On Overflow of Unsigned Integer Multiplication

Yue LI

May 7, 2023

The x86 unsigned multiplication instruction MUL multiplies RAX with some quadword and stores the result in RDX:RAX. The overflow flag OF and carry flag CF are set if the high-order bits of the result, which are stored in RDX, are non-zero. The notion of overflow applicable to the MUL instruction is therefore that multiplication of two n-bit (unsigned) integers has a result that is longer than n bits. Taking into account that MUL actually uses $2n$ bits to store the result of multiplication of two n-bit numbers, in this blog we ask and answer a different overflow question: *is it possible that multiplying two n-bit unsigned integers and the result is longer than 2n bits?*

We shall answer negatively, and prove the following Proposition.

Proposition. *For all* $n = 1, 2, 3, \ldots$*, the result of multiplication of two unsigned* n*-bit integers has at most* $2n$ *bits.*

Since an all-ones, like 11111111111, is the largest n-bit unsigned integer for every n, if we can show that two n-bit all-ones multiply and the result is no more than $2n$ bits, then the Proposition easily follows.

Lemma. *For all* $n = 1, 2, 3, \ldots$*, the square of the largest* n*-bit unsigned integer has at most* $2n$ *bits.*

Our proof for the Lemma is inductive, but before examining the formal arguments, let's warm up by looking at some particular cases.

1 Pattern Discovery for Induction

Below we show that the Lemma holds for $1 \leq n \leq 6$. We shall use sum of powers of 2 to denote an unsigned binary integer, then e.g. 1111 is $2^3 + 2^2 + 2^1 + 2^0$. Equation 1 shows that 1^2 has 1 bit.

$$(2^0)^2 = 2^0 \tag{1}$$

Next, when building Equation 2 we use Equation 1 (as underlined).

$$
\begin{aligned}
& (2^1+2^0)^2 \\
= \quad & (2^1)^2 + 2\cdot 2^1 \cdot 2^0 + \underline{(2^0)^2} \\
= \quad & (2^2+2^2) + \underline{2^0} \text{ by } (1) \\
= \quad & 2^3 + 2^0
\end{aligned} \tag{2}
$$

Equation 2 shows that 11^2 has 4 bits. Next, when building Equation 3 we use Equation 2.

$$
\begin{aligned}
& (2^2+2^1+2^0)^2 \\
= \quad & (2^2)^2 + 2\cdot 2^2(2^1+2^0) + \underline{(2^1+2^0)^2} \\
= \quad & 2^4 + 2^3(2^1+2^0) + \underline{2^3+2^0} \text{ by } (2) \\
= \quad & (2^4+2^4) + (2^3+2^3) + 2^0 \\
= \quad & 2^5 + 2^4 + 2^0
\end{aligned} \tag{3}
$$

Equation 3 shows that 111^2 has 6 bits. Next, when building Equation 4 we use Equation 3.

$$
\begin{aligned}
& (2^3+2^2+2^1+2^0)^2 \\
= \quad & (2^3)^2 + 2\cdot 2^3(2^2+2^1+2^0) + \underline{(2^2+2^1+2^0)^2} \\
= \quad & 2^6 + 2^4(2^2+2^1+2^0) + \underline{2^5+2^4+2^0} \text{ by } (3) \\
= \quad & (2^6+2^6) + (2^5+2^4) + (2^5+2^4) + 2^0 \\
= \quad & 2^7 + 2^6 + 2^5 + 2^0
\end{aligned} \tag{4}
$$

Equation 4 shows that 1111^2 has 8 bits. Next, when building Equation 5 we use Equation 4.

$$
\begin{aligned}
& (2^4+2^3+2^2+2^1+2^0)^2 \\
= \quad & (2^4)^2 + 2\cdot 2^4(2^3+2^2+2^1+2^0) + \underline{(2^3+2^2+2^1+2^0)^2} \\
= \quad & 2^8 + 2^5(2^3+2^2+2^1+2^0) + \underline{2^7+2^6+2^5+2^0} \text{ by } (4) \\
= \quad & (2^8+2^8) + (2^7+2^6+2^5) + (2^7+2^6+2^5) + 2^0 \\
= \quad & 2^9 + 2^8 + 2^7 + 2^6 + 2^0
\end{aligned} \tag{5}
$$

Equation 5 shows that 11111^2 has 10 bits. Next, when building Equation 6 we use Equation 5.

$$
\begin{aligned}
& (2^5+2^4+2^3+2^2+2^1+2^0)^2 \\
= \quad & (2^5)^2 + 2\cdot 2^5(2^4+2^3+2^2+2^1+2^0) + \underline{(2^4+2^3+2^2+2^1+2^0)^2} \\
= \quad & 2^{10} + 2^6(2^4+2^3+2^2+2^1+2^0) + \underline{2^9+2^8+2^7+2^6+2^0} \text{ by (5)} \\
= \quad & (2^{10}+2^{10}) + (2^9+2^8+2^7+2^6) + (2^9+2^8+2^7+2^6) + 2^0 \\
= \quad & 2^{11}+2^{10}+2^9+2^8+2^7+2^0 \qquad (6)
\end{aligned}
$$

Equation 6 shows that 111111^2 has 12 bits.

2 Formal Inductive Proof

Based on Equations 1–6, it is reasonable to conjecture that for all $n = 0, 1, 2, 3, \ldots$,

$$
(2^n + 2^{n-1} + \cdots + 2^0)^2 = 2^{2n+1} + 2^{2n} + \cdots + 2^{n+2} + 2^0. \qquad (7)
$$

Note that on both sides of Equation 7 the powers of 2 are in descending order, so that the right hand side is instantiated by 2^0 when $n = 0$, by $2^3 + 2^0$ when $n = 1$ and by $2^5 + 2^4 + 2^0$ when $n = 2$, and so on.

Based on how we progress from Equation 1 to 6, we have the following scheme of progression from the square of sum up to n-th power of 2, to the square of sum up to $(n+1)$-th power of 2.

$$
\begin{aligned}
& (2^{n+1} + 2^n + \cdots + 2^0)^2 \\
= \quad & (2^{n+1})^2 + 2\cdot 2^{n+1}(2^n + 2^{n-1} + \cdots + 2^0) + \underline{(2^n + 2^{n-1} + \cdots + 2^0)^2} \\
= \quad & 2^{2(n+1)} + 2^{n+2}(2^n + 2^{n-1} + \cdots + 2^0) + \underline{2^{2n+1} + 2^{2n} \cdots + 2^{n+2} + 2^0} \text{ by (7)} \\
= \quad & \left(2^{2(n+1)} + 2^{2(n+1)}\right) + (2^{2n+1} + \cdots + 2^{n+2}) + (2^{2n+1} + \cdots + 2^{n+2}) + 2^0 \\
= \quad & 2^{2(n+1)+1} + 2^{2(n+1)} + \cdots + 2^{(n+1)+2} + 2^0 \qquad (8)
\end{aligned}
$$

Based on the facts that Equation 1 holds, and that for all $n = 0, 1, 2, 3, \ldots$, if Equation 7 holds then Equation 8 holds, we can justly conclude that our conjecture that for all $n = 0, 1, 2, 3, \ldots$ Equation 7 holds, is true. This proves our Lemma. Then the Proposition follows.