A note on well quasi-orderings for powersets

Petr Jančar*

Dept. of Computer Science, FEI, Techn. Univ. of Ostrava
17. listopadu 15, CZ-708 33 Ostrava-Poruba, Czech Republic
E-mail: Petr.Jancar@vsb.cz

Abstract

This note characterizes those quasi-orderings $(A, \preceq)$ for which $(\mathcal{P}(A), \sqsubseteq)$ are well quasi-orderings, where $B_1 \sqsubseteq B_2$ iff $(\forall y \in B_2)(\exists x \in B_1) : x \preceq y$ (for $B_1, B_2 \subseteq A$). It turns out that they are those which do not contain the "Rado structure", hence are ω^2-well quasi-orderings in other words. A motivation for the question has come from the area of verification of infinite-state systems, where the usefulness of well quasi-orderings has already been recognized. This note suggests that finer notions might be useful as well. In particular, ω^2-well quasi-orderings illuminate a specific problem related to termination of a reachability algorithm, which has been touched on by Abdulla and Jonsson (1998).

Keywords: theory of computation, well quasi-orderings, powersets

1 Introduction

When studying general reachability algorithms used in (symbolic) verification methods, Abdulla and Jonsson [2, 3] touched on the problem whether (or when) termination of an algorithm using "constraints" guarantees termination of a (more efficient) implementation which uses sets of constraints; in particular, they mention the problem for "regions" and "zones" (a zone is a concise representation of a finite set of regions). In fact, the termination is tightly related to the existence of a certain well quasi-ordering, and the relevant question can be formulated in general terms as follows.

$(A, \preceq)$ is a *quasi-ordering*, *qo* for short, iff $\preceq$ is a reflexive and transitive relation on the set A. $(A, \preceq)$ is a *well quasi-ordering*, *wqo*, iff there is no bad sequence of elements of A, where a *bad sequence* is an infinite sequence $a_1, a_2, a_3, \ldots$ s.t. $\forall i, j : i < j \Rightarrow a_i \not\preceq a_j$. The question is whether (or when) $(A, \preceq)$ being wqo guarantees that $(\mathcal{P}(A), \sqsubseteq)$ is wqo, where $\mathcal{P}(A)$ denotes the set of subsets of A and $\sqsubseteq$ is defined as follows: $B_1 \sqsubseteq B_2$ iff $(\forall y \in B_2)(\exists x \in B_1) : x \preceq y$.

Remark. For a qo $(A, \preceq)$, we denote by $Eq(\preceq)$ the equivalence $\{(x, y) \in A \times A \mid x \preceq y \wedge y \preceq x\}$; the set A is thus partitioned into $Eq(\preceq)$-classes. Given now a bad sequence $B_0, B_1, B_2, \ldots$ in $(\mathcal{P}(A), \sqsubseteq)$, we can replace each B_i by B'_i which contains just one element out of each $Eq(\preceq)$-class which has nonempty intersection with B_i, and then take B''_i as the set of the minimal elements of B'_i. Obviously, $B''_0, B''_1, B''_2, \ldots$ keeps the bad sequence property, and if $(A, \preceq)$ is

*The author is supported by the Grant Agency of the Czech Republic, Grant No. 201/97/0456

wqo then each B_i'' is *finite*. Hence our question for $\mathcal{P}(A)$ can be reduced to the question for $\mathcal{P}_{fin}(A)$ (meaning *finite* subsets).

This note shows that a necessary and sufficient condition for $(\mathcal{P}(A), \sqsubseteq)$ to be wqo is that $(A, \preceq)$ is ω^2-wqo, which is a deeper (and finer) notion from wqo theory. It seems that such a characterization has not appeared among published results in wqo theory. On the other hand, the results in [5] show that ω^2-wqo's enjoy similar closure properties as wqo's, and the given characterization is thus satisfactory from a "practical" point of view.

The relevance of the notion of wqo to some (aspects of) verification problems has been shown by some researchers (see, e.g., [1, 4]). This note suggests that finer notions of wqo can be also useful in some situations. In our particular case it is the notion of ω^2-wqo, but in general another deep notion—*better quasi-ordering*—seems to be more promising (some remarks related to this are given in Section 3).

2 Result

In this section we prove

Theorem 1 *For a qo $(A, \preceq)$, $(\mathcal{P}(A), \sqsubseteq)$ is wqo iff $(A, \preceq)$ is ω^2-wqo.*

We shall not give the (standard) definition of ω^2-wqo since it needs some technical notions and would not help our aims here; the reader can find it in [5]. The following characterization can serve as our working definition (its justification is explained at the end of this section).

*A qo $(A, \preceq)$ is ω^2-*wqo *iff it is wqo and does not contain (an isomorphic copy of) the Rado structure.*

Here the *Rado structure* is $(\{(i,j) \in \mathbb{N}\times\mathbb{N} \mid i < j\}, \leq_{rado})$ where $\mathbb{N} = \{0, 1, 2, \ldots\}$ and

$$(i_1, j_1) \leq_{rado} (i_2, j_2) \;\Leftrightarrow_{df}\; (i_1 = i_2 \text{ and } j_1 \leq j_2) \text{ or } (j_1 < i_2).$$

It will be useful to imagine infinite columns $C_0, C_1, C_2, \ldots$ and finite rows $R_0, R_1, R_2, \ldots$ so that (i,j) is considered as residing in column C_i and row R_j; row R_0 is thus empty. By help of this, we can easily verify that the Rado structure is wqo. If we restrict i in (i,j) to $i < n$, we get the *Rado substructure with n columns* (namely $C_0, C_1, C_2, \ldots, C_{n-1}$).

Figure 1 sketches the Rado structure, highlighting row R_{n-1} and column C_{n-1}. On the figure, the union of the parts I, II and R_{n-1}, C_{n-1} depicts the Rado substructure with n columns; part III depicts the rest. It will be useful to note that $(\forall x \in R_{n-1})(\forall y \in C_{n-1}) : x \not\preceq y$, $(\forall x \in R_{n-1})(\forall y \in III) : x \preceq y$, and $(\forall x \in III)(\forall y \in C_{n-1} \cup II \cup R_{n-1} \cup I) : x \not\preceq y$.

Let us now confirm the "only if" direction of Theorem 1:

Lemma 2 *If $(\mathcal{P}(A), \sqsubseteq)$ is wqo then $(A, \preceq)$ is wqo and does not contain the Rado structure.*

Proof: If $(A, \preceq)$ is not wqo then $(\mathcal{P}(A), \sqsubseteq)$ is not wqo either since a bad sequence in $(A, \preceq)$ gives rise to a bad sequence in (singletons in) $(\mathcal{P}(A), \sqsubseteq)$. If $(A, \preceq)$ contains the Rado structure then its rows $R_0, R_1, R_2, \ldots$ constitute a bad sequence in $(\mathcal{P}(A), \sqsubseteq)$: for each i, j with $i < j$, $R_i \not\sqsubseteq R_j$, as evidenced by the element of R_j in column C_i: $(i,j) \in R_j$ and $\forall k < i : (k, i) \not\leq_{rado} (i,j)$ (i.e., $\forall x \in R_i : x \not\leq_{rado} (i,j)$). $\square$

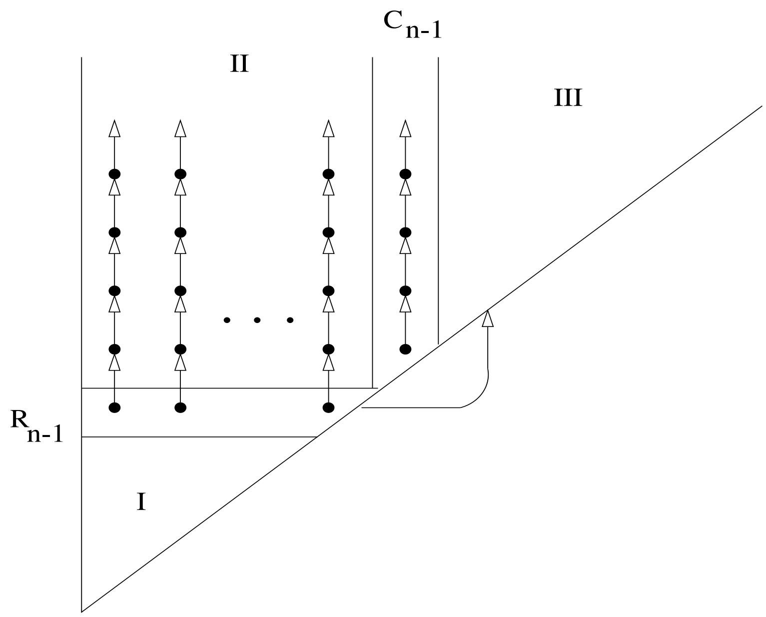

Figure 1:

The "if" direction of the theorem is more involved. The strategy can be sketched as follows. We start with a bad sequence $R_0, R_1, R_2, \ldots$ in $(\mathcal{P}(A), \sqsubseteq)$; for the moment, R_j's have nothing to do with the rows (of the Rado structure). We shall transform $R_0, R_1, R_2, \ldots$ by (infinitely many) steps Step 0, Step 1, Step 2, $\ldots$; each Step consists of removing some R_j's and some elements from some R_j's so that the resulting sequence, for simplicity, always (re)named $R_0, R_1, R_2, \ldots$, is again a bad sequence.

Remark. Note that removing some R_j's, if still infinitely many are left, surely keeps the bad sequence property. When removing elements of R_j's, we have to be more careful.

Moreover, Step n will not affect the prefix $R_0, R_1, \ldots, R_{n-1}$, so the (limit) sequence resulting from performing all Step 0, Step 1, Step 2, $\ldots$ is well-defined. Our aim is that the limit sequence will exactly correspond to the (rows of the) Rado structure. In fact, we shall start with a bad sequence satisfying a certain condition of minimality. We make now this condition precise, while also demonstrating our general strategy.

We say that a *sequence* $R_0, R_1, R_2, \ldots$ (in $(\mathcal{P}(A), \sqsubseteq)$) *is created from elements* of $B \subseteq A$ iff $\bigcup_{j=0}^{\infty} R_j \subseteq B$. A *bad sequence* $R_0, R_1, R_2, \ldots$ is *minimal* iff

1. for every $z \in \bigcup_{j=0}^{\infty} R_j$ there is no bad sequence created from elements of $\bigcup_{j=0}^{\infty} R_j \setminus \{x \mid z \preceq x\}$, i.e., from elements of $\{y \in \bigcup_{j=0}^{\infty} R_j \mid z \not\preceq y\}$, and
2. each $Eq(\preceq)$-class has nonempty intersection with at most one R_j, and such a nonempty intersection is then a singleton.

Lemma 3 *Assume that $(A, \preceq)$ is wqo, and $(\mathcal{P}(A), \sqsubseteq)$ is not wqo. Then there is a minimal bad sequence $R_0, R_1, R_2, \ldots$ in $(\mathcal{P}(A), \sqsubseteq)$; in particular, each R_j is finite.*

Proof: Consider a bad sequence $R_0, R_1, R_2, \dots$ in $(\mathcal{P}(A), \sqsubseteq)$. Suppose there is $z_1 \in \bigcup_{j=0}^{\infty} R_j$ s.t. there is a bad sequence $R_0^1, R_1^1, R_2^1, \dots$ created from elements of $\{y \in \bigcup_{j=0}^{\infty} R_j \mid z_1 \not\preceq y\}$. Further suppose there is $z_2 \in \bigcup_{j=0}^{\infty} R_j^1$ s.t. there is a bad sequence $R_0^2, R_1^2, R_2^2, \dots$ created from elements of $\{y \in \bigcup_{j=0}^{\infty} R_j^1 \mid z_2 \not\preceq y\}$. Note that $z_1 \not\preceq z_2$. If we continue this reasoning, we would get a sequence $z_1, z_2, z_3, \dots$ (of elements of A) s.t. for $i < j$ we have $z_i \not\preceq z_j$. But such a sequence can not be infinite since $(A, \preceq)$ is wqo. Therefore there is a bad sequence $R_0, R_1, R_2, \dots$ satisfying condition 1.

We have already discussed that we can suppose that the intersection of each $Eq(\preceq)$-class C with any R_j has at most one element, i.e., C is represented in each R_j just by one element if at all. Moreover, we can suppose the R_j's to be *finite* sets (taking the minimal elements). If now a class C is represented in infinitely many R_j's, by an element x_0 (among others), then we can remove all R_j's where C is not represented, and then remove in each (remaining) R_j all elements y s.t. $x_0 \preceq y$. By doing this, we obviously can not spoil the bad sequence property ($R_{j_1} \not\sqsubseteq R_{j_2}$ for $j_1 < j_2$) which contradicts the condition 1.

So each C is represented only in finitely many R_j's. We can now perform Step 0, Step 1, Step 2, ... where Step n consists of removing all (finitely many) R_j's, $j \geq n$, in which an $Eq(\preceq)$-class represented in any of $R_0, R_1, \dots, R_{n-1}$ is represented as well. (In fact, it suffices to consider just classes represented in R_{n-1}; we then declare Step 0 to be empty.) The limit sequence surely satisfies both 1. and 2. □

An additional ingredient we shall use is the next lemma which immediately follows from Ramsey's Theorem for infinite countable sets. (Ramsey's Theorem shows it for any binary relation; transitivity of $\preceq$ allows a more direct proof.)

Lemma 4 *Given a qo $(A, \preceq)$, if $a_1, a_2, a_3 \dots$ does not contain a bad subsequence then it contains a perfect subsequence, i.e., an infinite subsequence $a_{i_1}, a_{i_2}, a_{i_3}, \dots$ s.t. $\forall j, k : j < k \Rightarrow a_{i_j} \preceq a_{i_k}$.*

Now we are ready to prove the "if" part of Theorem 1.

Lemma 5 *If $(A, \preceq)$ is wqo and $(\mathcal{P}(A), \sqsubseteq)$ is not wqo then $(A, \preceq)$ contains the Rado structure.*

Proof: Let us fix a minimal bad sequence $R_0, R_1, R_2, \dots$ in $(\mathcal{P}(A), \sqsubseteq)$ (guaranteed by Lemma 3).

We perform Step 0, Step 1, Step 2, ... so that, for any $n \geq 0$, the first n steps (Step 0, Step 1, ..., Step $(n-1)$) result in a sequence (also (re)named $R_0, R_1, R_2, \dots$) satisfying the following property INV(n) (see also Fig. 2):

- $R_0, R_1, R_2, \dots$ is a minimal bad sequence,
- $\forall j = 0, 1, \dots, n-1 : R_j$ has j elements, denoted $(0, j), (1, j), \dots, (j-1, j)$,
- there are disjoint sets $C_0, C_1, C_2, \dots, C_{n-1}$ s.t. for all $i = 0, 1, \dots, n-1$ we have $\forall j \leq i :$ $C_i \cap R_j = \emptyset$ and for all $j > i$, $C_i \cap R_j$ is a singleton, denoted by $\{(i, j)\}$.
- Moreover, denoting $RSS(n) = \bigcup_{i=0}^{n-1} C_i$ and $REST(n) = \bigcup_{j=0}^{\infty} R_j \setminus RSS(n)$ ($= \bigcup_{j=n}^{\infty} R_j \setminus RSS(n)$), we have

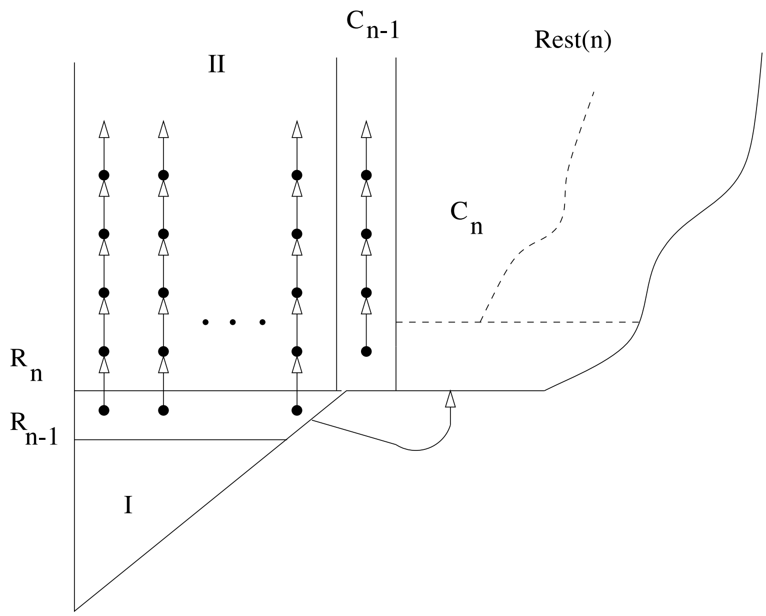

Figure 2:

1. $(RSS(n), \preceq)$ ($\preceq$ induced by $(A, \preceq)$) is the Rado substructure with n columns,
2. $(\forall x \in REST(n))(\forall y \in RSS(n)) : x \not\preceq y$,
3. $(\forall i < n{-}1)(\forall x \in REST(n)) : (i, n{-}1) \preceq x$.

An important observation is that removing any R_j's with $j \geq n$ (while infinitely many are left) keeps the property INV(n).

Since Step n will not affect $R_0, R_1, \ldots, R_{n-1}$, we shall be done once we show that, for each $n \in \mathbb{N}$, INV(n) holds after n steps (Step 0, Step 1, ..., Step ($n{-}1$)); we proceed by induction. INV(0) is (vacuously) satisfied. So we assume that INV(n) is satisfied (after n steps), and we shall show Step n after which INV($n{+}1$) is guaranteed. The task of Step n is to "extract" an appropriate column C_n from $REST(n)$, remove all "excessive" elements from R_n, i.e., those outside $\{(0,n), (1,n), \ldots, (n{-}1,n)\}$, and make further necessary changes to establish INV($n{+}1$) (in particular, the final condition 3.).

Let us define $C_n = \{x \in \bigcup_{j=n+1}^{\infty} R_j \mid \forall y \in R_n : y \not\preceq x\}$; note that $R_n \not\sqsubseteq \{x\}$ for every $x \in C_n$. In fact, in the case $n = 0$ (when defining Step 0) we need $R_0 \neq \emptyset$, which can be safely supposed. That is also the reason why we remove all "excessive" elements of R_n *after* handling C_n (R_0 *then* becomes $\emptyset$). (In fact, for $n \geq 1$ we could remove these excessive elements immediately but it does not matter.)

Note that $C_n \cap RSS(n) = \emptyset$, i.e., $C_n \subseteq REST(n)$, surely also $R_n \cap C_n = \emptyset$, and moreover, for each $j \geq n{+}1$, $C_n \cap R_j \neq \emptyset$ (since $R_n \not\sqsubseteq R_j$). Also note that $(\forall x \in REST(n) \setminus C_n)(\forall y \in C_n) : x \not\preceq y$. (This will guarantee condition 2. in INV($n{+}1$).)

Now observe that the sequence $C_n \cap R_{n+1}, C_n \cap R_{n+2}, C_n \cap R_{n+3}, \ldots$ cannot contain a bad subsequence since no bad sequence can be created from elements of C_n (due to minimality of $R_0, R_1, R_2, \ldots$). Therefore due to Lemma 4 it contains a perfect subsequence and we can immediately suppose (removing some R_j's, and renaming afterwards) that $(C_n \cap R_{n+1}) \sqsubseteq$

$(C_n \cap R_{n+2}) \sqsubseteq (C_n \cap R_{n+3}) \sqsubseteq \dots$ is a perfect sequence. From each R_j, $j \geq n{+}1$, we now remove all but one element of $C_n \cap R_j$. Obviously, $R_{j_1} \not\sqsubseteq R_{j_2}$ will keep holding for any $j_1 < j_2$, and the other conditions of INV(n) are not affected by this change either. We have achieved that $C_n \cap R_j$ are singletons, and surely, $C_n \cap R_{n+1}, C_n \cap R_{n+2}, C_n \cap R_{n+3}, \dots$ again contains a perfect subsequence, so we can again immediately suppose that $(C_n \cap R_{n+1}) \sqsubseteq (C_n \cap R_{n+2}) \sqsubseteq (C_n \cap R_{n+3}) \sqsubseteq \dots$ is a perfect sequence. We denote the single element of $C_n \cap R_j$ as (n, j) (for all $j \geq n{+}1$); thus we have $(n, n+1) \preceq (n, n+2) \preceq (n, n+3) \preceq \dots$. Moreover, $(n, j+\ell) \not\preceq (n, j)$ for all $j \geq n{+}1$, $\ell \geq 1$; this follows from the condition 2. of minimal bad sequence.

Now we get rid of excessive elements, i.e., we remove all elements from R_n except for $(0, n), (1, n), \dots, (n{-}1, n)$, and we are almost done. We have achieved a further row, namely R_n, and a further column, namely C_n, and it is straightforward to verify that $(RSS(n{+}1), \preceq)$ is the Rado substructure with $n{+}1$ columns. Condition 2. is also clear, but we still need to guarantee condition 3., i.e., $(\forall i < n)(\forall x \in REST(n{+}1)) : (i, n) \preceq x$. We shall achieve this by the following process, which can not affect the other conditions of INV$(n{+}1)$:

Let us fix some $y \in R_n = \{\, (0, n), (1, n), \dots, (n{-}1, n) \,\}$, and denote $U_y = \{\, z \in REST(n{+}1) \mid y \not\preceq z \,\}$. If elements of U_y are not present in almost all R_j's (for $j \geq n{+}1$) then we can get rid of them by removing all R_j's containing them. Otherwise we can suppose that all $R_{n+1} \cap U_y$, $R_{n+2} \cap U_y$, $R_{n+3} \cap U_y$, $\dots$ are nonempty, and moreover we can suppose them to contain, or better immediately to be, a perfect sequence (recalling minimality of $R_0, R_1, R_2, \dots$ and Lemma 4). But then simple removing of elements of $R_j \cap U_y$ from R_j $(j \geq n{+}1)$ keeps all the achieved conditions of INV$(n+1)$ (in particular, it can not affect $R_{j_1} \not\sqsubseteq R_{j_2}$ for $j_1 < j_2$), and guarantees that $\forall x \in REST(n{+}1) : y \preceq x$. After repeating this modification for each $y \in \{\, (0, n), (1, n), \dots, (n{-}1, n) \,\}$ we achieve the desired property 3. and we are done. $\square$

Now we give some remarks to justify the used characterization of ω^2-wqo. A *sequence* of elements of a qo $(A, \preceq)$ *with length* α, for an ordinal α, is a function $f : \alpha \to A$. For two sequences f, g (possibly with different lengths), we define $f \preceq g$ iff there is a strictly increasing function $\psi : \operatorname{dom} f \to \operatorname{dom} g$ s.t. $\forall \beta \in \operatorname{dom} f : f(\beta) \preceq g(\psi(\beta))$. We can find in [6] (Theorem 1.11.) that a wqo A does not contain the Rado structure iff A^ω (the set of sequences with length ω) is wqo. The latter is equivalent to $A^{<\omega^2}$ (the set of sequences with length less than ω^2) being wqo; the equivalence follows from Higman's Theorem (A wqo implies $A^* = A^{<\omega}$ wqo) which can also be found in [6]. And the last condition is equivalent to A being ω^2-wqo due to [5] (Theorem 2.8.).

We should also remark that the Rado structure as given by Milner [6] differs from our definition above: it stipulates $(j_1 \leq i_2)$ instead of $(j_1 < i_2)$ (and is thus not directly suitable for our aims). But that causes no problem since, denoting "Milner sense qo" by $\leq_{Mil}$ and "our sense qo" by $\leq_{our}$, we have $(i_1, j_1) \leq_{our} (i_2, j_2) \Leftrightarrow (i_1, j_1{+}1) \leq_{Mil} (i_2, j_2{+}1)$ and $(i_1, j_1) \leq_{Mil} (i_2, j_2) \Leftrightarrow (2i_1{+}1, 2j_1) \leq_{our} (2i_2{+}1, 2j_2)$. Hence "our structure" can be found in "Milner's structure" and vice versa.

3 Additional Remarks

The results in [5] imply, e.g., that any well ordering is ω^2-wqo, and that we have the following ("Higman-like") closure property: if $(A, \preceq)$ is ω^2-wqo then $(A^*, \preceq)$ is ω^2-wqo. These, and similar, facts can be used to show that a given qo is ω^2-wqo; in other words, the "practical" techniques used for proving that a qo is wqo show that the relevant qo is ω^2-wqo, in fact. Moreover, deep results of wqo theory point to a still finer notion—namely *better quasi-ordering, bqo*—as to "the right notion", since it has very strong closure properties and all "naturally arising" wqo's seem to be bqo's (see also the survey [6]).

Remark. Bqo is also defined by the absence of a "bad pattern", which resembles the above definition of wqo. Nevertheless, to describe (and understand) the bad pattern is technically much more complicated.

The strength of bqo's is also illustrated by the related result—$(A, \preceq)$ is bqo iff $(\mathcal{P}(A), \sqsubseteq)$ is bqo—which was announced by Alberto Marcone in the below mentioned email discussion.

Acknowledgements

I thank Parosh Abdulla for posing the question with its motivation, for further discussions on the topic, and for initiating a very useful email discussion with Alberto Marcone, who was also the first to show that the Rado example contradicts the conjecture "$(A, \preceq)$ wqo $\Rightarrow$ $(\mathcal{P}(A), \sqsubseteq)$ wqo". My thanks also go to Faron Moller for his interest and discussions, and to anonymous referees for some useful remarks.

References

[1] Abdulla P.A., Čerāns K., Jonsson B., Yih-Kuen T. (1996). General decidability theorems for infinite-state systems; in Proc. 11th IEEE Int. Symp. on *Logic in Computer Science*, pp. 313–321. (To appear in *Information and Computation*.)

[2] Abdulla P.A., Jonsson B. (1998). Verifying networks of timed processes; in Proc. 7th Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'98), *Lecture Notes in Computer Science*, Vol. 1384, Springer-Verlag, pp. 298–312.

[3] Abdulla P.A., Jonsson B. (1998). Ensuring Completeness of Symbolic Verification Methods for Infinite-State Systems. To appear in *Theoretical Computer Science.*

[4] Finkel A., Schnoebelen Ph. (1998). Fundamental structures in well-structured infinite transition systems; in Proc. 3rd Latin American Theoretical Informatics Symposium (LATIN'98), *Lecture Notes in Computer Science*, Vol. 1380, Springer-Verlag, pp. 102–118.

[5] Marcone A. (1994). Foundations of bqo theory; in *Transactions of the AMS*, Vol. 345, No. 2,, pp. 641–660.

[6] Milner E.C. (1985). Basic wqo- and bqo-theory; in I. Rival (ed.), Graphs and Orders, D. Reidel Publishing Company, pp. 487–502.