thm_2Ewords_2EROL__BITWISE (TMdoTuXsMBfxNhzMUN1cji3JqaNZAQpmnvT)

October 26, 2020

Definition 1 *We define* c_2Emin_2E_3D *to be* $\lambda A.\lambda x \in A.\lambda y \in A.inj\_\_o\ (x = y)$ *of type* $\iota \Rightarrow \iota$.

Definition 2 *We define* c_2Ebool_2ET *to be* $(ap\ (ap\ (\text{c\_2Emin\_2E\_3D}\ (2^2))\ (\lambda V0x \in 2.V0x))\ (\lambda V1x \in 2.V1$

Let $ty\_2Enum\_2Enum : \iota$ be given. Assume the following.

$$nonempty\ ty\_2Enum\_2Enum \tag{1}$$

Let $c\_2Earithmetic\_2EMOD : \iota$ be given. Assume the following.

$$c\_2Earithmetic\_2EMOD \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \tag{2}$$

Let $ty\_2Ebool\_2Eitself : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty\ A0 \Rightarrow nonempty\ (ty\_2Ebool\_2Eitself\ A0) \tag{3}$$

Let $c\_2Ebool\_2Ethe\_\_value : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow c\_2Ebool\_2Ethe\_\_value\ A\_27a \in (ty\_2Ebool\_2Eitself\ A\_27a) \tag{4}$$

Let $c\_2Efcp\_2Edimindex : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow c\_2Efcp\_2Edimindex\ A\_27a \in (ty\_2Enum\_2Enum^{(ty\_2Ebool\_2Eitself\ A\_27a)}) \tag{5}$$

Let $c\_2Earithmetic\_2E\_2D : \iota$ be given. Assume the following.

$$c\_2Earithmetic\_2E\_2D \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \tag{6}$$

Let $c\_2Earithmetic\_2E\_2B : \iota$ be given. Assume the following.

$$c\_2Earithmetic\_2E\_2B \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \tag{7}$$

Let $ty\_2Efcp\_2Efinite\_\_image : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty\ A0 \Rightarrow nonempty\ (ty\_2Efcp\_2Efinite\_\_image\ A0) \tag{8}$$

Definition 3 *We define* c_2Ebool_2E_21 *to be* $\lambda A\_27a : \iota.(\lambda V0P \in (2^{A\_27a}).(ap\ (ap\ (c\_2Emin\_2E\_3D\ (2^{A\_27}$

Definition 4 *We define* c_2Ebool_2EF *to be* $(ap\ (c\_2Ebool\_2E\_21\ 2)\ (\lambda V0t \in 2.V0t))$.

Definition 5 *We define* c_2Emin_2E_3D_3D_3E *to be* $\lambda P \in 2.\lambda Q \in 2.inj\_\_o\ (p\ P \Rightarrow p\ Q)$
of type ι.

Definition 6 *We define* c_2Ebool_2E_7E *to be* $(\lambda V0t \in 2.(ap\ (ap\ c\_2Emin\_2E\_3D\_3D\_3E\ V0t)\ c\_2Ebool\_2EF$

Definition 7 *We define* c_2Ebool_2E_2F_5C *to be* $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap\ (c\_2Ebool\_2E\_21\ 2)\ (\lambda V2t \in 2$

Let $c\_2Enum\_2EREP\_\_num : \iota$ be given. Assume the following.

$$c\_2Enum\_2EREP\_\_num \in (omega^{ty\_2Enum\_2Enum}) \tag{9}$$

Let $c\_2Enum\_2ESUC\_\_REP : \iota$ be given. Assume the following.

$$c\_2Enum\_2ESUC\_\_REP \in (omega^{omega}) \tag{10}$$

Let $c\_2Enum\_2EABS\_\_num : \iota$ be given. Assume the following.

$$c\_2Enum\_2EABS\_\_num \in (ty\_2Enum\_2Enum^{omega}) \tag{11}$$

Definition 8 *We define* c_2Enum_2ESUC *to be* $\lambda V0m \in ty\_2Enum\_2Enum.(ap\ c\_2Enum\_2EABS\_\_num\ ($

Definition 9 *We define* c_2Emin_2E_40 *to be* $\lambda A.\lambda P \in 2^A$**.if** $(\exists x \in A.p\ (ap\ P\ x))$ **then** $(the\ (\lambda x.x \in A \wedge p$
of type $\iota \Rightarrow \iota$.

Definition 10 *We define* c_2Ebool_2E_3F *to be* $\lambda A\_27a : \iota.(\lambda V0P \in (2^{A\_27a}).(ap\ V0P\ (ap\ (c\_2Emin\_2E\_40$

Definition 11 *We define* c_2Eprim__rec_2E_3C *to be* $\lambda V0m \in ty\_2Enum\_2Enum.\lambda V1n \in ty\_2Enum\_2Enu$

Definition 12 *We define* c_2Ebool_2E_3F_21 *to be* $\lambda A\_27a : \iota.(\lambda V0P \in (2^{A\_27a}).(ap\ (ap\ c\_2Ebool\_2E\_2F\_5C$

Definition 13 *We define* c_2Efcp_2Efinite__index *to be* $\lambda A\_27a : \iota.(ap\ (c\_2Emin\_2E\_40\ (A\_27a^{ty\_2Enum\_2Enu}$

Let $ty\_2Efcp\_2Ecart : \iota \Rightarrow \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty\ A0 \Rightarrow \forall A1.nonempty\ A1 \Rightarrow nonempty\ (ty\_2Efcp\_2Ecart\ A0\ A1) \tag{12}$$

Let $c\_2Efcp\_2Edest\_\_cart : \iota \Rightarrow \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow \forall A\_27b.nonempty\ A\_27b \Rightarrow c\_2Efcp\_2Edest\_\_cart\ A\_27a\ A\_27b \in ((A\_27a^{(ty\_2Efcp\_2Efinite\_\_image\ A\_27b)})^{(ty\_2Efcp\_2Ecart\ A\_27a\ A\_27b)}) \tag{13}$$

Definition 14 *We define* c_2Efcp_2Efcp__index *to be* $\lambda A\_27a : \iota.\lambda A\_27b : \iota.\lambda V0x \in (ty\_2Efcp\_2Ecart\ A\_27$

Definition 15 *We define* c_2Efcp_2EFCP *to be* $\lambda A\_27a : \iota.\lambda A\_27b : \iota.(\lambda V0g \in (A\_27a^{ty\_2Enum\_2Enum}).(ap\ ($

Definition 16 *We define* c_2Ewords_2Eword__ror *to be* $\lambda A\_27a : \iota.\lambda V0w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).\lambda V1$

Definition 17 *We define* c_2Ewords_2Eword__rol *to be* $\lambda A\_27a : \iota.\lambda V0w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).\lambda V1$

Definition 18 *We define* c_2Ewords_2Eword__xor *to be* $\lambda A\_27a : \iota.\lambda V0v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).\lambda V1$

Definition 19 *We define* c_2Ebool_2E_5C_2F *to be* $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap\ (\text{c\_2Ebool\_2E\_21}\ 2)\ (\lambda V2t \in$

Definition 20 *We define* c_2Ewords_2Eword__or *to be* $\lambda A\_27a : \iota.\lambda V0v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).\lambda V1\iota$

Definition 21 *We define* c_2Ewords_2Eword__and *to be* $\lambda A\_27a : \iota.\lambda V0v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).\lambda V$

Assume the following.

$$True \tag{14}$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow (\forall V0x \in A\_27a.((V0x = V0x) \Leftrightarrow True)) \tag{15}$$

Assume the following.

$$\begin{gathered}\forall A\_27a.nonempty\ A\_27a \Rightarrow ((\forall V0n \in ty\_2Enum\_2Enum.\\ (\forall V1v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V2w \in (ty\_2Efcp\_2Ecart\\ 2\ A\_27a).((ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_and}\ A\_27a)\ (ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_ror}\\ A\_27a)\ V2w)\ V0n))\ (ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_ror}\ A\_27a)\ V1v)\ V0n)) =\\ (ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_ror}\ A\_27a)\ (ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_and}\\ A\_27a)\ V2w)\ V1v))\ V0n)))))\wedge((\forall V3n \in ty\_2Enum\_2Enum.(\forall V4v \in\\ (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V5w \in (ty\_2Efcp\_2Ecart\ 2\\ A\_27a).((ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_or}\ A\_27a)\ (ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_ror}\\ A\_27a)\ V5w)\ V3n))\ (ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_ror}\ A\_27a)\ V4v)\ V3n)) =\\ (ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_ror}\ A\_27a)\ (ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_or}\\ A\_27a)\ V5w)\ V4v))\ V3n)))))\wedge(\forall V6n \in ty\_2Enum\_2Enum.(\forall V7v \in\\ (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V8w \in (ty\_2Efcp\_2Ecart\ 2\\ A\_27a).((ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_xor}\ A\_27a)\ (ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_ror}\\ A\_27a)\ V8w)\ V6n))\ (ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_ror}\ A\_27a)\ V7v)\ V6n)) =\\ (ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_ror}\ A\_27a)\ (ap\ (ap\ (\text{c\_2Ewords\_2Eword\_\_xor}\\ A\_27a)\ V8w)\ V7v))\ V6n)))))))\end{gathered} \tag{16}$$

Theorem 1

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow \forall A\_27b.nonempty\ A\_27b \Rightarrow \forall A\_27c.\ nonempty\ A\_27c \Rightarrow ((\forall V0n \in ty\_2Enum\_2Enum.(\forall V1v \in (\ ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V2w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).\ ((ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_and}\ A\_27a)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_rol}\ A\_27a)\ V2w)\ V0n))\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_rol}\ A\_27a)\ V1v)\ V0n)) = (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_rol}\ A\_27a)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_and}\ A\_27a)\ V2w)\ V1v))\ V0n)))))\wedge((\forall V3n \in ty\_2Enum\_2Enum.(\forall V4v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27b).(\forall V5w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27b).((ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_or}\ A\_27b)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_rol}\ A\_27b)\ V5w)\ V3n))\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_rol}\ A\_27b)\ V4v)\ V3n)) = (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_rol}\ A\_27b)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_or}\ A\_27b)\ V5w)\ V4v))\ V3n)))))\wedge(\forall V6n \in ty\_2Enum\_2Enum.(\forall V7v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27c).(\forall V8w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27c).((ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_xor}\ A\_27c)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_rol}\ A\_27c)\ V8w)\ V6n))\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_rol}\ A\_27c)\ V7v)\ V6n)) = (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_rol}\ A\_27c)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_xor}\ A\_27c)\ V8w)\ V7v))\ V6n)))))))$$