

thm_2Ewords_2EROR__BITWISE
(TMaKsG8JgGikbLGKjiKVGPWebpogw3SMo2b)

October 26, 2020

Let $ty_2Enum_2Enum : \iota$ be given. Assume the following.

$$nonempty\ ty_2Enum_2Enum \tag{1}$$

Let $c_2Earithmetic_2EDIV : \iota$ be given. Assume the following.

$$c_2Earithmetic_2EDIV \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \tag{2}$$

Let $c_2Earithmetic_2E_2A : \iota$ be given. Assume the following.

$$c_2Earithmetic_2E_2A \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \tag{3}$$

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 $(ap (ap (c_2Emin_2E_3D (2^2)) (\lambda V0x \in 2.V0x)) (\lambda V1x \in 2.V1x))$

Definition 3 We define $c_2Ebool_2E_21$ to be $\lambda A.27a : \iota.(\lambda V0P \in (2^{A-27a}).(ap (ap (c_2Emin_2E_3D (2^{A-27a}))$

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 $\lambda P \in 2.\lambda Q \in 2.inj_o (p \Rightarrow q)$ of type ι .

Definition 6 We define $c_2Ebool_2E_2F_5C$ to be $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap (c_2Ebool_2E_21 2) (\lambda V2t \in 2.V2t))$

Let $ty_2EfcP_2Efinite_image : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty\ A0 \Rightarrow nonempty (ty_2EfcP_2Efinite_image\ A0) \tag{4}$$

Let $ty_2Ebool_2Eitself : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty\ A0 \Rightarrow nonempty (ty_2Ebool_2Eitself\ A0) \tag{5}$$

Let $c_2Ebool_2Ethe_value : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow c_2Ebool_2Ethe_value\ A_27a \in (ty_2Ebool_2Eitself\ A_27a) \quad (6)$$

Let $c_2Efcf_2Edimindex : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow c_2Efcf_2Edimindex\ A_27a \in (ty_2Enum_2Enum^{(ty_2Ebool_2Eitself\ A_27a)}) \quad (7)$$

Definition 7 We define c_2Ebool_2E7E to be $(\lambda V0t \in 2.(ap\ (ap\ c_2Emin_2E_3D_3D_3E\ V0t)\ c_2Ebool_2E7E))$

Let $c_2Enum_2EREP_num : \iota$ be given. Assume the following.

$$c_2Enum_2EREP_num \in (\omega^{ty_2Enum_2Enum}) \quad (8)$$

Let $c_2Enum_2ESUC_REP : \iota$ be given. Assume the following.

$$c_2Enum_2ESUC_REP \in (\omega^{\omega}) \quad (9)$$

Let $c_2Enum_2EABS_num : \iota$ be given. Assume the following.

$$c_2Enum_2EABS_num \in (ty_2Enum_2Enum^{\omega}) \quad (10)$$

Definition 8 We define c_2Enum_2ESUC to be $\lambda V0m \in ty_2Enum_2Enum.(ap\ c_2Enum_2EABS_num\ V0m)$

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

Definition 10 We define $c_2Ebool_2E_3F$ to be $\lambda A_27a : \iota.(\lambda V0P \in (2^{A_27a}).(ap\ V0P\ (ap\ (c_2Emin_2E_40\ A_27a)\ V0P)))$

Definition 11 We define $c_2Eprim_rec_2E_3C$ to be $\lambda V0m \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum.(ap\ V1n\ (ap\ c_2Eprim_rec_2E_3C\ V0m\ V1n))$

Definition 12 We define $c_2Ebool_2E_3F_21$ to be $\lambda A_27a : \iota.(\lambda V0P \in (2^{A_27a}).(ap\ (ap\ c_2Ebool_2E_2F_5C\ A_27a)\ V0P))$

Definition 13 We define $c_2Efcf_2Efinite_index$ to be $\lambda A_27a : \iota.(ap\ (c_2Emin_2E_40\ (A_27a\ ty_2Enum_2Enum)))$

Let $ty_2Efcf_2Ecart : \iota \Rightarrow \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty\ A0 \Rightarrow \forall A1.nonempty\ A1 \Rightarrow nonempty\ (ty_2Efcf_2Ecart\ A0\ A1) \quad (11)$$

Let $c_2Efcf_2Edest_cart : \iota \Rightarrow \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow \forall A_27b.nonempty\ A_27b \Rightarrow c_2Efcf_2Edest_cart\ A_27a\ A_27b \in ((A_27a^{(ty_2Efcf_2Efinite_image\ A_27b)})^{(ty_2Efcf_2Ecart\ A_27a\ A_27b)}) \quad (12)$$

Definition 14 We define $c_2Efcf_2Efcf_index$ to be $\lambda A_27a : \iota.\lambda A_27b : \iota.\lambda V0x \in (ty_2Efcf_2Ecart\ A_27a\ A_27b).$

Definition 15 We define c_2Efcf_2EFCF to be $\lambda A_27a : \iota.\lambda A_27b : \iota.(\lambda V0g \in (A_27a\ ty_2Enum_2Enum)).(ap\ V0g\ (ap\ c_2Efcf_2EFCF\ A_27a\ A_27b\ V0g))$

Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow (\forall V0x \in A_27a. (\forall V1y \in A_27a. ((V0x = V1y) \Leftrightarrow (V1y = V0x)))) \quad (21)$$

Assume the following.

$$(\forall V0t \in 2. (((True \Leftrightarrow (p\ V0t)) \Leftrightarrow (p\ V0t)) \wedge (((p\ V0t) \Leftrightarrow True) \Leftrightarrow (p\ V0t)) \wedge (((False \Leftrightarrow (p\ V0t)) \Leftrightarrow \neg(p\ V0t)) \wedge (((p\ V0t) \Leftrightarrow False) \Leftrightarrow \neg(p\ V0t)))))) \quad (22)$$

Assume the following.

$$(\forall V0t1 \in 2. (\forall V1t2 \in 2. (\forall V2t3 \in 2. (((p\ V0t1) \Rightarrow ((p\ V1t2) \Rightarrow (p\ V2t3))) \Leftrightarrow (((p\ V0t1) \wedge (p\ V1t2)) \Rightarrow (p\ V2t3)))))) \quad (23)$$

Assume the following.

$$(\forall V0x \in 2. (\forall V1x_27 \in 2. (\forall V2y \in 2. (\forall V3y_27 \in 2. (((p\ V0x) \Leftrightarrow (p\ V1x_27)) \wedge ((p\ V1x_27) \Rightarrow ((p\ V2y) \Leftrightarrow (p\ V3y_27)))))) \Rightarrow (((p\ V0x) \Rightarrow (p\ V2y)) \Leftrightarrow ((p\ V1x_27) \Rightarrow (p\ V3y_27)))))) \quad (24)$$

Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow \forall A_27b.nonempty\ A_27b \Rightarrow (\forall V0x \in (ty_2EfcP_2Ecart\ A_27a\ A_27b). (\forall V1y \in (ty_2EfcP_2Ecart\ A_27a\ A_27b). ((V0x = V1y) \Leftrightarrow (\forall V2i \in ty_2Enum_2Enum. ((p\ (ap\ c_2Eprim_rec_2E_3C\ V2i)\ (ap\ (c_2EfcP_2Edimindex\ A_27b)\ (c_2Ebool_2Ethe_value\ A_27b)))) \Rightarrow ((ap\ (ap\ (c_2EfcP_2EfcP_index\ A_27a\ A_27b)\ V0x)\ V2i) = (ap\ (ap\ (c_2EfcP_2EfcP_index\ A_27a\ A_27b)\ V1y)\ V2i)))))) \quad (25)$$

Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow \forall A_27b.nonempty\ A_27b \Rightarrow (\forall V0g \in (A_27a^{ty_2Enum_2Enum}). (\forall V1i \in ty_2Enum_2Enum. ((p\ (ap\ (ap\ c_2Eprim_rec_2E_3C\ V1i)\ (ap\ (c_2EfcP_2Edimindex\ A_27b)\ (c_2Ebool_2Ethe_value\ A_27b)))) \Rightarrow ((ap\ (ap\ (c_2EfcP_2EfcP_index\ A_27a\ A_27b)\ (ap\ (c_2EfcP_2EFCP\ A_27a\ A_27b)\ V0g))\ V1i) = (ap\ V0g\ V1i)))))) \quad (26)$$

Assume the following.

$$(\forall V0t \in 2. ((\neg(\neg(p\ V0t))) \Leftrightarrow (p\ V0t))) \quad (27)$$

Assume the following.

$$(\forall V0A \in 2. ((p\ V0A) \Rightarrow ((\neg(p\ V0A)) \Rightarrow False))) \quad (28)$$

Assume the following.

$$(\forall V0A \in 2. (\forall V1B \in 2. (((\neg((p V0A) \vee (p V1B))) \Rightarrow False) \Leftrightarrow ((p V0A) \Rightarrow False) \Rightarrow ((\neg(p V1B)) \Rightarrow False)))) \quad (29)$$

Assume the following.

$$(\forall V0A \in 2. (\forall V1B \in 2. (((\neg(\neg(p V0A)) \vee (p V1B))) \Rightarrow False) \Leftrightarrow ((p V0A) \Rightarrow ((\neg(p V1B)) \Rightarrow False)))) \quad (30)$$

Assume the following.

$$(\forall V0A \in 2. (((\neg(p V0A)) \Rightarrow False) \Rightarrow (((p V0A) \Rightarrow False) \Rightarrow False))) \quad (31)$$

Assume the following.

$$(\forall V0p \in 2. (\forall V1q \in 2. (\forall V2r \in 2. (((p V0p) \Leftrightarrow (p V1q) \Leftrightarrow (p V2r)) \Leftrightarrow (((p V0p) \vee ((p V1q) \vee (p V2r))) \wedge (((p V0p) \vee (\neg(p V2r)) \vee (\neg(p V1q)))) \wedge (((p V1q) \vee ((\neg(p V2r)) \vee (\neg(p V0p)))) \wedge ((p V2r) \vee ((\neg(p V1q)) \vee (\neg(p V0p)))))))))) \quad (32)$$

Assume the following.

$$(\forall V0p \in 2. (\forall V1q \in 2. (((p V0p) \Leftrightarrow (\neg(p V1q))) \Leftrightarrow (((p V0p) \vee (p V1q)) \wedge ((\neg(p V1q)) \vee (\neg(p V0p)))))) \quad (33)$$

Assume the following.

$$\forall A_27a. nonempty A_27a \Rightarrow (p (ap (ap (c_2Eprim_rec_2E_3C c_2Enum_2E0) (ap (c_2Efc_2Edimindex A_27a) (c_2Ebool_2Ethe_value A_27a)))) \quad (34)$$

Theorem 1

$$\begin{aligned} & \forall A_27a. nonempty A_27a \Rightarrow ((\forall V0n \in ty_2Enum_2Enum. \\ & (\forall V1v \in (ty_2Efc_2Ecart 2 A_27a). (\forall V2w \in (ty_2Efc_2Ecart \\ & 2 A_27a). ((ap (ap (c_2Ewords_2Eword_and A_27a) (ap (ap (c_2Ewords_2Eword_ror \\ & A_27a) V2w) V0n)) (ap (ap (c_2Ewords_2Eword_ror A_27a) V1v) V0n)) = \\ & (ap (ap (c_2Ewords_2Eword_ror A_27a) (ap (ap (c_2Ewords_2Eword_and \\ & A_27a) V2w) V1v)) V0n)))) \wedge ((\forall V3n \in ty_2Enum_2Enum. (\forall V4v \in \\ & (ty_2Efc_2Ecart 2 A_27a). (\forall V5w \in (ty_2Efc_2Ecart 2 \\ & A_27a). ((ap (ap (c_2Ewords_2Eword_or A_27a) (ap (ap (c_2Ewords_2Eword_ror \\ & A_27a) V5w) V3n)) (ap (ap (c_2Ewords_2Eword_ror A_27a) V4v) V3n)) = \\ & (ap (ap (c_2Ewords_2Eword_ror A_27a) (ap (ap (c_2Ewords_2Eword_or \\ & A_27a) V5w) V4v)) V3n)))) \wedge ((\forall V6n \in ty_2Enum_2Enum. (\forall V7v \in \\ & (ty_2Efc_2Ecart 2 A_27a). (\forall V8w \in (ty_2Efc_2Ecart 2 \\ & A_27a). ((ap (ap (c_2Ewords_2Eword_xor A_27a) (ap (ap (c_2Ewords_2Eword_ror \\ & A_27a) V8w) V6n)) (ap (ap (c_2Ewords_2Eword_ror A_27a) V7v) V6n)) = \\ & (ap (ap (c_2Ewords_2Eword_ror A_27a) (ap (ap (c_2Ewords_2Eword_xor \\ & A_27a) V8w) V7v)) V6n)))))) \end{aligned}$$