Preface

The 33rd edition of the Italian Convention of Computational Logic (CILC 2018), the annual meeting organized by GULP (Gruppo ricercatori e Utenti Logic Programming), was hosted by the Free University of Bozen-Bolzano, from September 20th to September 22nd, 2018. CILC is the leading forum for the exchange of ideas and experiences between Italian researchers working in the theory and practice of computational logic, although it has broaden its topics of interest also to related areas.

The technical program of CILC 2018 included 21 presentations, among which 13 papers are included in these proceedings and further 8 appeared or have been submitted elsewhere. Paper selection was made by peer reviewing, and each submitted paper received three reviews by members of the Program Committee. The contributions address different topics related to computational logic, including verification and validation, temporal and spatial reasoning, description logics, probabilistic reasoning, constraint logic programming.

The program was also enriched by the keynote “Reasoning and Planning for $\mathrm{LTL}_f/\mathrm{LDL}_f$ goals" by *Giuseppe De Giacomo*, Sapienza University of Rome, and with 2 tutorials:

- Probabilistic logic languages and their combination
  Riccardo Zese, University of Ferrara
- Ontology-based Data Access: Relational Data and Beyond
  Diego Calvanese, Free University of Bozen-Bolzano

In addition, we had the pleasure of hosting a special session where *Alberto Pettorossi* shared his professional experience and highlighted his personal contribution to the field of computational logic.

The presentations of papers not included in the proceedings were the following:

- Reasoning with Justifiable Exceptions in Contextual Hierarchies
  Loris Bozzato, Thomas Eiter, Luciano Serafini
- Meta-programming and symbolic execution for detecting run-time errors in Erlang programs
  Emanuele De Angelis, Fabio Fioravanti, Adrian Palacios, Alberto Pettorossi, Maurizio Proietti
- Deciding the Consistency of Branching Time Interval Networks
  Marco Gavanelli, Alessandro Passantino, Guido Sciavicco
- A set-based reasoner for the description logic $DL_D^{4,\times}$
  Domenico Cantone, Marianna Nicolosi-Asmundo, Daniele Francesco Santamaria
- Persistent Stochastic Non-Interference
  Carla Piazza, Sabina Rossi, Jane Hillston
- Verification of Data-Aware Processes via Array-Based Systems (Abridged Version)
  Diego Calvanese, Silvio Ghilardi, Alessandro Gianola, Marco Montali, Andrey Rivkin
- Modeling and Reasoning over Declarative Data-Aware Processes: The Object-Centric Behavioral Constraint Approach
  Alessandro Artale, Marco Montali, Wil van der Aalst
- Declarative Parameterized Verification of Topology-sensitive Distributed Protocols
  Giorgio Delzanno, Sylvain Conchon, Angelo Ferrando

We would like to thank all the people who have contributed to the success of CILC 2018: the authors, the tutorials and keynote speakers, the reviewers, the participants, the local organizers and sponsors. Special thanks goes to the President of GULP, Agostino Dovier, and the secretary of GULP, Marco Gavanelli, for their support in the organization of the event.

September 2018
Paolo Felli, Marco Montali

On perfect matchings for some bipartite graphs*

Alberto Casagrande[1], Francesco Di Cosmo[2], and Eugenio G. Omodeo[3]

[1] Dept. of Mathematics and Geosciences, University of Trieste, Italy.
acasagrande@units.it
[2] University of Trieste, Italy.
dicosmo.francesco@gmail.com
[3] Dept. of Mathematics and Geosciences, University of Trieste, Italy.
eomodeo@units.it

Abstract. Inspired by some recent revisitations of the Cantor-Bernstein theorem, in particular its formalizations in ZF carried out via the proof assistant AProS by W. Sieg and P. Walsh, we are carrying out the proof of a related graph-theoretical proposition. Our development is assisted by the proof checker ÆtnaNova, and our proof pattern is drawn from Halmos's classic 'Naive set theory'. This case-study illustrates the flexibility of a proof environment rooted in Set Theory, which can be bent with equal ease toward declarative and procedural styles of proof.

Key words Proof checking, set-based specifications, Zermelo-Fraenkel set theory, connected graphs.

Introduction

Riding the wave of a revival of interest in the proofs of the Cantor-Bernstein theorem, in short CBT (cf. [7]), and particularly inspired by [14], we have formalized Paul Halmos's account [6] of Gyula Kőnig's proof [8] of that proposition.

Stated in streamlined terms, the Cantor-Bernstein theorem claims that

> whenever α, β are injections such that $\mathbf{range}(\alpha) \subseteq \mathbf{domain}(\beta)$ and $\mathbf{range}(\beta) \subseteq \mathbf{domain}(\alpha)$, a one-one correspondence exists between $\mathbf{domain}(\alpha)$ and $\mathbf{domain}(\beta)$.

Proving this amounts to building, out of the given α and β, an injection γ from $A = \mathbf{domain}(\alpha)$ *on*to $B = \mathbf{domain}(\beta)$. Without loss of generality, Halmos [6, pp. 88–89] proceeds under the disjointedness assumption $A \cap B = \emptyset$ — Kőnig's original proof, which is slightly more informal, does not mention this assumption.

The elegance of Halmos's approach stems from his focusing on bipartite graphs rather than on 1-1 mappings; and we further stress the graph-theoretical nature of his argument by ignoring the orientation of the mappings. Halmos's argument—we contend—could well be referred to the undirected graph whose (typically infinite) sets of vertices and edges are, respectively:

$$V = A \uplus B \text{ and } E = \big\{\{x, y\} : \langle x\,,\, y\rangle \in \alpha \cup \beta \;\&\; \langle y\,,\, x\rangle \notin \alpha \cup \beta\big\}.$$

* This work has been partially supported by INdAM-GNCS and by the project FRA-UniTS 2016.

The proof-checker ÆtnaNova [13], also known as Ref, is firmly Set Theory oriented[1]. This enables one to try different ways of formulating definitions and claims, with the reward, at times, of discovering proofs that are more straightforward or transparent than long-established ones. For instance, non-cut vertices are, traditionally, defined in terms of paths; thanks to ÆtnaNova, we were able to propose an alternative characterization for them [2] and to ease the proof that every finite and connected claw-free graph admits an extensional acyclic orientation [11, 12].

In this new formal essay, again based on ÆtnaNova and related to graph connectivity, our aim is twofold:

(1) capture the structural properties of the graph $G = (V, E)$ resulting from generic injections α and β in the manner explained above;
(2) show that any graph enjoying such properties has a *perfect matching*—namely, it has a set M of edges which is a partition of V.

In preparation for this task, we also need to

(3) treat the *connected components* of an arbitrary graph (actually, of any family E of edges—even an infinite E whose elements are not doubletons, see Fig. 1); for, the sought matching will result from the disjoint union of perfect matchings, one for each connected component of G.

$$
\begin{array}{rcl}
\mathsf{DisconPartn}(P) & \leftrightarrow_{\mathrm{Def}} & \emptyset \notin P \;\&\; \big(\forall b \in P \mid \bigcup b \cap \bigcup(\bigcup(P \setminus \{b\})) = \emptyset \;\& \\
 & & \qquad (\emptyset \in b \rightarrow b = \{\emptyset\})\big) \\
\mathsf{ReachCl}(Q, E) & \leftrightarrow_{\mathrm{Def}} & (\bigcup Q) \cap \bigcup(E \setminus Q) = \emptyset \\
\mathsf{CoCo}(C, E) & \leftrightarrow_{\mathrm{Def}} & \{\, q \subseteq C \cap E \mid \mathsf{ReachCl}(q, E) \;\&\; q \neq \emptyset \,\} = \{C\} \\
\mathsf{CoCo}(C, E) & \rightarrow & \{\, q \subseteq C \mid \mathsf{ReachCl}(q, C) \,\} \subseteq \{\emptyset\,,\ C\} \\
\mathsf{CoCo}(C, C) & \leftrightarrow & \{\, q \subseteq C \mid \mathsf{ReachCl}(q, C) \,\} \subseteq \{\emptyset\,,\ C\} \;\&\; C \neq \emptyset \\
R \in E & \rightarrow & \big(\, \exists c \mid \mathsf{CoCo}(c\,,\ E) \;\&\; R \in c \,\big) \\
\multicolumn{3}{l}{K = \{\, c \subseteq E \mid \mathsf{CoCo}(c, E) \,\} \rightarrow \mathsf{DisconPartn}(K) \;\&\; \bigcup K = E}
\end{array}
$$

Fig. 1. Connected components of generic set E: definitions and properties

The paper is organized as follows: we offer a quick view of the ÆtnaNova proof-specification language through examples related to our case-study in Section 1. Then, after highlighting Halmos's proof of the Cantor-Bernstein theorem in Section 2, we show how his idea can be adapted to the seemingly different situation related to bipartite graphs. In the conclusions, we relate the contribution of this paper with ongoing studies on the interplay between sets and graphs in formal reasoning within the respective theories. For the sake of completeness, in Appendix A we outline a different proof pattern for the Cantor-Bernstein theorem, closer in spirit to the viewpoint which historically led to its discovery.

[1] ÆtnaNova is available as a service at URL `http://aetnanova.units.it/`, while all of the proof-checking experiments discussed in this paper are available at URL `http://aetnanova.units.it/scenarios/BeyondCantorBernstein`.

1 The ÆtnaNova system: a panoramic tour

ÆtnaNova's users organize definitions, theorem statements, and proof specifications, in files named *scenarios*[2], which ÆtnaNova processes in order to establish whether or not they comply with the mathematical standards of rigor built into it. The logical system underlying ÆtnaNova is a variant of the Zermelo-Fraenkel set theory with axioms of foundation and universal choice.

Only two axioms occur in ÆtnaNova explicitly; they are:

- $\mathbf{s}_\infty \neq \emptyset \;\&\; (\forall\, x \in \mathbf{s}_\infty \mid \{x\} \in \mathbf{s}_\infty)$
- $\mathbf{arb}(\emptyset) = \emptyset \;\&\; \big(\forall\, x \mid \; x = \emptyset \;\vee\; \big(\mathbf{arb}(x) \in x \;\&\; x \cap \mathbf{arb}(x) = \emptyset\,\big)\big)$

The former, involving the special constant $\mathbf{s}_\infty$, acts as infinity axiom; the latter characterizes the universal choice operator and embodies von Neumann's assumption that $\in$ is a well-founded relationship. The contents of most familiar axioms of ZF are built into the inferential armory of ÆtnaNova, which handles competently many familiar set constructs: the membership and equality relators $\in$ and $=$, the constant $\emptyset$, the dyadic operators $\cap$, $\setminus$, $\cup$, the "elementary set" constructor $\{S_1, \dots, S_n\}$, the pairing construct $\langle X\,,\;Y\rangle$ and the conjugated projections associated with it (see the first three lines of Fig. 6), and a very flexible set abstraction construct (e.g., see [9, pp. 42–45]), of the form

$$\{\,\mathrm{set\_term} : \mathrm{iterators} \mid \mathrm{condition}\,\}\;.$$

ÆtnaNova embodies two kinds of application: when the notation $f{\upharpoonright}x$ is used, f is a *set* (typically a set of pairs) and $f{\upharpoonright}x$ denotes the value y which f associates with x and, usually, this is the second component of a pair $\langle x\,,\;y\rangle$ belonging to f, but $f{\upharpoonright}x$ equals $\emptyset$ for any x outside the *set* $\mathbf{domain}(f)$; when the notation $g(x)$ is used—as in $\mathbf{arb}(\cdot)$, $\mathbf{range}(\cdot)$, or $\mathsf{descs}_\Theta(\cdot)$—, g denotes a 'global' function: to wit, a *proper class* of pairs, whose domain consists of all sets.

$$\begin{array}{rcl}
\mathscr{P}(S) & =_{\mathrm{Def}} & \{y : y \subseteq S\} \\
\bigcup S & =_{\mathrm{Def}} & \{y : x \in S\,,\; y \in x\} \\
\mathsf{Finite}(F) & \leftrightarrow_{\mathrm{Def}} & (\forall\, g \in \mathscr{P}(\mathscr{P}(F)) \setminus \{\emptyset\} \mid (\exists\, m \mid g \cap \mathscr{P}(m) = \{m\}\,)) \\
\mathsf{Partition}(P) & \leftrightarrow_{\mathrm{Def}} & (\forall\, b \in P \mid \Big\{k \in P \mid k \cap b \neq \emptyset\Big\} = \{b\}\,) \\
\mathsf{next}(I) & =_{\mathrm{Def}} & I \cup \{I\} \\
\mathsf{nat}(I, S) & =_{\mathrm{Def}} & \mathbf{arb}\Big(\{\,\mathsf{next}\big(\mathsf{nat}(j, S)\big) : j \in I \mid I = \{j\} \cap S\,\}\Big) \\
\mathbb{N} & =_{\mathrm{Def}} & \{\mathsf{nat}(i, \mathbf{s}_\infty) : i \in \mathbf{s}_\infty\} \\
\mathsf{Even}(M) & \leftrightarrow_{\mathrm{Def}} & M = \emptyset \;\vee\; \Big(\exists\, i \in M \mid \mathsf{Even}(i) \;\&\; \mathsf{next}\big(\mathsf{next}(i)\big) = M\Big) \\
\mathsf{ChSet}(C\,,\;T) & \leftrightarrow_{\mathrm{Def}} & \{\;\{x\}\; : x \in C\,\} \;=\; \{\,C \cap b : b \in T\,\} \\
\mathsf{PeMa}(M\,,\;E) & \leftrightarrow_{\mathrm{Def}} & M \subseteq E \;\&\; \bigcup E \subseteq \bigcup M \;\&\; \big(\forall\, h \in M\,,\; k \in M \setminus \{h\} \mid h \cap k = \emptyset\big)
\end{array}$$

Fig. 2. ÆtnaNova definitions can rely on $\in$-recursion

[2] Sample scenarios can be found at http://aetnanova.units.it/scenarios/.

Three ÆtnaNova-specified definitions have already been shown on the top of Fig. 1; many more are listed in Fig. 2 and Fig. 6; all of these play a role in the 'proof-pearl' under development which we are discussing here. Note that recursive specifications such as the definition of the function $\mathsf{nat}(I,S)$ ('I-th natural number relative to the set S of indices') and the definition of the property $\mathsf{Even}(M)$ ('M is an even number') make sense thanks to the assumed well-foundedness of $\in$.

An example of an ÆtnaNova-specified proof is shown in Fig. 3. As one sees, proofs are formed by two-portion lines: the second portion of each line, separated by the sign $\Rightarrow$ from the first and at times carrying an identifying label of the form Statxxx, is the *assertion* being derived; the first portion is the *hint*, referencing the basic inference mechanism which enables that derivation in ÆtnaNova. Occasionally an assertion is represented laconically by the keyword AUTO, when no ambiguity or obscurity can ensue from this.

Theorem ch_0 : [Every partition has a choice set] $\mathsf{Partition}(P) \rightarrow (\,\exists\, c \mid \mathsf{ChSet}(c,P)\,)$.

Proof : $\mathsf{Suppose\_not}(p_0) \Rightarrow \mathsf{Stat0} : \big(\neg\exists\; c \mid \mathsf{ChSet}(c,p_0)\big)\ \&\ \mathsf{Partition}(p_0)$

> For, suppose that p_0 makes a counterexample. In particular, the inequality $\big\{\{\mathbf{arb}(b)\}\ :\ b \in p_0\big\} \neq \big\{\{\mathbf{arb}(b)\ :\ b \in p_0\} \cap b : b \in p_0\big\}$ must hold, in view of the definition of $\mathsf{ChSet}(c,p_0)$.

$\{\mathbf{arb}(b)\ :\ b \in p_0\} \hookrightarrow \mathsf{Stat0} \Rightarrow \neg\,\mathsf{ChSet}(\{\mathbf{arb}(b)\ :\ b \in p_0\}\,,\ p_0)$

$\mathsf{Use\_def}(\mathsf{ChSet}) \Rightarrow \big\{\{x\}\ :\ x \in \{\mathbf{arb}(b)\ :\ b \in p_0\}\big\} \neq \big\{\{\mathbf{arb}(b)\ :\ b \in p_0\} \cap b : b \in p_0\big\}$

$\mathsf{SIMPLF} \Rightarrow \mathsf{Stat1} : \big\{\{\mathbf{arb}(b)\}\ :\ b \in p_0\big\} \neq \big\{\{\mathbf{arb}(b)\ :\ b \in p_0\} \cap b : b \in p_0\big\}$

> Therefore, some block b_0 of the partition p_0 exists which witnesses the said inequality. Since blocks are non-null, $\mathbf{arb}(b_0) \in b_0$.

$\mathsf{Use\_def}(\mathsf{Partition}) \Rightarrow \mathsf{Stat2} : (\,\forall\, b \in p_0 \mid \Big\{k \in p_0 \mid k \cap b \neq \emptyset\Big\} = \{b\}\,)$

$b_0 \hookrightarrow \mathsf{Stat1} \Rightarrow \mathsf{Stat3} : \{\mathbf{arb}(b_0)\} \neq (\,\{\mathbf{arb}(b)\ :\ b \in p_0\} \cap b_0\,)\ \&\ b_0 \in p_0$

$b_0 \hookrightarrow \mathsf{Stat2}(\mathsf{Stat2}^*) \Rightarrow \mathsf{Stat4} : \Big\{k \in p_0 \mid k \cap b_0 \neq \emptyset\Big\} = \{b_0\}$

> Consequently, $\mathbf{arb}(b_0) \in \{\mathbf{arb}(b) : b \in p_0\} \cap b_0$ holds. This enables simplification of the inequality $\{\mathbf{arb}(b_0)\} \neq \{\mathbf{arb}(b)\ :\ b \in p_0\} \cap b_0$ into $\{\mathbf{arb}(b)\ :\ b \in p_0\} \cap b_0 \not\subseteq \mathbf{arb}(b_0)$; therefore, an a_0 other than $\mathbf{arb}(b_0)$ belongs to both of b_0 and $\{\mathbf{arb}(b)\ :\ b \in p_0\}$.

$\mathsf{Suppose} \Rightarrow \mathbf{arb}(b_0) \notin (\,\{\mathbf{arb}(b)\ :\ b \in p_0\} \cap b_0\,)$

$\quad k_0 \hookrightarrow \mathsf{Stat4}(\mathsf{Stat4}^*) \Rightarrow \mathsf{Stat5} : \mathbf{arb}(b_0) \notin \{\mathbf{arb}(b)\ :\ b \in p_0\}$

$\quad b_0 \hookrightarrow \mathsf{Stat5} \Rightarrow \mathsf{AUTO}$

$(\mathsf{Stat3}^*)\mathsf{Discharge} \Rightarrow \mathsf{AUTO}$

$a_0 \hookrightarrow \mathsf{Stat3}(\mathsf{Stat3}^*) \Rightarrow \mathsf{Stat6} : a_0 \in \{\mathbf{arb}(b)\ :\ b \in p_0\}\ \&\ a_0 \in b_0\ \&\ a_0 \neq \mathbf{arb}(b_0)$

> Such an a_0 can be rewritten as $\mathbf{arb}(b_1)$ for some b_1 other than b_0 in p_0, but this contradicts the fact that any two blocks in p_0 are disjoint.

$b_1 \hookrightarrow \mathsf{Stat6}(\mathsf{Stat6}\,,\mathsf{Stat4}) \Rightarrow \mathsf{Stat7} : b_1 \notin \Big\{k \in p_0 \mid k \cap b_0 \neq \emptyset\Big\}\ \&\ b_1 \in p_0\ \&\ a_0 = \mathbf{arb}(b_1)$

$b_1 \hookrightarrow \mathsf{Stat2}(\mathsf{Stat7}^*) \Rightarrow \mathsf{Stat8} : b_1 \in \Big\{k \in p_0 \mid k \cap b_1 \neq \emptyset\Big\}$

$(\,) \hookrightarrow \mathsf{Stat8}(\mathsf{Stat7}) \Rightarrow a_0 \in b_1$

$b_1 \hookrightarrow \mathsf{Stat7} \Rightarrow \mathsf{AUTO}$

$(\mathsf{Stat6}^*)\mathsf{Discharge} \Rightarrow \mathsf{QED}$

Fig. 3. Proof, carried out with ÆtnaNova, of the controversial Zermelo's principle

ÆtnaNova includes an important construct, named THEORY (cf. [10] and [13, pp.19–25]), designed to support reusability of proofware components. ÆtnaNova's THEORYs are akin to a mechanism for parameterized specifications available in the Clear language [1]; in a sense, they resemble procedures of a programming language. Typically, a THEORY has formal parameters which get bound to actual parameters when it gets applied; in return, the THEORY will supply useful information. Actual input parameters must satisfy a conjunction of statements, called THEORY *assumptions*.

Besides providing theorems of which it holds the proofs, a THEORY has the ability to instantiate special variables (whose names are subscripted with the Θ sign), which play the role of output parameters and bear special relationships with the input parameters. Two examples of ÆtnaNova THEORY appear in Fig. 4. THEORY reachability has two parameters: a property V of sets and a dyadic relation E over sets; its assumption requires that for every set x enjoying the property $\mathsf{V}(x)$, the collection of all sets such that $\mathsf{E}(x, y)$ holds forms a set (not a proper class).

```
THEORY reachability( V(X) , E(X,Y) )
    $(\forall x \mid V(x) \rightarrow (\exists c, \forall y \mid E(x,y) \,\&\, V(y) \rightarrow y \in c))$
$\Longrightarrow$(descs$_\Theta$)
    $(\forall s, x, y \mid s \subseteq descs_\Theta(s) \,\&$
                                    $(x \in descs_\Theta(s) \,\&\, V(x) \,\&\, V(y) \,\&\, E(x,y) \rightarrow y \in descs_\Theta(s)))$
    $(\forall y, x, z \mid y \in descs_\Theta(\{x\}) \,\&\, z \in descs_\Theta(\{y\}) \rightarrow z \in descs_\Theta(\{y\}))$
    $(\forall s, t \mid s \subseteq t \,\&\, (\forall x, y \mid x \in t \,\&\, V(x) \,\&\, V(y) \,\&\, E(x,y) \rightarrow y \in t) \rightarrow$
                                                                        $descs_\Theta(s) \subseteq t)$
END reachability
```

```
THEORY connComp( $\boldsymbol{H}$ )
   $\emptyset \neq \boldsymbol{H}$
$\Longrightarrow$(th$_\Theta$ , cc$_\Theta$)
   $(\forall i, r \mid th_\Theta(i,r) = \textbf{if } i = \emptyset \textbf{ then}\{ \textbf{if } r \in \boldsymbol{H} \textbf{ then } r \textbf{ else arb}(\boldsymbol{H}) \textbf{ fi}\} \textbf{ else}$
                              $\{ w : j \in i, u \in th(j,r), w \in \boldsymbol{H} \mid i = j \cup \{j\} \,\&\, u \cap w \neq \emptyset \} \textbf{ fi})$
   $(\forall r \mid cc_\Theta(r) = \bigcup \{th(i,r) : i \in \mathbb{N}\})$
   $(\forall r \mid r \in \boldsymbol{H} \rightarrow CoCo(cc_\Theta(r), \boldsymbol{H}))$
END connComp
```

Fig. 4. Reachability in a 'big graph' and connected components of a 'small' hypergraph

This THEORY returns a function, descs$_\Theta$, that sends every set s into the sets of its 'E-descendants'; that is, descs$_\Theta$(s) is the set of all sets y such that a finite sequence $x_0, \ldots, x_n$ exists satisfying the conditions $x_0 \in \mathsf{s}$, $y = x_n$, and $\mathsf{E}(x_{i-1}, x_i)$ for $i = 1, \ldots, n$. The three statements appearing below the assumption of reachability in Fig. 4 are theorems, derived once and for all by the proof developer inside this THEORY which, from then on, can be applied to any pair $\mathsf{V}(x)$, $\mathsf{E}(x,y)$ consisting of a property and a dyadic relation.

The other THEORY shown in Fig. [4], namely $\mathsf{connComp}$, can be applied to any nonnull set $\boldsymbol{H}$. For any given element r of $\boldsymbol{H}$, it returns the stages $\mathsf{th}_{\Theta}(i,\mathsf{r})$ of an inductive construction of the unique set $c = \mathsf{cc}_{\Theta}(\mathsf{r})$ such that $\mathsf{CoCo}(c,\boldsymbol{H})$ & $\mathsf{r} \in c$ holds. It can be exploited to ascertain, in a somewhat procedural way, the last two statements of Fig. [1]. It should be noted, though, that those claims can be proved in a totally different fashion, by resorting to Zorn's lemma (see Fig. [5] and [13, pp. 398–405]) instead of to natural numbers.

$$\begin{aligned}
&\{x \subseteq T \mid (\forall\, u \in x\,,\ v \in x\,,\ z \in T \mid (u \supseteq v \vee v \supseteq u)\ \&\ (\exists\, y \in x \mid z \not\supseteq y))\} = \emptyset \quad \longrightarrow \\
&\qquad\qquad\qquad\qquad (\exists\, m \mid \big\{x \in T \mid x \supseteq m\big\} = \{m\}) \\
&\{p \subseteq S \mid \big\{x \in \bigcup S \mid (\forall\, y \in p \mid x \in y)\big\} \notin S\} = \emptyset\ \ \&\ \ U \in S \quad \longrightarrow \\
&\qquad\qquad\qquad\qquad (\exists\, w \subseteq U \mid \big\{x \in S \mid w \supseteq x\big\} = \{w\})
\end{aligned}$$

Fig. 5. Zorn's lemma and one of its corollaries

The user is referred to [11, Sec. 3] for a crash course on ÆtnaNova, and to [13] for a much wider introduction to this proof-verifier and its underlying logic. A quick comparison of this system with other set-oriented proof-assistants can be found at [11, Sec. 6]; moreover, [10, Sec. 6] carries out a comparison of ÆtnaNova's THEORYs with various related modularization constructs available, in particular, in the OBJ family of languages (see [5]) and in the Interactive Mathematical Proof System (IMPS) described in [4].

2 Kőnig-Halmos's proof of the Cantor-Bernstein theorem

> *J. Kőnig's proof certainly merited Poincaré's attention. It brought a new gestalt to CBT proofs which had "remarkable generalizations" $\cdots$ in new contexts that could not have been foreseen by either J. Kőnig or Poincaré. $\cdots$ J. Kőnig's son, D. Kőnig, $\cdots$ leveraged on his father's 1906 gestalt, to produce results in set theory, graph theory, and other branches of mathematics.*
>
> (Hinkis [7, pp. 217–218])

Given injections α, β satisfying the constraints stated in the Introduction and echoed by the assumptions of the THEORY cbh in Fig. [7], consider the *di*graph whose sets of vertices and arcs are, respectively, the disjoint union $V = A \uplus B$ of the domain A of α with the domain B of β, and

$$E' = \big\{\, \langle w\,,\ v\rangle \ :\ w \in V\,,\ v \in V \mid \langle v\,,\ w\rangle \in \alpha \cup \beta \big\}.$$

In connection with this digraph $D = (V, E')$, consider the *ancestry* function @ sending each $W \subseteq V$ into the set $@\,W$ of all vertices u such that there is a path (of length $\geqslant 0$) leading from a vertex $w \in W$ to u in D. It should be clear that this function can be obtained in ÆtnaNova by actualizing the parameters of the THEORY reachability shown in Fig. 4 as follows:

$$\textsc{Apply}(\mathsf{descs}_\Theta : @)\ \mathsf{reachability}\big(\,\mathsf{V(X)} \mapsto \mathsf{X} \in A \cup B\,,\ \mathsf{E(X,Y)} \mapsto \langle \mathsf{Y}\,,\ \mathsf{X}\rangle \in \alpha \cup \beta\big).$$

(Since E reverses all pairs forming $\alpha \cup \beta$, it seems natural to us to regard the elements of $@\{x\}$ as ancestors, instead of as descendants, of x.)

Ordered pair according to Kuratowski $\langle \mathsf{X}\,,\ \mathsf{Y}\rangle =_{\text{Def}} \{\{\mathsf{X}\}\ ,\ \{\mathsf{X}\,,\ \mathsf{Y}\}\}$

1^{st} of an ordered pair $\mathsf{P}^{[1]} =_{\text{Def}} \mathbf{arb}\Big(\Big\{\mathsf{x} : \mathsf{s} \in \mathsf{P}\,,\ \mathsf{x} \in \mathsf{s} \mid \mathsf{s} = \{\mathsf{x}\}\Big\}\Big)$

2^{nd} of an ordered pair $\mathsf{P}^{[2]} =_{\text{Def}} \mathbf{arb}\Big(\Big\{\mathsf{y} : \mathsf{d} \in \mathsf{P}\,,\ \mathsf{y} \in \mathsf{d} \mid \mathsf{P} = \{\{\mathsf{y}\}\} \vee \mathsf{d} \setminus \{\mathsf{y}\} \in \mathsf{P}\Big\}\Big)$

Map domain, i.e. set of first components of pairs in map $\mathbf{domain}(\mathsf{F}) =_{\text{Def}} \Big\{\mathsf{p}^{[1]} : \mathsf{p} \in \mathsf{F}\Big\}$

Map restriction $\mathsf{F}_{|\mathsf{A}} =_{\text{Def}} \Big\{\mathsf{p} \in \mathsf{F} \mid \mathsf{p}^{[1]} \in \mathsf{A}\Big\}$

Image, i.e. value, of single-valued function $\mathsf{F}\!\upharpoonright\!\mathsf{Y} =_{\text{Def}} \mathbf{arb}\big(\mathsf{F}_{|\{\mathsf{Y}\}}\big)^{[2]}$

Map range, i.e. set of second components of pairs in map $\mathbf{range}(\mathsf{F}) =_{\text{Def}} \Big\{\mathsf{p}^{[2]} : \mathsf{p} \in \mathsf{F}\Big\}$

Map predicate $\mathsf{Is\_map}(\mathsf{F}) \leftrightarrow_{\text{Def}} \Big(\forall \mathsf{p} \in \mathsf{F} \mid \mathsf{p} = \Big\langle \mathsf{p}^{[1]}\,,\ \mathsf{p}^{[2]}\Big\rangle\Big)$

Single-valuedness predicate $\mathsf{Svm}(\mathsf{F}) \leftrightarrow_{\text{Def}} \Big(\forall \mathsf{p} \in \mathsf{F}\,,\ \mathsf{q} \in \mathsf{F} \mid \mathsf{p}^{[1]} = \mathsf{q}^{[1]} \ \rightarrow\ \mathsf{p} = \mathsf{q}\Big)\ \&$
$\mathsf{Is\_map}(\mathsf{F})$

Injection $\mathsf{1\text{–}1}(\mathsf{F}) \leftrightarrow_{\text{Def}} \mathsf{Svm}(\mathsf{F})\ \&\Big(\forall \mathsf{p} \in \mathsf{F}\,,\ \mathsf{q} \in \mathsf{F} \mid \mathsf{p}^{[2]} = \mathsf{q}^{[2]} \ \rightarrow\ \mathsf{p} = \mathsf{q}\Big)$

Map product $\mathsf{G} \circ \mathsf{F} =_{\text{Def}} \Big\{\Big\langle \mathsf{p}^{[1]}\,,\ \mathsf{q}^{[2]}\Big\rangle : \mathsf{p} \in \mathsf{F}\,,\ \mathsf{q} \in \mathsf{G} \mid \mathsf{p}^{[2]} = \mathsf{q}^{[1]}\Big\}$

Inverse map $\mathsf{F}^{\smile} =_{\text{Def}} \Big\{\Big\langle \mathsf{p}^{[2]}\,,\ \mathsf{p}^{[1]}\Big\rangle : \mathsf{p} \in \mathsf{F}\Big\}$

Fig. 6. Definitions related to pairs, maps, single-valued maps, and one-one maps

```
THEORY cbh( α , β )   -- - The Cantor-Bernstein Theorem proved à la Kőnig-Halmos
    1–1(α) & 1–1(β)
    range(α) ⊆ domain(β) & range(β) ⊆ domain(α)
    domain(α) ∩ domain(β) = ∅
⟹(γ_Θ)
    1–1(γ_Θ) & domain(γ_Θ) = domain(α) & range(γ_Θ) = domain(β)
END cbh
```

$$\big(\,1\text{–}1(F)\ \&\ 1\text{–}1(G)\ \&\ \mathbf{range}(F) \subseteq \mathbf{domain}(G)\ \&\ \mathbf{range}(G) \subseteq \mathbf{domain}(F)\,\big) \ \rightarrow$$
$$\big(\exists\, h \mid 1\text{–}1(h)\ \&\ \mathbf{domain}(h) = \mathbf{domain}(F)\ \&\ \mathbf{range}(h) = \mathbf{domain}(G)\big)$$

Fig. 7. The Cantor-Bernstein theorem specified first as a THEORY, then as a formula

As will turn out, the sought injection of A onto B is the relationship

$$\gamma = \big\{\, \langle x\,,\ \alpha\upharpoonright x\rangle\ : x \in A \mid B \cap @\,\{x\} \subseteq \mathbf{range}(\alpha)\big\} \cup \\ \big\{\, \langle \beta\upharpoonright y\,,\ y\rangle\ : y \in B \mid B \cap @\,\{y\} \not\subseteq \mathbf{range}(\alpha)\big\}.$$

Here is the heuristic idea lying behind this choice of γ, treated in pedagogical terms. If an element y_0 of B does not equal $\alpha\upharpoonright x$ for any $x \in A$, in order to make it an α-image under the guidance of β, we would like to modify α by setting $\alpha \coloneqq \alpha \cup \{\langle \beta\upharpoonright y_0\,,\ y_0\rangle\}$; such a naive readjustment would create a collision with the preexisting value $\alpha\upharpoonright\beta\upharpoonright y_0$, though, causing α to cease being single-valued. It hence seems that the right retouch to be made to α is, rather: $\alpha \coloneqq \alpha \setminus \{\langle \beta\upharpoonright y_0, \alpha\upharpoonright\beta\upharpoonright y_0\rangle\} \cup \{\langle \beta\upharpoonright y_0, y_0\rangle\}$. But, then, the previous $y_1 = \alpha\upharpoonright\beta\upharpoonright y_0$ will no longer be an α-image; hence, in order to fix the situation, we are to proceed in analogy with our previous move: inside α, we will now replace the pair $\langle \beta\upharpoonright y_1\,,\ \alpha\upharpoonright\beta\upharpoonright y_1\rangle$ by $\langle \beta\upharpoonright y_1\,,\ y_1\rangle$, etc. Ultimately, fix after fix, we will assign a new image to each element $x_i = \beta\upharpoonright y_i$ of A which originally had y_0 in its ancestry: initially α sent x_i to $\alpha\upharpoonright x_i = y_{i+1}$, but at the end of the replacements its image will turn out to be y_i. The sequence of replacements described so far for a single $y_0 \in B_* = B \setminus \{\, \alpha\upharpoonright x : x \in A\,\}$ should be developed likewise for all others; consequently, at the end of the overall processing, the original edges $\langle y\,,\ \beta\upharpoonright y\rangle$ with $B_* \cap @\,\{y\} \neq \emptyset$ will turn out to be reversed, and the corresponding edges $\langle \beta\upharpoonright y\,,\ \alpha\upharpoonright\beta\upharpoonright y\rangle$ withdrawn, precisely in the manner described in the definition of γ.

In a formal check that the said γ meets our desiderata, the key steps are:

(1) $(\forall\, y \in B \mid @\{\beta\upharpoonright y\} = \{\beta\upharpoonright y\} \cup @\{y\})$;
(2) $(\forall\, x \in A \mid @\{\alpha\upharpoonright x\} = \{\alpha\upharpoonright x\} \cup @\{x\})$;
(3) $\{x \in A \mid B \cap @\{x\} \neq \emptyset\} \subseteq \mathbf{range}(\beta)$;
(4) $\{y \in B \mid B \cap @\{y\} \subseteq \mathbf{range}(\alpha)\} \subseteq \mathbf{range}(\alpha)$;
(5) $\mathsf{Svm}\big(\{\langle \beta\upharpoonright y\,,\ y\rangle\ : y \in B \mid B \cap @\,\{y\} \not\subseteq \mathbf{range}(\alpha)\}\big)$;
(6) $\mathsf{1\text{–}1}\big(\{\langle \beta\upharpoonright y\,,\ y\rangle\ : y \in B \mid B \cap @\,\{y\} \not\subseteq \mathbf{range}(\alpha)\}\big)$;
(7) $\mathsf{Svm}\big(\{\langle x\,,\ \alpha\upharpoonright x\rangle\ : x \in A \mid B \cap @\,\{x\} \subseteq \mathbf{range}(\alpha)\}\big)$ &
$\{\langle x\,,\ \alpha\upharpoonright x\rangle\ : x \in A \mid B \cap @\,\{x\} \subseteq \mathbf{range}(\alpha)\} \subseteq \alpha$;
(8) $\mathsf{1\text{–}1}\big(\,\{\langle x\,,\ \alpha\upharpoonright x\rangle\ : x \in A \mid B \cap @\,\{x\} \subseteq \mathbf{range}(\alpha)\}\,\big)$;
(9) $\mathsf{1\text{–}1}\big(\gamma\big)$;
(10) $\mathsf{domain}\big(\gamma\big) = A$;
(11) $\mathsf{range}\big(\gamma\big) = B$.

Next we want to get rid of the assumption—inherent in what precedes—that $A \cap B = \emptyset$, so as to prove the Cantor-Bernstein theorem in its full extent, to wit:

$$\begin{pmatrix} \mathsf{1\text{–}1}(F)\ \&\ \mathsf{1\text{–}1}(G) & \& \\ \mathbf{range}(F) \subseteq \mathbf{domain}(G) & \& \\ \mathbf{range}(G) \subseteq \mathbf{domain}(F) & \end{pmatrix} \rightarrow \exists\, h \begin{pmatrix} \mathsf{1\text{–}1}(h) & \& \\ \mathbf{domain}(h) = \mathbf{domain}(F) & \& \\ \mathbf{range}(h) = \mathbf{domain}(G) & \end{pmatrix}.$$

Under the new less constraining hypothesis, we put $A_\star = \mathbf{domain}(F)$, $B = \mathbf{domain}(G)$, and $A = \big\{x \cup \{A_\star \cup B\} : x \in A_\star\big\}$; thus,

$$E = \big\{\, \langle x \cup \{A_\star \cup B\}\,,\ x\rangle\ : x \in A_\star\big\}$$

turns out to be an injection with $\textbf{range}(E) = A_\star$ and $\textbf{domain}(E) = A$ disjoint from B. Then we take $\alpha = F \circ E = \big\{ \langle x \cup \{A_\star \cup B\}\, ,\, F\!\upharpoonright\! x\rangle : x \in A_\star \big\}$ and $\beta = E^\smile \circ G = \big\{ \langle y\, ,\, (G\!\upharpoonright\! y) \cup \{A_\star \cup B\}\rangle : y \in B \big\}$, so that an injection γ with $\textbf{domain}(\gamma) = A$, $\textbf{range}(\gamma) = B$ can be singled out on the grounds of what precedes. The sought h is just: $h = \gamma \circ E^\smile = \big\{ \langle x\, ,\, \gamma\!\upharpoonright\!(x \cup \{A_\star \cup B\})\rangle : x \in A_\star \big\}$.

An ÆtnaNova scenario developed from the bare rudiments of set theory and containing the above-outlined proof of the Cantor-Bernstein theorem is available at URL `http://aetnanova.units.it/scenarios/BeyondCantorBernstein/`. This scenario contains 13 definitions and 48 theorems, organized in 5 Theorys. The overall number of proof lines is 680, there are only four proofs exceeding the lenght of 24 lines, and processing the entire scenario takes less than 5 seconds.

The said scenario could be developed rather quickly (namely, in about three weeks), because most of the needed preparatory lemmas had been developed long before: in particular, we could take advantage of the availability of the reachability Theory shown in the upper part of Fig. 4 (cf. [13, pp. 378–386]); roughly, only one third of the proofs was new. The situation with the extension that will be discussed next is different; we have not yet formalized all details, but devoted much time in finding the best usable definitions (e.g., see the definition of $\mathsf{CoCo}(\cdot,\cdot)$ in Fig. 1 and the ones of $\mathsf{ChSet}(\cdot,\cdot)$ and $\mathsf{PeMa}(\cdot,\cdot)$ in Fig. 2), as well as in properly formulating a graph-theoretical counterpart of the Cantor-Bernstein theorem. We feel that we are now at the end of the design phase.

3 Halmos's proof pattern adapted to special graphs

As announced in item (1) of the Introduction, we want to capture the structural properties of the graph induced (in the manner explained there) by a pair α, β of domain-disjoint injections such that $\textbf{range}(\alpha) \subseteq \textbf{domain}(\beta)$ and $\textbf{range}(\beta) \subseteq \textbf{domain}(\alpha)$. Fig. 8 shows the outcome of this elicitation task, formalized as an ÆtnaNova's Theory.

When the ÆtnaNova's Theory graphCBH shown in Fig. 9 gets applied, the set of edges of a graph induced by injections α, β is provided as parameter $\boldsymbol{E}$: we can focus on this set alone, taking it for granted that the set $\boldsymbol{V}$ of vertices equals $\bigcup \boldsymbol{E}$. The perfect matching constructed inside this Theory is returned via pm_Θ. The assumptions to which $\boldsymbol{E}$ is subject match the conclusions of the previous Theory bij_bip. Besides requiring that no vertex has more than two incident edges, those assumptions yield that the connected components of $\boldsymbol{E}$ are vertex-disjoint paths of three kinds:

a) cycles involving an *even* number of edges—each finite component is in fact required to have a choice set ch;
b) infinite simple paths endowed with one endpoint;
c) infinite simple paths devoid of endpoints.

It should be intuitively clear that paths of kind b) have exactly one perfect matching, whereas paths of kinds a) and c) have two; this indicates the rationale

THEORY $\mathsf{bij\_bip}(\boldsymbol{\alpha}, \boldsymbol{\beta})$

$\quad \mathsf{1\text{–}1}(\boldsymbol{\alpha})\ \&\ \mathsf{1\text{–}1}(\boldsymbol{\beta})$

$\quad \mathbf{range}(\boldsymbol{\alpha}) \subseteq \mathbf{domain}(\boldsymbol{\beta})\ \&\ \mathbf{range}(\boldsymbol{\beta}) \subseteq \mathbf{domain}(\boldsymbol{\alpha})$

$\quad \mathbf{domain}(\boldsymbol{\alpha}) \cap \mathbf{domain}(\boldsymbol{\beta}) = \emptyset$

$\Longrightarrow(\mathsf{ecbh}_\Theta\,,\ \mathsf{acbh}_\Theta)$

$\quad \mathsf{ecbh}_\Theta \ = \ \Big\{ \{\mathsf{q}^{[1]}, \mathsf{q}^{[2]}\} : \mathsf{q} \in \boldsymbol{\alpha} \cup \boldsymbol{\beta} \mid \langle \mathsf{q}^{[2]}, \mathsf{q}^{[1]} \rangle \notin \boldsymbol{\alpha} \cup \boldsymbol{\beta} \Big\}$

$\quad \mathsf{acbh}_\Theta \ = \ \mathbf{domain}(\boldsymbol{\alpha})$

$\quad \big(\forall \mathsf{q} \in \mathsf{ecbh}_\Theta \mid (\exists \mathsf{x}, \mathsf{y} \mid \mathsf{q} \cap \mathsf{acbh}_\Theta = \{\mathsf{x}\}\ \&\ \mathsf{q} \setminus \mathsf{acbh}_\Theta = \{\mathsf{y}\})\big)$

$\quad \big(\forall \mathsf{q} \in \mathsf{ecbh}_\Theta\,,\ \mathsf{h} \in \mathsf{ecbh}_\Theta\,,\ \mathsf{k} \in \mathsf{ecbh}_\Theta \mid \mathsf{h} \neq \mathsf{q}\ \&\ \mathsf{k} \neq \mathsf{q}\ \&\ \mathsf{k} \neq \mathsf{h}\ \rightarrow\ \mathsf{q} \cap \mathsf{h} \cap \mathsf{k} = \emptyset\big)$

$\quad \big(\forall \mathsf{p} \subseteq \mathsf{ecbh}_\Theta \mid \mathsf{ReachCl}(\,\mathsf{p}\,,\ \mathsf{ecbh}_\Theta\,)\ \&\ \mathsf{Finite}(\mathsf{p})\ \rightarrow$

$\qquad\qquad \big(\forall \mathsf{h} \in \mathsf{p} \mid \mathsf{h} \setminus \bigcup(\mathsf{p} \setminus \{\mathsf{h}\}) = \emptyset\big)\ \&\ \big(\exists\, ch \mid \mathsf{ChSet}(ch\ \mathsf{p})\big)\ \big)$

END $\mathsf{bij\_bip}$

Fig. 8. Properties of the undirected graph induced by two injections

THEORY $\mathsf{graphCBH}(\boldsymbol{E})$

$\quad \big(\forall \mathsf{q} \in \boldsymbol{E}, \mathsf{h} \in \boldsymbol{E}, \mathsf{k} \in \boldsymbol{E} \mid \big(\exists \mathsf{x}, \mathsf{y} \mid \mathsf{q} = \{\mathsf{x}, \mathsf{y}\}\ \&\ \mathsf{x} \neq \mathsf{y}\big)\ \&$

$\qquad\qquad \big(\mathsf{h} \neq \mathsf{q}\ \&\ \mathsf{k} \neq \mathsf{q}\ \&\ \mathsf{k} \neq \mathsf{h}\ \rightarrow\ \mathsf{q} \cap \mathsf{h} \cap \mathsf{k} = \emptyset\big)\big)$

$\quad \big(\forall \mathsf{p} \subseteq \boldsymbol{E} \mid \mathsf{CoCo}(\mathsf{p}, \boldsymbol{E})\ \&\ \mathsf{Finite}(\mathsf{p})\ \rightarrow$

$\qquad\qquad \{\mathsf{h} \setminus \bigcup(\mathsf{p} \setminus \{\mathsf{h}\}) : \mathsf{h} \in \mathsf{p}\} \subseteq \{\emptyset\}\ \&\ \big(\exists\, ch \mid \mathsf{ChSet}(ch, \mathsf{p})\big)\big)$

$\Longrightarrow(\mathsf{pm}_\Theta)$

$\quad \mathsf{pm}_\Theta = \bigcup\{\, pm : cc \subseteq \boldsymbol{E}\,,\ pm \subseteq cc \mid \mathsf{CoCo}(\,cc\,,\ \boldsymbol{E}\,)\ \&$

$\qquad\qquad pm = \mathbf{arb}\big(\{\mathsf{q} \subseteq cc \mid \mathsf{PeMa}(\,\mathsf{q}\,,\ cc\,)\,\}\big)\}$

$\quad \mathsf{PeMa}(\,\mathsf{pm}_\Theta\,,\ \boldsymbol{E}\,)$

END $\mathsf{graphCBH}$

Fig. 9. A graph-theoretical counterpart of the Cantor-Bernstein theorem

for imposing, in the above specification of pm_Θ, that

$$pm = \mathbf{arb}\big(\{q \subseteq cc \mid \mathsf{PeMa}(\,q\,,\ cc\,)\}\big)$$

holds: should we only require $pm \in \{q \subseteq cc \mid \mathsf{PeMa}(\,q\,,\,cc\,)\}$, we might be putting in pm_Θ too much. One way of constructing each set $\{q \subseteq cc \mid \mathsf{PeMa}(\,q\,,\ cc\,)\}$, with cc connected component of $\boldsymbol{E}$, is by considering the sum sets

$$\bigcup\Big\{\, th(i, r) \setminus \bigcup\{\, th(j, r) : j \in i\} : i \in \mathbb{N} \mid \mathsf{Even}(i)\,\Big\}$$

associated with the elements r of cc. When cc is of kind either a) or c), all such sum sets (of which only two differ) are perfect matchings; as regards a component cc of kind b), the sole $r \in cc$ to be taken into account is the one that includes the singleton $\big\{\, k \in cc \mid k \setminus \bigcup\big(cc \setminus \{k\}\big) \neq \emptyset\big\}$.

In Section 2 we gave clues on how, inside the THEORY cbh outlined in Fig. 7, one can construct $\boldsymbol{\gamma}_\Theta$ and prove the pertaining facts (e.g., its injectivity) in a stand-alone fashion. Here below we discuss a slicker implementation of the internals of cbh, which will come into effect once the Theorys bij_bip and graphCBH of Fig. 8 and Fig. 9 will be available.

Under the assumptions of cbh, which are identical to the ones of bij_bip, we can apply the latter Theory to $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, and so get $\mathsf{acbh} = \mathbf{domain}(\boldsymbol{\alpha})$ along with an ecbh complying with the statements that appear in the lower part of Fig. 8; in their turn, those statements enable application of the Theory graphCBH to $\boldsymbol{E} = \mathsf{ecbh}$, which then provides a perfect matching pm for the graph endowed with vertices $\bigcup \mathsf{ecbh}$ and edges ecbh. To obtain the desired one-one correspondence, it now suffices to put

$$\boldsymbol{\gamma}_{\Theta} = \big\{ \langle x\,,\, y \rangle \,:\, e \in \mathsf{pm}\,,\; x \in e \cap \mathsf{acbh}\,,\; y \in e \setminus \mathsf{acbh} \big\} \cup \\ \big\{ a \in \boldsymbol{\alpha} \mid \big\langle a^{[2]}\,,\, a^{[1]} \big\rangle \in \boldsymbol{\beta} \big\}.$$

Conclusions

The ‘proof pearl’ highlighted in this paper adds a tile to a much larger-scale mosaic of proof scenarios which have to do with the interplay between sets and graphs (e.g., see [11, 12]), as well as with representation theorems of the kind illustrated by the classical Stone’s results on Boolean algebras that states that every unital ring where the identities $X + X = 0$ and $X \cdot X = X$ hold is isomorphic to the field of the clopen sets of a totally disconnected compact Hausdorff space where intersection and symmetric set-difference act as multiplication and addition (see [15, 16, 17] and [3]).

Those many experiments are intended to contribute collectively to a unitary study on the foundations of discrete mathematics; therefore each of them is meant to have a bearing on others, and is designed in such terms that it can reuse achievements of previous efforts and can easily be integrated with the rest.

This explains why, even though only graphs and digraphs enter the proof of the Cantor-Bernstein theorem, we chose to define the connected components of an arbitrary set E—not obligatorily one consisting of doubletons—, seen as the set of edges of a *hypergraph*. By so doing, we can more easily merge the proof scenario discussed in this paper with the one of [2] (downsized in [9, pp.251–262]).

Also, the collection $\{\, c \subseteq E \mid \mathsf{ReachCl}(c, E) \,\}$ of those sets of (hyper)edges that are closed under reachability forms, one readily sees, a Boolean algebra: in fact, it is closed under intersection and symmetric difference and E is one of its members. Elsewhere, in proving Stone’s results, we had to bring into play Zorn’s lemma; accordingly, in this paper we found it convenient to opt for a declarative definition of connected components, albeit a characterization of connected components relying either upon paths or—which amounts, roughly, to the same—upon the Theory connComp seen in Fig. 4 would have sufficed for the limited goals addressed above.

Acknowledgements

Discussions with Francesco Cancian were fruitful for the matters of this paper.

References

[1] R. M. Burstall and J. A. Goguen. Putting theories together to make specifications. In R. Reddy, editor, *Proc. 5$^{\text{th}}$ International Joint Conference on Artificial Intelligence*, pages 1045–1058, Cambridge, MA, 1977.

[2] A. Casagrande and E. G. Omodeo. Reasoning about connectivity without paths. In S. Bistarelli and A. Formisano, editors, *Proceedings of the 15th Italian Conference on Theoretical Computer Science, Perugia, Italy, September 17-19, 2014.*, volume 1231 of *CEUR Workshop Proceedings*, pages 93–108. CEUR-WS.org, 2014.

[3] R. Ceterchi, E. G. Omodeo, and A. I. Tomescu. The representation of Boolean algebras in the spotlight of a proof checker. In L. Giordano, V. Gliozzi, and G. L. Pozzato, editors, *CILC 2014: Italian Conference on Computational Logic*, volume 1195 `http://ceur-ws.org/Vol-1195/`, ISSN 1613-0073, pages 287–301. CEUR Workshop Proceedings, July 2014.

[4] W. M. Farmer, J. D. Guttman, and F. J. Thayer. IMPS: An interactive mathematical proof system. *J. Autom. Reason.*, 11:213–248, 1993.

[5] J. A. Goguen and G. Malcolm. *Algebraic Semantics of Imperative Programs*. MIT Press, Cambridge, MA, USA, 1996.

[6] P. R. Halmos. *Naive Set Theory*. Van Nostrand, 1960. Reprinted by Springer-Verlag, Undergraduate Texts in Mathematics, 1974.

[7] A. Hinkis. *Proofs of the Cantor-Bernstein Theorem: A mathematical excursion*, volume 45 of *Science Networks. Historical Studies*. Birkhäuser Basel, 2013.

[8] J. König. Sur la théorie des ensembles. *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, 143:110–112, Paris, 1906.

[9] E. G. Omodeo, A. Policriti, and A. I. Tomescu. *On Sets and Graphs: Perspectives on Logic and Combinatorics*. Springer Publishing Company, Inc., 1st edition, 2017.

[10] E. G. Omodeo and J. T. Schwartz. A 'Theory' mechanism for a proof-verifier based on first-order set theory. In A. Kakas and F. Sadri, editors, *Computational Logic: Logic Programming and beyond — Essays in honour of Bob Kowalski, part II*, volume 2408, pages 214–230. Springer, 2002.

[11] E. G. Omodeo and A. I. Tomescu. Set graphs. III. Proof pearl: Claw-free graphs mirrored into transitive hereditarily finite sets. *J. Autom. Reason.*, 52(1):1–29, 2014.

[12] E. G. Omodeo and A. I. Tomescu. Set graphs. V. On representing graphs as membership digraphs. *J. Log. Comput.*, 25(3):899–919, 2015.

[13] J. T. Schwartz, D. Cantone, and E. G. Omodeo. *Computational Logic and Set Theory - Applying Formalized Logic to Analysis*. Springer, 2011.

[14] W. Sieg and P. Walsh. Natural Formalization: Deriving the Cantor-Bernstein Theorem in ZF. (Private communication), 2017.

[15] M. H. Stone. The theory of representations for Boolean algebras. *Transactions of the American Mathematical Society*, 40:37–111, 1936.

[16] M. H. Stone. Applications of the theory of Boolean rings to general topology. *Transactions of the American Mathematical Society*, 41:375–481, 1937.

[17] M. H. Stone. The representation of Boolean algebras. *Bulletin of the American Mathematical Society*, 44(Part 1):807–816, 1938.

A Cardinalities and the Cantor-Bernstein theorem

When the discovery of the Cantor-Bernstein theorem took place (late 19^{th} century), it contributed to clarifying the then emerging notions of equipotence and cardinality.

Equipotence is the equivalence relationship that holds between two sets whose respective elements can be put in one-one correspondence. Denote by $\preceq$ the relation between sets:

$$\begin{array}{rl} A \preceq B \ \leftrightarrow_{\text{Def}} & \text{an } \alpha \text{ exists such that } \mathsf{1\text{--}1}(\alpha) \text{ and} \\ & \mathbf{domain}(\alpha) = A\,,\ \mathbf{range}(\alpha) \subseteq B\,; \end{array}$$

then we can phrase the Cantor-Bernstein theorem as follows:

‖ When $A \preceq B$ and $B \preceq A$ both hold, A and B are equipotent.

Cardinality—as seen from a contemporary viewpoint—is the function that sends every set S to a canonical representative, $\#S$, of the equipotence class to which S belongs. Hence, we can also thus state the Cantor-Bernstein theorem:

‖ When $A \preceq B$ and $B \preceq A$ both hold, $\#A = \#B$ holds as well.

It has today become customary to regard *cardinals*—namely, the representatives of equipotence classes—as forming a strict subclass of the class of von Neumann's *ordinal* numbers. In their turn, ordinals are special sets internally well-ordered by membership; they enable one to impose a well-ordering to a set S whatsoever by somehow 'enumerating' the elements of S. Specifically, under the assumption that membership is a well-founded relation over sets, ordinals can be defined *à la* Raphael M. Robinson as follows:

$$\mathsf{Ord}(O) \ \leftrightarrow_{\text{Def}} \ \big(\forall\, x \in O\,,\ y \in O \setminus \{x\} \mid x \in y \ \lor \ y \in x\big) \ \&\ O \supseteq \bigcup O\,;$$

then, after formulating the recursive definition of the enumeration process as

$$\begin{array}{rl} \mathsf{enum}(X, S) \ =_{\text{Def}} & \mathbf{if} \qquad S \subseteq \{\mathsf{enum}(y, S) : y \in X\} \ \ \mathbf{then}\ S \\ & \mathbf{else}\ \mathbf{arb}(S \setminus \{\mathsf{enum}(y, S) : y \in X\})\ \mathbf{fi}\,, \end{array}$$

one proves that

$$\Big(\exists\, o \mid \ \mathsf{Ord}(o) \ \&\ S = \{\mathsf{enum}(y, S) : y \in o\} \ \& \\ \big(\forall\, u \in o\,,\ v \in o \setminus \{u\} \mid \mathsf{enum}(u, S) \neq \mathsf{enum}(v, S)\big)\Big)$$

holds for every S .

Through Skolemization—which in ÆtnaNova acts as a built-in THEORY—, this claim leads to the definition of a global function, $\mathsf{enum}_{\mathsf{ord}}$, such that

$$\Big(\forall\, s \mid \ \mathsf{Ord}\big(\mathsf{enum}_{\mathsf{ord}}(s)\big) \ \&\ s = \big\{\mathsf{enum}(y, s) : y \in \mathsf{enum}_{\mathsf{ord}}(s)\big\} \ \& \\ \big(\forall\, u \in \mathsf{enum}_{\mathsf{ord}}(s)\,,\ v \in \mathsf{enum}_{\mathsf{ord}}(s) \setminus \{u\} \mid \mathsf{enum}(u, s) \neq \mathsf{enum}(v, s)\big)\Big).$$

The cardinality of a set can then be defined as follows:

$$\#S =_{\text{Def}} \mathbf{arb}\Big(\{\, o \in \mathsf{next}\big(\mathsf{enum}_{\mathsf{ord}}(S)\big) \mid \big(\exists\, f \mid \mathsf{1\text{–}1}(f) \;\&\; \mathbf{domain}(f) = o \;\; \mathbf{range}(f) = S\,\big)\,\} \Big);$$

namely, $\#S$ is the least ordinal number o that is equipotent to S.

To end, here is the definition of a cardinal number:

$$\begin{aligned}\mathsf{Card}(C) \leftrightarrow_{\text{Def}} &\ \mathsf{Ord}(C)\ \& \\ &\big(\forall\, o \in C \mid \big(\neg\exists\, f \mid \mathsf{Svm}(f)\ \&\ \mathbf{domain}(f) = o\ \&\ \mathbf{range}(f) = C\big)\big);\end{aligned}$$

that is to say, a cardinal number is an ordinal number C such that no function f exists mapping an ordinal o smaller than C onto C.

Along the path discussed in [13, Section 5.3], one reaches two key theorems,

$$\mathsf{1\text{–}1}(F)\ \&\ \mathsf{Card}\big(\mathbf{domain}(F)\big) \rightarrow \mathbf{domain}(F) = \#\mathbf{range}(F)$$

and

$$C = \#S \leftrightarrow \mathsf{Card}(C)\ \&\ \big(\exists\, f \mid \mathsf{1\text{–}1}(f)\ \&\ \mathbf{domain}(f) = C\ \&\mathbf{range}(f) = S\big),$$

whence

$$\mathsf{1\text{–}1}(F)\ \&\ \mathsf{Card}\big(\mathbf{domain}(F)\big)\ \&\ \mathsf{Ord}\big(\mathbf{range}(F)\big) \rightarrow \mathbf{domain}(F) \subseteq \mathbf{range}(F)\,,$$

which leads straightforwardly to the Cantor-Bernstein theorem, in a way that differs substantially from the pattern discussed earlier (see Sections 2 and 3).