# Algorithmic Aspects of WQO Theory

[S. Schmitz & P. Schnoebelen, Lecture Notes, 2012]

## Complexity Upper Bounds

<u>Goal</u>: · Many algorithms rely on wqo arguments to prove termination (we saw Abdulla's backwards search).
· We want to obtain <u>complexity upper bounds</u> for such algorithms.

## Recall:

$(A, \leq)$ is a wqo iff every infinite sequence $(a_i)_{i \in \mathbb{N}}$ contains an <u>increasing pair</u> $a_i \leq a_j$ with $i < j$.

We call sequences with an increasing pair <u>good</u>, and sequences without <u>bad</u>.

Hence, every infinite sequence over a wqo is good, and every bad sequence over a wqo is finite.

<u>Key question</u>: How long can bad sequences be?
<u>Contribution</u>: Techniques to bound the length. Are very generic/powerful.
↳ Only the dimension/wqo and the complexity of operations matter.

<u>Example</u>:

<u>SIMPLE(a,b)</u>:
  c = 1;
  <u>while</u> $a > 0 \wedge b > 0$ <u>do</u>
    $l: (a,b,c) = (a-1, b, 2c)$
  $+$ $r: (a,b,c) = (2c, b-1, 1)$
  <u>od</u>

One can check that, in any run,
the sequence of values taken by a and b,

$(a_0, b_0), (a_1, b_1), \dots$

is a bad sequence over $(\mathbb{N}^2, \leq)$.
Since this is a wqo by Dickson's lemma,
the bad sequence is finite and so
SIMPLE$(a_0, b_0)$ terminates.

How long can it run?
Say $(a_0, b_0) = (2, 3)$.

$$\underset{\overset{\shortparallel}{1}}{(2,3,2^0)} \xrightarrow{\ell} (1,3,2^1) \xrightarrow{r} (2^2,2,1)$$

$$\xrightarrow{\ell^{2^2-1}.r} (2^{2^2},1,1)$$

$$\xrightarrow{\ell^{2^{2^2}-1}.r} (2^{2^{2^2}},0,1)$$

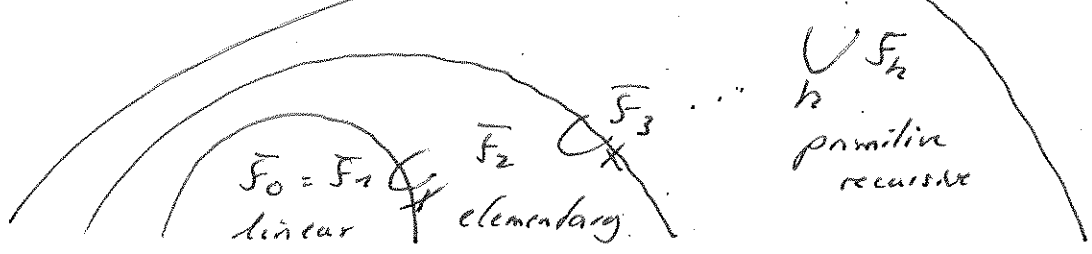
Has length

$$2 + 2^2 + 2^{2^2}.$$

This is non-elementary in the size of the initial values.

<u>Fact</u>:
- Linear operations and dimension 2 yield complexities beyond the elementary hierarchies.
- Distinctions between time and space complexity and non-determinism vs. determinism become irrelevant.
- A hierarchy of non-elementary complexity useful here is this

<u>Grzegorczyk hierarchy</u>:



In the case of SIMPLE, there is a function in $\mathcal{F}_3$ that bounds the length of all runs.

## The Length of Controlled Bad Sequences

Problem: Consider $(\mathbb{N}^2, \leq)$.

Then
$$\overset{x_0}{\overset{\shortparallel}{(0,1)}}, \overset{x_1}{\overset{\shortparallel}{(L,0)}}, (L-1,0), (L-2,0), \ldots$$
is a bad sequence of length $L+1$, for every $L \in \mathbb{N}$.

We have an uncontrolled jump from $x_0$ to an arbitrarily high $x_1$.
To obtain bounds on the length of bad sequences, we need to assume programs transform states in a controlled way.

Definition:
Let $(A, \leq)$ be a wqo.

- A norm is a function $|\cdot| : A \to \mathbb{N}$ so that $A_{\leq n} := \{a \in A \mid |a| \leq n\}$ is finite f.a. $n \in \mathbb{N}$.
  We call $(A, \leq, |\cdot|)$ a normed wqo.

  As an example, on $(\mathbb{N}^2, \leq)$ we have $|(m,n)|_{\mathbb{N}^2} := \max\{m, n\}$.

- We assume there is a control function $g : \mathbb{N} \to \mathbb{N}$ that bounds the growth of elements when we go through a sequence $(a_i)_{i \in \mathbb{N}}$ in $A$.
  We assume $g$ is strictly increasing, $g(x+1) \geq g(x) + 1$.

- A sequence $(a_i)_{i\in\mathbb{N}}$ over $(A, \leq, |\cdot|)$ is *$(g,n)$-controlled* with $n\in\mathbb{N}$, if for all $i\in\mathbb{N}$,

$$|a_i| \leq g^i(n) \quad \text{with } g^0 = id,\ g^{i+1} = g\circ g^i.$$

The value $n$ is also called *initial norm*.

*Example:*

SIMPLE is $(g,n)$-controlled

with $g(x) = 2x$

$n = \max\{a_0, b_0\}$.

*Definition:*

- We let $[k]$ be the nwqo $(\{0,\dots,k-1\}, \leq, |\cdot|_{[k]})$ with
  - $\leq$ the usual $\leq$ on natural numbers
  - $|j|_{[k]} = j$.
- We let $\Gamma_k$ be the nwqo $(\{a_0,\dots,a_{k-1}\}, =, |\cdot|_{\Gamma_k})$ with $|a_j|_{\Gamma_k} = 0$.

*Length function:*

For every nwqo $(A, \leq_A, |\cdot|_A)$,

there is a longest $(g,n)$-controlled bad sequence:

↳ organize these sequences into a tree by sharing prefixes,

↳ the outdegree is bounded by $|A_{\leq g^i(n)}|$ for a node at depth $i$,

↳ the depth is bounded thanks to the wqo.

By König's lemma, the tree is finite.

Let $L_{g,n,A}$ be its height,

which is the length of the longest

$(g,n)$-controlled bad sequence in $A$.

We are interested in this length as a function in $n$:

$$L_{g,A}(n) := L_{g,n,A}.$$

We then obtain complexity bounds on $L_{g,A}$.

<u>Remark:</u>

$L_{g,A}(n)$ is monotonic in $n$ and in $g$.

If $g(x) \leq h(x)$ f.a. $x$,

then every $(g,n)$-controlled bad sequence

is also $(h,n)$-controlled.

Hence, $L_{g,A}(n) \leq L_{h,A}(n)$ f.a. $n$.

## <u>Polynomial NWQOs</u>

<u>Definition:</u>

We call nwqos $(A, \leq_A, |\cdot|_A)$ and $(B, \leq_B, |\cdot|_B)$ <u>isomorphic</u>,

$A \equiv B$, if there is a bijection $f: A \to B$ so that

$\forall a_1, a_2 \in A$.
- $a_1 \leq_A a_2$ iff $f(a_1) \leq_B f(a_2)$
- $|a_1|_A = |f(a_1)|_B$.

Note that then $L_{g,A} = L_{g,B}$.

Examples:

1) $[0] \equiv T_0$ // no elements, called empty nwqo

2) $[1] \equiv T_1$ since $|a_0|_{T_1} = 0 = |0|_{[1]}$. // called singleton nwqo

3) $[2] \not\equiv T_2$: The ordering is not isomorphic:

$0 \leq_{[2]} 1$ but $a_0 \not\leq_{T_2} a_1$.

The norm is not the same:

$|1|_{[2]} = 1$ but $|a_1|_{T_2} = 0$.

The controlled bad sequences differ:

$a_1 . a_0$ is $(g, 0)$-controlled in $T_2$

only $0$ is $(g, 0)$-controlled in $[2]$.

Hence, also the length functions are different

Definition: Let $(A_1, \leq_{A_1}, |\cdot|_{A_1})$ and $(A_2, \leq_2, |\cdot|_2)$ be two nwqos.

The disjoint sum of $A_1$ and $A_2$ is

$$(A_1 + A_2, \leq_{A_1+A_2}, |\cdot|_{A_1+A_2})$$

with

$$A_1 + A_2 := (\{1\} \times A_1) \cup (\{2\} \times A_2)$$

$$(i, a) \leq_{A_1+A_2} (j, b), \text{ if } \quad i = j \text{ and } a \leq_{A_i} b$$

$$|(i,a)|_{A_1+A_2} := |a|_{A_i}.$$

The Cartesian product

$$(A_1 \times A_2, \leq_{A_1 \times A_2}, |\cdot|_{A_1 \times A_2})$$

is defined by

$$(a_1, a_2) \leq_{A_1 \times A_2} (b_1, b_2), \text{ if } \quad a_1 \leq_{A_1} b_1 \text{ and } a_2 \leq_{A_2} b_2.$$

$$|(a_1, a_2)|_{A_1 \times A_2} := \max\{|a_1|_{A_1}, |a_2|_{A_2}\}.$$

That this is a wqo is Dickson's lemma.

- We write $A \cdot n$ for $\underbrace{A + A + \ldots + A}_{n\text{-times}}$.

  Then $T_n \equiv T_1 \cdot n$, in particular $T_0 \equiv A \cdot 0$.

- We write $A^d$ for $\underbrace{A \times A \times \ldots \times A}_{d\text{-times}}$.

  Then $A^0 \equiv T_1$, the singleton set with $()$ in it, the size is $0$.

- We also need the natural numbers $(\mathbb{N}, \leq_{\mathbb{N}}, |\cdot|_{\mathbb{N}})$ with $|n|_{\mathbb{N}} = n$.

<u>Definition</u>:

The set of <u>polynomial nwqos</u> is the smallest set of nwqos with

- $T_0, T_1, \mathbb{N}$ in it and
- closed under $+$ and $\times$.

<u>Example</u>:

The configurations of a $d$-dimensional VASS are states $Q$ with $|Q| = p$ is isomorphic to $\mathbb{N}^d \times T_p$, which is a polynomial nwqo.

<u>Lemma</u>:

The class of nwqos factorized along $\equiv$ forms a <u>commutative</u> <u>semiring</u>:

$(NWQOs/_{\equiv}, +, T_0)$ is a commutative monoid

$(NWQOs/_{\equiv}, \times, T_1)$ is a commutative monoid

$T_0 \times A \equiv T_0 \equiv A \times T_0$, $T_0$ is absorbing for $\times$

$A \times (B + C) \equiv (A \times B) + (A \times C)$ Distributivity.

<u>Remark</u>:

By the previous lemma,
every polynomial nwqo can be brought into
<u>polynomial normal form (PNF)</u>:

$$A \equiv \mathbb{N}^{d_1} + \dots + \mathbb{N}^{d_m}, \quad m, d_1, \dots, d_m \in \mathbb{N}$$

Recall that $\mathbb{N}^0 \equiv \Gamma_1$.

We will later denote $\Gamma_0$ by $0$ and $\Gamma_1$ by $1$,
and we will only be working with polynomial nwqos in PNF.

<u>Example</u>:

$$\begin{aligned} &\mathbb{N}^d \times \Gamma_p \\ &\equiv \mathbb{N}^d \times (\underbrace{\Gamma_1 + \dots + \Gamma_1}_{p\text{-times}}) \\ &\equiv (\mathbb{N}^d \times \Gamma_1) + \dots + (\mathbb{N}^d \times \Gamma_1) \\ &\equiv \mathbb{N}^d + \dots + \mathbb{N}^d \\ &= p \cdot \mathbb{N}^d \end{aligned}$$

## <u>Subrecursive Functions</u>

<u>Goal</u>: Study in slightly more detail
functions that are <u>non-elementary</u> but <u>primitive recursive</u>.

<u>Definition</u>:

The <u>Grzegorczyk hierarchy</u> $(\mathfrak{F}_k)_{k \in \omega}$
is a hierarchy of
classes of primitive recursive functions
with

$$\bigcup_{k \in \omega} \mathfrak{F}_k = PR \leftarrow \text{all primitive recursive functions.}$$

We have:

$\mathfrak{F}_0 = \mathfrak{F}_1 =$ linear functions.

$\mathfrak{F}_2 =$ elementary functions. (shifted from level 1)

The definition uses the <u>k-th fast growing function</u> $F_k : \mathbb{N} \to \mathbb{N}$:

$$F_0(x) := x+1$$

$$F_{k+1}(x) := F_k^{x+1}(x) := \overbrace{F_k(\dots(F_k(x))\dots)}^{x+1 \text{ times}}.$$

Then $\mathfrak{F}_k := \{ f \mid \exists i.\ f \text{ is computed in time/space} \leq F_k^i \}$.

Example:

- $$F_1(x) = F_0^{x+1}(x)$$
$$= \underbrace{((x+1)+1)+1}_{x+1}$$
$$= x + (x+1)\cdot 1 = 2x+1$$

- $$F_2(x) = F_1^{x+1}(x)$$
$$= \underbrace{2(2(2x+1)+1)+1}_{x+1}$$
$$= 2^{x+1}\cdot x + \sum_{i=0}^{x} 2^i$$
$$= 2^{x+1}\cdot x + 2^{x+1} - 1$$
$$= 2^{x+1}(x+1) - 1$$

- $F_3(x) > 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}} \Big\}\ x\text{-times}$

Remark:

- The functions $F_k$ are honest:
  they can be computed in time/space elementary in $F_k$,
  even in space $O(F_k)$:
  $F_k(\ldots(F_k(F_{k-1}(\ldots(F_{k-1}(F_{k-2}(\ldots$
  This means $F_k \in \mathfrak{F}_k$.
- All functions $f \in \mathfrak{F}_k$ are eventually (for large enough inputs) bounded by $F_{k+1}$.
  Hence, $F_{k+1} \notin \mathfrak{F}_k$.

Upper Bounds for Dickson's Lemma:

Theorem (Length Function Theorem): Let $g$ be a control function bounded by a function in $\mathfrak{F}_\gamma$, $\gamma \geq 1$. Let $d, p \geq 0$.
Then $L_{g, \mathbb{N}^d \times \Gamma_p}$ is bounded by $\mathfrak{F}_{\gamma+d}$.

Example (Shadow memory):

SIMPLE(a, b):

$c := 1;$

while $a > 0 \wedge b > 0$ do

$\ell: (a, b, c) := (a-1, b, 2c)$

$+ \; r: (a, b, c) := (2c, b-1, 1)$

od

The bad sequences in SIMPLE over $\mathbb{N}^3$
are also bad sequences over $\mathbb{N}^2$
when we only consider a and b.
The control function for this sequence over $\mathbb{N}^2$
is
$$g(x) = 2x \quad \text{in } \mathcal{F}_1.$$

Note that this is not immediate:

$$(5, 1, 1) \xrightarrow{\ell^4} (1, 1, 2^4) \xrightarrow{r} (2^5, 0, 1)$$

Although the r transition changes
the value of a drastically,
we have
$$2^5 \leq g^5(5)$$
$$= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 = 2^5 \cdot 5.$$

The length function theorem
applied with $\gamma = 1$ and $\rho = 1$
yields a function in $\mathcal{F}_3$
that bounds the length of all runs in SIMPLE.

What is needed to hide some part of the state for the length estimation?

↳ Hiding has to preserve the bad sequences.
If the original sequence was bad,
so should be the sequence resulting from hiding.

↳ The control function has to be large enough
to cover the effect that the hidden part has
on the non-hidden part of the state
when taking a transition.