Análisis de la herramienta TLA+ Proof System

Pablo Celayes, Giovanni Rescia, Ariel Wolfmann

Facultad de Matemática, Astronomía y Física
Universidad Nacional de Córdoba

Junio 2015

Veremos...

Veremos...

Veremos...

Contexto

Objetivos

Descripción del lado del usuario

Aspectos técnicos

Casos de aplicación

Comparación con otras herramientas

Ejemplo

Conclusiones

Veremos...

Contexto

Objetivos

Descripción del lado del usuario

Aspectos técnicos

Casos de aplicación

Comparación con otras herramientas

Ejemplo

Conclusiones

Veremos...

Veremos...

Veremos...

Veremos...

- Contexto
- Objetivos
- Descripción del lado del usuario
- Aspectos técnicos
- Casos de aplicación
- Comparación con otras herramientas
- Ejemplo
- Conclusiones

1977

Pnueli introduce su lógica temporal para describir sistemas.

- útil para ciertas propiedades, limitada para otras
- se combinaba con formas más tradicionales de descripción

1977

Pnueli introduce su lógica temporal para describir sistemas.

- útil para ciertas propiedades, limitada para otras
- se combinaba con formas más tradicionales de descripción

1977

Pnueli introduce su lógica temporal para describir sistemas.

- útil para ciertas propiedades, limitada para otras
- se combinaba con formas más tradicionales de descripción

fin de los 80's

Lamport introduce TLA

- variante de la lógica temporal de Pnueli
- mayormente notación matemática tradicional
- lógica temporal sólo donde es imprescindible

fin de los 80's

Lamport introduce TLA

- variante de la lógica temporal de Pnueli
- mayormente notación matemática tradicional
- lógica temporal sólo donde es imprescindible

fin de los 80's

Lamport introduce TLA

- variante de la lógica temporal de Pnueli
- mayormente notación matemática tradicional
- lógica temporal sólo donde es imprescindible

fin de los 80's

Lamport introduce TLA

- variante de la lógica temporal de Pnueli
- mayormente notación matemática tradicional
- lógica temporal sólo donde es imprescindible

2001...

Lamport se va a Microsoft Research

- Surge TLA+ (extensión de TLA para escribir **pruebas**)
- Desarrollo del **Toolbox** y el TLA+ Proof System

2001...

Lamport se va a Microsoft Research

- Surge TLA+ (extensión de TLA para escribir **pruebas**)
- Desarrollo del **Toolbox** y el TLA+ Proof System

2001...

Lamport se va a Microsoft Research

- Surge TLA+ (extensión de TLA para escribir **pruebas**)
- Desarrollo del **Toolbox** y el TLA+ Proof System

...2015

Tools for Proofs

- Colaboración Microsoft - INRIA
- Proyecto activo (issue tracker, mailing list)
- Aplicación en academia e industria

...2015

Tools for Proofs

- Colaboración Microsoft - INRIA
- Proyecto activo (issue tracker, mailing list)
- Aplicación en academia e industria

...2015

Tools for Proofs

- Colaboración Microsoft - INRIA
- Proyecto activo (issue tracker, mailing list)
- Aplicación en academia e industria

...2015

Tools for Proofs

- Colaboración Microsoft - INRIA
- Proyecto activo (issue tracker, mailing list)
- Aplicación en academia e industria

Objetivos

- TLA+: lenguaje de especificación formal
- TLAPS permite verificar la correctitud de pruebas (especificaciones) escritas en TLA+

Objetivos

- TLA+: lenguaje de especificación formal
- TLAPS permite verificar la correctitud de pruebas (especificaciones) escritas en TLA+

Descripción del lado del usuario

Posee un IDE **Toolbox**, que integra las siguientes herramientas:

- **PlusCal**: Lenguaje algorítmico simple que se compila a TLA+
- **Modelo Standard**: Un sistema se describe como un conjunto de comportamientos
- **TLC**: *Model Checker*
- **TLA+ Proof System**: Desarrollo y verificación mecánica de demostraciones

Descripción del lado del usuario

Posee un IDE **Toolbox**, que integra las siguientes herramientas:

- **PlusCal**: Lenguaje algorítmico simple que se compila a TLA+
- **Modelo Standard**: Un sistema se describe como un conjunto de comportamientos
- **TLC**: *Model Checker*
- **TLA+ Proof System**: Desarrollo y verificación mecánica de demostraciones

Descripción del lado del usuario

Posee un IDE **Toolbox**, que integra las siguientes herramientas:

- **PlusCal**: Lenguaje algorítmico simple que se compila a TLA+
- **Modelo Standard**: Un sistema se describe como un conjunto de comportamientos
- **TLC**: *Model Checker*
- **TLA+ Proof System**: Desarrollo y verificación mecánica de demostraciones

Descripción del lado del usuario

Posee un IDE **Toolbox**, que integra las siguientes herramientas:

- **PlusCal**: Lenguaje algorítmico simple que se compila a TLA+
- **Modelo Standard**: Un sistema se describe como un conjunto de comportamientos
- **TLC**: *Model Checker*
- **TLA+ Proof System**: Desarrollo y verificación mecánica de demostraciones

Aspectos técnicos

Una especificación en TLA+ es un módulo raíz, que puede importar otros módulos por extensión e instanciación de sus respectivos parámetros.
La arquitectura de TLAPS se divide en:

- TLAPM
- Backends

TLAPM

Se encarga de:

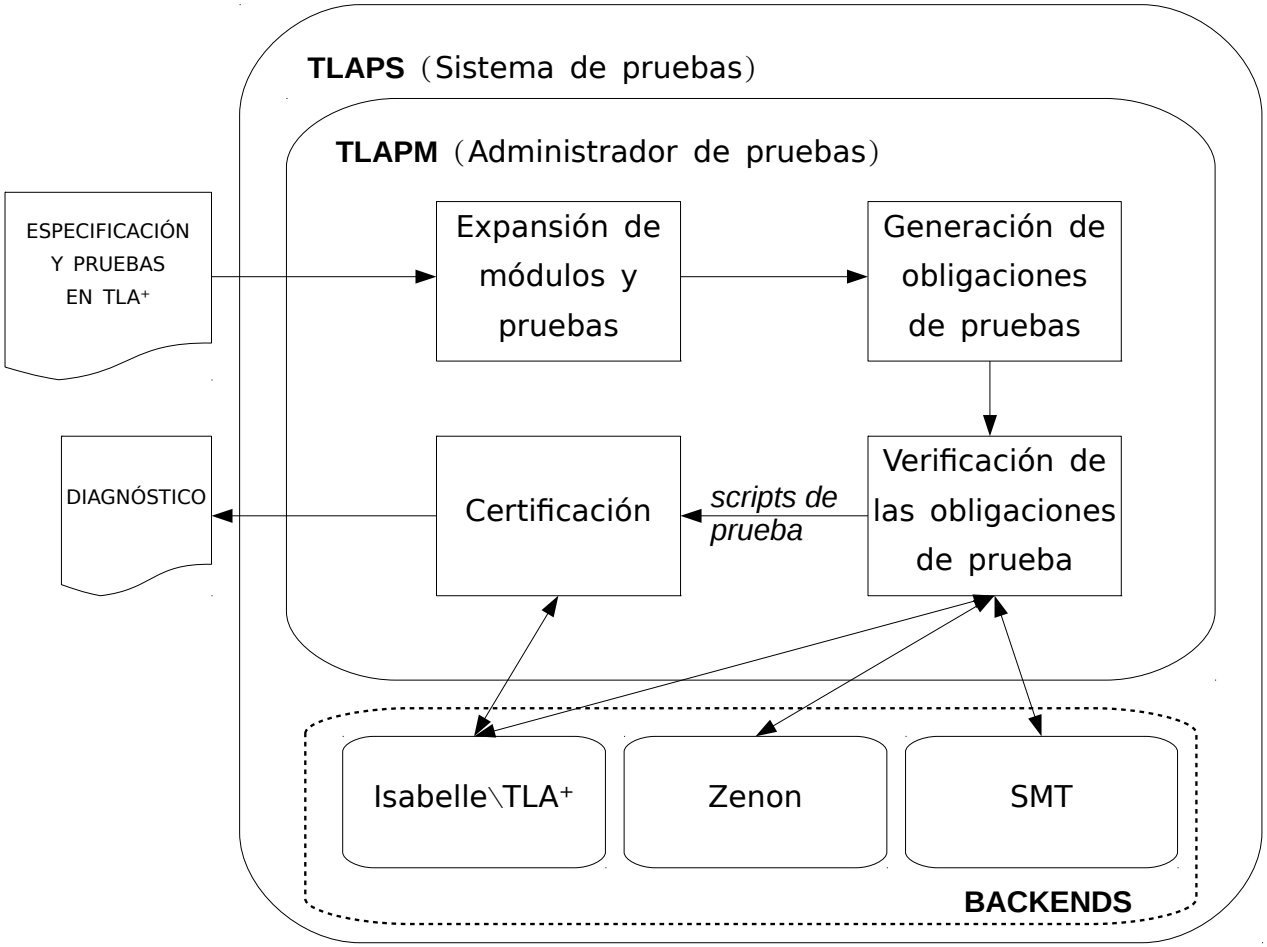
- Expandir e instanciar módulos (usando estado implícito)
- Generar obligaciones de prueba
- Invocar a los backends para verificar las obligaciones de pruebas
- Generar estructura del lema
- Generar prueba del teorema usando las obligaciones ya certificadas

Backends

Para corroborar una obligación de prueba, el comportamiento por defecto de TLAPS es probar con 3 backends en sucesión:

- SMT: invocado por defecto, timeout: 5 segundos
- Zenon: lógica de primer orden, timeout: 10 segundos
- Isa: probador automático de Isabelle, timeout: 30 segundos

Si Isabelle no puede encontrar una prueba, TLAPS (por medio de TLAPM) reporta una falla al intentar demostrar dicha obligación.



Arquitectura general de TLAPS

- Amazon
  - DynamoDB, S3, EBS
  - Bugs críticos pero sutiles: ¡trazas de hasta **35** pasos!
  - creciente adopción en la empresa
- XBOX 360
  - bug **crítico** en sistema de memoria
  - lo descubrió un pasante con TLA+
  - cada XBOX 360 se habría colgado tras 4 horas de uso

- Amazon
  - DynamoDB, S3, EBS
  - Bugs críticos pero sutiles: ¡trazas de hasta **35** pasos!
  - creciente adopción en la empresa
- XBOX 360
  - bug **crítico** en sistema de memoria
  - lo descubrió un pasante con TLA+
  - cada XBOX 360 se habría colgado tras 4 horas de uso

- Amazon
  - DynamoDB, S3, EBS
  - Bugs críticos pero sutiles: ¡trazas de hasta **35** pasos!
  - creciente adopción en la empresa
- XBOX 360
  - bug **crítico** en sistema de memoria
  - lo descubrió un pasante con TLA+
  - cada XBOX 360 se habría colgado tras 4 horas de uso

- Amazon
  - DynamoDB, S3, EBS
  - Bugs críticos pero sutiles: ¡trazas de hasta **35** pasos!
  - creciente adopción en la empresa
- XBOX 360
  - bug **crítico** en sistema de memoria
  - lo descubrió un pasante con TLA+
  - cada XBOX 360 se habría colgado tras 4 horas de uso

- Amazon
  - DynamoDB, S3, EBS
  - Bugs críticos pero sutiles: ¡trazas de hasta **35** pasos!
  - creciente adopción en la empresa
- XBOX 360
  - bug **crítico** en sistema de memoria
  - lo descubrió un pasante con TLA+
  - cada XBOX 360 se habría colgado tras 4 horas de uso

- Amazon
  - DynamoDB, S3, EBS
  - Bugs críticos pero sutiles: ¡trazas de hasta **35** pasos!
  - creciente adopción en la empresa
- XBOX 360
  - bug **crítico** en sistema de memoria
  - lo descubrió un pasante con TLA+
  - cada XBOX 360 se habría colgado tras 4 horas de uso

- Amazon
  - DynamoDB, S3, EBS
  - Bugs críticos pero sutiles: ¡trazas de hasta **35** pasos!
  - creciente adopción en la empresa
- XBOX 360
  - bug **crítico** en sistema de memoria
  - lo descubrió un pasante con TLA+
  - cada XBOX 360 se habría colgado tras 4 horas de uso

- Amazon
  - DynamoDB, S3, EBS
  - Bugs críticos pero sutiles: ¡trazas de hasta **35** pasos!
  - creciente adopción en la empresa
- XBOX 360
  - bug **crítico** en sistema de memoria
  - lo descubrió un pasante con TLA+
  - cada XBOX 360 se habría colgado tras 4 horas de uso

- Farsite
  - Sistema de archivos distribuido ≈ NTFS
  - TLA+ para especificar y verificar propiedades concurrentes
- Byzantine Paxos
  - Tolerancia a fallas maliciosas en sistemas distribuidos
  - Prueba formal

- Farsite
  - Sistema de archivos distribuido ≈ NTFS
  - TLA+ para especificar y verificar propiedades concurrentes
- Byzantine Paxos
  - Tolerancia a fallas maliciosas en sistemas distribuidos
  - Prueba formal

- Farsite
  - Sistema de archivos distribuido ≈ NTFS
  - TLA+ para especificar y verificar propiedades concurrentes
- Byzantine Paxos
  - Tolerancia a fallas maliciosas en sistemas distribuidos
  - Prueba formal

- Farsite
  - Sistema de archivos distribuido ≈ NTFS
  - TLA+ para especificar y verificar propiedades concurrentes
- Byzantine Paxos
  - Tolerancia a fallas maliciosas en sistemas distribuidos
  - Prueba formal

- Farsite
  - Sistema de archivos distribuido ≈ NTFS
  - TLA+ para especificar y verificar propiedades concurrentes
- Byzantine Paxos
  - Tolerancia a fallas maliciosas en sistemas distribuidos
  - Prueba formal

- Farsite
  - Sistema de archivos distribuido $\approx$ NTFS
  - TLA+ para especificar y verificar propiedades concurrentes
- Byzantine Paxos
  - Tolerancia a fallas maliciosas en sistemas distribuidos
  - Prueba formal

TLA+ vs Alloy

- Concepto de modelado similar
- TLA+ es mucho mas expresivo que Alloy
- Importancia en la práctica
- Muchas especificaciones reales escritas en TLA+ son casi imposibles de escribir en Alloy

TLA+ vs Alloy

- Concepto de modelado similar
- TLA+ es mucho mas expresivo que Alloy
- Importancia en la práctica
- Muchas especificaciones reales escritas en TLA+ son casi imposibles de escribir en Alloy

TLA+ vs Alloy

- Concepto de modelado similar
- TLA+ es mucho mas expresivo que Alloy
- Importancia en la práctica
- Muchas especificaciones reales escritas en TLA+ son casi imposibles de escribir en Alloy

TLA+ vs Alloy

- Concepto de modelado similar
- TLA+ es mucho mas expresivo que Alloy
- Importancia en la práctica
- Muchas especificaciones reales escritas en TLA+ son casi imposibles de escribir en Alloy

Herramientas similares a TLAPS

- Isar
  - Corre sobre Isabelle
  - Estilo de desarrollo diferente
  - Bueno para pruebas cortas pero no tanto para pruebas largas
- Focal
  - Subconjunto de TLA+, que incluye el desarrollo de demostraciones jerárquicamente.
- Coq
  - Corre sobre Zenon
  - Desarrollo semi-interactivo

Herramientas similares a TLAPS

- Isar
  - Corre sobre Isabelle
  - Estilo de desarrollo diferente
  - Bueno para pruebas cortas pero no tanto para pruebas largas
- Focal
  - Subconjunto de TLA+, que incluye el desarrollo de demostraciones jerárquicamente.
- Coq
  - Corre sobre Zenon
  - Desarrollo semi-interactivo

Herramientas similares a TLAPS

- Isar
  - Corre sobre Isabelle
  - Estilo de desarrollo diferente
  - Bueno para pruebas cortas pero no tanto para pruebas largas
- Focal
  - Subconjunto de TLA+, que incluye el desarrollo de demostraciones jerárquicamente.
- Coq
  - Corre sobre Zenon
  - Desarrollo semi-interactivo

Herramientas similares a TLAPS

- Isar
  - Corre sobre Isabelle
  - Estilo de desarrollo diferente
  - Bueno para pruebas cortas pero no tanto para pruebas largas
- Focal
  - Subconjunto de TLA+, que incluye el desarrollo de demostraciones jerárquicamente.
- Coq
  - Corre sobre Zenon
  - Desarrollo semi-interactivo

Herramientas similares a TLAPS

- Isar
  - Corre sobre Isabelle
  - Estilo de desarrollo diferente
  - Bueno para pruebas cortas pero no tanto para pruebas largas
- Focal
  - Subconjunto de TLA+, que incluye el desarrollo de demostraciones jerárquicamente.
- Coq
  - Corre sobre Zenon
  - Desarrollo semi-interactivo

Herramientas similares a TLAPS

- Isar
  - Corre sobre Isabelle
  - Estilo de desarrollo diferente
  - Bueno para pruebas cortas pero no tanto para pruebas largas
- Focal
  - Subconjunto de TLA+, que incluye el desarrollo de demostraciones jerárquicamente.
- Coq
  - Corre sobre Zenon
  - Desarrollo semi-interactivo

Herramientas similares a TLAPS

- Isar
  - Corre sobre Isabelle
  - Estilo de desarrollo diferente
  - Bueno para pruebas cortas pero no tanto para pruebas largas
- Focal
  - Subconjunto de TLA+, que incluye el desarrollo de demostraciones jerárquicamente.
- Coq
  - Corre sobre Zenon
  - Desarrollo semi-interactivo

Herramientas similares a TLAPS

- Isar
  - Corre sobre Isabelle
  - Estilo de desarrollo diferente
  - Bueno para pruebas cortas pero no tanto para pruebas largas
- Focal
  - Subconjunto de TLA+, que incluye el desarrollo de demostraciones jerárquicamente.
- Coq
  - Corre sobre Zenon
  - Desarrollo semi-interactivo

Herramientas similares a TLAPS

- Isar
  - Corre sobre Isabelle
  - Estilo de desarrollo diferente
  - Bueno para pruebas cortas pero no tanto para pruebas largas
- Focal
  - Subconjunto de TLA+, que incluye el desarrollo de demostraciones jerárquicamente.
- Coq
  - Corre sobre Zenon
  - Desarrollo semi-interactivo

correctitud del algoritmo de Euclides

Conclusiones

- TLA+ :
  - Simple pero expresivo (notación matemática simple)
  - Toolbox facilita interacción
  - Buena aceptación en la industria
- TLAPS:
  - Ventaja de TLA+ sobre otros *Model Checkers*
  - Demasiado específico → Poco uso en la industria

Conclusiones

- TLA+ :
  - Simple pero expresivo (notación matemática simple)
  - Toolbox facilita interacción
  - Buena aceptación en la industria
- TLAPS:
  - Ventaja de TLA+ sobre otros *Model Checkers*
  - Demasiado específico → Poco uso en la industria

Conclusiones

- TLA+ :
  - Simple pero expresivo (notación matemática simple)
  - Toolbox facilita interacción
  - Buena aceptación en la industria
- TLAPS:
  - Ventaja de TLA+ sobre otros *Model Checkers*
  - Demasiado específico → Poco uso en la industria

Conclusiones

- TLA+ :
  - Simple pero expresivo (notación matemática simple)
  - Toolbox facilita interacción
  - Buena aceptación en la industria
- TLAPS:
  - Ventaja de TLA+ sobre otros *Model Checkers*
  - Demasiado específico → Poco uso en la industria

Conclusiones

- TLA+ :
  - Simple pero expresivo (notación matemática simple)
  - Toolbox facilita interacción
  - Buena aceptación en la industria
- TLAPS:
  - Ventaja de TLA+ sobre otros *Model Checkers*
  - Demasiado específico $\rightarrow$ Poco uso en la industria

Conclusiones

- TLA+ :
  - Simple pero expresivo (notación matemática simple)
  - Toolbox facilita interacción
  - Buena aceptación en la industria
- TLAPS:
  - Ventaja de TLA+ sobre otros *Model Checkers*
  - Demasiado específico $\rightarrow$ Poco uso en la industria

Conclusiones

- TLA+ :
  - Simple pero expresivo (notación matemática simple)
  - Toolbox facilita interacción
  - Buena aceptación en la industria
- TLAPS:
  - Ventaja de TLA+ sobre otros *Model Checkers*
  - Demasiado específico $\rightarrow$ Poco uso en la industria

¿Preguntas?

¡Gracias por escuchar!