Termination
Lecture 2 – Games

Readings

- Assigning Meaning to Programs", Floyd
- "Proving Termination with Multiset Orderings"

Overview

- Well-founded Orderings
- Multiset Orderings
- Nested Multiset Orderings

Proving Termination using Invariants-reminder

Consider the following program(Turing's program):

```
r=1,u=1
while r≤n :
        v=u
        s=1
        while s≤r:
                u=u+v
                s=s+1
        r=r+1
```

Note: Recall that termination of this program can be shown by induction on both outer and inner loop

Ackerman Function

Defined as followed, for non-negative integers:

a(0,n)=n+1

a(m,0)=a(m-1,1)

a(m,n)=a(m-1,a(m,n-1))

Ackerman function is increasing rapidly, for example:

Values of A(*m*, *n*)

*m**n*	0	1	2	3	4	n
0	1	2	3	4	5	$n+1$
1	2	3	4	5	6	$n+2=2+(n+3)-3$
2	3	5	7	9	11	$2n+3=2\cdot(n+3)-3$
3	5	13	29	61	125	$2^{(n+3)}-3$
4	13 $=2^{2^2}-3$	65533 $=2^{2^{2^2}}-3$	$2^{65536}-3$ $=2^{2^{2^{2^2}}}-3$	$2^{2^{65536}}-3$ $=2^{2^{2^{2^{2^2}}}}-3$	$2^{2^{2^{65536}}}-3$ $=2^{2^{2^{2^{2^{2^2}}}}}-3$	$\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n+3}-3$

Proving Ackerman's Function termination

We shall prove that ackerman function terminates , using double induction.

Base case: termination of a(0,n): for all $n \in N$ a(0,n)=(n+1).

Step: Assume some $m \in N$ and assume that a(m,n) is terminating for all $n \in N$, we'll prove that a(m+1,n) is terminating as well.

We will do this by inner induction on n.

If n=0, then we have a(m+1,0)=a(m,1) which is terminating by the hypothesis.

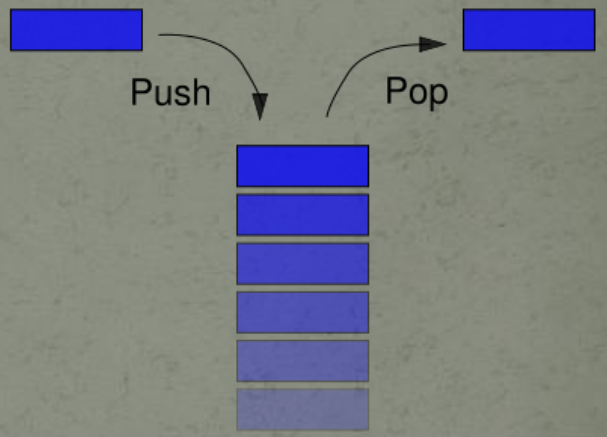
Assume n=n'+1, then we have a(m+1,n)=a(m,a(m+1,n')).

By the inner induction hypothesis, a(m+1,n') is terminating with some value x, thus a(m,a(m+1,n'))=

a(m,x), which terminates by outer induction hypothesis.⊠

Ackerman using stack

```
A(m,n):
    Init-stack(s)
    push(m,s)
    while not_empty(s)
            m=pop(s)
            if m=0
                        n=n+1
            else
                        if n=0
                                    n=1
                                    push(m-1,s)
                        else
                                    n=n-1
                                    push(m-1,s)
                                    push(m,s)
Return n
```



We will prove termination of this implementation later today , using multiset orderings

Orderings

- Definition: We will say that a binary relation, R, is a partial order over a set A, if R has the following properties:

- R is **irreflexive**
  $\forall a \in A. \neg R(a,a)$
- R is **asymmetric**
  $\forall a,b \in A. R(a,b) \wedge R(b,a) \Rightarrow a = b$
- R is **transitive**
  $\forall a,b,c \in A. R(a,b) \wedge R(b,c) \Rightarrow R(a,c)$

Orderings (Well-Founded)

Let A be a set and R be a binary relation over it,

If R is partial-order over A, and there is no infinite descending chain of elements in A (descending in the meaning of the relation R), we will say that (A,R) is well-founded.

Examples:

(N, >) : if k is the first element in the descending chain, then the chain contains at most k elements.

(Z-, <)

(Finite Trees , sub tree)

(NxN, lexicographic) -will be defined in the next slide

Couples-relations

There are few ways to compare between tuples of elements:

$\overset{?}{>}$

-Lexicographic: (a,b)>(a',b') if and only if

$$a > a' \vee (a = a' \wedge b > b')$$

-Component-wise: (a,b)>(a',b') if and only if

$$(a \geq a' \wedge b > b') \vee (a > a' \wedge b \geq b')$$

-Reverse Lexicographic: (a,b)>(a',b') if and only if

$$(a > a' \wedge b = b') \vee (b > b')$$

Mixed Couples

- If v and w are well-founded, then their pairs VxW are well-founded lexicographically.

Proof:

Assume by contradiction that VxW are not well-founded lexicographically, then there exists an infinite chain $(v_1, w_1) > (v_2, w_2) > (v_3, w_3) > \ldots$

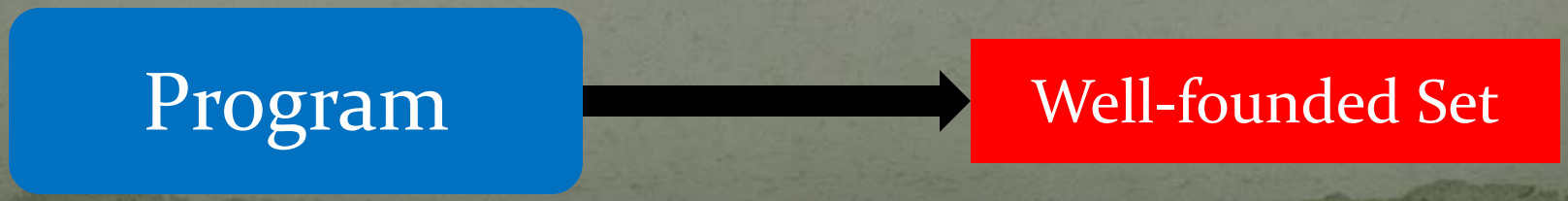
Hence, either V or W has an infinite descending chain of elements, making it not well-founded, contradiction. ⊠

Proving Termination using well-founded sets

In the next slides we will prove termination of programs using well-founded orderings.

But how?

The idea is to find a well-founded set and a termination function, that maps the value of the program variables into that set, such that the value of the termination function is repeatedly decreased throughout the computation. Since, by the definition of the set, the value cannot decrease indefinitely➔ the program must terminate.



Proving Termination using well-founded orderings- basic Ackerman function

a(0,n)=n+1

a(m,0)=a(m-1,1)

a(m,n)=a(m-1,a(m,n-1))

Termination proof:

We will use the pair (m,n) from the definition above, with lexicographic ordering. Both m and n are natural numbers, therefore $(m,n) \in NxN$,which is well-founded. With each phase of the function, the lexicographic value of the tuple decreases➔ termination is guaranteed.⊠

Proving Termination using well-founded orderings- Turing's program

Recall Turing's program from the beginning of the lecture

We will choose (n-r,r-s) as our pair, with lexicographic ordering.

With every iteration of the inner loop , s is incremented, until s=r, hence r-s decreases(while n-r is static), so the couple value will decrease.

With every iteration of the outer loop, r is incremented, until n=r, hence n-r decreases(in this case, we don't care that r-s increased, since the pair is ordered lexicographic), therefore the couple value will decrease

Hence, the program will terminate. ☒

```
r=1,u=1
while r≤n :
        v=u
        s=1
        while s≤r:
                u=u+v
                s=s+1
        r=r+1
```

Proving Termination using well-founded orderings- Dutch National Flag

Dutch National Flag problem:

- Input: a series of marbles, colored red, white and blue, placed side by side in no particular order:

- Output: the marbles sorted according to the Dutch flag(more or less ☺):

Dutch National Flag Program:

White,Red ➔ Red,White

Blue,Red ➔ Red,Blue

Blue,White ➔ White,Blue

The above rules may be applied in any order and to any pair of marbles matching a left-hand side of a rule.

The first rule, for example, states that if anywhere in the series there is a pair of marbles, the left one white and the right one red, then they should exchange places.

Clearly, if no rule can be applied, the marbles are in the desired order.

The only thing we need to assert is that the above program terminates.

Dutch National Flag Program Termination Proof

We will show termination of this program using a well-founded ordering.

We will use the binary relation between colors, defined as:

Blue>White>Red.

First, note that this relation is exactly the opposite of the desired order, in order to guarantee that our program value decreases with each phase.

Clearly, the above relation is well-founded.

Assume we have n marbles, we will map them to an n-tuple of colors, for example, the following order from the previous slide:

Will be mapped to the tuple (B,R,W,W,R,B,R),

Note that, for any rule of the program we apply, the tuple value will decrease lexicographically.

Since the tuple can't decrease indefinitely, termination is guaranteed. ☒

Multiset Orderings

- For a given partially-ordered set (S,>), where S is a set of elements, and “>” is a relation on S, we denote by M(S) the set of all finite multisets with elements taken from the set S. (note that unlike a regular set, a multiset may contain the same element more than once).
- For a partially-ordered set (S,>), we will define a multiset ordering >>, on M(S), defined as follows:
- M>>M’ if and only if there exists $A, B \in M(S)$, where

$$A \neq \phi, A \subseteq M \quad M' = (M - A) \cup B \quad \forall b \in B. \exists a \in A. (a > b)$$

- In other words, we will say that M>>M’ if and only if M’ can be achieved from M by the removal of at least one element, and replacing them by a finite number of elements- each of which is smaller than one of the elements that were removed.

Multiset Orderings-Examples

- Example: Assume S=N, with the regular binary relation "<"

Then , the following holds:

- $\{0,1,2,3,4\} \ll \{5\}$
- $\{5\} \ll \{5,5\}$
- $\{2,3,4\} \ll \{1,2,3,4\}$
- $\{5,6,7\} \ll \{1,3,8\}$

Konig's Lemma

Konig's Lemma: If G is connected graph, with infinite many of vertices, such that every vertex has a finite degree (degree of a vertex is defined to be the number of edges to other vertices), then G contains an infinite long simple path.

Proof: We will show that there exists an infinite sequence of vertices, $v_0, v_1, v_2 \ldots$ such that:

-v_0 is the root node

-v_{n+1} is a child of v_n

-each v_n has infinitely many descendants

It will follow that $v_0, v_1, v_2 \ldots$ Is such a simple path of infinite length.

Konig's Lemma-Proof

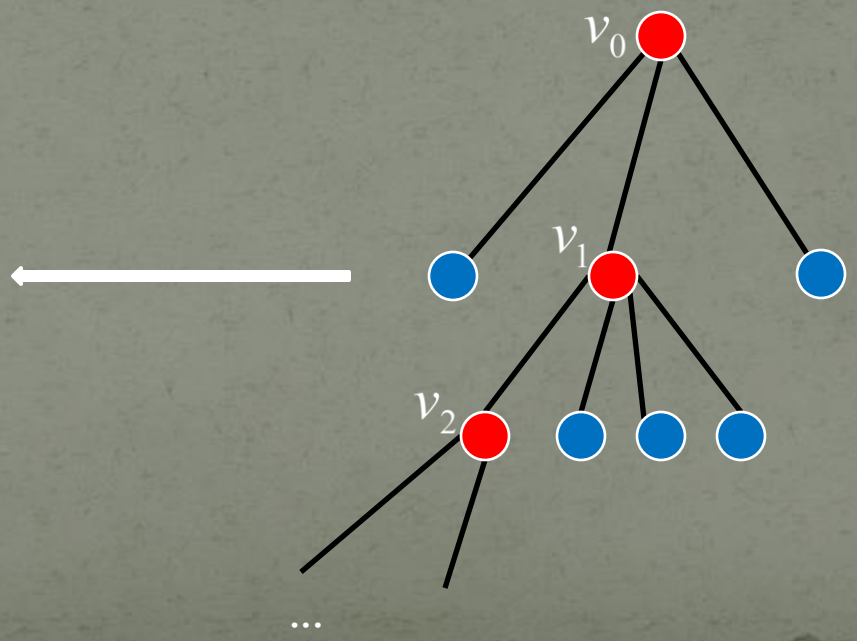
Choose some v_0 arbitrary, by definition it has a finite number of children.

Suppose that all of these children had a finite number of descendants, then that would mean that v_0 had a finite number of descendants, making G finite.

Hence , there exists some v_1, such that v_1 is a child of v_0, and v_1 has infinite many descendants.

We'll continue in the same fashion from v_1 , creating an infinite long path. ⊠

One of these has an infinite many of descendants



Back to Multiset Orderings

- **Theorem** : The Multiset ordering (M(S),>>) over (S,>) is well-founded if and only if (S,>) is well-founded.

Proof:

➔Assume (S,>) is not well-founded, we will show that (M(S),>>) is not well-founded by showing an infinite decreasing chain.

Since (S,>) is not well-founded, there exists an infinite long decreasing sequence of elements: $s_1 > s_2 > s_3 > \ldots$.

The sequence $\{s_1\} >> \{s_2\} >> \{s_3\} >> \ldots$ forms an infinite descending sequence of elements in M(S), therefore (M(S),>>) is not well-founded.

Multiset are well-founded – Proof

- Assume that (S,>) is well-founded. And let $S' = S \cup \{x\}$, such that x is a new element (meaning $x \notin S$), and:

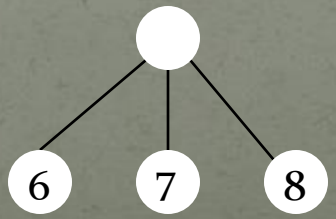
$\forall y \in S.y > x$,clearly, (S',>) is well-founded.

Suppose by contradiction that (M(S),>>) is not well-founded, therefore there exists an infinite descending sequence

$M_1 >> M_2 >> M_3 >> \ldots$

We will construct the following tree:

Each node in the tree is labeled with some element of S', at each stage of the construction , the set of all leaf nodes in the tree forms a multiset in M(S'). Begin with a some root node, and define his children to be all of the elements in M1 (for example, assume M1={6,7,8}), after the first step our tree will be:



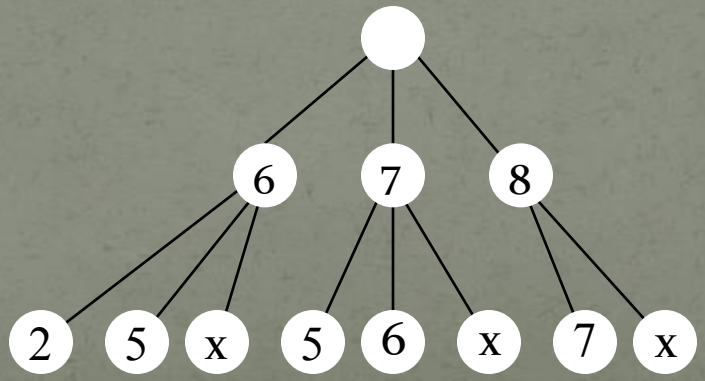
Multiset are well-founded – Proof

- Since $M_1 >> M_2$,then for every element ‘u’ in M_2 , which is not in M_1 , there exists an element ‘v’ in M_1 such that v>u, we will set u as the child of v.

In addition, grow a child x (the new added element) from each element v, that grew a new child, u.

Note: If there are no new elements in M_2 (which are not in M_1) , then that means that we simply “deleted” some elements from M_1 in order to get M_2, then simply grow a child x from each deleted element.

For example, if M_2 ={6,7,8} as before, and M_1 ={2,5,5,6,7} than our tree may look like:



Multiset are well-founded – Proof

We'll repeat this process with M_2 , M_3 and so on…

Clearly, the number of children (degree) of each node is finite.

Since at least one node is added to the tree for each multiset M_i (x) and there are infinite $M_i's$, the tree is infinite.

But by Konig's Infinity Lemma, an infinite tree (with a finite number of children – degree, for each node), must have an infinite path.

Therefore our tree contains an infinite long simple path.

But notice that any path in the tree is decreasing (the value of the nodes)➔ There exists an infinite decreasing chain of elements in S' , which is a contradiction, since S' is well-founded.

Hence, (M(S),>>) is indeed well-founded.⊠

Back to Ackerman

Let's recall the Ackerman function computation using a stack:

```
A(m,n):
    Init-stack(s)
    push(m,s)
    while not_empty(s)
            m=pop(s)
            if m=0
                    n=n+1
            else
                    if n=0
                            n=1
                            push(m-1,s)
                    else
                            n=n-1
                            push(m-1,s)
                            push(m,s)
Return n
```

Ackerman using Stack-termination

We will use a multiset of tuples $\{(a_1, b_1), (a_2, b_2)...\}$, which are compared lexicographically.

We will have an amount of tuples, that is corresponding to the amount of elements in the stack at that time, for example, if the stack is $\{s_1, s_2...., s_k\}$, where s_1 is the top of the stack ,then our tuple-multiset will be:

$\{(s_1, n), (s_2, \infty), ...(s_k, \infty)\}$,note that these tuples are well-founded, since any " ∞ " can only descend to a natural number.

We will show that for each phase of the loop, the multiset value is decreasing, that will guarantee termination.

Ackerman using Stack-termination

We'll look at some iteration of the loop:

First, we pop some element m, thus, we remove the element (m,n) from the multiset. Assume $\{(m,n),(m',\infty)...,t_k\}$ is the multiset, before the loop iteration.

If we use the first "if" branch, then afterwards, our multiset will be $\{(m',n+1)...t_k\}$, since we "popped" m from the stack, meaning removing (m,n) from the multiset (and pushing nothing in return). Since $(m',\infty) > (m',n+1)$,our multiset decreased.

If we use the second "if" branch, then afterwards, our multiset will be $\{(m-1,1),(m',\infty)...t_k\}$ which is of course $<\{(m,0),(m',\infty)...t_k\}$, since (m,0)>(m-1,1).

If we use the third "if" branch, then afterwards, our multiset will be $\{(m,n-1),(m-1,\infty),(m',\infty)...t_k\}$,and it is smaller than $\{(m,n),(m',\infty)...,t_k\}$,since both (m,n)>(m,n-1) and $(m,n) > (m-1,\infty)$.

In any case, our multiset decreased ☒

```
A(m,n):
    Init-stack(s)
    push(m,s)
    while not_empty(s)
        m=pop(s)
        if m=0
            n=n+1
        else
            if n=0
                n=1
                push(m-1,s)
            else
                n=n-1
                push(m-1,s)
                push(m,s)
    Return n
```

Nested Multisets

We now turn to consider nested multisets, by which we mean that the elements of the multisets may belong to some base set S, or may be multisets of elements of S, or may be multisets containing both elements of S, and multisets of elements of S, and so on… for Example:

{ {1,1}, {{0},1,2}, 0} is a nested multiset.

Formally, a nested multiset over S is either an element of S, or else it is a finite multiset of nested multisets over S.

We denote by M*(S) the set of nested multisets over S.

Nested Orderings

Now, we shall define a nested multiset ordering >>*, on M*(S), it is a recursive version of the standard multiset ordering.

We will say that M >>* M' if one of the following holds:

- $M, M' \in S$, and M>M' by the regular relation ">" over S.
- $M \notin S, M' \in S$ – meaning that any multiset is greater than any element of the base set.
- $M, M' \notin S$, and $\exists A, B \in M^*(S)$ where $A \neq \phi, A \subseteq M$, and the following holds: $M' = (M - A) \cup B$, and

$\forall b \in B. \exists a \in A. a >> * b$

Nested Ordering-Examples

- Examples:
- {{1,1},{{0},1,2},0} >>* {{1,0,0},5,{{0},1,2}, 0}, since {1,1} >>*5,0,{1,0,0}
- {{1,1},{{0},1,2},0} >*> {{{ },1,2},{5,5,2},5} , since {{0},1,2} >>* {{ },1,2} and of course {{0},1,2} >>* {5,5,2}, 5.
- Let $M^i(S)$ denote the set of all nested multisets of "depth" i. In other words, $M^0(S) = S$,and $M^{i+1}(S)$ contains the multisets whose elements are taken from $M^0(S)...M^i(S)$

Nested Multisets Depth

Property:

For two nested multisets, M and M', if the depth of M is greater than the depth of M', then M >>* M'

Proof:

We will prove this property by induction on the depth of M. It clearly holds for depth 0.

For the inductive step, assume that nested multisets of depth i are greater than nested multisets of depth less than i, we must show that nested multiset M of depth i+1, is greater than any nested multiset M' of depth<i+1 .

If the depth of M' is 0, $M \notin S, M' \in S$, so M>>*M' is by definition.

Therefore assume the depth of M' is k, where 0<k<i+1, then each element in M' is of depth < i . M, on the other hand, is of depth i+1, therefore must contain an element, x, of depth i, by the induction hypothesis, x, is greater than every element in M', it follows that M>>*M'. ⊠

Nested Multisets are well-founded

Theorem: The nested multiset ordering (M*(S),>>*) over (S,>) is well-founded , if and only if (S,>) is well-founded.

Proof:

➔Assume (S,>) is not well-founded, then there exists an infinite chain of descending elements in S, $S_1 > S_2 > S_3 > \ldots$

This exact sequence is also an infinite descending sequence of elements in M*(S) with >>*, therefore (M*(S),>>*) is not-well founded.

Nested Multisets are well-founded

- If there exists an infinite descending chain $M_1 >>* M_2 >>* M_3 >>* \ldots$,and M_1's depth is k, then all $M_2, M_3 \ldots$ are of depth ≤k (by the property we proved)

Therefore ,there exists some $0<i\leq k$ such that there is an infinite descending chain of M's in depth i, therefore if we prove that $M^i(S)$ is well-founded, for all i, it follow that M*(S) is well founded.

Hence, we shall prove prove that $M^i(S)$ is well-founded by induction on i.

If i=0, then $M^i(S) = M^0(S) = S$, which is well-founded.

Therefore, assume that $(M^j(S), >>*)$ is well-founded, for every j<i. Note that every element of $M^i(S)$,is a member of the union $M^0(S) \cup \ldots \cup M^{i-1}(S)$,by the induction hypothesis, each of these $M^j(S)$ is well founded under >>*, therefore, their union is also well-founded under >>*.

Since the ordering >>* on two nested elements in $M^i(S)$ is exactly the standard multiset ordering (that we showed before) over the above union, and since a multiset ordering is well-founded if the ordering on the elements is (proof in slide 24) , it follows that $M^i(S)$ is also well-founded under >>*. ⊠

Goodstein Sequences

The Goodstein sequence (named after Reuben Goodstein) , G(m), of a natural number m, is a sequence of natural numbers.

The first element in the sequence G(m) is m itself.

To get the next element in the sequence, write m in hereditary base 2 notation, change all the 2's to 3's, and then subtract 1 from the result. To get the third element of G(m), write the second element in hereditary base 3 notation, change all 3's to 4's, and subtract 1 again.

Continue in this fashion to get the complete sequence, once element 0 is reached, the sequence terminates.

Goodstein Sequence-Examples

Let's look at **G(3)**:

#Element	Base	Hereditary Notation	Value
1	2	2^1+2^0	3
2	3	$3^1+3^0-1=3^1$	3
3	4	$4^1-1=3*4^0$	3
4	5	$3*5^0-1=2*5^0$	2
5	6	$2*6^0-6^0=6^0$	1
6	7	7^0-1	0

Goodstein-another example

G(4):

4,26,41,60,83,109,139,173….1058,1151,1222,1295….3407,11115,11327…,40492,40985,…,154349,162129585780031489,162129585853378 55, $3*2^{402653210}-1$ …,2,1,0

Claim: Every Goodstein sequence eventually terminates at 0 (Reuben Goodstein himself proved it at 1944).

We will prove it using nested multisets.

Goodstein Sequence-Mapping to nested multisets

Consider the following Nested Multiset bag for each element in the sequence:

First, we will define a set, who contains the following elements:

For each number in the sequence, write it in the corresponding hereditary base, as a sum of powers (just as we did).

We'll show how to map every element of the sum to an element in the above set:

Assume the current base is k, and look at some element in the sum:

$m * k^l$,this element maps to m sets, each containing the element l (note that the power l, may also be an element with base k, in this case , the element will be mapped to a nested multiset).

Don't Worry, an example is on the way ☺!

Goodstein Sequence-Mapping to nested multisets

Consider our first element is 19, which is $19 = 2^{2^{2^1}} + 2^1 + 1$

The multiset for this element, will be : **{ {{{1}}},{1}, 1 }**

{{{1}}} = $2^{2^{2^1}}$, why?

2^k , "opens" a set with k in it

But k is 2^{2^1} , then a new set is opened

With 2^1 in it, then a new set is opened

With 1 in it , hence {{{1}}} is the corresponding bag!

{1}= 2^1, since 2^1 , is as defined, a set with 1 ,meaning {1}.

In the case of the simple "1", it is simply mapped to 1.

Goodstein Sequence-Mapping to nested multisets

Let's look back at G(3) , with the corresponding nested multiset to each element:

#Element	Base	Hereditary Notation	Value	Corresponding Nested multiset
1	2	2^1+2^0	3	{{1},{}}
2	3	$3^1+3^0-1=3^1$	3	{{1}}
3	4	$4^1-1=3*4^0$	3	{{},{},{}}
4	5	$3*5^0-1=2*5^0$	2	{{},{}}
5	6	$2*6^0-6^0=6^0$	1	{{}}
6	7	7^0-1	0	{}

Goodstein Sequence-Termination proof

Note that, if we wouldn't subtract 1 at each phase, then for all elements in some sequence, their nested multiset would be exactly the same!

But since we decrement 1 at each phase, the nested multiset will decrease.

Hence, the sequence will terminate (with {}=0).⊠