A Note on a Parameterized Version of the Well-Founded Induction Principle *

Bernhard Gramlich **
Fachbereich Informatik, Universität Kaiserslautern
Postfach 3049, 67653 Kaiserslautern, Germany
gramlich@informatik.uni-kl.de

May 23, 1995

SEKI-Report SR–95–08 (SFB)

Abstract

The well-known and powerful proof principle by well-founded induction says that for verifying $\forall x : P(x)$ for some property P it suffices to show $\forall x : [[\forall y < x : P(y)] \implies P(x)]$, provided $<$ is a well-founded partial ordering on the domain of interest. Here we investigate a more general formulation of this proof principle which allows for a kind of parameterized partial orderings $<_x$ which naturally arises in some cases. More precisely, we develop conditions under which the parameterized proof principle $\forall x : [[\forall y <_x x : P(y)] \implies P(x)]$ is sound in the sense that $\forall x : [[\forall y <_x x : P(y)] \implies P(x)] \implies \forall x : P(x)$ holds, and give counterexamples demonstrating that these conditions are indeed essential.

1 Introduction and Motivation

In proofs by well-founded induction (cf. e.g. [Coh65], [Fef77], [MW93]) one usually tries to verify

$$\forall\, x : P(x) \tag{1}$$

by showing

$$\forall\, x : [\,[\forall\, y < x : P(y)\,] \implies P(x)\,] \tag{2}$$

where $<$ is a fixed well-founded partial ordering on the domain of interest. In fact, $<$ need not be a partial ordering. Any well-founded or terminating relation suffices.

*This paper is a revised and extended version of the contribution in *Bulletin of the EATCS* 52, pp. 274–277, February 1994.

**This research was supported by the 'Deutsche Forschungsgemeinschaft, SFB 314 (D4-Projekt)'.

Definition 1.1 (cf. e.g. [Wec92]) Let R be a (binary) relation on a set A.

- Let B be a non-empty subset of A. An element $b \in B$ is said to be *R-minimal* (or simply *minimal*) if, for all $a \in A$, bRa implies $a \notin B$.
- R is called *well-founded* (or *Noetherian*) if every non-empty subset of A has a minimal element.[1]
- R is called *terminating* if there is no infinite sequence $(a_n)_{n \in \mathbb{N}}$ such that $a_n R a_{n+1}$ for all $n \in \mathbb{N}$.

Well-foundedness and termination are equivalent notions. Well-foundedness obviously implies termination, and the reverse direction is also easy but requires the *Axiom of (Dependent) Choice* (cf. e.g. [Jec77]).

Theorem 1.2 (cf. e.g. [Wec92])
A (binary) relation is well-founded if and only if it is terminating.

In practice, i.e. when trying to apply the general principle of proof by well-founded induction, it often occurs that an appropiate well-founded partial ordering either is not available or unknown, or – if some partial ordering seems to be an obvious candidate – its well-foundedness is not guaranteed or somehow depends on the property to be proved. To illustrate this situation consider the following simple example.

Example 1.3 Let $\mathcal{A} = (A, \rightarrow)$ be an *abstract reduction system (ARS)*, i.e. $\rightarrow \subseteq A \times A$ is a binary relation on A. Let us denote the transitive and the transitive-reflexive closure of $\rightarrow$ by $\rightarrow^+$ and $\rightarrow^*$, respectively. Joinability is denoted by $\downarrow$, i.e. if for $a, b \in A$ there exists $c \in \mathcal{A}$ with $a \rightarrow^* c \;{}^*\!\!\leftarrow b$ then this is denoted by $a \downarrow b$. $\mathcal{A}$ is said to be *confluent* or *has the Church-Rosser property (CR)* if for all $a, b, c \in A$ with $b \;{}^*\!\!\leftarrow a \rightarrow^* c$ we have $b \downarrow c$. $\mathcal{A}$ is *weakly (or locally) confluent* or *weakly Church-Rosser (WCR)* if for all $a, b, c \in A$ with $b \leftarrow a \rightarrow c$ we have $b \downarrow c$. $\mathcal{A}$ is *terminating* or *strongly normalizing (SN)* if there is no infinite reduction sequence $a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow \ldots$ in $\mathcal{A}$. The properties CR, WCR and SN can also be defined for elements of A in the obvious manner. For instance, SN(a) (for $a \in A$) means that there is no infinite reduction sequence in $\mathcal{A}$ starting with a, and CR(a), $a \in A$, means that for all $b, c \in A$ with $b \;{}^*\!\!\leftarrow a \rightarrow^* c$ we have $b \downarrow c$. A well-known and important basic result for ARSs is *Newman's Lemma ([New42]* which may be formulated as follows:

> Every strongly normalizing and locally confluent ARS $\mathcal{A} = (A, \rightarrow)$ is confluent (or more succintly: $\mathrm{SN}(\mathcal{A}) \wedge \mathrm{WCR}(\mathcal{A}) \implies \mathrm{CR}(\mathcal{A})$).

Usual proofs of this lemma proceed by well-founded induction taking $\rightarrow^+$ as the well-founded partial ordering needed for the induction principle to be valid. A stronger local version of Newman's Lemma may be stated as follows:

[1]Following common usage, we call a partial ordering relation denoted by $<$ *well-founded / terminating* if $> := <^{-1}$ is well-founded / terminating.

Every strongly normalizing element $a \in A$ in a locally confluent ARS $\mathcal{A} = (A, \to)$ is confluent (or more succintly: $\forall\, s \in A\, :\, \mathrm{SN}(s) \wedge \mathrm{WCR}(\mathcal{A}) \implies \mathrm{CR}(s)$).

A typical proof of this lemma might looks as follows:

Proof: Let $\mathcal{A} = (A, \to)$ be an ARS with $\mathrm{WCR}(\mathcal{A})$, and let $s \in A$ with $\mathrm{SN}(s)$ be given. Let $Q(x)$ (for $x \in A$) be defined by

$$Q(x) :\equiv \mathrm{CR}(x)\,.$$

We proceed by induction over x w.r.t. the ordering $> := >_s := \to^+ |_{G(s)\times G(s)}$, where the *reduction graph* $G(s)$ of s is given by $G(s) := \{t \in A \,|\, s \to^* t\}$, showing

$$\forall\, x \in A, x \leq s\, :\, Q(x)\,.$$[2]

Observe that we have $x > y \iff s \to^* x \to^+ y$, and $x \geq y \iff s \to^* x \to^* y$ (for the reflexive ordering $\geq$ corresponding to (the strict partial ordering) $>$). By the assumption $\mathrm{SN}(s)$ we know that $> = \to^+ |_{G(s)\times G(s)}$ is well-founded. Now, assuming $s \geq x$ and $y\, {}^*\!\!\leftarrow x \to^* z$, we have several cases. If y or z equals x, we are done. This includes the case that x is a minimal element w.r.t. $>$, i.e. irreducible. Otherwise, there exist $y', z' \in A$ with $y\, {}^*\!\!\leftarrow y' \leftarrow x \to z' \to^* z$. By $\mathrm{WCR}(x)$, which follows from $\mathrm{WCR}(\mathcal{A})$,[3] we know that there exists some u with $y' \to^* u\, {}^*\!\!\leftarrow z'$. By induction hypothesis for y' ($x > y'$ due to $s \to^* x \to y'$) we conclude that there exists some v with $y \to^* v\, {}^*\!\!\leftarrow u$ and the induction hypothesis for z' ($x > z'$ due to $s \to^* x \to z'$) yields the existence of some w with $y' \to^* u \to^* v \to^* w\, {}^*\!\!\leftarrow z\, {}^*\!\!\leftarrow z'$. Summarizing we get $y \to^* v \to^* w\, {}^*\!\!\leftarrow z$ as, hence $\mathrm{CR}(x)$ desired. ■

Note that in the above proof the ordering used for showing

$$\forall x \in B : Q(x)$$

with $B = \{x \in A \,|\, x \leq_s s\}$ depends on s and its well-foundedness was assumed before. A careful inspection of the proof which was done via the instantiated scheme

$$\forall x \in B : [\forall y <_s x : Q(y)] \implies Q(x) \tag{3}$$

reveals that in the induction step we could have also used the induction hypotheses

$$\forall y <_x x : Q(y)$$

[2]Note that in general the statement $\forall x \in A, x \leq s : Q(x)$ (with $\leq_s$ reflexive) is stronger than $Q(s)$ (although here both are equivalent)! In fact, it is well-known that in proofs by induction it is often easier to prove a stronger statement than the original one since this also provides stronger induction hypotheses.

[3]Obviously, the assumption $\mathrm{WCR}(\mathcal{A})$ in the local version of Newman's Lemma can even be weakened to $\mathrm{WCR}(\mathcal{G}(a))$ where $\mathcal{G}(s) = (G(s), \to |_{G(s)\times G(s)})$ is the *sub-ARS* of $\mathcal{A}$ determined by the element s.

instead of

$$\forall y <_s x : Q(y)$$

with $<_x$ defined by

$$u >_x v \iff s \to^* x \to^* u \to^+ v \,, \tag{4}$$

i.e., according to the instantiated scheme

$$\forall x \in B : [\forall y <_x x : Q(y)] \implies Q(x) \,. \tag{5}$$

Similarly, when defining $Q'(x)$ (for $x \in A$) by

$$Q'(x) :\equiv [\mathrm{SN}(x) \implies \mathrm{CR}(x)]$$

the dependence on well-foundedness of the applied partial ordering is incorporated in $Q'(x)$. Then, proving the local version of Newman's Lemma above amounts to showing

$$\forall x \in A : Q'(x)$$

which one might be tempted to accomplish by showing

$$\forall x \in A : [\forall y \in A, y <_x x : Q'(y)] \implies Q'(x) \tag{6}$$

with $<_x$ defined by $(u, v \in A)$:

$$u >_x v \iff x \to^* u \to^+ v \,. \tag{7}$$

Here, the proof of (6) is analogous to the proof of (5).[4]

2 A Parameterized Principle of Well-Founded Induction

Note that proceeding as sketched above presupposes in general correctness of the following induction principle which is parameterized by a family of (strict partial) orderings $<_x$:

$$\forall x : [\forall y <_x x : P(y)] \implies P(x) \tag{8}$$

The correctness of (8) is expressed by

$$[\forall x : [[\forall y <_x x : P(y)] \implies P(x)]] \implies [\forall x : P(x)] \tag{9}$$

and obviously depends on properties of the involved ordering relations $<_x$. As already mentioned, a careful inspection of the above proof for the local version of Newman's Lemma shows that essentially the same proof can be used for establishing (8) with P instantiated appropiately (by Q) and $<_x$ defined by (4). Hence, in this special case the induction scheme (8) is correct, i.e. (9) holds. So one may ask in general, under what conditions concerning the applied family of orderings $<_x$ and the involved predicate $Q(x)$ is (8) a correct induction principle as expressed by (9)? That correctness is not assured in general, can be seen from the following counterexamples.

[4] From an intuitive point of view one would usually prefer to proceed according to (3) (or (5)) since there the well-foundedness assumption and the statement to be proved are clearly separated, and thus easier to understand.

Example 2.1 Let $G = \{a, b\}$ be a set of two elements and $<_a$, $<_b$ be two partial orderings on G given by $<_a := \{(b, a)\}$, $<_b := \{(a, b)\}$. Moreover let Q be some unary predicate on G such that $\neg Q(a)$ and $\neg Q(b)$ hold, i.e. Q is neither satisfied for a nor for b. Then the induction principle (8) with P instantiated by Q becomes

$$\forall x \in G : [\forall y \in G, y <_x x : Q(y)] \implies Q(x) \tag{10}$$

which is equivalent to

$$[\,[\forall y <_a a : Q(y)\,] \implies Q(a)\,] \wedge [\,[\forall y <_b b : Q(y)\,] \implies Q(b)\,]$$

which in turn is, by definition of $<_a$, $<_b$, equivalent to

$$Q(b) \implies Q(a) \qquad \wedge \qquad Q(a) \implies Q(b)\,. \tag{11}$$

Note that due to the assumptions $\neg Q(a)$, $\neg Q(b)$ we obviously have that (11) holds. However,

$$\forall x \in G : Q(x)$$

is false, hence the instantiated version of the parameterized induction scheme (8) is incorrect, i.e.

$$[\forall x \in G : [\,[\forall y \in G, y <_x x : Q(y)] \implies Q(x)\,]\,] \implies [\forall x \in G : Q(x)\,] \tag{12}$$

is false.

Note that in the above example the parameterized ordering relations $<_a$, $<_b$ are clearly well-founded, but the ordering information of $<_a$, $<_b$ is 'contradictory'. The latter is not the case in the following example.

Example 2.2 Let $G = \{a_0, a_1, a_2, \ldots\}$ be a denumerable set with ordering relations $<_{a_i}$ (for $i \geq 0$) defined by

$$\begin{array}{ccccccccc}
a_0 & >_{a_0} & a_1 & >_{a_0} & a_2 & >_{a_0} & a_3 & >_{a_0} & a_4 & \ldots \\
 & & a_1 & >_{a_1} & a_2 & >_{a_1} & a_3 & >_{a_1} & a_4 & \ldots \\
 & & & & a_2 & >_{a_2} & a_3 & >_{a_2} & a_4 & \ldots \\
 & & & & & & \ldots & \ldots & \ldots & \ldots,
\end{array}$$

i.e. $<_{a_i}$ is defined by $<_{a_i} := \{(a_k, a_j) \mid k > j \geq i\}$. Moreover, for some unary predicate Q on G let $\neg Q(a_i)$ hold for all $i \geq 0$. Then the induction principle (8) with P instantiated by Q becomes

$$\forall x \in G : [\forall y \in G, y <_x x : Q(y)] \implies Q(x) \tag{13}$$

which holds since the induction hypothesis $[\forall y \in G, y <_x x : Q(y)]$ is never satisfied (note that for any $a_j \in G$ there exists $a_k \in G$ (choosing e.g. $k = j + 1$) with $a_k <_{a_j} a_j$ but not $Q(a_k)$).

Note that in this example the ordering information is somehow consistent, but $<_{a_i}$ is clearly not well-founded.

The previous examples motivate the following abstract correctness conditions for the parameterized induction principle (8):

$$\forall x, y : \; [y <_x x \implies <_y \subseteq <_x] \tag{14}$$

and

$$\forall x : \; [\neg P(x) \implies <_x \text{ is well-founded. }] \tag{15}$$

We shall show now that if both the "compatibility" condition (14) and the "well-foundedness" condition (15) hold, then the parameterized induction principle (8) is correct as expressed by (9).

Theorem 2.3 The principle of parameterized (well-founded) induction (8) is correct, i.e. (9) holds, provided that the "compatibility" condition (14) and the "well-foundedness" condition (15) are satisfied.

We shall present two alternative proofs for this result. The first one is a more direct one and works by contradiction, and the second one essentially shows that (8) is equivalent to the usual principle of well-founded induction using one fixed uniform well-founded ordering.

Proof: (by contradiction)
Assume that (14) and (15) are satisfied, and assume that (8) holds, but not (9). Hence, there exists some x with $\neg P(x)$, let's say x_0. Condition (15) implies that $<_{x_0}$ is well-founded. Now (8) implies in particular

$$[\forall y <_{x_0} x_0 \, : \, P(y)] \implies P(x_0)$$

which, due to $\neg Q(x_0)$, yields the existence of some $x_1 <_{x_0} x_0$ with $\neg P(x_1)$. Choosing $x = x_1$ in (8) and using $\neg P(x_1)$ we know that there is some $x_2 <_{x_1} x_1$ with $\neg P(x_2)$, and so on.[5] Hence, by (ordinary) induction (on the ordering of the natural numbers) we can conclude that (for every $i \geq 0$) there exists some x_i with $\neg P(x_i)$ and

$$x_0 >_{x_0} x_1 >_{x_1} x_2 >_{x_2} x_3 >_{x_3} x_4 \ldots .$$

Applying repeatedly condition (14) we get

$$x_0 >_{x_0} x_1 >_{x_0} x_2 >_{x_0} x_3 >_{x_0} x_4 \ldots .$$

But this means that $<_{x_0}$ is not well-founded, contradicting condition (15). ■

Proof: (by ordinary well-founded induction)
Assume that (14) and (15) are satisfied. Then we define a binary relation $<$ as follows:

$$u < v \quad :\iff \quad \neg P(v) \wedge u <_v v \, . \tag{16}$$

[5]Note that this actually requires the *Axiom of Choice*.

Next we show that $<$ is a well-founded partial ordering, i.e. it is irreflexive, transitive, and well-founded. Irreflexivity of $<$ follows from irreflexivity of $<_u$ for all u. For showing transitivity we have to show that $u < v$ and $v < w$ implies $u < w$. By definition of $<$ the assumption yields $u <_v v <_w w$. Using (14) we get $u <_w v <_w w$ which, by transitivity of $<_w$, implies $u <_w w$. From $v < w$ we get $\neg P(w)$, hence together this yields $u < w$. For proving well-foundedness of $<$ (by contradiction) assume that

$$u_0 > u_1 > u_2 > u_3 > \ldots$$

is an infinite decreasing $>$-chain. This implies

$$\forall i \geq 0 \, : \, \neg P(u_i)$$

and

$$u_0 >_{u_0} u_1 >_{u_1} u_2 >_{u_2} u_3 >_{u_3} u_4 \ldots$$

which, again by the compatibility condition (14), yields

$$u_0 >_{u_0} u_1 >_{u_0} u_2 >_{u_0} u_3 >_{u_0} u_4 \ldots .$$

But this means that $<_{u_0}$ is not well-founded contradicting (15). Hence, we conclude that $<$ is indeed a well-founded partial ordering, for which the principle of well-founded induction (2) is correct. Thus, substituting the definition of $<$ into (2) we obtain

$$\forall\, x : [\, [\forall y : \neg P(x) \wedge y <_x x \implies P(y)\,] \implies P(x)\,]$$

which is equivalent to

$$\forall\, x : [\, [\forall y : P(x) \vee \neg(y <_x x) \vee P(y)\,] \implies P(x)\,]$$

and to

$$\forall\, x : [\, [\, [\forall y : y <_x x \implies P(y)\,] \vee P(x)\,] \implies P(x)\,]$$

hence yielding

$$\forall\, x : [\, [\forall y, y <_x x : P(y)\,] \implies P(x)\,] .$$

Thus, correctness of the ordinary well-founded induction principle (2) implies correctness of the parameterized (well-founded) induction principle (8) under the conditions (14) and (15) as was to be shown. ∎

The counterexamples (2.1) and (2.2) above demonstrate that the "compatibility" condition (14) and the "well-foundedness" condition (15) cannot be dropped without loosing correctness of the principle of parameterized (well-founded) induction (8) in general. In our introductory Example 1.3 we observe that these two conditions are indeed satisfied. In fact, with $>_u$ defined by

$$x >_u y \iff s \to^* u \to^* x \to^+ y \ ,$$

compatibility means

$$x >_x y \implies >_x \supseteq >_y$$

or equivalently

$$x >_x y \implies [\forall u, v : u >_y v \implies u >_x v]$$

which holds, since $x >_x y$ and $u >_y v$ imply $s \to^* x \to^* x \to^+ y$, $s \to^* y \to^* u \to^+ v$, hence $s \to^* x \to^+ y \to^* u \to^+ v$ and thus $u >_x v$. The well-foundedness condition (15) is also satisfied, since every $>_x$ is well-founded by the global assumption SN(s).

Although the second proof of Theorem 2.3 reveals that (8) is not more powerful than ordinary well-founded induction, the parameterized induction principle (8) has the advantage that one may directly work with (8), i.e. with a family of ordering relations, which may arise quite naturally in certain cases. The only thing to be verified for correctness is to ensure that the abstract properties (14) and (15) are satisfied. Working directly with with (8) may be useful (from a conceptual point of view) for instance in inductive proofs by some counterexample x which is assumed to be minimal w.r.t. some well-founded ordering $>$, in the sense that w.l.o.g. x may be assumed to be minimal w.r.t. some (naturally defined) $>_x$ (instead of minimal w.r.t. $>$). This may be beneficial for the sake of better understanding the essence of the involved inductive reasoning, in particular in cases where the whole inductive proof is very complicated (see [Gra95] for a non-trivial example).

Finally let us mention that the two conditions (14) and (15) are only one possibility for guaranteeing correctness of (8). Indeed, let us consider the following modification of Example 2.2.

Example 2.4 Let $G = \{a_0, a_1, a_2, \ldots\}$ be a countable set with ordering relations $<_{a_i}$ (for $i \geq 0$) defined by

$$>_{a_i} := \{(a_i, a_{i+1})\} \ .$$

Moreover, for some unary predicate Q on G let $\neg Q(a_i)$ hold for all $i \geq 0$. Then the induction principle (8) with P instantiated by Q becomes

$$\forall x \in G : [\forall y \in G, y <_x x : Q(y)] \implies Q(x) \qquad (17)$$

which holds since the induction hypothesis $[\forall y \in G, y <_x x : Q(y)]$ is never satisfied (note that for any $a_j \in G$ we have $a_{j+1} <_{a_j} a_j$ but not $Q(a_{j+1})$). Hence,

$$[\forall x : [[\forall y <_x x : P(y)] \implies P(x)]] \quad \implies \quad [\forall x : P(x)]$$

is obviously incorrect in this case.

In this example, the ordering relations $(>_{a_i})_{i \geq 0}$ are all well-founded, and compatible in the sense that combining any two $>_{a_i}$, $>_{a_j}$ of them (or even finitely many $>_{a_k}$) still yields a well-founded relation. However, the problem is, that $\bigcup_{i\geq 0} >_{a_i}$ is not well-founded any more. In fact, the crucial point for correctness of (8) is that an infinite sequence of the form

$$x_0 >_{x_0} x_1 >_{x_1} x_2 >_{x_2} x_3 >_{x_3} x_4 \ldots .$$

issuing from some counterexample x_0 (i.e. with $\neg P(x_0)$) is impossible (cf. the (first) proof of Theorem 2.3). To ensure this property, one might require instead of (14), (15) the following more general condition:

$$\forall x_0 : \; [\neg P(x_0) \Longrightarrow (\bigcup_x >_x)_{below\, x_0} \text{ is well-founded}] \tag{18}$$

where, for some binary relation R, $R_{below\, y}$ is given by

$$R_{below\, y} \;=\; R \cap \{(u,v) \,|\, yR^*uRv\} = R|_{\{z \,|\, yR^*z\}^2} \;.$$

Then the proof(s) of the modified version of Theorem 2.3 go through as well,[6] just as before.

In order to ensure correctness of (8) as a general scheme – and not only of specific instances of (8) as considered above and in particular in Theorem 2.3 – one simply has to require well-foundedness of

$$\bigcup_x >_x \;\; .$$

Acknowledgements: I would like to thank Claus-Peter Wirth for useful comments on a draft version of this paper.

References

[Coh65] P.M. Cohn. *Universal Algebra*, volume 6 of *Mathematics and Its Applications*. D. Reidel Publishing Company, Dordrecht: Holland, Boston: USA, London: England, 1965.

[Fef77] S. Feferman. Theories of finite type related to mathematical practice. In J. Barwise et al., editor, *Handbook of Mathematical Logic*, volume 90 of *Studies in Logic and The Foundations of Mathematics*, chapter D.4., pages 913–971. North Holland, Amsterdam, New York, Oxford, 1977.

[Gra95] B. Gramlich. On termination and confluence of conditional rewrite systems. In N. Dershowitz and N. Lindenstrauss, editors, *Proc. 4th Int. Workshop on Conditional (and Typed) Term Rewriting Systems (1994)*, *Lecture Notes in Computer Science*, to appear, 1995.

[6] Note that any well-founded (binary) relation can be turned into a well-founded (strict partial) ordering, simply by taking the transitive closure. Thus, for proofs by well-founded induction, it does not really matter whether the underlying well-founded relation is an ordering or not, since transitivity can always be enforced.

[Jec77] T.J. Jech. About the Axiom of Choice. In J. Barwise et al., editor, *Handbook of Mathematical Logic*, volume 90 of *Studies in Logic and The Foundations of Mathematics*, chapter B.2., pages 345–370. North Holland, Amsterdam, New York, Oxford, 1977.

[MW93] Z. Manna and R. Waldinger. *The Deductive Foundations of Computer Programming.* Addison Wesley, 1993.

[New42] M.H.A. Newman. On theories with a combinatorial definition of equivalence. *Annals of Mathematics*, 43(2):223–242, 1942.

[Wec92] W. Wechler. *Universal Algebra for Computer Scientists*, volume 25 of *EATCS Monographs on Theoretical Computer Science.* Springer-Verlag, 1992.