THE DECIDABILITY OF THE BERNAYS-SCHÖNFINKEL-RAMSEY CLASS FOR SET THEORY

EUGENIO OMODEO AND ALBERTO POLICRITI

ABSTRACT. As is well-known, the Bernays-Schönfinkel-Ramsey class of all prenex $\exists^*\forall^*$-sentences which are provable in first-order predicate calculus is decidable. This paper shows that an analogous result holds when the only available predicate symbols are $\in$ and $=$, no constants or function symbols are available, and one moves inside a (rather generic) set theory whose axioms yield the well-foundedness of membership.

Key words: Satisfiability decision algorithms, extended multilevel syllogistics, computable set theory.

INTRODUCTION

In this paper we prove the decidability of the satisfiability problem for the celebrated *Bernays-Schönfinkel-Ramsey class (BSR-class)* in a (rather generic) set-theoretic context. The BSR-class has a history for inspiring interesting and deep combinatorial problems and results—Ramsey theorem above all, see [Ram28]—and the set theoretic context in which we are tackling the problem provides a further case in which a non-trivial (infinitary) combinatorial treatment turns out to be necessary to prove its decidability.

Definition 1. A prenex sentence Φ belongs to the BERNAYS-SCHÖNFINKEL-RAMSEY CLASS (BSR-CLASS) if its quantificational prefix has the form $\exists^*\forall^*$.

An open formula $\varphi(x_1, \ldots, x_n)$ all of whose quantifiers are grouped at the beginning belongs to the BSR-CLASS if its quantificational prefix has the form $\forall^*$.[1] $\square$

The reader is referred to [BGG97, DG79, Lew79] for basic notions on the taxonomy of quantificational classes and key results on the Classical Decision Problem.

The basic language we consider contains equality and one binary relational symbol $\in$ to be interpreted as the *membership* relation. The set-theoretic satisfiability issue we will consider concerns the existence of an algorithmic procedure which can establish, given a formula $\varphi(x_1, \ldots, x_n)$ in the BSR-class, whether or not there are n sets satisfying φ in the *standard* (von Neumann) universe of sets $\mathbb{V}$, namely the class inductively defined on all ordinals by the recursion

$$\mathbf{V}_\alpha \quad = \quad \bigcup_{\beta<\alpha} \mathscr{P}(\mathbf{V}_\beta) \quad ,$$

where $\mathscr{P}(\cdot)$ designates the power-set operation and α, β range over ordinals.

Date: January 27th, 2008. This research has been partially funded by PRIN project 2006/2007 *'Large-scale development of certified mathematical proofs'*.

[1] Occasionally, e.g. when speaking of *restricted* BSR-formulae, we will slightly abuse terminology and ascribe to the BSR-class also formulae which are trivially equivalent to formulae in the BSR-class proper, as can be shown by elementary syntactic transformations.

Our answer to the said decision problem will be affirmative: actually, we will single out a specific algorithm solving the satisfiability problem addressed above. Related result were presented in [OPP93], which treated a decision algorithm for the subclass $\exists^*\forall$ (with only one universal quantifier) of the BSR-class, and in [BP06], which solved the decision problem for the subclass $\exists^*\forall\forall$ (with two universals).

With our novel approach, decidability will ensue from the following observations:

- Within the BSR-class, we can associate with any formula φ an equi-satisfiable formula φ' whose quantifiers are of the restricted form $\forall\, y \in z$.
- This restricted form of quantification enables one, when the set values for the free variables of φ' are drawn from a family $\mathcal{F}$, to evaluate φ' within a confined domain of discourse: the *transitive closure* (see below) T of $\mathcal{F}$.
- There is a subset W of T which retains enough of the structure of T to enable one to determine the truth value of φ' in $\mathcal{F}$; despite not being finite in general, this W can be adequately *represented* by a finite data structure.
- Indicating by ν the overall number of distinct variables in φ, we can set a computable bound $f(\nu)$ on the size of the finite representation of W. Indirectly, this sets a bound on the amount of time needed to explore the search space within which a "witness" W of the satisfiability of φ' can lie.

As will emerge from the ongoing, although we have cast it in semantic terms, our decision problem could easily be referred to the classical axiomatic theory of sets ZF, or to a weaker theory postulating among others the existence of infinite sets and the well-foundedness of membership.

1. Basics and Preliminary Results

We begin with a few simple notions (the reader can refer to [Lev79] for a more detailed treatment) and basic results.

Throughout, we will assume the membership relation $\in$ to be *well-founded* on the class $\mathbb{V}$ of all sets (i.e., any non-empty subset of $\mathbb{V}$ has a $\in$-minimal element) and we introduce the usual notion of *rank* as follows:

Definition 2. The RANK function rk, taking values on the ordinal numbers, is recursively defined over $\mathbb{V}$ as follows:

$$\mathsf{rk}(x) \quad = \quad sup\{\mathsf{rk}(y)+1 : y \in x\}.$$

In $\mathbb{V}$ the only element of rank 0 is $\emptyset$ and a set is said to be HEREDITARILY FINITE whenever its rank is a natural number. We often use the abbreviation

$$x^{\Re\alpha} = \{\, y \in x \mid \mathsf{rk}(x)\Re\alpha \,\},$$

where x is a set, α is an ordinal, and $\Re$ is a binary relation: thus, e.g.,

$$x^{>\alpha} = \{\, y \in x \mid \mathsf{rk}(x) > \alpha \,\},\ x^{<\alpha} = x \cap \mathbf{V}_\alpha, \text{ and } x^{\geqslant\alpha} = x \setminus \mathbf{V}_\alpha.$$

Definition 3. Given a set $\mathbf{v}$, we denote by $\mathsf{TrCl}(\mathbf{v})$ the TRANSITIVE CLOSURE of $\mathbf{v}$, defined through the recursion

$$\mathsf{TrCl}(\mathbf{v}) \quad = \quad \mathbf{v} \cup \bigcup_{\mathbf{u}\in\mathbf{v}} \mathsf{TrCl}(\mathbf{u}).$$

Definition 4. Given an acyclic graph $G = \langle V, E\rangle$, we define the MOSTOWSKI COLLAPSE OF G to be the family $\mathbf{M}(G)$ of sets defined as

$$\mathbf{M}(v, G) \quad = \quad \{\mathbf{M}(u, G) : \langle v, u\rangle \in E\}.$$

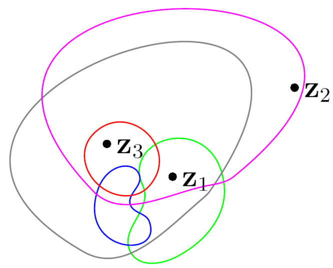

FIGURE 1. A minimal differentiating set of three elements for a family $\mathcal{F}$ of five sets.

Moreover, given $Z \subseteq V$, we define the MOSTOWSKI COLLAPSE OF G WITH PARAMETER Z to be the family $\mathbf{M}(G;Z)$ of sets defined as

$$\mathbf{M}(v,G;Z) \quad = \quad \begin{cases} \{\mathbf{M}(u,G;Z) : \langle v,u\rangle \in E\}; & \text{if } v \notin Z \\ \mathbf{A}_Z(v) & \text{if } v \in Z, \end{cases}$$

where $\mathbf{A}_Z$ is an arbitrary bijection between Z and a set none of whose elements comes to equal any $\mathbf{M}(v,G;Z)$—this can be achieved simply by requiring that all images of $\mathbf{A}_Z$ have rank $|V|+1$. □

When using the above definition we will omit the parameter G in the notation whenever this is clear from the context.

Definition 5. Given a set $\mathbf{V}$, we denote by $G_{\mathbf{V}}$ the graph $\langle \mathbf{V}, E_{\mathbf{V}}\rangle$ whose nodes are the elements of $\mathbf{V}$ and whose edge relation is the inverse of membership. □

Let $\mathcal{F}$ be a finite family of sets. Given $\mathbf{z} \in \bigcup\mathcal{F}$, we denote by $\mathcal{F}(\mathbf{z})$ the set $\{\mathbf{v} \setminus \{\mathbf{z}\} \mid \mathbf{v} \in \mathcal{F}\}$.

Definition 6. A $\mathbf{z} \in \bigcup\mathcal{F}$ is said to be REDUNDANT if $|\mathcal{F}| = |\mathcal{F}(\mathbf{z})|$. We say that $\mathcal{F}$ is IRREDUNDANT if no element of $\bigcup\mathcal{F}$ is redundant. □

If $\mathcal{F}$ is irredundant then $\bigcup\mathcal{F}$ is also called a *minimal differentiating set for $\mathcal{F}$* (see Fig. 1). What is important for our combinatorial problem, is the size of such a minimal differentiating set as well as technique to determine it. The following lemma and its proof (see also [PPR97, Bol86]) give us indications on those two issues.

Lemma 1.1 (**Discrimination lemma).** *Given an n-element nonempty family $\mathcal{F} = \{\mathbf{v}_1,\dots,\mathbf{v}_n\}$, we can determine $\mathbf{z}_1,\dots,\mathbf{z}_k \in \bigcup\mathcal{F}$, with $k \leqslant n-1$, so that the family*

$$\{\mathbf{v}_i \cap \{\mathbf{z}_1,\dots,\mathbf{z}_k\} \mid \mathbf{v}_i \in \mathcal{F}\}$$

is irredundant and has cardinality n.

Proof. By induction on n, where the case $n=1$ is trivial. As for the inductive step, assume a minimal differentiating set $\{\mathbf{z}_1,\dots,\mathbf{z}_{k'}\} \subseteq \bigcup\{\mathbf{v}_1,\dots,\mathbf{v}_{n-1}\}$ has already been determined. To conclude it is sufficient to observe that either $\{\mathbf{v}_i \cap$

$\{\mathbf{z}_1, \ldots, \mathbf{z}_{k'}\} \mid \mathbf{v}_i \in \mathcal{F}\}$ is irredundant—and we are done—or, for a unique $i \in \{1, \ldots, n-1\}$, we have:

$$\mathbf{v}_i \cap \{\mathbf{z}_1, \ldots \mathbf{z}_{k'}\} \quad = \quad \mathbf{v}_n \cap \{\mathbf{z}_1, \ldots \mathbf{z}_{k'}\}.$$

In the latter case just one element needs to be added to $\{\mathbf{z}_1, \ldots \mathbf{z}_{k'}\}$ in order to obtain a minimal differentiating set for $\mathcal{F}$. $\square$

A useful variant of the above lemma is stated below.

Lemma 1.2 (**Élite discrimination lemma**). *Given an n-element family $\mathcal{F} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, such that $\mathsf{rk}(\mathcal{F}) - 1 = \varrho + 1$ for some ordinal ρ (i.e., the maximum rank of an element of $\mathcal{F}$ is a successor ordinal), we can determine $\mathbf{z}_1, \ldots, \mathbf{z}_k \in \bigcup \mathcal{F}$, with $k \leqslant n$, so that the family*

$$\{\mathbf{v}_i \cap \{\mathbf{z}_1, \ldots, \mathbf{z}_k\} \mid \mathbf{v}_i \in \mathcal{F}\}$$

has cardinality n and, for every $i \in \{1, \ldots, n\}$,

$$\mathsf{rk}(\mathbf{v}_i) = \varrho + 1 \quad \textit{implies} \quad \mathsf{rk}(\mathbf{v}_i \cap \{\mathbf{z}_1, \ldots, \mathbf{z}_k\}) = \varrho + 1.$$

Proof. The proof proceeds by induction on the number $m = |\{v \in \mathcal{F} \mid \mathsf{rk}(v) = \varrho + 1\}|$ of sets of maximum rank in $\mathcal{F}$. We will assume in the ongoing that $z \in w \in \mathcal{F}$ and $\mathsf{rk}(z) = \rho$. Observe that the claim of this theorem trivially holds when $m = n = 1$ (just take $k = 1$ and $\mathbf{z}_1 = z$); if this is not the case, then we can determine $\mathbf{z}_2, \ldots, \mathbf{z}_k \in \bigcup(\mathcal{F} \setminus \{w\})$ with $k \leqslant n$ so that the family $\{\mathbf{v}_i \cap \{\mathbf{z}_2, \ldots, \mathbf{z}_k\} : \mathbf{v}_i \in \mathcal{F} \setminus \{w\}\}$ has cardinality $n - 1$, by exploiting either Lemma 1.1 (if $m = 1$) or the induction hypothesis. When $m = 1 < n$, we get the desired $\mathbf{z}_1, \ldots, \mathbf{z}_k \in \bigcup \mathcal{F}$ by simply adding $\mathbf{z}_1 = z$, because $w \cap \{\mathbf{z}_1, \ldots, \mathbf{z}_k\} = \{\mathbf{z}_1\} \not\subseteq v \cap \{\mathbf{z}_1, \ldots, \mathbf{z}_k\}$ for any $v \in \mathcal{F} \setminus \{w\}$ in this case.

When $m > 1$, we can inductively assume that

$$\mathsf{rk}(\mathbf{v}_i) = \varrho + 1 \quad \text{implies} \quad \mathsf{rk}(\mathbf{v}_i \cap \{\mathbf{z}_2, \ldots, \mathbf{z}_k\}) = \varrho + 1$$

for every $\mathbf{v}_i \in \mathcal{F}$ other than $\mathbf{v}_i = w$. If $\mathsf{rk}\,(w \cap \{\mathbf{z}_2, \ldots, \mathbf{z}_k\}) \neq \varrho + 1$, then we put $\mathbf{z}_1 = z$, so that $\mathsf{rk}\,(w \cap \{\mathbf{z}_1, \ldots, \mathbf{z}_k\}) = \rho + 1$ and the set $w \cap \{\mathbf{z}_1, \ldots, \mathbf{z}_k\}$ differs from any set $v \cap \{\mathbf{z}_1, \ldots, \mathbf{z}_k\}$ with $\mathsf{rk}(v) \leqslant \rho$ (since $\mathbf{z}_1 \in w$ and $\mathsf{rk}(\mathbf{z}_1) = \varrho$) and it also differs from any set $\mathbf{v}_i \cap \{\mathbf{z}_1, \ldots, \mathbf{z}_k\}$ with $\mathbf{v}_i \in \mathcal{F} \setminus \{w\}$ and $\mathsf{rk}(\mathbf{v}_i) = \varrho + 1$ (since $\mathbf{v}_i \cap \{\mathbf{z}_2, \ldots, \mathbf{z}_k\}$ has an element $\mathbf{z}_j$ of rank ρ not belonging to w). If, on the contrary, $\mathsf{rk}\,(w \cap \{\mathbf{z}_2, \ldots, \mathbf{z}_k\}) = \rho + 1$, then either $w \cap \{\mathbf{z}_2, \ldots, \mathbf{z}_k\}$ already differs from any $\mathbf{v}_i \cap \{\mathbf{z}_2, \ldots, \mathbf{z}_k\}$ with $\mathbf{v}_i \in \mathcal{F} \setminus \{w\}$, in which case we do not need a *new* $\mathbf{z}_1$ (and we can put $\mathbf{z}_1 = \mathbf{z}_2$), or else we can arbitrarily pick $\mathbf{z}_1$ out of that unique symmetric difference $(w \cap \{\mathbf{z}_2, \ldots, \mathbf{z}_k\}) \bigtriangleup (\mathbf{v}_i \cap \{\mathbf{z}_2, \ldots, \mathbf{z}_k\})$, with $\mathbf{v}_i \in \mathcal{F}$, which is not empty. $\square$

The decidability of restricted unnested BSR-formulae. Let us start by giving a rather simplified and intuitive satisfiability test for the subclass of *restricted unnested BSR-formulae* defined below.

Definition 7. A BSR-formula $\varphi(x_1, \ldots, x_n)$ is said to be RESTRICTED if all of its universal quantifiers are bounded. A restricted formula is UNNESTED if for any bounded quantifier $\forall y \in x$ the variable x is free in φ. $\square$

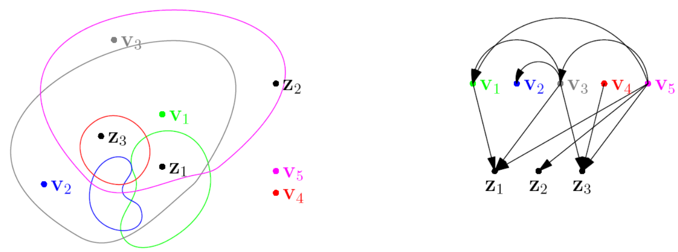

FIGURE 2. A family $\mathcal{F}$ of five sets with a minimal differentiating set and the associated membership graph (without edges among the elements of the differentiating set).

Given a restricted unnested formula $\varphi(x_1, \ldots, x_n)$, if there are sets $\mathbf{v}_1, \ldots, \mathbf{v}_n$ satisfying it, consider the graph $G_{\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}}$ (see Definition (5)). Such graph is a finite structure that can simply be "guessed" as a non deterministic step of our satisfiability procedure. The problem is that we are generally unable, given such a structure, to reconstruct the tuple of sets satisfying the formula (or even another one). The natural move would be trying to use the Mostowski collapse of $G_{\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}}$, namely the family

$$\mathbf{M}(\mathbf{v}_j) \quad = \quad \{\mathbf{M}(\mathbf{v}_i) : \langle \mathbf{v}_j, \mathbf{v}_i \rangle \in E_{\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}}\}$$

with $j = 1, \ldots, n$; however, such sets have the obvious problem that it can easily be the case that $\mathbf{v}_h \neq \mathbf{v}_k$ while $\mathbf{M}(\mathbf{v}_h) = \mathbf{M}(\mathbf{v}_k)$. To avoid this problem, we should enrich the graph with further nodes acting as witnesses and use the parametric version of the Mostowski collapse.

Such an enrichment is always possible. In fact, recalling Lemma 1.1 we have that $k < n$ new elements of $\mathbf{v}_1 \cup \cdots \cup \mathbf{v}_n$ are sufficient as witnesses of the differences among $\mathbf{v}_1, \ldots, \mathbf{v}_n$. These extra nodes $\mathbf{z}_1, \ldots, \mathbf{z}_k$ can be "guessed" from the outset by our algorithm.

At this point—as the reader can easily verify—the Mostowski collapse with parameter $\mathbf{Z} = \{\mathbf{z}_1, \ldots, \mathbf{z}_k\}$ ensures that all equalities and membership relations among $\mathbf{M}(\mathbf{v}_1; \mathbf{Z}), \ldots, \mathbf{M}(\mathbf{v}_n; \mathbf{Z})$ and their elements mimic exactly the ones among $\mathbf{v}_1, \ldots, \mathbf{v}_n$ and their elements.

Notice that it is the universal character of φ that allows us to conclude. In fact, if the sets $\mathbf{M}(\mathbf{v}_1; \mathbf{Z}), \ldots, \mathbf{M}(\mathbf{v}_n; \mathbf{Z})$ were not to satisfy φ, then a counterexample to the satisfiability of φ by $\mathbf{v}_1, \ldots, \mathbf{v}_n$ (using $\mathbf{v}$'s and witnesses only) could easily be built. This is the key point in the construction where the assumption of unnestedness plays its role: a counterexample to a purely universal unnested formula could never use an element which does not correspond to a node in $G_{\{\mathbf{v}_1,\ldots,\mathbf{v}_n,\mathbf{z}_1,\ldots,\mathbf{z}_k\}}$.

An algorithm which solves the satisfiability problem for restricted un-nested formulae was proposed in [BFOS81], as one of the first results in Computable Set Theory. The argument used in [BFOS81] was different from the one presented above and the decidability result was also extended to cover some extra constructors (notably arithmetic ones) that were shown to maintain both the property of reflection into the (hereditarily) finite sets and decidability.

The absence of nested quantifiers is crucial in showing the property of reflection into finite sets: below we examine a restricted and nested formula which is satisfiable without being finitely satisfiable (cf. [PP88, PP90, PP91]). Consider the formula in two variables—to be denoted ω_0 and ω_1, respectively—constituted by the following sub-formulae where $b = 0, 1$:

a) $\forall y \in \omega_b \forall x \in y (x \in \omega_{1-b})$, that is $\omega_b \subseteq \mathscr{P}(\omega_{1-b})$;
b) $\omega_b \notin \omega_{1-b}$;
c) $\omega_0 \neq \omega_1$.

Two sets satisfying the above conditions are not necessarily infinite; in fact $\omega_0 = \{\emptyset, \{\{\emptyset\}\}\}$, $\omega_1 = \{\{\emptyset\}, \{\{\{\emptyset\}\}\}\}$ would satisfy our formula.

However, the above interpretation can be seen as the beginning of a back-and-forth process that will eventually force both ω_0 and ω_1 to become infinite.

Assuming that $\in$ does not form either cycles or infinite descending chains, either one of the following conditions will do to the case (cf. [PP88, PP90]):

d) $\forall x_1, x_2 \in \omega_0 \forall y_1, y_2 \in \omega_1 (x_1 \in y_1 \in x_2 \in y_2 \ \rightarrow\ x_1 \in y_2)$,
e) $\forall x \in \omega_0 \forall y \in \omega_1 (x \in y \vee y \in x)$.

In case membership is allowed to be a non well-founded relation, the conjunction of the above is necessary (see [PP91]).

Since here we assume membership to be well-founded and the result is easily proved, we state:

Lemma 1.3. *The conjunction of conditions* a), b), c), *and* e) *force both* ω_0 *and* ω_1 *to have the same limit rank (and hence to be infinite).*

Proof. Suppose, by contradiction and w.l.o.g., that ω_0 has rank strictly less than the rank of ω_1 and consider an element $z \in \omega_1$ having the smallest rank greater than or equal to the rank of ω_0. By condition *a)* we have that $z \subseteq \omega_0$ and by condition *e)* and the fact that the rank of z is greater than or equal to the rank of ω_0, we have that $\omega_0 \subseteq z$. Hence $\omega_0 = z \in \omega_1$, which contradicts *b)*. Moreover, observe that the (common) rank of ω_0 and ω_1 cannot be a successor ordinal, otherwise two elements of highest rank in the two sets would fail to satisfy condition *e)*. □

The above result can be seen pictorially: two sets satisfying conditions *a), b)* and *c)* on ω_0 and ω_1 must have elements of increasing rank $\omega_{0,i}$ and $\omega_{1,i}$, respectively, as in Fig. 3. Stopping at any given finite even rank i forces ω_0 to become $\omega_{1,i}$ and ω_1 to become $\omega_{0,i-1}$, from which $\omega_1 \in \omega_0$ follows. For odd ranks the situation is symmetric.

There is nothing special about the fact that *two* sets are involved in the above example. A more general situation which, for any nonnegative n, analogously forces $n + 2$ sets ω_i to have limit rank, is described by the formula appearing in the following proposition, easily rewritable as a BSR-formula[2]:

[2]In the ongoing, $\bmod$ designates the integer remainder operation.

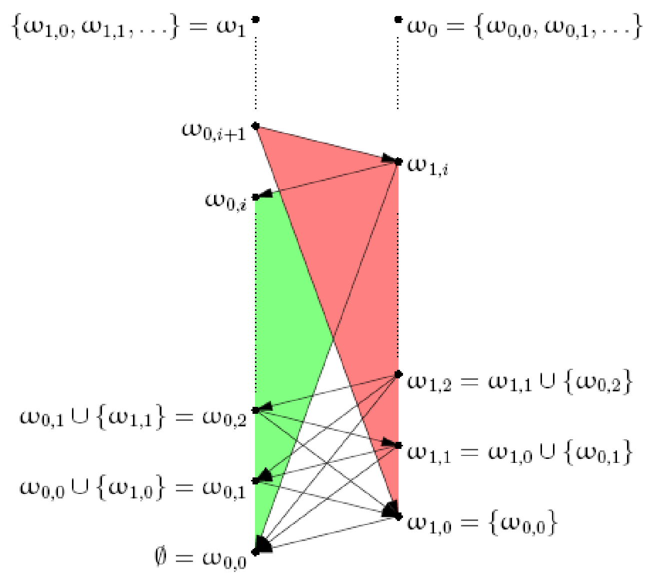

FIGURE 3. A pictorial proof of Lemma 1.3.

Lemma 1.4. *The formula*

$$\emptyset \neq \omega_0 \;\wedge\; \bigwedge_{i=0}^{n+1} \left(\omega_i \notin \omega_{(i+1) \mod (n+2)}\right) \;\wedge\; \bigwedge_{i=0}^{n+1} \left(\bigcup \omega_{(i+1) \mod (n+2)} \subseteq \omega_i\right) \;\wedge$$
$$(\forall x_0 \in \omega_0, \ldots, x_{n+1} \in \omega_{n+1}) \left(\bigvee_{i=0}^{n+1} x_i \in x_{(i+1) \mod (n+2)}\right)$$

is satisfiable but is not finitely satisfiable.

Proof. For readability, consider all arithmetic operations on indices as modulo $n+2$.

To see that the above formula is satisfiable, interpret each ω_i as the collection $\{\omega_{i,0}, \omega_{i,1}, \ldots\}$ of hereditarily finite sets where, for $i = 0, \ldots, n+1$ and for every natural number r:

$$\omega_{i,r} \quad = \quad \left\{\omega_{(i-1),r'} : r' = 0, 1, \ldots, r-1\right\}$$

(so that, in particular, $\omega_{0,0} = \emptyset$).

To see that the said formula is not finitely satisfiable, suppose that $\omega_0, \ldots, \omega_{n+1}$ satisfy it. We will assume first that some ω_i be null, then that some ω_i has a successor rank, getting into a contradiction in either case. The conclusion will be that every ω_i has a limit rank and hence has an infinite cardinality.

As a preliminary remark, observe that

$$\mathbf{x} \in \omega_i \;\text{ always implies }\; \omega_{(i-1)} \not\subseteq \mathbf{x}\;;$$

for, assuming the contrary, the equality $\omega_{(i-1)} = \mathbf{x}$ would hold because $\mathbf{x} \subseteq \bigcup \omega_i \subseteq \omega_{(i-1)}$; but then $\omega_{(i-1)} \in \omega_i$ would hold, contradiction.

Under the temporary assumption that some ω_i can be null, consider the largest k for which $\omega_k = \emptyset$; then, since $\omega_{(k+1)} \neq \emptyset$, we can pick an element $\mathbf{x} \in \omega_{(k+1)}$ and we know from the previous remark that $\omega_k \not\subseteq \mathbf{x}$, contradiction.

Suppose next that ω_k has a successor rank, and that $\mathbf{x} \in \omega_k$, $\mathsf{rk}(\mathbf{x})+1 = \mathsf{rk}(\omega_k)$. Put $\mathbf{x}_k = \mathbf{x}$. Then, for $i = 0, \dots, n$, by repeatedly taking into account our earlier remark, we can pick an element

$$\mathbf{x}_{(k-i-1)} \in \omega_{(k-i-1)} \setminus \mathbf{x}_{(k-i)} .$$

In view of the condition

$$(\forall x_0 \in \omega_0, \dots, x_{n+1} \in \omega_{n+1}) \left(\bigvee_{i=0}^{n+1} x_i \in x_{(i+1)} \right),$$

we have that $\mathbf{x} \in \mathbf{y} \in \omega_{(k+1)}$ for a suitable $\mathbf{y}$. The leftward loop which has enabled us to obtain $\mathbf{y}$ from $\mathbf{x}$ can be placed inside a rightward loop whose second iteration, starting with $\mathbf{y}$ (in the same role which $\mathbf{x}$ held before) and proceeding similarly, will find a $\mathbf{z} \in \omega_{(k+2)}$ such that $\mathbf{y} \in \mathbf{z}$. Repeated for long enough, this outer loop will construct a membership chain reaching an $\mathbf{x}'$ belonging to the same ω_k with which we have started, with $\mathsf{rk}(\mathbf{x}) < \mathsf{rk}(\mathbf{x}')$, contradiction.

(Notice that a single execution of the inner loop would have sufficed for the conclusion that $\omega_0 \cup \dots \cup \omega_{n+1}$ cannot be finite; actually, assuming the contrary, we could have supposed ω_k to be of maximum rank amid the ω_i's. However, with minimum extra effort, we have managed to distill more information from our proof.) □

2. The syntactic reduction

In this section we show that the (satisfiability) decision problem for the entire BSR-class can be reduced to the subclass of restricted BSR-formulae.

To see this we begin by proving that every BSR-sentence can always be cast in the following simple format:

Proposition 2.1. *Every prenex sentence*

$$\Phi \quad \equiv \quad (\exists x_1, \dots, x_n)(\forall y_1, \dots, y_m)\phi(x_1, \dots, x_n, y_1, \dots, y_m)$$

in the BSR-class is logically equivalent to a sentence

$$\Phi \quad \equiv \quad (\exists x_1, \dots, x_n) \bigwedge_{i=1}^{k} (\forall y_1, \dots, y_m)\phi_i(x_1, \dots, x_n, y_1, \dots, y_m),$$

where each ϕ_i is a disjunction of literals of the forms

$$z \in w \ , \ z \notin w \ , \ z = w \ , \ z \neq w \ ,$$

with $z, w \in \{x_1, \dots, x_n, y_1, \dots, y_m\}$.

To see that the above proposition is true, it suffices to bring the matrix ϕ of Φ to conjunctive normal form, then interchanging universal quantifiers and conjunction.

Our next step will be to perform a transformation, rather common in decision procedures for fragments of set theory, which does not apply to *sentences* but to the corresponding formulae obtained by withdrawing the existential quantifiers (see Definition (1)). Here the notion of *injective* satisfiability, meaning "satisfiability by a tuple of pairwise distinct sets", enters into play. We are about to observe that, within pure first order logic, we can restrain our analysis to equality-free formulae:

Lemma 2.2. *For any given formula φ in n free variables of the BSR-class, one can determine a finite collection of conjunctions*

$$\varphi_h = \bigwedge_{i=1}^{k_h} (\forall y_1, \dots, y_m) \phi_i(x_{j_1}, \dots, x_{j_{n_h}}, y_1, \dots, y_m)$$

of BSR-formulae, where $n_h \leqslant n$ and every ϕ_i is a disjunction of literals of the forms

$$z \in w \ , \ z \notin w \ ,$$

with $z, w \in \{x_{j_1}, \dots, x_{j_{n'}}, y_1, \dots, y_m\}$, so that φ is satisfiable if and only if some φ_h is injectively satisfiable.

(Sets satisfying the original φ will correspond to sets injectively satisfying one of the φ_h's.)

Proof. To see the result it is sufficient to observe that, by taking an assignment, any n-tuple of sets satisfying the original formula can always be reduced to an n'-tuple of sets injectively satisfying the version of the formula deprived of equalities (that become identities) and inequalities (that become unsatisfiable). See [COP01, Section 6.3.4]. □

On the ground of the above result, from now on we will assume that no equalities/inequalities appear in the matrix of BSR-formulae/sentences and we will intend "satisfiability" as actually meaning "injective satisfiability".

Our last result in this section proves that we can further restrict our consideration to the bounded-quantifier case:

Lemma 2.3. *Any conjunction*

$$\bigwedge_{i=1}^{k} (\forall y_1, \dots, y_m) \phi_i(x_1, \dots, x_n, y_1, \dots, y_m)$$

of BSR-formulae, where each ϕ_i is an disjunction of literals of the forms $z \in w$ and $z \notin w$, is equivalent to an alike formula in which every ϕ_i involving a variable y_j comprises at least one literal of the form

$$y_j \notin z \ ,$$

with $z \in \{x_1, \dots, x_n, y_1, \dots, y_{j-1}\}$.

Proof. Assume first that there exist a y_j and a ϕ_i within which y_j, but no literal $y_j \notin z$ with

$$z \in \{x_1, \dots, x_n, y_1, \dots, y_{j-1}, y_{j+1}, \dots, y_m\},$$

occurs. Hence, all literals involving y_j within ϕ_i are of the forms

$$z \in y_j \ , \ z \notin y_j \ , \ y_j \in z \ .$$

If $\phi_i(x_1, \dots, x_n, y_1, \dots, y_m)$ is true for some n-tuple $X_1, \dots, X_n$ of sets and for every m-tuple $Y_1, \dots, Y_m$ of sets, then consider any specific such m-tuple $Y_1, \dots, Y_m$, and replace Y_j in such a tuple by a set Y'_j which satisfies all literals

$$Y'_j \notin X_1, \dots, Y'_j \notin X_n, Y'_j \notin Y_1, \dots, Y'_j \notin Y_m$$

and also satisfies all biimplications

$$Z \in Y'_j \quad \text{if and only if} \quad \phi_i \text{ does not comprise the literal } z \in y_j$$

with $z \in \{x_1, \dots, x_n, y_1, \dots, y_{j-1}, y_{j+1}, \dots, y_m\}$. It is easy to see that one such Y'_j can always be found; therefore truth (under the assignment $x_k \mapsto X_k$ is preserved if ϕ_i is replaced by its sub-formula ϕ'_i obtained by withdrawing all literals which involve y_j.

At this point, if a chain of the form

$$y_j \notin z_1, \dots, z_h \notin y_j$$

appears in a conjunct ϕ_i, we can discard the conjunct inasmuch as blatantly true. Hence, we can rename the universally quantified variables in every conjunct, so as to meet the claim of this theorem. $\square$

On the ground of the above result we can assume the following *restricted* format for formulae of the BSR-class:

$$\bigwedge_{i=1}^{k} (\forall y_1 \in z_1, \dots, y_{m_i} \in z_{m_i}) \phi_i(x_1, \dots, x_n, y_1, \dots, y_{m_i}),$$

where $z_h \in \{x_1, \dots, x_n, y_1, \dots, y_{h-1}\}$ for $h \in \{1, \dots, m_i\}$.

3. The semantic reduction

In this section we present an argument to prove that a finite (and bounded) description of a finite family satisfying a given restricted BSR-formula can always be built. Our general strategy will be to extend the proof used for the unnested case (see Section (1)) by producing a family of witnesses that will not need the parametric version of the Mostowski collapse.

We will begin with the following definition that characterizes the self-sustaining sets of witnesses we are looking for.

Definition 8. Given a family $\mathcal{F}$, we say that $\mathbf{W} \subseteq \mathsf{TrCl}(\mathcal{F})$ REPRESENTS $\mathcal{F}$ if:

- $\mathcal{F} \subseteq \mathbf{W}$, and
- for all $\mathbf{u}, \mathbf{v} \in \mathbf{W}$, if $\mathbf{u} \neq \mathbf{v}$ then $\mathbf{M}(\mathbf{u}, G_{\mathbf{W}}) \neq \mathbf{M}(\mathbf{v}, G_{\mathbf{W}})$.
  (That is, the Mostowski collapse on $\mathbf{W}$ is injective.) $\square$

Proposition 3.1. *If $\varphi(x_1, \dots, x_n)$ is a restricted BSR-formula satisfied by $\mathbf{v}_1, \dots, \mathbf{v}_n$ and $\mathbf{W}$ represents $\mathcal{F} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$, then also the n-tuple*

$$\mathbf{M}(\mathbf{v}_1, G_{\mathbf{W}}), \dots, \mathbf{M}(\mathbf{v}_n, G_{\mathbf{W}})$$

satisfies $\varphi(x_1, \dots, x_n)$.

Proof. The proof is entirely analogous to the one given in the unnested case (see Section (1)). $\square$

From now on when two elements $\mathbf{u}, \mathbf{v} \in \mathbf{W}$ are such that $\mathbf{u} \neq \mathbf{v}$ and $\mathbf{M}(\mathbf{u}, G_{\mathbf{W}}) = \mathbf{M}(\mathbf{v}, G_{\mathbf{W}})$, we say that $\mathbf{u}$ and $\mathbf{v}$ *collide*.

The following lemma is our first step.

Lemma 3.2. *Given a finite family $\mathcal{F}$, a set $\mathbf{W}$ can be determined so that:*

1. $\mathbf{W}$ *represents $\mathcal{F}$;*
2. $\mathbf{W}$ *owns at most $|\mathcal{F}|$ members of rank α, for each ordinal α;*
3. $|\{\mathbf{w} \in \mathbf{W} \mid \mathsf{rk}(\mathbf{M}(\mathbf{w}, G_{\mathbf{W}}))$ *is a limit ordinal*$\}| < \omega$.

Proof. We proceed by induction on $\mathsf{rk}(\mathcal{F})$.

If $\mathsf{rk}(\mathcal{F}) \leqslant 1$, then the claim trivially holds, since either $\mathcal{F}$ is empty or $|\mathcal{F}| = 1$. As a matter of fact, if $|\mathcal{F}| = 1$ then for any value of $\mathsf{rk}(\mathcal{F})$ it suffices to take $\mathbf{W} = \mathcal{F}$.

For the inductive step, let $\mathcal{F} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. We will consider two cases: either $\mathsf{rk}(\mathcal{F}) - 1$ (i.e. the maximum rank of a $\mathbf{v}_i$) is a successor, or is a limit ordinal.

In case $\mathsf{rk}(\mathcal{F}) - 1$ is a successor, say $\varrho + 1$ for some ϱ, we can apply the élite discrimination lemma (Lemma (1.2)) to the set $\{\mathbf{v} \in \mathcal{F} \mid \mathsf{rk}(\mathbf{v}) = \varrho + 1\}$ thus determining elements $\mathbf{z}_1, \ldots, \mathbf{z}_k$ complying with the claim of that lemma. We can then apply the inductive hypothesis to get a set $\mathbf{W}'$ satisfying analogs of the conditions (1), (2), (3) relative to the family

$$\mathcal{F}' = \{\mathbf{v} \in \mathcal{F} \mid \mathsf{rk}(\mathbf{v}) \leqslant \varrho\} \cup \{\mathbf{z}_1, \ldots, \mathbf{z}_k\},$$

(notice that $\mathsf{rk}(\mathcal{F}') = \mathsf{rk}(\mathcal{F}) - 1$ and $|\mathcal{F}'| \leqslant n$). Next we show that we achieve our goal if we put

$$\mathbf{W} = \mathbf{W}' \cup \mathcal{F} (= \mathbf{W}' \cup \{\mathbf{v} \in \mathcal{F} \mid \mathsf{rk}(\mathbf{v}) = \varrho + 1\}).$$

To see that $\mathbf{W}$ represents $\mathcal{F}$ (claim (1)), observe that:

- two elements of $\mathbf{W}'$ cannot collide, by the induction hypothesis;
- two elements of $\mathcal{F} \setminus \mathbf{W}'$ $(= \{\mathbf{v} \in \mathcal{F} \mid \mathsf{rk}(\mathbf{v}) = \varrho + 1\})$ cannot collide, because the differentiating set $\{\mathbf{z}_1, \ldots, \mathbf{z}_k\}$ for $\mathcal{F} \setminus \mathbf{W}'$ has been included in $\mathbf{W}'$;
- there can be no collision between an element of $\mathcal{F} \setminus \mathbf{W}'$ and an element of $\mathbf{W}'$, as by Lemma (1.2) every element of $\mathcal{F} \setminus \mathbf{W}'$ owns an element $\mathbf{z}_i$ of rank ϱ, which cannot be the case for any element in $\mathbf{W}'$.

Claims (2) and (3) are easily seen to follow from the inductive hypothesis.

In case $\mathsf{rk}(\mathcal{F}) - 1$ is a limit ordinal λ, assume that $\mathsf{rk}(\mathbf{v}_1) \leqslant \mathsf{rk}(\mathbf{v}_2) \leqslant \cdots \leqslant \mathsf{rk}(\mathbf{v}_n)$ and that $\{\mathbf{v}_i, \ldots, \mathbf{v}_n\}$ are the elements of rank λ in $\mathcal{F}$. Let

$$\alpha = \mathsf{rk}(\{\mathbf{v}_1, \ldots \mathbf{v}_{i-1}\}) \cup \mathsf{rk}(\{\mathbf{z}_1, \ldots, \mathbf{z}_{n'}\}),$$

where $\{\mathbf{z}_1, \ldots, \mathbf{z}_{n'}\}$ is a differentiating set for $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$; actually, it would suffice here to choose α to be any ordinal (strictly below λ) which exceeds all of the ranks $\mathsf{rk}(\mathbf{v}_1), \ldots, \mathsf{rk}(\mathbf{v}_{i-1})$ and is high enough to ensure that $\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_i^{<\alpha}, \ldots, \mathbf{v}_n^{<\alpha}$ are n distinct sets.

Let $\mathcal{F}^0 = \{\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}\} \cup \{\mathbf{v}_i^{<\alpha}, \ldots, \mathbf{v}_n^{<\alpha}\}$, and apply the inductive hypothesis to get a set $\mathbf{W}^0$ satisfying analogs of (1), (2), and (3) relative to $\mathcal{F}^0$.

For every $u \in \omega$, let $\mathbf{z}_i^u, \ldots, \mathbf{z}_n^u$ be $n - i + 1$ sets belonging to $\mathbf{v}_i, \ldots, \mathbf{v}_n$, respectively (see Figure (4)), such that:

- $\alpha < \mathsf{rk}(\mathbf{z}_i^0)$,
- $\mathsf{rk}(\mathbf{z}_i^u) < \ldots < \mathsf{rk}(\mathbf{z}_n^u) < \mathsf{rk}(\mathbf{z}_i^{u+1})$ for all $u \in \omega$.

Now, for every $u \in \omega$, define the $(n - i + 1)$-tuple $t_u = \langle t_u(i), \ldots, t_u(n)\rangle$ by putting

$$t_u(\ell) \quad = \quad \begin{cases} \ell' & \text{if } \mathbf{z}_\ell^u = \mathbf{v}_{\ell'}^{<\mathsf{rk}(\mathbf{z}_\ell^u)} = \{x \in \mathbf{v}_{\ell'} \mid \mathsf{rk}(x) < \mathsf{rk}(\mathbf{z}_\ell^u)\}, \\ 0 & \text{otherwise.} \end{cases}$$

Notice that the above definition is well posed, as $\mathbf{z}_\ell^u$ can be at most one among $\mathbf{v}_i^{<\mathsf{rk}(\mathbf{z}_\ell^u)}, \ldots, \mathbf{v}_n^{<\mathsf{rk}(\mathbf{z}_\ell^u)}$, since otherwise two elements among $\mathbf{v}_i^{<\mathsf{rk}(\mathbf{z}_\ell^u)}, \ldots, \mathbf{v}_n^{<\mathsf{rk}(\mathbf{z}_\ell^u)}$ would collide, contradicting the fact that there are witnesses of their difference at a rank smaller than $\alpha < \mathsf{rk}(\mathbf{z}_\ell^u)$.

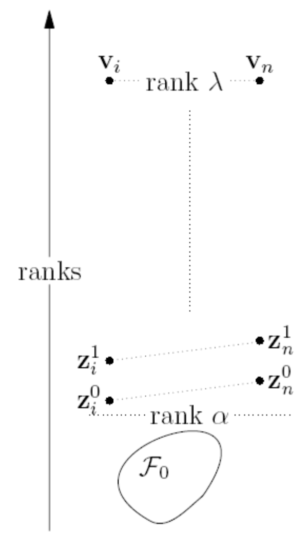

FIGURE 4. Positions of $\mathbf{z}_i^u, \ldots, \mathbf{z}_n^u$ relative to $\mathbf{v}_i, \ldots, \mathbf{v}_n$, for $u = 0, 1, \ldots$.

Clearly every t_u can be seen as a character in a finite alphabet, hence the infinite sequence $t_0, t_1, \ldots$ must contain an infinitely repeating character. Let $t_{r_0}, t_{r_1}, \ldots$ be a subsequence of $t_0, t_1, \ldots$ consisting of one such infinitely repeating character. Moreover, let $\bar{t}_{r_0}, \bar{t}_{r_1}, \ldots$ be the sequence resulting from $t_{r_0}, t_{r_1}, \ldots$ through replacement of each t_{r_j} by the $\bar{t}_{r_j}$ defined as

$$\bar{t}_{r_j}(\ell) \quad = \quad \begin{cases} t_{r_j}(\ell) & \text{if } \exists v(\ell \neq t_{r_j}(\ell) = \ell_1 \wedge t_{r_j}(\ell_1) = \ell_2 \wedge \cdots \wedge t_{r_j}(\ell_v) = \ell), \\ 0 & \text{otherwise.} \end{cases}$$

We claim that by putting

$$\mathbf{W} \quad = \quad (\mathbf{W}^0 \cap \mathsf{TrCl}(\mathcal{F})) \cup \{\mathbf{z}_\ell^{r_j} : j \in \omega, \ell \in \{i, \ldots, n\} \mid \bar{t}_{r_0}(\ell) \neq 0\} \cup \{\mathbf{v}_i, \ldots, \mathbf{v}_n\}$$

we meet the conditions (1), (2), and (3).

Concerning claim (1) we proceed by contradiction, assuming that $\mathbf{x}, \mathbf{y} \in \mathbf{W}$, despite being different, own the same successors in $G_{\mathbf{W}}$.

Consider the following three cases:

i) $\mathsf{rk}(\mathbf{x}) \geqslant \mathsf{rk}(\mathbf{y}) > \alpha$;
ii) $\mathsf{rk}(\mathbf{x}) > \alpha > \mathsf{rk}(\mathbf{y})$;
iii) $\alpha > \mathsf{rk}(\mathbf{x}) \geqslant \mathsf{rk}(\mathbf{y})$.

Case i) splits into three subcases:

i.1) $\mathbf{x}, \mathbf{y} \in \{\mathbf{v}_i, \ldots, \mathbf{v}_n\}$. This case cannot hold, because $\mathbf{W}^0$ includes a differentiating set for $\{\mathbf{v}_i^{<\alpha}, \ldots, \mathbf{v}_n^{<\alpha}\}$ (and therefore for $\{\mathbf{v}_i, \ldots, \mathbf{v}_n\}$).

i.2) $\mathbf{x} \in \{\mathbf{v}_i, \ldots, \mathbf{v}_n\}$ and $\mathbf{y} \notin \{\mathbf{v}_i, \ldots, \mathbf{v}_n\}$. In this case the equality $\mathbf{y} = \mathbf{z}_\ell^{r_j}$ must hold for some j and ℓ. Let $\bar{t}_{r_j}(\ell) = \ell' \notin \{0, \ell\}$.

It cannot be the case that $\mathbf{x} = \mathbf{v}_{\ell'}$ as otherwise, by definition of $\bar{t}_{r_j}$, it would be the case that $\exists v(t_{r_j}(\ell) = \ell' = \ell_1 \wedge t_{r_j}(\ell_1) = \ell_2 \wedge \cdots \wedge t_{r_j}(\ell_v) = \ell)$.

From this it would follow that $\bar{t}_{r_j}(\ell') = \bar{t}_{r_j}(\ell_1) \neq 0$ (as well as $\bar{t}_{r_j}(\ell_2) \neq 0, \ldots, \bar{t}_{r_j}(\ell_v) \neq 0$). As $\bar{t}_{r_j}(\ell') \neq 0$, there would be infinitely many elements of rank greater than α witnessing the difference between $\mathbf{x}$ and $\mathbf{y}$.

Moreover, it cannot be the case that $\mathbf{x} = \mathbf{v}_{\ell''} \neq \mathbf{v}_{\ell'}$, since by definition $\mathbf{z}_{\ell}^{r_j} = \mathbf{v}_{\ell'}^{<\mathsf{rk}(\mathbf{z}_{\ell}^{r_j})}$, and therefore a witness of the difference between $\mathbf{v}_{\ell''}^{<\alpha}$ and $\mathbf{v}_{\ell'}^{<\alpha}$ is also a witness of the difference between $\mathbf{x}$ and $\mathbf{y}$.

i.3) $\mathbf{x}, \mathbf{y} \notin \{\mathbf{v}_i, \ldots, \mathbf{v}_n\}$. This case is entirely analogous to the previous one. Details are left to the reader.

Case ii) cannot occur, as if $\mathbf{x}$ and $\mathbf{y}$ could collide, their respective ranks being greater and smaller than α, then $\mathbf{v}_{\ell'}^{<\alpha}$ and $\mathbf{y}$ would also collide, for some $\ell' \in \{i, \ldots, n\}$, contradicting the inductive hypothesis on $\mathbf{W}^0$.

Case iii) cannot occur, due to the inductive hypothesis, as both $\mathbf{x}$ and $\mathbf{y}$ belong to $\mathbf{W}^0$.

Claim (2) follows from the definition of the $\mathbf{z}_{\ell}^{r_j}$'s and from the inductive hypothesis.

Claim (3) is a plain consequence of the above construction.

$\square$

Given $\mathcal{F}$, the proof of the above lemma implicitly defines a procedure to determine a (countable) $\mathbf{W}$ representing it. Such a procedure—to be specified in a more "algorithmic" format in the second appendix—inserts elements of decreasing ranks in $\mathbf{W}$ and, for a finite number

$$h \quad = \quad |\{\mathbf{w} \in \mathbf{W} \mid \mathsf{rk}(\mathbf{M}(\mathbf{w}, G_{\mathbf{W}})) \text{ is a limit ordinal}\}|$$

of times, introduces elements of the form $\mathbf{z}_{\ell}^{r_j}$. We will denote such elements in $\mathbf{W}$ as $\mathbf{z}_{k,i_k}^{j}, \ldots, \mathbf{z}_{k,n_k}^{j}$ for $j \in \omega$ and $k \leqslant h$, and call them the *rotors* of $\mathbf{W}$. The (extra) index k in $\mathbf{z}_{k,\ell}^{j}$ indicates that the rotor was introduced while dealing with the k-th limit ordinal.

We will work with the following definition.

Definition 9. Let $\mathbf{W}$ be a countable set representing the family $\mathcal{F}$ so that

$$\{\mathsf{rk}(\mathbf{w}) : \mathbf{w} \in \mathbf{W} \mid \mathsf{rk}(\mathbf{M}(\mathbf{w}, G_{\mathbf{W}})) \text{ is a limit ordinal}\} = \{\lambda_1, \ldots, \lambda_h\},$$

has cardinality $h < \omega$. Assume $\lambda_1 < \cdots < \lambda_h$ for definiteness.

A ROTOR SYSTEM for $\mathbf{W}$ is a decomposition

$$\mathbf{W} \;=\; c(\mathbf{W}) \cup R_1 \cup \cdots \cup R_h$$

of $\mathbf{W}$ into disjoint sets such that

- $c(\mathbf{W})$, to be called the CORE of $\mathbf{W}$, is finite;
- each R_k, to be called the k-th LEVEL of $\mathbf{W}$, consists of distinct elements

$$\mathbf{z}_{k,i_k}^{j}, \ldots, \mathbf{z}_{k,n_k}^{j} \qquad (j \in \omega)$$

of rank less than λ_k, to be called the ROTORS ASCRIBED TO λ_k. $\square$

The reader can easily verify that rotors determined as in the proof of Lemma (3.2) are *downward uniform*, in the sense that of two rotors having the same subscripts and different superscripts one is always included in the other. More precisely: if

$j < j'$, then $\mathbf{z}^{j}_{k,\ell} \subsetneq \mathbf{z}^{j'}_{k,\ell}$. Indeed, this follows directly from the fact that rotors with the same subscripts, by definition, collide with the same element (of the core) at different stages of our procedure.

The definition below captures the symmetrical property of *upward uniformity* whose fulfillment, as we will see, can be achieved jointly with downward uniformity.

Definition 10. Let $\mathbf{W}$ represent $\mathcal{F}$ and satisfy the claims of Lemma (3.2). We will say that $\mathbf{W}$ is UPWARD UNIFORM (respectively, DOWNWARD UNIFORM) if for $k \leqslant h$ and $j, j' \in \omega$, any pair $\mathbf{z}^{j}_{k,\ell}, \mathbf{z}^{j'}_{k,\ell}$ of rotors belong to the same elements of $\mathbf{W}$ (respectively, $\mathbf{z}^{j}_{k,\ell} \subsetneq \mathbf{z}^{j'}_{k,\ell}$, if $j < j'$). □

In order to fulfill upward uniformity, we can proceed from higher to lower λ_k, erasing some of the rotors ascribed to λ_k, but preserving infinitely many of them along each "track" ℓ, and managing things in such a way that all rotors $\mathbf{z}^{j}_{k,\ell}$ left on the same track belong to the same elements above. More precisely:

Lemma 3.3. *Given a finite family $\mathcal{F}$, a set $\mathbf{W}$ can be determined so that:*

(1) $\mathbf{W}$ *represents $\mathcal{F}$;*
(2) $\mathbf{W}$ *owns at most $|\mathcal{F}|$ members of rank α, for each ordinal α;*
(3) $|\{\mathbf{w} \in \mathbf{W} \mid \mathsf{rk}(\mathbf{M}(\mathbf{w}, G_{\mathbf{W}}))$ *is a limit ordinal*$\}| < \omega$*;*
(4) $\mathbf{W}$ *is downward and upward uniform.*

Proof. On the ground of Lemma 3.2, we need only concentrate on the upper uniformity part of (4).

Let $n = |\mathcal{F}|$, and $h = |\{\mathbf{w} \in \mathbf{W} \mid \mathsf{rk}(\mathbf{M}(\mathbf{w}, G_{\mathbf{W}}))$ is a limit ordinal$\}|$. Let moreover $\lambda_1, \ldots, \lambda_h$, with $\lambda_1 < \cdots < \lambda_h$, be the limit ranks to which the rotors in $\mathbf{W}$ have been ascribed.

We begin by proving that we can shrink $\mathbf{W}$ into a $\mathbf{W}^1$ whose rotors $\mathbf{z}^{j}_{h,\ell}, \mathbf{z}^{j'}_{h,\ell}$ ascribed to λ_h belong (when, as shown, the subscripts they bear are the same) to the same elements of $\mathbf{W}$ (and hence of $\mathbf{W}^1$). To see this, it suffices to observe that the infinite sequence of tuples

$$\mathbf{z}^{j}_{h,i_h}, \ldots, \mathbf{z}^{j}_{h,n_h} \quad (j \in \omega),$$

admits an infinite subsequence of tuples of elements with the required property. This fact easily follows from the fact that there are only finitely many elements of $\mathbf{W}$ whose ranks exceed λ_h and that for $j' \leqslant j$,

$$\mathbf{z}^{j'}_{h,\ell} \in \mathbf{z}^{j}_{h,\ell'} \text{ holds if and only if } \mathbf{z}^{j'}_{h,\ell} \in \mathbf{v}_{\ell''},$$

where $\ell'' \in \{i_h, \ldots, n_h\}$ is such that $\mathbf{z}^{0}_{h,\ell'} = \mathbf{v}_{\ell''}^{<\mathsf{rk}(\mathbf{z}^{0}_{h,\ell'})}$.

Assume that $\mathbf{W}^u$ has been so constructed that its rotors ascribed to λ_{h-u+1} and bearing the same rotors belong to the same elements of $\mathbf{W}^{u-1}$. In order to conclude, it suffices to iterate the above technique also taking into account that for $h - u + 1 \leqslant k \leqslant h$ and $j' \leqslant j$,

$$\mathbf{z}^{j'}_{h-u,\ell} \in \mathbf{z}^{j}_{k,\ell'} \text{ holds if and only if } \mathbf{z}^{j'}_{h-u,\ell} \in \mathbf{v}_{k,\ell''},$$

where $\mathbf{v}_{k,\ell''} \in \{\mathbf{v} \in \mathbf{W} \mid \mathsf{rk}(\mathbf{v}) = \lambda_k\}$ is such that $\mathbf{z}^{0}_{h-u,\ell'} = \mathbf{v}_{k,\ell''}^{<\mathsf{rk}(\mathbf{z}^{0}_{h-u,\ell'})}$. □

A rotor system $\mathbf{W}$ as above, representing a family $\mathcal{F}$ which satisfies a given restricted BSR-formula, can be encoded as follows by a finite graph:

Definition 11. Let $\mathbf{W}$ represent $\mathcal{F}$ in downward and uniform fashion, with h levels of rotors. We define the ENCODING of $\mathbf{W}$ to be the graph $G^{\mathcal{F}}_{\mathbf{W}} = \langle V, E\rangle$ whose nodes V result from the disjoint union of sets V_c and V_r defined as follows:

$$\begin{array}{rcl} V_c & = & \big\{ v_i : \mathbf{w}_i \in c(\mathbf{W}) \big\}, \\ V_r & = & \big\{ z_{k,i_k}, \ldots, z_{k,n_k} : (\mathbf{z}^0_{k,i_k}, \ldots, \mathbf{z}^0_{k,n_k} \in \mathbf{W}),\ k \in \{1, \ldots, h\} \big\}, \end{array}$$

and whose set E of arcs results from the disjoint union of four sets (the second of which is generally not an acyclic relation) defined as follows:

$$\begin{array}{rcl} E_{cc} & = & \big\{ \langle v_j, v_i\rangle : v_i, v_j \in V_c \mid \mathbf{w}_i \in \mathbf{w}_j \,\big\}, \\ E_{rr} & = & \big\{ \langle z_{k,\ell}, z_{k',\ell'}\rangle : (z_{k',\ell'}, z_{k,\ell} \in V_r),\ b \in \{0,1\} \mid \mathbf{z}^b_{k',\ell'} \in \mathbf{z}^b_{k,\ell} \,\big\}, \\ E_{rc} & = & \big\{ \langle z_{k,\ell}, v_i\rangle : z_{k,\ell} \in V_r,\ v_i \in V_c \mid \mathbf{v}_i \in \mathbf{z}^0_{k,\ell} \,\big\}, \\ E_{cr} & = & \big\{ \langle v_i, z_{k,\ell}\rangle : z_{k,\ell} \in V_r,\ v_i \in V_c \mid \mathbf{z}^0_{k,\ell} \in \mathbf{v}_i \,\big\}. \end{array}$$

□

The encoding $G^{\mathcal{F}}_{\mathbf{W}}$ retains the overall information necessary to obtain a set $\mathbf{W}' = \mathbf{W}(G^{\mathcal{F}}_{\mathbf{W}})$ mimicking $\mathcal{F}$ in the sense to be clarified by Propositions (3.4,3.5) below.

Definition 12. The ω-UNROLLING of $G^{\mathcal{F}}_{\mathbf{W}} = \langle V, E\rangle$ is defined to be the set

$$\mathbf{W}(G^{\mathcal{F}}_{\mathbf{W}}) = \mathbf{W}_c(G^{\mathcal{F}}_{\mathbf{W}}) \cup \mathbf{W}_r(G^{\mathcal{F}}_{\mathbf{W}}),$$

where

$$\mathbf{W}_c(G^{\mathcal{F}}_{\mathbf{W}}) = \{\, \mathbf{v} : v \in V_c \,\}, \qquad \mathbf{W}_r(G^{\mathcal{F}}_{\mathbf{W}}) = \{\, \mathbf{z}^j : z \in V_c,\ j \in \omega \,\},$$

and the following equalities are recursively satisfied for all $v \in V_c$, $z = z_{k,\ell} \in V_r$, and $j \in \omega$:

$$\begin{array}{rcl} \mathbf{v} & = & \{\, \mathbf{w} : \langle v, w\rangle \in E_{cc} \,\} \cup \{ \tilde{\mathbf{z}}^j : \langle v, \tilde{z}\rangle \in E_{cr},\ j \in \omega \,\}, \\ \mathbf{z}^j & = & \{\, \mathbf{w} : \langle z, w\rangle \in E_{rc} \,\} \cup \\ & & \{ \tilde{\mathbf{z}}^{j'} : \tilde{z} = z_{k',\ell'} \in V_r,\ \langle z, \tilde{z}\rangle \in E_{rr} \mid k' < k \vee j' < j \vee (j' = j \wedge \ell' < \ell) \,\}. \end{array}$$

We get a fully analogous definition of m-UNROLLING by putting $m+1$ in place of ω in the above characterizations. □

To achieve full rigor, we could recast the above as a definition based on induction over a well-founded structure. In fact, as the reader can easily check, a vice in the definition of the ω-unrolling would stem either from a cycle appearing in the acyclic part of the encoding or from an infinite descending chain of natural numbers (the indices ℓ involved in the definition of $\mathbf{z}^j$), neither of which is possible.

Although not essential to our decidability result, our next proposition clarifies the notion of ω-unrolling introduced above. The proof of the fact reported below it relates to our goals more directly.

Proposition 3.4. *Given* $\mathbf{W}$ *representing* $\mathcal{F}$*, we have that:*

$$\mathbf{W}(G^{\mathcal{F}}_{\mathbf{W}}) \quad = \quad \mathbf{M}(\mathbf{W}, G_{\mathbf{W}}).$$

Proposition 3.5. *Given a restricted BSR-formula $\varphi = \varphi(x_1, \dots, x_n)$ and a family $\mathcal{F} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ represented by $\mathbf{W}$ in downward and upward uniform fashion, one can establish whether or not $\mathbf{v}_1, \dots, \mathbf{v}_n$ satisfy φ on the basis of the encoding $G^{\mathcal{F}}_{\mathbf{W}}$.*

Proof. Proposition (3.1) implies that if $\mathbf{v}_1, \dots, \mathbf{v}_n$ satisfy $\varphi(x_1, \dots, x_n)$, then by taking $\mathcal{F} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ and by choosing a $\mathbf{W}$ representing $\mathcal{F}$, we will have $\mathbf{M}(\mathbf{v}_1, G_{\mathbf{W}}), \dots, \mathbf{M}(\mathbf{v}_n, G_{\mathbf{W}})$ satisfying $\varphi(x_1, \dots, x_n)$. We will now show that testing $\varphi(x_1, \dots, x_n)$ for satisfaction under the assignment $x_i \mapsto \mathbf{M}(\mathbf{v}_i, G_{\mathbf{W}})$ is possible by mere inspection of the (finite) graph $G^{\mathcal{F}}_{\mathbf{W}}$.

To this end notice that if the formula

$$\varphi(x_1, \dots, x_n) \quad = \quad \bigwedge_{i=1}^{k} (\forall y_{i,1} \in z_{i,1}, \dots, y_{i,m_i} \in z_{i,m_i}) \phi_i(x_1, \dots, x_n, y_{i,1}, \dots, y_{i,m_i})$$

is not satisfied by $\mathbf{M}(\mathbf{v}_1, G_{\mathbf{W}}), \dots, \mathbf{M}(\mathbf{v}_n, G_{\mathbf{W}})$, then there is a conjunct in φ whose negation is satisfied by such sets. Namely, for some $i \in \{1, \dots, k\}$ the formula

$$(\exists y_{i,1} \in z_{i,1}, \dots, y_{i,m_i} \in z_{i,m_i}) \neg\phi_i(x_1, \dots, x_n, y_{i,1}, \dots, y_{i,m_i}),$$

is satisfied by $\mathbf{M}(\mathbf{v}_1, G_{\mathbf{W}}), \dots, \mathbf{M}(\mathbf{v}_n, G_{\mathbf{W}})$. In this case, let $\mathbf{y}_{i,1}, \dots, \mathbf{y}_{i,m_i}$ be m_i elements that, together with $\mathbf{M}(\mathbf{v}_1, G_{\mathbf{W}}), \dots, \mathbf{M}(\mathbf{v}_n, G_{\mathbf{W}})$, satisfy

$$\neg\phi_i(x_1, \dots, x_n, y_{i,1}, \dots, y_{i,m_i}).$$

It can easily be seen that since $\mathbf{W}$ is downward and upward uniform, all the rotors among $\mathbf{y}_{i,1}, \dots, \mathbf{y}_{i,m_i}$ can be assumed to be of level less than m_i. From this it follows that the m_i-unrolling of $G^{\mathcal{F}}_{\mathbf{W}}$ would be sufficient to check whether φ is satisfied by $\mathbf{M}(\mathbf{v}_1, G_{\mathbf{W}}), \dots, \mathbf{M}(\mathbf{v}_n, G_{\mathbf{W}})$ and hence by $\mathbf{v}_1, \dots, \mathbf{v}_n$. $\square$

In consequence of the above series of results, the decidability result announced at the beginning of this paper will ensue from our ability to place a bound on the size of the core of a set representing a family potentially satisfying a restricted BSR-formula $\varphi(x_1, \dots, x_n)$: once that bound is known, from the given φ we can determine a list of all candidate encodings, and testing φ for satisfiability will amount to checking that one of those actually encodes a satisfying tuple.

Lemma 3.6. *Given $\mathcal{F} = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ and an integer m, there exist a computable function f and a rotor system $\mathbf{W}^*$ such that:*

(1) *$\mathbf{W}^*$ represents $\mathcal{F}$ in upward and downward uniform fashion;*
(2) *$\mathbf{M}(\mathbf{W}^*)$ (i.e. $\{\mathbf{M}(\mathbf{w}, G_{\mathbf{W}^*}) : \mathbf{w} \in \mathbf{W}^*\}$) satisfies any BSR-formula in n free variables and m universally quantified variables satisfied by $\mathcal{F}$;*
(3) *the* size *$\|G^{\mathcal{F}}_{\mathbf{W}^*}\|$ of $G^{\mathcal{F}}_{\mathbf{W}^*}$ (the number of nodes plus the number of edges) meets the inequality $\|G^{\mathcal{F}}_{\mathbf{W}^*}\| \leqslant f(n, m)$.*

Proof. We assume, without loss of generality, that $\mathbf{v}_1 = \emptyset$. To prove our claim by induction on the number n of free (understood as existentially bound) variables, we add the following extra condition to the above clauses (1)–(3):

(4) for all $\mathbf{u} \in \mathbf{W}^*$,
   – if $\mathsf{rk}(\mathbf{M}(\mathbf{u}, \mathbf{W}^*))$ is a successor, ρ, then $\exists \mathbf{u}' \in \mathbf{u}(\mathbf{u}' \in \mathbf{W}^* \wedge \mathsf{rk}(\mathbf{M}(\mathbf{u}', \mathbf{W}^*)) = \rho - 1)$;
   – if $\mathsf{rk}(\mathbf{M}(\mathbf{u}, \mathbf{W}^*))$ is a limit ordinal, then all rotors in the transitive closure of $\mathbf{u}$ and ascribed to $\mathsf{rk}(\mathbf{u})$ are in $\mathbf{W}^*$.

Case $n = 1$ is trivial, as in this case $\mathbf{W}^* = \{\mathbf{v}_1\}(= \mathcal{F})$ will satisfy (1)–(4).

In case $n > 1$, recalling Lemma (3.3), assume that $\mathbf{W}$ is a downward and upward uniform set representing $\mathcal{F}$ whose core (finite, as ever) has least possible cardinality. After isolating as $\mathbf{v}_n$ an element of maximum rank in $\mathcal{F}$, consider the family

$$\mathcal{F}' \quad = \quad \{\mathbf{M}(\mathbf{v}_1, \mathbf{W}), \ldots, \mathbf{M}(\mathbf{v}_{n-1}, \mathbf{W})\},$$

and let $\mathbf{W}'$ satisfy analogs of (1)–(4) relative to $\mathcal{F}'$.

To obtain a bounded-core $\mathbf{W}^*$ representing $\mathcal{F}$ and satisfying (1)–(4), we will construct a list $\mathbf{W}^0, \mathbf{W}^1, \ldots, \mathbf{W}^k, \ldots$ issuing from $\mathbf{W}^0 = \mathbf{M}^{-1}(\mathbf{W}')$ and $\mathbf{W}^1 = \mathbf{W}^0 \cup \{\mathbf{v}_n\}$, where the inclusions $\mathbf{W}^k \subsetneq \mathbf{W}^{k+1} \subsetneq \mathbf{W}$ hold as long as the component $\mathbf{W}^{k+1}$ must be introduced, namely as long as putting $\mathbf{W}^* = \mathbf{W}^k$ would not suffice to ensure injectivity of the Mostowski collapse (associated with $G_{\mathbf{W}^k}$) and the satisfaction of condition (4). After we discuss the rules for progressively prolonging this list, it will be clear that its overall length must be finite; hence we can define $\mathbf{W}^*$ to be its last component.

If no collisions take place in $\mathbf{W}^k$, which however fails to meet condition (4), then choose an element $\mathbf{y}$ of $\mathbf{M}(\mathbf{W}^k)$ not belonging to $\mathbf{M}(\mathbf{W}^{k-1})$, so that $\mathsf{rk}(\mathbf{y})$ is as small as possible. If $\mathsf{rk}(\mathbf{y})$ is a successor, then put $\mathbf{W}^{k+1} = \mathbf{W}^k \cup \{\mathbf{w}\}$, where $\mathbf{w}$ is such that $\mathbf{M}(\mathbf{w}, \mathbf{W}) \in \mathbf{y}$ and $\mathsf{rk}(\mathbf{M}(\mathbf{w}, \mathbf{W})) + 1 = \mathsf{rk}(\mathbf{y})$; otherwise, let $\mathbf{W}^{k+1} \setminus \mathbf{W}^k$ be the set of all rotors ascribed to $\mathsf{rk}(\mathbf{M}^{-1}(\mathbf{y}, \mathbf{W}))$ which belong to $\mathsf{TrCl}(\mathbf{M}^{-1}(\mathbf{y}, \mathbf{W}))$.

If a collision takes place in $\mathbf{W}^k$, the reader can verify that only one element $\mathbf{x}$ in $\mathbf{W}^k \setminus \mathbf{W}^{k-1}$ can collide with an $\mathbf{x}'$ in $\mathbf{W}^{k-1}$ (this element is in fact the rotor of least rank, unless $|\mathbf{W}^k \setminus \mathbf{W}^{k-1}| = 1$). Then pick an element $\mathbf{w} \in \mathbf{W}^k$ in the symmetric difference $\mathbf{x} \bigtriangleup \mathbf{x}' = (\mathbf{x} \setminus \mathbf{x}') \cup (\mathbf{x} \setminus \mathbf{x}')$.

If $\mathbf{M}(\mathbf{x}, \mathbf{W})$ has limit rank, then let $\mathbf{W}^{k+1} \setminus \mathbf{W}^k$ be the set of all rotors ascribed to $\mathsf{rk}(\mathbf{x})$ which belong to $\mathsf{TrCl}(\mathbf{x})$. Otherwise we act as described in the following, depending on whether

i) $\mathsf{rk}(\mathbf{x}') > \mathsf{rk}(\mathbf{x})$,
ii) $\mathsf{rk}(\mathbf{x}') = \mathsf{rk}(\mathbf{x})$, or
iii) $\mathsf{rk}(\mathbf{x}) > \mathsf{rk}(\mathbf{x}')$.

i) This case cannot occur as otherwise, -by (4), in $\mathbf{W}^{k-1}$ there would be an element of $\mathbf{x}'$ endowed with rank greater than or equal to $\mathsf{rk}(\mathbf{x})$, and hence no collision could take place.
ii) Let $\mathbf{W}^{k+1} \setminus \mathbf{W}^k = \{\mathbf{w}\}$ (Notice that (4) ensures that $\mathbf{W}^k$ owns an element $\mathbf{x}$ of maximum rank in this case.)
iii) Let $\mathbf{W}^{k+1} \setminus \mathbf{W}^k = \{\mathbf{w}\}$, with $\mathbf{w}$ an element of $\mathbf{x}$ of rank $\mathsf{rk}(\mathbf{x}) - 1$.

It is straightforward to check that the proposed action will enforce injectivity, save possibly on the element of least rank in $\mathbf{W}^{k+1} \setminus \mathbf{W}^k$, without disrupting (4). At the end, it can easily be seen that the elements in $\mathbf{W}^* \setminus \mathbf{W}^0$ have pairwise distinct ranks.

Consider any BSR-formula φ in n existentially and m universally quantified variables satisfied by $\mathcal{F}$. As for the core of $\mathbf{W}^*$, the minimality of $|c(\mathbf{W})|$ guarantees that $|c(\mathbf{W})| = |c(\mathbf{W}^*)|$. Its size can be determined as the sum of the following two values:

$$a = \left|\{\mathbf{w} \in c(\mathbf{W}^*) \mid |c(\mathbf{W}^*)^{=\mathsf{rk}(\mathbf{w})}| = 1\}\right|;$$
$$b = \left|\{\mathbf{w} \in c(\mathbf{W}^*) \mid |c(\mathbf{W}^*)^{=\mathsf{rk}(\mathbf{w})}| > 1\}\right|.$$

Clearly $b \leqslant 2 \cdot |\mathbf{M}^{-1}(c(\mathbf{W}'))| = 2 \cdot |c(\mathbf{W}')|$ and hence, by the inductive hypothesis, b is bounded by $2 \cdot f(n-1, m)$..

In order to put a bound on a, we prove that any collection of elements $\mathbf{u}_1, \dots, \mathbf{u}_k \in \mathbf{W}^*$ such that for $i \in \{1, \dots, k\}$:

$$|\{\mathbf{w} \in c(\mathbf{W}^*) \mid \mathsf{rk}(\mathbf{w}) = \mathsf{rk}(\mathbf{u}_i)\}| = 1,$$

and $\mathbf{u}_1 \ni \mathbf{u}_2 \ni \cdots \ni \mathbf{u}_k$, can be limited in length.

We begin by treating the case when $\mathbf{u}_i \not\ni \mathbf{u}_j$ whenever $j > i+1$. In this case, let Σ whose characters are the subsets of the finite set $c(\mathbf{W}^*)^{>\mathsf{rk}(\mathbf{u}_1)}$. Consider then the string of sets:

$$\{\mathbf{w} \in c(\mathbf{W}^*)^{>\mathsf{rk}(\mathbf{u}_1)} \mid \mathbf{u}_1 \in \mathbf{w}\} \cdots \{\mathbf{w} \in c(\mathbf{W}^*)^{>\mathsf{rk}(\mathbf{u}_1)} \mid \mathbf{u}_k \in \mathbf{w}\}.$$

that we will denote by $u_1 \cdots u_k$, with $u_i \in \Sigma$ for $i \in \{1, \dots, k\}$.

We claim that the minimality of $|c(\mathbf{W}^*)|$ implies that the above string cannot own a repeated substring of length exceeding m. In order to prove the claim, arguing by contradiction let us assume that this is not the case and let $j < j' < k$ be such that

$$u_j \cdots u_{j+m} = u_{j'} \cdots u_{j'+m}.$$

Let $\overline{\mathbf{W}}$ be the set resulting from $\mathbf{W}^*$ through the replacement of $\mathbf{u}_{j+h}$ by $\mathbf{u}_{j'+h}$, for $0 \leqslant h \leqslant m$, in any $\mathbf{w} \in \mathbf{W}^*$ having $\mathbf{u}_{j+h}$ as an element. Formally:

$$\overline{\mathbf{W}} \quad = \quad \{(\mathbf{w} \setminus \{\mathbf{u}_{j+h}\}) \cup \{\mathbf{u}_{j'+h}\} : \mathbf{w} \in \mathbf{W}^*, 0 \leqslant h \leqslant m \mid \mathbf{u}_{j+h} \in \mathbf{w}\}.$$

We want to prove that the Mostowski collapse of $\overline{\mathbf{W}}$, still satisfies φ. As $|c(\overline{\mathbf{W}})| < |c(\mathbf{W}^*)|$, this would contradict the minimality of $|c(\mathbf{W}^*)|$.

First of all notice that the Mostowski collapse of $G_{\overline{\mathbf{W}}}$ is injective (details are left to the reader). To see that if $\mathcal{F}$ satisfies φ then also $\mathbf{M}(G_{\overline{\mathbf{W}}})$ satisfies it, we proceed again by contradiction. Reasoning as in the proof of Proposition (3.1), we assume that $\mathbf{y}_{i,1}, \dots, \mathbf{y}_{i,m_i}$ are m_i elements which, together with $\mathbf{M}(\mathbf{v}_1, G_{\overline{\mathbf{W}}}), \dots, \mathbf{M}(\mathbf{v}_n, G_{\overline{\mathbf{W}}})$, satisfy

$$\neg\phi_i(x_1, \dots, x_n, y_{i,1}, \dots, y_{i,m_i}),$$

with ϕ_i conjunct of φ.

If none of $\mathbf{y}_{i,1}, \dots, \mathbf{y}_{i,m_i}$ is among $\mathbf{u}_{j'}, \dots, \mathbf{u}_{j'+m}$, then $\mathbf{y}_{i,1}, \dots, \mathbf{y}_{i,m_i}$ would prove the unsatisfiability of φ by $\mathcal{F}$.

Otherwise, let $\mathbf{y}_{i,h} = \mathbf{u}_{j'+r}$. Since $m \geqslant m_i$, the following two cases cannot occur together:

(1) $\mathbf{u}_{j-1}, \mathbf{u}_{j'}, \dots, \mathbf{u}_{j'+r} \in \{\mathbf{y}_{i,1}, \dots, \mathbf{y}_{i,m_i}\}$;
(2) $\mathbf{u}_{j'+r}, \dots, \mathbf{u}_{j'+m}, \mathbf{u}_{j'+m+1} \in \{\mathbf{y}_{i,1}, \dots, \mathbf{y}_{i,m_i}\}$.

By replacing every element $\mathbf{y}_{i,h} = \mathbf{u}_{j'+r}$ by $\mathbf{u}_{j+r}$ whenever the first case occurs, the reader can verify that an m_i-tuple of sets satisfying $\neg\phi_i$ together with $\mathcal{F}$ can be obtained. This contradicts the satisfiability of φ by $\mathcal{F}$.

The last remaining case is the one in which in the list

$$\mathbf{u}_1 \ni \mathbf{u}_2 \ni \cdots \ni \mathbf{u}_k,$$

there exist some index i for which $\mathbf{u}_i \ni \mathbf{u}_j$ and $j > i+1$. We claim that there are at most $|c(\mathbf{W}^*)^{>\mathsf{rk}(\mathbf{u}_1)}|$ such indexes and, moreover, that the overall number of $\mathbf{u}_h$'s such that $i > h > j$ is again limited by $|c(\mathbf{W}^*)^{>\mathsf{rk}(\mathbf{u}_1)}|$. To see this notice that, given $\mathbf{u}_i, \mathbf{u}_j$ such that $\mathbf{u}_i \ni \mathbf{u}_j$ with $j > i+1$, either $\mathbf{u}_h$ with $i > h > j$

differentiates a pair of elements in $c(\mathbf{W}^*)^{>\mathsf{rk}(\mathbf{u}_1)}$ or it can be eliminated without causing any collision and thereby contradicting the minimality of $c(\mathbf{W}^*)$. This, by Proposition (1.1), bounds to $|c(\mathbf{W}^*)^{>\mathsf{rk}(\mathbf{u}_1)}|$ the overall number of possible h's; from such a bound also the bound on the number of possible i's follows.

The above two bounds on the length of chains of elements in

$$\{\mathbf{w} \in c(\mathbf{W}^*) \mid |c(\mathbf{W}^*)^{=\mathsf{rk}(\mathbf{w})}| = 1\},$$

allow us to recursively specify the function $f(n, m)$—details can be found in the first appendix—and conclude our proof of point (3).

□

We can now conclude with the following:

Theorem 3.7. *The BSR-class is decidable in Set Theory.*

Proof. By Lemma (2.3) we have that the satisfiability problem for the BSR-class is equivalent to the satisfiability problem for the restricted BSR-class.

By Lemmas (3.3) and (3.6), if a formula in n variables is satisfied by a family $\mathcal{F}$, then there exists a downward and upward uniform set $\mathbf{W}$ representing $\mathcal{F}$; moreover, under these hypotheses, the size of an encoding $G^{\mathcal{F}}_{\mathbf{W}}$ of $\mathbf{W}$ is bounded by a computable value g.

Accordingly, we can list all possible encodings of size less than g and apply Proposition (3.5) to test whether any of them is the encoding of a satisfying tuple. If this is not the case, we can declare the formula to be unsatisfiable. □

References

[BFOS81] M. Breban, A. Ferro, E. G. Omodeo, and J. T. Schwartz. Decision Procedures for Elementary Sublanguages of Set Theory. II: Formulas involving Restricted Quantifiers, together with Ordinal, Integer, Map, and Domain Notions. *Comm. Pure Appl. Math.*, 34:177–195, 1981.

[BGG97] Egon Börger, Erich Grädel, and Yuri Gurevich. *The Classical Decision Problem.* Perspectives in Mathematical Logic. Springer, 1997.

[Bol86] B. Bollobás. *Combinatorics.* Cambridge University Press, 1986.

[BP06] D. Bellè and F. Parlamento. Truth in $\mathbf{V}$ for $\exists^*\forall\forall$-sentences is decidable. *The Journal of Symbolic Logic*, 71(4):1200–1222, 2006.

[COP01] D. Cantone, E. G. Omodeo, and A. Policriti. *Set Theory for Computing. From Decision Procedures to Declarative Programming with Sets.* Monographs in Computer Science. Springer-Verlag, 2001.

[DG79] B. Dreben and W.D. Goldfarb. *The Decision Problem. Solvable Classes of Quantificational Formulas.* Addison-Wesley, Reading, MA, 1979.

[Lev79] A. Levy. *Basic Set Theory.* Springer-Verlag, 1979. Perspectives in Mathematical Logic.

[Lew79] H.R. Lewis. *Unsolvable Classes of Quantificational Formulas.* Addison-Wesley, Reading, MA, 1979.

[OPP93] E. G. Omodeo, F. Parlamento, and A. Policriti. A derived algorithm for evaluating ε-expressions over abstract sets. *Journal of Symbolic Computation*, 15(5-6):673–704, 1993. Special issue on Automatic Programming, A. W. Biermann and W. Bibel (eds.).

[PP88] F. Parlamento and A. Policriti. The Logically Simplest Form of the Infinity Axiom. *Proceedings of the American Mathematical Society*, 103(1):274–276, May 1988.

[PP90] F. Parlamento and A. Policriti. Note on: The Logically Simplest Form of the Infinity Axiom. *Proceedings of the American Mathematical Society*, 108(1), 1990.

[PP91] F. Parlamento and A. Policriti. Expressing Infinity without Foundation. *Journal of Symbolic Logic*, 56(4):1230–1235, 1991.

[PPR97] F. Parlamento, A. Policriti, and K. P. S. B. Rao. Witnessing Differences Without Redundancies. *Proceedings of the American Mathematical Society*, 125(2):587–594, February 1997.

[Ram28] F. P. Ramsey. On a problem of formal logic. *Proceedings of the London Mathematical Society*, 30(2):338–384, 1928.

Appendix: Bound on $f(n,m)$ of Lemma 3.6

Below we outline the argument enabling one to establish a (gross) recursive bound on the value $f(n,m)$.

First of all notice that $f(1,m)$ equals 1 for every m.

In case $n>1$ let $\mathbf{u}_1^1 \cdots \mathbf{u}_{k_1}^1$ be the first chain of elements in

$$a \quad = \quad \{\mathbf{w} \in c(\mathbf{W}^*) \mid |c(\mathbf{W}^*)^{=\mathsf{rk}(\mathbf{w})}| = 1\},$$

such that $\mathbf{u}_i^1 \ni \mathbf{u}_{i+1}^1$. The cardinality $\sigma_1 = \left|c(\mathbf{W}^*)^{>\mathsf{rk}(\mathbf{u}_1^1)}\right|$ is at most $2 \cdot f(n-1,m)$. Since there can be no repeated substring of length m in the string over the alphabet $\mathscr{P}(c(\mathbf{W}^*)^{>\mathsf{rk}(\mathbf{u}_1^1)})$ and the number of $\mathbf{u}_h^1$'s for which there exist i,j such that $i > h > j$ and $\mathbf{u}_i^1 \ni \mathbf{u}_j^1$ cannot exceed σ_1, the overall length k_1 of the first chain of elements in a meets the inequality:

$$k_1 \quad < \quad \sigma_1 \cdot (2^{m\cdot\sigma_1} + m) \leqslant 2 \cdot f(n-1,m) \cdot (2^{m\cdot 2\cdot f(n-1,m)} + m)$$

Likewise we can put a bound on the cardinality σ_2 of the set $c(\mathbf{W}^*)^{>\mathsf{rk}(\mathbf{u}_1^2)}$, relative to the second chain of elements in a, namely

$$\sigma_2 \quad \leqslant \quad \sigma_1 + k_1 + 2 \cdot f(n-1,m).$$

From such a bound, arguing as in the first case, we obtain the bound $k_2 < \sigma_2 \cdot (2^{m\cdot\sigma_2} + m)$ on the length of the second chain of elements in a.

Our final bound is obtained by simply observing that there must be fewer than $f(n-1,m)$ chains and hence

$$f(n,m) \quad \leqslant \quad \sigma_{f(n-1,m)-1}.$$

Appendix: Algorithmic Specifications

The procedures 'represents' (with its subordinate 'findRotors') and 'reprUniformly' (with its subordinate 'findUniformRotors') in this appendix specify in detail the (perpetual) construction of a set W representing a given finite family $\mathcal{F}$, as carried out within the proof of Lemma (3.2) and within the proof of Lemma (3.3), respectively. Both procedures receive $\mathcal{F}$ as an input parameter and return W (along with additional information concerning the rotors) as a result; the second input parameter of 'reprUniformly', $\mathcal{A}$, should be actualized as the empty set at top level and will grow progressively across recursion, inside the core of W.

procedure represents($\mathcal{F}$);
    assert $|\mathcal{F}| < \omega$;
    $\mu := \bigcup\{\, \mathsf{rk}(x) : x \in \mathcal{F}\,\}$;
    $\mathcal{T} := \{\, x \in \mathcal{F} \mid \mathsf{rk}(x) = \mu \,\}$;
    if $|\mathcal{F}| \leqslant 1$ **then**
        return $[\,\mathcal{F},\ \emptyset,\ \mathcal{F}\,]$;
    elseif $\exists \varrho \in \mu \mid \mu = \varrho + 1$ **then**
        $[\,\mathbf{W}', \text{rotors}', \text{core}'] :=$ represents$\big((\mathcal{F} \setminus \mathcal{T}) \cup \text{elite}(\mathcal{T})\big)$;
        return $[\,\mathbf{W}' \cup \mathcal{T},\ \ \text{rotors}',\ \ \text{core}' \cup \mathcal{T}\,]$;
    else
        $\alpha := \mathsf{rk}\big((\mathcal{F} \setminus \mathcal{T}) \cup \text{differentiators}(\mathcal{F})\big)$;

```
        [ W_0, rotors_0, core_0 ] := represents((F \ T) ∪ { v^{<α} : v ∈ T });
        rotors_1 := findRotors(α, T);
        return [ (W_0 ∩ TrCl(F)) ∪ T ∪ ⋃rotors_1,
                 rotors_0 ∪ rotors_1,    (core_0 ∩ TrCl(F)) ∪ T ];
    end if;
end represents;

procedure findRotors(α, T);
    assert |T| < ω &
        (∃ λ | α < λ & { rk(v) : v ∈ T } = {λ} & λ ≠ ∅ & (∀ ϱ ∈ λ | λ ≠ ϱ + 1));
    v⃗ := [ v : v ∈ T ];   β := α;   Z := [ ];
    for j ∈ ω loop
        z⃗ := [ ];
        for v = v⃗(ℓ) loop
            z⃗ := z⃗ with (z := arb(v^{>β}));   β := rk(z);
        end loop;
        Z := Z with z⃗;
    end loop;
    j := 1;
    repeat t⃗ := template(Z(j));   j := j + 1;
    until |{ r ∈ ω \ j | template(Z(r)) = t⃗ }| = ω;
    return { { Z(r)(ℓ) : r ∈ ω \ 1 | template(Z(r)) = t⃗ } :
                              ℓ ∈ {1, ..., |T|} | inCycle(ℓ, t⃗) };

    procedure template(z⃗);
        return [ if ∃ v = v⃗(p) | z = v^{<rk(z)} then p else 0 end if : z = z⃗(ℓ) ];
    end template;

end findRotors;

procedure inCycle(ℓ, t⃗);
    seen := {0};   p := ℓ;
    while p ∉ seen loop seen := seen with p;   p := t⃗(p) end loop;
    return t⃗(ℓ) ≠ ℓ & ℓ ∈ seen;
end inCycle;


procedure reprUniformly(F, A);
    assert |F| < ω;
    μ := ⋃{ rk(x) : x ∈ F };
    T := { x ∈ F | rk(x) = μ };
    if |F| ⩽ 1 then
        return [ F, ∅ ];
    elseif ∃ϱ ∈ μ | μ = ϱ + 1 then
        [ W′, rotors′ ] := reprUniformly((F \ T) ∪ elite(T),  A ∪ T );
        return [ W′ ∪ T,  rotors′ ];
    else
        α := rk((F \ T) ∪ differentiators(F));
```

```
        [ W_0, rotors_0 ] := reprUniformly((F \ T) ∪ { v^{<α} : v ∈ T },  A ∪ T);
        rotors_1 := findUniformRotors(α, T, A);
        return [ (W_0 ∩ TrCl(F)) ∪ T ∪ ⋃ rotors_1,   rotors_0 ∪ rotors_1 ];
    end if;
end reprUniformly;

procedure findUniformRotors(α, T, A);
    assert |T| < ω &
        (∃ λ | α < λ & { rk(v) : v ∈ T } = {λ} & λ ≠ ∅ & (∀ ϱ ∈ λ | λ ≠ ϱ + 1));
    v⃗ := [ v : v ∈ T ];    β := α;    Z := [ ];
    for j ∈ ω loop
        z⃗ := [ ];
        for v = v⃗(ℓ) loop
            z⃗ := z⃗ with (z := arb(v^{>β}));    β := rk(z);
        end loop;
        Z := Z with z⃗;
    end loop;
    j := 1;
    repeat t⃗ := template(Z(j));    j := j + 1;
    until |{ r ∈ ω \ j | template(Z(r)) = t⃗ }| = ω;
    Z := shrink([ Z(r) : r ∈ ω \ 1 | template(Z(r)) = t⃗ ],
                m⃗ := [ℓ ∈ {1, ..., |T|} | inCycle(ℓ, t⃗) ],      A ∪ T);
    return { { Z(r)(ℓ) : r ∈ ω \ 1 } : ℓ = m⃗(k) };

    procedure shrink(Z, m⃗, A);
        assert |A| < ω & (∀ j ∈ ω \ 1, a ∈ A, ℓ = m⃗(k) | rk(Z(j)(ℓ)) < rk(a));
        j := 1;
        repeat s⃗ := [{ a ∈ A | Z(j)(ℓ) ∈ a } : ℓ = m⃗(k)];    j := j + 1;
            S := { q ∈ ω \ j | [{ a ∈ A | Z(q)(ℓ) ∈ a } : ℓ = m⃗(k)] = s⃗ };
        until |S| = ω;
        return S;
    end shrink;
    procedure template(z⃗);
        return [ if ∃ v = v⃗(p) | z = v^{<rk(z)} then p else 0 end if : z = z⃗(ℓ) ];
    end template;
end findUniformRotors;
```

E. Omodeo: Dipartimento di Matematica e Informatica, Università di Trieste, 34127, via Valerio 12/b, Italy.

E-mail address: eomodeo@units.it

A. Policriti: Dipartimento di Matematica e Informatica, Università di Udine, 33100, via Delle Scienze 206, Italy.

E-mail address: policriti@dimi.uniud.it