Appendix G: Some questions concerning the representation of theorems

Specific discussion points

1. What should the " meta-structure" to represent mathematics, in which theorems naturally fall, be? There obviously should be [108]:

   - definitions
   - axioms
   - postulates
   - theorems
   - propositions
   - lemmas
   - corollaries
   - conjectures

What other structures are needed to describe generic mathematics? Should this meta-level contain semantic information (e.g. if a conjecture has been proved or disproved)?
What meta-level information (such as author, year, etc.) should be encoded?
How does this meta-information fit into the semantic language itself?

2. Should the semantic representation of each theorem have the same formal structure? In particular, should the structure be something like:

Variables: ...

Assumptions: ...

Definitions: ...

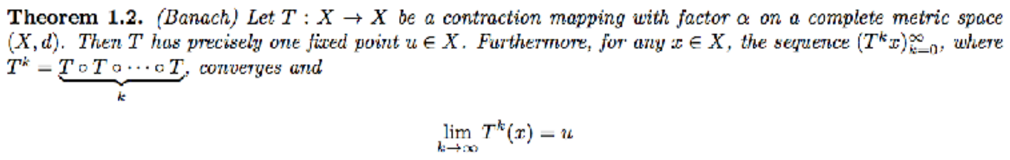
Restrictions: ...

Conclusions: ...

or should it just be of the form $\forall_{\texttt{conditions}} \texttt{statement}$ as in the following statement of the classical central limit theorem:

$$\forall_{\mathrm{IID}(X_1, X_2, \ldots)} \left(\forall_{n \in \mathbb{N}^+} \left(S_n =_{\mathrm{df}} \sum_{i=1}^{n} X_i \bigwedge \overline{X_n} = \mu \bigwedge \mathrm{Var}(X_n) = \sigma^2 \right) \Rightarrow \frac{S_n - n\,\mu}{\sigma\,\sqrt{n}} \longrightarrow_{\mathcal{D}} \mathcal{N}(0, 1) \right)$$

Or Banach's fixed-point theorem:

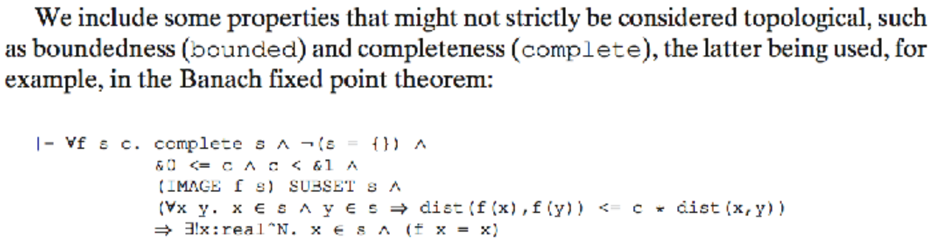


Theorem 1.2. *(Banach) Let $T : X \to X$ be a contraction mapping with factor α on a complete metric space (X, d). Then T has precisely one fixed point $u \in X$. Furthermore, for any $x \in X$, the sequence $(T^k x)_{k=0}^{\infty}$, where $T^k = \underbrace{T \circ T \circ \cdots \circ T}_{k}$, converges and*

$$\lim_{k \to \infty} T^k(x) = u$$

$$\forall_{\{X,d\},\text{ClassElement}(\{X,d\},\text{CompleteMetricSpaces})} \forall_{f,f\in\text{Mappings}(X,X)} \left(\exists_{a,0<a<1} \forall_{\{x,y\},(x|y)\in X}\, d(f(x), f(y)) \le a\, d(x, y) \Rightarrow \right.$$
$$\left. \exists_{x_0,x\in X} \left(f(x) = x \bigwedge \forall_{\{x,s\},x\in X \bigwedge s\in\text{Sequences}(X) \bigwedge s(0)=x \bigwedge \forall_{n,n\in\mathbb{Z}\wedge n\ge 0} s(n+1)=f(s(n))} \text{SequenceLimit}(s) = x\right)\right)$$

Commonly a more precise statement (as, for instance, needed in theorem proving) comes with the price of decreased readability. For instance, here is the formalization of Banach's fixed point theorem from the *N*-dimensional Euclidean space module of HOL Light [67]:

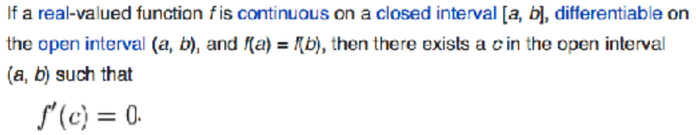


We include some properties that might not strictly be considered topological, such as boundedness (`bounded`) and completeness (`complete`), the latter being used, for example, in the Banach fixed point theorem:

```
|- ∀f s c. complete s ∧ ¬(s = {}) ∧
           &0 <= c ∧ c < &1 ∧
           (IMAGE f s) SUBSET s ∧
           (∀x y. x ∈ s ∧ y ∈ s ⇒ dist(f(x),f(y)) <= c * dist(x,y))
           ⇒ ∃!x:real^N. x ∈ s ∧ (f x = x)
```

3. How are deduction steps best represented? [78], [79], [90] What is the role of natural deduction [111] with the semantic representation of mathematics?

4. How generously should named objects be introduced? Rolle's theorem [49] provides a good example, since it is easy to state in a few words and symbols:



If a real-valued function *f* is continuous on a closed interval [*a*, *b*], differentiable on the open interval (*a*, *b*), and *f*(*a*) = *f*(*b*), then there exists a *c* in the open interval (*a*, *b*) such that

$$f'(c) = 0.$$

If concepts involved are " spelled out" in symbols, a sprinkling of epsilons and deltas is needed:

Let $\{a, b\} \in \mathbb{R}$

$f \in \texttt{FunctionFromTo}(\mathbb{R} \to \mathbb{R}\}$

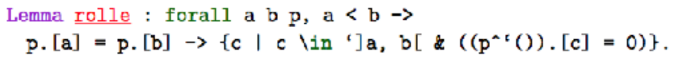
$\texttt{FunctionProperties} \to \{\forall_{x,a\le x\le b} \forall_{\epsilon,\epsilon>0} \exists_{\delta} (a \le \delta + x \le b \Rightarrow |f(x+\delta) - f(x) < \epsilon|),$
$\forall_{x,a<x<b} \forall_{h,h>0\wedge h+x<b} \exists_{m>0} |f(h+x) - f(x)| < h\, m|)\}$

then

$f(a) = f(b) \Rightarrow \exists_c\, (a < c < b \bigwedge f'(c) = 0)$

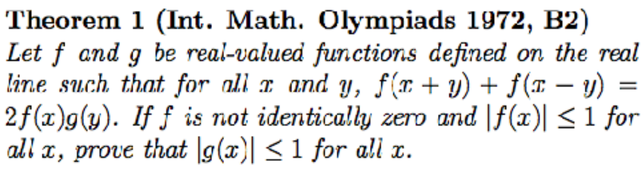
A semantic representation can therefore greatly benefit from introducing and using named objects such as " continuous function" and " differentiable function," both to improve (human) readability and concision and to avoid explicit instantiation and repetitive use of common concepts.

Here is a version of Rolle's theorem for polynomials from a Coq library [69]:

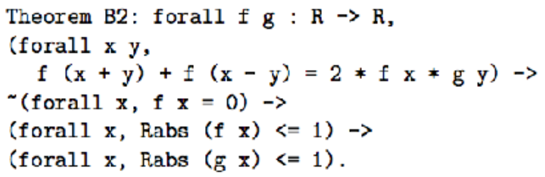


```
Lemma rolle : forall a b p, a < b ->
  p.[a] = p.[b] -> {c | c \in ']a, b[ & ((p^`()).[c] = 0)}.
```

And this is another formalized version of a theorem in Coq [88]:

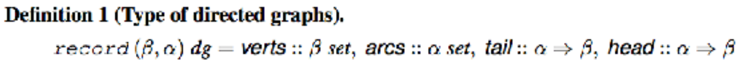


Theorem 1 (Int. Math. Olympiads 1972, B2)
Let f and g be real-valued functions defined on the real line such that for all x and y, $f(x+y)+f(x-y)=2f(x)g(y)$. If f is not identically zero and $|f(x)|\leq 1$ for all x, prove that $|g(x)|\leq 1$ for all x.



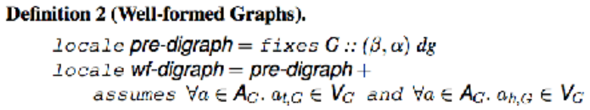
```
Theorem B2: forall f g : R -> R,
(forall x y,
  f (x + y) + f (x - y) = 2 * f x * g y) ->
~(forall x, f x = 0) ->
(forall x, Rabs (f x) <= 1) ->
(forall x, Rabs (g x) <= 1).
```

The definition of a digraph in Isabelle [113] is:



Definition 1 (Type of directed graphs).

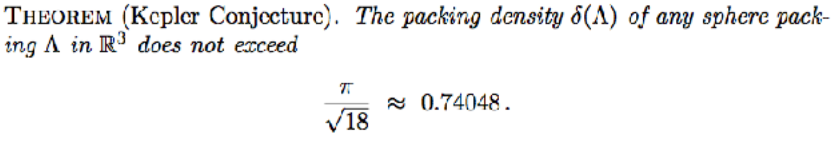
$\texttt{record}\ (\beta,\alpha)\ dg = \mathsf{verts} :: \beta\ set,\ \mathsf{arcs} :: \alpha\ set,\ \mathsf{tail} :: \alpha \Rightarrow \beta,\ \mathsf{head} :: \alpha \Rightarrow \beta$



Definition 2 (Well-formed Graphs).

$\texttt{locale}\ \mathsf{pre\text{-}digraph} = \texttt{fixes}\ G :: (\beta,\alpha)\ dg$
$\texttt{locale}\ \mathsf{wf\text{-}digraph} = \mathsf{pre\text{-}digraph} +$
$\quad \texttt{assumes}\ \forall a \in A_G.\ a_{t,G} \in V_G\ \texttt{and}\ \forall a \in A_G.\ a_{h,G} \in V_G$

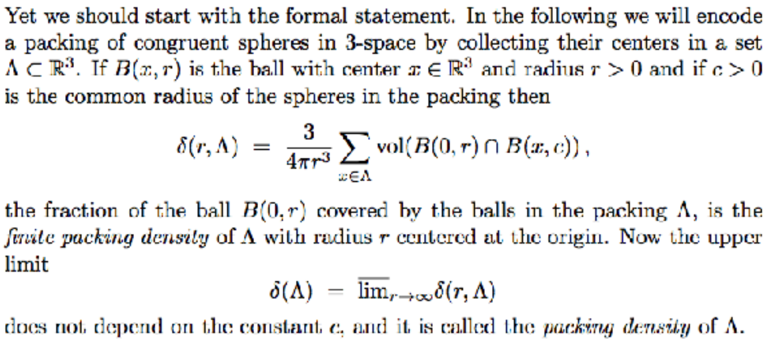
5. How should definitions be hierarchically arranged? For example, the Kepler conjecture can be succinctly stated as:



THEOREM (Kepler Conjecture). *The packing density $\delta(\Lambda)$ of any sphere packing Λ in $\mathbb{R}^3$ does not exceed*

$$\frac{\pi}{\sqrt{18}} \approx 0.74048 .$$

But the succinctness requires $\delta(\Lambda)$ and $\delta(\Lambda, r)$ to first be defined:



Yet we should start with the formal statement. In the following we will encode a packing of congruent spheres in 3-space by collecting their centers in a set $\Lambda \subset \mathbb{R}^3$. If $B(x,r)$ is the ball with center $x \in \mathbb{R}^3$ and radius $r > 0$ and if $c > 0$ is the common radius of the spheres in the packing then

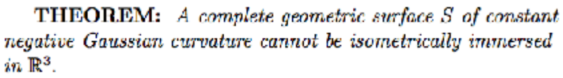
$$\delta(r,\Lambda) \;=\; \frac{3}{4\pi r^3}\sum_{x\in\Lambda} \mathrm{vol}(B(0,r)\cap B(x,c))\,,$$

the fraction of the ball $B(0,r)$ covered by the balls in the packing Λ, is the *finite packing density* of Λ with radius r centered at the origin. Now the upper limit

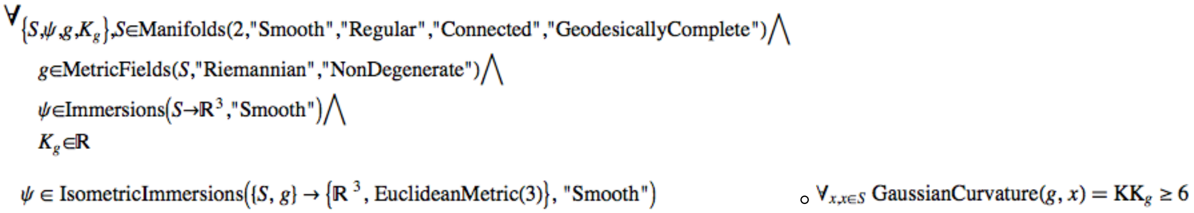
$$\delta(\Lambda) \;=\; \overline{\lim}_{r\to\infty}\delta(r,\Lambda)$$

does not depend on the constant c, and it is called the *packing density* of Λ.

6. How should mathematical objects that are described through a list or sequence of properties be best described? To see the issue, consider the example provided by the surfaces in Hilbert (differential geometric) theorem [58]:



THEOREM: *A complete geometric surface S of constant negative Gaussian curvature cannot be isometrically immersed in $\mathbb{R}^3$.*



$$\forall_{\{S,\psi,g,K_g\},S\in\text{Manifolds}(2,\text{"Smooth"},\text{"Regular"},\text{"Connected"},\text{"GeodesicallyComplete"})\bigwedge}$$

$$g\in\text{MetricFields}(S,\text{"Riemannian"},\text{"NonDegenerate"})\bigwedge$$

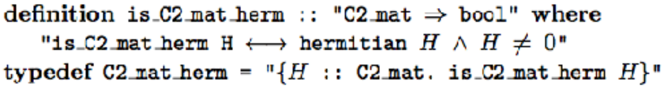
$$\psi\in\text{Immersions}\left(S\to\mathbb{R}^3,\text{"Smooth"}\right)\bigwedge$$

$$K_g\in\mathbb{R}$$

$$\psi\in\text{IsometricImmersions}\left(\{S,g\}\to\left\{\mathbb{R}^3,\text{EuclideanMetric}(3)\right\},\text{"Smooth"}\right)\qquad\circ\ \forall_{x,x\in S}\ \text{GaussianCurvature}(g,x)=\text{KK}_g\geq 6$$

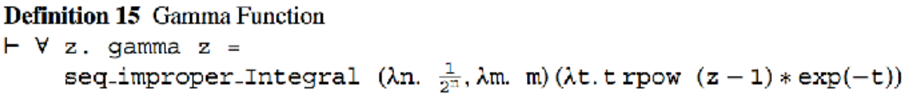
7. How much should specialized (two-dimensional) notation be used? Two-dimensional notations for arithmetic operations and quantifiers are surely uncontroversial. Functions, " big O" notation, symbolic vectors and matrices, immersions, set-builder, group actions, and closures are examples that simplify and make the representation compact, but might be hard to read for newcomers.

8. How can an extensible (large) list of predefined objects and operations be maintained at the same time as allowing users to define their own terms and descriptions? Consider, for example, the definition of a Hermitian matrix from a recent Isabelle/HOL implementation of formalized complex plane geometry [81]:



```
definition is_C2_mat_herm :: "C2_mat ⇒ bool" where
  "is_C2_mat_herm H ⟷ hermitian H ∧ H ≠ 0"
typedef C2_mat_herm = "{H :: C2_mat. is_C2_mat_herm H}"
```

And here is the definition of the (complete) gamma function in HOL4 [85]:

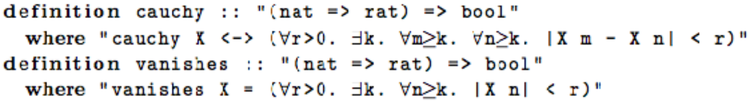


Definition 15 Gamma Function

⊢ ∀ z. gamma z =

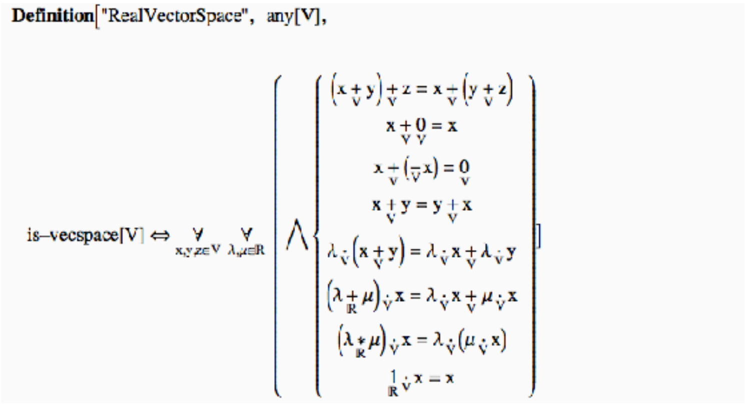
seq_improper_Integral (λn. $\frac{1}{2^n}$, λm. m)(λt. t rpow (z − 1) ∗ exp(−t))

9. What should be taken as concepts, those things that, within a semantic representation, are not defined through other objects [116]? For instance, is a Cauchy sequence of real numbers an " elementary object," or is it a defined object, as in this Isabelle/HOL definition [87]:



```
definition cauchy :: "(nat => rat) => bool"
  where "cauchy X <-> (∀r>0. ∃k. ∀m≥k. ∀n≥k. |X m - X n| < r)"
definition vanishes :: "(nat => rat) => bool"
  where "vanishes X = (∀r>0. ∃k. ∀n≥k. |X n| < r)"
```

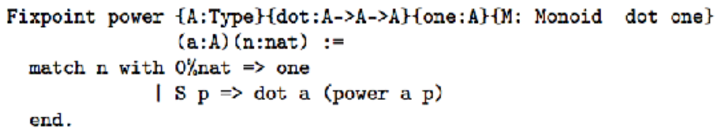
Here is the definition of a real vector space in *Theorema*:



Definition["RealVectorSpace", any[V],

$$\text{is–vecspace}[V] \Leftrightarrow \underset{x,y,z\in V}{\forall}\ \underset{\lambda,\mu\in\mathbb{R}}{\forall} \left(\bigwedge \begin{cases} \left(x \underset{V}{+} y\right) \underset{V}{+} z = x \underset{V}{+} \left(y \underset{V}{+} z\right) \\ x \underset{V}{+} \underset{V}{0} = x \\ x \underset{V}{+} \left(\underset{V}{-} x\right) = \underset{V}{0} \\ x \underset{V}{+} y = y \underset{V}{+} x \\ \lambda \underset{V}{\cdot} \left(x \underset{V}{+} y\right) = \lambda \underset{V}{\cdot} x \underset{V}{+} \lambda \underset{V}{\cdot} y \\ \left(\lambda \underset{\mathbb{R}}{+} \mu\right) \underset{V}{\cdot} x = \lambda \underset{V}{\cdot} x \underset{V}{+} \mu \underset{V}{\cdot} x \\ \left(\lambda \underset{\mathbb{R}}{*} \mu\right) \underset{V}{\cdot} x = \lambda \underset{V}{\cdot} \left(\mu \underset{V}{\cdot} x\right) \\ \underset{\mathbb{R}}{1} \underset{V}{\cdot} x = x \end{cases} \right)]$$

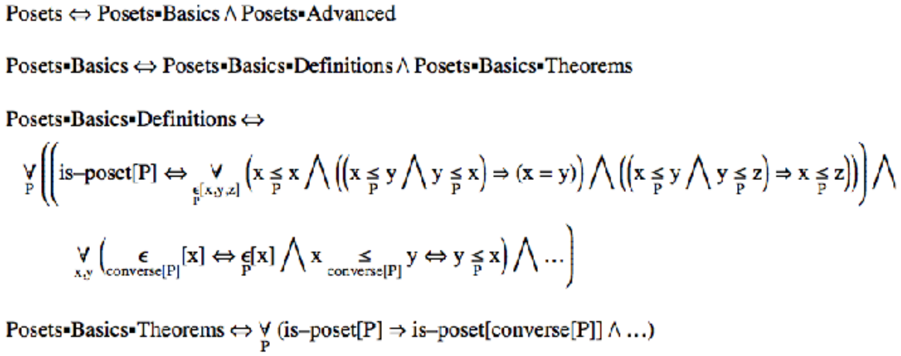
10. How much typing (in the sense of type theory) should such a semantic representation allow and enforce? Should most objects be classified as fields, rings, groups, modules, groupoids, monoids, or setoids? [71], [75], [77], [82], [83] Here is a generic definition of a power function within monoids [92]:



```
Fixpoint power {A:Type}{dot:A->A->A}{one:A}{M: Monoid  dot one}
                (a:A)(n:nat) :=
 match n with 0%nat => one
           | S p => dot a (power a p)
 end.
```

Which algebraic structures are so common that they should be named and predefined, and which ones should be (easily) definable?

11. How can nontrivial connections between various mathematical results be represented? Often the application of techniques from one field of mathematics to another allows new insights and advances. Given an already semantically encoded set of mathematical results, what semantic tags, generalizations, and comment structures are needed within the semantic language itself (rather than as an annotation layer on top)? Here is a definition of a poset in *Theorema* together with tagging within the definition [91]:



Posets ⇔ Posets▪Basics ∧ Posets▪Advanced

Posets▪Basics ⇔ Posets▪Basics▪Definitions ∧ Posets▪Basics▪Theorems

Posets▪Basics▪Definitions ⇔

$$\underset{P}{\forall}\left(\left(\text{is–poset}[P] \Leftrightarrow \underset{\underset{P}{\in}[x,y,z]}{\forall} \left(x \underset{P}{\leq} x \bigwedge \left(\left(x \underset{P}{\leq} y \bigwedge y \underset{P}{\leq} x\right) \Rightarrow (x = y)\right) \bigwedge \left(\left(x \underset{P}{\leq} y \bigwedge y \underset{P}{\leq} z\right) \Rightarrow x \underset{P}{\leq} z\right)\right)\right) \bigwedge \right.$$

$$\left. \underset{x,y}{\forall} \left(\underset{\text{converse}[P]}{\in}[x] \Leftrightarrow \underset{P}{\in}[x] \bigwedge x \underset{\text{converse}[P]}{\leq} y \Leftrightarrow y \underset{P}{\leq} x\right) \bigwedge \ldots\right)$$

Posets▪Basics▪Theorems ⇔ $\underset{P}{\forall}$ (is–poset[P] ⇒ is–poset[converse[P]] ∧ …)

12. Some areas of mathematics use certain mathematical constructs in ways differing from their " standard" meanings (e.g. nonstandard analysis and synthetic differential geometry). Are the real numbers being considered not as a metric space, but rather just as a topological space or a locally compact space? How can one best differentiate between these nuanced meanings without making the semantic encoding overly complicated?

13. While a full encoding of proofs is far too large a task to be attempted, partial semantic encoding of proof ideas would be very useful in preserving faith and confidence in the correctness of a proof [64], [86]. What would be appropriate language constructs to underpin this?

General discussion points

In addition to these concrete language design issues, methodological problems of organizing the process of designing a semantic mathematical language will be discussed. Should workshops for individual mathematical fields eventually be organized and, if so, at what granularity? Should one attempt to represent the results of survey papers and monographs first before attempting to deal with a wide array of mathematical papers? As a semantic representation of mathematics will unavoidably contain thousands of concepts and mathematical structures, how can we ensure the uniformity and coherence of the language while it is developed? What are the best initial fields to tackle? Abstract topics that are today not very well developed computationally (for instance, operator algebras) will be confronted with representational problems up-front, while topics that are already quite computational (e.g. special functions or probability theory) have a solid foundation to build on so extension of the proposed language should be more straightforward and uncontroversial.