Notes on Orevkov's Theorem*

Damiano Mazza†

October 18, 2003

Orevkov's result [Ore82], [Ore91] states that, in the case of first order logic, the hyperexponential upper bound on the length of the normalization of an intuitionistic proof can actually be attained:

Theorem 1 (Orevkov, 1982) *There exists a sequence $\{C_k\}_{k\in\mathbb{N}}$ of first order formulas such that, for every k, C_k has a non-normal proof of size $O(k)$, while all cut-free proofs of C_k have size $\Omega(2_k)$, where 2_n is the hyperexponential function defined by $2_0 = 1$, $2_{n+1} = 2^{2_n}$.*

The general idea behind Orevkov's proof is that of logically encoding the hyperexponential function itself, by means of simple first order formulas. The language that needs to be considered has the following symbols:

- A constant symbol, $\mathsf{0}$.
- A unary function symbol, s.
- A ternary relation symbol, R.

The symbols $\mathsf{0}$ and s are obviously intended to be interpreted respectively by zero and successor, while R is meant to represent the graph of the function

$$f(x, y) = 2^x + y$$

In other words, $Rxyz$ is supposed to mean $z = f(x, y)$. The meaning of R is coded by the following two formulas:

$$\begin{array}{rcl} \mathbf{H}_1 & := & \forall y.R\mathsf{0}y(\mathsf{s}y) \\ \mathbf{H}_2 & := & \forall xywz.(Rxyw \Rightarrow Rxwz \Rightarrow R(\mathsf{s}x)yz) \end{array}$$

We now consider the following sequence of formulas:

$$\mathbf{C}_k := \exists z_0 \ldots \exists z_k.\mathbf{R}_k\vec{z}$$

where

$$\mathbf{R}_k\vec{z} := R\mathsf{0}\mathsf{0}z_k \wedge Rz_k\mathsf{0}z_{k-1} \wedge \ldots \wedge Rz_1\mathsf{0}z_0$$

*Richard Statman claims he actually proved this theorem *before* Orevkov; here we used "Orevkov's Theorem" since the result came to be most widely and generally known with this name.

†These notes aim at reorganizing and restating Orevkov's proof in a hopefully simpler and more understandable manner. Fundamental contributions to this (admittedly not so easy) work have been given by Lorenzo Tortora de Falco, Harry Mairson, and Simone Martini.

Since $R00z_k$ means $z_k = 1$, and since in general $Rz_{i+1}0z_i$ means $z_i = 2^{z_{i+1}}$, $\mathbf{C}_k$ is simply stating that the hyperexponential function is defined for all non-negative integers up to k. Orevkov indeed proved that each formula $\mathbf{H}_1 \Rightarrow \mathbf{H}_2 \Rightarrow \mathbf{C}_k$ has no cut-free proof of size less than 2_k, while there exist non-normal proofs of the same formulas whose size is linear in k.

To prove $\mathbf{C}_k$ in sequent calculus under the hypotheses $\mathbf{H}_1$ and $\mathbf{H}_2$ obviously amounts to derive the sequent $\mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{C}_k$. In order to do this, we will need a sequence of auxiliary formulas, each containing a free variable:

$$\begin{aligned} \mathbf{A}_0 x &:= \forall y.\exists z.Rxyz \\ \mathbf{A}_{i+1} x &:= \forall y.(\mathbf{A}_i y \Rightarrow \exists z.(\mathbf{A}_i z \wedge Rxyz)) \end{aligned}$$

We will write $\mathbf{A}_i xt$ to note the formula $\mathbf{A}_i x$ where the universal quantifier has been removed and every occurrence of the quantified variable has been replaced by the term t.

The intuitive meaning of the formulas $\mathbf{A}_i$ can be described as follows. We've said that what we are trying to prove is actually that, from the two hypotheses introduced, one can deduce that the hyperexponential function is well defined anywhere. But the values taken by the hyperexponential function are nothing more that towers of exponentials; therefore, if we can prove that towers of any height are well defined, we are done. We will see that the $\mathbf{A}_i$ formulas are indeed a very smart way of describing the recursive definition of each tower as a function of the previous. In particular, they state that to obtain the definition of a tower of height $i + 1$ *anywhere*, the tower of height i needs only be defined *in zero*.

To see this, consider $\mathbf{A}_0 x0$; from what we said earlier about the signification of R, this formula means that the exponential function is defined for any non-negative integer x. Now take $\mathbf{A}_1 x0$; this one says "if the exponential function is defined in zero, then it is also defined in any other value of the form 2^x". In other words, if the exponential is defined *in zero*, the double exponential is defined *anywhere*. $\mathbf{A}_2 x0$ obviously takes care of the triple exponential, and so on.

To sum things up, if we put

$$\begin{aligned} \mathbf{B}_0 z &:= Rz_1 0z \\ \mathbf{B}_i z &:= \mathbf{A}_{i-1} \wedge Rz_{i+1} 0z \end{aligned}$$

we can say that $\exists z.\mathbf{B}_i z$ means "the tower of height i is defined on any non-negative integer z_{i+1}"; therefore, a good idea would be to look for a proof of something like

$$\exists z.\mathbf{B}_0 z, \ldots, \exists z.\mathbf{B}_k z \vdash \mathbf{C}_k$$

and then use the $\mathbf{A}_i$'s to obtain, for each $0 \leq i \leq k$, a proof of

$$\mathbf{H}_1, \mathbf{H}_2 \vdash \exists z.\mathbf{B}_i z$$

to cut against the former proof.

Let us then start our search for the proof of $\mathbf{C}_k$. Our first partial result is the following:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{R00z_k \vdash R00z_k}}{\mathbf{B}_k z_k \vdash R00z_k} \qquad \begin{array}{c}\dfrac{\dfrac{\dfrac{}{Rz_2 0 z_1 \vdash Rz_2 0 z_1}}{\mathbf{B}_1 z_1 \vdash Rz_2 0 z_1} \qquad \dfrac{}{\mathbf{B}_0 z_0 \vdash \mathbf{B}_0 z_0}}{\mathbf{B}_0 z_0, \mathbf{B}_1 z_1 \vdash \mathbf{R}_1 \vec{z}} \\ \vdots \\ \mathbf{B}_0 z_0, \ldots, \mathbf{B}_{k-1} z_{k-1} \vdash \mathbf{R}_{k-1}\vec{z}\end{array}}{\mathbf{B}_0 z_0, \ldots, \mathbf{B}_k z_k \vdash \mathbf{R}_k \vec{z}}}{\mathbf{B}_0 z_0, \ldots, \mathbf{B}_k z_k \vdash \mathbf{C}_k}$$

It's not exactly what we were looking for — but it's close. The only thing that seems quite annoying concerns the existential quantification of the various $\mathbf{B}_i$, which is rendered impossible by the fact that each variable z_i (apart from z_0) occurs free both in $\mathbf{B}_i$ and $\mathbf{B}_{i-1}$, so that no formula (except $\mathbf{B}_0$) can be quantified first. But this is not going to be a problem; in fact, we can proceed by quantifying over z_0 in $\mathbf{B}_0$ (which is the only quite possible thing to do), then get rid of $\exists z.\mathbf{B}_0 z$ by cutting it against some proof of $\Gamma \vdash \exists z.\mathbf{B}_0 z$, so that now it is safe to quantify over z_1 in $\mathbf{B}_1$, and so on.

Our next task will be to show that those proofs of $\Gamma \vdash \exists z.\mathbf{B}_i z$ actually exist, and in this respect our definition of the sequence $\mathbf{A}_i$ will be of the greatest help. Like we said, the $\mathbf{A}_i$'s are made in such a way that the definition of a tower of exponentials becomes a consequence of the definition of the previous tower *in zero*. As a result, if we find, for any i, a proof of $\mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{A}_i 0$, then it cannot possibly take too long to arrive to our goal, i.e., prove that for any i, $\mathbf{H}_1, \mathbf{H}_2 \vdash \exists z.\mathbf{B}_i z$. This is the object of the following lemma:

Lemma 2 *For each i, there is a proof of $\mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{A}_i 0$ whose size is $O(1)$, i.e., it is bounded by a constant.*

Proof. Case $i = 0$ is easy:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{R0y(\mathsf{s}y) \vdash R0y(\mathsf{s}y)}}{\mathbf{H}_1 \vdash R0y(\mathsf{s}y)}}{\mathbf{H}_1 \vdash \mathbf{A}_0 0}}{\mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{A}_0 0}$$

For the other cases, let us remark that if we have a proof of $\mathbf{H}_2, \mathbf{A}_{i-1} y \vdash \mathbf{A}_{i-1}(\mathsf{s}y)$, then we can obtain the desired proof in the following manner:

$$\dfrac{\dfrac{\dfrac{\dfrac{\mathbf{H}_2, \mathbf{A}_{i-1} y \vdash \mathbf{A}_{i-1}(\mathsf{s}y) \qquad \dfrac{}{R0y(\mathsf{s}y) \vdash R0y(\mathsf{s}y)}}{R0y(\mathsf{s}y), \mathbf{H}_2, \mathbf{A}_{i-1} y \vdash \mathbf{A}_{i-1}(\mathsf{s}y) \wedge R0y(\mathsf{s}y)}}{\mathbf{H}_1, \mathbf{H}_2, \mathbf{A}_{i-1} y \vdash \exists z.(\mathbf{A}_{i-1} z \wedge R0yz)}}{\mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{A}_{i-1} y \Rightarrow \exists z.(\mathbf{A}_{i-1} z \wedge R0yz)}}{\mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{A}_i 0}$$

For $i = 1$, the missing part is

$$
\begin{prooftree}
\AxiomC{}
\UnaryInfC{$Ryuz \vdash Ryuz$}
\AxiomC{}
\UnaryInfC{$Ryzw \vdash Ryzw$}
\AxiomC{}
\UnaryInfC{$R(\mathsf{s}y)uw \vdash R(\mathsf{s}y)uw$}
\BinaryInfC{$Ryzw \Rightarrow R(\mathsf{s}y)uw, Ryzw \vdash R(\mathsf{s}y)uw$}
\BinaryInfC{$Ryuz \Rightarrow Ryzw \Rightarrow R(\mathsf{s}y)uw, Ryuz, Ryzw \vdash R(\mathsf{s}y)uw$}
\doubleLine
\UnaryInfC{$\mathbf{H}_2, Ryuz, Ryzw \vdash R(\mathsf{s}y)uw$}
\UnaryInfC{$\mathbf{H}_2, Ryuz, Ryzw \vdash \exists c.R(\mathsf{s}y)uc$}
\UnaryInfC{$\mathbf{H}_2, Ryuz, \exists c.Ryzc \vdash \exists c.R(\mathsf{s}y)uc$}
\UnaryInfC{$\mathbf{H}_2, Ryuz, \mathbf{A}_0 y \vdash \exists c.R(\mathsf{s}y)uc$}
\doubleLine
\UnaryInfC{$\mathbf{H}_2, \mathbf{A}_0 y, \mathbf{A}_0 y \vdash \exists c.R(\mathsf{s}y)uc$}
\UnaryInfC{$\mathbf{H}_2, \mathbf{A}_0 y, \mathbf{A}_0 y \vdash \mathbf{A}_0(\mathsf{s}y)$}
\UnaryInfC{$\mathbf{H}_2, \mathbf{A}_0 y \vdash \mathbf{A}_0(\mathsf{s}y)$}
\end{prooftree}
$$

The general case of $i \geq 2$ is taken care of by the following derivation:

$$
\begin{prooftree}
\AxiomC{$\vdots\ \theta_2$}
\AxiomC{$\vdots\ \theta_1$}
\AxiomC{}
\UnaryInfC{$\mathbf{A}_{i-2}w \vdash \mathbf{A}_{i-2}w$}
\UnaryInfC{$\mathbf{A}_{i-2}w \wedge Rxzw \vdash \mathbf{A}_{i-2}w$}
\AxiomC{}
\UnaryInfC{$Rxyz \vdash Rxyz$}
\AxiomC{}
\UnaryInfC{$Rxzw \vdash Rxzw$}
\AxiomC{}
\UnaryInfC{$R(\mathsf{s}x)yw \vdash R(\mathsf{s}x)yw$}
\BinaryInfC{$Rxzw \Rightarrow R(\mathsf{s}x)yw, Rxzw \vdash R(\mathsf{s}x)yw$}
\BinaryInfC{$Rxyz \Rightarrow Rxzw \Rightarrow R(\mathsf{s}x)yw, Rxyz, Rxzw \vdash R(\mathsf{s}x)yw$}
\doubleLine
\UnaryInfC{$\mathbf{H}_2, Rxyz, Rxzw \vdash R(\mathsf{s}x)yw$}
\doubleLine
\UnaryInfC{$\mathbf{H}_2, \mathbf{A}_{i-2}z \wedge Rxyz, \mathbf{A}_{i-2}w \wedge Rxzw \vdash R(\mathsf{s}x)yw$}
\BinaryInfC{$\mathbf{H}_2, \mathbf{A}_{i-2}z \wedge Rxyz, (\mathbf{A}_{i-2}w \wedge Rxzw)^{(2)} \vdash \mathbf{A}_{i-2}w \wedge R(\mathsf{s}x)yw$}
\doubleLine
\UnaryInfC{$\mathbf{H}_2, \mathbf{A}_{i-2}z \wedge Rxyz, \mathbf{A}_{i-2}w \wedge Rxzw \vdash \exists z.(\mathbf{A}_{i-2}z \wedge R(\mathsf{s}x)yz)$}
\UnaryInfC{$\mathbf{H}_2, \mathbf{A}_{i-2}z \wedge Rxyz, \exists w.(\mathbf{A}_{i-2}w \wedge Rxzw) \vdash \exists z.(\mathbf{A}_{i-2}z \wedge R(\mathsf{s}x)yz)$}
\RightLabel{cut}
\BinaryInfC{$\mathbf{H}_2, \mathbf{A}_{i-1}x, (\mathbf{A}_{i-2}z \wedge Rxyz)^{(2)} \vdash \exists z.(\mathbf{A}_{i-2}z \wedge R(\mathsf{s}x)yz)$}
\doubleLine
\UnaryInfC{$\mathbf{H}_2, \mathbf{A}_{i-1}x, \exists z.(\mathbf{A}_{i-2}z \wedge Rxyz) \vdash \exists z.(\mathbf{A}_{i-2}z \wedge R(\mathsf{s}x)yz)$}
\RightLabel{cut}
\BinaryInfC{$\mathbf{H}_2, (\mathbf{A}_{i-1}x)^{(2)}, \mathbf{A}_{i-2}y \vdash \exists z.(\mathbf{A}_{i-2}z \wedge R(\mathsf{s}x)yz)$}
\doubleLine
\UnaryInfC{$\mathbf{H}_2, \mathbf{A}_{i-1}x \vdash \mathbf{A}_{i-1}(\mathsf{s}x)$}
\end{prooftree}
$$

where θ_1 and θ_2 are respectively

$$
\begin{prooftree}
\AxiomC{}
\UnaryInfC{$\mathbf{A}_{i-2}z \vdash \mathbf{A}_{i-2}z$}
\AxiomC{}
\UnaryInfC{$\exists w.(\mathbf{A}_{i-2}w \wedge Rxzw) \vdash \exists w.(\mathbf{A}_{i-2}w \wedge Rxzw)$}
\BinaryInfC{$\mathbf{A}_{i-2}z \Rightarrow \exists w.(\mathbf{A}_{i-2}w \wedge Rxzw), \mathbf{A}_{i-2}z \vdash \exists w.(\mathbf{A}_{i-2}w \wedge Rxzw)$}
\UnaryInfC{$\mathbf{A}_{i-1}x, \mathbf{A}_{i-2}z \vdash \exists w.(\mathbf{A}_{i-2}w \wedge Rxzw)$}
\UnaryInfC{$\mathbf{A}_{i-1}x, \mathbf{A}_{i-2}z \wedge Rxyz \vdash \exists w.(\mathbf{A}_{i-2}w \wedge Rxzw)$}
\end{prooftree}
$$

and

$$
\begin{prooftree}
\AxiomC{}
\UnaryInfC{$\mathbf{A}_{i-2}y \vdash \mathbf{A}_{i-2}y$}
\AxiomC{}
\UnaryInfC{$\exists z.(\mathbf{A}_{i-2}z \wedge Rxyz) \vdash \exists z.(\mathbf{A}_{i-2}z \wedge Rxyz)$}
\BinaryInfC{$\mathbf{A}_{i-2}y \Rightarrow \exists z.(\mathbf{A}_{i-2}z \wedge Rxyz), \mathbf{A}_{i-2}y \vdash \exists z.(\mathbf{A}_{i-2}z \wedge Rxyz)$}
\UnaryInfC{$\mathbf{A}_{i-1}x, \mathbf{A}_{i-2}y \vdash \exists z.(\mathbf{A}_{i-2}z \wedge Rxyz)$}
\end{prooftree}
$$

We see that the derivation has exactly the same size for any $i \geq 2$, so that in general all proofs of $\mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{A}_i\mathsf{0}$ admit a constant bounding their sizes. $\square$

We remark that, by the lemma we just proved, also $\mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{A}_i 0t$ is provable in constant size, for every i and for any term t.

Now all that remains to do is to show the provability, for all fixed k and for all $0 \leq i \leq k$, of $\Gamma \vdash \exists z \mathbf{B}_i z$, where Γ is an appropriate context. Case $i = 0$ doesn't need lemma 2:

$$\cfrac{\cfrac{\cfrac{}{\exists z.\mathbf{B}_0 z \vdash \exists z.\mathbf{B}_0 z}}{\mathbf{A}_0 z_1 \vdash \exists z.\mathbf{B}_0 z}}{\mathbf{B}_1 z_1 \vdash \exists z.\mathbf{B}_0 z}$$

For $0 < i < k-1$, we use the following derivation:

$$\cfrac{\cfrac{\cfrac{\begin{matrix}\vdots\ \text{lemma 2}\\ \mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{A}_{i-1} 0\end{matrix} \qquad \cfrac{}{\exists z.\mathbf{B}_i z \vdash \exists z.\mathbf{B}_i z}}{\mathbf{H}_1, \mathbf{H}_2, \mathbf{A}_i z_{i+1} 0 \vdash \exists z.\mathbf{B}_i z}}{\mathbf{H}_1, \mathbf{H}_2, \mathbf{A}_i z_{i+1} \vdash \exists z.\mathbf{B}_i z}}{\mathbf{H}_1, \mathbf{H}_2, \mathbf{B}_{i+1} z_{i+1} \vdash \exists z.\mathbf{B}_i z}$$

Last but not least, the case $i = k$:

$$\cfrac{\cfrac{\begin{matrix}\vdots\ \text{lemma 2}\\ \mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{A}_k 00\end{matrix} \qquad \cfrac{\begin{matrix}\vdots\ \text{lemma 2}\\ \mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{A}_{k-1} 0\end{matrix} \qquad \cfrac{}{\exists z.\mathbf{B}_k z \vdash \exists z.\mathbf{B}_k z}}{\mathbf{H}_1, \mathbf{H}_2, \mathbf{A}_k 00 \vdash \exists z.\mathbf{B}_k z}}{\mathbf{H}_1, \mathbf{H}_1, \mathbf{H}_2, \mathbf{H}_2 \vdash \exists z.\mathbf{B}_k z}\,\mathsf{cut}}{\mathbf{H}_1, \mathbf{H}_2 \vdash \exists z.\mathbf{B}_k z}$$

Now the first main result:

Proposition 3 *For any k, the formula $\mathbf{H}_1 \Rightarrow \mathbf{H}_2 \Rightarrow \mathbf{C}_k$ has a non-normal proof of size $O(k)$.*

Proof. It suffices to consider the following derivation, which uses the strategy previously discussed in order to avoid variable problems in existential quantifications on the left:

$$\cfrac{\cfrac{\begin{matrix}\vdots\\ \mathbf{H}_1, \mathbf{H}_2 \vdash \exists z.\mathbf{B}_k z\end{matrix} \qquad \begin{matrix}\cfrac{\begin{matrix}\vdots\\ \mathbf{H}_1, \mathbf{H}_2, \mathbf{B}_2 z_2 \vdash \exists z.\mathbf{B}_1 z\end{matrix} \qquad \cfrac{\cfrac{\begin{matrix}\vdots\\ \mathbf{B}_1 z_1 \vdash \exists z.\mathbf{B}_0 z\end{matrix} \qquad \cfrac{\begin{matrix}\vdots\\ \mathbf{B}_0 z_0, \ldots, \mathbf{B}_k z_k \vdash \mathbf{C}_k\end{matrix}}{\exists z.\mathbf{B}_0 z, \ldots, \mathbf{B}_k z_k \vdash \mathbf{C}_k}}{\mathbf{B}_1 z_1, \mathbf{B}_1 z_1, \ldots, \mathbf{B}_k z_k \vdash \mathbf{C}_k}\,\mathsf{cut}}{\exists z.\mathbf{B}_1 z, \ldots, \mathbf{B}_k z_k \vdash \mathbf{C}_k}}{\mathbf{B}_2 z_2, \mathbf{B}_2 z_2, \ldots, \mathbf{B}_k z_k, \mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{C}_k}\,\mathsf{cut}\\ \vdots\\ \exists z.\mathbf{B}_k z, \mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{C}_k\end{matrix}}{\mathbf{H}_1, \mathbf{H}_1, \mathbf{H}_2, \mathbf{H}_2 \vdash \mathbf{C}_k}\,\mathsf{cut}}{\vdash \mathbf{H}_1 \Rightarrow \mathbf{H}_2 \Rightarrow \mathbf{C}_k}$$

The size of the sub-proof of $\mathbf{B}_0 z_0, \ldots, \mathbf{B}_k z_k \vdash \mathbf{C}_k$ is obviously linear in k (the derivation is the one we introduced first). After that, the number of cuts performed is $k+1$, so by lemma 2 we still remain linear in k. $\square$

If n is a non-negative integer, we put

$$\overline{n} := \underbrace{\mathsf{s} \ldots \mathsf{s}}_{n} \mathsf{0}.$$

This notation will be convenient for the following result:

Lemma 4 *Any normal proof of* $\mathbf{H}_1, \mathbf{H}_2 \vdash R\overline{m}\overline{n}\overline{k}$ *has size* $\Omega(2^m)$ *and satisfies* $k = 2^m + n$.

Proof. By induction on m. We start with $m = 0$, for which the shortest cut free proof is

$$\cfrac{\cfrac{\cfrac{}{R\overline{0}\overline{n}(\mathsf{s}\overline{n}) \vdash R\overline{0}\overline{n}(\mathsf{s}\overline{n})}}{\mathbf{H}_1 \vdash R\overline{0}\overline{n}(\mathsf{s}\overline{n})}}{\mathbf{H}_1, \mathbf{H}_2 \vdash R\overline{0}\overline{n}(\mathsf{s}\overline{n})}$$

The size is 3, which can be put in the form $9 \cdot 2^0 - 6$, and the three terms $\overline{m}$, $\overline{n}$, and $\overline{k}$ respect $k = 2^m + n$, since $k = n + 1$ and $m = 0$.

For the induction step, the shortest proof of $\mathbf{H}_1, \mathbf{H}_2 \vdash R(\mathsf{s}\overline{m})\overline{n}\overline{k}$ is

$$\cfrac{\cfrac{\begin{array}{c}\vdots\ \theta_2\\ \mathbf{H}_1,\mathbf{H}_2 \vdash R\overline{m}\overline{n}\overline{u}\end{array} \qquad \cfrac{\begin{array}{c}\vdots\ \theta_1\\ \mathbf{H}_1,\mathbf{H}_2\vdash R\overline{m}\overline{u}\overline{k}\end{array} \qquad \cfrac{}{R(\mathsf{s}\overline{m})\overline{n}\overline{k}\vdash R(\mathsf{s}\overline{m})\overline{n}\overline{k}}}{R\overline{m}\overline{u}\overline{k}\Rightarrow R(\mathsf{s}\overline{m})\overline{n}\overline{k}, \mathbf{H}_1,\mathbf{H}_2\vdash R(\mathsf{s}\overline{m})\overline{n}\overline{k}}}{R\overline{m}\overline{n}\overline{u}\Rightarrow R\overline{m}\overline{u}\overline{k}\Rightarrow R(\mathsf{s}\overline{m})\overline{n}\overline{k}, \mathbf{H}_1^{(2)},\mathbf{H}_2^{(2)}\vdash R(\mathsf{s}\overline{m})\overline{n}\overline{k}}}{\mathbf{H}_1,\mathbf{H}_2\vdash R(\mathsf{s}\overline{m})\overline{n}\overline{k}}$$

By induction hypothesis, the sizes of θ_1 and θ_2 are both $9 \cdot 2^m - 6$, and we have $u = 2^m + n$ and $k = 2^m + u$. That yields $2 \cdot 9 \cdot 2^m - 12 + 6$ for the size of the whole proof, which is exactly equal to $9 \cdot 2^{m+1} - 6$. Moreover, $k = 2^m + 2^m + n = 2^{m+1} + n$, so we are done. $\square$

We can now state the other main result, which, combined with proposition 3, gives theorem 1:

Proposition 5 *Every normal proof of* $\mathbf{H}_1 \Rightarrow \mathbf{H}_2 \Rightarrow \mathbf{C}_k$ *has size* $\Omega(2_k)$.

Proof. The right implication rule is negative, i.e. reversible, so we are looking for a cut-free proof of $\mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{C}_k$. Since $(\mathbf{H}_1 \wedge \mathbf{H}_2) \Rightarrow\perp$ admits a counter-model (namely our standard interpretation of R as a relation over $\mathbb{N}$), by soundness $\mathbf{H}_1, \mathbf{H}_2 \vdash$ is not provable, so $\mathbf{C}_k$ cannot have been introduced by weakening. Moreover, by the sub-formula property, $\mathbf{C}_k$ is not a direct conclusion of an axiom, since in the general case it contains several conjunctions, and there is no trace of them on the left (the same applies for $\mathbf{H}_1$ and $\mathbf{H}_1$). Therefore, $\mathbf{C}_k$ must have been built up from its atoms, by means of k right conjunction rules and $k+1$ right existential quantification rules. Now $\mathbf{H}_1$ and $\mathbf{H}_2$ are positive, and if we consider the conjunctions in $\mathbf{C}_k$ as negative, we can make the universal rules on the left commute with the conjunction rules on the right, in order to "push down" these latter, and transform any proof of $\mathbf{H}_1, \mathbf{H}_2 \vdash \mathbf{C}_k$ into something like this, up to a certain (irrelevant) number of contractions:

$$
\dfrac{\begin{array}{c}\vdots\\ \mathbf{H}_1,\mathbf{H}_2 \vdash R\mathsf{00}t_k\end{array} \qquad \begin{array}{c} \dfrac{\begin{array}{c}\vdots\\ \mathbf{H}_1,\mathbf{H}_2\vdash Rt_2\mathsf{0}t_1\end{array}\qquad \begin{array}{c}\vdots\\ \mathbf{H}_1,\mathbf{H}_2\vdash Rt_1\mathsf{0}t_0\end{array}}{\mathbf{H}_1,\mathbf{H}_2\vdash Rt_2\mathsf{0}t_1\wedge Rt_1\mathsf{0}t_0}\\ \vdots \\ \mathbf{H}_1,\mathbf{H}_2 \vdash Rt_k\mathsf{0}t_{k-1}\wedge\ldots\wedge Rt_2\mathsf{0}t_1\wedge Rt_1\mathsf{0}t_0\end{array}}{\dfrac{\mathbf{H}_1,\mathbf{H}_2\vdash \mathbf{R}_k\vec{t}}{\mathbf{H}_1,\mathbf{H}_2\vdash \mathbf{C}_k}}
$$

where $\vec{t}$ are $k+1$ terms, none of which is a variable. We can make this assumption without losing any generality, since those terms are all converted into variables upon existential quantification; if any among them were already a variable, we could replace it all through the proof with any constant term (for example $\mathsf{0}$) with no difference.

So every t_i must be in the form $\overline{n}$ for some non-negative integer n; by lemma 4, we know that $t_k = \overline{1}$, $t_{k-1} = \overline{2}$, and, in general, $t_i = \overline{2_{k-i}}$. Therefore, still by lemma 4, the derivation of $\mathbf{H}_1, \mathbf{H}_2 \vdash Rt_1\mathsf{0}t_0$, which is just a part of the whole derivation, has size $\Omega(2^{2_{k-1}}) = \Omega(2_k)$. $\square$

The fact of having used sequent calculus to state the lower bound does not turn out to be restrictive. As a matter of fact, Orevkov originally proved his result for Hilbert-style deduction systems, and the same argument we used here applies to natural deduction systems as well; a proof can be found in [TS96].

References

[Ore82] Vladimir Orevkov. **Lower bounds for increasing complexity of derivations after cut elimination**. *Journal of Soviet Mathematics*, 20(4), 1982.

[Ore91] Vladimir Orevkov. *Complexity of Proofs and Their Transformations in Axiomatic Theories*, volume 128 of *Translations of Mathematical Monographs*. American Mathemetical Society, 1991.

[TS96] Anne Sjerp Troelstra and Helmut Schwichtenberg. *Basic Proof Theory*, volume 43 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1996.