OOPSLA 2019를 다녀와서

Athens, Greece
2019.10.20 – 2019.10.27
고려대학교 소프트웨어 분석 연구실
소순범

Figure 1: 아크로폴리스에서 바라본 풍경

1 머리말

OOPSLA는 PL 응용 분야에서 최고 수준의 학회이다. 나는 발표할 논문이 없었지만, 지도 교수님인 오학주 교수님께서 참석할 기회를 주셔서, 운이 좋게 즐겁고 유익한 경험들을 할 수 있었다. 경험하고 느꼈던 바들을 공유하고자 본 여행기를 적는다.

2 학회장 이야기

2019년도 SPLASH는 그리스 아테네에 위치한 5성급 호텔인 Royal Olympic Hotel에서 개최되었다. SPLASH는 메인 학회인 OOPSLA를 중심으로 하여, GPCE 등 여러 소규모 학회 및 워크샵들이 함께 열리는 학술 대회 모임이다. SPLASH 전체 일정(10.20–10.25) 중 OOPSLA는 3일(10.23–10.25)에 걸쳐 열렸고, 포스터 발표는 이틀간(10.21, 10.24) 진행되었다. 나는 OOPSLA 및 포스터 발표에 참석하였다.

Figure 2: Reception 음식

여태껏 참석했던 학회들에서 제공되었던 식사들과 달리, 이번 학회에서 제공되는 음식들은 내 입맛에 정말 딱 맞았다. 뷔페식으로 제공되었는데, 매 식사마다 한번 먹고 또 먹고 싶을 정도였다. Reception에서 나온 음식들도 정말 맛있었다.

OOPSLA는 최고 수준의 학회임에도 불구하고, 2–3개의 발표 세션이 동시에 진행되어서 인지, 세션 당 참석 인원은 그다지 많게 느껴지지는 않았다. 그래도 웬만하면 매 발표마다 적어도 2–3개의 질문은 있었던 것으로 기억한다.

3 포스터 발표

나는 2020년도 IEEE S&P에 수락된 'VeriSmart: A Highly Precise Safety Verification for Ehtereum Smart Contracts' 논문에 대한 포스터 발표를 진행하였다. 특히 이번 포스터 발표는 프로그램 분석/검증 분야의 유명인사인 Yannis Smaragdakis, Zhong Shao 교수님들께 내 연구를 소개할 수 있는 매우 뜻 깊은 시간이었다.

포스터 발표를 진행하면서 느낀 바는, '포스터 발표는 2분–3분 길이의 설명을 준비하자'는 것이다. 처음에는 9분 정도의 설명을 준비했었는데, 논문 작성할 때와 같이 예제 코드의 디테일을 일일이 설명하려다보니 설명자인 나조차 지루함을 느꼈다. 어차피 떠날 사람은 떠나고, 관심이 있는 사람은 꼬리에 꼬리를 물어 질문을 한다. 그 동안 적지 않은 수의 포스터 발표를 진행해왔는데, 각 포스터를 준비하는 과정에서 더 신경을 썼다면 한참 오래 전에 깨달았어야 할 것을 왜 이제야 느끼게 되었는지, 나의 아둔함을 반성할 수 밖에 없었다.

포스터 발표를 진행하면서 받았던 질문들로는, VeriSmart가 어떠한 종류의 취약점들을 탐지할 수 있는지, 검증하고자 하는 성질을 어떻게 명세할 수 있는지, 명세 언어(specification language)를 확장할 경우 사용자 입장에서 어려움을 느낄 수도 있을 텐데 이에 대해 어떻게 생각하는지, 불변식(invariant)을 생성하는 것이 검증하는데 어떻게 도움이 될 수 있는지, 알고리즘이 구체적으로 어떻게 동작하는지 등이 있었다. 쉽게 대답해줄 수 있는 내용들도 있었지만, 만족스러운 답변을 하지 못한 경우도 적지 않았다. 이번 포스터 발표를 통해, 내가 미처 생각해보지 못했던 사항들이

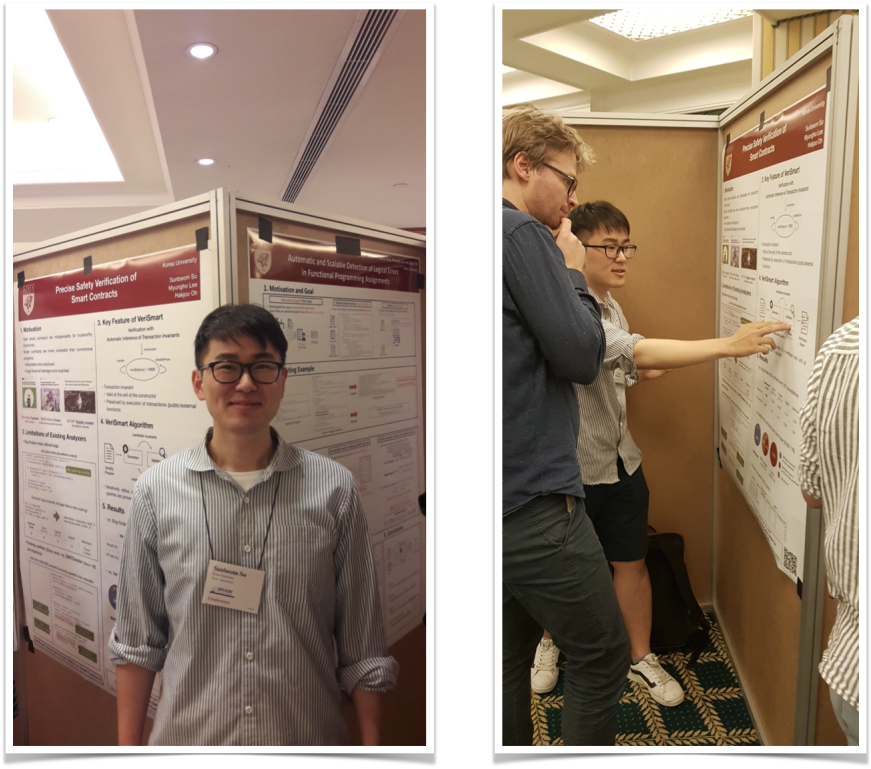

Figure 3: 포스터 발표하는 모습

무엇인지(예: 명세 언어와 관련된 사항), 나는 당연하다고 가정했지만 청중에게는 당연하지 않은 사항들이 무엇인지(예: 불변식을 생성하는게 왜 좋은지), 설명 준비가 충분히 되지 않은 내용이 무엇인지(예: 알고리즘의 구체적인 동작 방식)를 알 수 있었다.

종합적으로, 내년 5월에 있을 논문 발표를 위해 준비해야할 사항들이 무엇인지 알아볼 수 있는 뜻 깊은 시간이었다.

4 흥미있었던 논문들

- **Modular Verification of Web Page Layout**

  이 논문은 웹 페이지 레이아웃과 관련된 성질(예: 화면의 크기에 상관없이 글씨가 깨지지 않고 잘 보인다)을 검증하는 것에 관한 내용을 다룬다. 나는 응용 도메인 보다는 기술적인 측면(modular verification)에 관심이 있어서 발표를 들었는데, 기술적으로 아주 특별한 내용이 있지는 않았다. 검증은 크게 두 단계로 이루어진다. 먼저, 'Visual Logic'이라는 명세 언어를 이용하여 각 페이지 내의 컴포넌트(예: header, footer)들에 대한 명세를 작성하고, 각 컴포넌트가 명세들을 만족하는지를 확인한다. 그 다음, 각 컴포넌트의 명세들이 만족될 때, 전체 페이지에 대한 명세(whole-page property)가 만족되는지를 확인한다. 만약 충족되지 않는 명세가 존재할 경우, 사용자가 명세를 직접 정제해주어야 한다. '웹페이지에 대한 엄밀한 정형 검증의 필요성'에 대해서는

약간 의문이 들지만, modular verification의 현 주소에 대해 파악할 수 있어서 꽤나 유익한 논문이었다.

- **Precise Reasoning with Structured Time, Structured Heaps, and Collective Operations**

  이 논문은 매우 기술적인 논문인데, 구체적으로는 프로그램 분석에서 요약과 관련된 두 가지 문제를 인식하고 해결하고자 한다: 1) 대개의 요약은 보통 집단적인(collective) 특성을 직접적으로 표현하지 않기 때문에 분석 결과가 부정확할 수 있다. 2) 대개의 분석에서는 시간 측면에 관한 정보가 뭉개진다 (즉, 변수의 값이 룹 회차에 따라 달라질 수 있으나, 이를 하나의 값으로 요약한다). 첫 번째 문제를 해결하기 위해, 배열의 합과 같은 성질을 표현할 수 있는 집단 연산자(collective operation)를 제안하고 있는데, 정량자(quantifier)와 재귀적 정의(recursive definition)를 필요로 하지 않는 것이 특징이다. 두 번째 문제를 해결하기 위해, 힙을 룹 회차에 따라 정확하게 모델링하고 분석할 수 있는 방법을 소개한다.

  위 두 가지를 달성하기 위한 개략적인 절차는 다음과 같다. 먼저 원시 언어(source language)를 간단한 형태의 명령형 언어를 가정하고, 이를 목표 언어(target language)인 함수형 언어로 의미가 보존되게끔(semantics-preserving) 변환한다. 이 함수형 언어는 리스트, 배열 등에 대해 Σ 등 집단적인 특성을 계산할 수 있는 연산자들을 문법으로 지니고 있는 것이 특징이다. 그 다음, 집단 연산자를 유한하게 계산할 수 있는 형태(closed-form)로 변환할 수 있는 규칙을 정의하고 이 규칙에 따라 연산자들을 변환한다. 이러한 변환 과정을 통해 고수준(high-level)의 정보를 잃지 않음으로써 정확한 분석을 수행할 수 있다고 한다.

  실험은 SV-COMP(프로그램 검증 경진대회) 벤치마크들을 사용하였는데, 기존의 검증기들보다 더 정확하고 빠르게 검증할 수 있음을 보였다. 디테일을 간략하게 살펴보았는데, 간단한 형태의 룹이 아닐 경우 적용이 어려울 듯 하다. 실제 응용분야에서 논문에서 대상으로 하는 성질까지 추론해야할 필요가 얼마나 있을지는 잘 모르겠지만, 이론적인 측면에 관심이 있기도 하고 나중에 SV-COMP에 도전할 의향이 있어서 나름대로 흥미있었던 논문이다.

- **Relational Verification using Reinforcement Learning**

  이 논문 또한 기술적인 논문에 속한다. 구체적으로는 임의의 두 프로그램이 주어졌을 때, 두 프로그램 간의 관계(예: 두 프로그램이 의미적으로 같은지의 여부)를 빠르게 검증하기 위한 방법으로서 강화학습을 적용한 논문이다. 더 구체적으로는, 두 프로그램 간의 관계를 증명하기 위한 일련의 추론 규칙(inference rule)들이 존재할 때 (논문에서는 37가지의 추론 규칙을 디자인하였음), 증명 트리를 빠르게 완성하기 위한 추론 규칙 적용 순서에 대한 휴리스틱을 강화학습으로 배우고, 학습된 정책(policy)을 기반으로 증명 탐색을 효율적으로 가이드 하는 기법을 소개하고 있다. 내가 현재 연구하고 있는 스마트 컨트랙트 도메인에서도 복수 개의 컨트랙트들이 상호작용하는 경우가 꽤 있는데, 스마트 컨트랙트 도메인에서 관계 검증에 관한 연구를 할 경우 유용한 참고자료가 될것으로 보인다.

- **Safer Smart Contract Programming with Scilla**

  스마트 컨트랙트의 안전성이 이슈로 떠오르면서 최근 여러 분석기들이 등장하였는데, 본 논문에서는 약간 다른 방향으로 스마트 컨트랙트의 안전성 문제를 해결하고자 한다. 구체적으로는, 스마트 컨트랙트를 안전하게 작성할 수 있도록 디자인된, Scilla라는 새로운 함수형 언어를 소개한다. Scilla의 핵심 특징은 다음과 같다.

  - 타입 건전성(type soundness): Scilla의 타입 시스템은 다형 람다 칼큘러스(polymorphic lambda calculus, System F)로부터 유래한 것으로서, 타입 건전성을 지닌다. 따라서, 예기치 않은 런타임 오류가 발생하지 않음을 보장한다.
  - 튜링 불완전(turing-incomplete): 모든 트랜잭션이 정상적으로 종료됨을 보장하기 위해, 임의의 룹/재귀 함수를 허용하지 않고, 제한된 형태의 룹만을 허용한다 (예: 리스트 타입에 대해 fold 함수 제공). 실제로 솔리디티 스마트 컨트랙트를 살펴보면, 대부분의 컨트랙트가 매우 제한적이고 간단한 형태의 룹을 구현하고 있다. 이 점 때문에, 평소에 스마트 컨트랙트 언어에 대하여 튜링 완전성을 제공하는 것이 얼마나 큰 이점인지 의구심을 품어왔다. 나는 이러한 점에서 제한된 형태의 룹만을 허용하는 것은 매우 합리적인 선택이라 생각한다.

  (이 외에도 논문에서는 다양한 이점을 주장하는데, 이점에 대한 그 근거가 뚜렷하지 않아 개인적으로 동의하기 힘든 부분은 본 여행기에서 생략하였다.)

  개인적으로는 어느 프로그래밍 언어를 사용하든지 결국에는 분석/검증을 필요로 한다고 생각한다. 따라서, 현재로서는 본 논문에서와 같이 언어 디자인에 의해 안전성을 보장하는 방향에는 크게 관심이 없다. 하지만, 프로그래밍 언어를 디자인하는 저자들의 철학에 대해 엿볼 수 있었다는 측면에서 재미있는 논문이었다.

- **Detecting Nondeterministic Payment Bugs in Ethereum Smart Contracts**

  나의 현재 연구 분야인 스마트 컨트랙트 분석에 관한 논문이다. 구체적으로는, 스마트 컨트랙트의 비결정적(non-deterministic)인 요소로 인해 의도치 않은 지불을 하게 되는 취약점을 탐지하는 것을 목표로 하는 논문이다. 예를 들어, 다음의 시나리오에서 사용자 A는 본래 의도와 달리 더 많은 금액을 지출하게 된다: 1) 현재 물건의 값이 10으로 설정되어 있는 상태에서 A가 물건을 사기 위한 트랜잭션 T1을 요청, 2) 컨트랙트의 주인인 B가 물건의 값을 20으로 재조정하는 트랜잭션 T2를 요청, 3) 마이너(miner)는 T2를 먼저 처리한 후 T1을 처리.

  기술적으로는, 대상으로 하는 취약점 탐지에 특화된 테인트 분석(taint analysis)을 디자인한 것으로서 크게 새로운 측면은 없었다. 하지만, 발표가 매우 인상적이었다. 연구 내용을 이해하기 위해 필요한, 블록체인과 스마트 컨트랙트에 대한 기본적인 배경 설명부터 본론까지 아주 영리하게 잘 집약돼있다고 느꼈다. 앞으로 논문 발표 준비를 할 때 본보기로 삼고자 한다.

논문에서 대상으로 하는 취약점 특성상, 분석기가 유용해지기 위해서는 문제가 될 수 있는 트랜잭션 순서를 분석기의 최종 출력으로서 제공해주어야 한다고 생각하는데, 발표가 끝난 후 저자에게 개인적으로 물어보니 그러한 순서를 출력하지는 않는다고 한다. 이는 유용성 측면에서 아쉬운 점이라고 생각한다.

5 아테네 여행

OOPSLA 개최 일정 전후의 시간 여유를 활용하여 아크로폴리스, 아크로폴리스 박물관 등 아테네의 관광지들을 둘러볼 수 있었다. 특히 아크로폴리스 언덕에서는 아테네 시내 전역의 멋진 풍경을 바라볼 수 있었다. 10월의 아테네는 반바지를 입어도 될 정도로 약간 덥고 건조하였다. 로컬 음식들은 너무 짜거나/달거나 양 극단 중 하나에 속하는 경우가 대부분이었는데, 내 입맛에 맞는 음식들도 꽤나 있었다. 아테네에 관광객들이 많아서인지는 모르겠으나, 대부분의 그리스 사람들은 영어를 잘해서 여행하는데 큰 어려움은 없었다.

Figure 4: 아테네 밤 풍경

Figure 5: 먹었던 음식들

6 맺음말

석박통합과정 7학기 차에 접어들었지만, 아직까지도 내 배경지식의 부족함으로 인해, 대강의 발표 내용조차 파악이 안 되는 경우들이 꽤나 있었다. 본 연구를 진행하는 것 외에도 관련 배경 지식들을 틈틈이 쌓도록 노력해야겠다.

유익한 경험을 할 수 있도록 학회 참석기회를 주신 오학주 교수님께 감사드립니다.