Confidentiality and Integrity

Ross Tate

October 23, 2014

Theorem. *In* **CAT***, given* **E** *and* **C***, let* π *be the functor from* **E** *to* $(\mathbf{E} \pitchfork \mathbf{C}) \twoheadrightarrow \mathbf{C}$ *demonstrating that* $\mathbf{E} \pitchfork \mathbf{C}$ *is a power. Then, provided* **C** *has products, for each* $\mathcal{E} : \mathbf{E}$*, the functor* $\pi_{\mathcal{E}} : \mathbf{E} \pitchfork \mathbf{C} \to \mathbf{C}$ *has a right adjoint, and, provided* **C** *has coproducts,* $\pi_{\mathcal{E}}$ *also has a left adjoint.*

Let $C_{\mathcal{E}} : \mathbf{C} \to \mathbf{E} \pitchfork \mathbf{C}$ *be a right adjoint to* $\pi_{\mathcal{E}}$*. This means that there is a morphism* $c_{\mathcal{E},\mathcal{C}} : \pi_{\mathcal{E}}(C_{\mathcal{E}}(\mathcal{C})) \to \mathcal{C}$ *for every object* $\mathcal{C}$ *of* **C***, and for every object* $\mathcal{P}$ *of* $\mathbf{E} \pitchfork \mathbf{C}$ *and morphism* $p : \pi_{\mathcal{E}}(\mathcal{P}) \to \mathcal{C}$*, there exists a unique morphism* $p^{\rightarrow} : \mathcal{P} \to C_{\mathcal{E}}(\mathcal{C})$ *in* $\mathbf{E} \pitchfork \mathbf{C}$ *such that* $\pi_{\mathcal{E}}(p^{\rightarrow})\,;c_{\mathcal{E},\mathcal{C}}$ *equals* p*. To construct such a* $C_{\mathcal{E}}$*, recall that an object of* $\mathbf{E} \pitchfork \mathbf{C}$ *is a functor from* **E** *to* **C***. Consequently, for any such object* $\mathcal{P}$ *the morphism* $p : \pi_{\mathcal{E}}(\mathcal{P}) \to \mathcal{C}$ *provides a morphism from* $\mathcal{P}(\mathcal{E}')$ *for each object* $\mathcal{E}'$ *and morphism* $e : \mathcal{E}' \to \mathcal{E}$ *of* **E***, given by* $\mathcal{P}(e)\,;p$*. So, we can define* $C_{\mathcal{E}}(\mathcal{C})(\mathcal{E}')$ *to be* $\&_{e:\mathcal{E}'\to\mathcal{E}}\,\mathcal{C}$*, meaning* $\mathcal{C}$ *producted with itself once for each morphism* $\mathcal{E}' \to \mathcal{E}$*, and every* $\mathcal{P}(\mathcal{E}')$ *will have a morphism to* $C_{\mathcal{E}}(\mathcal{C})(\mathcal{E}')$ *given by* $\langle \mathcal{P}(e)\,;p\rangle_{e:\mathcal{E}'\to\mathcal{E}}$*. Also, given an object* $\mathcal{E}''$ *and morphism* $e' : \mathcal{E}'' \to \mathcal{E}'$*, we can define* $C_{\mathcal{E}}(e')$ *to be* $\langle \pi_{e'\,;\,e}\rangle_{e:\mathcal{E}'\to\mathcal{E}}$*, and then the collection of morphisms presented earlier is guaranteed to form a natural transformation from* $\mathcal{P}$ *to* $C_{\mathcal{E}}(\mathcal{C})$*, i.e. a morphism of* $\mathbf{E} \pitchfork \mathbf{C}$*. Finally, we can define* $c_{\mathcal{E},\mathcal{C}} : \pi_{\mathcal{E}}(I_{\mathcal{E}}(\mathcal{C})) \to \mathcal{C}$ *to be* $\pi_{id_{\mathcal{E}}} : \left(\&_{e:\mathcal{E}\to\mathcal{E}}\,\mathcal{C}\right) \to \mathcal{C}$*, and so* $\langle \mathcal{P}(e)\,;p\rangle_{e:\mathcal{E}\to\mathcal{E}}\,;\pi_{id}$ *equals* $\mathcal{P}(id_{\mathcal{E}})\,;p$ *which equals* p *as desired.* $C_{\mathcal{E}}$ *can be extended into a functor because* $\&$ *is functorial and* π *is natural.*

A similar argument applies to the left adjoint. Let $I_{\mathcal{E}} : \mathbf{C} \to \mathbf{E} \pitchfork \mathbf{C}$ *be a left adjoint to* $\pi_{\mathcal{E}}$*. This means that there is a morphism* $i_{\mathcal{E},\mathcal{C}} : \mathcal{C} \to \pi_{\mathcal{E}}(I_{\mathcal{E}}(\mathcal{C}))$ *for every object* $\mathcal{C}$ *of* **C***, and for every object* $\mathcal{P}$ *of* $\mathbf{E} \pitchfork \mathbf{C}$ *and morphism* $p : \mathcal{C} \to \pi_{\mathcal{E}}(\mathcal{P})$*, there exists a unique morphism* $p^{\leftarrow} : I_{\mathcal{E}}(\mathcal{C}) \to \mathcal{P}$ *in* $\mathbf{E} \pitchfork \mathbf{C}$ *such that* $i_{\mathcal{E},\mathcal{C}}\,;\pi_{\mathcal{E}}(p^{\leftarrow})$ *equals* p*. To construct such a* $I_{\mathcal{E}}$*, recall that an object of* $\mathbf{E} \pitchfork \mathbf{C}$ *is a functor from* **E** *to* **C***. Consequently, for any such object* $\mathcal{P}$ *the morphism* $p : \mathcal{C} \to \pi_{\mathcal{E}}(\mathcal{P})$ *provides a morphism to* $\mathcal{P}(\mathcal{E}')$ *for each object* $\mathcal{E}'$ *and morphism* $e : \mathcal{E} \to \mathcal{E}'$ *of* **E***, given by* $p\,;\mathcal{P}(e)$*. So, we can define* $C_{\mathcal{E}}(\mathcal{C})(\mathcal{E}')$ *to be* $\bigoplus_{e:\mathcal{E}\to\mathcal{E}'}\mathcal{C}$*, meaning* $\mathcal{C}$ *coproducted with itself once for each morphism* $\mathcal{E} \to \mathcal{E}'$*, and every* $\mathcal{P}(\mathcal{E}')$ *will have a morphism from* $C_{\mathcal{E}}(\mathcal{C})(\mathcal{E}')$ *given by* $[p\,;\mathcal{P}(e)]_{e:\mathcal{E}\to\mathcal{E}'}$*. Also, given an object* $\mathcal{E}''$ *and morphism* $e' : \mathcal{E}' \to \mathcal{E}''$*, we can define* $C_{\mathcal{E}}(e')$ *to be* $[\kappa_{e\,;\,e'}]_{e:\mathcal{E}\to\mathcal{E}'}$*, and then the collection of morphisms presented earlier is guaranteed to form a natural transformation from* $C_{\mathcal{E}}(\mathcal{C})$ *to* $\mathcal{P}$*, i.e. a morphism of* $\mathbf{E} \pitchfork \mathbf{C}$*. Finally, we can define* $i_{\mathcal{E},\mathcal{C}} : \mathcal{C} \to \pi_{\mathcal{E}}(C_{\mathcal{E}}(\mathcal{C}))$ *to be* $\kappa_{id_{\mathcal{E}}} : \mathcal{C} \to \bigoplus_{e:\mathcal{E}\to\mathcal{E}}\mathcal{C}$*, and so* $\kappa_{id_{\mathcal{E}}}\,;[p\,;\mathcal{P}(e)]_{e:\mathcal{E}\to\mathcal{E}}$ *equals* $p\,;\mathcal{P}(id_{\mathcal{E}})$ *which equals* p *as desired.* $I_{\mathcal{E}}$ *can be extended into a functor because* $\oplus$ *is functorial and* κ *is natural.*