. Aïda Valls (Coordinator of the Ph.D. program), Mrs. Olga Segú, Ms. Miriam Martínez and Mr. Edgar Zamora.

We could not finish without first thanking the invited speakers for accepting the invitation of the organization committee and for giving us such interesting conferences. Second, we thank all the participants and especially, the students that presented their work in this DCSM workshop. Finally, also want to thank "Universitat Rovira i Virgili" (URV), the Department of Computer Science and Mathematics (DEIM), and the School of Engineering (ETSE) for their support.

Dr. Marc Sánchez and Aïda Valls (Editors)

Contents

Cross-swarm bundling in personal Clouds: Perspectives and limitations

Rahma Chaabouni[⋆]

Universitat Rovira i Virgili, Tarragona-Spain. rahma.chaabouni@urv.cat

1 Context

Users are unceasingly relying on personal cloud (PC) systems (like Dropbox, Google Drive, Box. . .) to store, edit and retrieve their files. These systems generally rely on a client-server architecture. This means that all the download requests will be handled by a central entity which sends the requested content in a single stream. PCs that have limited bandwidth budget can benefit from the upload speed of their clients in order to improve the overall download time. This can be done by introducing a peer-to-peer content distribution protocol and facilitate collaboration between PC clients. The two following common file distribution scenarios could benefit from this download strategy:

1. *Synchronization*: User A is adding a new file to his personal account. During the synchronization process, this file will be download by all the other synchronized devices of A
2. *Sharing*: User A is sharing a file with other users (B and C). In this case, the file will be downloaded by all the synchronized devices of B and C

We have proven in [1,2] that the use of BitTorrent (BT) [3] in PC to serve files to end-users can significantly reduce the download time of the clients while offloading the cloud server. However, due to the reduced sharing among PC clients, the total number of peers that can benefit from this download strategy remains very limited and the sizes of BT swarms are quite small (most BT swarms are composed of 2 peers only). To increase the number and size of BT swarms, we propose to use cross-swarm bundling in order which has been proven to be efficient in BitTorrent systems [4,5].

In this paper, we first describe the architecture of a PC that supports peer-to-peer collaboration and then evaluate the use of cross-swarm bundling techniques in these systems.

[⋆] PhD advisors: Marc Sanchez Artigas, Pedro Garcia Lopez

2 System Architecture

A Personal Cloud (PC) is a term generally used to refer to a file hosting service that allows its users to store, synchronize and share content over the Internet. The main components of a classic PC are:

- **Meta-data service:** The meta-data servers contain all the meta-data information related to the clients and the files.
- **Storage service:** The storage service refers to the physical locations where the users' file content are stored. It can be local, in the form of local storage servers accessed via FTP/SFTP, or external, provided by a third-party (Amazon, Google…).
- **Notification service:** The notification service is dedicated to monitoring whether or not any changes have been made to the users' accounts.
- **Processing service:** The processing service is responsible for processing the files and ensuring their delivery to the end-users.

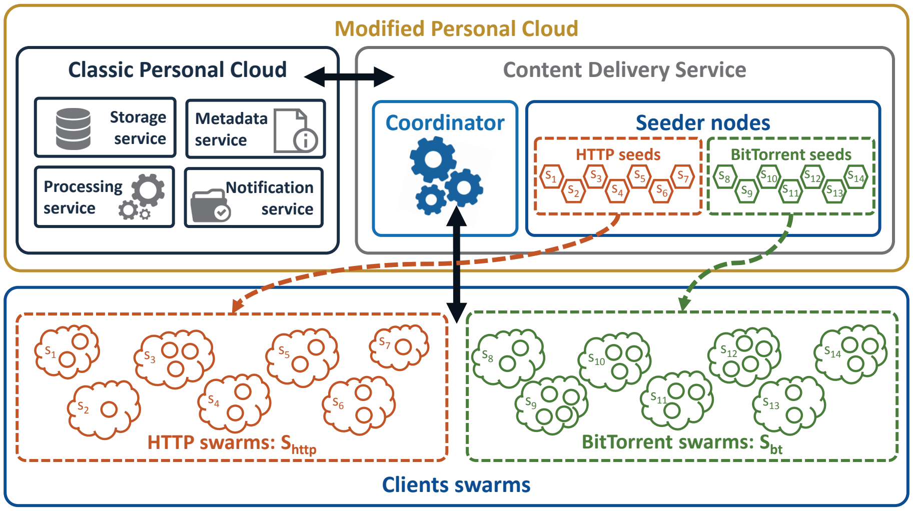


Fig. 1: System architecture

To allow inter-client content transfers via BT, the classic PC is extended with the following components which , as detailed in Figure 1:

- **Content Delivery Service :** The content delivery service processes the requests coming from the end-users and ensures the delivery of the files to the corresponding requesters. It is composed of:
  - **Coordinator:** The coordinator is responsible for managing the clients' requests and the cloud's resources.

  - **Seeder nodes:** The seeder nodes are the entities responsible for delivering the requested content from the storage back-end servers to the end-users. To each file being distributed corresponds one seeder node. We distinguish two types of seeds: *HTTP seeds* and *BitTorrent seeds* depending on the protocol used to distribute the content to end-users.
- **Clients swarms:** All the end-user peers are organized into swarms. We define a swarm by the set of peers that are requesting the same file. Similar to the seeds, we distinguish two types of swarms: *HTTP swarms* and *BitTorrent swarms* depending on the protocol used.

3 Cross-swarm bundling in PCs

Bundling consists in grouping a set of contents into a single file for download. Peers download a bundle that contains both the desired files along with some other files that make up the bundle [5]. This technique was mainly proposed to increase the availability of the least available swarms in BT systems. Bundling can be *static* when a pre-determined set of files are grouped together by the publisher, or *dynamic* if peers are assigned complementary content to download at the time they decide to download a particular file. Though static bundling is easy to implement, it may result in wasted downloads as every peer has to download the entire bundle. Dynamic bundling offers more flexibility since it can adapt to the current state of the publishers which might help in avoiding wasted downloads.

In our PC system, low content availability, which was the main motivation for bundling, is not an issue thanks to the cloud seeders. However, dynamic bundling can be used to reduce the load on cloud seeders and improve the download time of the clients. To this extend, we can differentiate between the following bundling variants, depending on the protocol being used by the bundled swarms:

- **BT-swarms bundling**: In BT-swarms bundling, a number N of distinct BT swarms sharing N distinct files can be grouped together. In this case, bundling implies creating bigger swarms sharing bigger files.
- **HTTP-swarms bundling**: In HTTP-swarms bundling, a number N of distinct HTTP swarms downloading N distinct files can be grouped together. In this case, bundling implies switching the transfer protocol from HTTP to BT for some HTTP swarms
- **Hybrid-swarms bundling**: In hybrid-swarms bundling, a number N_1 of BT swarms sharing N_1 distinct files are bundled with N_2 HTTP swarms which are downloading N_2 distinct files. In this case, bundling implies having bigger BT swarms and switching from HTTP to BT for some swarms.

Despite its benefits, there are possible security concerns that can be associated with bundling. As a matter of fact, grouping files of different users

can jeopardize the privacy of the users' sensitive information. This risk can be easily overcome by encrypting the user's data. This encryption can be implemented in two different levels: in the cloud's side or in the client's side.
The client's side encryption is already implemented in different PC providers, such as *Wuala* [6], *SpiderOak* [7] and *Dropbox Enterprise* [8]. Moreover, there are some commercial solutions, such as *Boxcryptor* [9], that allow the users to encrypt their data locally before sending them to the cloud.
The cloud's side encryption is another possible solution to ensure privacy between the clients. Nevertheless, it is important that the time needed for encryption/decryption is negligible compared to the time of information retrieval.

Acknowledgement. This work has been partially supported by the Martí-Franquès Research grants Program and the EU in the context of the project *CloudSpaces*: Open Service Platform for the Next Generation of Personal clouds (FP7-317555).

References

[1] R. Chaabouni, P. Garcia-Lopez, M. Sanchez-Artigas, S. Ferrer-Celma and C. Cebrian. "Boosting Content Delivery with BitTorrent in Online Cloud Storage Services". *Peer-to-Peer Computing (P2P), 13-th IEEE International Conference on*, pp.1,2, 9-11 Sept. 2013 doi: 10.1109/P2P.2013.6688731

[2] R. Chaabouni, M. Sanchez-Artigas and P. Garcia-Lopez. "Reducing Costs in the Personal Cloud: Is BitTorrent a Better Bet?". *Peer-to-Peer Computing (P2P), 14-th IEEE International Conference on*, pp.1,10, 8-12 Sept. 2014 doi: 10.1109/P2P.2014.6934302

[3] B. Cohen. "Incentives Build Robustness in BitTorrent". *Workshop on Economics of P2P systems.* June 2003.

[4] J. Han, T. Chung, S. Kim, H. Kim, J. Kangasharju, T. Kwonabd Y. Choi. "Strategic bundling for content availability and fast distribution in BitTorrent". *Computer Communications* 43: 64-73 (2014)

[5] S. Zhang, N. Carlsson, S. L. Eager, Z. Li, A. Mahanti. "Dynamic file bundling for large-scale content distribution". *Local Computer Networks (LCN), 2012 IEEE 37th Conference on*, pp.601,609, 22-25 Oct. 2012 doi: 10.1109/LCN.2012.6423681

[6] Wuala, `https://www.wuala.com`

[7] SpiderOak, `https://spideroak.com`

[8] Dropbox Enterprise, `https://www.dropbox.com/business`

[9] Boxcryptor, `https://www.boxcryptor.com`

Improving Prediction in the Routing Layer of Wireless Networks Through Social Behaviour

Pere Millán*

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
pere.millan@urv.cat

Abstract. Community networking, together with the Bottom-up-Broadband initiative, is an emerging model for the Future Internet across Europe and beyond where communities of citizens build, operate and own open IP-based networks, a key infrastructure for individual and collective digital participation. As any other network that mixes wired and wireless links, the routing protocol must face several challenges that arise from the unreliable nature of the wireless medium, the self-management by the users, and the organic growth. Our research focus on improving the performance of routing protocols in wireless networks. The first research topic is about predicting both the link quality and the path quality in wireless community networks. In the second research topic, we analyse the prediction opportunities of the control packets in the routing layer of the OLSR protocol (in Mobile Ad-hoc Networks, MANETs). This paper contains the main results we have obtained in both topics. We also explain our current research on the "social behaviour" of people who carry with them the devices that form the nodes of wireless networks (e.g. smartphones) in real scenarios.

Keywords: Routing Protocols, Wireless Networks, Network Topology Prediction, Link & Path Quality Prediction, Social Behaviour, Community Networks, MANETs.

1 Link Quality Prediction

Link quality (LQ) tracking helps the routing layer to select links that provide the best features for communication. Moreover, LQ prediction has proved to be a technique that surpasses LQ tracking by foreseeing which links are more likely to change its quality. In [3] we focus on LQ prediction by means of a time series analysis. We apply it in the routing layer of large-scale, distributed and decentralized networks. We demonstrate that this type of prediction achieves a success probability of about 98% in both the short and long term.

In [2] we enhanced and extended the previous work by giving more detailed discussion of the previously presented global studies and including a

* PhD advisors: Carlos Molina (URV), Roc Meseguer (UPC).

new one that relates topological features of a link with the behaviour of its link quality. We included two new subjects. The first analyses the variability of LQ prediction (1) between links and (2) over time. A second new subject proposes and discusses an enhancement to the prediction process that benefits from the global and individual behaviour of link qualities observed.

Those studies demonstrate that time series analysis is a promising approach to accurately predict LQ values in community networks. This technique can be used to improve the performance of the routing protocol by providing information to make appropriate and timely decisions.

As future work, we plan to identify which links contribute most to the error in the LQ prediction and to understand what factors make it more difficult to predict the behaviour of these links. We also want to analyse if there is a subset of links that provides real trends in LQ. Moreover, we plan to improve the prediction process discarding those links whose relation between LQ and prediction accuracy is above a certain threshold. Furthermore, we are currently implementing our proposal, that will allow us to determine its cost, how to be used by routing protocols, and if the addition of other sources of information (e.g. NIC parameters) could improve the predictions. Finally, we want to extend our analysis to other community networks, to evaluate if the observed behaviour could be generalized.

2 Path Quality Prediction

End-to-End or Path Quality (PQ) tracking helps the routing layer to select paths that provide the best features for communication. We believe that PQ prediction surpasses PQ tracking by foreseeing which paths are more likely to change its quality. In [1] we focus on PQ prediction by means of time-series analysis. We apply this prediction technique in the routing layer of community networks. We demonstrate that it is possible to accurately predict PQ with an average Mean Absolute Error of just 2.4%. Particularly, we analyze the path properties and path ETX[1] behavior to identify the best prediction algorithm. Moreover, we analyze the PQ prediction accuracy some steps ahead in the future and also its dependency of the time of the day.

We have presented results from 4 well known learning algorithms that model time series. All of them achieved high percentages of success, with average Mean Absolute Error values per link between 2.4% and 5% when predicting the next value of the PQ. We also analyzed the error variability and found that three of them presented similar performance, whereas the fourth performs worse due to outliers with larger errors. A more detailed study of the best prediction shows an average absolute error less than 1. We have also

[1] ETX is the number of expected transmissions of a packet necessary for it to be received without error at its destination. ETX varies from number of HOPS (perfect) to infinity.

observed differences in the prediction behavior during day and during night, as it happens with actual ETX values.

The future work in PQ is similar to LQ. We want to extend this analysis to other community networks. Moreover, we plan to identify which paths contribute most to the errors in the PQ prediction and to understand what factors make it more difficult to predict them. We also want to study the impact of errors in routing decisions, and to study a solution with two different predictors for day and night. Finally, we plan to improve the prediction process discarding those paths whose relation between PQ and prediction accuracy is above a certain threshold.

3 Control Information Prediction

Several social computing participation strategies use mobile ad hoc or opportunistic networks to support the users activities. The unreliability and dynamism of these communication links make routing protocols a key component to achieve efficient and reliable data communication in physical environments. Often these routing capabilities come at expenses of flooding the network with a huge amount of Topology Control Information (TCI), which can overload the communication links and dramatically increase the energy consumption of the participating devices. In previous works we have shown that predicting the network topology in these work scenarios helps reduce the number of control packets delivered through the network. This saves energy and increases the available bandwidth. In [4] we present a study that extends previous works, by identifying the impact of predicting the TCI generated by routing protocols in these networks. The prediction process is done following a history-based approach that uses information of the nodes past behavior. The paper also determines the predictability limits of this strategy, assuming that a TCI message can be correctly predicted if it appeared at least once in the past. The results show that the upper-bound limit of the history-based prediction approach is high, and that realistic prediction mechanisms can achieve significant ratios of accuracy.

The main contributions are: (1) we observed that around 80% of the times, for low densities of nodes, a packet has already appeared in the past. This percentage falls to 50% when considering a network with a higher node density. This demonstrates that the upper bound limits of our strategy remain high for an ample variety of interaction scenarios, which make us expecting important benefits for mobile collaborative applications that use these networks as communication support. (2) the results also show that few packets contribute significantly to the total percentage of packets delivered through the network. This means that there is a high opportunity for predicting the TCI, and this prediction can be just focused on a small subset of packets. (3) we have identified the role played by different history-depth patterns, prediction policies, confidence mechanisms, and the combination of several approaches.

As a future work, we plan to analyze in detail all combinations of work scenarios, considering node density, speed, and mobility patterns. We also want to develop more complex confidence mechanisms, and combine the prediction approaches to see if their benefits can be accumulated. Moreover, it would also be interesting to analyze the prediction performance in opportunistic networks involving heterogeneous environments (to address IoT-based solutions).

4 Improving Prediction Through Social Behaviour

Our previous research steps have demonstrated the importance of the prediction for both Link & Path Quality, and also for Control Information packets. In a real scenario, the nodes that compose the wireless network correspond to the communication devices carried by the people (e.g. smartphones). Our current research topic is to incorporate the social behaviour of people in the prediction process and to study if this new factor improves the obtained results. We want to asses if this "social behaviour" is real or just virtual. We focus our analysis in the mobility of people (e.g. a group of people in a museum guided visit) and in time factors (e.g. day and night, workdays and weekend).

Acknowledgement. This work has been partially supported by the Spanish Ministry of Science and Innovation (MCI) and FEDER funds of the EU under contracts TIN2013-44375-R, TIN2013-47245-C2-1-R, TIN2013-47245-C2-2-R and TIN2012-37171-C02- 02, and also the Community Networks Testbed for the Future Internet (CONFINE) project: FP7-288535, and also by the Generalitat de Catalunya as a Consolidated Research Group 2014-SGR-881.

References

[1] P. Millán, C. Molina, E. Dimogerontakis, L. Navarro, R. Meseguer, B. Braem, C. Blondia. Tracking and Predicting End-to-End Quality in Wireless Community Networks. *Proc. 4th International Workshop on Community Networks and Bottom-up-Broadband (CNBuB'15)*, Rome, Italy, August 2015.

[2] P. Millán, C. Molina, E. Medina, D. Vega, R. Meseguer; B. Braem, C. Blondia. Time Series Analysis to Predict Link Quality of Wireless Community Networks. *Computer Networks*, 2015 [*under review*].

[3] P. Millán, C. Molina, R. Meseguer, E. Medina, D. Vega, B. Braem, C. Blondia. Tracking and Predicting Link Quality in Wireless Community Networks. *Proc. 10th IEEE Int. Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB'14)*, 239–244, Larnaca, Cyprus, October 2014.

[4] P. Millán, C. Molina, R. Meseguer, S.F. Ochoa, R. Santos. Using a History-Based Approach to Predict Topology Control Information in Mobile Ad Hoc Networks. *Proc. 7th International Conference on Internet and Distributed Computing Systems (IDCS'14)*, 237–249, Calabria, Italy, September 2014.

Towards Cooperative Analytics in Disaggregated Big Data Clusters

Josep Sampé *

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
josep.sampe@urv.cat

1 Introduction

The advent of Big Data has emerged from the increasing necessity that companies and organizations face of extracting value from very large amounts of raw data produced during their daily operation. In this sense, it is common to find large-scale data processing scenarios where compute clusters and data stores are physically disaggregated, usually being interconnected by a high speed networking layer. In terms of management, disaggregating or specializing storage and computation clusters seems reasonable given the disparate requirements of storage and computing tasks. Moreover, this scenario enables storage and compute resources to be easily shared across multiple tenants via virtualization techniques.

Despite its benefits, the unintended consequence of disaggregating storage and compute resources is that it may represent a performance barrier to scale-out Big Data analytics [3]. That is, data should be moved or batch loaded from the data store to the compute cluster before the actual computation takes place, deriving in an intense activity over the network. Consequently, companies are forced to adopt a “store-first-query-later” approach for processing large volumes of data.

1.1 Compute clusters

In today’s Big Data environments, compute clusters usually run a variety of computing frameworks for data processing, such as Apache Hadoop [2] or Spark [4], among others. These frameworks are based in the MapReduce paradigm. MapReduce is a paradigm for parallel computation that consists of two main functions called Map and Reduce. Map function takes as input a key-value pair and produces multiple key-value pairs called intermediate-results, then, the output of the Map function is grouped by keys and sent

* PhD advisors: Pedro García López, Marc Sánchez Artigas

to the Reduce function which takes this intermediate results as input, runs aggregation, and produce final results. Unlike Hadoop, Spark is designed for advanced, real-time analytics. Spark runs in memory making it, in some cases, 100 times faster than Hadoop. One additional benefit of both frameworks is that they have SQL interpreters (Hive and SparkSQL), which enable the user to manage data via SQL-like statements, avoiding the need for a user of developing low-level Hadoop/Spark jobs.

1.2 Storage clusters: More than just data silos

Currently, storage clusters are divided into three different types of storage in function of what they store: files, blocks or objects. In this work, we are focusing on use object storage clusters, designed to store unstructured and large amounts of data. One of the most commonly used object storage platform is OpenStack Swift. Swift is a highly scalable redundant unstructured data store that leverages commodity hardware, making it widely used by companies and organizations for building their own storage clusters. Moreover, we can interact with Swift via an HTTP restful API, leveraging easy and ubiquitous data access.

Although storage clusters are normally dedicated to provide storage services, in the last years several works have advocated for converting the data store into a computation capable entity introducing the concept of Active Storage [1]. The main benefit of Active Storage is that it reduces the amount of data movement needed between storage and compute nodes. In Swift there are two frameworks providing Active Storage: ZeroCloud [5] and IBM Storlets [6]. Both ZeroCloud and Storlets are executed into a sandboxed environment, isolating the storage layer from compute tasks for security reasons.

In this work, we are using IBM Storlets. This novel framework allows us to develop filters called Storlets that are installed in the Input/Output flow of an object in Swift. Storlets are executed just before Swift stores data to or after reads data from storage nodes' disks. We can develop many types of Storlets, for example, Storlets related to encryption or data reduction tasks.

Nowadays, storage nodes have sufficient resources for doing basic computation tasks without moving all data to the compute cluster, and then, move the results back to the storage nodes, saving thus a lot of bandwidth and other resources. Furthermore, this approach will allows us to provide services at storage level such as filtering, data reduction, or advanced Extract-Transform-Load (ETL) capabilities, that is, services to scale-out Big Data analytics in disaggregated clusters.

2 Cooperative Clusters for Big Data Analytics

In this thesis, we aim at enabling cooperation in disaggregated Big Data environments to reduce data movement between compute and storage clusters.

Approach. Common compute clusters have limited resources so it is very important load only the needed data to compute cluster for reducing resource usage. In our approach, we enable communication between compute and storage clusters by modifying HTTP headers of requests at compute side, thereby allowing Storlet invocation at storage side. Furthermore, we may add parameters in these headers to run additional or specific functionalities in the Storlets. Our approach is transparent to users, so that they may run computation tasks without noticing that the storage cluster is helping in compute tasks.

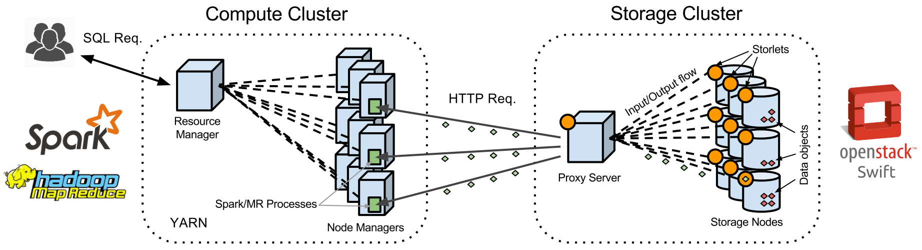


Fig. 1: High level overview of our approach architecture.

Proof of concept. We executed an experiment where we can see the benefits of using cooperative analytics. The experiment consists of processing log traces from a production system (14.8GB) with Map Reduce. The compute cluster will count the total number of transactions done by each user in the trace. We executed our experiments in a 7-machines rack formed by a compute cluster (3 Dell Servers R420) and a storage cluster (4 Dell Servers R320). Both clusters are interconnected via a 1Gb switched network.

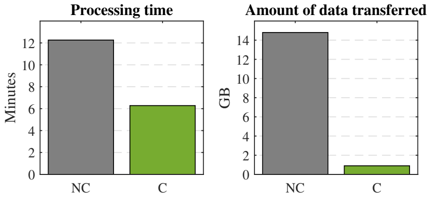


Fig. 2: Experiment results: Non Cooperative (NC), Cooperative (C)

In Fig. 2, Grey bars (NC) show the performance of executing the previous experiment in a standard Hadoop/Swift installation, whereas green bars (C) reflect the performance of our cooperative analytics framework. As we can observe, the cooperative analytics approach reduces by the half the time spent to perform computations. Moreover, the total amount of data transferred between compute and storage clusters is reduced by 90%. This gives a sense on the potential of cooperative Big Data clusters in disaggregated environments.

3 Final Remarks and Future Work

In this paper, we presented the concept of making compute and storage clusters to cooperate in disaggregated Big Data analytics environments. Our early experiments show the potential gains that an active object store may provide when it cooperates in the data analytics lifecycle, concretely in terms of bandwidth reduction and compute times. However, there are still many challenges to face in the near future.

For instance, making use of Spark/Hadoop to process data files on top of OpenStack Swift produces a high number of concurrent requests, since both frameworks have been designed to perform parallel computation. Unfortunately, this type of computation over Swift derives in some drawbacks at storage side, such as resource contention or performance interference at Storlet level. That is why currently our research is focused on determine what kind of Storlets produces resource contention and how much workload supports this type of Active Storage, and then, decide how to optimize resource usage to avoid these problems when compute clusters process Swift datasets.

Acknowledgement. This work has been partially supported by the EU in the context of the project IOStack: Software-defined storage for Big Data (H2020-ICT-2014-7-1), and the project CloudSpaces: Open Service Platform for the Next Generation of Personal clouds (FP7-317555).

References

[1] E. Riedel, G. Gibson, and C. Faloutsos. Active storage for large-scale data mining and multimedia applications. *VLDB'98: 24th international Conference on Very Large Databases*, 62-73, New York, NY, August 1998.

[2] Jeffrey Dean and Sanjay Ghemawat. MapReduce: Simplified Data Processing on Large Clusters. *OSDI'04: Sixth Symposium on Operating System Design and Implementation.*, San Francisco, CA, December, 2004.

[3] L. Rupprecht, R. Zhang, and D. Hildebrand. Big Data analytics on object stores: A performance study. *SC14: Conference for high performance computing, networking, storage and analysis*, New Orleans, LA, November 2014.

[4] M. Zaharia, M. Chowdhury, M. J. Franklin, S. Shenker, I. Stoica. Spark: Cluster Computing with Working Sets. *HotCloud'10: 2nd usenix conference on hot topics in cloud computing*, Boston, MA, June 2010.

[5] P. Rad, V. Lindberg, J. Prevost, W. Zhang, and M. Jamshidi. ZeroVM: Secure Distributed Processing for Big Data Analytics. *World Automation Congress*, 1-6, Waikoloa, Hawaii, August 2014.

[6] S. Rabinovici-Cohen, E. Henis, J. Marberg, K. Nagin. Storlet Engine: Performing Computations in Cloud Storage. *Technical report H-0320, IBM Research*, Haifa, Israel, August 2014.

Cyclic codes, Equiangular Polygons and New Decoding Algorithms

Marta Pujol[⋆]

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
marta.pujol@.urv.cat

1 Introduction

During this year I have worked on two main topics related to coding theory which have derived in two accepted articles and one ongoing preprint. The first accepted article deals with the relationship between cyclic codes and side lengths of equiangular polygons. It was published in May in American Mathematical Monthly. It is the topic of the next section. In the third section I present the results of our second accepted (proceedings) article, which focuses in the algorithms that decode errors and erasures of Reed-Solomon codes and a new version of the key equation. The results of this research will be presented in Kalamata, Greece in July 2015. We are trying to publish a journal version of them.

2 Side Lengths of Equiangular Polygons (as seen by a coding theorist)

An equiangular polygon is a polygon whose vertex angles are equal. Equiangular polygons arise, for instance, in connection with the area enclosed by binary forms through the so-called Schwarz-Christoffel mapping [2,3].

An ordered set of positive real numbers $a_1, \ldots, a_n$ (or the corresponding n-tuple) is said to be *equiangulable* if there exists an equiangular polygon with side lengths consecutively equal to $a_1, \ldots, a_n$. It can be proved, (see for instance [1,10]), that equiangulable n-tuples can be characterized, using complex numbers, as the n-tuples for which $a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-1}x+a_n$ vanishes at $e^{\frac{2\pi}{n}i}$. Indeed, just consider the rotations at every angle and the shifts along every side of the polygon. We proved an equivalent result without using complex numbers, but some frequent tricks used in the theory of cyclic codes. One new insight in the proof is the definition and characterization of shift-stable linear spaces.

[⋆] PhD advisor: Maria Bras

Finally, we have worked on an application of this research to the construction of slot car circuits. We assume that the pieces (straights and archs) are compound of sides of an equiangular polygon. So, giving the pieces of a circuit in order, like a polygon, to the application that we have developed, it will notify if this circuit will close or not. Therefore, we will be informed of the possibility of a circuit that closes before being assembled. This opens the door to a tool for deciding what circuits can be formed with a given set of non necessarily ordered slot pieces.

3 A New Approach to the Key Equation and to the Berlekamp-Massey Algorithm

The two primary decoding algorithms for Reed-Solomon codes are the Berlekamp-Massey algorithm [8] and the Sugiyama et al. adaptation of the Euclidean algorithm [11], both designed to solve Berlekamp's key equation [4]. The connections between the two algorithms were analyzed in [5,7,9]. We present a new version of the key equation for errors and erasures, more natural in the sense that correction polynomials are based on error locations rather than their inverses, as in the classical equations. We give a way to use the Euclidean algorithm to solve the new key equation. A straightforward reorganization of the algorithm yields the Berlekamp-Massey algorithm. Hence, our new approach can be seen as an alternative, more natural, explanation of the Berlekamp-Massey algorithm.

3.1 Settings on Reed-Solomon Codes

Let $\mathbb{F}$ be a finite field of size q and let α be a primitive element in $\mathbb{F}$. Let $n = q - 1$. We identify the vector $u = (u_0, \ldots, u_{n-1})$ with the polynomial $u(x) = u_0 + \cdots + u_{n-1}x^{n-1}$ and denote $u(a)$ the evaluation of $u(x)$ at a. Classically the (primal) Reed-Solomon code $C^*(k)$ of dimension k is defined as the cyclic code with generator polynomial $(x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{n-k})$, The dual Reed-Solomon code $C(k)$ of dimension k is the cyclic code with generator polynomial $(x - \alpha^{n-(k+1)})(x - \alpha^{n-(k+2)}) \cdots (x - \alpha)(x - 1)$.

Both codes have minimum distance $d = n - k + 1$. Furthermore, $C(k)^{\perp} = C^*(n - k)$. There is a natural bijection from ^{n} to itself which we denote by $c \mapsto c^*$. It takes $C(k)$ to $C^*(k)$. The codeword c^* can be defined either as $iG^*(k) \in C^*(k)$ where i is the information vector of dimension k such that $c = iG(k) \in C(k)$ or componentwise as The codeword c^* can be defined either as $iG^*(k) \in C^*(k)$ where i is the information vector of dimension k such that $c = iG(k) \in C(k)$ or componentwise as

$c^* = (c_0, \alpha^{-1}c_1, \alpha^{-2}c_2, \ldots, \alpha c_{n-1})$ where $c = (c_0, c_1, \ldots, c_{n-1})$. Then, $(c_0^*, \alpha c_1^*, \alpha^2 c_2^*, \ldots, \alpha^{n-1} c_{n-1}^*)$.

A decoding algorithm for a primal Reed-Solomon code may be used to decode a dual Reed-Solomon code by first applying the bijection $*$ to the received vector u. If u differs from a codeword $c \in C(k)$ by an error vector e of weight t, then u^* differs from the codeword $c^* \in C^*(k)$ by the error vector e^* of weight t. If the primal Reed-Solomon decoding algorithm can decode u^* to obtain c^* and e^* then, transforming by the inverse of $*$ we may obtain c and e. Conversely, a decoding algorithm for a dual Reed-Solomon code may be used to decode a primal Reed-Solomon code by applying the inverse of $*$, decoding, and then applying $*$.

3.2 Decoding for Errors and Erasures

Suppose that $c \in C(k)$ is transmitted and that errors occurred at t different positions and that other s positions were erased, with $2t+s < d$. Suppose that u is the received word once the erased positions are put to 0 and that $e = u-c$. Define the *erasure locator polynomial* as $\varLambda_r = \prod_{i:c_i \text{was erased}}(x-\alpha^i)$ and the *error locator polynomial* as $\varLambda_e = \prod_{i:e_i\neq 0, c_i \text{not erased}}(x-\alpha^i)$. We will use $\varLambda$ for the product $\varLambda_r\varLambda_e$. Notice that $\varLambda_r$ is known from the received word, while $\varLambda_e$ is not. Define the error evaluator as $\varOmega = \sum_{\substack{i:e_i\neq 0 \\ \text{or } c_i \text{ erased}}} e_i \prod_{\substack{j:e_j\neq 0 \text{ or } c_j \text{ erased,} \\ \text{and } j\neq i}}(x-\alpha^i)$. The error positions can be identified by $\varLambda_e(\alpha^i) = 0$ and the error values, as well as the erased values, can be derived from an analogue of the Forney formula [6], $e_i = \frac{\varOmega(\alpha^i)}{\varLambda'(\alpha^i)}$.

The *syndrome polynomial* is defined as $S = e(\alpha^{n-1}) + e(\alpha^{n-2})x + \cdots + e(\alpha)x^{n-2} + e(1)x^{n-1}$. It can be proved that $\varOmega(x^n-1) = \varLambda S$. The general term of S is $e(\alpha^{n-1-i})x^i$, but from a received word we only know $e(1) = u(1), \ldots, e(\alpha^{n-k-1}) = u(\alpha^{n-k-1})$. Define $\bar{S} = e(\alpha^{n-k-1})x^k + e(\alpha^{n-k-2})x^{k+1} + \cdots + e(1)x^{n-1}$. The polynomial $\varOmega(x^n-1) - \varLambda\bar{S} = \varLambda(S-\bar{S})$ has degree at most $t+s+k-1 < \frac{d-s}{2} + s + n - d = n - \frac{d-s}{2}$. Next theorem provides an alternative key equation for dual Reed-Solomon codes.

Theorem 1. *If s erasures and at most $\lfloor\frac{d-s-1}{2}\rfloor$ errors occurred, then $\varLambda_e$ and $\varOmega$ are the unique polynomials f and φ satisfying the following properties. 1. $\deg(f\varLambda_r\bar{S} - \varphi(x^n-1)) < n - \frac{d-s}{2}$; 2. $\deg(f) \leq \frac{d-s}{2}$; 3. f, φ are coprime; 4. f is monic*

Suppose first that only erasures occurred. Then $\varLambda = \varLambda_r$, $\varLambda_e = 1$, and $\varOmega$ can be directly derived from this inequality. Indeed, $\varOmega$ is the sum of monomials in $\varLambda_r\bar{S}$ with degrees at least $n - \frac{d-s}{2}$, divided by $x^{n-\frac{d-s}{2}}$.

Suppose that a combination of errors and erasures occured. The extended Euclidean algorithm applied to $\varLambda_r\bar{S}$ and $-(x^n-1)$ computes not only $\gcd(\varLambda_r\bar{S}, x^n-1)$ but also two polynomials $\lambda(x)$ and $\eta(x)$ such that $\lambda\varLambda_r\bar{S} - \eta(x^n-1) = \gcd(\varLambda_r\bar{S}, x^n-1)$. At each intermediate step a new remainder r_i is computed, with decreased degree, together with two intermediate polynomials $\lambda_i(x)$ and $\eta_i(x)$ such that $\lambda_i \Lambda_r \bar{S} - \eta_i(x^n - 1) = r_i$. Truncating this algorithm at a proper point we can get a pair of polynomials λ_i and η_i such that $\lambda_i \Lambda_r \bar{S} - \eta_i(x^n - 1)$ has degree as small as desired (in particular, smaller than $n - \frac{d-s}{2}$). Little modifications to the Euclidean algorithm to simplify its computations will lead in a natural way to the Berlekamp-Massey algorithm.

4 Conclusions and Future Work

As we commented in the introduction, our next steps are the presentation in Kalamata and the publication of the Reed-Solomon article. Also we are developing the codification of the algorithms of this last document, programming in sage. We will try to introduce this example before sending the article to a journal.

Acknowledgement. Thanks to URV to give me the Martí Franquès grant.

References

[1] Derek Ball. Equiangular polygons. *The Mathematical Gazette*, 86(507):396–407, 2002.

[2] Michael A. Bean. Binary forms, hypergeometric functions and the Schwarz-Christoffel mapping formula. *Trans. Amer. Math. Soc.*, 347(12):4959–4983, 1995.

[3] Michael A. Bean and Richard S. Laugesen. Binary forms, equiangular polygons and harmonic measure. *Rocky Mountain J. Math.*, 30(1):15–62, 2000.

[4] Elwyn R. Berlekamp. *Algebraic coding theory.* McGraw-Hill Book Co., New York, 1968.

[5] Jean-Louis Dornstetter. On the equivalence between Berlekamp's and Euclid's algorithms. *IEEE Trans. Inform. Theory*, 33(3):428–431, 1987.

[6] G. David Forney, Jr. On decoding BCH codes. *IEEE Trans. Information Theory*, IT-11:549–557, 1965.

[7] Agnes E. Heydtmann and Jørn M. Jensen. On the equivalence of the Berlekamp-Massey and the Euclidean algorithms for decoding. *IEEE Trans. Inform. Theory*, 46(7):2614–2624, 2000.

[8] James L. Massey. Shift-register synthesis and BCH decoding. *IEEE Trans. Information Theory*, IT-15:122–127, 1969.

[9] Todd D. Mateer. On the equivalence of the Berlekamp-Massey and the Euclidean algorithms for algebraic decoding. In *Information Theory (CWIT), 2011 12th Canadian Workshop on*, pages 139–142, 2011.

[10] K. Robin McLean. A powerful algebraic tool for equiangular polygons. *The Mathematical Gazette*, 88:513–514, 2004.

[11] Yasuo Sugiyama, Masao Kasahara, Shigeichi Hirasawa, and Toshihiko Namekawa. A method for solving key equation for decoding Goppa codes. *Information and Control*, 27:87–99, 1975.

Privacy-preserving Mechanisms for e-Commerce

Alberto Blanco Justicia [*]

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
alberto.blanco@urv.cat

1 Introduction

Electronic commerce offers great advantages to both customers and vendors. Customers have a clear advantage: convenience. Vendors, on the other hand, can improve their inner processes thanks to the information they gather from their transactions. Also, they can form a clear idea of what their clients buy and, consequently, what they might want to buy in the future, by building profiles of their customers.

Of course, e-commerce, and particularly e-commerce through handheld devices (mostly because of poorer passwords), introduces some threats, that are mainly related to the security of the communications, but also to the privacy of the customers because of profiling, segmentation, purchase lists kept by credit card issuers, etc. In some cases, these profiles are not kept by the participating parties only, but are shared with or sold to other organizations, such as data brokers, which collect information about individual customers from several sources. These sources include vendors, cookies, usage statistics from the users' devices, etc. Using all these data, data brokers offer security and authentication services, by means of identity managers and the like.

Our general objective is to provide secure e-commerce protocols that provide the advantages of e-commerce that we mentioned above, but that preserve the privacy of the customer at least up to an agreed level between the customer and the vendor. Also, by building and keeping the users' profiles, even if they are kept private, we can devise protocols that increase the security of the communications, namely in the areas of authentication and authorization, without the aid of third parties like data brokers.

2 Related Work

Privacy Enhancing Technologies are a set of ICT measures and techniques that, when integrated into online services or applications, prevent the unnec-

[*] PhD advisor: Josep Domingo Ferrer

essary or unwanted processing of personal data. PETs are typically classified as cryptographic techniques and non-cryptographic techniques.

Cryptographic techniques are not only limited to data encryption, but also include primitives such as blind signatures [5] and zero-knowledge proofs [8], which and have been widely used in the field. Protocols such as electronic cash (including Bitcoin), anonymous digital credentials and anonymous identification typically make use of such primitives. Other relevant techniques include secret sharing schemes [1,11], threshold cryptography, secure multiparty computation [13] and identity-based cryptography [12,4].

Non-cryptographic techniques include data minimization, splitting, aggregation and database protection techniques, such as those coming from Statistical Disclosure Control [10].

Finally, implicit authentication is defined as the ability to authenticate a user based on the her profile, which is built from the typical behaviour when using her device. This type of authentication is particularly well-suited for mobile devices, where limited input space makes users choose weaker passwords. Also, mobile devices typically have many sensors, including several network interfaces, which are a good source from which to build the user's profile.

3 Obtained Results

This section is divided in two parts: the first part deals with results obtained for specific e-Commerce services, for which mechanisms are provided to help in protecting potentially confidential data. The second part deals with results obtained for the management of private user profiles.

3.1 e-Commerce

We proposed in [6] a mechanism for group discounts that allows groups of people to prove the size of their group while remaining anonymous to the verifier [6]. The protocol is based on an Identity-based Dynamic-threshold signature scheme presented in [9], a novel key management strategy and short-range communication technologies to communicate among group members. The protocol is implemented as an Android application, and results indicate that it is usable in practice.

In [3], we presented a mechanism to allow the implementation of loyalty programs that support the issuance and submission of loyalty points in an anonymous and unlinkable way. Also, customers obtain verifiable proofs of purchases from which they can build their own (generalized) profiles which can then be submitted to vendors. Customers and vendors can agree upon the level of generalization of the profiles, awarding more loyalty points to those customers that provide more accurate profiles.

3.2 Managment of user profiles

Stored user profiles, obtained from purchase histories, browser histories, mobile devices' sensor data, etc. can be used for a wide number of applications. For example, by comparing user profiles, we can identify users with similar tastes in social networks.

We presented a mechanism to compute the similarity (or distance) between user profiles in [2]. It is based on a class of secure multiparty computation protocols called *private set intersection.* In PSI protocols, the users' inputs are sets, and both parties obtain the intersection of the sets without leaking any other information from the original sets (*e.g.* their contents, their size, etc.). A slightly different version of this primitive, PSI-CA, outputs the size of the intersection instead of the intersection itself. In this work, we encode the user profiles as sets of features, which can be categorical (independent or correlated) or numeric and use the homomorphic properties of the Paillier cryptosystem to instantiate a PSI-CA protocol. By obtaining the cardinality of their intersection, we can compute the similarity between the two user profiles while keeping the profiles private.

In [7] we use a variation of the protocol in [2] to present an implicit authentication protocol that preserves the privacy of the users.

Acknowledgement. The author is supported by an FI-DGR grant from the Government of Catalonia and the European Social Fund. The following funding sources are acknowledged: Google (Faculty Research Award to the PhD advisor) and the European Commission (projects FP7 “Inter-Trust”, H2020 “CLARUS”). The authors are with the UNESCO Chair in Data Privacy, but they are solely responsible for the views expressed in this paper, which do not necessarily reflect the position of UNESCO nor commit that organization.

References

[1] G.R. Blakley. Safeguarding cryptographic keys. *Proceedings of the National Computer Conference*, 313–317, New York: AFIPS Press, 1979.

[2] A. Blanco-Justicia *et al.* Distance Computation between Two Private Preference Functions. *SEC 2014*, 460–470, 2014.

[3] A. Blanco-Justicia, J. Domingo-Ferrer. Privacy-preserving Loyalty Programs. *DPM/SETOP/QASA 2014*, 133–146, 2014.

[4] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *CRYPTO 2001*, 213–229, Springer, 2001.

[5] D. Chaum. Blind signatures for untraceable payments. *CRYPTO 1982*, 192–213, Plenum Press, 1983.

[6] J. Domingo-Ferrer, A. Blanco-Justicia. Group Discounts compatible with Buyer Privacy. *DPM/SETOP/QASA 2014*, 47–57, 2014

[7] J. Domingo-Ferrer, Q. Wu, A. Blanco-Justicia. Flexible and Robust Privacy-Preserving Implicit Authentication. *SEC 2015*, 18–34, Springer International Publishing, 2015.

[8] S. Goldwasser *et al.* The knowledge complexity of interactive proof systems. *SIAM Journal on computing 18.1*, 186–208, 1989.

[9] J. Herranz *et al.*, Short attribute-based signatures for threshold predicates. *RSA Conference CT-RSA 2012, LNCS 7178*, 51–67, 2012.

[10] A. Hundepool *et al.*, Statistical Disclosure Control. Wiley, 2012.

[11] A. Shamir. How to Share a Secret. *Communications of the ACM*, 22:612–613, 1979.

[12] A. Shamir. Identity-based cryptosystems and signature schemes. *Advances in cryptology*, 47–53, Springer Berlin Heidelberg, 1985.

[13] A. C. Yao. Protocols for secure computations. *FOCS 82*, 160–164, 1982.

Access Control Management and Enforcement

Malik Imran Daud [*]

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
malikimran.daud@urv.cat

1 Introduction

Access control management has been the focal area of research by the research community. In the field of information security, access control management is a method to manage the access to the resources based on the identity of the users [3]. In the environment that are distributed and has a large number of users (e.g. social networks and Cloud), access control management for such users' is a challenging job.

In view of above, the researchers have proposed many solutions [7,2] to address such issues. Though, the proposed solutions may not be feasible due to the following reasons: i) a lot of manual management of access rights by the users or by the administrator of the system, ii) performance of these methods decreases proportionally as the number of users increase, iii) rigidity of access control mechanism implemented by the proposed systems, and iv) the users lack of technical knowledge of these mechanisms.

In view of above mentioned shortcomings, we propose solutions that are capable of management, delegation and enforcement of the access rights of the users in a distributed or large-scale environments (e.g. social networks and Clouds). The research contributions are are based on the following notions:

- Privacy-driven access control in social network by means of automatic semantic annotation.
- Ontology based delegation of access control and its enforcement in the Cloud.

The rest of the paper is organized as follows. In section 2, we present access control mechanism for social network (SN). In section 3, the ontology-based delegation mechanism and its enforcement is presented.

[*] PhD advisors: Alexandre Viejo and David Sánchez

2 Access Control Mechanism for Social Network

Online Social networks such as Twitter, Facebook, Google+, Myspace etc, are platforms where people interact with each other by publishing messages. Very frequently, the published content may contain sensitive data such as date of birth, political views, religious views, medical-related information or others. Publicly shared content containing that sensitive information can be easily revealed by means of messages, profile data or social apps (like games). Therefore, in order to protect such sensitive information is a challenging task.

The scientific community has proposed some access control solutions for social networks (Masoumzadeh et al [1] & Carminati et al. [2]) that take into consideration the type of resources to be protected (e.g., photos, videos, wall messages, etc.) before allowing/rejecting an access request. These methods rely on ad-hoc structures (i.e., application ontologies) to provide a preliminary modeling of resources. In order to manage the access control, the users or the SN administrators need to define access control rules for each resource type. The proposed solutions bear some limitations. On one hand, the classification of resources is coarse grained, fixed and rigid. Similarly, access control policies are applied as a whole on the object or resource, regardless of their actual contents or sensitiveness. As a result, the access to the resource is binary, that is, complete access or complete restriction. For example, if a user declares WallMessages as private for a special group of friends, all published messages will be hidden from that category of friends, regardless the messages contain any sensitive information or not. Furthermore, it is usually difficult for the users to configure the access control policies, since they may not be familiar with such notations and privacy issues.

In order to address the limitations introduced above, in this paper, we present a new scheme to enforce access control over resources published in social networks. We next summarize the main contributions of our work:

- We propose a transparent, dynamic and privacy-driven access control mechanism. Privacy is ensured by automatically protecting the content of messages to be published according to the privacy requirements of the publishers. The privacy requirements are defined by stating the type of information and the level of detail that is allowed to be accessed by each type of publisher's contact within the SN. Contrary to access control policies defined over specific resources, such requirements are only defined once in a generic way and can be intuitively stated. Moreover, the user does not need to have a priori privacy notions.
- Contrary to related works, privacy assessment is performed by semantically analyzing the contents to be published in an automatic way. Moreover, instead of evaluating the privacy for a resource (e.g. a publication) as a whole, our approach examines the privacy risk of each part of the resource individually (i.e. each textual term in a message).

- The semantics that drive the privacy assessment are gathered by means of an automatic semantic annotation process, which relies on available knowledge bases (i.e. DBPedia) and several linguistic tools.
- In contrast to the binary access control policies proposed by other researchers (which just completely allow or deny the access to a resource), our access control enforcement provides each type of reader with a sanitized version of the original publication that is coherent with the privacy requirements specified by the publisher for that type of reader. The different sanitized versions are semantically coherent with regard to the original publication, and are created automatically according to the semantic annotation process and the privacy risk assessment.

3 Ontology-based Delegation Mechanism and its Enforcement in the Cloud

Cloud computing has attracted many business organizations and end users (or tenants) due to its minimal management efforts, maintenance cost and ubiquitous access of outsourced resources, which can be hardware or software [7]. In a multi-tenant environment (i.e. a single resource shared with multiple users), access control management on shared services is a serious concern for Cloud service providers (CSPs) [5]. To handle this situation, one of the solutions implemented by the CSPs is delegation of access control. With delegation, a CSP (in this case called delegator) can transfer its administrative privileges on a particular service to other tenants that are called delegatees.

Due to heterogeneity of the Cloud federation [6] (a cloud environment where CSPs share cloud resources to other service providers) and the lack of trust, the delegation of access rights can be a serious concern for end-to-end authorization and verification of the delegators [4]. We next summarize the main contributions of our work:

- We propose an ontology that models the entities involved in the delegation process in Cloud scenarios, which includes subjects (i.e., delegators or delegatees), objects (resources or services), policies (document that translate delegated privileges) and their interrelations. This ontology facilitates to keep a track of who is delegating, what privileges on a resource are being delegated and also provides an intuitive solution to verify the attributes of the actors involved in the delegation.
- We present a distributed delegation model for the Cloud by classifying its main actors (e.g. cloud providers, CSPs, organizations and users) into different delegation levels, wherein the access rights on the resources can be delegated in a distributed way. In contrast to related solutions, the delegation of access rights are managed in a distributed way and the authenticity of the delegation policy is verified with the trusted policy that is written and signed by the CSP (which is the owner of the resource).

- In contrast to the methods that verify delegator's authority through roles (as done by other solutions), our system automatically verifies the authority through the attributes of the Cloud entities and the policy of the delegator by following the interrelations of the entities (represented as instances of the ontology), within in the Cloud levels, which leads to the trusted policy.
- Contrary to related work, our system does not require the specification of rules for delegation enforcement, but it automatically enforces delegation, verifies the delegated authority and also revokes the delegated privileges by using simple algorithms. In addition, we do not require any additional rules to implement delegated policies, instead, it automatically implements a delegated policy by applying a policy combining algorithm that combines the normal access policy and the delegated policy. Moreover, this algorithm resolves possible policy conflicts within the Cloud entities occurred at any level of the Cloud.

Acknowledgement. This work was partly supported by the European Commission under FP7 project Inter-Trust, by the H2020 project CLARUS. The author is a Martí-Franquès grantholder at the Universitat Rovira i Virgili (Tarragona, Spain).

References

[1] A. Masoumzadeh, J. Joshi. Anontology-based access control model for social networking systems. *IEEE Social Computing (SocialCom).*, 751 – 759, (2010).

[2] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, B.M. Thuraisingham. Semantic web-based social network access control. *Computers & Security.*, 30(2-3), 108-115, (2011).

[3] Ferraiolo, D.F., Kuhn, R.D., Chandramouli, R. Role-Based Access Control. *Artech House, Inc.*, Second Edition, (2007).

[4] K. Nahrstedt, R. Campbell. NSF Workshop on Security for Cloud Computing (Report). *National Science Foundation (NSF).*,(2012).

[5] S.S. Manvi, G. Krishna Shyam. Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey. *Journal of Network and Computer Applications.*, 41, 424-440, (2014).

[6] T. Kurze, M. Klemsy, D. Bermbachy, A. Lenkz, S. Taiy, M. Kunze. Cloud Federation. *2nd International Conference on Cloud Computing , GRIDs, and Virtualization.*, pp. 32-38, (2011).

[7] Y. Younis A, K. Kifayat, M. Merabti. An access control model for cloud computing. *Journal of Information Security and Applications.*, 19, 45-60, (2014).

CLARUS: User-Centered Privacy and Security in the Cloud

Jordi Ribes González [*]

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
jordi.ribesg@estudiants.urv.cat

Abstract. In the context of cloud computing, the issue of securing outsourced data against semi-trusted cloud service providers has seen a growing interest in recent years. The CLARUS project seeks to develop a framework that provides cloud users with adequate security measures in this setting. We present the cryptographic techniques applied on the CLARUS framework.

1 Introduction

Over the past few years, cloud computing has seen tremendous growth. Data outsourcing allows data owners to remotely access massively scalable data storage, usually reducing costs and improving availability and performance.

While migrating to the cloud can indeed bring great benefits to data owners and users, it also introduces several security and privacy concerns apart from the traditional ones.

Consider for instance a scenario concerning e-health. Outsourcing medical data offers many advantages, such as cheap storage of large data files and distributed access to this data through the Internet. Nevertheless, the sensitive nature of medical data makes data outsourcing a high-risk option if no proper security guarantees are taken. Another scenario is the publication of geo-referenced data on the Internet. Many institutions and organizations are in charge of big amounts of geo-referenced data that may be judged sensitive, for instance because of its high business potential or its private nature. Application cases include environmental data, mission-critical data, personal location data and consumer related statistics. There is high interest in outsourcing this large volume of data while preserving its functionality, but security concerns are indeed an obstacle in this task.

The main perceived threat in data outsourcing is that the security mechanisms offered by cloud service providers are usually located within the cloud

[*] PhD advisor: Oriol Farràs Ventura

platform, and the cloud service provider has full access over the possibly sensitive data. This compels users to completely trust in cloud service providers, agree with their privacy policies and rely on the security measures they may apply.

In this sense, it would be desirable to provide the user with security measures against non-trusted or semi-trusted cloud service providers. This would benefit both end users and cloud service providers, as enhancing trust in cloud storage would clearly foster the migration to cloud architectures.

2 CLARUS

CLARUS: User-Centered Privacy and Security in the Cloud is a project aiming to develop a framework to assure secure storage and processing of data outsourced to the cloud in the face of semi-trusted cloud service provider.

The solution will be implemented in the form of a dedicated proxy between the user and the cloud. This proxy is assumed to be deployed in a domain trusted by the user. It will be completely transparent to the user, and provide all necessary privacy and security techniques to allow the user to securely store, process and audit outsourced data.

2.1 Cryptographic techniques

Regarding cryptographic techniques, in some cases privacy risks may force data owners to encrypt part of their outsourced data.

Nevertheless, providing user-centered encryption techniques in the cloud computing setting is not a trivial task. The main reason is that, to the end of taking advantage of cloud architectures, functionalities such as searching, ordering or computing statistics are normally delegated to the cloud.

Therefore, end-to-end encryption techniques should still allow the desired functionalities to be carried out on encrypted data, all with the appropriate security guarantees and without weakening the performance and cost-saving benefits of cloud architectures.

There exist a variety of cryptographic techniques fitting the CLARUS setting ([1], [2], [3], [4], [5], [6], [7]), depending on the functionality to be preserved. For example, Searchable Encryption schemes give the user the ability to delegate search capabilities on encrypted data. Another cryptographic tool is Attribute-Based Encryption, which provides access control on data decryption. Finally, Homomorphic Encryption permits computations to be carried out on the ciphertext, thus allowing the user to take advantage of the cloud computational power without revealing the computed data to the cloud service provider.

In this talk we survey the specific cryptographic techniques applied in the CLARUS framework.

Acknowledgement. This work is partly supported by the European Commission under the H2020 project "CLARUS", ref. H2020-ICT-2014-1-644024.

References

[1] E. O. Blass, R. Di Pietro, R. Molva, and M. Önen: PRISM: privacy-preserving search in mapreduce. In Proceedings of the 12th international conference on Privacy Enhancing Technologies (PETS'12). Springer-Verlag, Berlin, Heidelberg, 180-200 (2012).

[2] D. Boneh, G. Crescenzo, R. Ostrovsky, G. Persiano: Public Key Encryption with Keyword Search. EUROCRYPT 2004. LNCS, vol. 3027, pp. 506-522. Springer, Heidelberg (2004).

[3] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky: Searchable symmetric encryption: Improved definitions and efficient constructions. J. Comput. Secur. 19, 5, 895-934 (2011).

[4] K. Elkhiyaoui, M. Önen, R. Molva: Privacy preserving delegated word-search in the cloud, SECRYPT - 11th International conference on Security and Cryptography, 28-30 (2014).

[5] R. Ostrovsky. 1990. Efficient computation on oblivious RAMs. In Proceedings of the twenty-second annual ACM symposium on Theory of computing (STOC '90). ACM, New York, NY, USA, 514-523 (1990).

[6] R. Ostrovsky, W. E. Skeith: A survey of single-database private information retrieval: techniques and applications. In Proceedings of the 10th international conference on Practice and theory in public-key cryptography (PKC'07). Springer-Verlag, Berlin, Heidelberg, 393-411 (2007).

[7] D. X. Song, D. Wagner, A. Perrig: Practical Techniques for Searches on Encrypted Data. In Proceedings of the 2000 IEEE Symposium on Security and Privacy (SP '00). IEEE Computer Society, Washington, DC, USA, 44-, (2000).

Co-Utility in Crowd-Based Business Model

Abeba Nigussie Turi [*] [**]

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
abebanigussie.turi@urv.cat

1 Abstract

We analyze the application of the notion of co-utility, a new concept describing self-enforcing and mutually beneficial interactions among self-interested agents, to the crowd-based business model. Based on the definition of co-utility amenable games, we show that the crowd sourcing e-market is naturally co-utile without additional incentives. Furthermore, we analyze the equity crowdfunding industry and propose solutions that can neutralize the fear and mistrust effects underlying its market in order to make it strictly co-utile.

The core idea behind this novel concept of Co-Utility and analysis is to design interaction protocols among agents that consulate their selfish and rational choices with societal welfare. With the current global trend of organized mutual interdependency, co-utility is especially timely. Hence, in this paper, we aim at applying this concept to two well-known crowd based business models: crowdfunding and crowdsoursing. This is the first analysis of these business models within the framework of co-utility and promise to open new way of analyzing various interactions between different agents having diverse interests and complementary goals.

This paper contributes to the literature of crowd-based business models with its analysis through the novel concept of co-utility, which has a potential for extension to other co-utility amenable games beyond these business models. We considered uniform distribution of returns and classical negative exponential utility functions for the analysis of equity crowdfunding. In addition, we took a reputation-based incentive mechanism, while there might be some other possible incentive schemes that can also ensure a safe transaction by changing the rules of the game. Hence, directions for future modeling would be: i) to consider other distributions of returns; ii) to consider other forms of risk-avert investors' utility functions

[*] PhD advisor: Josep Domingo Ferrer

[**] Other collaborators: Sánchez D., Osmani D.

with modifications of the underlying assumptions; and iii) to allow for other possible incentive schemes that can help to design a co-utile protocol for the market.

Furthermore, our analysis of the crowdfunding market is limited to equity crowdfunding. Other forms of crowdfunding, like donation-based crowdfunding, are clearly different and require a different analysis that can capture the motivations of donors and project owners under the general umbrella of co-utility.

Co-utility based analysis could be extended to other systems in the collaborative economy, albeit it requires case-specific incentive schemes capturing the dynamics of each system. For instance, in the games that incorporate some element of competition between the players, changing the rules of the game requires a different analysis.

Additional future directions of our work include extending the application of co-utility to other potential co-utility amenable games in the collaborative economy and also tackling other scenarios like international environmental agreements, self-enforcing antitrust cases, trans-boundary water issues, tax policies, etc.

Co-Utility

In a recent work, Domingo et al. (2015), defined a *co-utility amenable game* as a sequential Bayesian game G for n agents such that the utility of any agent is independent of the types of the other agents, i.e., $\forall i, j$ with $i \neq j$ and $\forall t_i, t'_i \in T_i$ one has $u_j(s_1, \ldots, s_n, t_1, \ldots, t_i, \ldots, t_n) = u_j(s_1, \ldots, s_n, t_1, \ldots, t_i, \ldots, t_n)$, where $(s_1, \ldots, s_n)$ is the strategy profile of agents, T_i is the set of types of agent i, and u_j is the utility for agent j.

2 Case Study I: Crowdsourcing

Given a crowdsourcing platform and a vector U of agent utility functions, there exists a co-utile protocol with respect to U, which is mutually beneficial for worker and requester irrespective of their individual interest. Co-utility in this market is viable provided that the goals of requester and worker are complementary and the qualification type of the worker matches the task. Based on this specification, we define the respective utility function for each agent as follows.

1. *Worker's utility function*
   The utility worker i gets by performing task T through crowdsourcing is given by:

$$U_i(T, e) = f_i(T)[\alpha_i r_i(e) - c_i(T, e)]$$

Where, the actions available to the worker are to participate or not to participate; $f_i(T)$ is a binary function that specifies whether or not task T matches worker i's interest and qualifications (ability); $f_i(T) = 0$ means worker is not interested or not qualified to perform the task; $f_i(T) = 0$ if worker i is qualified and willing to exert effort towards this specific task. $e =$ Level of effort to perform the task; $r_i(e) =$ Expected reward to worker i for effort e; α_i is a weight variable reflecting how much the individual values the reward; $c_i(T, e) =$ Task-specific cost of effort to worker i (it can take the form of time devoted to reading, understanding and performing the task, expenses incurred to perform the task, etc.). Given the utility function and the rationality assumption, worker participates in the crowdsourcing market if $u_i(T, e) > 0$ and $u_i(T, e) > u_i(l)$, where l stands for leisure; otherwise he refuses the offer and does not participate.

2. *R*equester's utility function

   Consider the monetary reward-based crowdsourcing. The goal of the requester is to maximize her expected utility, $\max u(\pi)$. The available actions for the requester are to request to the crowd or not to request (and rely on a traditional employee). The utility function of requester j can be formulated as:

   $$u_j = u_j(y, w_j, \mathrm{Crd}, \mu_j, T) = \alpha_j(y - w_j\mathrm{Crd} - \mu_j(T))$$

   Where, α_j is a weight variable reflecting how much the requester values the overall gain from the output; $\mu(T)$ is the minimum threshold she expects to gain from the task accomplishment; y stands for the total output by the crowd workers; Crd stands for the crowd labor supply; w_j is the per task pay offered by requester j.A rational requester who wants a task T to be performed will post the task to the anonymous crowd only if $u_j(y, w_j, \mathrm{Crd}, \mu_j, T) > 0$.

3 Case Study II: Equity Crowdfunding

Assume that an entrepreneur has a creative project to be posted on one of the online platforms for crowdfunding. Let us further consider the following assumptions:

1. Being the owner of the project, the entrepreneur has much more information about her investment project (return, actual output, risk, actions of the entrepreneur, etc.) than the potential crowd investors.
2. The investor incurs a verification cost α to gather enough information on the project details to make an investment decision; this verification cost is assumed to be compensated by the entrepreneur (see Romer 2011).
3. The project financing wholly relies on crowdfunding (as a special case of Romer's financial markets imperfections analysis, we here assume the

entrepreneur's wealth invested in this project is zero) and has an expected output of Γ, which might be different from the actual output, y.

4. There is large number of crowd investors and there exists competition among them.
5. The investors are risk-averse and their investment decision takes in to account the interest rate, r, which will give them a choice to either invest in a safe asset or undertake the project investment.
6. Entrepreneurs in online platforms also are risk-averse towards publicizing creative project ideas/products to the anonymous crowd for fear of being copied.

Apart from the net return based investment decisions, some other factors might discourage the participation of each agent in the industry. One of the main deterring factors is mistrust by funders regarding possible frauds. Funders want to be sure that their investment goes to the right project and they want to be guaranteed the promised return. From the entrepreneur's point of view, *fear of failure*, *imitation* or *plagiarism with full content disclosure* (loss of intellectual property) are deterring factors for crowdfunded ventures. This element of fear on the side of the entrepreneurs affects the extent they could freely signal quality and preparedness of their project idea to the general public. As a result, the entrepreneur faces a trade-off between a need of raising capital and threat of their idea being copied by other market participants (Pazowski et al. 2014).

The utility function for crowd investor i, u_i, accounting for the mistrust effect, assuming a negative exponential utility function (fulfilling the properties of non-satiation and risk aversion) is defined as:

$$u_i(R,\Gamma) = \begin{cases} -e^{-\beta\Gamma R} & \text{for } \Gamma \neq 0 \\ 0 & \text{for } \Gamma = 0 \end{cases}$$

Where, $\beta > 0$ is the risk aversion factor, R stands for the return to investor, Γ is the variable for trust taking values in the interval between $[0,1]$ where the boundaries are defined as 1 (if the potential crowd investors completely trust the entrepreneur that the project rewards the expected return) and 0 (if the potential crowd investors do not trust the entrepreneur at all). Hence, with no trust on a given project (case $\Gamma = 0$), a potential investor does not take part in the crowdfunding of the project, because she obtains no utility from it.

Likewise, the utility function for entrepreneur, j, accounting for the *fear of disclosure effect* is defined as:

$$u_i(C,r,\gamma,V,F) = \begin{cases} -e^{-\beta F(\gamma-(1+r)C-\alpha-V)} & \text{for } F \neq 0 \\ 0 & \text{for } F = 0 \end{cases}$$

Where, C is the total invested amount, r stands for the interest rate, γ is the total output of the project, V is value of the project if sold to second party without being run by the project owner, F stands for the fear of content disclosure (loss of intellectual property or being copied), and it takes values between $[0, 1]$, where F is 1 if the entrepreneur can broadcast her project content with no fear of being copied by others and no other project-related fear (e.g. failure), and 0 if the entrepreneur is in complete fear of broadcasting her project content (there is no utility for her in broadcasting the project).

The incentive schemes proposed in this paper to neutralize the disclosure fear and trust effects arising in the market are: a reputation mechanism with a signaling effect on the general public and more specifically, through the head of a special interest group issuing a protection note on the members; and encryption of publicly posted projects with decentralized time stamps guaranteeing self-enforcing intellectual property protection. Therefore, with the mechanisms we propose here in this paper; neutralization of the fear of disclosure and mistrust effects ensures the equity crowdfunding market to be strictly co-utile to all involved in the market, regardless of their respective types and thus enhancing the crowd-based startup financing efficiency.

To sum up, given the online platforms facilitating the equity crowdfunding industry, and the artificial incentives we propose, there exists a co-utile protocol with respect to the respective utility functions of the agents which is mutually optimal at a predefined optimal debt contract through the convertible notes.

References

[1] Domingo-Ferrer J., Soria-Comas J., Ciobotaru O. (2015). Co-utility: self-enforcing protocols without coordination mechanisms. In 2015 International Conference on Industrial Engineering and Operations Management-IEOM 2015, IEEE.

[2] Mollick E. (2013). The dynamics of crowdfunding: an exploratory study. Journal of Business Venturing, 29(1):1–16.

[3] Pazowski P., Czudec W. (2014). Economic prospects and conditions of crowdfunding. In: Human Capital without Borders.

[4] International Conference Management Knowledge and Learning 2014, pp. 1079-1088. Portoroz, Slovenia.

[5] Romer D. (2011). Advanced Macroeconomics. New York: McGraw Hill.

[6] Slivkins A., Vaughan J. W. (2014). Online decision making in crowdsourcing markets: theoretical challenges. ACM SIGecom Exchanges, 12(2):4–23.

Breast cancer computer-aided diagnosis systems: analysis of breast tissues in mammograms and ultrasound images

Mohamed Abdel-Nasser [*]

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
mohamed.abdelnasser@urv.cat

1 Introduction

Breast cancer attacks women in their 40s. Based on a statistic in the European Union, breast cancer is the leading cause of cancer death in 2014 [5]. Early detection through screening with computer aided diagnosis (CAD) systems can help to reduce the fatalities. The causes of breast cancer are still unknown; however, there are several factors that can indicate the risk of breast cancer such as *age*, *family profile*, *genetics* and *breast density.* Mammographies are considered the most effective tool for early detection of breast cancer. Figure 1 shows an example for breast screening using a mammography and the appearance of breast cancer in the mammogram.

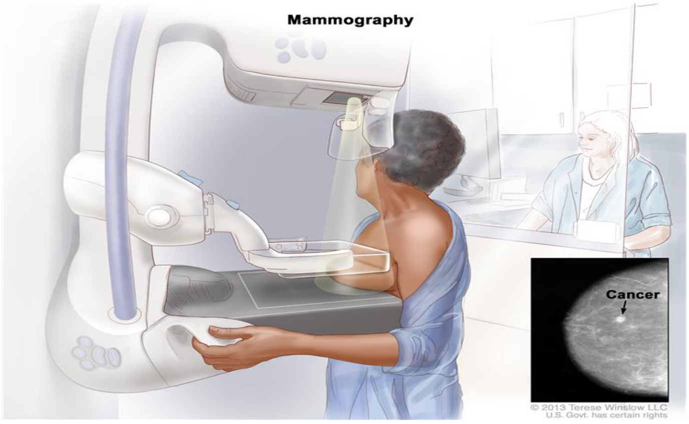


Fig. 1: Breast screening through mammography. Reprinted from: http://www.cancer.gov/types/breast/patient/breast-treatment-pdq

[*] PhD advisors: Dr. Antonio Moreno and Dr. Domenec Puig.

In a mammography, each breast is compressed using compression plates, and then X-rays are used to take images of breast tissue. A study in [4] showed that younger women usually have *denser breasts* than older women. *Dense* breasts have more glandular and fibrous tissues, and they appear white in the mammogram. Thus, they hide masses, which also usually appear white in mammograms. On the contrary, *fatty* tissues appear grey in mammograms.
Breast ultrasound (BUS) images are superior to mammograms in their ability to detect abnormalities in dense breasts. BUS is considered a complementary tool to mammograms in breast cancer detection. They cannot replace a mammogram for breast screening, but they can provide more information to physicians. Figure 2 shows breast tissues in a BUS image and a mammogram for the same breast.

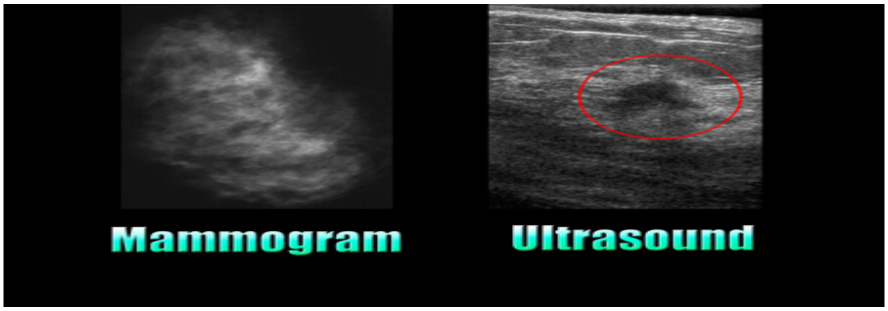


Fig. 2: A mammogram and BUS image for the same breast. Reprinted from: *http://www.thedoctorstv.com/articles/1442-procedures-you-need-to-know*

CAD systems are typically used to analyse mammograms in screening. They use several *machine learning*, *computer vision* and *image processing* techniques. A breast cancer CAD system consists of three main stages: *segmentation* of a region of interest (ROI) from the image, *feature extraction* from the ROI, and *classification.* The literature shows no consensus on the optimal feature set for breast tissue characterization. A poor description of the breast tissues leads to a high number of false positives (ROIs interpreted by a CAD system as abnormal cases when they are actually normal).
In our study, we focus on the feature extraction sub-task of a breast cancer CAD system, where we analyse breast cancer in both mammograms and BUS images. Although several feature extraction methods have been proposed for mammogram and BUS images analysis, improving the classification results remains a challenge. Texture analysis methods constitute one of the options for improving the performance of classification algorithms used in breast CAD systems. To that purpose, we analyse the performance of various texture analysis methods for breast mass classification aiming at reducing the number of *false positives.* Moreover, we propose novel descriptors.

2 Texture analysis for breast mass classification

2.1 Materials

In our experiments, we use several publicly available mammography databases such as mini-MIAS, DDSM and INbreast [6]. To analyse BUS images, we use a BUS database that was collected in UDIAT Diagnostic Centre of Sabadell (Spain).

2.2 Methods

We analyse the performance of several texture analysis methods for breast mass classification in mammograms and BUS images. We have selected widely used texture analysis methods such as local binary pattern (LBP), local directional number (LDN), histogram of oriented gradients (HOG), Gabor filters (GF) and Haralick's features (HAR). In addition, we used several classification methods such as k-nearest neighbour, linear discriminant analysis, linear support vector machines (LSVM), non-linear support vector machines (NLSVM), and random forests (RF). The performance of the CAD systems was measured in terms of the area under the curve (AUC) of the receiver operating curve (ROC), the sensitivity and the specificity. Our study is organized as follows.

1- Study of the performance of various texture analysis methods with breast mass classification in mammograms.
2- Study the effect of breast density on texture analysis for mass classification in mammograms.
3- Propose a fuzzy logic-based texture analysis method for breast mass detection in BUS images.

3 Results

In [1,2], we performed a twofold analysis. Firstly, we analysed the performance of several texture methods individually. As shown, LDN improved the results of well-known texture analysis methods like LBP, HOG, HAR or GF. It achieved a sensitivity of 84.0% with the KNN and a specificity of 99.0% with the LSVM. Secondly, we evaluated two feature combination techniques: the majority output of the individual classifiers and building new models on the concatenation of features provided by different texture methods. Among all combinations, $LDN + LBP$ gave the smallest percentage of false positives. It achieved a sensitivity of 92.0% with the NLSVM and a specificity of 96.5% with the RF.

In [3], we proposed the fuzzy local directional pattern (FLDP) for breast tissue characterization. It describes each pixel in a given ROI by its edge responses and makes use of fuzzy membership functions. The rationale behind the use of fuzzy logic is to compensate the uncertainty of the visual appearance of breast tissues due to noise, breast density and the variation in breast compressions. FLDP properly discriminates between mass and normal tissues in both dense and fatty breasts. We showed that the use of FLDP improved the classification results of breast tissues in BUS images when compared to some of the state-of-the-art descriptors such as LBP, HOG, LDN, HAR and GF. It achieved an AUC of 0.87 with the LSVM and 0.914 with the NLSVM.

4 Future work

The future work includes a study for breast tumour changes through several motion analysis methods. We will explore the use of the anatomical information in the breast region (nipple position, pectoral muscle, fatty and dense regions) to tune the results of motion analysis methods.

Acknowledgement. Mohamed Abdel-Nasser was awarded a Ph.D. grant from URV in 2013 (Martí Franquès program). Our work was partly supported by the Spanish Government through project TIN2012-37171-C02-02.

References

[1] Mohamed Abdel-Nasser, Antonio Moreno, and Domenec Puig. Towards cost reduction of breast cancer diagnosis using mammography texture analysis. *Journal of Experimental & Theoretical Artificial Intelligence*, 0(0):1–18, 2015.

[2] Mohamed Abdel-Nasser, Domenec Puig, and Antonio Moreno. Improvement of mass detection in breast X-ray images using texture analysis methods. In *Artificial Intelligence Research and Development: Recent Advances and Applications*, volume 269, pages 159–168. IOS Press, 2014.

[3] Mohamed Abdel-Nasser, Domenec Puig, Antonio Moreno, Adel Saleh, Joan Marti, Luis Martin, and Anna Magarolas. Breast tissue characterization in x-ray and ultrasound images using fuzzy local directional patterns and support vector machines. In *Proc. of the International Conference on Computer Vision Theory and Applications (VISAPP 2015)*, volume 1, pages 387–394, 2015.

[4] Karla Kerlikowske, Deborah Grady, John Barclay, Edward A Sickles, and Virginia Ernster. Effect of age, breast density, and family history on the sensitivity of first screening mammography. *Journal of the American Medical Association*, 276(1):33–38, 1996.

[5] M. Malvezzi, P. Bertuccio, F. Levi, C. La Vecchia, and E. Negri. European cancer mortality predictions for the year 2014. *Annals of Oncology*, 2014.

[6] Inês C Moreira, Igor Amaral, Inês Domingues, António Cardoso, Maria João Cardoso, and Jaime S Cardoso. Inbreast: toward a full-field digital mammographic database. *Academic radiology*, 19(2):236–248, 2012.

The local metric dimension of a graph from its primary subgraphs

Gabriel A. Barragán-Ramírez [⋆]

Departament d'Enginyeria Informàtica i Matemàtiques, Universitat Rovira i Virgili,
Av. Països Catalans 26, 43007 Tarragona, Spain.
gbrbcn@gmail.com

1 Introduction

Given a connected graph G, we define a *local metric generator* as a set of vertices such that given two adjacent vertices $u, v \in V(G)$ there is at least an element of this set, say w, for which we have $d_G(u, w) \neq d_G(v, w)$.

A local metric generator with minimum cardinality is called a *local metric basis* for G. The cardinality of the local metric basis is denoted by $\dim_l(G)$ and it is called the *local metric dimension* of G.

In this paper we show that the computation of the local metric dimension of a graph with cut vertices is reduced to the computation of the local metric dimension of the so-called primary subgraphs. The main results are applied to specific constructions including bouquets of graphs, block graphs and chain of graphs. We would point out that this work is an extended abstract of [1].

2 Main results

Let $G[\mathcal{H}]$ be a connected graph constructed from a family of pairwise disjoint (non-trivial) connected graphs $\mathcal{H} = \{G_1, ..., G_k\}$ as follows. Select a vertex of G_1, a vertex of G_2, and identify these two vertices. Then continue in this manner inductively. More precisely, suppose that we have already used $G_1, ..., G_i$ in the construction, where $2 \leq i \leq k-1$. Then select a vertex in the already constructed graph (which may in particular be one of the already selected vertices) and a vertex of G_{i+1}; we identify these two vertices. Note that any graph $G[\mathcal{H}]$ constructed in this way has a tree-like structure, the $G_i's$ being its building stones. (see Figure 1).

We will briefly say that $G[\mathcal{H}]$ is obtained by *point-attaching* from $G_1, ..., G_k$ and that $G_i's$ are the *primary subgraphs* of $G[\mathcal{H}]$. We will also say that the vertices of $G[\mathcal{H}]$ obtained by identifying two vertices of different primary subgraphs are the *attachment vertices* of $G[\mathcal{H}]$.

[⋆] PhD advisors: Juan Alberto Rodríguez, Carlos García

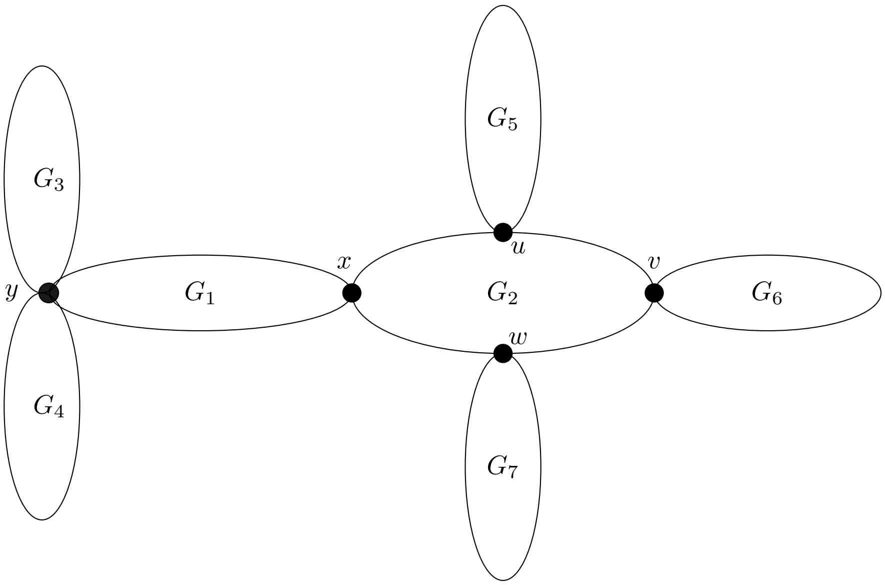


Fig. 1: A graph $G[\mathcal{H}]$ obtained by point-attaching from $\mathcal{H} = \{G_1, G_2, ..., G_7\}$

To begin with the study of the local metric dimension of $G[\mathcal{H}]$ we need some additional terminology. Given an attachment vertex x of $G[\mathcal{H}]$ and a primary subgraph G_j such that $x \in V(G_j)$, we define the subgraph $G_j(x^+)$ of $G[\mathcal{H}]$ as follows. We remove from $G[\mathcal{H}]$ all the edges connecting x with vertices in G_j, then $G_j(x^+)$ is the connected component which has x as a vertex.

Let $J_{\mathcal{H}} \subseteq [k]$ be the set of subscripts such that $j \in J_{\mathcal{H}}$ whenever G_j is a non-bipartite primary subgraph of $G[\mathcal{H}]$. Note that $J_{\mathcal{H}} = \emptyset$ if and only if $G[\mathcal{H}]$ is bipartite, *i.e.*, $J_{\mathcal{H}} = \emptyset$ if and only if $\dim_l(G[\mathcal{H}]) = 1$. From now on we assume that $J_{\mathcal{H}} \neq \emptyset$.

Now, let C_j be the set composed by attachment vertices of $G[\mathcal{H}]$ belonging to $V(G_j)$ such that $x \in C_j$ whenever $G_j(x^+)$ is not bipartite.

For any $j \in J_{\mathcal{H}}$ we define

$$\alpha_j = \max_{B \in \mathcal{B}(G_j)} \{|C_j \cap B|\},$$

where $\mathcal{B}(G_j)$ is the set of local metric bases of G_j, *i.e.*, α_j is the maximum cardinality of a set $\{x_1, x_2, ..., x_{\alpha_j}\} \subseteq V(G_j)$ composed by attachment vertices of $G[\mathcal{H}]$ belonging simultaneously to a local metric basis of G_j such that for every $l \in \{1, ..., \alpha_j\}$ the subgraph $G_j(x_l^+)$ is not bipartite.

Theorem 1. *For any non-bipartite graph $G[\mathcal{H}]$ obtained by point-attaching from a family of connected graphs $\mathcal{H} = \{G_1, ..., G_k\}$,*

$$\dim_l(G[\mathcal{H}]) \leq \sum_{j \in J_{\mathcal{H}}} (\dim_l(G_j) - \alpha_j).$$

Theorem 2. *Let $G[\mathcal{H}]$ be a non-bipartite graph obtained by point-attaching from a family of connected graphs $\mathcal{H} = \{G_1, ..., G_k\}$. If for each $j \in [k]$ it holds that any minimal local metric generator for G_j is minimum, then*

$$\dim_l(G[\mathcal{H}]) = \sum_{j\in J_{\mathcal{H}}} (\dim_l(G_j) - \alpha_j).$$

For any $j \in J_{\mathcal{H}}$ we define $\Gamma(G_j)$ as the family of local metric generators for G_j, and

$$\rho_j = \min_{S\subseteq V(G_j)} \{|S| : \; S \cup C_j \in \Gamma(G_j)\}.$$

Also, any set for which the above minimum is attained will be denoted by R_j.

Theorem 3. *For any non-bipartite graph $G[\mathcal{H}]$ obtained by point-attaching from a family of connected graphs $\mathcal{H} = \{G_1, ..., G_k\}$,*

$$\dim_l(G[\mathcal{H}]) = \sum_{j\in J_{\mathcal{H}}} \rho_j.$$

The remain sections of this article are devoted to derive some consequences of Theorem 3. We also give several families of graphs where the equality of Theorem 1 is achieved.

3 Block graphs

A *block graph* is a graph whose blocks are cliques. Since any block graph is obtained by point-attaching from $G_1 = K_{t_1}, G_2 = K_{t_2}, ..., G_k = K_{t_k}$, as a consequence of Theorem 3 we obtain a formula for the local metric dimension of any block graph. Our next result shows how the formula is reduced when every block has order $t_i \geq 3$.

Corollary 1. *Let $\mathcal{H} = \{G_1 = K_{t_1}, G_2 = K_{t_2}, ..., G_k = K_{t_k}\}$ be a finite sequence of pairwise disjoint complete graphs of order $t_i \geq 3$, $i = 1, ..., k$. Then for any block graph $G[\mathcal{H}]$,*

$$\dim_l(G[\mathcal{H}]) = \sum_{j=1}^{k} (t_j - 1 - \alpha_j).$$

In this case α_j becomes $t_j - 1$ if every vertex of K_{t_j} is a cut vertex of $G[\mathcal{H}]$ and it becomes the number of cut vertices of $G[\mathcal{H}]$ belonging to the clique K_{t_i} in otherwise.

4 Bouquet of graphs

Let $\mathcal{H} = \{G_1, G_2, ..., G_k\}$ be a finite sequence of pairwise disjoint connected graphs and let $x_i \in V(G_i)$. By definition, the *bouquet* $\mathcal{H}_x$ of the graphs in $\mathcal{H}$ with respect to the vertices $\{x_i\}_{i=1}^{k}$ is obtained by identifying the vertices $x_1, x_2, ..., x_k$ with a new vertex x. Clearly, the bouquet $\mathcal{H}_x$ is a graph obtained by point-attaching from $G_1, G_2, ..., G_k$. Therefore, as a consequence of Theorem 3 we obtain the following result.

Corollary 2. *Let $\mathcal{H} = \{G_1, G_2, ..., G_k\}$ be a finite sequence of pairwise disjoint connected graphs and let $x_i \in V(G_i)$ such that $J_{\mathcal{H}} \neq \emptyset$. If $\mathcal{H}_x$ is the bouquet obtained from $\mathcal{H}$ by identifying the vertices $x_1, x_2, ..., x_k$ with a new vertex x, then*

$$\dim_l(\mathcal{H}_x) = \sum_{j \in J_{\mathcal{H}}} (\dim_l(G_j) - \alpha_j).$$

Note that in this case $\alpha_i = 1$ if x_i belongs to a local metric basis of G_i and $\alpha_i = 0$ in otherwise.

5 Chain of graphs

Let $\mathcal{H} = \{G_1, G_2, ..., G_k\}$ be a finite sequence of pairwise disjoint connected non-trivial graphs and let $x_i, y_i \in V(G_i)$. By definition, the *chain* $\mathcal{C}(\mathcal{H})$ of the graphs in $\mathcal{H}$ with respect to the set of vertices $\{y_1, x_k\} \cup \left(\cup_{i=2}^{k-1} \{x_i, y_i\}\right)$ is the connected graph obtained by identifying the vertex y_i with the vertex x_{i+1} for $i \in [k-1]$. Clearly, the chain $\mathcal{C}(\mathcal{H})$ is a graph obtained by point-attaching from $G_1, G_2, ..., G_k$.

The formula for $\dim_l(\mathcal{C}(\mathcal{H}))$ is directly obtained from Theorem 3.

References

[1] Juan A. Rodríguez-Velázquez, Carlos García-Gómez and Gabriel Barragán-Ramírez, Computing the local metric dimension of a graph from the local metric dimension of primary subgraphs. International Journal of Computer Mathematics 92 (4) (2015) 686-693.

The k-adjacency dimension of graphs

Alejandro Estrada-Moreno [⋆] [⋆⋆]

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
alejandro.estrada@urv.cat

1 Introduction

A generator of a metric space (X, d) is a set $S \subset X$ of points in the space with the property that every point of X is uniquely determined by the distances from the elements of S. Given a simple and connected graph $G = (V, E)$, we consider the function $d_G : V \times V \to \mathbb{N} \cup \{0\}$, where $d_G(x, y)$ is the length of a shortest path between u and v and $\mathbb{N}$ is the set of positive integers. Then (V, d_G) is a metric space. A vertex $v \in V$ is said to *distinguish* two vertices x and y if $d_G(v, x) \neq d_G(v, y)$. A set $S \subset V$ is said to be a *metric generator* for G if any pair of vertices of G is distinguished by some element of S. A minimum cardinality metric generator is called a *metric basis*, and its cardinality the *metric dimension* of G, denoted by $\dim(G)$.

Uniquely determining the localization of an intruder in a network was the problem that motivated Slater in [7] to use the notion of metric dimension of a graph, where the metric generators were called *locating sets*. The concept of metric dimension of a graph was also introduced by Harary and Melter in [5], where metric generators were called *resolving sets*.

The concept of adjacency generator[3] was introduced by Jannesari and Omoomi in [6] as a tool to study the metric dimension of lexicographic product graphs. This concept has been studied further by Fernau and Rodríguez-Velázquez in [3,4] where they showed that the (local) metric dimension of the corona product of a graph of order n and some non-trivial graph H equals n times the (local) adjacency metric dimension of H. As a consequence of this strong relation they showed that the problem of computing the adjacency metric dimension is NP-hard. A set $S \subset V$ of vertices in a graph $G = (V, E)$ is said to be an *adjacency generator* for G if for every two vertices $x, y \in V - S$ there exists $s \in S$ such that s is adjacent to exactly one of x and y. A minimum cardinality adjacency generator is called an *adjacency basis* of G, and

[⋆] PhD advisors: I. G. Yero (UCA), J. A. Rodríguez-Velázquez (URV)

[⋆⋆] Other collaborators: Y. Ramírez Cruz (URV)

[3] Adjacency generators were called adjacency resolving sets in [6].

its cardinality the *adjacency dimension* of G, denoted by $\operatorname{adim}(G)$. Since any adjacency basis is a metric generator, $\dim(G) \leq \operatorname{adim}(G)$. Besides, for any connected graph G of diameter at most two, $\operatorname{adim}(G) = \dim(G)$. As pointed out in [3,4], any adjacency generator of a graph $G = (V, E)$ is also a metric generator in a suitably chosen metric space. Given the distance function $d_{G,2} : V \times V \to \mathbb{N} \cup \{0\}$, where

$$d_{G,2}(x, y) = \min\{d_G(x, y), 2\}.$$

Note that the metric dimension of $(V, d_{G,2})$ is equal to $\operatorname{adim}(G)$.

We introduced the concept of k-adjacency generator in [1,2]. We say that a set $S \subseteq V(G)$ is a *k-adjacency generator* for G if for every two vertices $x, y \in V(G)$, there exist at least k vertices $w_1, w_2, ..., w_k \in S$ such that

$$d_{G,2}(x, w_i) \neq d_{G,2}(y, w_i), \text{ for every } i \in \{1, ..., k\},$$

A minimum k-adjacency generator is called a *k-adjacency basis* of G and its cardinality, the *k-adjacency dimension* of G, is denoted by $\operatorname{adim}_k(G)$.

The general objective of our work is to study the problem of finding the k-adjacency dimension of a graph.

2 Some results on the *k*-adjacency dimension of graphs

In this section we present some results that allow us to compute the largest integer k' such that there exists a k'-adjacency basis, as well as, the k-adjacency dimension of several families of graphs. We also give some tight bounds on the k-adjacency dimension of a graph.

A graph G is said to be a *k-adjacency dimensional graph* if k is the largest integer such that there exists a k-adjacency basis. Given a connected graph G and two different vertices $x, y \in V(G)$, we denote by $\mathcal{C}_G(x, y)$ the set of vertices that distinguish the pair x, y with regard to the metric (1), *i.e.*, $\mathcal{C}_G(x, y) = \{z \in V(G) : \ d_{G,2}(z, y) \neq d_{G,2}(z, y)\}$. We define the following global parameter

$$\mathcal{C}(G) = \min_{x,y \in V(G)} \{|\mathcal{C}_G(x, y)|\}.$$

Theorem 1. [1] *A graph G is k-adjacency dimensional if and only if $k = \mathcal{C}(G)$. Moreover, $\mathcal{C}(G)$ can be computed in $O(n^3)$ time.*

The problem of computing the value k for which a given graph is k-adjacency dimensional is polynomial as we showed in Theorem 1. It was shown in [3,4] that the problem of finding the adjacency dimension of a graph is NP-complete. The NP-completeness of the problem of finding the k-adjacency dimension of a graph has not studied for $k > 1$. However, it is interesting to study this invariant for particular classes of graphs, specially for value of k greater than one.

We now present some results that allow us to compute the k-adjacency dimension of several families of graphs. We also give some tight bounds on the k-adjacency dimension of a graph.

Theorem 2 (Monotony of the k-adjacency dimension). [1] *Let G be a k-adjacency dimensional graph and let k_1, k_2 be two integers. If $1 \leq k_1 < k_2 \leq k$, then $\operatorname{adim}_{k_1}(G) < \operatorname{adim}_{k_2}(G)$.*

Corollary 1. [1] *Let G be a k-adjacency dimensional graph of order n.*

(i) (i) (i)

1. *For any $r \in \{2, ..., k\}$, $\operatorname{adim}_r(G) \geq \operatorname{adim}_{r-1}(G) + 1$.*
2. *For any $r \in \{1, ..., k\}$, $\operatorname{adim}_r(G) \geq \operatorname{adim}(G) + (r-1)$.*
3. *For any $r \in \{1, ..., k-1\}$, $\operatorname{adim}_r(G) < n$.*

Theorem 3. [1] *Let G be a k-adjacency dimensional graph of order $n \geq 2$. Then $\operatorname{adim}_k(G) = n$ if and only if $\mathcal{C}_k(G) = V(G)$.*

Since $\mathcal{C}_G(x, y) = \mathcal{C}_{\overline{G}}(x, y)$ for all $x, y \in V(G)$, we deduce the following result, which was previously observed for $k = 1$ by Jannesari and Omoomi in [6].

Observation 1 [1] *For any nontrivial graph G and $k \in \{1, 2, \ldots, \mathcal{C}(G)\}$,*

$$\operatorname{adim}_k(G) = \operatorname{adim}_k(\overline{G}).$$

Proposition 1. [1] *If G is a graph of order $n \geq 2$, then $\operatorname{adim}_k(G) = k$ if and only if $k \in \{1, 2\}$ and $G \in \{P_2, P_3, \overline{P}_2, \overline{P}_3\}$*

Theorem 4. [1] *For any graph G of order $n \geq 7$ and $k \in \{1, \ldots, \mathcal{C}(G)\}$, $\operatorname{adim}_k(G) \geq k + 2$.*

Observation 2 [1] *A graph G of order greater than or equal to four satisfies $\operatorname{adim}_3(G) = 4$ if and only if $G \in \{P_4, C_5\}$.*

Observation 3 [1] *A graph G of order $n \geq 5$ satisfies that $\operatorname{adim}_4(G) = 5$ if and only if $G \cong C_5$.*

The join $G+H$ of two vertex-disjoint graphs $G = (V_1, E_1)$ and $H = (V_2, E_2)$ is the graph with vertex set $V(G + H) = V_1 \cup V_2$ and edge set $E(G + H) = E_1 \cup E_2 \cup \{uv : u \in V_1, v \in V_2\}$.

Theorem 5. [1] *For any nontrivial graph H, the following assertions are equivalent:*

(i) (i) (i)

1. *There exists a k-adjacency basis A of H such that $|A - N_H(y)| \geq k$, for all $y \in V(H)$.*
2. *$\operatorname{adim}_k(K_1 + H) = \operatorname{adim}_k(H)$.*

Corollary 2. [1] *For any graph H of diameter $D(H) \geq 6$ and $k \in \{1, \ldots, \mathcal{C}(K_1+H)\}$, $\mathrm{adim}_k(K_1+H) = \mathrm{adim}_k(H)$.*

Corollary 3. [1] *Let H be a graph of girth $\mathsf{g}(H) \geq 5$ and minimum degree $\delta(H) \geq 3$. Then for any $k \in \{1, \ldots, \mathcal{C}(K_1+H)\}$, $\mathrm{adim}_k(K_1+H) = \mathrm{adim}_k(H)$.*

Theorem 6. [1] *Let G and H be two nontrivial graphs. Then the following assertions are equivalent:*

(i)

1. *There exists a k-adjacency basis A_G of G and a k-adjacency basis A_H of H such that $|(A_G - N_G(x)) \cup (A_H - N_H(y))| \geq k$, for all $x \in V(G)$ and $y \in V(H)$.*
2. $\mathrm{adim}_k(G+H) = \mathrm{adim}_k(G) + \mathrm{adim}_k(H)$.

Acknowledgement. Martí-Franquès Research grants Programme of Universitat Rovira i Virgili.

References

[1] A. Estrada-Moreno, Y. Ramírez-Cruz, J. A. Rodríguez-Velázquez, On the adjacency dimension of graphs, arXiv:1501.04647 [math.CO].

[2] A. Estrada-Moreno, I. G. Yero, J. A. Rodríguez-Velázquez, The k-metric dimension of the lexicographic product of graphs, Submitted.

[3] H. Fernau, J. A. Rodríguez-Velázquez, On the (adjacency) metric dimension of corona and strong product graphs and their local variants: combinatorial and computational results, arXiv:1309.2275 [math.CO].

[4] H. Fernau, J. A. Rodríguez-Velázquez, Notions of metric dimension of corona products: combinatorial and computational results, in: Computer science—theory and applications, vol. 8476 of Lecture Notes in Comput. Sci., Springer, Cham, 2014, pp. 153–166.

[5] F. Harary, R. A. Melter, On the metric dimension of a graph, Ars Combinatoria 2 (1976) 191–195.

[6] M. Jannesari, B. Omoomi, The metric dimension of the lexicographic product of graphs, Discrete Mathematics 312 (22) (2012) 3349–3356.

[7] P. J. Slater, Leaves of trees, Congressus Numerantium 14 (1975) 549–559.

Computability of the Simultaneous (Strong) Metric Dimension of a Graph Family

Yunior Ramírez-Cruz [⋆] [⋆⋆]

Departament d'Enginyeria Informàtica i Matemàtiques, Universitat Rovira i Virgili
Tarragona, Spain
yunior.ramirez@urv.cat

1 Definitions and general aims of our work

A generator of a metric space is a set S of points in the space with the property that every point of the space is uniquely determined by its distances from the elements of S. Given a simple and connected graph $G = (V, E)$, we consider the function $d_G : V \times V \rightarrow \mathbb{N}$, where $d_G(x, y)$ is the length of a shortest path between u and v and $\mathbb{N}$ is the set of non-negative integers. Clearly, (V, d_G) is a metric space. A vertex $v \in V$ is said to *distinguish* two vertices x and y if $d_G(v, x) \neq d_G(v, y)$. A set $S \subset V$ is said to be a *metric generator* for G if any pair of different vertices of G is distinguished by some element of S. A minimum metric generator is called a *metric basis*, and its cardinality the *metric dimension* of G, denoted by $\dim(G)$.

The concept of metric dimension of a graph was introduced by Slater in [10], where metric generators were called *locating sets*, and, independently, by Harary and Melter in [4], where metric generators were called *resolving sets.*

Now, we describe the navigation problem proposed in [6], where navigation was studied in a graph-structured framework in which a point robot moves from node to node of a "graph space". The robot can locate itself by the presence of distinctively labeled "landmark" nodes in the graph space. On a graph, there is neither the concept of direction nor that of visibility. Instead, it was assumed in [6] that a robot navigating on a graph can sense the distances to a set of landmarks. Evidently, if the robot knows its distances to a sufficiently large set of landmarks, its position on the graph is uniquely determined. This suggests the following problem: given a graph G, what is the smallest number of landmarks needed, and where should they be located, so that the distances to the landmarks uniquely determine the robot's position on G? The solution of this problem requires us to determine the metric dimension and a metric basis of G. In our work we consider the following extension of this problem.

[⋆] PhD advisors: Carlos García-Gómez(URV), Juan A. Rodríguez-Velázquez(URV)

[⋆⋆] Other collaborators: Ortrud R. Oellermann(UWinnipeg), Alejandro Estrada-Moreno(URV)

Suppose that the topology of the navigation network may change within a range of possible graphs, say $G_1, G_2, ..., G_k$. In this case, the aforementioned problem becomes that of determining the minimum cardinality of a set S which is a metric generator for each graph G_i, $i \in \{1, ..., k\}$. So, if S is a solution for this problem, then the position of each robot can be uniquely determined by the distance to the elements of S, regardless of the graph G_i that models the network at each moment.

Given a family $\mathcal{G} = \{G_1, G_2, ..., G_k\}$ of (not necessarily edge-disjoint) connected graphs $G_i = (V, E_i)$ on a common vertex set V (the union of whose edge sets is not necessarily the complete graph), we define in [8] a *simultaneous metric generator* for $\mathcal{G}$ as a set $S \subset V$ such that S is a metric generator for every $G_i \in \mathcal{G}$. We say that a minimum simultaneous metric generator for $\mathcal{G}$ is a *simultaneous metric basis* of $\mathcal{G}$, and its cardinality the *simultaneous metric dimension* of $\mathcal{G}$, denoted by $\mathrm{Sd}(\mathcal{G})$ or explicitly by $\mathrm{Sd}(G_1, G_2, ..., G_k)$. An example is shown in Figure 1, where $\{u_3, u_4\}$ is a simultaneous metric basis of $\{G_1, G_2, G_3\}$.

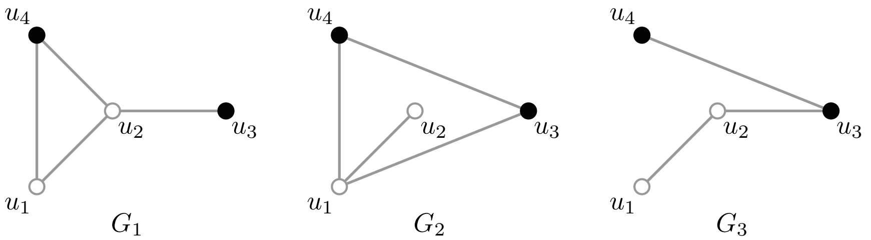


Fig. 1: The set $\{u_3, u_4\}$ is a simultaneous metric basis of $\{G_1, G_2, G_3\}$. Thus, $\mathrm{Sd}(G_1, G_2, G_3) = 2$.

Several variations on the concept of metric dimension have been studied. In our work, we pay special attention to the strong metric dimension. In a graph G, a vertex v is said to *strongly distinguish* two different vertices x and y if there exists a shortest $v - x$ path containing y or there exists a shortest $v - y$ path containing x, *i.e.* $d_G(v, x) = d_G(v, y) + d_G(x, y)$ or $d_G(v, y) = d_G(v, x) + d_G(x, y)$. A set $S \subset V$ is said to be a *strong metric generator* for $G = (V, E)$ (also *strong resolving set*) if any pair of different vertices of G is strongly distinguished by some element of S. A minimum strong metric generator is called a *strong metric basis*, and its cardinality the *strong metric dimension* of G, denoted by $\dim_s(G)$ [9]. Note that any strong metric generator for a graph G is also a metric generator.

We define in [2] a *simultaneous strong metric generator* for $\mathcal{G}$ as a set $S \subset V$ such that S is a strong metric generator for every $G_i \in \mathcal{G}$. We say that a minimum simultaneous strong metric generator for $\mathcal{G}$ is a *simultaneous strong metric basis* of $\mathcal{G}$, and its cardinality the *simultaneous strong metric dimension* of $\mathcal{G}$, denoted by $\mathrm{Sd}_s(\mathcal{G})$ or explicitly by $\mathrm{Sd}_s(G_1, G_2, ..., G_k)$.

To illustrate the relation between the simultaneous metric dimension and the simultaneous strong metric dimension, Figure 2 shows a graph family $\mathcal{G} = \{G_1, G_2\}$ where $\mathrm{Sd}(\mathcal{G}) = 4$, whereas $\mathrm{Sd}_s(\mathcal{G}) = 6$.

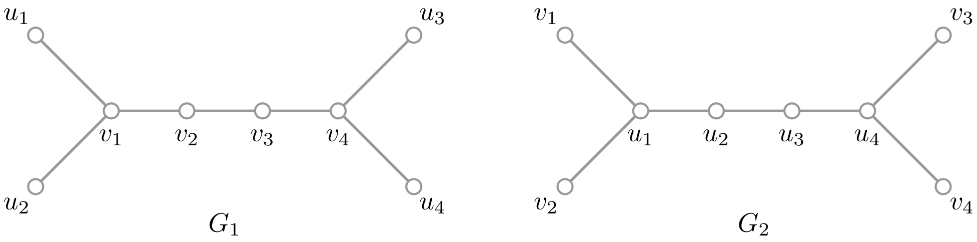


Fig. 2: The family $\mathcal{G} = \{G_1, G_2\}$ satisfies $\mathrm{Sd}(\mathcal{G}) = 4$ and $\mathrm{Sd}_s(\mathcal{G}) = 6$. For instance, the set $\{u_1, u_3, v_1, v_3\}$ is a simultaneous metric basis of $\mathcal{G}$, whereas the set $\{u_1, u_2, u_3, v_1, v_2, v_3\}$ is a simultaneous strong metric basis.

The general aim of our work is to investigate the properties of these types of simultaneous dimension, and related variants, as well as their relations.

2 A note on the computability of $\mathrm{Sd}(\mathcal{G})$ and $\mathrm{Sd}_s(\mathcal{G})$

It is proven in [6] that the problem of finding the metric dimension of a graph is NP-hard. Moreover, the NP-hardness of finding the strong metric dimension of a graph is proven in [7]. These problems are formally stated as decision problems as follows:

Metric Dimension (DIM) / Strong Metric Dimension (SDIM)
INSTANCE: A graph $G = (V, E)$ and an integer p, $1 \leq p \leq |V(G)| - 1$.
QUESTION: Is $\dim(G) \leq p$? / Is $\dim_s(G) \leq p$?

In an analogous manner, we define the decision problems associated to finding the simultaneous (strong) metric dimension of a graph family.

Simultaneous Metric Dimension (SD) / Simultaneous Strong Metric Dimension (SSD)
INSTANCE: A graph family $\mathcal{G} = \{G_1, G_2, \ldots, G_k\}$ on a common vertex set V and an integer p, $1 \leq p \leq |V| - 1$.
QUESTION: Is $\mathrm{Sd}(\mathcal{G}) \leq p$? / Is $\mathrm{Sd}_s(\mathcal{G}) \leq p$?

It is simple to see that determining whether a vertex set $S \subset V$, $|S| \leq p$, is a simultaneous (strong) metric generator for $\mathcal{G}$ can be done in polynomial time, so SD and SSD are in NP. Moreover, for any graph $G = (V, E)$ and any integer $1 \leq p \leq |V(G)| - 1$, the corresponding instance of DIM or SDIM can be transformed into an instance of SD or SSD, respectively, in polynomial time by making $\mathcal{G} = \{G\}$, so SD and SSD are NP-complete.

Beyond this trivial fact, we explore the manner in which the requirement of simultaneity makes computing the simultaneous (strong) metric dimension difficult, even for families composed by graphs whose individual (strong) metric dimension is easily computable. We focus on the case of families composed by trees, as $\dim(T)$ and $\dim_s(T)$ can be computed in polynomial time for any tree T [1,9]. We proved that SD and SSD are NP-complete for families composed by trees. In the case of SD, we showed in [8] a polynomial time transformation of the *Hitting Set Problem* (HSP), which was shown to be NP-complete by Karp [5], into SD.

Hitting Set Problem (HSP)
INSTANCE: A collection $\mathcal{C} = \{C_1, C_2, \ldots, C_k\}$ of non-empty subsets of a finite set S and a positive integer $p \leq |S|$.
QUESTION: Is there a subset $S' \subseteq S$ with $|S'| \leq p$ such that S' contains at least one element from each subset in $\mathcal{C}$?

It is known that HSP is NP-complete even if $|C_i| \leq 2$ for every $C_i \in \mathcal{C}$ [3]. We refer to this subcase of HSP as HSP2. To prove the NP-completeness of SSD, we showed in [2] a polynomial time transformation of HSP2 into SSD.

Acknowledgement. This work is supported by Martí-Franquès Predoctoral Research Grant 2013PMF–PIPF–25, from Universitat Rovira i Virgili.

References

[1] G. Chartrand, L. Eroh, M. A. Johnson, O. R. Oellermann. Resolvability in graphs and the metric dimension of a graph. *Discrete Applied Mathematics* 105(1-3):99–113, 2000.

[2] A. Estrada-Moreno, C. García-Gómez, Y. Ramírez-Cruz, J. A. Rodríguez-Velázquez. The simultaneous strong metric dimension of graph families. *Submitted*, arXiv:1504.04820 [math.CO].

[3] M. R. Garey, D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness.* W. H. Freeman & Co., New York, 1979.

[4] F. Harary, R. A. Melter. On the metric dimension of a graph. *Ars Combinatoria* 2:191–195, 1976.

[5] R. Karp. Reducibility among combinatorial problems. in *Complexity of Computer Computations*, Plenum Press, New York, 1972.

[6] S. Khuller, B. Raghavachari, A. Rosenfeld. Landmarks in graphs. *Discrete Applied Mathematics* 70(3):217–229, 1996.

[7] O. R. Oellermann, J. Peters-Fransen. The strong metric dimension of graphs and digraphs. *Discrete Applied Mathematics* 155(3):356–364, 2007.

[8] Y. Ramírez-Cruz, O. R. Oellermann, J. A. Rodríguez-Velázquez. The simultaneous metric dimension of graph families. *Discrete Applied Mathematics* (*to appear*), arXiv:1501.00565 [math.CO].

[9] A. Sebö, E. Tannier. On metric generators of graphs. *Mathematics of Operations Research* 29(2):383–393, 2004.

[10] P. J. Slater. Leaves of trees. *Congressus Numerantium* 14:549–559, 1975.

Object Recognition using Visual Attributes and Bayesian Network: Applied on Traffic Sign Recognition Problem

Elnaz Jahani Heravi [*]

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
elnaz.jahani@estudiants.urv.cat

1 Introduction

According to the World Health Organization, road traffic injuries caused an estimated 1.24 million deaths worldwide in the year 2010, slightly down from 1.26 million in 2000. That means one person is killed every 25 seconds. On the other hand, scientists of all fields help human to make a safe, happy and healthy life. Nowadays, computer science facilitates our life and affects it evidently. For instance, advanced driver assistance systems help drivers to have a safe and comfortable driving. There are many challenges such as lane departure warning system, recognition of horizontal signs on the road, traffic sign recognition, wrong way driving warning and lane change assistance in which an advanced driver assistance systems could help.

Traffic sign detection and recognition system is one of the indispensable parts of intelligent cars and it is composed of *detection* and *recognition* parts. The input of the detection part is the image of a scene and its output is the areas of the image where they contain a traffic sign. Then, the recognition module analyses these areas and recognizes the traffic signs.

One of the important characteristics of traffic signs is their simple design which helps the driver to detect and recognize them easily. Specifically, they have simple geometrical shape such as circle, triangle, polygon or rectangle and they are marked using basic colors such as red, green, blue, black, white and yellow that makes them distinguishable from most of objects in the scene. Finally, the meaning of a traffic sign is acquired using the pictograph in the center. Even though the design is clear and discriminative for a human, but there are challenging problems for detecting and recognizing traffic signs in real world applications such as shadow, camera distance, weather condition, perspective and age of the sign. Moreover, there could be some false-positive outputs from the detection stage that do not have to be fetched into the

[*] PhD advisor: Dr.Domenec Puig

recognition module. In other words, the recognition module must deal with the novel inputs that have not been observed during the training stage.

In general, most of the state of art works in traffic sign recognition have only tried to improve the classification accuracy on the limited number of traffic sign classes. Furthermore, none of the methods in the literature have tried to recognize traffic signs in a coarse to fine fashion. In general, there are some issues that should be considered in practical applications.

One of the issues is that most of the state of art methods are not scalable. In addition, the recognition module should be trained again if we add a new traffic sign to our dataset. On the other hand, by increasing the number of classes, it is likely some classes overlap in the feature space. Last not the least, all of theses methods do not take into account the novel inputs that the recognition stage may receive from the detection stage. In other words, all the methods will classify the false-positive results to one of the traffic sign classes.

In this work, we propose a coarse to fine method for recognizing a large number of traffic signs with ability to identify the novel inputs. In addition, adding a new class to the system requires to update a few models instead of the whole system. It should be noted that our goal is not to notably improve the numerical results of the state-of-art methods since the current performance is roughly $\sim 99\%$ but to propose a more scalable and applicable method with better performance which is also able to detect the novel inputs and provide some high level information about the any inputs.

To this end, we first perform a coarse classification on the input image using visual attributes and classify it into one of the abstract traffic sign categories. An abstract category contains some traffic signs with similar attributes. Then, a fine-grained classification is done on the signs of the detected category. However, because the attributes of a sign are detected using a one-versus-all classifier, it is possible that some attributes of the object are not detected and some irrelevant attributes are detected for the same sign. To deal with this problem, we take into account the correlation between the attributes as well as the uncertainty in the observations and build a Bayesian network. Next, we enter our observation to the Bayesian network and select the most probable explanation of the attributes. Finally, the refined attributes are used to find the category of the traffic sign or ascertain if it is a novel input.

2 Proposed Method

Traffic sign recognition is a multi-class classification problem with hundreds of classes. On the other hand, we are not able to collect real-world images for each class equally. Because there are some signs that we see them frequently such as “curve” signs compared with the “be aware of snow” sign. So, the collected dataset will be highly unbalanced. As a result, the accuracy of the classes with fewer images might decrease. To deal with this problem, the recognition

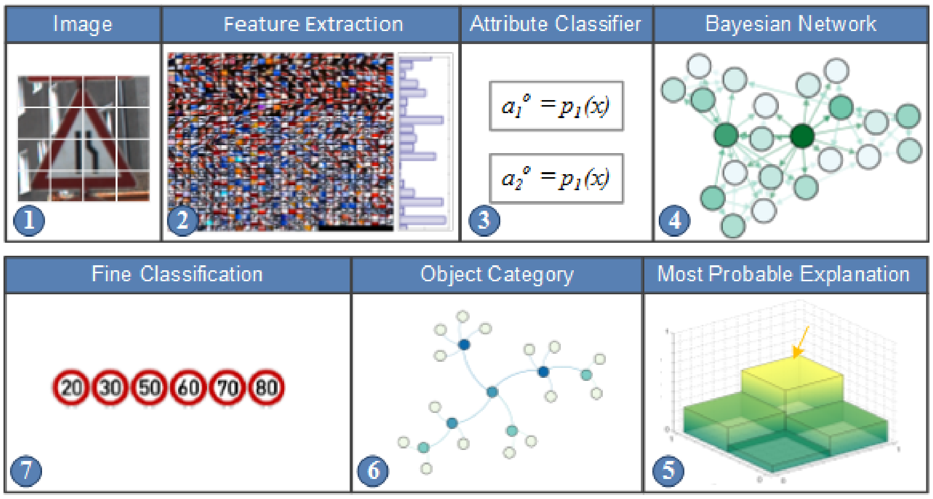


Fig. 1: Overview of the proposed method (best viewed in color).

model should be updated time to time. On the other hand, if we train only one model for all the traffic sign classes, retraining the recognition model will be time consuming. However, if we divide all the signs into some categories based on their attributes, then we might need to retrain the recognition models of the related category instead of retraining all the recognition models when we add a new traffic sign into our dataset.

From another perspective, temporal information plays an important role in human inference system. For example, if we observe the “no passing” sign at time t_1 we expect to see the “end of no passing zone”, at time t_2. Assume the sign “end of no passing zone” is impaired because of its age and it is hard to see its pictograph and the stripped crossing. In this case, if we follow the classification approaches that we mentioned in the previous section, the “end of no passing zone” sign can be incorrectly classified. However, if we provide some more abstract information such as “the input image has a circular shape with black-white color,” the traffic sign recognition system can infer that the image is related to the previously observed “no passing” sign. Hence, it probably indicates the “end of no passing zone” traffic sign.

In this work, we propose a coarse to fine classification approach using the semantic attributes of the object. Fig.1 shows the overview of the proposed method. In the first stage, the image is divided into several regions and each region is coded using a feature extraction method. Then, the feature vector is obtained by concatenating the locally pooled coded vectors. Next, the feature vector is individually applied on the attribute classifiers and the classification score of each attribute is computed. Finally, the certain state (*i.e.* absence or presence) of each attribute is estimated by plugging the scores into a Bayesian network (shown in Fig. 2) and calculating the most probable explanation of the attributes. In the next step, the category of the image is found using the attribute configuration. Having the sign category found, the fine-grained classifier of this category is used to do the final classification.

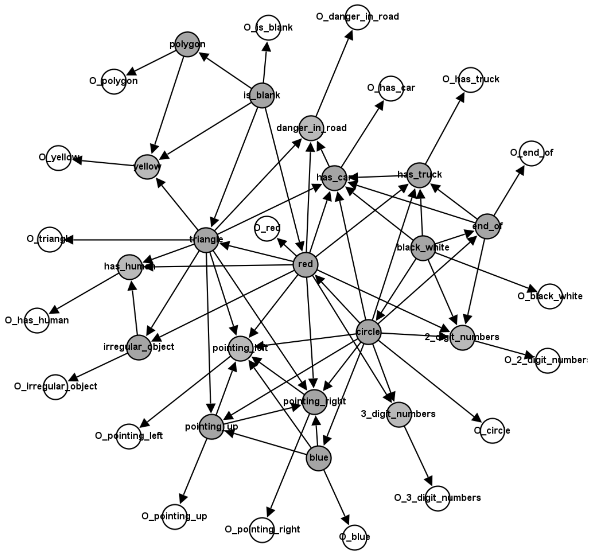


Fig. 2: The proposed Bayesian network for refining attributes.

References

[1] S.M. Bascón,J. A. Rodríguez, S. L. Arroyo, A.F.Caballero and F. Lopéz-Ferreras. An optimization on pictogram identification for the road-sign recognition task using SVMs. *Computer Vision and Image Understanding*, 114(3):373 – 383, 2010.

[2] K. Cheng and X. Tan. Sparse representations based attribute learning for flower classification. *Neurocomputing*, 145(0):416 – 426, 2014.

[3] S. Houben, J. Stallkamp, J. Salmen, M. Schlipsing and C.Igel. Detection of traffic signs in real-world images: The German Traffic Sign Detection Benchmark. *International Joint Conference on Neural Networks, number 1288*, 2013.

[4] S. Maldonado- Bascón, S. Lafuente-Arroyo, P. Gil-Jimenez, H. Gómez-Moreno and F. F. Lopéz-Ferreras. Road-sign detection and recognition based on support vector machines. *Intelligent Transportation Systems, IEEE Transactions on*8(2):264–278, 2007.

[5] F. Zaklouta and B. Stanciulescu. Warning traffic sign recognition using a HOG-based K-d tree. *Intelligent Vehicles Symposium (IV), IEEE*1019–1024, 2011.

[6] F. Zaklouta, B. Stanciulescu and O. Hamdoun. Traffic sign classification using K-d trees and Random Forests. *Neural Networks (IJCNN), The International Joint Conference on*2151–2155, 2011.

Using Humanoid Robots to Convey Rehabilitation Therapies to Disabled People

Jainendra Shukla [*]

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
jainendra.shukla@estudiants.urv.cat

1 Introduction

The thesis aims to develop a system to automatically create rehabilitation therapies for patients with disabilities (mental and physical), in the form of psycho-motor activities/games, dance or workout routines that incorporate the use of humanoid robots within the therapeutic loop by cloning human behavior learned by imitation. The objective of this research project is to implement a system that will be able to generate therapeutic routines from imitation of human actors and, also, objectively measure both the interaction between robot and the patients, as well as the effectiveness of these techniques on the patients.

1.1 Patients

The author is working on his PhD at URV with Ave Maria Foundation[2]. Ave Maria Foundation is the residential and clinical facility of the patients. These patients are individuals with profound and multiple learning disabilities (PMLD). Individuals with PMLD have more than one disability. One very important symptom is that they have profound learning disability. Generally they also have an associated medical condition which could be neurological, and physical or sensory impairments [1]. Due to all these conditions they require a constant general support.

1.2 Robot

The robot that will be used for this research is NAO NextGen (Model H25, Version 4). NAO is a 58 cm tall humanoid robot developed by Aldebaran[3].

The reasons to choose NAO for this research are as follows:

[*] PhD advisor: Prof. Domenec Puig

[2] Ave Maria Fundacio, http://www.avemariafundacio.org/inici.html

[3] Aldebaran, https://www.aldebaran.com/en

Fig. 1: NAO robot

1. Its small humanoid form and extreme interactivity makes it really endearing and lovable to the type of individuals in our study.
2. NAO can move, recognize objects and people, can hear and can even talk to individuals. These features makes it suitable for all the categories of clinical applications of interactive robots.
3. The size of NAO is as of human toddler, which is found to be most suitable for clinical applications of interactive robots [2].
4. NAO is easily and commercially available.

1.3 Why Robots

There is no medical cure available for individuals with such disabilities [3]. However, higher engagement rate has been reported by the use of humanoid robots among students with profound and multiple learning disabilities (PMLD) [6]. Many other researches also claim positive effects of using robots or robot like toys to increase interaction among individuals with intellectual disabilities [4,5].

This research is a small step towards the long-term goal of making a fully autonomous robotic system to encourage autonomy in life of individuals with PMLD.

2 Initial Ideas

The thesis is in the starting phase but some initial ideas are as follows:

1. Design of many interesting set of routines using a humanoid robot to unlock basic social and learning skills of people with disabilities in a comfortable and confident manner.
2. Use of different kind of sensors (e. g. RGB-D cameras, Stereo-vision cameras etc.) with humanoid robot NAO for a more human like interaction with disabled people.

3 Progress

Keeping above ideas in mind a small but significant step was taken to advance in this direction. Different types of activities were designed to observe the response of individuals with PMLD in different categories. Elder people with PMLD were included in the trails to analyze the effect of their interactions with the robot. The results were very exciting. An average improvement for the participants in all categories was observed as **47.79%** which indicates that robot interaction is effective to good extent. The result of this work surely suggests that robot interactions can be very helpful to improve the conditions of individuals with PMLD even at an elder age. Used in proper settings, robotic interactions can help to induce a target behavior, to teach and to encourage these individuals which can bring an autonomy to certain extent in their life.

Acknowledgement. This research work is supported by Industrial Doctorate program (Ref. ID.:2014-DI-022) of AGAUR, Government of Catalonia.

References

[1] Bellamy, G., Croot, L., Bush, A. et al. A study to define: profound and multiple learning disabilities (PMLD). *Journal of Intellectual Disabilities*, vol. 14, no. 3, pp. 221-235, 2010

[2] Giullian, N., Ricks, D., Atherton, A., Colton, M., Goodrich, M., Brinton, B. Detailed requirements for robots in autism therapy. *IEEE International Conference on Systems Man and Cybernetics (SMC)*, pp. 2595-2602, IEEE Press, New York, 2010

[3] Jose-Ramon Rueda, Javier Ballesteros, and Maria-Isabel Tejada. Systematic review of pharmacological treatments in fragile X syndrome. *BMC Neurology* , 9-53, 2009

[4] B. Robins, K. Dautenhahn, Te Boekhorst, and A. Billard. 2005. Robotic assistants in therapy and education of children with autism: can a small humanoid robot help encourage social interaction skills?. *Univers. Access Inf. Soc.* , Vol. 4, 2, 105-120, 2005

[5] Scassellati, B., Quantitative metrics of social response for autism diagnosis. *IEEE International Workshop on Robot and Human Interactive Communication*, pp.585,590, 13-15 Aug., 2005.

[6] Standen P., Brown D., Roscoe J., et. al. Engaging Students with Profound and Multiple Disabilities Using Humanoid Robots, *Universal Access in Human-Computer Interaction. Universal Access to Information and Knowledge*, LNCS, vol. 8514, pp. 419-430. Springer International Publishing, Heidelberg, 2014

Recommender Systems with Privacy for Context-Aware Services

Fran Casino [⋆]

SMART HEALTH Research Group. Department of Computer Engineering and Mathematics, Rovira i Virgili University.
Av. Països Catalans 26. 43007 Tarragona. Catalonia. Spain
Corresponding author e-mail: franciscojose.casino@urv.cat

1 Introduction

Automatic recommender systems have become a cornerstone of e-commerce, especially after the great welcome of *Web 2.0* based on participation and interaction of Internet users. Moreover, the new way to use and understand the network based on the *Web 3.0*, which enforces the user&computer interaction, leads recommender systems to another level, integrating them into everyday life in a transparent and efficient manner. Collaborative Filtering (CF) [7] is a recommender system that comprises a large family of recommendation methods. The aim of CF is to make suggestions on a set of items I (*e.g.* books, films or routes) based on the preferences of a set of users U that have already acquired and/or rated some of those items. Recommendations provided by CF methods are based on the premise that similar users are interested in similar items (*i.e* they share similar patterns). Therefore, items which pleased user u_a could be recommended to user u_b, if u_a and u_b are similar. In order to predict whether an item would interest a given user, CF methods rely on a matrix M of n users (rows) and m items (columns), where each matrix cell $M_{i,j}$ stores the rate of user i on item j. The interested reader could refer to [9] for detailed CF's state-of-the-art.

2 Recommender Systems and Context-Aware Services

Population is moving into cities and this urbanisation process poses severe challenges to cities. In big cities, factors related to economies of scale help to reduce operational costs. However, managing big cities is challenging due to the large number of inhabitants and their needs. Thus, the management procedures of cities have to be adapted to a growing and very demanding population. As a result of these needs, the concept of smart city was born. The

[⋆] PhD advisor: Agustí Solanas

cities of the future will be equipped with full of sensors and actuators (*e.g.* temperature and humidity sensors, pollution and allergens sensors, luminosity sensors or crowds detectors) that would improve the citizens' quality of life. One of the most challenging aspects within this framework is to achieve sustainable healthcare service provisioning, not only in the case of hospitalized patients, but also to monitor chronic diseases, improve social welfare and in general to improve the overall citizenship health levels. In this context, wireless communication systems play a key role, as enablers of real time and location independent connectivity, increasing system functionality and decreasing operational costs. As a result, the healthcare sector has turned into the aforementioned context to create a powerful symbiosis and create Smart Health [2], which is defined as *the provision of health services by using the context-aware network and sensing infrastructure of smart cities.*

2.1 Communication Networks and Collaborative Filtering

One of the issues to consider in the design of communication networks in the context of a Smart Health cenario is their performance in terms of coverage/capacity ratios, with particular consideration of the impact of interference due to simultaneous use of multiple users and systems. It is in this case where careful radiofrequency signal analysis, in terms of useful signal transmission and existence of potential interference levels must be estimated, as a function of user density, transceiver type and location (Figure 1). Wireless signal analysis in large complex scenarios is computationally costly and requires the use of optimized deterministic techniques, such as 3D Ray Launching (RL) and Ray Tracing approximations, coupled to Geometric Optics and Uniform Theory of Diffraction. In the case of very large scenarios, such as cities, this approach can still be computationally too demanding and combination with other estimation approaches is compulsory [8]. In order to minimize the computational cost for certain scenarios within the potential applications of Smart Health, we propose the combination of in-house developed 3D Ray Launching code with Collaborative Filtering techniques as showed in [3] and [4].

2.2 Healthcare and Collaborative Filtering

In our society, citizens perform physical activities in the city, namely cycling, jogging, running, etc. With the aim to promote these healthy habits, it would be desirable to count with a system that could dynamically adapt to the needs and tastes of the citizens. Within this context, we propose a new way of using the sensing capabilities of smart cities by means of recommender systems that allow citizens to obtain recommendations about the routes that better fit their capabilities.

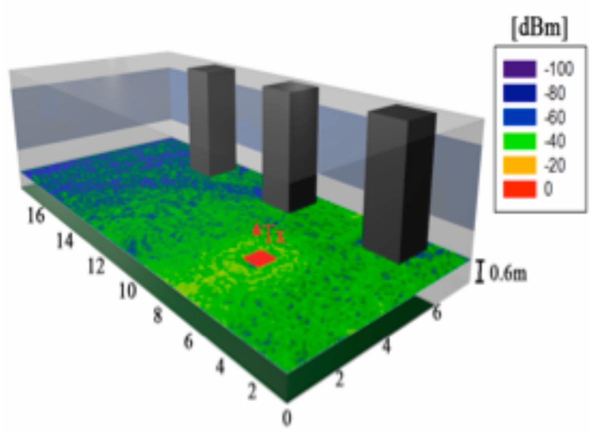


Fig. 1: Example of a scenario with received signal power estimations.

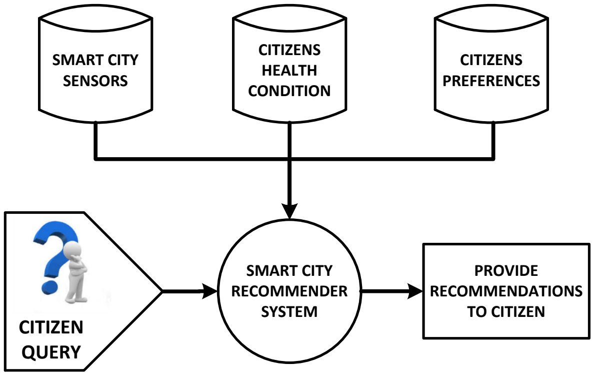

SMART CITY SENSORS
CITIZENS HEALTH CONDITION
CITIZENS PREFERENCES
CITIZEN QUERY
SMART CITY RECOMMENDER SYSTEM
PROVIDE RECOMMENDATIONS TO CITIZEN

Fig. 2: Overview and basic operation of a Smart Health recommender system.

The system would consider real-time constraints and information from several sources: (i) citizens' preferences, (ii) citizens' health conditions and, (iii) real-time information provided by the smart city infrastructure.

The architecture of our system and its main actors are shown in Figure 2. Sensors provide real-time environmental information (*e.g.* luminosity, temperature, humidity, pollution) to the Smart City Recommender System (SCRS) through the communication infrastructure of the smart city. Upon the reception of citizen queries the SCRS checks the health information of citizens and their preferences and cross them with the real-time information of the smart city sensors to finally compute real-time recommendations that are forwarded back to the citizens.

3 Privacy and Collaborative Filtering

The collection of private behavioural information in a wide variety of contexts (*e.g.* places to go, things to do, or products to buy), which conforms the basis of CF systems, provides great opportunities and benefits to both companies and users. However, the lack of privacy for the contributing users is a major drawback. Careless management of personal information, besides being agains the legislation of most countries, could lead to serious consequences for both users, whose information is stored, as well as companies. In order to address such privacy issues, current research focuses on Privacy Preserving Collaborative Filtering (PPCF) methods [6]. Users' privacy concerns affect their behaviour, resulting in a reduction of both the number of given assessments as well as their quality. The lack of privacy could also result in a massive information retrieval conducted by companies, which could acquire data of the preferences of many users in a given market, getting a big advantage over other competitors. Moreover, the existence of large monopolies on the Internet (Google, Amazon) allows for the sharing of data between different entities managed by large companies, without user's awareness. Whilst privacy preserving CF methods obfuscate and/or hide information on user profiles, sometimes users wish to find other users having similar profiles and form a community. Indeed, communities are very usual in the network, but they can be a double-edged sword. On the one hand, users can conveniently obtain reliable recommendations on items from communities in a particular context. On the other hand, communities can generate a *value homophily* problem in the network, so that recommendations outside the context of the community would give results with little sense, precisely because of the homogeneity of the group. For more on PPCF, we point the interested reader to [1], where a PPCF survey is presented and to [5], where a classification of PPCF methods is given according to how information is stored and how recommendations are computed.

4 Conclusions and Future Work

Collaborative Filtering is a recommender system used to perform automatic recommendations to users in multiple contexts. Despite the great advantages of using CF, we have highlighted its downside regarding users' privacy, which is probably the most significant challenge to overcome.

In addition, we have proposed the idea of using recommender systems integrated with the sensing infrastructure of smart cities to improve the sustainability by optimizing the resource usage in the communication networks field. Moreover, we have focused on the citizen's quality of life and proposed a method to provide citizens with real-time routes recommendations that take into account their health conditions and preferences.

Future work will focus in the implementation of new ontologies which could use more context-aware information to improve the citizen's quality of life while preserving their privacy.

Acknowledgments and disclaimer

This work is partly supported by La Caixa Foundation through Project SIMPATIC and the Spanish Ministry of Economy and Competitiveness under project 'Co-Privacy" "TIN2011-27076-C03-01", and by the Government of Catalonia under grant 2004-SGR-537. We would also like to thank our colleagues from the Electrical and Electronic Engineering Department of the Public University of Navarra who provided insight and expertise that greatly assisted the research presented in this paper.

References

[1] A. Bilge, C. Kaleli, I. Yakut, I. GunesS, and H. Polat, A survey of privacy-preserving collaborative filtering schemes, *International Journal of Software Engineering and Knowledge Engineering*, vol. 23, no. 08, pp. 1085-1108, 2013.

[2] A. Solanas, C. Patsakis, M. Conti, I. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. Pérez-Martínez, R. Di Pietro, D. Perrea and P.Martínez-Ballesté. Smart health: A context-aware health paradigm within smart cities. *IEEE Communications Magazine, Vol. 52, No. 8, pp. 74-81*, August. (2014).

[3] F. Casino, L. Azpilicueta, P. Lopéz-Iturri, E. Aguirre, F. Falcone, and A. Solanas, Optimized wireless channel characterization in large complex environments by hybrid ray launching collaborative filtering approach, *Tech. Rep.*, February 2015. [Online]. Available: http://s-health.eu/publications/technical_report_optimized_ray_launching.pdf

[4] F. Casino, L. Azpilicueta, P. Lopéz-Iturri, E. Aguirre, F. Falcone, and A. Solanas, Hybrid-based Optimization of Wireless Channel Characterization for Health Services in Medical Complex Environments. *IISA*, July. (2015). (In press).

[5] F. Casino, C. Patsakis, D. Puig, and A. Solanas, On privacy preserving collaborative filtering: Current trends, open problems, and new issues. *ICEBE*, pp. 244-249. (2013).

[6] F. Casino, J. Domingo-Ferrer, C. Patsakis, D. Puig, and A. Solanas, A k-anonymous approach to privacy preserving collaborative filtering, *Journal of Computer and System Sciences, Vol. 81, Issue. 6, pp. 1000-1011*, Dec. 2014.

[7] Goldberg, D., Nichols, D., Oki, B. M., Terry, D., Using collaborative filtering to weave an information tapestry. *Communications of the ACM*, 35(12), 61-70. (1992).

[8] L. Azpilicueta, M. Rawat, K. Rawat, F. Ghannouchi and F. Falcone, Convergence Analysis in Deterministic 3D Ray Launching Radio Channel Estimation in Complex Environments. *Applied Computational Electromagnetic Society Journal, Vol. 29, No. 4, pp. 256-271, April (2014)*

[9] Shi, Y., Larson, M., Hanjalic, A. Collaborative filtering beyond the user-item matrix: A survey of the state of the art and future challenges. *ACM Computing Surveys (CSUR)*, 47(1), 1-45. (2014).

Consensus Calculation of Multiple Input Correspondences

Carlos Francisco Moreno-Garcia *

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
carlosfrancisco.moreno@estudiants.urv.cat

1 Introduction

When several subjects decide to solve the assignment problem, differences on the points' mapping may occur. These differences appear due to several factors. For example, one of the subjects gives more importance to some of the point attributes than the rest. For instance, if the sets of points represent regions of segmented images, one subject can think the area is more important than the colour while another subject believes the opposite. If the assignment problem is solved by an artificial system, the fact of "believing" the area is more important than the colour is gauged by some weights. Another factor could be that the assignment problem is computed in a suboptimal algorithm, and different non-exact assignments can appear between two or more parties. In these scenarios, our system can intervene as a mediator that decides the final assignment as a consensus of all initial assignments. This is very important since it is very likely some discrepancies will appear, especially as the number of involved subjects increase.

1.1 Example

To better understand the scenario we intend to solve, let us introduce the following example: Figure 1 shows two images in which four different subjects identify different sets of points and correspondences. The salient points extractors and matching algorithms are: 1.a) SIFT extractor [6] and the Hungarian method [5]. 1.b) SURF extractor [1] and Hungarian method [5]. 1.c) Harris corners [3] and matchFeatures (MF) function from Matlab [7]. 1.d) SIFT extractor [6] and the PF-Registration Method [8],[9].

Each case represents a correspondence which is different to the rest; nevertheless we are able to identify common mappings between the cases. Additionally, all of the subjects' proposals contain mistaken mappings. Due to the

* PhD advisor: Francesc Serratosa

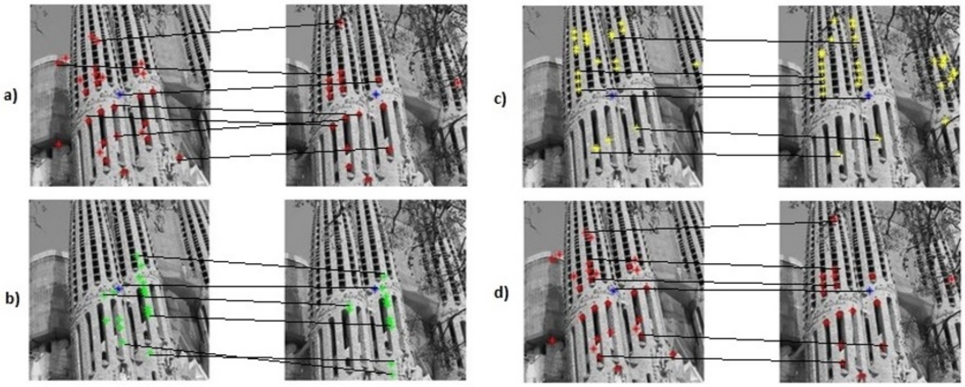


Fig. 1: Four possible salient point correspondences using different combinations of feature extractors and matching methods.

noisy nature of the errors, mistaken mappings tend to be non-repetitive. For this reason, if a consensus correspondence is defined, the final correspondence tends to have less mapping errors than the original ones

2 Basic Definitions

Suppose two sets of elements $A = (a_1, ..., a_n, a_{n+1}, ..., a_{n+m})$ and $A' = (a'_1, ..., a'_n, a'_{n+1}, ..., a'_{n+m})$ with order n+m must be matched. The distance between sets which delivers the minimum cost of all the correspondences is defined as

$$ds(A, A') = min_{\forall f:AxA'}(Cost(A, A', f)) \tag{1}$$

We define the cost of this correspondence as the addition of individual element costs in a similar way as in the Graph Edit Distance [8],

$$Cost(A, A', f) = \Sigma_{i=1}^{n+m} c(a_i, a'_i) \tag{2}$$

The correspondence that obtains this distance is known as the optimal correspondence f^* , and it is defined as

$$f^* = argmin_{\forall f:AxA'} Cost(A, A', f) \tag{3}$$

Separately, the Hamming distance between two correspondences is the number of element mappings that do not have the same codomain. Assume f^k and f^t are two bijective correspondences between sets A and A' . We define the Hamming distance between f^k and f^t as

$$d_H(f^k, f^t) = \Sigma_{i=1}^{n+m}(1 - \delta(a'_x, a'_y)) \tag{4}$$

being x and y such that $f^k(a_i) = a'_x$ and $f^t(a_i) = a'_y$. Function δ is the well-known Kronecker Delta.

3 Method

We propose a standard minimisation approach that aims to find an optimal element e^* that globally minimises a specific function. Usually, this function is composed of an empirical risk $\bigtriangledown(e)$ plus a regularization term $\Omega(e)$ weighted by a parameter λ [13]. The empirical risk is the function to be minimised per see, and the regularisation term is a mathematical mechanism to impose some restrictions. Parameter λ weights how much these restrictions have to be imposed.

$$e^* = argmin_{\forall e} \lambda \cdot \bigtriangledown(e) + (1 - \lambda) \cdot \Omega(e) \tag{5}$$

To find an approximation of the mean correspondence given a set of correspondences between two sets f^* the following equation must hold:

$$f^* = argmin_{\forall f : AxA'} \lambda \cdot \bigtriangledown(f) + (1 - \lambda) \cdot \Omega(e) \tag{6}$$

When dealing with multiple inputs, the main function can be implemented as

$$f^* = min_{\forall f : AxA'} \{\lambda / N \cdot \Sigma_{k=1}^{N} d_H(f^k, f) + (1 - \lambda) \cdot Cost(A, A', f)\} \tag{7}$$

where $\Sigma_{k=1}^{N} d_H(f^k, f)$ represents the addition of the Hamming distances from each initial proposal to the optimal correspondence, and $Cost(A, A', f)$ is the cost defined on equation 2. This function can be implemented using matrices, being $\bigtriangledown(f)$ a correspondence matrix F^k (inserting a 1 when two elements are mapped and 0 otherwise) and $\Omega(f)$ a cost matrix C^k filled with the average cost $C^k_{i,j}$ between two elements. To allow the system identify spurious mappings (outliers), we have structured F^k and C^k as used in the Bipartite Graph Matching method (BP) [11][14][15], one of the most well known and efficient linear solvers used for these cases. Therefore, the cost matrix C^k contain a deletion cost $C^k_{\varepsilon,j}$ or an insertion cost $C^k_{i,\varepsilon}$ in the diagonal of the second and third quadrants respectively. These costs are also used in the first quadrant when a mapping between two elements is not possible. The final construction of F^k and C^k is shown in figure 2.

4 Experimentation Settings

The experimental validation has been performed using a database comprised of 5 sequences called ”BOAT”, ”EASTPARK”, ”EASTSOUTH”, ”RESIDENCE” and ”ENSIMAG” [2]. These sequences are composed of 11 pictures taken from the same object, but from different points of views and scales. We extracted from each picture the 50 most reliable salient points and their features using 5 methodologies: FAST [12], HARRIS [3], MINEIGEN [4], SURF [1] and SIFT [6]. Then, we matched the first image of the sequence to the 10 remaining images in its sequence using the MF [7] (with a Maximum Ratio=1)

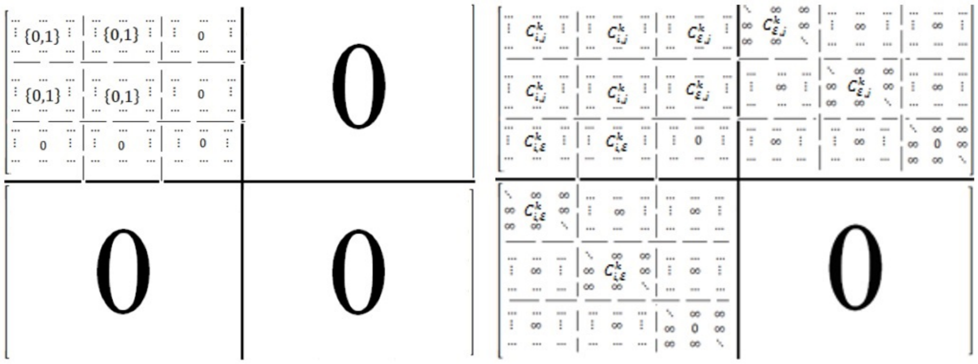


Fig. 2: Correspondence Matrix F^k and Cost Matrix C^k

and the BP method presented in [14] using $C^k_{i,\varepsilon}$,$C^k_{\varepsilon,j}$=0.2 (considering costs are normalised). Both the Maximum Ratio and $C^k_{i,\varepsilon}$,$C^k_{\varepsilon,j}$ were set to obtain the most possible number of pairings for each matching algorithm, however, if a duplicated or non-bijective mapping was found, it was discarded. The original database provides the homographies that convert the first images of the five sequences to the rest of images in the sequences. Using this homography, we generated a ground truth correspondence c_i for every pair of images thus allowing us to validate every correspondence calculated.

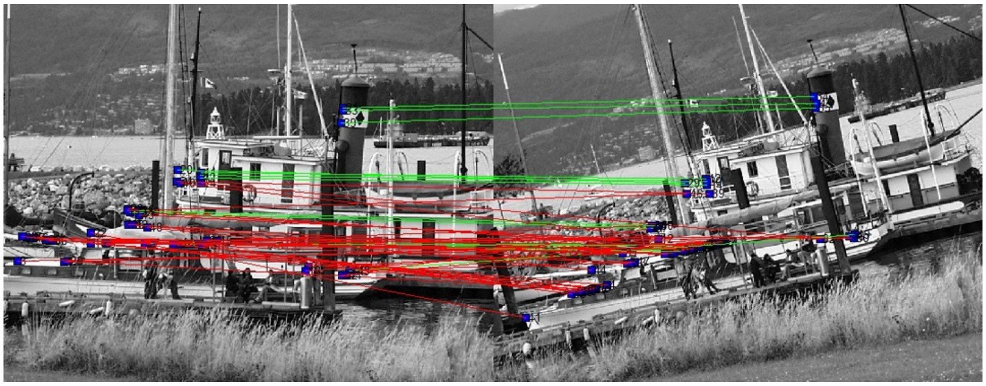


Fig. 3: A correspondence between the first two images of the BOAT sequence with the correct (green) and incorrect (red) mappings generated by the Match-Features functions contained in Matlab.

We compare this method with two proposals which were presented in [10], called iterative method and voting method. We are currently testing the three methods in terms of accuracy, average cost, end point error and runtime.

Acknowledgement. This research is supported by the Spanish CICYT project DPI2013-42458-P, by project TIN2013-47245-C2-2-R and by Consejo Nacional de Ciencia y Tecnología (CONACyT Mexico)

References

[1] Bay, H., Ess, A., Tuytelaars, T., Van Gool, L., ”SURF: speeded up robust features”. *Computer Vision and Image Understanding (CVIU)*, Vol. 110(3), pp. 346—359, 2008.

[2] FEATURESPACE. http://www.featurespace.org. *Accesed 12th May 2015.*

[3] Harris, C., Stephens, M., *“Proceedings of the 4th Alvey Vision Conference”.* pp. 147–151, 1988.

[4] Jolliffe, I.T., “Principal component analysis”. *Second Edition. Springer. 2002.*

[5] Kuhn, H.W., “The hungarian method for the assignment problem export”. *Naval Research Logistics Quarterly 2(1-2), 83–97, 1955.*

[6] Lowe, D.G., “Distinctive image features from scale-invariant keypoints”. *IJCV 60(2), pp. 91–110. 2004.*

[7] MATLAB Frameworks. http://es.mathworks.com/help/vision/ref/matchfeatu *res.html. Accesed 12th May 2015.*

[8] Moreno-Garcia, C. F., Serratosa, F., ”Fast and efficient palmprint identification of a small sample within a full image”. *Computación y Sistemas 18(4), 2014.*

[9] Moreno-Garcia, C. F., Cortes, X., Serratosa, F., ”Partial to full image registration based on candidate positions and multiple correspondences”. *CIARP 2014, LNCS 745.*

[10] Moreno-Garcia, C. F., Cortes, X., Serratosa, F., ”Iterative versus voting method to reach consensus given multiple correspondences of two sets ”. *IbPRIA, 2015.*

[11] Riesen, K., Bunke, H., “Approximate graph edit distance computation by means of bipartite graph matching”. *Image Vision Comput. 27 (7), pp. 950-959, 2009.*

[12] Rosten, E., Reid Porter, R., Drummond, T., ”Faster and better: a machine learning approach to corner detection”. *IEEE Trans. Pattern Analysis and Machine Intelligence 32, pp. 105–119, 2010.*

[13] Saha, S., Ekbal, A., “Combining multiple classifiers using vote based classifier ensemble technique for named entity recognition”. *Data & Knowledge Engineering 85, pp: 15-39, 2013.*

[14] Serratosa, F., “Fast computation of bipartite graph matching”. *Pattern Recognition Letters 45, pp: 244–250, 2014.*

[15] Serratosa, F., “Speeding up fast bipartite graph matching trough a new cost matrix”. *International Journal of Pattern Recognition and Artificial Intelligence 29 (2), 2015.*

This proceeding book contains the contributions presented at the 2nd URV Doctoral workshop in Computer Science and Mathematics. The main aim of this workshop is to promote the dissemination of the ideas, methods and results that are developed by the students of our PhD program.

[DΣIM] Departament d'Enginyeria
Informàtica i Matemàtiques

ETSE Escola Tècnica Superior
d'Enginyeria
Universitat Rovira i Virgili