Gemas de la Computación Teórica

Coq: qué, cómo y porqué (Parte II)

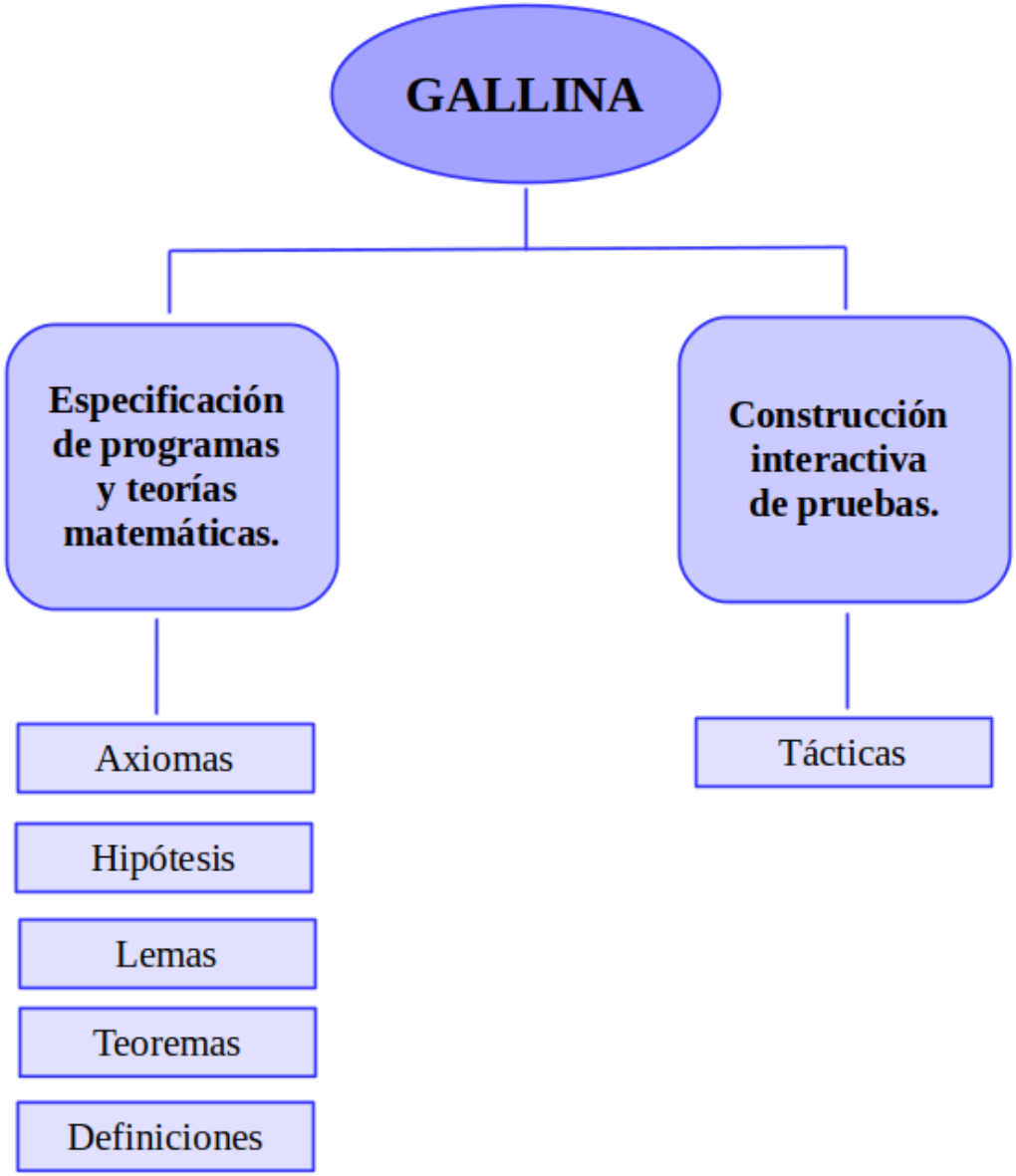
Lourdes González Huesca
luglzhuesca@ciencias.unam.mx

Selene Linares Arévalo
selene_linares@ciencias.unam.mx

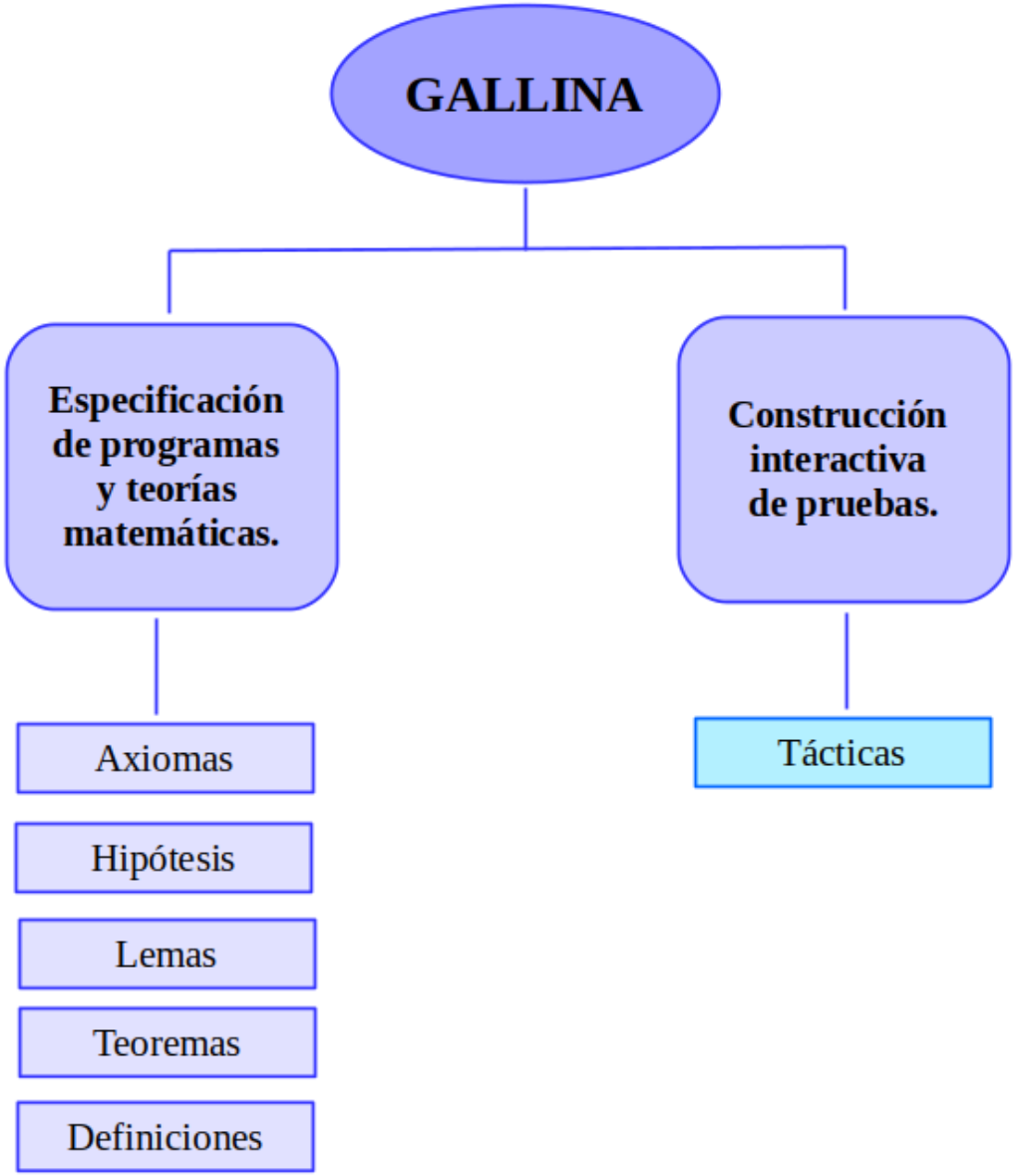
Facultad de Ciencias, UNAM
Proyecto PAPIME PE102117

21 y 23 de agosto 2018

Gallina

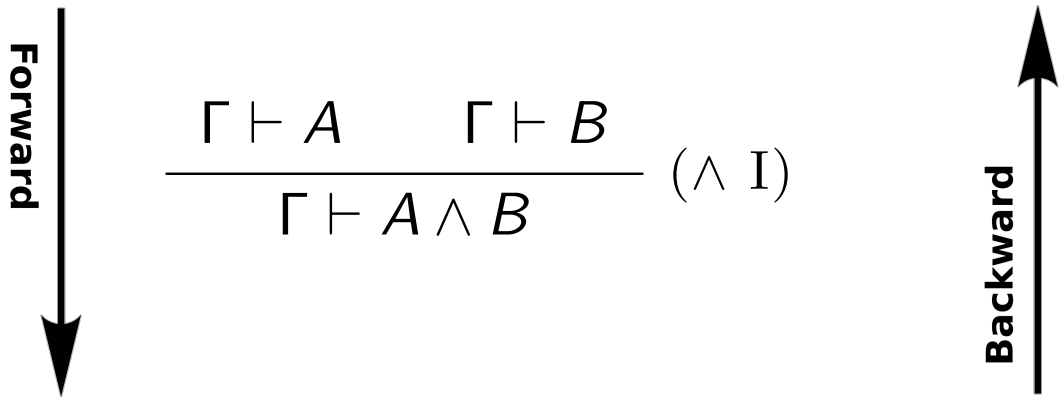

GALLINA
Especificación de programas y teorías matemáticas.
Construcción interactiva de pruebas.
Axiomas
Hipótesis
Lemas
Teoremas
Definiciones
Tácticas

Gallina


GALLINA
Especificación de programas y teorías matemáticas.
Construcción interactiva de pruebas.
Axiomas
Hipótesis
Lemas
Teoremas
Definiciones
Tácticas

Tácticas

Una regla de deducción puede ser leída de dos maneras:



have to prove B. This is backward reasoning from conclusion to premises. We say that the conclusion is the *goal* to prove and premises are the *subgoals*. The tactics implement *backward reasoning*. When applied to a goal, a tactic replaces this goal with the subgoals it generates. We say that a tactic reduces a goal to its subgoal(s).

Tácticas

¿Qué tienen en común?

```
(** Ahora una sencilla verificacion:
asegurarse que las funciones antes definidas son inversas *)
Theorem inject_inverse :
  forall (ls : list nat), unject (inject ls) = ls.
Proof.
induction ls.
- simpl.
  reflexivity.
- simpl.
  rewrite IHls.
  reflexivity.
Qed.

Check inject_inverse.
Print inject_inverse.
```

Tácticas

Razonamiento ecuacional

$$\frac{}{\Gamma \vdash t = t}\ \textsc{Refl}$$

para mostrar $\Gamma \vdash t = t$, no es necesario mostrar algo más.

`reflexivity`: $\quad \Gamma \vdash C = C\,;\mathcal{S} \quad \triangleright \quad \mathcal{S}$

Tácticas

Razonamiento ecuacional

$$\frac{\Gamma, H : t = s \vdash E[x := s]}{\Gamma, H : t = s \vdash E[x := t]}\ \textsc{Rewrite}(\mathrm{H})$$

Para mostrar que $\Gamma, H : t = s \vdash E[x := t]$ es suficiente mostrar que

$$\Gamma, H : t = s \vdash E[x := s].$$

`rewrite H`:

$\Gamma, H : t = s \vdash E[x := t]\,; \mathcal{S} \quad \triangleright \quad \Gamma, H2 : t = s \vdash E[x := s]\,; \mathcal{S}$

Tácticas

Razonamiento ecuacional

$$\frac{\Gamma, H : t = s \vdash E[x := t]}{\Gamma, h : t = s \vdash E[x := s]}\ \textsc{Rewrite}(\mathrm{H})$$

Para mostrar que $\Gamma, H : t = s \vdash E[x := s]$ es suficiente mostrar que

$$\Gamma, H : t = s \vdash E[x := t].$$

`rewrite <- H`:

$\Gamma, H : t = s \vdash E[x := s]\,;\mathcal{S} \quad \triangleright \quad \Gamma, H2 : t = s \vdash E[x := t]\,;\mathcal{S}$

Tácticas

Conectivos Lógicos

- **Inversión de reglas de Introducción :**
  - `intro`: $\Gamma \vdash A \to B; \mathcal{S} \rhd \Gamma, A \vdash B; \mathcal{S}$
  - `split`: $\Gamma \vdash A \wedge B; \mathcal{S} \rhd \Gamma \vdash A; \Gamma \vdash B; \mathcal{S}$
  - `left`: $\Gamma \vdash A \vee B; \mathcal{S} \rhd \Gamma \vdash A; \mathcal{S}$
  - `right`: $\Gamma \vdash A \vee B; \mathcal{S} \rhd \Gamma \vdash B; \mathcal{S}$
  - `intro`: $\Gamma \vdash \forall x A; \mathcal{S} \rhd \Gamma \vdash A; \mathcal{S}$ where w.l.o.g., $x \notin FV(\Gamma)$
  - `exists`: $\Gamma \vdash \exists x A; \mathcal{S} \rhd \Gamma \vdash A[x := t]; \mathcal{S}$

Tácticas

Reglas de Eliminación

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma,\ H1 : A \vdash C \qquad \Gamma,\ H2 : B \vdash C}{\Gamma \vdash C}\ (\vee\ \mathrm{E})$$

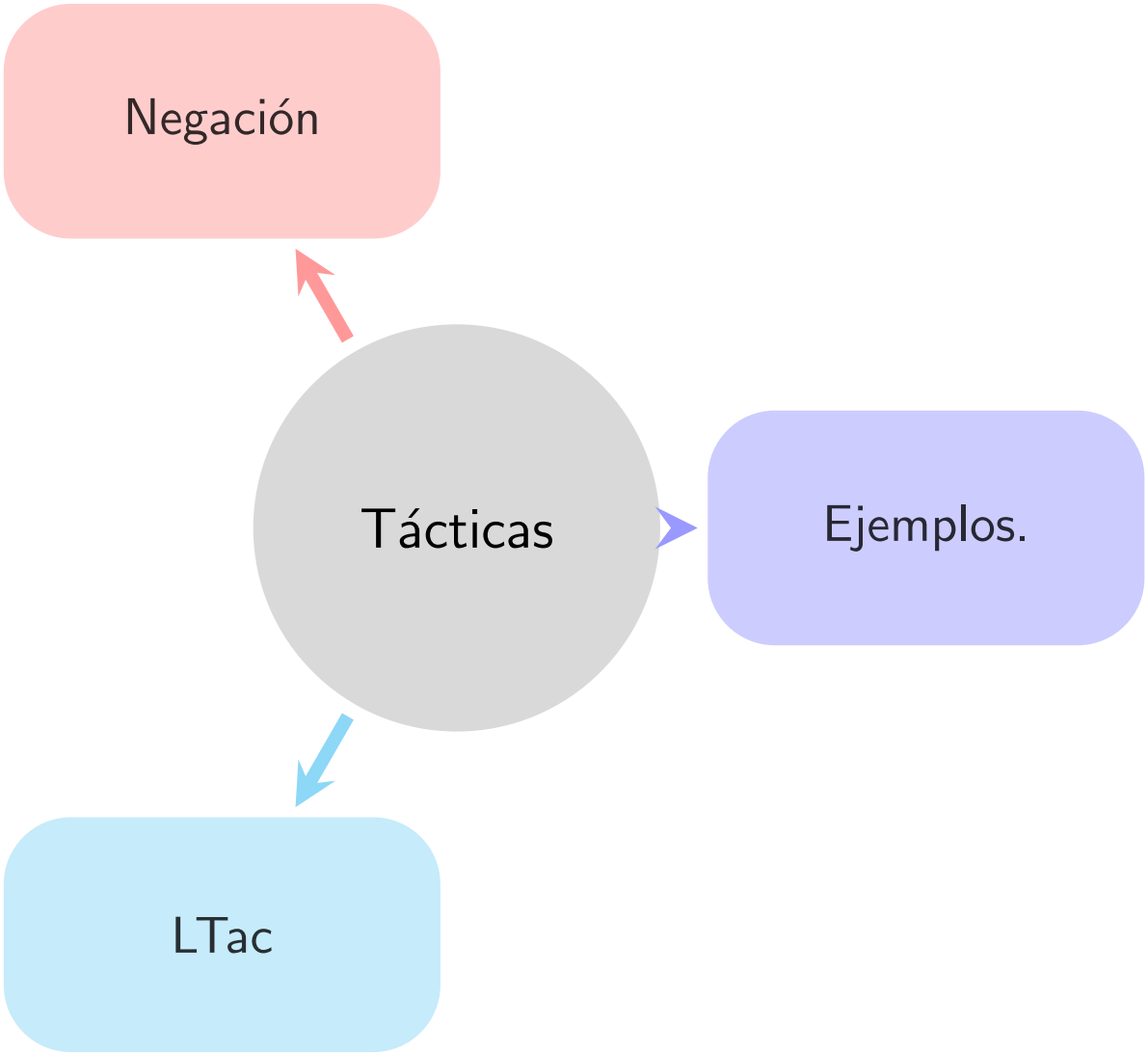
Para mostrar que $\Gamma, H : A \vee B \vdash C$ es suficiente con demostrar que

$$\Gamma, H1 : A \vdash C \quad \text{y} \quad \Gamma, H2 : B \vdash C.$$

$$\frac{\Gamma,\ H1 : A \vdash C \qquad \Gamma,\ H2 : B \vdash C}{\Gamma,\ H : A \vee B \vdash C}\ (\vee\ \mathrm{P})$$

`destruct`: $\Gamma, H : A \vee B \vdash C; \mathcal{S} \ \triangleright\ \Gamma, H1 : A \vdash C\ \mathbf{;}\ \Gamma, H2 : B \vdash C\ \mathbf{;}\ \mathcal{S}$

Tácticas



A Formal Specification of the MIDP 2.0 Security Model*

Santiago Zanella Béguelin[1], Gustavo Betarte[2], and Carlos Luna[2]

[1] INRIA Sophia Antipolis, 06902 Sophia Antipolis Cedex, France
Santiago.Zanella@sophia.inria.fr
[2] InCo, Facultad de Ingeniería, Universidad de la República, Montevideo, Uruguay
{gustun,cluna}@fing.edu.uy

Abstract. This paper presents, to the best of our knowledge, the first formal specification of the application security model defined by the Mobile Information Device Profile 2.0 for Java 2 Micro Edition. The specification, which has been formalized in Coq, provides an abstract representation of the state of a device and the security-related events that allows to reason about the security properties of the platform where the model is deployed. We state and sketch the proof of some desirable properties of the security model. Although the abstract specification is not executable, we describe a refinement methodology that leads to an executable prototype.

A Formal Specification of the DNSSEC Model

Ezequiel Bazan Eixarch[1], Gustavo Betarte[2], and Carlos Luna[2]

[1] ezequielbazan@gmail.com
Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Universidad Nacional de Rosario, Rosario, Argentina

[2] [gustun,cluna]@fing.edu.uy
Instituto de Computación, Facultad de Ingeniería
Universidad de la República, Montevideo, Uruguay

Abstract: The Domain Name System Security Extensions (DNSSEC) is a suite of specifications that provide origin authentication and integrity assurance services for DNS data. In particular, DNSSEC was designed to protect resolvers from forged DNS data, such as the one generated by DNS cache poisoning. This article presents a minimalistic specification of a DNSSEC model which provides the grounds needed to formally state and verify security properties concerning the chain of trust of the DNSSEC tree. The model, which has been formalized and verified using the Coq proof assistant, specifies an abstract formulation of the behavior of the protocol and the corresponding security-related events, where security goals, such as the prevention of cache poisoning attacks, can be given a formal treatment.

Keywords: DNS, DNSSEC, security properties, formal modelling, Coq

¡GRACIAS!