Rend. Istit. Mat. Univ. Trieste
Volume 42 (2010), 211–234.

Bisimilarity, Hypersets, and Stable Partitioning: a Survey

Eugenio G. Omodeo

Abstract. *Since Hopcroft proposed his celebrated $n \log n$ algorithm for minimizing states in a finite automaton, the race for efficient partition refinement methods has inspired much research in algorithmics. In parallel, the notion of bisimulation has gained ground in theoretical investigations not less than in applications, till it even pervaded the axioms of a variant Zermelo-Fraenkel set theory. As is well-known, the coarsest stable partitioning problem and the determination of bisimilarity (i.e., the largest partition stable relative to finitely many dyadic relations) are two faces of the same coin. While there is a tendency to refer these topics to varying frameworks, we will contend that the set-theoretic view not only offers a clear conceptual background (provided stability is referred to a non-well-founded membership), but is leading to new insights on the algorithmic complexity issues.*

Keywords: Partition Refinement, Bisimulation, Bisimilarity, Stability, Non-Well-Founded Sets.
MS Classification 2010: 03E30, 03E70, 03E75, 05C85, 68Q25

Introduction

When, as it seldom happens, a novel notion acquires significance in various branches of mathematics at the same time, that pervasive notion gradually slides down towards the first principles and it candidates for a preeminent role in the foundations of mathematics. This happened when, in the 1920s, recursion gained ground as a convenient way of hooking the specifications of functions and relations of domain V to a dyadic relation E that meets, on V, suitable conditions. This happened again in the 1980s, when bisimilarity imposed itself as a ubiquitous equivalence criterion for partitioning a class V in a way that again relies on a dyadic relation E on V. In 1925 von Neumann managed to tie recursion directly to set membership by introducing a new axiom, *regularity* [26], among the postulates of the Zermelo-Fraenkel set theory

ZF. Likewise, around 1985, Aczel investigated the consequences of superseding regularity by an *anti-foundation axiom*: *AFA* [2].[1] While disrupting the hierarchical structure of von Neumann's universe of sets by enriching it with a host of new entities (at times called '*hypersets*' [4]), AFA also avoids overcrowding the universe, by enforcing bisimilarity as a criterion for equality between sets.

Aczel's universe of sets—to which much of our subsequent discussion will refer—hence encompasses von Neumann's celebrated *cumulative hierarchy*. Its greater richness eases the modeling of circular phenomena, with special success when bisimilarity is at work. Typical situations of this nature are associated with automata, Kripke structures, communicating systems (cf. [9]): when referring to these, in fact, one is often confronted with structures endowed with a multitude of 'states', which become more manageable and easier to subdue to formal verification methods if bisimilarity is exploited to identify indistinguishable states with one another.[2] The so-called *coarsest stable partition refinement* problem, a classic in algorithmics [22], can be very naturally cast as the problem of determining bisimilarity between the nodes of a graph $\mathcal{G} = (V, E)$, thinking without loss of generality that arcs represent membership relations [9], i.e., there is an arc $x \overset{E}{\to} y$ if and only if $x \ni y$.

Let us adopt this definition of the REFINEMENT relation between arbitrary sets P, Q:

$$P \sqsubseteq Q \quad \Leftrightarrow_{\text{Def}} \quad \bigcup P = \bigcup Q \,\&\, \forall\, p \in P\; \exists!\, q \in Q\; p \cap q \neq \emptyset;$$

in words, P is *finer* than Q (and Q is *coarser* than P) if the members of sets in P are the same as the members of sets in Q and every set belonging to P intersects one and only one set belonging to Q. Then we can define π to be a PARTITION (in the usual sense) iff $\pi \sqsubseteq \pi$ holds. Let us also define the STABILITY of a partition π with respect to all members of a set S:

$$\pi \dot{\simeq} S \quad \Leftrightarrow_{\text{Def}} \quad \forall\, a \in S\; \forall\, p \in \pi \;\; \emptyset \in \{\, p \cap a,\; p \setminus a \,\}.$$

How far-reaching are generalizations of the following classical proposition?

THEOREM 1 (Venn's partition lemma). *For any set S of sets, there is a partition $\pi_\star$ of $\bigcup S$ which is stable and is coarser than any other stable partition of $\bigcup S$:*

$$\forall\, S\; \exists\, \pi_\star \sqsubseteq \left\{\bigcup S\right\}\; \forall\, \pi \sqsubseteq \left\{\bigcup S\right\}\; \left(\pi \dot{\simeq} S \Leftrightarrow \pi \sqsubseteq \pi_\star\right).$$

---

[1] [5, p. 5] indicates [13] as a precursor of Aczel's set theory.

[2] This point is well explained in [14], which also draws a parallel between bisimilarity and an akin notion of *similarity*: one often resorts to either notion in order to reduce the size of a modeling structure, but there are situations in which similarity serves this purpose better than bisimilarity.

$$
\begin{aligned}
P \preccurlyeq Q \;&\Leftrightarrow_{\text{Def}}\; \forall\, p \in P\; \exists!\, q \in Q\; p \cap q \neq \emptyset \\
\mathsf{ls\_partition}(\pi) \;&\Leftrightarrow_{\text{Def}}\; \pi \preccurlyeq \pi \\
\pi \sqsubseteq Q \;&\Leftrightarrow_{\text{Def}}\; \pi \preccurlyeq \pi \;\&\; \pi \preccurlyeq Q \;\&\; \bigcup \pi = \bigcup Q \\
R^{-1}[Y] \;&=_{\text{Def}}\; \{\, x\colon\, \langle x, y\rangle \in R \;\&\; y \in Y \,\} \\
\pi \doteq \Re \;&\Leftrightarrow_{\text{Def}}\; \forall\, R \in \Re\, \forall\, p \in \pi\, \forall\, q \in \pi \quad \emptyset \in \{\, p \cap R^{-1}[q],\; p \setminus R^{-1}[q] \,\}
\end{aligned}
$$

Figure 1: Notions of partition, refinement, and stability

$$
\mathsf{ls\_partition}(\pi^\star)\;\&\;\Re \subseteq \mathscr{P}\left(\bigcup \pi^\star \times \bigcup \pi^\star\right) \Longrightarrow \\
\exists\, \pi_\star \sqsubseteq \pi^\star\, \forall\, \pi \sqsubseteq \pi^\star\, (\, \pi \doteq \Re \Leftrightarrow \pi \sqsubseteq \pi_\star\,)
$$

Figure 2: Statement of existence of the coarsest stable partition

Over the years, the scientific community bestowed a lot of attention to such generalizations, partly motivated—at least initially—by the study of Robin Milner's calculus of communicating systems [20]. In particular, Paris Kanellakis and Scott Smolka [17, 18] thought of adapting John Hopcroft's celebrated algorithm (1971) for minimizing a deterministic finite automaton to finite state *processes* "slightly more general than the familiar non-deterministic finite state automata with empty moves".[3]

In Hopcroft's minimization problem one must again refine a given partition, the one dividing the set $\mathcal{Q}$ of states into the block $\mathcal{F}$ of all accepting states and the block $\mathcal{Q} \setminus \mathcal{F}$ of nonaccepting states; the sought partition must discern whether or not two states behave the same, but it should be as coarse as possible: coarseness implying that the numer of states will be low in the reduced automaton.

1. Big, Small, and Very Small Graphs

Bisimulations, whose notion will be introduced later on, presuppose *systems*. We readily define the latter notion, along with two specialized variants of it:

1. A SYSTEM $\mathcal{M} = (V, E)$ is a class V of NODES paired with a class E of EDGES, $E \subseteq V \times V$. The nodes V can form a *proper* class;[4] consequently, E can in its turn be proper. Anyway, one insists that

[3]We remind the reader that R. Milner received the 1991 Turing award for achievements which included the general CCS theory of concurrency just mentioned.

[4]In Cantor's metaphor, a class is *proper* when it is 'too big' to be a set (consider, e.g., the class of all ordinals). Intuitively speaking, this happens when one cannot attribute a cardinality to a class. Technically, in the formalized von Neumann-Gödel-Bernays theory of sets and classes, a class is proper if and only if it belongs to no class.

the 'children' $a{\uparrow} =_{\text{Def}} \{\, b\colon b \in V \,\&\, a\, E\, b \,\}$ form a *set*, for each node a.

2. A GRAPH is a '*small*' system; namely, one whose edges and nodes form two sets.

3. A FINITE GRAPH has finitely many edges and nodes. (Accordingly, the entities relevant for its study—in particular the forthcoming bisimulations—can be algorithmically constructed and manipulated).

An example of kind 1. is the pair $\mathsf{Sets} = (\mathcal{U}, \ni)$, where $\mathcal{U}$ is the universe of all sets and $\ni$ is the converse of the membership relation between sets.[5]

An example of kind 2. is the pair $(\mathsf{trCl}(\upsilon), \ni_\upsilon)$, where $\mathsf{trCl}(\upsilon)$ is the TRANSITIVE CLOSURE of a set υ, viz. the least full superset τ of υ:

- $\tau \supseteq \upsilon$;
- $\tau \subseteq \mathscr{P}(\tau)$, i.e., $X \in \tau$ implies $X \subseteq \tau$ for all X (*fullness*);
- $\tau \subseteq \tau'$ for every $\tau' \supseteq \upsilon$ such that $\tau' \subseteq \mathscr{P}(\tau')$ (*minimality*);

and where $\ni_\upsilon =_{\text{Def}} \ni \cap\big(\mathsf{trCl}(\upsilon) \times \mathsf{trCl}(\upsilon)\big)$ designates the restriction of $\ni$ to this 'small universe' $\mathsf{trCl}(\upsilon)$.

An example of kind 3. is the pair $(\mathcal{Q}, d_{\mathsf{a}})$, where $\mathcal{Q}$ is the set of all states of a deterministic finite automaton (in short, a 'DFA') [8], a is a symbol of the automaton's alphabet $\mathcal{A}$, and d_{a} is the function consisting of all pairs $\langle q, q'\rangle$ of states such that the automaton has a transition labeled a leading from q to q'. Another related example is the transition graph of the automaton deprived of edge labels, namely $(\mathcal{Q}, \bigcup_{\mathsf{a}\in\mathcal{A}} d_{\mathsf{a}})$.

By reflecting upon the structure of the graphs $(\mathsf{trCl}(\{\upsilon\}), \ni_{\{\upsilon\}})$ and upon the relationship between each of them and the global system $\mathcal{U} = (\mathcal{U}, \ni)$, one gets the following notions:

apg: An ACCESSIBLE POINTED GRAPH is a triple (V, E, ν_0) where (V, E) is a graph, $\nu_0 \in V$ is a distinguished node, and every $\nu \in V$ has at least one path $\nu_0\, E\, \nu_1\, E \cdots E \nu_m$ issuing from the distinguished node and leading to $\nu_m = \nu$ through a finite sequence of edges $\langle \nu_i, \nu_{i+1}\rangle$. When there is only one such path for each ν, the apg is called a TREE.

$\mathcal{M}_\upsilon$: Let $\mathcal{M} = (V, E)$ be a system and υ one of its nodes. Put $T_0(\upsilon) =_{\text{Def}} \{\upsilon\}$, $T_{i+1}(\upsilon) =_{\text{Def}} \bigcup\{v{\uparrow} : v \in T_i(\upsilon)\}$, so that the j-th stage $T_j(\upsilon)$ is the set of those nodes of $\mathcal{M}$ that end paths of length j issuing from υ, for each

---

[5] The CONVERSE E^{-1} of a dyadic relation E is, by definition, the class $\{\, \langle w, v\rangle : v\ E\ w \,\}$. Occasionally we will also refer to the COMPOSITION $E \circ E' =_{\text{Def}} \{\, \langle x, z\rangle : \exists\, y\, (\langle x, y\rangle \in E \,\&\, \langle y, z\rangle \in E') \,\}$ of E with another dyadic relation E'.

natural number j. As final stage, take the union $T_\infty(\upsilon) =_{\text{Def}} \bigcup_{j\in\mathbb{N}} T_j(\upsilon)$ of all stages. Thus $\mathcal{M}_\upsilon = (T_\infty(\upsilon), E_\upsilon, \upsilon)$, where $E_\upsilon = E \cap (T_\infty(\upsilon) \times T_\infty(\upsilon))$, will be the APG ISSUING FROM υ IN $\mathcal{M}$.

Besides the apgs $\mathcal{M}_\upsilon$ (of which the pointed graphs $(\mathsf{trCl}(\{\upsilon\}), \ni_{\{\upsilon\}}, \upsilon)$ plainly are a special case), an example of apg is, typically, the transition graph $(\mathcal{Q}, \bigcup_{\mathsf{a}\in\mathcal{A}} d_\mathsf{a}, q_0)$ of a DFA whose initial state, q_0, is singled out as the distinguished node (states unreachable from q_0, e.g. because they are isolated, would be totally useless in the DFA's description).

One has *no* guarantee, in general, that

$$\text{the 'parents' } b^{\curvearrowleft} =_{\text{Def}} \{\, a\colon a \in V \,\&\, a\, E\, b \,\} \text{ form a } \textit{set}, \text{ for each node } a,$$

in a system $\mathcal{M} = (V, E)$; but in the favorable cases when this happens, e.g. when $\mathcal{M}$ is a graph, one can define the SYMMETRIC CLOSURE $\widehat{\mathcal{M}}$ of $\mathcal{M}$, as well as the SYMMETRIC-TRANSITIVE-REFLEXIVE CLOSURE $\mathcal{M}^*$ of $\mathcal{M}$:

$$\begin{array}{rcl} \widehat{\mathcal{M}} & =_{\text{Def}} & (V, E \cup E^{-1}), \\ \mathcal{M}^* & =_{\text{Def}} & (V, \{\, \langle v, w\rangle : w \in \widehat{\mathcal{M}}_v \,\}). \end{array}$$

To end with one more example, consider the system $\mathsf{next} = (\mathcal{U}, +1)$ whose edges are the pairs $\langle x, x \cup \{x\}\rangle$ with x a set. Then $\mathsf{next}_\emptyset = (\mathbb{N}, \{\langle i, i+1\rangle : i \in \mathbb{N}\}, 0)$ if we intend natural numbers *à la* von Neumann, as forming the set

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\} = \big\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots\big\}.$$

2. Well-Foundedness

We say that a system $\mathcal{M} = (V, E)$ is WELL-FOUNDED if

$$\forall\, w\big(\, w \subseteq V \,\&\, w \neq \emptyset \Longrightarrow \exists\, m \in w\, (m^{\curvearrowright} \cap w = \emptyset)\,\big),$$

namely if every nonnull set w of nodes has a 'minimal' element m relative to the converse E^{-1} of E—traditionally it is E^{-1} (not E, notice) which is said to be well-founded when the above condition is met.[6]

It would not be restrictive in the above condition for well-foundedness to require the cardinality w not to exceed the first infinite cardinal; indeed, it would be equivalent to say:

---

[6] An immaterial change we could make inside our definition of well-foundedness would be to replace '$w \subseteq V$' by '$w \subseteq \mathsf{dom}\, E$', where

$$\mathsf{dom}\, E \quad =_{\text{Def}} \quad \{\, t\colon t \in V \,\&\, \exists s\, t\, E\, s \,\}\,;$$

inside a $w \subseteq V$, any element not belonging to $\mathsf{dom}\, E$ is in fact minimal relative to E^{-1}.

$\mathcal{M}$ is well-founded iff there are no infinite paths $a_0\, E\, a_1\, E\, a_2 \cdots$ in V.

The latter characterization helps intuition (e.g., it readily shows us that well-foundedness implies that E has no finite cycles), but it is less basic. Actually, how do we characterize finitude in the first place? One can define a set F to be FINITE when the graph $(\mathscr{P}(F), \supsetneq)$, whose nodes are the subsets of F, is well-founded:

$$\mathsf{Is\_finite}(F) \;\Leftrightarrow_{\text{Def}}\; \forall\, w \,\big(\, w \subseteq \mathscr{P}(F)\,\&\, w \neq \emptyset \Longrightarrow \exists\, m \in w\, \neg\exists\, t \in w\; m \supsetneq t\,\big).$$

Remarkably, the well-foundedness of $\mathcal{M}$ implies that every *class* w of nodes of $\mathcal{M}$ owns a minimal element m. In fact, when w is a proper class, the minimal elements of any *set* $T_\infty(w_0) \cap w$ with w_0 belonging to w are also minimal in w.

After John von Neumann, the universe $\mathcal{U}$ of all sets is the CUMULATIVE HIERARCHY [27], over which membership forms no infinite 'descending chains' $a_0 \ni a_1 \ni a_2 \ni \cdots$. Before von Neumann included REGULARITY

$$\textbf{(R)} \quad \forall\, w\big(w \neq \emptyset \Longrightarrow \exists\, m \in w\,(m \cap w = \emptyset)\big)$$

[26] among the postulates of set theory, this well-foundedness assumption was not (even tacitly) made.

Since Zermelo's pioneering postulates for set theory [29] did not encompass regularity, he had to be cautious in stating the INFINITY axiom, which he did essentially in the following terms:

$$\textbf{(I)} \quad \exists s\big(\emptyset \in s\,\&\,\forall\, t \in s(\{t\} \in s)\big).$$

Had he resorted to the weaker statement

$$\exists s\big(\emptyset \neq s\,\&\,\forall\, t \in s(\{t\} \in s)\big)$$

(or to the even weaker statement **(I′)** shown in the Appendix), how could he have excluded that s, instead of being infinite, were a solution for the equation $X = \{X\}$, and hence a singleton?

Zermelo's epochal paper [29] also contains a proof that $x \neq \mathscr{P}(x)$ holds for every set x. His proof was of a charming simplicity, but it was not as plain as it would be in ZF, namely in the Zermelo-Fraenkel(-von Neumann) set theory as known today. Suppose $\mathscr{P}(x) \subseteq x$ could hold; then, since $x \subseteq x$ and hence $x \in \mathscr{P}(x)$, we would have $x \in x$, against the acyclicity of membership.

Through regularity one gains a powerful mechanism for making definitions, based on $\in$-recursion. Without entering into much detail, let us exemplify this through the following definitions of a HEREDITARILY FINITE set, of the RANK of a set, and of the set of ULTIMATE MEMBERS of any set X:

$$\begin{aligned}
\mathsf{HF}(F) \;&\Leftrightarrow_{\text{Def}}\; \mathsf{Is_finite}(F)\,\&\,\forall\, y \in F\ \mathsf{HF}(y),\\
\mathsf{rk}(X) \;&=_{\text{Def}}\; \sup\{\,\mathsf{rk}(y)+1\colon y \in X\,\},\\
\mathsf{ult_membs}(X) \;&=_{\text{Def}}\; X \cup \bigcup\{\,\mathsf{ult_membs}(y)\colon y \in X\,\}.
\end{aligned}$$

(The latter is an alternative, more straightforward characterization of the transitive closure operation introduced above).

Other useful notions definable recursively (their rationale being regularity again) are the following, where F and F' are restrained to be hereditarily finite sets:

$$\begin{array}{lll} A_{\mathbb{N}}(F) & =_{\text{Def}} & \sum_{h\in F} 2^{A_{\mathbb{N}}(h)}, \\ F \lhd F' & \Leftrightarrow_{\text{Def}} & F \subsetneq F' \vee \big(F' \not\subseteq F \;\&\; \max_{\lhd}(F \setminus F') \lhd \max_{\lhd}(F' \setminus F)\big). \end{array}$$

The former is a noticeable bijection, discovered by Wilhelm Ackermann [1], between the hereditarily finite sets and $\mathbb{N}$; the latter is a strict ('anti-lexicographic') ordering over the hereditarily finite sets, which is isomorphic to the standard ordering of $\mathbb{N}$ (actually, $F \lhd F' \Leftrightarrow A_{\mathbb{N}}(F) < A_{\mathbb{N}}(F')$ holds when $\mathsf{HF}(F)$, $\mathsf{HF}(F')$).[7]

In spite of its appeal, regularity is not universally adopted. As we are about to see, in Peter Aczel's recent theory of *non-well-founded sets* [2], the regularity axiom gets replaced by an axiom quite opposite in flavor.

3. Ill-Foundedness

> I came to learn that the notion of a concurrent process was a good deal more complex and subtle than I had thought when I first started to think about the notion and its relationship to non-well-founded sets. Robin Milner's work on SCCS was the direct cause for my original interest in non-well-founded sets.
>
> *Peter Aczel (1987)*

Think of a graph $\mathcal{G} = (V, E)$ as of a (possibly infinite) system of equations, that must be solved by an assignment $v \mapsto \dot{v}$ of sets to its nodes so as to satisfy the condition

$$\dot{v} \;=\; \{\, \dot{u} \colon u \in v^{\curvearrowright} \,\}$$

(i.e., $\dot{v} = \{\, \dot{u} \colon u \in V \,\&\, v\, E\, u \,\}$), for all $v \in V$. Such an assignment will be called a DECORATION of $\mathcal{G}$. When does a decoration exist? When is it unique?

---

[7] The following slick, but somewhat cryptic, recursive definition of $\lhd$ over *all* sets was given and explained in [6]:

$$\begin{array}{lll} P \,\partial\, Q & =_{\text{Def}} & \Big\{ v \colon v \in P \,\&\, Q \supseteq \{\, w \colon w \in P \,\&\, v \lhd w \}\Big\} \setminus Q\,, \\ X \lhd Y & \Leftrightarrow_{\text{Def}} & \Big((X \cup Y) \,\partial\, (X \cap Y)\Big) \cap Y \neq \emptyset\,. \end{array}$$

The restriction of this $\lhd$ to HF yields the same well-ordering defined above; but in its enlarged version the relation $\lhd$ ceases to be an ordering.

Trivially, the identity function $v \mapsto v$ is a 1-1 decoration in the special case when $\mathcal{G} = (\mathsf{trCl}(\upsilon), \ni_\upsilon)$ for some υ, so let us begin by examining this simple case first. According to the tradition of ZF, which combines the EXTENSIONALITY axiom

$$\textbf{(E)} \quad \forall\, x\, \forall\, y\, \big(\, x \neq y \Longrightarrow \exists\, d\, (\, d \in x \Leftrightarrow d \notin y\,)\,\big)$$

with the above-discussed regularity axiom **(R)**, this graph is

extensional: No two nodes have the same children.

well founded: There are no infinite paths; and, consequently, no cycles.

The following proposition, which we recall without proof, states a sort of converse of the facts just observed:

THEOREM 2 (Mostowski's collapsing lemma). *According to ZF, a graph admits a decoration if and only if it is devoid of infinite paths. The decoration, when it exists, is unique; and then it is 1-1 if and only if the graph is extensional.*

In a variant of ZF sometimes named HYPERSET theory [4], a postulate antithetic to regularity, named the ANTI-FOUNDATION AXIOM [2, 5], states that in a richer universe of 'sets'

$$\textbf{(AFA)} \qquad \begin{array}{c} \textit{Every graph has a decoration...} \\ \textit{...which is ever unique.} \end{array}$$

Here the graph can have infinite paths, cycles, or even loops $\langle x, x\rangle \in E$.

Throughout, we will use the word SET without committing ourselves to the classical well-founded view; but whenever we will classify a set s as being a HYPERSET we will be referring to a universe complying with AFA and we will understand that membership restricted to the transitive closure $\mathsf{trCl}(s)$ of s has at least one *infinite descending chain* $x_0 \ni x_1 \ni x_2 \ni \cdots$.

Before adopting **(AFA)** as an axiom, one withdraws **(R)** and **(E)** for opposite reasons: the novel axiom consists, in fact, of an *existence* claim (antifoundation proper) which often conflicts with **(R)**, and a *uniqueness* claim, which can be shown to yield **(E)** as a consequence (this is why the uniqueness claim was named *hyperextensionality* in [21]).

To grasp in what sense AFA boosts extensionality, consider the graphs

$$\mathcal{G}_0 = (\{v_0\}, \{\langle v_0, v_0\rangle\}), \quad \mathcal{G}_1 = (\{v_1, v_2\}, \{\langle v_1, v_2\rangle\, , \langle v_2, v_1\rangle\}),$$

with v_1, v_2 distinct nodes. Note that if Ω is the set assigned to v_0 in the decoration of $\mathcal{G}_0$, then the assignment $v_1 \mapsto \Omega, v_2 \mapsto \Omega$ meets the requirements

for being a decoration, hence it is *the* decoration, of $\mathcal{G}_1$;[8] thus the sentence

$$\forall v_1 \forall v_2 \, (v_1 = \{v_2\} \,\&\, v_2 = \{v_1\} \Longrightarrow v_1 = v_2 \,)$$

— which **(E)** does not pronounce about—is provable under AFA.

Now the question arises: how can one establish whether two nodes of a graph $\mathcal{G}$ designate the same set or different sets in the decoration of $\mathcal{G}$? Seeking an answer to this (cf. [13, 2]) is one among several rationales for bringing the notion of *bisimilarity* onto the scene, as we will soon do.

3.1. Anti-Foundation as a Sentence

How can one be more formal in stating AFA? Expressing it as a first-order sentence is easier if we allow us to use the syntactic device of *setformers*: these are not a native construct of predicate calculus, but they can be introduced as a conservative extension in any suitably rich set theory. Curiously, Aczel does not propose a sentence for AFA, as we do here:

$$\forall v \forall e \exists ! f \;\big(f = \big\{ \big\langle x, \{\zeta \colon y \in v \,,\; \langle y, \zeta\rangle \in f \,\&\, \langle x, y\rangle \in e \,\}\big\rangle \colon x \in v \,\big\}\big) \,.$$

By expanding here the quantifier $\exists ! f$ according to its defining macro, we get

$$\forall v \forall e \exists g \forall f \;\big(f = g \Leftrightarrow f = \big\{\big\langle x, \{\zeta \colon y \in v,\; \langle y, \zeta\rangle \in f \,\&\, \langle x, y\rangle \in e \,\}\big\rangle \colon x \in v \,\big\}\big) \,,$$

whose implication '$\Longrightarrow$' corresponds to antifoundation proper, whereas the implication of opposite orientation corresponds to (hyper)extensionality.

4. Bisimulations and Bisimilarity, after Aczel

Stability of a relation over a system is sometimes defined as follows:

Definition 4.1. *A* symmetric *dyadic relation* $\flat$ *between the nodes of a system* $\mathcal{M} = (V, E)$ *is said to be* stable *over* $\mathcal{M}$ *if* $u \flat u'$ *always implies that*

every child of u' *is related by* $\flat$ *to some child of* u*:*

$$\forall v' \in u'^{\uparrow} \;\; \exists v \in u^{\uparrow} \;\; v \flat v' \,.$$

Here $y \in x^{\uparrow}$ indicates, as usual, that $x \mathcal{M} y$; or, more precisely, that $\langle x, y\rangle$ is an edge of $\mathcal{M}$. In full, this definition of stability could be formulated as follows (see Fig. 3):

$$\mathsf{Is\_stable}(\flat, \mathcal{M}) \;\Leftrightarrow_{\text{Def}} \forall u, u', v' \big(u \flat u' \,\&\, u' E v' \;\Longrightarrow\; \exists v (u E v \,\&\, v \flat v')\big),$$

leaving it as understood here that $\flat \subseteq V \times V$.

---

[8] This argument generalizes to any graph each of whose nodes has some outgoing edges: the decoration of such a graph must send every node to Ω.

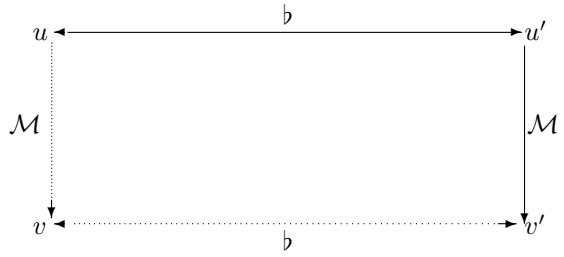

Figure 3: Diagram depicting the property of $\flat$ being stable relative to $\mathcal{M}$

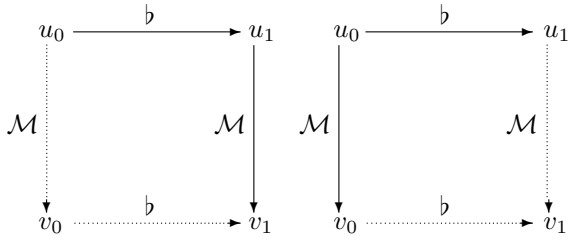

Figure 4: Diagram depicting the properties of a bisimulation $\flat$ on $\mathcal{M}$

The following is the definition of *bisimulation* proposed by Aczel, who instead of insisting (as many authors do) that a relation of this kind must be symmetric prefers to split the stability requirement into two conditions:

DEFINITION 4.2. *A dyadic relation $\flat$ between the nodes of a system $\mathcal{M}$ is said to be a* BISIMULATION *on $\mathcal{M}$ if $u_0 \flat u_1$ always implies that*

$$\&_{j=0}^{1}\, \forall\, v_j \in u_j{}^{\curvearrowright}\ \exists\, v_{1-j} \in u_{1-j}{}^{\curvearrowright}\ \ v_0 \flat v_1\,, \quad \textit{i.e.:}$$

- *for every child v_1 of u_1, u_0 has at least one child v_0 such that $v_0 \flat v_1$, and*
- *for every child v_0 of u_0, u_1 has at least one child v_1 such that $v_0 \flat v_1$.*

In full, this notion could be formulated as follows (see Fig. 4):

$$\begin{aligned}\mathsf{Is\_bisim}(\flat, \mathcal{M}) \ \Leftrightarrow_{\text{Def}} \forall\, u_0, u_1 \Big(& u_0 \flat u_1 \implies \\ & \&_{j=0}^{1}\ \big(\forall\, v_j\, (u_j \mathcal{M} v_j \implies (\exists\, v_{1-j} (u_{1-j} \mathcal{M} v_{1-j}\ \&\ v_0 \flat v_1))\big)\Big).\end{aligned}$$

Here are short specifications—independent of one another—in the map calculus [25, 12] of the properties of symmetry, transitivity, stability, and bisimulation:

symmetry: $\flat = \flat^{-1}$;

transitivity: $\flat \circ \flat = \flat$;

stability: $\flat \circ E \subseteq E \circ \flat$;

bisimulation: $\flat \circ E \subseteq E \circ \flat, \quad E^{-1} \circ \flat \subseteq \flat \circ E^{-1}$.

Remarkably, when it makes sense to speak of *the symmetric-transitive-reflexive closure* $\flat^*$ *of a bisimulation* $\flat$—e.g., because $\flat$ is small—, this *turns out to be a bisimulation.* (As we will not need this fact, we omit its proof.)

The rest of this section is devoted to Aczel's proof that there is an inclusion-maximal bisimulation $\equiv_{\mathcal{M}}$ on any system $\mathcal{M}$ and that this is an equivalence relation: hence, the partition it induces over the nodes of $\mathcal{M}$ will be the *coarsest* of all partitions induced by equivalence bisimulations.

Definition 4.3. Bisimilarity *is the dyadic relation* $\equiv_{\mathcal{M}}$ *defined over* $\mathcal{M}$ *as follows: for all nodes* u, v*,*

$$u \equiv_{\mathcal{M}} v \;\Leftrightarrow_{Def} u \flat v \text{ holds for some small bisimulation } \flat$$

('small' meaning here, as usual, that $\flat$ *must be a set, not a proper class, of pairs of nodes).*

Theorem 3 (Bisimilarity, 1). *1.* $\equiv_{\mathcal{M}}$ *is a bisimulation on* $\mathcal{M}$*;*

2. $\equiv_{\mathcal{M}}$ *includes every bisimulation on* $\mathcal{M}$*.*

Proof. As regards 1., observe that when $u \equiv_{\mathcal{M}} u'$ and $u' \mathcal{M} v'$: $u \flat u'$ holds for some small bisimulation $\flat$, hence there is a v such that $u \mathcal{M} v \flat v'$, and hence $v \equiv_{\mathcal{M}} v'$. This ensures the stability of $\equiv_{\mathcal{M}}$ over $\mathcal{M}$. To treat the opposite side, one argues analogously.

As regards 2., assuming that β is a bisimulation on $\mathcal{M}$ and that $u \beta v$ holds, observe that $\flat = \beta \cap (\mathcal{M}_u \times \mathcal{M}_v)$ is a small bisimulation such that $u \flat v$ holds, and therefore $u \equiv_{\mathcal{M}} v$. Hence $\beta \subseteq \equiv_{\mathcal{M}}$. □

Theorem 4 (Bisimilarity, 2). *Bisimilarity is an equivalence relation over* V*. The relation that holds between two nodes* u, v *when their apgs* $\mathcal{M}_u, \mathcal{M}_v$ *are isomorphic is a refinement of bisimilarity.*

Proof. To see reflexivity, notice that every relation of the form $\{\langle u, u \rangle\}$, with u a node, is a small bisimulation. Symmetry is also very easily checked: when $u \flat v$ holds for a small bisimulation $\flat$, then $v \flat^{-1} u$ holds, where the converse $\flat^{-1}$ of $\flat$ plainly is a small bisimulation. Transitivity is also straightforward, because when $u \flat v$ and $v \flat' w$ hold for small bisimulations $\flat, \flat'$, then $u \flat \circ \flat' w$ holds, where the composition $\flat \circ \flat'$ plainly is a small bisimulation.

Suppose next that an isomorphism $\flat\colon \mathcal{M}_u \longrightarrow \mathcal{M}_v$ exists. To see that then $u{\equiv_{\mathcal{M}}}v$ holds, it suffices to observe that $\flat$ is a bisimulation: actually a small one, insofar as it is included in the Cartesian product $T_\infty(u) \times T_\infty(v)$ of two sets; moreover, it obviously meets the properties depicted in Fig. 4. □

A variant notion of bisimilarity, for which analogs of the above two theorems hold, can be associated with any triple $S, \Re, \simeq$ such that $\Re \subseteq \mathscr{P}(S \times S)$ and $\simeq$ is an equivalence relation over S. In this case we define BISIMILARITY to be the relation

$$\equiv_{S,\Re,\simeq} \quad =_{\mathrm{Def}} \quad \bigcup \Big\{ \flat\colon \flat \subseteq \simeq \ \&\quad \flat \text{ is a bisimulation on each graph } (S,R) \text{ with } R \in \Re \Big\},$$

so that the following propositions hold:

- $\equiv_{S,\Re,\simeq}$ is a bisimulation on every graph (S, R) with $R \in \Re$, and the largest among such simultaneous bisimulations;
- $\equiv_{S,\Re,\simeq}$ is an equivalence relation over S, refining $\simeq$;
- $\equiv_{S,\Re,\simeq}$ is refined by the equivalence relation that holds between two nodes u, v when the apgs $\mathcal{M}_u, \mathcal{M}_v$ are isomorphic for all $\mathcal{M} = (S, R)$ with $R \in \Re$.

REMARK 4.4. *Even though Aczel's hyperset universe is richer than the von Neumann cumulative hierarchy, the two do not differ in a crucial point. They both meet (hyper)*extensionality *in the following form of 'parsimony' criterion:*[9]

$$u \equiv_{\mathcal{U}} v \Longrightarrow u = v$$

(where $\mathcal{U}$ is richer or poorer, respectively), so they are on a par in complying with Occam's razor principle that

entia non sunt multiplicanda praeter necessitatem.

4.1. A Superlarge Category

System maps generalize the notion of decoration introduced in Sec. 3:

DEFINITION 4.5. *A* SYSTEM MAP

$$\dot{}\colon \mathcal{M} \longrightarrow \mathcal{M}'$$

[9] We omit the proof of this fact, about which the reader can refer to [2, pp. 19–22].

between two systems $\mathcal{M} = (V, E)$ *and* $\mathcal{M}' = (V', E')$ *is a mapping* $\dot{} : V \longrightarrow V'$ *that meets the condition*

$$\dot{v}\vec{\ }' \quad = \quad \{\, \dot{u} : u \in v\vec{\ } \,\}$$

(i.e., $\{\, w : w \in V' \,\&\, \dot{v}\, E'\, w\} = \{\, \dot{u} : u \in V \,\&\, v\, E\, u \,\}$*), for all* $v \in V$*.*

About these, Aczel [2, p. 24] proves that

THEOREM 5. *When*

$$\dot{} : \mathcal{M} \longrightarrow \mathcal{M}' \quad \textit{and} \quad \ddot{} : \mathcal{M} \longrightarrow \mathcal{M}'$$

are system maps*, the following hold:*

- *if* $\flat$ *is a bisimulation on* $\mathcal{M}$ *then* $\{\, \langle \dot{u}, \ddot{v} \rangle : \dot{u} \in V' \,\&\, \ddot{v} \in V' \,\&\, u \flat v \,\}$ *is a bisimulation on* $\mathcal{M}'$*;*
- *if* $\flat'$ *is a bisimulation on* $\mathcal{M}'$*, then* $\{\, \langle u, v \rangle : u \in V \,\&\, v \in V \,\&\, \dot{u} \flat' \ddot{v} \,\}$ *is a bisimulation on* $\mathcal{M}$*.* □

It should be clear that a *decoration* of $\mathcal{M}$ simply is a system map between $\mathcal{M}$ and the set system $\mathcal{U}$.

5. Hereditarily Finite Sets

In the framework of hyperset theory, we can no longer define hereditarily finite sets as simply as seen in Sec. 2. That notion now splits into three: the old *well-founded* hereditarily finite sets, which are

$$\begin{array}{lll} \mathsf{HF}(F) & \Leftrightarrow_{\text{Def}} & \mathsf{Is\_finite}(\mathsf{trCl}(F)) \,\& \\ & & \forall\, w \subseteq \mathsf{trCl}(F)\ (\, w \neq \emptyset \Longrightarrow \exists\, m \in w \ \ m \cap w = \emptyset\,), \end{array}$$

and two ill-founded variants of it:

$$\begin{array}{lll} \overline{\mathsf{HF}}(F) & \Leftrightarrow_{\text{Def}} & \mathsf{Is\_finite}(\mathsf{trCl}(F)), \\ \overline{\overline{\mathsf{HF}}}(F) & \Leftrightarrow_{\text{Def}} & \forall\, y \in \mathsf{trCl}(\{F\})\ \ \mathsf{Is\_finite}(y). \end{array}$$

The sets captured by the new definition of $\mathsf{HF}(\cdot)$ do not differ from those captured by our previous definition. The crucial part of the argument that shows this goes as follows:

> Let F be hereditarily finite in the old sense, so that $\mathsf{trCl}(F)$ is well-founded. Consider the irredundant representation of F by means of an apg devoid of distinct bisimilar nodes. This directed acyclic graph has finitely many edges issuing from each node; moreover, it

is devoid of infinite paths. Therefore, by the well-known König's lemma, it is finite. In order to get the irredundant representation of $\mathsf{trCl}(F)$ from the apg of F when $F \neq \mathsf{trCl}(F)$, we simply are to replace the node representing F by a node whose children are all other nodes. Thus the apg of $\mathsf{trCl}(F)$ is finite, and $\mathsf{ls\_finite}(\mathsf{trCl}(F))$ holds.

It is obvious that $\overline{\mathsf{HF}}(F)$ follows from $\mathsf{HF}(F)$ and that $\overline{\overline{\mathsf{HF}}}(F)$ follows from $\overline{\mathsf{HF}}(F)$. To see that $\overline{\mathsf{HF}}$ is actually richer than HF, notice that $\overline{\mathsf{HF}}(\Omega)$ if $\Omega = \{\Omega\}$. Infinitely many hereditarily finite sets exist, as

$$\mathsf{HF}\left(\underbrace{\{\cdots\{\{\emptyset\}\}\cdots\}}_{n}\right)$$

holds for every $n \in \mathbb{N}$; but the sets F satisfying $\overline{\mathsf{HF}}(F)$ are countably many, which is not true of the ones which satisfy $\overline{\overline{\mathsf{HF}}}(F)$. Concerning the number of sets in $\overline{\mathsf{HF}}$, observe that the apg of any X satisfying $\overline{\mathsf{HF}}(X)$ is finite, and there are—to whithin isomorphism, which is a finer equivalence criterion than bisimilarity—countably many such graphs.

To show that $\overline{\overline{\mathsf{HF}}}$ is uncountable, we will now encode every subset x of HF by an e_x such that $\overline{\overline{\mathsf{HF}}}(e_x)$ holds (along with $\neg\overline{\mathsf{HF}}(e_x)$).

We begin with the case when x is infinite, by writing x as

$$x \quad = \quad \{\, h_{i_0}, h_{i_1}, h_{i_2}, \ldots\},$$

where $h_{i_j} \lhd h_{i_{j+1}}$ holds in Ackermann's lexicographic ordering $\lhd$ (cf. Sec. 2), for each $j \in \mathbb{N}$. In this case we take as e_x the value of X_0 in the solution to the infinite system

$$X_0 = \{h_{i_0}, X_1\}, \quad X_1 = \{h_{i_1}, X_2\}, \quad X_2 = \{h_{i_2}, X_3\}, \ldots$$

of equations, easily describable by a graph. When $\bar{x} = \mathsf{HF} \setminus x$ is finite, we encode $\bar{x}$ by the hyperset $e_{\bar{x}}$ that meets the condition $e_{\bar{x}} = \{e_{\bar{x}}, e_x\}$.

6. The Stable Partition Refinement Problem

DEFINITION 6.1. *We say that a set σ'* REFINES *a set σ (and, reciprocally, that σ is* COARSER *than σ') when the following condition is met:*

$$\bigcup\sigma = \bigcup\sigma' \;\&\; \forall\, p \in \sigma'\; \exists!\, q \in \sigma\; p \cap q \neq \emptyset\,.$$

Whatever set π refines itself is called a PARTITION *(of $\bigcup\pi$), and its elements are also called its* blocks.

It is most well known that every partition π induces an equivalence relation

$$\sim_\pi \quad =_{\text{Def}} \quad \{\, \langle u, v\rangle : \exists p\, (p \in \pi \,\&\, u \in p \,\&\, v \in p)\,\}$$

over $\bigcup \pi$; reciprocally, every equivalence relation is induced by the partition

$$\pi_\sim \quad =_{\text{Def}} \quad \big\{\, \{\, y\colon y \in \mathsf{dom}(\sim) \,\&\, x \sim y\,\}\colon x \in \mathsf{dom}(\sim)\,\big\}$$

of its domain.

The following STABLE PARTITION REFINEMENT problem arises in many situations:

- A partition $\pi^\star$ is given;
- a set of graphs (S, R) is also given, all with nodes $S = \bigcup \pi^\star$, their sets of edges R varying over some $\Re \subseteq \mathscr{P}(S \times S)$;
- one must find the coarsest of all partitions π of S (hence the one which has the fewest blocks) that refine $\pi^\star$ and satisfy the condition

  $$\forall\, R \in \Re\, \forall\, q \in \pi\, \forall\, p \in \pi (p \cap R^{-1}[q] \neq \emptyset \implies p \subseteq R^{-1}[q]),$$

  where $R^{-1}[q]$ denotes the PREIMAGE $\{\, v\colon \exists\, w\, (\langle v, w\rangle \in R \,\&\, w \in q)\,\}$.

When this is tackled as an *algorithmic* problem, S (and, consequently, $\bigcup \Re$) is usually finite. Two basic strategies can be followed:

Bottom-up: Start with a partition π consisting of singleton blocks; repeatedly merge two or more blocks until π is as desired. (Cf. [23].)

Top-down: The algorithm maintains a partition π that is initially $\pi^\star$ and gets refined until it is the coarsest stable refinement. (Cf. [22, pp. 977-983].)

6.1. The ur-Example: Venn's Partitioning

With any set $\mathbf{s}$, one associates the following equivalence relation over $\mathcal{U}$:

$$u \sim_{\mathbf{s}} v \quad \Leftrightarrow_{\text{Def}} \quad \{\, x\colon x \in \mathbf{s} \,\&\, u \in x\,\} = \{\, x\colon x \in \mathbf{s} \,\&\, v \in x\,\}.$$

The blocks of the partition induced by $\sim_{\mathbf{s}}$ are the *Venn's regions* associated with $\mathbf{s}$, whose number cannot exceed $2^{|\mathbf{s}|}$. One and only one region fails to be a set, namely the equivalence class formed by whatever lies outside $\bigcup \mathbf{s}$.

Ignoring this big region, observe that the remaining blocks form the partition

$$\Big\{ \bigcap B \setminus \bigcup (\mathbf{s} \setminus B)\colon B \subseteq \mathbf{s} \,\&\, B \neq \emptyset \Big\} \setminus \{\emptyset\},$$

which plainly solves the stable partitioning problem with input

$$\pi^\star = \Big\{ \bigcup \mathbf{s} \Big\} \quad \text{and} \quad \Re = \Big\{ \Big(\bigcup \mathbf{s},\ a \times \bigcup \mathbf{s} \Big) : a \in \mathbf{s} \Big\}.$$

This hence is the coarsest of all partitions π of $\bigcup \mathbf{s}$ that meet the property

$$\forall\, a \in \mathbf{s}\, \forall\, p \in \pi\, (\, p \cap a \neq \emptyset \Longrightarrow p \subseteq a\,)\,.$$

One can see in watermark, in this last formula, the stability condition given in Sec. 4, here referred to all graphs of the form $(\bigcup \mathbf{s}, a \times \bigcup \mathbf{s})$, $a \in \mathbf{s}$, and to a partition π instead of to the corresponding equivalence relation.

More generally, when $\flat$ is an equivalence relation, so that it induces the partition $\pi_\flat$ of its domain, if $\mathcal{G} = (S, R)$ is a graph with $\mathsf{dom}\, \flat \subseteq S$, then plainly the following is equivalent to the condition given in Sec. 4 for the stability of $\flat$ over $\mathcal{G}$:

stability: for all pairs p, q of blocks in $\pi_\flat$,

$$p \cap R^{-1}[q] \neq \emptyset \implies p \subseteq R^{-1}[q].$$

This link with bisimulations clearly points out why *stable partitioning admits a solution in general*. This problem amounts, in fact, to finding the bisimilarity $\equiv_{S,\Re,\sim_\pi}$; whose existence has already been proved

Let us go back to Venn's partitioning. It is not difficult to provide an algorithm that when $\bigcup \mathbf{s}$ is finite solves this problem, on input $\mathbf{s}$, in time and space $\mathcal{O}(|\bigcup \mathbf{s}|)$. It may hence simplify things if, as a step preliminary to the solution of an instance of stable partitioning with input $\pi^\star, \Re$, one performs Venn's partitioning of the set $\mathbf{s} = \pi^\star \cup \{\mathsf{dom}\, R \colon R \in \Re\}$; blocks not intersecting any $\mathsf{dom}\, R$ will, in fact, need no further modification afterwards. In consequence of this remark, requiring that $\pi^\star = \bigcup_{R \in \Re} \mathsf{dom}\, R$ would be an only apparent limitation to the general stable partitioning problem.

6.2. A Paradigmatic Example: DFA State Minimization

Consider a deterministic finite automaton $\mathbb{A} = (\mathcal{A}, \mathcal{Q}, q_0, \mathcal{F}, d)$ over the alphabet $\mathcal{A}$, with states $\mathcal{Q}$, initial state q_0, accepting (or 'final') states $\mathcal{F}$, and transition function d. Moreover, let the d_a's originate from d as said in Sec. 1 (for convenience, assume these to be *total* on $\mathcal{Q}$). Solving the stable partition refinement problem with input

$$\pi^\star = \{\mathcal{F}, \mathcal{Q} \setminus \mathcal{F}\} \quad \text{and } \Re = \{\, d_\mathsf{a} \colon \mathsf{a} \in \mathcal{A}\,\},$$

amounts to *minimizing* the DFA in the sense that if $\pi_\star$ is the resulting coarsest stable partition, then:

PANEL 6.1. **Stable partitioning**

Let π be a partition of S, with $\pi = S/\sim_\pi$. We say that π is *stable*, relative to an $R \subseteq S \times S$, iff $\sim_\pi \circ R \subseteq R \circ \sim_\pi$ holds.
More generally, π is said to be STABLE with respect to

- a $Q \subseteq S$ (relative to a fixed $R \subseteq S \times S$), when
$$\forall\, p \in \pi \quad \emptyset \in \big\{ p \cap R^{-1}[Q],\ p \setminus R^{-1}[Q] \big\}\,;$$
- an $R \subseteq S \times S$, when π is stable with respect to each of its own blocks, relative to R;
- an $\Re \subseteq \mathscr{P}(S \times S)$, when π is stable relative to all $R \in \Re$, i.e.,
$$\forall\, R \in \Re\, \forall\, q \in \pi\, \forall\, p \in \pi\ \big(p \cap R^{-1}[q] \neq \emptyset \implies p \subseteq R^{-1}[q] \big).$$

The STABLE PARTITIONING PROBLEM, in its strongest formulation, is the problem of determining the partition of S that

- is finer than a given partition $\pi^\star$ of S,
- is stable with respect to a given $\Re \subseteq \mathscr{P}(S \times S)$, and
- is the coarsest of all partitions that fulfill the preceding two conditions.

A number of sophisticated algorithms are available today to solve this problem either in full generality (save for the assumption that $|S| < \omega$) or in restricted forms, e.g. under the assumptions that $\Re$ consist of functions and/or that $\Re$ be singleton. A variety of problems can easily be reduced to stable partitioning; e.g., the minimization problem for deterministic finite automata, where $\Re$ consists of functions.

As a special case of stable partitioning, the VENN'S PARTITIONING PROBLEM is the one of determining, given a set $\mathcal{A}$ of sets, the coarsest of all partitions of $S = \bigcup \mathcal{A}$ that are stable with respect to $\Re = \{\, a \times S \,:\, a \in \mathcal{A} \,\}$. One way to see that this problem always admits solution consists of checking directly that
$$\Big\{\ \bigcap B \setminus \bigcup(\mathcal{A} \setminus B) \,:\, B \in \mathscr{P}(\mathcal{A}) \setminus \{\emptyset\}\ \Big\} \setminus \{\emptyset\}$$
is a partition meeting the desired requirements.

One can perform Venn's partitioning of $\mathcal{A} = \pi \cup \{\, \mathsf{dom}\, R_1, \ldots, \mathsf{dom}\, R_n \,\}$ as a step *preliminary to* stable partitioning of $\pi^\star$ and $\Re = \{\, R_1, \ldots, R_n \,\}$, so that blocks not intersecting any $\mathsf{dom}\, R_j$ will need no further modification afterwards. Only the following *multirelational coarsest partition problem* will then remain to be solved: Maps $R_1, \ldots, R_n$ are given, along with a partition π' of $S = \bigcup_{i=1}^{n} \mathsf{dom}\, R_i$; determine the coarsest of all partitions of S that are finer than π' and are stable with respect to $R_1, \ldots, R_n$.

- The DFA $\mathbb{A}' = (\mathcal{A}, \pi_\star, p_0, \mathscr{P}(\mathcal{F}) \cap \pi_\star, d')$, where $q_0 \in p_0 \in \pi_\star$, and $d(q, \mathsf{a}) \in d'(p, \mathsf{a}) \in \pi_\star$ when $q \in p \in \pi_\star$, accepts the same (regular) language as the original $\mathbb{A}$.
- No DFA with fewer states than $\mathbb{A}'$ accepts the same language as $\mathbb{A}$.

(Moreover, two states q_1, q_2 of $\mathbb{A}$ belong to the same block of $\pi_\star$ if and only if the same language is accepted by $(\mathcal{A}, \mathcal{Q}, q_1, \mathcal{F}, d)$ and by $(\mathcal{A}, \mathcal{Q}, q_2, \mathcal{F}, d)$.)

John E. Hopcroft proposed in [16] a top-down algorithm of complexity $\mathcal{O}(|\mathcal{Q}| \log |\mathcal{Q}|)$ for solving this specialized version of the stable partitioning problem (where, among other specificities, $\Re$ consists of functions). A linear-time bottom-up algorithm was then proposed in [23] for the case when $\Re$ consists of a single function[10] (this can hence be used for DFA minimization when $\mathcal{A}$ is singleton). Then Robert Paige and Robert E. Tarjan, in [22] (cf. also [19]), combined the key point "process the smaller half" of Hopcroft's strategy with novel ideas to design an algorithm, running in $\mathcal{O}(|R| \log |S|)$ time and $\mathcal{O}(|R| + |S|)$ space, for the stable partitioning problem with $\Re = \{R\}$. This hence is an upper bound for the complexity of computing bisimilarity on a graph, in general; but when the input graph is acyclic, the problem can be solved by an $\mathcal{O}(|R|)$ algorithm [9], deep-rooted in Ackermann's order of the well-founded hereditarily finite sets.

6.3. Contraction of an NFA

One can exploit stable partition refinement, in a way analogous to its use for DFA minimization, in order to contract a *non-deterministic* finite automaton (in short, an 'NFA') $\mathbb{A} = (\mathcal{A}, \mathcal{Q}, q_0, \mathcal{F}, \delta)$. As customary, this differs from a DFA in that the transitions form a *relation* $\delta \subseteq \mathcal{Q} \times (\mathcal{A} \cup \{\, \epsilon \,\}) \times \mathcal{Q}$, within which in-place transitions of the form $\langle q, \epsilon, q' \rangle$ may occur (cf. [8]).

Non-singleton strongly connected components of the relation

$$\delta_\epsilon \quad = \quad \{\, \langle q, q' \rangle : \langle q, \epsilon, q' \rangle \in \delta \,\},$$

if any, could each be contracted to a single state during a pre-processing phase; hence let us assume without loss of generality that δ_ϵ is acyclic. Likewise, we can and will assume that $q' \,\delta_\epsilon\, q''$ ensues from $q' \,\delta_\epsilon\, q$ and $q \,\delta_\epsilon\, q''$.

To work with an instance of the coarsest stable partition refinement problem in this non-deterministic case, we must start with the partition $\pi^\star = \{\, \mathcal{F} \cup$

[10] In this special case, where $\Re = \{f\}$ and f is a function from the entire S into S, stability amounts to the requirement that $f(b) \in q$ must follow from $\{a, b\} \subseteq p$ and $f(a) \in q$, with p, q blocks. This partitioning problem is treated at length in [3, pp. 157–162], which gives a top-down algorithm for its solution whose running time is $\mathcal{O}(|S| \log |S|)$.

$\delta_\epsilon^{-1}[\mathcal{F}],\ \mathcal{Q} \setminus (\mathcal{F} \cup \delta_\epsilon^{-1}[\mathcal{F}])\,\}$ and with $\Re = \{\,\delta_{\mathsf{a}} : \mathsf{a} \in \mathcal{A}\,\}$, where

$$\delta_{\mathsf{a}} \quad =_{\text{Def}} \quad \{\,\langle q', q''\rangle : q' \in \mathcal{Q}\ \&\ q'' \in \mathcal{Q}\ \&\ \exists\, q\,(q'\ \delta_\epsilon\ q\ \&\ \langle q, \mathsf{a}, q''\rangle \in \delta)\,\},$$

holds for each a.

7. Splitting

> The theme of this paper is partition refinement as an algorithmic paradigm. We consider three problems that can be solved efficiently using a repeated refinement strategy.
>
> *Robert Paige, Robert Tarjan (1987)*

In [22], the following $\mathsf{split}_R(Q, \pi)$ operation is defined, relative to a graph (S, R) such that $Q \subseteq S$ and $\bigcup \pi = S$:

$$\mathsf{split}_R(Q,\pi) \quad =_{\text{Def}} \quad \bigcup\{ \quad \begin{array}{l} \textbf{if } \emptyset \notin \{\,p \cap R^{-1}[Q],\ p \setminus R^{-1}[Q]\,\} \\ \textbf{then } \{\,p \cap R^{-1}[Q],\ p \setminus R^{-1}[Q]\,\} \\ \textbf{else } \{\,p\,\}\ \textbf{fi}\colon\ p \in \pi \end{array} \quad \}.$$

The authors suggest that the following basic refinement step is at the core of top-down stable partitioning:

Split: Replace the current partition π by $\mathsf{split}_R(Q, \pi)$, where $Q \subseteq S$ is a SPLITTER of π, in the sense that $\mathsf{split}_R(Q, \pi) \neq \pi$ and Q is a union of blocks of π.

Leaving R as understood when $R = \ni$, in this case we have in particular:

$$\mathsf{split}(Q,\pi) \quad = \quad \bigcup\Big\{ \quad \begin{array}{l} \textbf{if } \emptyset \notin \{\,\{\,x \in p\ \&\ x \cap Q \neq \emptyset\,\},\ \{\,x \in p\ \&\ x \cap Q = \emptyset\,\}\,\} \\ \textbf{then } \{\,\{\,x \in p\ \&\ x \cap Q \neq \emptyset\,\},\ \{\,x \in p\ \&\ x \cap Q = \emptyset\,\}\,\} \\ \textbf{else } \{\,p\,\}\ \textbf{fi}\colon\ p \in \pi \end{array} \quad \Big\}.$$

EXAMPLE 7.1. *Let* $\bar{\mathcal{H}}_0 = \mathsf{HF}$, $\pi_0 = \{\bar{\mathcal{H}}_0\}$, $R = \ni$, *and*

$$\pi_{i+1} \quad = \quad \mathsf{split}(\bar{\mathcal{H}}_i, \pi_i) \quad = \quad \{\,\mathcal{H}_i', \bar{\mathcal{H}}_{i+1}\,\} \cup (\pi_i \setminus \{\bar{\mathcal{H}}_i\}),$$

for $i = 0, 1, 2, \ldots$. *At the first limit ordinal, we will get the refinement* π_∞ *of* π_0, *not yet a stable partition; nonetheless, something will have been achieved: the* $\mathcal{H}_i'$*s are the subdivision of* HF *into rank-equality classes.*[11]

---

[11] Putting $\mathcal{H}_0 =_{\text{Def}} \emptyset$, and $\mathcal{H}_{i+1} =_{\text{Def}} \mathscr{P}(\mathcal{H}_i)$ for all $i \in \mathbb{N}$, one readily recognizes that $\mathcal{H}_i' = \mathcal{H}_{i+1} \setminus \mathcal{H}_i$ and $\bar{\mathcal{H}}_i = \mathsf{HF} \setminus \mathcal{H}_i$.

Noticeable properties of split_R are (cf. [22]):

- If ϱ refines π (both being partitions), and π is stable with respect to Q, then ϱ is stable with respect to Q.
- If π is stable with respect to Q and to Q', then π is stable with respect to $Q \cup Q'$.
- If ϱ refines π, then $\mathsf{split}_R(Q, \varrho)$ refines $\mathsf{split}_R(Q, \pi)$.
- The following sort of commutative law holds:

$$\mathsf{split}_R(Q, \mathsf{split}_R(Q', \pi)) \quad = \quad \mathsf{split}_R(Q', \mathsf{split}_R(Q, \pi)),$$

  both of whose sides hence denote the coarsest refinement of π which is stable with respect to both Q and Q'.

Here we are calling STABLE with respect to a $Q \subseteq S$ (leaving a fixed graph (S, R) as understood) those partitions π of S that satisfy $\mathsf{split}_R(Q, \pi) = \pi$.

Orthogonally, we can say that a block p, inside π, is UNSTABLE (relative to a graph $(\bigcup \pi, R)$ as above) if π has blocks q for which

$$\emptyset \notin \{\, p \cap R^{-1}[q], p \setminus R^{-1}[q] \,\}$$

holds; if this is the case, we can refine π into $(\pi \setminus \{\, p \,\}) \cup p_R$, where

$$p_R \quad =_{\text{Def}} \quad \big\{\, p \cap r \colon r \text{ is a Venn region associated with } \{\, R^{-1}[q] \colon q \in \pi \,\} \,\big\},$$

i.e., p_R is the quotient of p relative to the equivalence relation

$$u \overset{R}{\sim} v \quad \Leftrightarrow_{\text{Def}} \quad \{\, q \colon q \in \pi \,\&\, u \in R^{-1}[q] \,\} = \{\, q \colon q \in \pi \,\&\, v \in R^{-1}[q] \,\}.$$

EXAMPLE 7.2. *Referring again to $R = \ni$, we can complete the stabilization of the partition treated in our preceding example, by proceeding as follows. Start with $\pi_0^j = \mathcal{H}_j$ for all $j \in \mathbb{N}$. Then, for each $i \in \mathbb{N}$,*

- *determine the first h for which π_i^h is unstable inside $\pi_i = \{\, \pi_i^j : j \in \mathbb{N} \,\}$;*
- *split π_i^h into $\pi_{i+1}^h, \ldots, \pi_{i+1}^{h+m+1}$ by means of the quotient operation relative to $\overset{\ni}{\sim}$, placing the resulting blocks in such an order that the following holds for $h' = h, \ldots, h+m$:*

$$\exists\, k \in \mathbb{N} \,\big(\quad \pi_{i+1}^{h'} \cap \pi_i^k = \emptyset \quad \& \quad \pi_{i+1}^{h'+1} \cap \pi_i^k \neq \emptyset \quad \&$$
$$\forall\, j > k \,(\, \pi_{i+1}^{h'} \cap \pi_i^j = \emptyset \quad \Leftrightarrow \quad \pi_{i+1}^{h'+1} \cap \pi_i^j = \emptyset \,) \quad \big);$$

- *to end, put* $\pi^j_{i+1} = \pi^j_i$ *for* $j < h$, *and put* $\pi^{j+h+m+1}_{i+1} = \pi^j_i$ *for* $j > h$.

The partition π_∞ *of* HF *resulting at the limit will consist of singletons* $\pi^i_\infty = \{\, h_i \,\}$ *ordered* à la *Ackermann, in the sense that* $A_{\mathbb{N}}(h_i) = i$ *holds for each* i.

The construction of this last example has been proposed in [7] recently, along with a suitable analog of it, wich works for the whole of $\overline{\mathsf{HF}}$. Thanks to this extension, a convenient encoding *à la* Ackermann has been found for the sets forming $\overline{\mathsf{HF}}$; the image of the bijection, in this novel encoding, instead of being $\mathbb{N}$, is the set of all rational numbers of the dyadic form $n/2^m$ $(n, m \in \mathbb{N})$.

Appendix: An Axiomatization for Classical ZF

We propose here a first-order axiomatization of the Zermelo-Fraenkel set theory. Our formulation of the axioms (cf. [10]) slightly differs from, but is equivalent to, versions of this theory which can be found in the literature.

(E) $\forall x\, \forall y\, \exists d \big((\, d \in x \Leftrightarrow d \in y\,) \Longrightarrow x = y \big)$

(D) $\forall x\, \forall y\, \exists d \Big(y \in d \,\&\, \forall v \,\big(v = x \Leftrightarrow \exists w\,(v \in w \,\&\, w \in d) \,\&\, \exists \ell\,(v \notin \ell \,\&\, \ell \in d)\,\big)\Big)$

(P) $\forall x\, \exists p\, \forall y \big((\forall v \in y\ v \in x) \Longrightarrow y \in p \big)$

(T) $\forall x\, \exists t\, (\, x \in t \,\&\, \forall v \in y\, \forall y \in v \quad y \in t\,)$

(S) $\forall a\, \exists b\, \forall c \Big(c \in b \Leftrightarrow \exists d \,\big(\forall x\, (\, \varphi[a, x] \Leftrightarrow x = d\,) \,\&\, c \in d \,\&\, \psi[a, c]\,\big)\Big)$

(S′) $\forall a'\, \forall a\, \exists b\, \forall c \,\big(\exists e \in a'\, \exists d\, \forall x\, (\, \chi[e, a, x] \Leftrightarrow x = d\,) \Longrightarrow c \in b \big)$

(I) $\forall x\, \exists i \,\big(x \in i \,\&\, \forall y \in i\, \exists u \in i\, \forall z\, (\, z \in u \Leftrightarrow z = y\,)\,\big)$

(R) $\forall x\, \exists m\, \forall y \ \big(y \in x \Longrightarrow m \in x \,\&\, y \notin m \big)$

(C) $\forall x \,\big(\forall p \in x\, \exists!\, q \in x\, \exists z \in p \ \ z \in q \implies \exists c\, \forall r \in x\, \exists!\, k \in c \ \ k \in r \big)$

Roughly cast in words, this is the content of each postulate:

(E) *Extensionality:* If two sets differ, one has a member not owned by the other.

(D) *Elementary sets:* An empty set exists; one can adjoin any set x as a new member to any set y, thereby getting a set w; one can remove from a set y any one of its members, thereby getting a set ℓ. (Cf. [11].)

(P) *Powerset:* For any set x, there is a set to which all subsets of x belong.

(T) *Transitive closure:* Any set x belongs to a *full* set, namely to a set t whose elements are also subsets of t.

(S) *Subsets:* To every set a, there corresponds a set b which is null unless there is exactly one d fulfilling $\varphi[a, d]$, and which in the latter case consists of all elements c of d for which $\psi[a, c]$ holds.

(S′) *Replacement:* To every pair a, a' of sets there corresponds a set comprising the images, under the functional part of $\chi[e, a, d]$, of all pairs e, a with e belonging to a'.

(I) *Infinity:* For any set x, one can form a set i to which x belongs, owning as a member, along with every y that belongs to it, the singleton set $\{y\}$. (Trivially i is infinite when x is not a singleton).[12]

(R) *Regularity:* Membership is well-founded.

(C) *Choice:* Every set x constituted by non-empty pairwise disjoint sets admits a 'choice' set, i.e., a set c whose intersection with any element of x is singleton.

As we have discussed in Sec. 3, it suffices to replace the pair **(R)**, **(E)** of axioms by **(AFA)** in order to get a hyperset theory closely analogous (but antithetic) to ZF; on the other hand, when **(R)** is available one can simplify **(I)** into

$$\textbf{(I′)} \quad \exists\, x\, \exists\, i\, (\, x \in i \,\&\, \forall\, y \in i\, \exists\, u \in i \;\; y \in u\,).$$

Acknowledgments. This survey results from many discussions which involved: on the one hand, colleagues at the University of Udine, namely Alberto Policriti, Giovanna D'Agostino, and Alexandru Tomescu; on the other hand, many participants to the Vigoni–DAAD project "Theory and applications of bisimulations", in particular Ernst-Erich Doberkat and Christoph Schubert, who contributed with discussions to the maturation of ideas reported in this paper. Thanks are due to the anonymous referee for helpful comments.

References

[1] W. Ackermann, *Die Widerspruchfreiheit der allgemeinen Mengenlehre*, Math. Ann. **114** (1937), 305–315.

[2] P. Aczel, *Non-well-founded sets*, CSLI Lecture Notes volume 14, Stanford University Press, Stanford (1988).

---

[12] The following alternative version of the infinity axiom, which deserves some interest, was proposed in [24]:

$$\exists\, a\, \exists\, b\Big(a \neq b \,\&\, a \notin b \,\&\, b \notin a \,\&\, \forall\, x \in a\, \forall\, y \in b\, (y \in x \vee x \in y) \,\&\, \forall\, x \in a\, \forall\, y \in x\; y \in b \,\&\, \forall\, x \in b\, \forall\, y \in x\; y \in a \,\&\, \forall\, x \in a\; x \notin b\Big).$$

[3] A.V. Aho, J.E. Hopcroft and J.D. Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, New York (1976).
[4] J. Barwise and L. Moss, *Hypersets*, Math. Intelligencer **13** (1991), 31–41.
[5] J. Barwise and L.S. Moss, *Vicious circles*, CSLI Lecture Notes volume 60, Stanford University Press, Stanford (1996).
[6] D. Cantone, C. Chiaruttini, M. Nicolosi Asmundo and E.G. Omodeo, *Cumulative hierarchies and computability over universes of sets*, Le Matematiche **63** (2008), 31–84.
[7] G. D'Agostino, E.G. Omodeo, A. Policriti and A.I. Tomescu, *Mapping hypersets into numbers*, in preparation (2010).
[8] M. D. Davis, R. Sigal and E.J. Weyuker, *Computability, complexity, and languages: Fundamentals of theoretical computer science*, 2nd edition, Academic Press, New York (1994).
[9] A. Dovier, C. Piazza and A. Policriti, *An efficient algorithm for computing bisimulation equivalence*, Theoret. Comput. Sci. **311** (2004), 221–256.
[10] A. Formisano and E. . Omodeo, *An equational re-engineering of set theories*, LNCS volume 1761, Springer, Berlin (2000), 175–190.
[11] A. Formisano, E.G. Omodeo and A. Policriti, *Three-variable statements of set-pairing*, Theoret. Comput. Sci. **322** (2004), 147–173.
[12] A. Formisano, E.G. Omodeo and M. Temperini, *Goals and benchmarks for automated map reasoning*, J. Symb. Comput. **29** (2000), 259–297.
[13] M. Forti and F. Honsell, *Set theory with free construction principles*, Annali Scuola Normale Superiore di Pisa, Classe di Scienze **IV** (1983), 493–522.
[14] R. Gentilini, C. Piazza and A. Policriti, *From bisimulation to simulation: Coarsest partition problems*, J. Automat. Reason. **31** (2003), 73–103.
[15] J. van Heijenoort, *From Frege to Gödel — A source book in mathematical logic,* 1879–1931, 3rd edition, Harvard University Press, Hervard (1977).
[16] J. E. Hopcroft, *An $n \log n$ algorithm for minimizing states in a finite automaton*, in Z. Kohavi and A. Paz, *Theory of machines and computations*, Academic Press, New York (1971), 189–196.
[17] P.C. Kanellakis and S.A. Smolka, *CCS expressions, finite state processes, and three problems of equivalence*, in the proceedings of *ACM Symposium on Principles of Distributed Computing*, (1983), 228–240.
[18] P.C. Kanellakis and S.A. Smolka, *CCS expressions, finite state processes, and three problems of equivalence*, Inform. and Comput. **86** (1990), 43–68.
[19] J.-P. Keller and R. Paige, *Program derivation with verified transformations — A case study*, Comm. Pure Appl. Math. **48** (1995), 1053–1113.
[20] R. Milner, *A calculus of communicating systems*, LNCS volume 92, Springer, Berlin (1980).
[21] E.G. Omodeo and A. Policriti, *Solvable set/hyperset contexts: I. Some decision procedures for the pure, finite case*, Comm. Pure Appl. Math. **48** (1995), 1123–1155.
[22] R. Paige and R.E. Tarjan, *Three partition refinement algorithms*, SIAM J. Comput. **16** (1987), 973–989.
[23] R. Paige, R.E. Tarjan and R. Bonic, *A linear time solution to the single function coarsest partition problem*, Theoret. Comput. Sci. **40** (1985), 67–84.

[24] F. Parlamento and A. Policriti, *The logically simplest form of the infinity axiom*, Proc. Amer. Math. Soc. **103** (1988), 274–276.
[25] A. Tarski and S. Givant, *A formalization of set theory without variables*, Colloquium Publications volume 41, American Mathematical Society, Providence (1987).
[26] J. von Neumann, *Eine Axiomatisierung der Mengenlehre*, J. Reine Angew. Math. **154** (1925), 219–240; reprinted also in [28, 34–56].
[27] J. von Neumann, *Über eine Widerspruchsfreiheitsfrage in der axiomatischen Mengenlehre*, J. Reine Angew. Math. **160** (1929), 227–241; reprinted also in [28, 494–508].
[28] J. von Neumann, *Collected works* vol. I*: Logic, theory of sets and quantum mechanics*, Pergamon Press, New York (1961).
[29] E. Zermelo, *Untersuchungen über die Grundlagen der Mengenlehre I*, Math. Ann. **65** (1908), 261–281; reprinted also in [15, 199–215].

Author's address:

Eugenio G. Omodeo
Dipartimento di Matematica e Informatica
Università degli Studi di Trieste
Via Valerio, 12/1, 34127 Trieste, Italy
E-mail: eomodeo@units.it

Received September 15, 2010
Revised October 30, 2010