

thm\_2Ebitstring\_2Eword\_slice\_v2w (TMMMr-  
VAEd7jyHfuWaPXFgTWfuckxjDzCnr4)

October 26, 2020

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

$$nonempty\ ty\_2Enum\_2Enum \quad (1)$$

Let  $ty\_2Elist\_2Elist : \iota \Rightarrow \iota$  be given. Assume the following.

$$\forall A0. nonempty\ A0 \Rightarrow nonempty\ (ty\_2Elist\_2Elist\ A0) \quad (2)$$

Let  $c\_2Elist\_2ELENGTH : \iota \Rightarrow \iota$  be given. Assume the following.

$$\forall A\_27a. nonempty\ A\_27a \Rightarrow c\_2Elist\_2ELENGTH\ A\_27a \in (ty\_2Enum\_2Enum^{(ty\_2Elist\_2Elist\ A\_27a)}) \quad (3)$$

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

$$c\_2Earithmetic\_2E\_2B \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \quad (4)$$

**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  $\lambda A\_27a : \iota. (\lambda V0P \in (2^{A\_27a}). (ap\ (ap\ (c\_2Emin\_2E\_3D\ (2^{A\_27a}))\ (\lambda V1P \in 2.V1P)))$

**Definition 4** We define  $c\_2Ebool\_2EF$  to be  $(ap\ (c\_2Ebool\_2E\_21\ 2)\ (\lambda V0t \in 2.V0t))$ .

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

$$c\_2Earithmetic\_2E\_2D \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \quad (5)$$

**Definition 5** We define  $c\_2Ecombin\_2EK$  to be  $\lambda A\_27a : \iota. \lambda A\_27b : \iota. (\lambda V0x \in A\_27a. (\lambda V1y \in A\_27b. V0x))$

Let  $c\_2Elist\_2EGENLIST : \iota \Rightarrow \iota$  be given. Assume the following.

$$\forall A\_27a. nonempty\ A\_27a \Rightarrow c\_2Elist\_2EGENLIST\ A\_27a \in (((ty\_2Elist\_2Elist\ A\_27a)^{ty\_2Enum\_2Enum})^{(A\_27a^{ty\_2Enum\_2Enum})}) \quad (6)$$

Let  $c\_2Elist\_2EAPPEND : \iota \Rightarrow \iota$  be given. Assume the following.

$$\forall A\_27a.\text{nonempty } A\_27a \Rightarrow c\_2Elist\_2EAPPEND A\_27a \in (((ty\_2Elist\_2Elist A\_27a)^{(ty\_2Elist\_2Elist A\_27a)})^{(ty\_2Elist\_2Elist A\_27a)}) \quad (7)$$

**Definition 6** We define  $c\_2Elist\_2EPAD\_RIGHT$  to be  $\lambda A\_27a : \iota. \lambda V0c \in A\_27a. \lambda V1n \in ty\_2Enum\_2Enum$

**Definition 7** We define  $c\_2Ebitstring\_2Eshiftl$  to be  $\lambda V0v \in (ty\_2Elist\_2Elist 2). \lambda V1m \in ty\_2Enum\_2Enum$

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

$$\forall A0.\text{nonempty } A0 \Rightarrow \text{nonempty } (ty\_2Ebool\_2Eitself A0) \quad (8)$$

Let  $c\_2Ebool\_2Ethethe\_value : \iota \Rightarrow \iota$  be given. Assume the following.

$$\forall A\_27a.\text{nonempty } A\_27a \Rightarrow c\_2Ebool\_2Ethethe\_value A\_27a \in (ty\_2Ebool\_2Eitself A\_27a) \quad (9)$$

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

$$\forall A\_27a.\text{nonempty } A\_27a \Rightarrow c\_2Efcp\_2Edimindex A\_27a \in (ty\_2Enum\_2Enum^{(ty\_2Ebool\_2Eitself A\_27a)}) \quad (10)$$

Let  $c\_2Elist\_2EDROP : \iota \Rightarrow \iota$  be given. Assume the following.

$$\forall A\_27a.\text{nonempty } A\_27a \Rightarrow c\_2Elist\_2EDROP A\_27a \in (((ty\_2Elist\_2Elist A\_27a)^{(ty\_2Elist\_2Elist A\_27a)})^{ty\_2Enum\_2Enum}) \quad (11)$$

**Definition 8** We define  $c\_2Elist\_2EPAD\_LEFT$  to be  $\lambda A\_27a : \iota. \lambda V0c \in A\_27a. \lambda V1n \in ty\_2Enum\_2Enum$

**Definition 9** We define  $c\_2Ebitstring\_2Ezero\_extend$  to be  $\lambda V0n \in ty\_2Enum\_2Enum. \lambda V1v \in (ty\_2Elist \_ 2)$

**Definition 10** 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 11** We define  $c\_2Ebool\_2E\_7E$  to be  $(\lambda V0t \in 2. (ap (ap c\_2Emin\_2E\_3D\_3D\_3E V0t) c\_2Ebool\_2E))$

**Definition 12** We define  $c\_2Ebool\_2E\_2F\_5C$  to be  $(\lambda V0t1 \in 2. (\lambda V1t2 \in 2. (ap (c\_2Ebool\_2E\_21 2) (\lambda V2t \in 2. (ap (ap c\_2Emin\_2E\_3D\_3D\_3E V2t) c\_2Ebool\_2E) V1t2) V0t1)))$

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

$$c\_2Enum\_2EREP\_num \in (\omega^{ty\_2Enum\_2Enum}) \quad (12)$$

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

$$c\_2Enum\_2ESUC\_REP \in (\omega^{\omega}) \quad (13)$$

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

$$c\_2Enum\_2EABS\_num \in (ty\_2Enum\_2Enum^{\omega}) \quad (14)$$

**Definition 13** We define  $c\_2Enum\_2ESUC$  to be  $\lambda V0m \in ty\_2Enum\_2Enum.(ap\ c\_2Enum\_2EABS\_num\ m)$

**Definition 14** We define  $c\_2Emin\_2E\_40$  to be  $\lambda A.\lambda P \in 2^A.\text{if } (\exists x \in A.p (ap\ P\ x)) \text{ then } (\lambda x.x \in A \wedge P(x)) \text{ else } \perp$

**Definition 15** We define  $c\_2Ebool\_2E\_3F$  to be  $\lambda A\_27a : \iota.(\lambda V0P \in (2^{A\_27a}).(ap\ V0P\ (ap\ (c\_2Emin\_2E\_40\ A\_27a)\ P)))$

**Definition 16** We define  $c\_2Eprim\_rec\_2E\_3C$  to be  $\lambda V0m \in ty\_2Enum\_2Enum.\lambda V1n \in ty\_2Enum\_2Enum.(ap\ (c\_2Eprim\_rec\_2E\_3C\ m)\ n)$

**Definition 17** We define  $c\_2Ebool\_2ECOND$  to be  $\lambda A\_27a : \iota.(\lambda V0t \in 2.(\lambda V1t1 \in A\_27a.(\lambda V2t2 \in A\_27a.(ap\ (c\_2Ebool\_2ECOND\ A\_27a)\ t1\ t2))))$

**Definition 18** We define  $c\_2Ebool\_2ELET$  to be  $\lambda A\_27a : \iota.\lambda A\_27b : \iota.(\lambda V0f \in (A\_27b^{A\_27a}).(\lambda V1x \in A\_27b.(ap\ (c\_2Ebool\_2ELET\ A\_27a)\ f\ x)))$

**Definition 19** We define  $c\_2Ebitstring\_2Efixwidth$  to be  $\lambda V0n \in ty\_2Enum\_2Enum.\lambda V1v \in (ty\_2Elist\_2Elist\ A\_27a).(\lambda V2w \in ty\_2Enum\_2Enum.(ap\ (c\_2Ebitstring\_2Efixwidth\ A\_27a)\ v\ w)))$

Let  $c\_2Elist\_2ETAKE : \iota \Rightarrow \iota$  be given. Assume the following.

$$\forall A\_27a.\text{nonempty } A\_27a \Rightarrow c\_2Elist\_2ETAKE\ A\_27a \in (((ty\_2Elist\_2Elist\ A\_27a)^{(ty\_2Elist\_2Elist\ A\_27a)})^{ty\_2Enum\_2Enum}) \quad (15)$$

**Definition 20** We define  $c\_2Ebitstring\_2Eshiftr$  to be  $\lambda V0v \in (ty\_2Elist\_2Elist\ 2).\lambda V1m \in ty\_2Enum\_2Enum.(ap\ (c\_2Ebitstring\_2Eshiftr\ 2)\ v\ m))$

**Definition 21** We define  $c\_2Ebitstring\_2Efield$  to be  $\lambda V0h \in ty\_2Enum\_2Enum.\lambda V1l \in ty\_2Enum\_2Enum.(ap\ (c\_2Ebitstring\_2Efield\ h)\ l))$

Let  $c\_2Elist\_2ENIL : \iota \Rightarrow \iota$  be given. Assume the following.

$$\forall A\_27a.\text{nonempty } A\_27a \Rightarrow c\_2Elist\_2ENIL\ A\_27a \in (ty\_2Elist\_2Elist\ A\_27a) \quad (16)$$

Let  $c\_2Elist\_2ECONS : \iota \Rightarrow \iota$  be given. Assume the following.

$$\forall A\_27a.\text{nonempty } A\_27a \Rightarrow c\_2Elist\_2ECONS\ A\_27a \in (((ty\_2Elist\_2Elist\ A\_27a)^{(ty\_2Elist\_2Elist\ A\_27a)})^{A\_27a}) \quad (17)$$

**Definition 22** We define  $c\_2Ebitstring\_2Etestbit$  to be  $\lambda V0b \in ty\_2Enum\_2Enum.\lambda V1v \in (ty\_2Elist\_2Elist\ 2).(\lambda V2w \in ty\_2Enum\_2Enum.(ap\ (c\_2Ebitstring\_2Etestbit\ 2)\ b\ v\ w)))$

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

$$\forall A0.\text{nonempty } A0 \Rightarrow nonempty\ (ty\_2Efcp\_2Efinite\_image\ A0) \quad (18)$$

**Definition 23** We define  $c\_2Ebool\_2E\_3F\_21$  to be  $\lambda A\_27a : \iota.(\lambda V0P \in (2^{A\_27a}).(ap\ (ap\ (c\_2Ebool\_2E\_3F\_21\ A\_27a)\ P)))$

**Definition 24** We define  $c\_2Efcp\_2Efinite\_index$  to be  $\lambda A\_27a : \iota.(ap\ (c\_2Emin\_2E\_40\ (A\_27a^{ty\_2Enum\_2Enum}))$

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

$$\forall A0.\text{nonempty } A0 \Rightarrow \forall A1.\text{nonempty } A1 \Rightarrow nonempty\ (ty\_2Efcp\_2Ecart\ A0\ A1) \quad (19)$$

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

$$\forall A\_27a.\text{nonempty } A\_27a \Rightarrow \forall A\_27b.\text{nonempty } A\_27b \Rightarrow c\_2Efcp\_2Edest\_cart\ A\_27a\ A\_27b \in ((A\_27a^{(ty\_2Efcp\_2Efinite\_image\ A\_27b)})^{(ty\_2Efcp\_2Ecart\ A\_27a\ A\_27b)}) \quad (20)$$

**Definition 25** We define  $c\_2Efcp\_2Efcp\_index$  to be  $\lambda A\_27a : \iota. \lambda A\_27b : \iota. \lambda V0x \in (ty\_2Efcp\_2Ecart\ A\_27a)$

**Definition 26** We define  $c\_2Efcp\_2EFCP$  to be  $\lambda A\_27a : \iota. \lambda A\_27b : \iota. (\lambda V0g \in (A\_27a^{ty\_2Enum\_2Enum}).(ap\ (c\_2Efcp\_2EFCP\ A\_27a)\ V0g))$

**Definition 27** We define  $c\_2Ebitstring\_2Ev2w$  to be  $\lambda A\_27a : \iota. \lambda V0v \in (ty\_2Elist\_2Elist\ 2).(ap\ (c\_2Efcp\_2Ebitstring\_2Ev2w\ A\_27a)\ V0v))$

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

$$c\_2Enum\_2EZERO\_REP \in \omega \quad (21)$$

**Definition 28** We define  $c\_2Enum\_2E0$  to be  $(ap\ (c\_2Enum\_2EABS\_num\ c\_2Enum\_2EZERO\_REP))$

**Definition 29** We define  $c\_2Earithmetic\_2EZERO$  to be  $c\_2Enum\_2E0$ .

**Definition 30** We define  $c\_2Earithmetic\_2EBIT1$  to be  $\lambda V0n \in ty\_2Enum\_2Enum.(ap\ (ap\ (c\_2Earithmetic\_2EBIT1\ A\_27a)\ V0n))$

**Definition 31** We define  $c\_2Earithmetic\_2ENUMERAL$  to be  $\lambda V0x \in ty\_2Enum\_2Enum.V0x$ .

**Definition 32** We define  $c\_2Earithmetic\_2EMIN$  to be  $\lambda V0m \in ty\_2Enum\_2Enum.\lambda V1n \in ty\_2Enum\_2Enum.(\lambda V2t \in$

**Definition 33** 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 34** We define  $c\_2Earithmetic\_2E_3C_3D$  to be  $\lambda V0m \in ty\_2Enum\_2Enum.\lambda V1n \in ty\_2Enum\_2Enum.$

**Definition 35** We define  $c\_2Ewords\_2Eword\_bits$  to be  $\lambda A\_27a : \iota. \lambda V0h \in ty\_2Enum\_2Enum.\lambda V1l \in ty\_2Enum\_2Enum.$

**Definition 36** We define  $c\_2Ewords\_2Eword\_lsl$  to be  $\lambda A\_27a : \iota. \lambda V0w \in (ty\_2Efcp\_2Ecart\ 2\ A\_27a).\lambda V1v \in$

**Definition 37** We define  $c\_2Ewords\_2Eword\_slice$  to be  $\lambda A\_27a : \iota. \lambda V0h \in ty\_2Enum\_2Enum.\lambda V1l \in ty\_2Enum\_2Enum.$

Assume the following.

$$\begin{aligned} & \forall A\_27a. nonempty\ A\_27a \Rightarrow (\forall V0n \in ty\_2Enum\_2Enum. ( \\ & \quad \forall V1v \in (ty\_2Elist\_2Elist\ 2).((ap\ (ap\ (c\_2Ewords\_2Eword\_lsl \\ & \quad A\_27a)\ (ap\ (c\_2Ebitstring\_2Ev2w\ A\_27a)\ V1v))\ V0n) = (ap\ (c\_2Ebitstring\_2Ev2w \\ & \quad A\_27a)\ (ap\ (ap\ c\_2Ebitstring\_2Eshiftl\ V1v)\ V0n)))))) \end{aligned} \quad (22)$$

Assume the following.

$$\begin{aligned} & \forall A\_27a. nonempty\ A\_27a \Rightarrow (\forall V0h \in ty\_2Enum\_2Enum. ( \\ & \quad \forall V1l \in ty\_2Enum\_2Enum. (\forall V2v \in (ty\_2Elist\_2Elist\ 2).((ap\ (ap\ (c\_2Ewords\_2Eword\_bits\ A\_27a)\ V0h)\ V1l) \\ & \quad (ap\ (c\_2Ebitstring\_2Ev2w\ A\_27a)\ V2v)) = (ap\ (c\_2Ebitstring\_2Ev2w\ A\_27a) \\ & \quad (ap\ (ap\ (ap\ c\_2Ebitstring\_2Efield\ V0h)\ V1l)\ (ap\ (ap\ c\_2Ebitstring\_2Efixwidth \\ & \quad (ap\ (c\_2Efcp\_2Edimindex\ A\_27a)\ (c\_2Ebool\_2Ethe\_value\ A\_27a))) \\ & \quad V2v))))))) \end{aligned} \quad (23)$$

Assume the following.

$$True \quad (24)$$

Assume the following.

$$\forall A\_27a.\text{nonempty } A\_27a \Rightarrow (\forall V0x \in A\_27a. ((V0x = V0x) \Leftrightarrow \text{True})) \quad (25)$$

Assume the following.

$$\begin{aligned} \forall A\_27a.\text{nonempty } A\_27a \Rightarrow & (\forall V0h \in \text{ty\_2Enum\_2Enum}. ( \\ & \forall V1l \in \text{ty\_2Enum\_2Enum}. (\forall V2w \in (\text{ty\_2Efcp\_2Ecart } 2 \\ & A\_27a). ((\text{ap } (\text{ap } (\text{ap } (\text{c\_2Ewords\_2Eword\_slice } A\_27a) V0h) V1l) \\ & V2w) = (\text{ap } (\text{ap } (\text{c\_2Ewords\_2Eword\_lsr } A\_27a) (\text{ap } (\text{ap } (\text{ap } (\text{c\_2Ewords\_2Eword\_bits } \\ & A\_27a) V0h) V1l) V2w)) V1l)))))) \end{aligned} \quad (26)$$

### Theorem 1

$$\begin{aligned} \forall A\_27a.\text{nonempty } A\_27a \Rightarrow & (\forall V0h \in \text{ty\_2Enum\_2Enum}. ( \\ & \forall V1l \in \text{ty\_2Enum\_2Enum}. (\forall V2v \in (\text{ty\_2Elist\_2Elist } \\ & 2). ((\text{ap } (\text{ap } (\text{ap } (\text{c\_2Ewords\_2Eword\_slice } A\_27a) V0h) V1l) (\text{ap } \\ & (\text{c\_2Ebitstring\_2Ev2w } A\_27a) V2v)) = (\text{ap } (\text{c\_2Ebitstring\_2Ev2w } \\ & A\_27a) (\text{ap } (\text{ap } \text{c\_2Ebitstring\_2Eshiftl } (\text{ap } (\text{ap } (\text{ap } \text{c\_2Ebitstring\_2Efield } \\ & V0h) V1l) (\text{ap } (\text{ap } \text{c\_2Ebitstring\_2Efixwidth } (\text{ap } (\text{c\_2Efcp\_2Edimindex } \\ & A\_27a) (\text{c\_2Ebool\_2Ethe\_value } A\_27a))) V2v))) V1l)))))) \end{aligned}$$