הערה 5.29 דוגמה: נוכיח כי $\vdash_p \{x=n\}\,y:=1;while\,\neg(x=1)\ do\ (y:=y*x;x:=x-1)\,\{y=n!\wedge n>0\}$.

נסמן ב-$P\,s$ את $(s\,y=(s\,n)!\wedge s\,n>0)$.
נסמן ב-$INV\,s$ את $(s\,x>0\Rightarrow((s\,y)*(s\,x)!=(s\,n)!\wedge s\,n\geq s\,x))$.
נסמן ב-S את $while\,\neg(x=1)\ do\ (y:=y*x;x:=x-1)$.
להלן גזירה מתאימה:

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{\{INV\,[x\mapsto x-1]\}\,x:=x-1\,\{INV\}}\,ass_p
\quad
\dfrac{\dfrac{}{\{INV\,[x\mapsto x-1]\}\,x:=x-1\,\{INV\}}\,ass_p}{\{INV\,[x\mapsto x-1]\,[y\mapsto y*x]\}\,y:=y*x\,\{INV\,[x\mapsto x-1]\}}\,ass_p
}{\{INV\,[x\mapsto x-1]\,[y\mapsto y*x]\}\,y:=y*x;x:=x-1\,\{INV\}}\,comp_p
}{\{\neg(x=1)\wedge INV\}\,y:=y*x;x:=x-1\,\{INV\}}\,cons_p^{*}
}{\{INV\}\,S\,\{x=1\wedge INV\}}\,while_p
}{\{INV\}\,S\,\{y=n!\wedge n>0\}}\,cons_p^{**}
\quad
\dfrac{\dfrac{}{\{INV\,[y\mapsto 1]\}\,y:=1\,\{INV\}}\,ass_p}{\{x=n\}\,y:=1\,\{INV\}}\,cons_p^{***}
}{\{x=n\}\,y:=1;S\,\{y=n!\wedge n>0\}}\,comp_p
$$

1. הסבר עבור $cons_p^{*}$: יהי s מצב. נניח ש $(\neg(x=1)\wedge INV)\,s=tt$. צריך להוכיח ש- $INV\,s'=tt$ עבור $s'=s\,[x\mapsto(s\,x)-1]\,[y\mapsto(s\,y)\cdot(s\,x)]$. נניח $s'\,x>0$. לכן $(s\,x)-1>0$ ובפרט $s\,x>0$. נקבל ש-$(s'\,y)\cdot(s'\,x)!=((s\,y)*(s\,x))*((s\,x)-1)!=(s\,y)*(s\,x)!=(s\,n)!$. השוויון הראשון נכון כי $s'\,y=(s\,y)\cdot(s\,x)$ וכי $s'\,x=(x\,x)-1$. השוויון השני מהגדרת פעולת העצרת. השוויון השלישי נכון כי $INV\,s=tt$. בנוסף, $s'\,n=s\,n\geq s\,x$ כי s' ו-s מסכימים על n וכי $INV\,s=tt$.

2. הסבר עבור $cons_p^{**}$: יהי s מצב. נניח כי $(x=1\wedge INV)\,s=tt$. נוכיח ש- $(y=n!\wedge n>0)\,s=tt$. כמובן, $s\,x=1>0$. לכן $s\,y\cdot(s\,x)!=(s\,n)!$. יתרה מזאת, $s\,x=1$ ולכן $s\,y=(s\,n)!$. לבסוף, מ-INV מקבלים גם $s\,n>s\,x>0$.

3. הסבר עבור $cons_p^{***}$: יהי s מצב. נניח כי $(x=n)\,s=tt$. נוכיח כי $(INV\,[y\mapsto 1])\,s=tt$. כלומר, צריך להוכיח ש $INV\,s'=tt$ עבור $s'=s\,[y\mapsto 1]$. אם $s'\,x\leq 0$ אז זה טריוויאלי. אחרת מכיוון ש-$s'\,x=s\,x$ ו-$s'\,y=1$, $(s'\,y)\cdot(s'\,x)!=(s\,x)!=(s\,n)!=(s'\,n)!$ כאשר השוויון הלפני-אחרון הוא כי $s\,x=s\,n$. וכמובן ש-$s'\,n=s\,n=s\,x=s'\,x$.