thm_2Ewords_2EWORD__EXTRACT__OVER__BITWISE (TMRzopWftWjYhbbvqrc3C5wo319322rDWpo)

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* $(ap\ (ap\ (\text{c\_2Emin\_2E\_3D}\ (2^2))\ (\lambda V0x \in 2.V0x))\ (\lambda V1x \in 2.V1$

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

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

Definition 5 *We define* c_2Ecombin_2Eo *to be* $\lambda A\_27a : \iota.\lambda A\_27b : \iota.\lambda A\_27c : \iota.\lambda V0f \in (A\_27b^{A\_27c}).\lambda V1g$

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

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

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

$$c\_2Earithmetic\_2E\_2B \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \tag{2}$$

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

$$\forall A0.nonempty\ A0 \Rightarrow nonempty\ (ty\_2Efcp\_2Efinite\_\_image\ A0) \tag{3}$$

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

$$\forall A0.nonempty\ A0 \Rightarrow nonempty\ (ty\_2Ebool\_2Eitself\ A0) \tag{4}$$

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

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow c\_2Ebool\_2Ethe\_\_value\ A\_27a \in (ty\_2Ebool\_2Eitself\ A\_27a) \tag{5}$$

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

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow c\_2Efcp\_2Edimindex\ A\_27a \in (ty\_2Enum\_2Enum^{(ty\_2Ebool\_2Eitself\ A\_27a)}) \tag{6}$$

Definition 6 *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 7 *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 8 *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.

$$c\_2Enum\_2EREP\_\_num \in (omega^{ty\_2Enum\_2Enum}) \tag{7}$$

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

$$c\_2Enum\_2ESUC\_\_REP \in (omega^{omega}) \tag{8}$$

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

$$c\_2Enum\_2EABS\_\_num \in (ty\_2Enum\_2Enum^{omega}) \tag{9}$$

Definition 9 *We define* c_2Enum_2ESUC *to be* $\lambda V0m \in ty\_2Enum\_2Enum.(ap\ c\_2Enum\_2EABS\_\_num$ (

Definition 10 *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 11 *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 12 *We define* c_2Eprim__rec_2E_3C *to be* $\lambda V0m \in ty\_2Enum\_2Enum.\lambda V1n \in ty\_2Enum\_2Enu$

Definition 13 *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 14 *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.

$$\forall A0.nonempty\ A0 \Rightarrow \forall A1.nonempty\ A1 \Rightarrow nonempty\ (ty\_2Efcp\_2Ecart\ A0\ A1) \tag{10}$$

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

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow \forall A\_27b.nonempty\ A\_27b \Rightarrow c\_2Efcp\_2Edest\_\_cart\ A\_27a\ A\_27b \in ((A\_27a^{(ty\_2Efcp\_2Efinite\_\_image\ A\_27b)})^{(ty\_2Efcp\_2Ecart\ A\_27a\ A\_27b)}) \tag{11}$$

Definition 15 *We define* c_2Efcp_2Efcp__index *to be* $\lambda A\_27a : \iota.\lambda A\_27b : \iota.\lambda V0x \in (ty\_2Efcp\_2Ecart\ A\_27$

Let $c\_2Enum\_2EZERO\_\_REP : \iota$ be given. Assume the following.

$$c\_2Enum\_2EZERO\_\_REP \in omega \tag{12}$$

Definition 16 *We define* c_2Enum_2E0 *to be* $(ap\ c\_2Enum\_2EABS\_\_num\ c\_2Enum\_2EZERO\_\_REP)$.

Definition 17 *We define* c_2Earithmetic_2EZERO *to be* c_2Enum_2E0.

Definition 18 *We define* c_2Earithmetic_2EBIT1 *to be* $\lambda V0n \in ty\_2Enum\_2Enum.(ap\ (ap\ c\_2Earithmetic$

Definition 19 *We define* c_2Earithmetic_2ENUMERAL *to be* $\lambda V0x \in ty\_2Enum\_2Enum.V0x.$

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

$$c\_2Earithmetic\_2E\_2D \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \tag{13}$$

Definition 20 *We define* c_2Ebool_2ECOND *to be* $\lambda A\_27a : \iota.(\lambda V0t \in 2.(\lambda V1t1 \in A\_27a.(\lambda V2t2 \in A\_27a.($

Definition 21 *We define* c_2Earithmetic_2EMIN *to be* $\lambda V0m \in ty\_2Enum\_2Enum.\lambda V1n \in ty\_2Enum\_2En$

Definition 22 *We define* c_2Ebool_2E_5C_2F *to be* $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap\ (c\_2Ebool\_2E\_21\ 2)\ (\lambda V2t \in$

Definition 23 *We define* c_2Earithmetic_2E_3C_3D *to be* $\lambda V0m \in ty\_2Enum\_2Enum.\lambda V1n \in ty\_2Enum\_2$

Definition 24 *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 25 *We define* c_2Ewords_2Eword__bits *to be* $\lambda A\_27a : \iota.\lambda V0h \in ty\_2Enum\_2Enum.\lambda V1l \in ty\_2$

Definition 26 *We define* c_2Earithmetic_2EBIT2 *to be* $\lambda V0n \in ty\_2Enum\_2Enum.(ap\ (ap\ c\_2Earithmetic$

Let $c\_2Earithmetic\_2EEXP : \iota$ be given. Assume the following.

$$c\_2Earithmetic\_2EEXP \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \tag{14}$$

Definition 27 *We define* c_2Ebit_2ESBIT *to be* $\lambda V0b \in 2.\lambda V1n \in ty\_2Enum\_2Enum.(ap\ (ap\ (ap$ (c_2Eboo

Let $c\_2Esum\_\_num\_2ESUM : \iota$ be given. Assume the following.

$$c\_2Esum\_\_num\_2ESUM \in ((ty\_2Enum\_2Enum^{(ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})})^{ty\_2Enum\_2Enum}) \tag{15}$$

Definition 28 *We define* c_2Ewords_2Ew2n *to be* $\lambda A\_27a : \iota.\lambda V0w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(ap\ (ap\ c$

Let $c\_2Earithmetic\_2EDIV : \iota$ be given. Assume the following.

$$c\_2Earithmetic\_2EDIV \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \tag{16}$$

Definition 29 *We define* c_2Ebit_2EDIV__2EXP *to be* $\lambda V0x \in ty\_2Enum\_2Enum.\lambda V1n \in ty\_2Enum\_2En$

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

$$c\_2Earithmetic\_2EMOD \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \tag{17}$$

Definition 30 *We define* c_2Ebit_2EMOD__2EXP *to be* $\lambda V0x \in ty\_2Enum\_2Enum.\lambda V1n \in ty\_2Enum\_2E$

Definition 31 *We define* c_2Ebit_2EBITS *to be* $\lambda V0h \in ty\_2Enum\_2Enum.\lambda V1l \in ty\_2Enum\_2Enum.\lambda V$

Definition 32 *We define* c_2Ebit_2EBIT *to be* $\lambda V0b \in ty\_2Enum\_2Enum.\lambda V1n \in ty\_2Enum\_2Enum.(ap$

Definition 33 *We define* c_2Ewords_2En2w *to be* $\lambda A\_27a : \iota.\lambda V0n \in ty\_2Enum\_2Enum.(ap$ (c_2Efcp_2EFC

Definition 34 *We define* c_2Ewords_2Ew2w *to be* $\lambda A\_27a : \iota.\lambda A\_27b : \iota.\lambda V0w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27$

Definition 35 *We define* c_2Ewords_2Eword__extract *to be* $\lambda A\_27a : \iota.\lambda A\_27b : \iota.\lambda V0h \in ty\_2Enum\_2Enum$

Definition 36 *We define* c_2Ewords_2Eword__xor *to be* $\lambda A\_27a : \iota.\lambda V0v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).\lambda V1$

Definition 37 *We define* c_2Ewords_2Eword__or *to be* $\lambda A\_27a : \iota.\lambda V0v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).\lambda V1v$

Definition 38 *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.

$$True \tag{18}$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow (\forall V0t \in 2.((\forall V1x \in A\_27a.(p\ V0t)) \Leftrightarrow (p\ V0t))) \tag{19}$$

Assume the following.

$$(\forall V0t \in 2.(((True \wedge (p\ V0t)) \Leftrightarrow (p\ V0t)) \wedge ((((p\ V0t) \wedge True) \Leftrightarrow (p\ V0t)) \wedge (((False \wedge (p\ V0t)) \Leftrightarrow False) \wedge ((((p\ V0t) \wedge False) \Leftrightarrow False) \wedge (((p\ V0t) \wedge (p\ V0t)) \Leftrightarrow (p\ V0t))))))) \tag{20}$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow (\forall V0x \in A\_27a.((V0x = V0x) \Leftrightarrow True)) \tag{21}$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow (\forall V0x \in A\_27a.(\forall V1y \in A\_27a.((V0x = V1y) \Leftrightarrow (V1y = V0x)))) \tag{22}$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow \forall A\_27b.nonempty\ A\_27b \Rightarrow \forall A\_27c.\ nonempty\ A\_27c \Rightarrow (\forall V0f \in (A\_27b^{A\_27a}).(\forall V1g \in (A\_27a^{A\_27c}).\ (\forall V2x \in A\_27c.((ap\ (ap\ (ap$ (c_2Ecombin_2Eo $A\_27c\ A\_27b\ A\_27a$) $V0f)\ V1g)\ V2x) = (ap\ V0f\ (ap\ V1g\ V2x))))))) \tag{23}$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow ((\forall V0h \in ty\_2Enum\_2Enum.(\forall V1l \in ty\_2Enum\_2Enum.(\forall V2v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V3w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).((ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_and}\ A\_27a)\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_bits}\ A\_27a)\ V0h)\ V1l)\ V2v))\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_bits}\ A\_27a)\ V0h)\ V1l)\ V3w)) = (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_bits}\ A\_27a)\ V0h)\ V1l)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_and}\ A\_27a)\ V2v)\ V3w)))))))\wedge((\forall V4h \in ty\_2Enum\_2Enum.(\forall V5l \in ty\_2Enum\_2Enum.(\forall V6v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V7w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).((ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_or}\ A\_27a)\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_bits}\ A\_27a)\ V4h)\ V5l)\ V6v))\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_bits}\ A\_27a)\ V4h)\ V5l)\ V7w)) = (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_bits}\ A\_27a)\ V4h)\ V5l)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_or}\ A\_27a)\ V6v)\ V7w)))))))\wedge(\forall V8h \in ty\_2Enum\_2Enum.(\forall V9l \in ty\_2Enum\_2Enum.(\forall V10v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V11w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).((ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_xor}\ A\_27a)\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_bits}\ A\_27a)\ V8h)\ V9l)\ V10v))\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_bits}\ A\_27a)\ V8h)\ V9l)\ V11w)) = (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_bits}\ A\_27a)\ V8h)\ V9l)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_xor}\ A\_27a)\ V10v)\ V11w)))))))) \tag{24}$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow \forall A\_27b.nonempty\ A\_27b \Rightarrow (\forall V0v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V1w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).((ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_and}\ A\_27b)\ (ap\ (\mathsf{c\_2Ewords\_2Ew2w}\ A\_27a\ A\_27b)\ V0v))\ (ap\ (\mathsf{c\_2Ewords\_2Ew2w}\ A\_27a\ A\_27b)\ V1w)) = (ap\ (\mathsf{c\_2Ewords\_2Ew2w}\ A\_27a\ A\_27b)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_and}\ A\_27a)\ V0v)\ V1w)))))\wedge((\forall V2v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V3w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).((ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_or}\ A\_27b)\ (ap\ (\mathsf{c\_2Ewords\_2Ew2w}\ A\_27a\ A\_27b)\ V2v))\ (ap\ (\mathsf{c\_2Ewords\_2Ew2w}\ A\_27a\ A\_27b)\ V3w)) = (ap\ (\mathsf{c\_2Ewords\_2Ew2w}\ A\_27a\ A\_27b)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_or}\ A\_27a)\ V2v)\ V3w)))))\wedge(\forall V4v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V5w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).((ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_xor}\ A\_27b)\ (ap\ (\mathsf{c\_2Ewords\_2Ew2w}\ A\_27a\ A\_27b)\ V4v))\ (ap\ (\mathsf{c\_2Ewords\_2Ew2w}\ A\_27a\ A\_27b)\ V5w)) = (ap\ (\mathsf{c\_2Ewords\_2Ew2w}\ A\_27a\ A\_27b)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_xor}\ A\_27a)\ V4v)\ V5w))))))) \tag{25}$$

Theorem 1

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow \forall A\_27b.nonempty\ A\_27b \Rightarrow \forall A\_27c.\ nonempty\ A\_27c \Rightarrow \forall A\_27d.nonempty\ A\_27d \Rightarrow ((\forall V0h \in ty\_2Enum\_2Enum.\ (\forall V1l \in ty\_2Enum\_2Enum.(\forall V2v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V3w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).((ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_and}\ A\_27b)\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_extract}\ A\_27a\ A\_27b)\ V0h)\ V1l)\ V2v))\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_extract}\ A\_27a\ A\_27b)\ V0h)\ V1l)\ V3w)) = (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_extract}\ A\_27a\ A\_27b)\ V0h)\ V1l)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_and}\ A\_27a)\ V2v)\ V3w)))))))\wedge ((\forall V4h \in ty\_2Enum\_2Enum.(\forall V5l \in ty\_2Enum\_2Enum.(\forall V6v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V7w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).((ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_or}\ A\_27c)\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_extract}\ A\_27a\ A\_27c)\ V4h)\ V5l)\ V6v))\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_extract}\ A\_27a\ A\_27c)\ V4h)\ V5l)\ V7w)) = (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_extract}\ A\_27a\ A\_27c)\ V4h)\ V5l)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_or}\ A\_27a)\ V6v)\ V7w)))))))\wedge(\forall V8h \in ty\_2Enum\_2Enum.(\forall V9l \in ty\_2Enum\_2Enum.(\forall V10v \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).(\forall V11w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).((ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_xor}\ A\_27d)\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_extract}\ A\_27a\ A\_27d)\ V8h)\ V9l)\ V10v))\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_extract}\ A\_27a\ A\_27d)\ V8h)\ V9l)\ V11w)) = (ap\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_extract}\ A\_27a\ A\_27d)\ V8h)\ V9l)\ (ap\ (ap\ (\mathsf{c\_2Ewords\_2Eword\_\_xor}\ A\_27a)\ V10v)\ V11w)))))))))$$