

# ICSE 2017

## 부에노스아이레스, 아르헨티나

홍성준

### 1. 개요

소프트웨어 공학 분야에서 가장 명성이 높은 학회 중 하나인 ICSE에 다녀왔습니다. 이번 ICSE는 아르헨티나의 수도인 부에노스아이레스에서 개최되었는데, 살면서 한 번 걱정하지 않고는 가기 힘든 나라라는 점과 제 생의 첫 학회 참석이자 첫 해외 여행이었기 때문에, 왕복 50시간이 넘는 긴 비행시간도 마냥 기대되기만 했습니다.

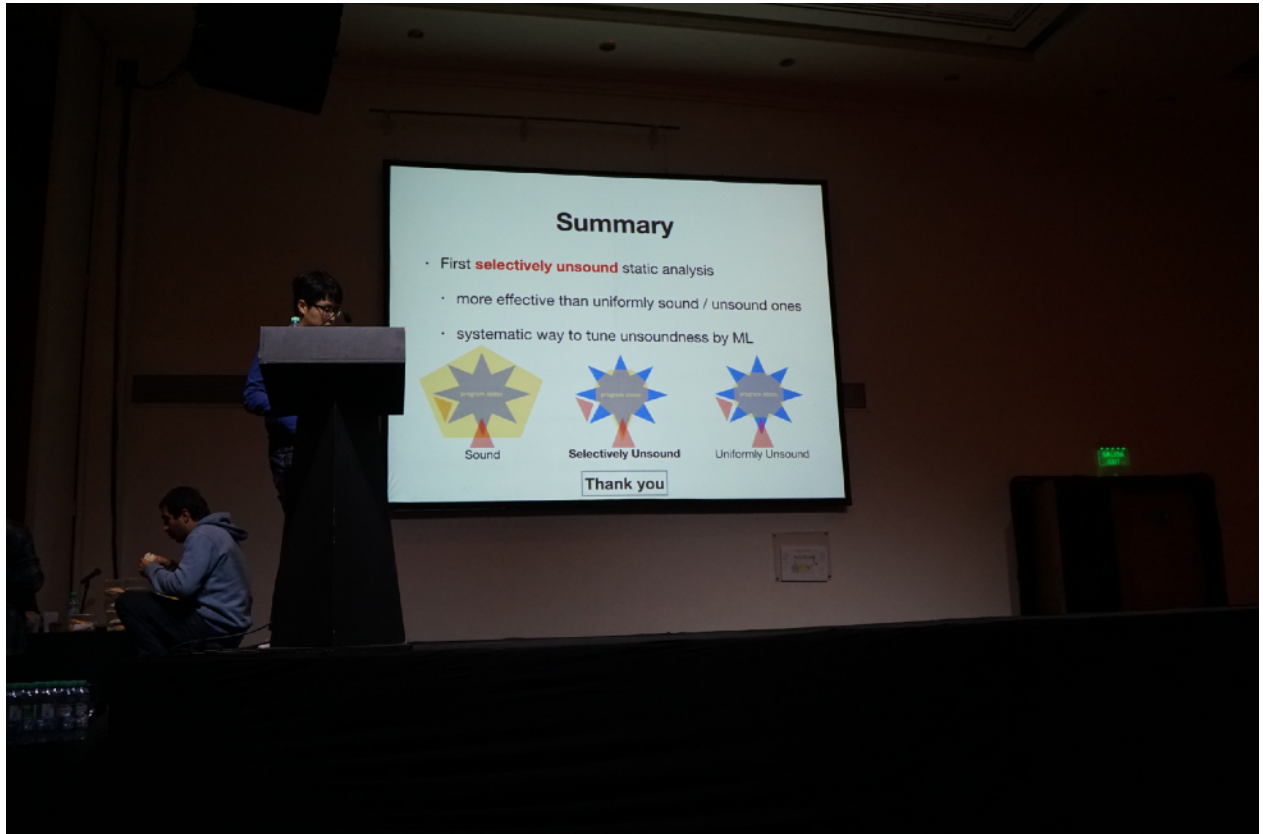
ICSE는 3일 내내 프레젠테이션에서만 6개의 세션이 동시에 열릴 정도로 규모가 굉장히 큰 학회였습니다. 특히 첫 날 개회식에서는 우리나라의 미래부 장관쯤 되는 아르헨티나 관리가 와서 연설을 했습니다. 여느 다른 학회도 마찬가지이겠지만, 각 세션이 끝나면 100명이 넘는 사람들이 홀을 꽉 채우고 끊임없이 떠들어댔습니다. 저는 아는 사람도 없고 딱히 공유할 만한 대화거리도 없어서 괜



히 서울대 허기홍 박사님이 어디있는지 찾아 댔습니다. 제가 쓴 논문이 몇 개라도 있었다면 뭔가를 소개할 만한 내용이라도 있을텐데 라는 아쉬움이 있었습니다.

## 2. 학회에서

- 허기홍 박사님



이번 ICSE에서는 허기홍 박사님의 selective unsoundness 연구가 accept 되어서 박사님을 학회 내내 만날 수 있었습니다. 점심을 먹고는 커피를 같이 마시면서 연구 얘기도 했습니다. 패치를 분석해서 개발자들의 리뷰 과정을 자동화 하는 방법에 대해 생각하고 있었는데, 대부분의 패치가 1~2 줄 이내의 코드만 수정한다는 점에 착안해서 코드의 일부 블록만 분석하되 최대의 정확도로 분석하는 방식에 대해 어떻게 생각하냐고 물어봤습니다. 너무 뜬구름 없는 질문이었지만 꽤 진지하게 고민하시고는 잘 안될거같다고 답변해주셨습니다.

허기홍 박사님의 발표도 들었는데, 이미 내용을 파악하고 있어서 인지 몰라도 발표를 잘 했다는 느낌이 들었습니다. Accent를 잘 살리면서도 담백하고 전달력 있는 발표였습니다. 발표 전에 노트 북을 연결해보고 각종 장비를 점검하는 모습은 배울만했습니다.

## • 탱고 세션



학회 첫 날 reception에서 탱고 공연이 열렸습니다. 재미있는 점은 탱고 공연이 끝나고 직접 탱고를 배울 수 있는 세션이 있었습니다. 배움의 길을 걷는 사람들이라 그런지 너도나도 탱고 배우기에 열중했습니다.

## • 카이스트 사람들

류석영 교수님 연구실 학생이 데모 세션에서 자바스크립트 정적분석기인 SAFE 2.0을 발표했습니다. 류 교수님도 뵙고 인사를 드렸습니다.

이번에 김문주 교수님 연구실의 김윤호 박사님이 학회에 오셨다고 했습니다. concolic testing 연구를 할 때, 김윤호 박사님의 자료와 벤치마크를 참조했었습니다. Concolic testing에 대해 이것저것 여쭙보려고 했는데 아쉽게도 뵙지 못했습니다. 아마 일면식도 없어서 마주치고도 지나쳤을지도 모르겠습니다.

## • 음식

학회는 웨라톤 부에노스아이레스 호텔에서 열렸는데, 호텔 음식이라 그런지 제법 퀄리티가 있었습니다. 음식은 뷔페식으로 제공되며 서서 먹었습니다. 웨이터가 돌아다니면서 음료를 주거나 접시를 수거해갔습니다.

### 3. 학회 발표 논문들

사실 대학원생으로서의 커리어를 이제 막 시작하는 입장에서 학회에 참석하여 무엇을 얻어가야 할지, 제가 무엇을 해야할지가 참 난감했습니다. 저명한 교수를 만나서 내 연구에 대해 조언을 구하거나, 나와 비슷한 연구를 하는 사람들에게 내 연구가 어떤지 물어보기에는 제가 가진 소스가 너무 없었습니다. 그래서 그냥 발표를 열심히 들었습니다.

SE는 가깝고도 먼 분야인 것 같습니다. 이번 ICSE에서는 testing, refactoring, program analysis 등의 친숙한 분야도 다뤄진 반면, 개발자 자체를 연구하는 세션도 있었습니다. Studies of Software Developers라는 이 세션에서는 프로그래머가 코드를 리뷰하는 동안 fMRI를 이용하여 뇌파를 측정하고 뇌의 어느 부분이 활성화 되는지를 연구한 논문이 발표되었는데, distinguished paper를 수상한 연구였습니다.<sup>1</sup> 저는 다른 세션을 듣느라 참가하지 못했는데, 수영이 형의 말에 따르면 후속 연구로 뒤에서 상사가 지켜보고 있을때 개발자의 어느 뇌파가 활성화되는지도 연구할 예정이라고 합니다. 가끔 교수님이 연구실에 오셔서 잘되고있는지 둘러보시는데, 이 때 내가 과연 집중을 더 하는지, 아니면 뇌의 새로운 부분이 자극되는지, 혹은 탄성을 피우게 되는지를 과학적으로 입증할 수 있다면 재미있을 것 같았습니다.

저는 주로 우리 연구실과 친숙한 분야를 위주로 발표를 들었는데, 그 중 기억에 남는 몇 가지를 소개하겠습니다:

#### *“TRAVIOLI: A Dynamic Analysis for Detecting Data-Structure Traversals”*

Concolic testing을 공부할 때 많이 봤던 Koushik Sen의 그룹에서 발표한 논문입니다. 프로그램의 성능에서 linked-list나 tree같은 data structure를 traverse하는 operation이 차지하는 비중이 매우 큰데, 이러한 traversal operation을 어떻게하면 잘 찾아낼 수 있을지에 관한 연구였습니다. 대략적인 아이디어는 같은 프로그램 포인트에서 다른 메모리 로케이션을 가리키면 traversal 함수라고 판단한다는 것인데, 이를 추적하기 위해 프로그램을 실행중에 각 프로그램 포인트마다 메모리 로케이션에 관한 event를 기록하는 것입니다. 일반적으로 정적분석에서는 까다로운 recursion에 대해서도 잘 작동한다고 하는데, 이 방식대로 찾는다면 당연히 문제가 없지 않나 싶다는 생각이 들었습니다. 참신한 아이디어는 아니었지만 목표 자체가 워낙 명료하고 기본적인 문제 해결방법도 쉽게 알 수 있었던 발표였습니다.

#### *“SPAIN: Security Patch Analysis for Binaries - Towards Understanding the Pain and Pills”*

프로그램에 적용된 security 관련 patch 자체를 분석하여 의미있는 정보를 얻어내는 연구입니다. 우선 프로그램 패치 자체를 분석한다는 점이 흥미로웠습니다. 왜냐하면 보통 program security 문제를 생각해보면, 프로그램 소스 코드를 보고 알려지지 않은 취약점을 미리 찾거나 혹은 취약한 부분을 자동으로 패치해주거나 하는 문제를 생각하기 마련인데, 이 연구에서는 n-day attack의

---

<sup>1</sup> Decoding the representation of code in the brain: An fMRI study of code review and expertise by Benjamin Floyd, Tyler Santander and Westley Weime

예를 들어 연구의 필요성을 설명했습니다. 실제 세계에서는 어떤 소프트웨어에서 취약점이 발견되어 패치가 이루어져도 다른 소프트웨어가 이를 반드시 패치하지는 않는다는 문제가 있습니다. 즉, 어떤 취약점 패치가 발견되어도 이를 방치하는 경우가 부지기수라는 것입니다. 또한 대부분의 상용 소프트웨어의 패치는 보안상의 이유로 바이너리 코드의 형태로 배포되기 때문에, 바이너리 레벨의 분석이 필요함을 잘 설득시켰습니다. 이 연구가 바이너리 패치 분석을 최초로 시도한 것은 아니었는데, 기존의 패치 분석 연구와의 차별점으로는 패치 내용 자체가 필요 없다는 점입니다. 즉, 어떤 부분이 패치되었는지 모르는 상황에서, 기존의 전체 프로그램 바이너리와 패치된 프로그램의 전체 바이너리만 가지고도 어떤 부분이 패치되었는지 알아냅니다. 이는 패치를 따로 배포하지 않고, 다음 버전의 전체 프로그램만 배포하는 시나리오에도 적용될 수 있다는 것이 기존 연구와의 차별점입니다. 기술적으로는 어떻게 했는지 잘 파악이 안됐지만 똑똑똑 한 것 같았습니다. 예를 들어 전 버전과 다음 버전의 프로그램을 비교할 때 어떤 부분이 패치에 관련된 부분인지 알아낼 때, 코드에서 변한 부분이 많이 없으면 보안 관련 패치라고 판단한다고 했습니다. 논문의 교신저자인 Fu Song 교수가 발표를 했는데, 여유도 있고 상당히 발표를 잘했습니다. 보안 취약점을 찾으면 돈을 많이 주고, 세금도 안 떼가서 학생들이 좋아한다고 자랑했습니다.

#### *“Learning to Prioritize Test Programs for Compiler Testing”*

북경대의 High Confidence Software Technologies 연구실에서 발표한 논문인데, 나중에 알고보니 이 연구실은 메모리 누수 패치 툴인 LeakFix를 만든 연구실이었습니다. 컴파일러 테스팅에서 버그를 일으킬 법한 테스트 케이스를 먼저 테스트 할 수 있도록 우선순위를 정해주는 연구입니다. 이 때 테스팅 케이스는 CSmith 등의 컴파일러 테스트 케이스 생성기를 통해 만드는데, CSmith는 예전에 랩 세미나에서 제가 발표했던 연구여서 반가웠습니다. 이 연구가 흥미로웠던 점은 테스트 케이스 우선순위를 학습을 통해 찾는다라는 것입니다. 각 테스트 케이스(프로그램)을 설명하는 feature를 디자인 하고, 케이스 별로 버그 발견 여부를 labeling한 뒤 offline learning으로 모델을 학습시키는 방식입니다. 우리 연구실에서 진행되었던 widening threshold나, 허기 홍씨가 다음 날 발표한 selective unsoundness 연구에서 제안한 방법과 비슷했습니다. 문제를 푸는 방식이 비슷해서 궁금한 내용이 많이 생겨 세션이 끝나고 포스터 세션에서 저자에게 제법 많은 질문을 했습니다. 가장 의아했던 점은 CSmith의 경우 실행 결과가 달라지는 buggy-case만 생성하는 것으로 알고 있는데, 이 경우에 테스트 케이스의 우선 순위는 어떻게 되는지가 명료하지 않았습니다. 그리고 언뜻 생각했을 때, 그냥 모든 테스트 케이스를 실행해보면 될 것 같은데 왜 우선 순위를 주는 것이 중요한 문제인지 명확하지 않았습니다. 또한 feature 디자인은 어떻게 했는지 자연스럽게 궁금해졌습니다. 접근 방식이 비슷한 concolic testing 연구에서도 다른 사람들이 이런 질문을 할 수 있겠구나 라는 생각이 들었습니다.

#### *“A Survey on Metamorphic Testing”*

Journal-First paper로, 저널에 이미 출판된 논문을 ICSE에서 초청하여 발표한 논문입니다. Software testing 분야에서 비중있는 문제중 하나는, 테스트 케이스가 출력해야 하는 정답이 무엇인지 결정해주는 test-oracle을 얻는 것이라고 합니다. 문제는 이 오라클을 얻는 것이 일반적인

로 항상 가능한 것이 아니라는 것입니다. 예를 들어, sine 값을 계산해주는 소프트웨어의 테스트 케이스를 만들려고 할 때, 테스트 케이스의 정답을 정하는 방법이 그렇게 자명한 것은 아닙니다. 이 때 sine 소프트웨어는  $\sin(x) = \sin(\pi - x)$ 라는 성질을 만족해야 한다는 사실을 이용하여 테스트 케이스의 쌍을 구성하면, 실제 sin 함수의 정확한 값을 모르고도 테스트를 수행할 수 있습니다. 이렇게 이미 존재하는 테스트 케이스의 input과 변형된 input 사이의 관계, 그리고 이 때 두 테스트 케이스가 가져야 하는 출력 사이의 관계를 기술하는 것이 metamorphic relation입니다. 발표에서 사용되었던 예시는 그래프에서 source와 destination 사이의 shortest path를 구하는 프로그램이었는데, 이 경우 source와 destination이 서로 뒤바뀌어도 output path의 길이는 서로 같아야 한다는 성질을 이용하여 테스트 케이스를 만들어 낼 수 있습니다. 예전에 랩 세미나에서 컴파일러 테스트 논문을 발표했을 때 differential testing이라는 개념을 공부했었는데, 컴파일러는 항상 모든 인풋에 대해 같은 결과를 출력하도록 코드를 생성해야 한다는 성질을 이용하여 이를 fail하는 테스트 케이스를 만들어내는 기술이었습니다. Differential testing 역시 metamorphic testing의 특수한 케이스로 설명할 수 있겠다는 생각을 했습니다. 지금까지 정적분석에서 공부했던 내용은 주로 모든 실행에 대하여 만족하는 성질을 찾아내는 것이었는데, 이렇게 서로다른 두 실행끼리의 성질만 비교하는 것으로 테스트 케이스를 만들어내는 점이 굉장히 흥미로웠습니다. 또한 introduction의 example이 남에게 문제를 이해시키는데 굉장히 중요한 역할을 하는 것 같다는 생각이 들었습니다.

## 4. 여행기

### 1) 이과수 폭포

아르헨티나에서의 여정중 가장 기억에 남는 것을 꼽으라면 단연 이과수 폭포였습니다. 폭포에 도착하기까지의 과정은 상당히 험난했는데, 비행기가 지연되어 호텔에서 짐을 풀고 샤워라도 하고 출발하려는 계획이 어긋나고, 이과수로 떠나는 공항에 도착해서도 체크인을 하지 못해서 비행기를 놓칠뻔 했습니다. 우여곡절 끝에 도착한 이과수 국립공원은 비가 내리기 시작하고 있어서인지, 사람이 별로 없었습니다.

이과수 폭포는 우리말로 “큰 물” 정도로 번역할 수 있는데, 이름에서 드러나듯 폭포의 규모가 어마어마 했습니다. 사실 세계에서 가장 큰 3대 폭포중 하나라고 합니다. 관광 명소를 찾아다니고 하는 것을 좋아하지는 않는 편인데, 이과수 폭포는 참 멋졌습니다. 이과수 폭포는 이과수 국립공원 안에 위치해 있는데, 국립공원 자체에도 볼거리가 많은 편이었습니다. 특히 기억에 남는 것은 강의 종류까지 이어지는 트레일인데, 숲에 진입하기전 기차길에서의 풍경이 참 아름다웠습니다. 개인적으로는 칙칙폭폭 소리가 나는 옛날느낌의 기차에 대한 로망이 있어서 기분이 매우 좋았습니다. 이과수 폭포 사진은 많이 알려져있으니 제가 잘나온 사진만 소개하고 폭포에서의 여정은 마무리 하겠습니다.



<트레일 위에서>



<이과수 폭포>



<이과수 스테이크>

저녁이 되어서 돌아오는 길에는 이과수 공항의 카페 겸 음식점에서 스테이크를 사먹었습니다. 옆의 방울 토마토를 보면 알겠지만 엄청 신경써서 만든 요리는 아니었던 것 같았는데, 이틀 정도의 비행 이후에 먹는 제대로된 첫 끼여서 매우 맛있었습니다. 가격은 만 원 언저리 였던 것 같습니다.

## 2) 산 마르틴 광장



호텔에서 학회장까지 가는 길목에 있던 공원입니다. 산 마르틴은 아르헨티나에서 태어나 페루와 칠레를 에스파냐로부터 독립시킨 장군인데, 이순신 장군과 같이 아르헨티나의 국민 영웅으로 추앙받는 인물입니다. 사진의 동상은 그를 기리는 동상인데, 동상이 고퀄리티라 햇빛을 받은 모습이 멋졌습니다.

부에노스아이레스는 도시 곳곳에 꽤 넓은 공원이 많았는데, 나무의 크기도 굉장히 크고 잘 가꿔진 느낌이었습니다. 아마 유럽

의 지배에 있을 때 영향을 많이 받은 것 같습니다.





<산 마르틴 광장의 나무>

### 3) 대통령 궁

금요일에는 아침 일찍 일어나서 학회 오전 세션이 시작하기 전에 잠을 내어 대통령 궁을 다녀왔습니다. 마침 당일이 아르헨티나 혁명 기념일이어서, 대통령 궁 근처 광장에서 행사가 있었습니다.



<대통령 궁 앞에서>

우리나라의 광복절 짬 되는 행사인 것 같았는데, 꽤 큰 국경일임에도 차분하게 진행되었습니다. 대통령 내외, 국회의원 및 장관들은 사진의 오른쪽 성당안에서 행사에 참석했습니다. 아르헨티나의 독립을 기념하는 리본을 들고다니는 어떤 누나가 리본을 가져가라갈래, 처음엔 잡상인인 줄 알고 무시하다가 “it’s free”라길래 냉큼 받아서 가슴팍에 달았습니다.



위의 성당 사진은 토요일 저녁에 찍었는데, 전날 독립기념일 행사 때문에 들어가보지 못해 아쉬워서 떠나는 비행기를 타기 전 부에노스아이레스에서의 여정의 마지막에 잠시 들렀습니다. 성당 내부는 굉장히 조용하고 엄숙했습니다.

## 4. 마치며

최고 퀄리티의 학회 분위기를 체험할 수 있는 좋은 기회였습니다. 개인적으로도 이전에 겪지 못했던 다양한 경험을 할 수 있었던 여행이었던 것 같습니다. 특히 내 나이 또래의 중국계 학생들이 ICSE에서 유창한 영어로 발표하는 모습은 질투심도 나고 큰 자극이 되었습니다.

마지막으로, 좋은 경험을 할 수 있게 지원해주신 오학주 교수님께 감사드립니다. 다음 학회는 좋은 연구로 발표자로서 참석할 수 있도록 노력하겠습니다.