Additional proofs for the UEFI Image Loader project

Marvin Häuser
Technische Universität Kaiserslautern;
Ivannikov Institute for System Programming
of the Russian Academy of Sciences
Kaiserslautern, Germany
mhaeuser@posteo.de

Vitaly Cheptsov
Ivannikov Institute for System Programming
of the Russian Academy of Sciences
Moscow, Russia
cheptsov@ispras.ru

Disclaimer: The theorems below were proven on paper due to time constraints for the initial revision of the script. They can and should be interactively proven in Coq plugin for Frama-C in further revisions. See more details for using Coq in "Introduction to C program proof with Frama-C and its WP plugin".

Definition. B-bit alignment safety predicate.

$$asafe_B(v, a) \stackrel{\text{def}}{=} 0 \leq v, a < 2^B \land (\exists i \in \mathbb{N}_0 : 2^i = a) \land v + (a-1) < 2^B$$

Theorem 1. *When the B-bit alignment safety predicate does not hold for value v and alignment $a = 2^i$, v aligned by a does not fit B bits.*

$$a < 2^B \leq v + (a-1) \Rightarrow 2^B \leq (v + (a-1)) - ((v + (a-1)) \bmod a)$$

Proof.

$$\begin{aligned}
& 2^i < 2^B \leq v + (2^i - 1) \\
\Leftrightarrow\quad & 2^i < 2^B \leq v + (2^i - 1) \land ((v + (2^i - 1)) - 2^B) \bmod 2^i \leq (v + (2^i - 1)) - 2^B \\
\Leftrightarrow\quad & 2^i < 2^B \leq v + (2^i - 1) \land ((v + (2^i - 1)) - 2^B) \bmod 2^i \bmod 2^i \leq (v + (2^i - 1)) - 2^B \\
\Leftrightarrow\quad & 2^i < 2^B \leq v + (2^i - 1) \land (((v + (2^i - 1)) - 2^B) \bmod 2^i + 2^B \bmod 2^i) \bmod 2^i \leq (v + (2^i - 1)) - 2^B \\
\Leftrightarrow\quad & 2^i < 2^B \leq v + (2^i - 1) \land ((v + (2^i - 1)) - 2^B + 2^B) \bmod 2^i \leq (v + (2^i - 1)) - 2^B \\
\Leftrightarrow\quad & 2^i < 2^B \leq v + (2^i - 1) \land (v + (2^i - 1)) \bmod 2^i \leq (v + (2^i - 1)) - 2^B \\
\Leftrightarrow\quad & 2^i < 2^B \leq v + (2^i - 1) \land 2^B \leq (v + (2^i - 1)) - (v + (2^i - 1)) \bmod 2^i \\
\Leftrightarrow\quad & a < 2^B \leq v + (a - 1) \land 2^B \leq (v + (a - 1)) - (v + (a - 1)) \bmod a
\end{aligned}$$

□

Proposition 1. Every two's potency is the successor of the sum of all lesser two's potencies.

Proof. We proceed using induction.

Base case: $2^0 = 1 = \sum_{j=0}^{0-1} 2^j + 1$

Induction step: $2^i = 2 \cdot 2^{i-1} = 2 \cdot (\sum_{j=0}^{i-2} 2^j + 1) = \sum_{j=1}^{i-1} 2^j + 2 = \sum_{j=0}^{i-1} 2^j + 1$

□

Definition. Binary bit test.

$$bt(v, i) \stackrel{\text{def}}{=} ((v \div 2^i) \bmod 2 = 1)$$

Definition. Binary set representation.

$$b2s(a) \stackrel{\text{def}}{=} \{i \in \mathbb{N}_0 \mid bt(a, i)\}$$
$$s2b(A) \stackrel{\text{def}}{=} \sum_{i \in A} 2^i$$

Proposition 2. The binary set representation is a correct decomposition.

Proof. The correctness follows directly from the definition of base 2. □

Definition. Binary division set.

$$bdiv(a, i) \stackrel{\text{def}}{=} b2s(a) \cap \{j \in \mathbb{N}_0 \mid i \leq j\}$$

Definition. Binary remainder set.

$$brem(a,i) \stackrel{\text{def}}{=} b2s(a) \cap \{j \in \mathbb{N}_0 \mid j < i\}$$

Lemma 1. *For an arbitrary value a and a two's potency $b = 2^i$, the binary division $div(a,i)$ and remainder $brem(a,i)$ sets are the two's potency decomposition of $a - a \bmod b$ and $a \bmod b$.*

Proof. We show that the division and remainder sets are disjunct and their union is the decomposition of a.

$$\begin{aligned} bdiv(a,i) \cap brem(a,i) &= (b2s(a) \cap \{j \in \mathbb{N}_0 \mid i \le j\}) \cap (b2s(a) \cap \{j \in \mathbb{N}_0 \mid j < i\}) = b2s(a) \cap \emptyset = \emptyset \\ bdiv(a,i) \cup brem(a,i) &= (b2s(a) \cap \{j \in \mathbb{N}_0 \mid i \le j\}) \cup (b2s(a) \cap \{j \in \mathbb{N}_0 \mid j < i\}) = b2s(a) \cap \mathbb{N}_0 = b2s(a) \\ s2b(bdiv(a,i)) + s2b(brem(a,i)) &= \sum_{j \in bdiv(a,i)} 2^j + \sum_{j \in brem(a,i)} 2^j = s2b(a) \end{aligned}$$

We derive from **Proposition 1** that there is no sum of two's potencies involving a two's potency less than 2^i that is 0 mod 2^i. Hence, $bdiv(a,i)$ corresponds to the division set if and only if the following holds:

$$\forall j \in b2s(a) : j \in bdiv(a,i) \Leftrightarrow 2^j \bmod 2^i = 0$$

We first show that $\forall j \in b2s(a) : j \in bdiv(a,i) \Rightarrow 2^j \bmod 2^i = 0$ holds.

$$\begin{gathered} \forall j \in \{j \in \mathbb{N}_0 \mid i \le j\} : 2^i \le 2^j \Leftrightarrow \forall j \in \{j \in \mathbb{N}_0 \mid i \le j\} : 2^j \bmod 2^i = 0 \\ bdiv(a,i) \subseteq \{j \in \mathbb{N}_0 \mid i \le j\} \Rightarrow \forall j \in b2s(a) : j \in bdiv(a,i) \Rightarrow 2^j \bmod 2^i = 0 \end{gathered}$$

Now we show that $\forall j \in b2s(a) : 2^j \bmod 2^i = 0 \Rightarrow j \in bdiv(a,i)$ holds.

$$\begin{gathered} \forall j \in \{j \in \mathbb{N}_0 \mid j < i\} : 2^j < 2^i \Leftrightarrow \forall j \in \{j \in \mathbb{N}_0 \mid j < i\} : 2^j \bmod 2^i \neq 0 \\ b2s(a) \setminus bdiv(a,i) \subseteq \{j \in \mathbb{N}_0 \mid j < i\} \Rightarrow \forall j \in b2s(a) : j \in b2s(a) \setminus bdiv(a,i) \Rightarrow 2^j \bmod 2^i \neq 0 \end{gathered}$$

It follows that the division set is the decomposition of $a - a \bmod b$. Because the division and the remainder sets are disjunct and their union is the decomposition of a, it follows that the remainder set is the decomposition of $a \bmod b$. □

Definition. Binary AND operation.

$$a \,\&\, b \stackrel{\text{def}}{=} s2b(b2s(a) \cap b2s(b))$$

Definition. Binary NOT operation.

$$\sim a \stackrel{\text{def}}{=} s2b(\{i \in \mathbb{N}_0 \mid \neg bt(a,i)\})$$

Lemma 2. *The set of bit indices of a two's potency a minus 1 is the set of all natural numbers less than i.*

Proof.

$$a - 1 = 2^i - 1 = \sum_{j=0}^{i-1} 2^j = s2b(\{j \in \mathbb{N}_0 \mid j < i\})$$

□

Theorem 2. *For an arbitrary value a and a two's potency $b = 2^i$, the following holds:*

$$\begin{gathered} a - a \bmod b = a \,\&\, \sim (b-1) \\ a \bmod b = a \,\&\, (b-1) \end{gathered}$$

Proof.

$$\begin{aligned} a \bmod b &= a \bmod 2^i = s2b(brem(a,i)) = s2b(b2s(v) \cap \{j \in \mathbb{N}_0 \mid j < i\}) = s2b(b2s(v) \cap b2s(b-1)) = a \,\&\, (b-1) \\ a - a \bmod b &= s2b(b2s(a) \setminus b2s(a \bmod b)) = s2b(b2s(a) \setminus (b2s(v) \cap b2s(b-1))) = s2b(b2s(v) \cap \sim b2s(b-1)) \\ &= a \,\&\, \sim (b-1) \end{aligned}$$

□

Lemma 3. *For all positive values, if its binary set representation and that of its predecessor are disjunct, it is a two's potency.*

$$0 < v \land b2s(v) \cap b2s(v-1) = \emptyset \Rightarrow \exists x \in \mathbb{N}_0 : v = 2^x$$

Proof. We proceed with a proof by contradiction. Assume we have a value v that is not the predecessor of a two's potency. Then $b2s(v)$ is non-consecutive as per **Proposition 1**. We can further decompose $v = u + w$ such that u is the predecessor of the lowest two's potency that is not part of the decomposition of v and $w = v - u$. Please note that w cannot be 0 as otherwise v would be the predecessor of a two's potency. $u + 1$ then yields a two's potency that is not part of the decomposition of v and in consequence is not part of the decomposition of w. Hence, it holds that $v + 1 = u + w + 1 = s2b(b2s(u + 1) \cup b2s(w))$. It is obvious that $b2s(v)$ and $b2s(v + 1)$ are not disjunct. □

Definition. Two's potency classification predicate.

$$is\_pow2(v) \stackrel{\text{def}}{=} 0 < v \land v \;\&\; (v-1) = 0$$

Theorem 3. *The two's potency classification predicate holds if and only if its operand is a two's potency.*

$$is\_pow2(v) \Leftrightarrow \exists x \in \mathbb{N}_0 : v = 2^x$$

Proof.

$$\begin{aligned}
& 0 < v \land b2s(v) \cap b2s(v-1) = \emptyset \Rightarrow \exists x \in \mathbb{N}_0 : v = 2^x \\
\Leftrightarrow\quad & 0 < v \land s2b(b2s(v) \cap b2s(v-1)) = 0 \Rightarrow \exists x \in \mathbb{N}_0 : v = 2^x \\
\Leftrightarrow\quad & 0 < v \land v \;\&\; (v-1) = 0 \Rightarrow \exists x \in \mathbb{N}_0 : v = 2^x \\
\Leftrightarrow\quad & is_pow2(v) \Rightarrow \exists x \in \mathbb{N}_0 : v = 2^x
\end{aligned}$$

$$\begin{aligned}
& \exists x \in \mathbb{N}_0 : v = 2^x \Rightarrow 0 < v \\
\Leftrightarrow\quad & \exists x \in \mathbb{N}_0 : v = 2^x \Rightarrow 0 < v \land v \bmod v = 0 \\
\Leftrightarrow\quad & \exists x \in \mathbb{N}_0 : v = 2^x \Rightarrow 0 < v \land v \;\&\; (v-1) = 0 \\
\Leftrightarrow\quad & \exists x \in \mathbb{N}_0 : v = 2^x \Rightarrow is_pow2(v)
\end{aligned}$$

□