A Formal Proof of the Basic Perturbation Lemma*

Jónathan Heras
(joint work with M. Poza, C. Domínguez, and J. Rubio)

Department of Mathematics and Computer Science
University of La Rioja (Spain)

December 2014
de Brún Workshop on Homological Perturbation Theory

*Partially supported by Ministerio de Educación y Ciencia, project MTM2009-13842-C02-01, and by European Commission FP7, STREP project ForMath, n. 243847

Motivation

Can we trust published mathematical-proofs?

Motivation

Can we trust published mathematical-proofs?

A. B. Kempe. On the geographical problem of four-colours. American Journal of Mathematics 2(3):193–200, 1879.

A. Wiles. Modular elliptic curves and Fermat's Last Theorem. Annals of Mathematics 142:443–551, 1995.

R. Mikhailov and J. Wu. On homotopy groups on the suspended classifying spaces. Algebraic and Geometric Topology 10:565–625, 2010.

E. Gallardo and C. Cowen. Rota's Universal Operators and Invariant Subspaces in Hilbert Spaces. Submitted but withdraw by the authors, 2013.

M. Lecat. Erreurs de Mathématiciens des origines à nos jours, 1935.

List of incomplete proofs: `http://en.wikipedia.org/wiki/List_of_incomplete_proofs`.

Motivation

Some proofs are really long and complex:

- A. Wiles. Modular elliptic curves and Fermat's Last Theorem. Annals of Mathematics 142:443–551, 1995. (98 pages.)
- N. Robertson and P. Seymour. Graph minors I–XX. Journal of Combinatorial Theory, Series B, 1983–2004. (Approximately 500 pages.)
- Classification of the Finite Simple Groups. (Approximately 500 papers and 100 authors.)

Motivation

Some proofs are really long and complex:

- A. Wiles. Modular elliptic curves and Fermat's Last Theorem. Annals of Mathematics 142:443–551, 1995. (98 pages.)
- N. Robertson and P. Seymour. Graph minors I–XX. Journal of Combinatorial Theory, Series B, 1983–2004. (Approximately 500 pages.)
- Classification of the Finite Simple Groups. (Approximately 500 papers and 100 authors.)

Some theorems are proven relying on results obtained by computers:

- K. Appel and W. Haken. Every Map is Four Colourable. Bulletin of the American Mathematical Society 82(5):711-712, 1976.
- T. C. Hales. A proof of the Kepler conjecture. Annals of Mathematics 162:1065–1185, 2005.
- A. Romero and J. Rubio. Homotopy groups of suspended classifying spaces: an experimental approach. Mathematics of Computation 82:2237–2244, 2013.

Formal Proofs

How can we increase the trustworthiness of our proofs?

Formal Proofs

How can we increase the trustworthiness of our proofs? Formal Proofs.

Formal Proofs

How can we increase the trustworthiness of our proofs? Formal Proofs.

Definition

A formal proof is a proof that has been verified from first principles.

Formal Proofs

How can we increase the trustworthiness of our proofs? Formal Proofs.

Definition

A formal proof is a proof that has been verified from first principles.

Generally speaking, formal proofs are constructed using computers. Namely, Interactive Proof Assistant:

Formal Proofs

How can we increase the trustworthiness of our proofs? Formal Proofs.

Definition

A formal proof is a proof that has been verified from first principles.

Generally speaking, formal proofs are constructed using computers. Namely, Interactive Proof Assistant:

- Software tool for the development of formal proofs.
- Require Man-Machine collaboration:
  - Human: designs the proofs.
  - Machine: fill the gaps.
- Several systems: Isabelle, HOL, ACL2, Mizar, Coq, ...
  - different underlying logics: set-theory, first-order logic, higher-order logic, Calculus of Inductive Constructions.

Interactive Proof Assistants

Can Interactive Proof Assistants be used in actual mathematics?

Interactive Proof Assistants

Can Interactive Proof Assistants be used in actual mathematics?

G. Gonthier. Formal proof — The Four-Colour Theorem. Notices of the American Mathematical Society 55(11):1382–1393, 2008.

G. Gonthier et al. A Machine-Checked Proof of the Odd Order Theorem. Proceedings of ITP'2013:163–179, 2013.

Flyspeck project. A formal proof of the Kepler conjecture. `https://code.google.com/p/flyspeck/wiki/AnnouncingCompletion`, 2014.

Other examples: the Jordan curve theorem, the prime number theorem, the fundamental theorem of algebra, . . .

Formalising 100 theorems (`http://www.cs.ru.nl/F.Wiedijk/100/index.html`) — currently at 90%.

An Interactive Proof Assistant: Coq

Coq:

- An Interactive Proof Assistant.
- Based on the Calculus of Inductive Constructions — a constructive higher-order typed lambda calculus.
- Constructive proofs — we can extract programs from the proofs.

An Interactive Proof Assistant: Coq

Coq:

- An Interactive Proof Assistant.
- Based on the Calculus of Inductive Constructions — a constructive higher-order typed lambda calculus.
- Constructive proofs — we can extract programs from the proofs.

SSReflect:

- Extension of Coq.
- Developed while formalising the Four Colour Theorem, and intensively used in the formalisation of the Odd Order Theorem.
- Simplifies Coq developments, and provides several useful libraries.

An Interactive Proof Assistant: Coq

Coq:

- An Interactive Proof Assistant.
- Based on the Calculus of Inductive Constructions — a constructive higher-order typed lambda calculus.
- Constructive proofs — we can extract programs from the proofs.

SSReflect:

- Extension of Coq.
- Developed while formalising the Four Colour Theorem, and intensively used in the formalisation of the Odd Order Theorem.
- Simplifies Coq developments, and provides several useful libraries.

A small demo.

Outline

1. Formal Proofs related to Homological Perturbation Theory
2. A Formal Proof of Sergeraert's Proof of the BPL
3. Conclusions

Outline

1. Formal Proofs related to Homological Perturbation Theory
2. A Formal Proof of Sergeraert's Proof of the BPL
3. Conclusions

Main Definition

Definition

A *reduction* ρ between two chain complexes C_* y D_* (denoted by $\rho : C_* \Rightarrow D_*$) is a triple $\rho = (f, g, h)$

$$\begin{tikzcd} C_* \arrow[loop left, "h"] \arrow[r, bend left, "f"] & D_* \arrow[l, bend left, "g"] \end{tikzcd}$$

satisfying the following relations:

1) $fg = \mathrm{Id}_{D_*}$;
2) $dh + hd = \mathrm{Id}_{C_*} - gf$;
3) $fh = 0$; $\quad hg = 0$; $\quad hh = 0$.

Theorem

If $C_* \Rightarrow D_*$, then $C_* \cong D_* \oplus A_*$, with A_* acyclic, which implies that $H_n(C_*) \cong H_n(D_*)$ for all n.

Formal Proofs related to HPT

Formalised in Isabelle/HOL (Higher-Order Logic):

Theorem (Basic Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{C_*}. We assume the nilpotency hypothesis is satisfied: for every $c \in C_n$, there exists $\nu \in \mathbb{N}$ such that $(\widehat{\delta} h)^\nu(c) = 0$. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + \widehat{\delta}) \Rightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

J. Aransay, C. Ballarin, and J. Rubio. A mechanized proof of the Basic Perturbation Lemma. Journal of Automated Reasoning, 40(4):271–292, 2008.

Theorem (Trivial Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{D_*}. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + g\widehat{\delta}f) \Rightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

J. Aransay and C. Domínguez. Modelling Differential Structures in Proof Assistants: The Graded Case. LNCS 5717:203–210, 2009.

Formal Proofs related to HPT

Formalisations in ACL2 (First-Order Logic):

Theorem (Normalisation Reduction)

Given a simplicial set K, there exists a reduction $C(K) \Rightarrow C^N(K)$, where $C(K)$ and $C^N(K)$ are, respectively, the chain complex and the normalised chain complex associated with K.

L. Lambán, F. J. Martín-Mateos, J. L. Ruiz-Reina, and J. Rubio. Formalization of a Normalization Theorem in Simplicial Topology. Annals of Mathematics and Artificial Intelligence 64(1):1–37, 2012.

Theorem (Eilenberg-Zilber Theorem)

Given two simplicial sets K^1 and K^2, there exists a reduction $C(K^1 \times K^2) \Rightarrow C(K^1) \otimes C(K^2)$.

L. Lambán, J. Rubio, F. J. Martín-Mateos, and J. L. Ruiz-Reina. Verifying the bridge between simplicial topology and algebra: the Eilenberg–Zilber algorithm. Logic Journal of the IGPL 22(1):39–65, 2013.

- Other formalisations: Cone Reduction theorem, Trivial Perturbation lemma and SES theorems.

Formal Proofs related to HPT

Formalisations in Coq (Constructive Higher-Order Logic):

Theorem (Effective Homology of Bicomplexes)

Let $B = \{B_p, b_p\}_{p \in \mathbb{N}}$ be a bicomplex such that each chain complex B_p is an object with effective homology, for all $p \in \mathbb{N}$. Then, the bicomplex B is an object with effective homology.

C. Domínguez and J. Rubio. Effective Homology of Bicomplexes, formalized in Coq. Theoretical Computer Science, 412:962–970, 2011.

Theorem (Vector-Field Reduction Theorem)

Let $C = (C_p, d_p)_{p \in \mathbb{N}}$ be a chain complex with a distinguished basis $\{\beta_p\}_{p \in \mathbb{N}}$, and $V = (\alpha_i, \beta_i)_{i \in \beta}$ be an admissible discrete vector field on C. Then the vector field V defines a canonical reduction $\rho = (f, g, h) : (C_p, d_p) \Rightarrow (C_p^c, d_p^c)$ where $C_p^c = \mathbb{Z}[\beta_p]$ is the free $\mathbb{Z}$-module generated by the critical p-cells.

M. Poza, C. Domínguez, J. Heras, and J. Rubio. A certified reduction strategy for homological image processing. ACM Transactions on Computational Logic, 15(3), 2014.

- Other formalisations: Cone Reduction theorem and Trivial Perturbation lemma.

Outline

A Formal Proof of Sergeraert's Proof

A formal proof of Sergeraert's proof of the BPL was presented in:

M. Poza, C. Domínguez, J. Heras, and J. Rubio. A certified reduction strategy for homological image processing. ACM Transactions on Computational Logic, 15(3), 2014.

M. Poza. Certifying homological algorithms to study biomedical images. Ph.D. thesis, University of La Rioja, 2013.

A Formal Proof of Sergeraert's Proof

A formal proof of Sergeraert's proof of the BPL was presented in:

M. Poza, C. Domínguez, J. Heras, and J. Rubio. A certified reduction strategy for homological image processing. ACM Transactions on Computational Logic, 15(3), 2014.

M. Poza. Certifying homological algorithms to study biomedical images. Ph.D. thesis, University of La Rioja, 2013.

- This proof was given in Coq/SSReflect, and it was restricted to finitely generated chain complexes over a field.

A Formal Proof of Sergeraert's Proof

A formal proof of Sergeraert's proof of the BPL was presented in:

M. Poza, C. Domínguez, J. Heras, and J. Rubio. A certified reduction strategy for homological image processing. ACM Transactions on Computational Logic, 15(3), 2014.

M. Poza. Certifying homological algorithms to study biomedical images. Ph.D. thesis, University of La Rioja, 2013.

- This proof was given in Coq/SSReflect, and it was restricted to finitely generated chain complexes over a field.
- In this scenario, we can use matrices to represent chain complexes, chain complex morphisms, and so on.

A Formal Proof of Sergeraert's Proof

A formal proof of Sergeraert's proof of the BPL was presented in:

M. Poza, C. Domínguez, J. Heras, and J. Rubio. A certified reduction strategy for homological image processing. ACM Transactions on Computational Logic, 15(3), 2014.

M. Poza. Certifying homological algorithms to study biomedical images. Ph.D. thesis, University of La Rioja, 2013.

- This proof was given in Coq/SSReflect, and it was restricted to finitely generated chain complexes over a field.
- In this scenario, we can use matrices to represent chain complexes, chain complex morphisms, and so on.
- Some figures:
    - 356 definitions (63 are new),
    - 532 lemmas (117 are new), and
    - 8419 lines of code (2416 related to BPL).

Some Aspects of the Formalisation

- The role of SSReflect.
- Main mathematical structures.
- Key points of the proof.
- Live proof of a property.

The Role of SSReflect

- SSReflect language improves efficiency when writing proofs.

The Role of SSReflect

- SSReflect language improves efficiency when writing proofs.
- Libraries:
  - basic infrastructure: natural numbers, integers, booleans, ...

The Role of SSReflect

- SSReflect language improves efficiency when writing proofs.
- Libraries:
  - basic infrastructure: natural numbers, integers, booleans, ...
  - matrix.v and mxalgebra.v: matrix theory (multiplication, determinant, matrix decomposition, ...).

    Lemma mul_row_col: $\left(\alpha \mid \beta \right) \times \left(\frac{\gamma}{\eta} \right) = \alpha \times \gamma + \beta \times \eta$

The Role of SSReflect

- SSReflect language improves efficiency when writing proofs.
- Libraries:
  - basic infrastructure: natural numbers, integers, booleans, ...
  - matrix.v and mxalgebra.v: matrix theory (multiplication, determinant, matrix decomposition, ...).

    `Lemma mul_row_col:` $\left(\alpha \mid \beta \right) \times \left(\frac{\gamma}{\eta} \right) = \alpha \times \gamma + \beta \times \eta$
  - bigop.v: library related to big operators.

    `Lemma big_distrr:` $a \times \sum_{0 \leq i < n} F_i = \sum_{0 \leq i < n} (a \times F_i)$.

The Role of SSReflect

- SSReflect language improves efficiency when writing proofs.
- Libraries:
  - basic infrastructure: natural numbers, integers, booleans, ...
  - matrix.v and mxalgebra.v: matrix theory (multiplication, determinant, matrix decomposition, ...).

    `Lemma mul_row_col:` $\begin{pmatrix} \alpha \mid \beta \end{pmatrix} \times \begin{pmatrix} \frac{\gamma}{\eta} \end{pmatrix} = \alpha \times \gamma + \beta \times \eta$
  - bigop.v: library related to big operators.
    `Lemma big_distrr:` $a \times \sum_{0 \leq i < n} F_i = \sum_{0 \leq i < n} (a \times F_i)$.
  - ...

Main Mathematical Structures

SSReflect provides the basic infrastructure, but we need to define our own notions.

Main Mathematical Structures

SSReflect provides the basic infrastructure, but we need to define our own notions.

- Finitely generated chain complexes over a field:

```
Variable K : fieldType.

Record FGChain_Complex :=
  { m : Z -> nat;
    diff : forall i:Z, M[K]_(m (i + 1), m i);
    boundary : forall i:Z, (diff (i + 1)) *m (diff i) = 0}.
```

Main Mathematical Structures

SSReflect provides the basic infrastructure, but we need to define our own notions.

- Finitely generated chain complexes over a field:

```
Variable K : fieldType.

Record FGChain_Complex :=
  { m : Z -> nat;
    diff : forall i:Z, M[K]_(m (i + 1), m i);
    boundary : forall i:Z, (diff (i + 1)) *m (diff i) = 0}.
```

- Chain complex morphisms and homotopy operators:

```
Record FGChain_Complex_Morphism (A B : FGChain_Complex) :=
  { M : forall i:Z, M[K]_((m A i),(m B i));
    M_well_defined : forall i:Z,
                     (diff A i) *m (M i) = (M (i+1)) *m (diff B i)}.

Record FGHomotopy_operator (A : FGChain_Complex) :=
  { Ho : forall i:Z, M[K]_(m A i, m A (i+1))}.
```

Main Mathematical Structures

- Reduction:

```
Record FGReduction :=
{ C : FGChain_Complex;
  D : FGChain_Complex;
  F : FGChain_Complex_Morphism C D;
  G : FGChain_Complex_Morphism D C;
  H : FGHomotopy_operator C;
  ax1 : forall i:Z, (M G i) *m (M F i) = 1%:M;
  ax2 : forall i:Z, (M F (i+1)) *m (M G (i+1)) +
                    ((Ho H (i+1)) *m (diff C (i+1))) +
                    ((diff C i) *m (Ho H i)) = 1%:M;
  ax3 : forall i:Z, (Ho H i) *m (M F (i+1)) = 0;
  ax4 : forall i:Z, (M G i) *m (Ho H i) = 0;
  ax5 : forall i:Z, (Ho H i) *m (Ho H (i+1)) = 0}.
```

Key Points of the Proof

Theorem (Basic Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{C_*}. We assume the nilpotency hypothesis is satisfied: for every $c \in C_n$, there exists $\nu \in \mathbb{N}$ such that $(\widehat{\delta} h)^\nu(c) = 0$. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + \widehat{\delta}) \Rightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

Key Points of the Proof

Theorem (Basic Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rrightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{C_*}. We assume the nilpotency hypothesis is satisfied: for every $c \in C_n$, there exists $\nu \in \mathbb{N}$ such that $(\widehat{\delta} h)^{\nu}(c) = 0$. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + \widehat{\delta}) \Rrightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

- Coq is a constructive system.

Key Points of the Proof

Theorem (Basic Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{C_*}. We assume the nilpotency hypothesis is satisfied: for every $c \in C_n$, there exists $\nu \in \mathbb{N}$ such that $(\widehat{\delta} h)^\nu(c) = 0$. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + \widehat{\delta}) \Rightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

- Coq is a constructive system.
- Is this important when proving the Basic Perturbation Lemma?

Key Points of the Proof

Theorem (Basic Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{C_*}. We assume the nilpotency hypothesis is satisfied: for every $c \in C_n$, there exists $\nu \in \mathbb{N}$ such that $(\widehat{\delta} h)^\nu(c) = 0$. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + \widehat{\delta}) \Rightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

- Coq is a constructive system.
- Is this important when proving the Basic Perturbation Lemma? Yes.

Key Points of the Proof

Theorem (Basic Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{C_*}. We assume the nilpotency hypothesis is satisfied: for every $c \in C_n$, there exists $\nu \in \mathbb{N}$ such that $(\widehat{\delta} h)^\nu(c) = 0$. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + \widehat{\delta}) \Rightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

- Coq is a constructive system.
- Is this important when proving the Basic Perturbation Lemma? Yes.
    - δ must be explicitly defined, and
    - ρ' must be explicitly constructed.

Key Points of the Proof

Theorem (Basic Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{C_*}. We assume the nilpotency hypothesis is satisfied: for every $c \in C_n$, there exists $\nu \in \mathbb{N}$ such that $(\widehat{\delta}h)^{\nu}(c) = 0$. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + \widehat{\delta}) \Rightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

- Coq is a constructive system.
- Is this important when proving the Basic Perturbation Lemma? Yes.
  - δ must be explicitly defined, and
  - ρ' must be explicitly constructed.
- Fortunately, Sergeraert's proof is constructive.

Key points of the proof

Theorem (Basic Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{C_*}. We assume the nilpotency hypothesis is satisfied: for every $c \in C_n$, there exists $\nu \in \mathbb{N}$ such that $(\widehat{\delta} h)^{\nu}(c) = 0$. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + \widehat{\delta}) \Rightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

Key points of the proof

Theorem (Basic Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{C_*}. We assume the nilpotency hypothesis is satisfied: for every $c \in C_n$, there exists $\nu \in \mathbb{N}$ such that $(\widehat{\delta} h)^\nu (c) = 0$. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + \widehat{\delta}) \Rightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

```
Variable rho : FGReduction.
```

Key points of the proof

Theorem (Basic Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{C_*}. We assume the nilpotency hypothesis is satisfied: for every $c \in C_n$, there exists $\nu \in \mathbb{N}$ such that $(\widehat{\delta} h)^{\nu}(c) = 0$. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + \widehat{\delta}) \Rightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

```
Variable rho : FGReduction.

Variable delta_hat : forall i:Z, 'M[K]_(m (C rho) (i+1), m (C rho) i).

Hypothesis perturbation_delta_hat : forall i:Z,
   (diff (C rho) (i+1) + delta_hat (i+1)) *m
   (diff (C rho) i + delta_hat i) = 0.
```

Key points of the proof

Theorem (Basic Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rrightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{C_*}. We assume the nilpotency hypothesis is satisfied: for every $c \in C_n$, there exists $\nu \in \mathbb{N}$ such that $(\widehat{\delta} h)^{\nu}(c) = 0$. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + \widehat{\delta}) \Rrightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

```
Variable rho : FGReduction.

Variable delta_hat : forall i:Z, 'M[K]_(m (C rho) (i+1), m (C rho) i).

Hypothesis perturbation_delta_hat : forall i:Z,
   (diff (C rho) (i+1) + delta_hat (i+1)) *m
   (diff (C rho) i + delta_hat i) = 0.

Hypothesis nilpotency_hp (n : nat) : forall i:Z,
   (delta_hat i *m (Ho (H rho)) i)^n = 0.
```

Key points of the proof

Theorem (Basic Perturbation Lemma)

Let $\rho = (f, g, h) : (C_*, d_{C_*}) \Rightarrow (D_*, d_{D_*})$ be a reduction, and $\widehat{\delta}$ a perturbation of d_{C_*}. We assume the nilpotency hypothesis is satisfied: for every $c \in C_n$, there exists $\nu \in \mathbb{N}$ such that $(\widehat{\delta} h)^\nu (c) = 0$. Then, a perturbation δ can be defined for the differential d_{D_*} and a new reduction $\rho' = (f', g', h') : (C_*, d_{C_*} + \widehat{\delta}) \Rightarrow (D_*, d_{D_*} + \delta)$ can be constructed.

```
Variable rho : FGReduction.

Variable delta_hat : forall i:Z, 'M[K]_(m (C rho) (i+1), m (C rho) i).

Hypothesis perturbation_delta_hat : forall i:Z,
   (diff (C rho) (i+1) + delta_hat (i+1)) *m
   (diff (C rho) i + delta_hat i) = 0.

Hypothesis nilpotency_hp (n : nat) : forall i:Z,
   (delta_hat i *m (Ho (H rho)) i)^n = 0.
```

Follow Sergeraert's proof-steps.

Live Proof of a Property

Theorem (Generalisation of the Hexagonal Lemma)

Let $C_* = (C_p, d_p)_{p\in\mathbb{Z}}$ be a chain complex such that every chain group C_p can be decomposed as $C_p = A_p \oplus B_p \oplus C'_p$. The boundary maps d_p are then decomposed in 3×3 block matrices $[d_{p,i,j}]_{1\leq i,j\leq 3}$. If every component of $d_{p,2,1} : A_p \rightarrow B_{p-1}$ is an isomorphism; then, the chain complex $(C_p, d_p)_{p\in\mathbb{Z}}$ can be reduced to a chain complex $(C'_p, d'_p)_{p\in\mathbb{Z}}$.

Proof.

The reduction has as components:

$d'_p = d_{p,3,3} - d_{p,3,1}d^{-1}_{p,2,1}d_{p,2,3} \quad f_p = [0 \quad -d_{p,3,1}d^{-1}_{p,2,1} \quad 1]$

$$g_p = \begin{pmatrix} -d^{-1}_{p,2,1}d_{p,2,3} \\ 0 \\ 1 \end{pmatrix} \; h_p = \begin{pmatrix} 0 & -d^{-1}_{p,2,1} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

□

Demo

$dh + hd + fg = id$

Outline

Conclusions

- It is feasible to use interactive proof assistants to formalise mathematics.
- Formal proofs do not start from scratch, but previously-developed libraries are used as a basis.
- Using different proof assistants, several results from homological perturbation theory have been already formalised.

A Formal Proof of the Basic Perturbation Lemma

Jónathan Heras
(joint work with M. Poza, C. Domínguez, and J. Rubio)

Department of Mathematics and Computer Science
University of La Rioja (Spain)

December 2014
de Brún Workshop on Homological Perturbation Theory