

# thm\_2Ewords\_2EWORD\_\_XOR\_\_ASSOC (TMa8yqFCP1cyFHXDEJBiPLvwBq7wzqzddce)

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  $c\_2Ebool\_2E\_ET$  to be  $(ap (ap (c\_2Emin\_2E\_3D (2^2)) (\lambda V0x \in 2.V0x)) (\lambda V1x \in 2.V1x))$

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

$$\forall A0.nonempty A0 \Rightarrow nonempty (ty\_2Ebool\_2Eitself A0) \quad (1)$$

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

$$\forall A\_27a.nonempty A\_27a \Rightarrow c\_2Ebool\_2Ethe\_value A\_27a \in (ty\_2Ebool\_2Eitself A\_27a) \quad (2)$$

Let  $ty\_2Eenum\_2Eenum : \iota$  be given. Assume the following.

$$nonempty ty\_2Eenum\_2Eenum \quad (3)$$

Let  $c\_2Efcfcp\_2Edimindex : \iota \Rightarrow \iota$  be given. Assume the following.

$$\forall A\_27a.nonempty A\_27a \Rightarrow c\_2Efcfcp\_2Edimindex A\_27a \in (ty\_2Eenum\_2Eenum^{(ty\_2Ebool\_2Eitself A\_27a)}) \quad (4)$$

**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  $c\_2Ebool\_2E\_EF$  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  $\iota$ .

**Definition 6** We define  $c\_2Ebool\_2E\_7E$  to be  $(\lambda V0t \in 2.(ap (ap c\_2Emin\_2E\_3D\_3D\_3E V0t) c\_2Ebool\_2E\_EF$

**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.

$$c\_2Enum\_2EREP\_num \in (\omega^{ty\_2Enum\_2Enum}) \quad (5)$$

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

$$c\_2Enum\_2ESUC\_REP \in (\omega^{\omega}) \quad (6)$$

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

$$c\_2Enum\_2EABS\_num \in (ty\_2Enum\_2Enum^{\omega}) \quad (7)$$

**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  $\lambda A. \lambda P \in 2^A. \text{if } (\exists x \in A. P\ x) \text{ then } (the\ (\lambda x. x \in A \wedge P\ x))$  of type  $\iota \Rightarrow \iota$ .

**Definition 10** We define  $c\_2Ebool\_2E\_3F$  to be  $\lambda A\_27a : \iota. (\lambda V0P \in (2^{A\_27a}). (ap\ V0P\ (ap\ (c\_2Emin\_2E\_40$

**Definition 11** We define  $c\_2Eprim\_rec\_2E\_3C$  to be  $\lambda V0m \in ty\_2Enum\_2Enum. \lambda V1n \in ty\_2Enum\_2Enum$

**Definition 12** We define  $c\_2Ebool\_2E\_5C\_2F$  to be  $(\lambda V0t1 \in 2. (\lambda V1t2 \in 2. (ap\ (c\_2Ebool\_2E\_21\ 2)\ (\lambda V2t \in$

Let  $ty\_2Efcf\_2Efinite\_image : \iota \Rightarrow \iota$  be given. Assume the following.

$$\forall A0. nonempty\ A0 \Rightarrow nonempty\ (ty\_2Efcf\_2Efinite\_image\ A0) \quad (8)$$

**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  $c\_2Efcf\_2Efinite\_index$  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.

$$\forall A0. nonempty\ A0 \Rightarrow \forall A1. nonempty\ A1 \Rightarrow nonempty\ (ty\_2Efcf\_2Ecart\ A0\ A1) \quad (9)$$

Let  $c\_2Efcf\_2Edest\_cart : \iota \Rightarrow \iota \Rightarrow \iota$  be given. Assume the following.

$$\forall A\_27a. nonempty\ A\_27a \Rightarrow \forall A\_27b. nonempty\ A\_27b \Rightarrow c\_2Efcf\_2Edest\_cart\ A\_27a\ A\_27b \in ((A\_27a^{(ty\_2Efcf\_2Efinite\_image\ A\_27b)})^{(ty\_2Efcf\_2Ecart\ A\_27a\ A\_27b)}) \quad (10)$$

**Definition 15** 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 16** We define  $c\_2Efcf\_2EFCF$  to be  $\lambda A\_27a : \iota. \lambda A\_27b : \iota. (\lambda V0g \in (A\_27a^{ty\_2Enum\_2Enum}). (ap\ (ap\ (c\_2Emin\_2E\_40$

**Definition 17** We define  $c\_2Ewords\_2Eword\_xor$  to be  $\lambda A\_27a : \iota. \lambda V0v \in (ty\_2Efcf\_2Ecart\ 2\ A\_27a). \lambda V1$

Assume the following.

$$True \quad (11)$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow (\forall V0x \in A\_27a. (\forall V1y \in A\_27a. ((V0x = V1y) \Leftrightarrow (V1y = V0x)))) \quad (12)$$

Assume the following.

$$(\forall V0t \in 2. (((True \Leftrightarrow (p\ V0t)) \Leftrightarrow (p\ V0t)) \wedge (((p\ V0t) \Leftrightarrow True) \Leftrightarrow (p\ V0t)) \wedge (((False \Leftrightarrow (p\ V0t)) \Leftrightarrow \neg(p\ V0t)) \wedge (((p\ V0t) \Leftrightarrow False) \Leftrightarrow \neg(p\ V0t)))))) \quad (13)$$

Assume the following.

$$(\forall V0t1 \in 2. (\forall V1t2 \in 2. (\forall V2t3 \in 2. (((p\ V0t1) \Rightarrow (p\ V1t2) \Rightarrow (p\ V2t3)) \Leftrightarrow (((p\ V0t1) \wedge (p\ V1t2)) \Rightarrow (p\ V2t3)))))) \quad (14)$$

Assume the following.

$$(\forall V0x \in 2. (\forall V1x\_27 \in 2. (\forall V2y \in 2. (\forall V3y\_27 \in 2. (((p\ V0x) \Leftrightarrow (p\ V1x\_27)) \wedge ((p\ V1x\_27) \Rightarrow ((p\ V2y) \Leftrightarrow (p\ V3y\_27)))))) \Rightarrow (((p\ V0x) \Rightarrow (p\ V2y)) \Leftrightarrow ((p\ V1x\_27) \Rightarrow (p\ V3y\_27)))))) \quad (15)$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow \forall A\_27b.nonempty\ A\_27b \Rightarrow (\forall V0x \in (ty\_2EfcP\_2Ecart\ A\_27a\ A\_27b). (\forall V1y \in (ty\_2EfcP\_2Ecart\ A\_27a\ A\_27b). ((V0x = V1y) \Leftrightarrow (\forall V2i \in ty\_2Enum\_2Enum. ((ap\ (ap\ c\_2Eprim\_rec\_2E\_3C\ V2i)\ (ap\ (c\_2EfcP\_2Edimindex\ A\_27b)\ (c\_2Ebool\_2Ethe\_value\ A\_27b)))) \Rightarrow ((ap\ (ap\ (c\_2EfcP\_2EfcP\_index\ A\_27a\ A\_27b)\ V0x)\ V2i) = (ap\ (ap\ (c\_2EfcP\_2EfcP\_index\ A\_27a\ A\_27b)\ V1y)\ V2i)))))) \quad (16)$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow \forall A\_27b.nonempty\ A\_27b \Rightarrow (\forall V0g \in (A\_27a^{ty\_2Enum\_2Enum}). (\forall V1i \in ty\_2Enum\_2Enum. ((p\ (ap\ (ap\ c\_2Eprim\_rec\_2E\_3C\ V1i)\ (ap\ (c\_2EfcP\_2Edimindex\ A\_27b)\ (c\_2Ebool\_2Ethe\_value\ A\_27b)))) \Rightarrow ((ap\ (ap\ (c\_2EfcP\_2EfcP\_index\ A\_27a\ A\_27b)\ (ap\ (c\_2EfcP\_2EFCP\ A\_27a\ A\_27b)\ V0g))\ V1i) = (ap\ V0g\ V1i)))))) \quad (17)$$

Assume the following.

$$(\forall V0t \in 2. ((\neg(\neg(p\ V0t))) \Leftrightarrow (p\ V0t))) \quad (18)$$

Assume the following.

$$(\forall V0A \in 2. ((p\ V0A) \Rightarrow ((\neg(p\ V0A)) \Rightarrow False))) \quad (19)$$

Assume the following.

$$(\forall V0A \in 2.(\forall V1B \in 2.(((\neg((p V0A) \vee (p V1B))) \Rightarrow False) \Leftrightarrow ((p V0A) \Rightarrow False) \Rightarrow ((\neg(p V1B)) \Rightarrow False)))) \quad (20)$$

Assume the following.

$$(\forall V0A \in 2.(\forall V1B \in 2.(((\neg(\neg(p V0A)) \vee (p V1B))) \Rightarrow False) \Leftrightarrow ((p V0A) \Rightarrow ((\neg(p V1B)) \Rightarrow False)))) \quad (21)$$

Assume the following.

$$(\forall V0A \in 2.(((\neg(p V0A)) \Rightarrow False) \Rightarrow (((p V0A) \Rightarrow False) \Rightarrow False))) \quad (22)$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.(\forall V2r \in 2.(((p V0p) \Leftrightarrow (p V1q) \Leftrightarrow (p V2r)) \Leftrightarrow (((p V0p) \vee ((p V1q) \vee (p V2r))) \wedge (((p V0p) \vee (\neg(p V2r)) \vee (\neg(p V1q)))) \wedge (((p V1q) \vee ((\neg(p V2r)) \vee (\neg(p V0p)))) \wedge ((p V2r) \vee ((\neg(p V1q)) \vee (\neg(p V0p)))))))))) \quad (23)$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.(((p V0p) \Leftrightarrow (\neg(p V1q))) \Leftrightarrow (((p V0p) \vee (p V1q)) \wedge ((\neg(p V1q)) \vee (\neg(p V0p)))))) \quad (24)$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.(((\neg((p V0p) \Rightarrow (p V1q))) \Rightarrow (\neg(p V1q)))))) \quad (25)$$

**Theorem 1**

$$\forall A_{.27a}.nonempty A_{.27a} \Rightarrow (\forall V0a \in (ty_{.2Efc}p_{.2Ecart} 2 A_{.27a}).(\forall V1b \in (ty_{.2Efc}p_{.2Ecart} 2 A_{.27a}).(\forall V2c \in (ty_{.2Efc}p_{.2Ecart} 2 A_{.27a}).((ap (ap (c_{.2E}words_{.2E}word_{\_xor} A_{.27a}) (ap (ap (c_{.2E}words_{.2E}word_{\_xor} A_{.27a}) V0a) V1b)) V2c) = (ap (ap (c_{.2E}words_{.2E}word_{\_xor} A_{.27a}) V0a) (ap (ap (c_{.2E}words_{.2E}word_{\_xor} A_{.27a}) V1b) V2c))))))$$