Chapter 7
IEEE-Compliant Square Root

Many of the preceding results are propositions pertaining to real variables, which are formalized by ACL2 events in which these variables are restricted to the rational domain. Many of the lemmas of this chapter similarly apply to arbitrary real numbers, but in light of our present focus, these results are formulated to correspond more closely with their formal versions. Apart from the informal discussion immediately below, the lemmas themselves contain no references to the real numbers or the square root function.

Establishing IEEE compliance of a floating-point square root module entails proving that the final value r computed for a given radicand x, rounding mode $\mathcal{R}$, and precision n satisfies

$$r = \mathcal{R}(\sqrt{x}, n). \tag{7.1}$$

We would like to formulate a proposition of rational arithmetic that is transparently equivalent to (7.1). This requirement is satisfied by the following criterion:

For all positive rational numbers ℓ *and* h, *if* $\ell^2 \leq x \leq h^2$, *then*

$$\mathcal{R}(\ell, n) \leq r \leq \mathcal{R}(h, n). \tag{7.2}$$

Obviously, the monotonicity of rounding (Lemma 6.95) and of the square root ensure that (7.1) implies (7.2). On the other hand, suppose that (7.2) holds. According to Lemma 6.100, either $\sqrt{x}$ is $(n+1)$-exact (and, in particular, rational) or for some $\epsilon > 0$, $\mathcal{R}(y, n) = \mathcal{R}(\sqrt{x}, n)$ for all y satisfying $|y - \sqrt{x}| < \epsilon$. In either case, there exist $\ell \in \mathbb{Q}$ and $h \in \mathbb{Q}$ such that $\ell \leq \sqrt{x} \leq h$ and $\mathcal{R}(\ell, n) = \mathcal{R}(\sqrt{x}, n) = \mathcal{R}(h, n)$. Since $\ell^2 \leq x \leq h^2$,

$$\mathcal{R}(\sqrt{x}, n) = \mathcal{R}(\ell, n) \leq r \leq \mathcal{R}(h, n) = \mathcal{R}(\sqrt{x}, n)$$

and hence $r = \mathcal{R}(\sqrt{x}, n)$.

D. M. Russinoff, *Formal Verification of Floating-Point Hardware Design*,
https://doi.org/10.1007/978-3-319-95513-1_7

Thus, we would like to prove formally that (7.2) is satisfied by the value r computed by a square root module of interest. For this purpose, it will be useful to have a function that computes, for given x and n, a rational number q that satisfies

$$\mathcal{R}(q, n) = \mathcal{R}(\sqrt{x}, n). \tag{7.3}$$

We shall define a conceptually simple (albeit computationally horrendous) rational function $\sqrt[(k)]{x}$ that serves this need. The definition is motivated by Lemma 6.101, which guarantees that if we are able to arrange that

$$\sqrt[(k)]{x} = RTO(\sqrt{x}, k), \tag{7.4}$$

where $k \geq n + 2$, then (7.3) holds for $q = \sqrt[(k)]{x}$. Of course, (7.4) will not be our formal definition of $\sqrt[(k)]{x}$, nor shall we prove any instance of (7.3). However, after formulating the definition, we shall prove the following (Lemma 7.17):

For all positive rationals ℓ and h and positive integers k and n, if $\ell^2 \leq x \leq h^2$ and $k \geq n + 2$, then

$$\mathcal{R}(\ell, n) \leq \mathcal{R}(\sqrt[(k)]{x}, n) \leq \mathcal{R}(h, n). \tag{7.5}$$

Thus, in order to prove that a computed value r satisfies (7.2), it will suffice to show that $r = \mathcal{R}(\sqrt[(k)]{x}, n)$ for some $k \geq n + 2$. This is the strategy followed in the correctness proof of Chap. 19.

7.1 Truncated Square Root

The first step toward the definition of $\sqrt[(n)]{x}$ is the following recursive function, the name of which is motivated by the unproven observation that for $\frac{1}{4} \leq x < 1$,

$$rtz\text{-}sqrt(x, n) = RTZ(\sqrt{x}, n).$$

Definition 7.1 Let $x \in \mathbb{R}$ and $n \in \mathbb{N}$. If $n = 0$, then $rtz\text{-}sqrt(x, n) = 0$ and if $n > 0$ and $z = rtz\text{-}sqrt(x, n - 1)$, then

$$rtz\text{-}sqrt(x, n) = \begin{cases} z & \text{if } (z + 2^{-n})^2 > x \\ z + 2^{-n} & \text{if } (z + 2^{-n})^2 \leq x. \end{cases}$$

Lemma 7.1 *Let $x \in \mathbb{Q}$ and $n \in \mathbb{N}$. If $x \geq \frac{1}{4}$, then*

$$\frac{1}{2} \leq rtz\text{-}sqrt(x, n) \leq 1 - 2^{-n}.$$

Proof If $n = 1$, then $rtz\text{-}sqrt(x, n) = \frac{1}{2}$ and the claim is trivial. Proceeding by induction, let $n > 1$, $z = rtz\text{-}sqrt(x, n-1)$, and $w = rtz(x, n)$, and assume that $\frac{1}{2} \le z \le 1 - 2^{1-n}$. If $w = z$, the claim follows trivially; otherwise, $w = z + 2^{-n}$ and

$$\frac{1}{2} \le z < w = z + 2^{-n} \le (1 - 2^{1-n}) + 2^{-n} = 1 - 2^{-n}.$$

□

Corollary 7.2 *Let $x \in \mathbb{Q}$ $n \in \mathbb{Z}^+$. If $x \ge \frac{1}{4}$, then $expo(rtz\text{-}sqrt(x, n)) = -1$.*

Lemma 7.3 *Let $x \in \mathbb{Q}$ and $n \in \mathbb{Z}^+$. If $x \ge \frac{1}{4}$, then $rtz\text{-}sqrt(x, n)$ is n-exact.*

Proof The claim is trivial for $n = 0$. Let $n > 1$, $z = rtz\text{-}sqrt(x, n-1)$, and $w = rtz(x, n)$, and assume that z is $(n-1)$-exact, i.e., $2^{n-1}z \in \mathbb{Z}$. Then either $w = z$ and $2^n w = 2(2^{n-1}z) \in \mathbb{Z}$ or

$$2^n w = 2^n(z + 2^{-n}) = 2(2^{n-1}z) + 1 \in \mathbb{Z}.$$

□

Lemma 7.4 *Let $x \in \mathbb{Q}$ and $n \in \mathbb{N}$. Assume that $\frac{1}{4} \le x < 1$ and let $w = rtz\text{-}sqrt(x, n)$. Then $w^2 \le x < (w + 2^{-n})^2$.*

Proof The claim is trivial for $n = 0$. Let $n > 0$, $z = rtz\text{-}sqrt(x, n-1)$, and assume that $z^2 \le x < (z + 2^{1-n})^2$. If $x < (z + 2^{-n})^2$ and $w = z$, the claim is trivial. Otherwise, $x \ge (z + 2^{-n})$, $w = z + 2^{-n}$, and

$$w^2 = (z + 2^{-n})^2 \le x \le (z + 2^{1-n})^2 = (w + 2^{-n})^2.$$

□

According to the next lemma, $rtz\text{-}sqrt(x, n)$ is uniquely determined by the above properties.

Lemma 7.5 *Let $x \in \mathbb{Q}$, $a \in \mathbb{Q}$, and $n \in \mathbb{Z}^+$. Assume that $\frac{1}{4} \le x < 1$ and $a \ge \frac{1}{2}$. If a is n-exact and $a^2 \le x < (a + 2^{-n})^2$, then $a = rtz\text{-}sqrt(x, n)$.*

Proof Let $w = rtz\text{-}sqrt(x, n)$. If $a < w$, then by Lemma 4.20,

$$w \ge fp^+(a, n) = a + 2^{expo(a)+1-n} \ge a + 2^{-n},$$

which implies $w^2 \ge (a + 2^{-n})^2 > x$, contradicting Lemma 7.4. But if $a > w$, then

$$a \ge fp^+(w, n) = w + 2^{-n},$$

and by Lemma 7.4, $a^2 \ge (w + 2^{-n})^2 > x$, contradicting our hypothesis. □

We have the following variation of Lemma 6.12.

Lemma 7.6 *Let $x \in \mathbb{Q}$, $m \in \mathbb{Z}^+$, and $n \in \mathbb{Z}^+$. If $x \geq \frac{1}{4}$ and $n \geq m$, then*

$$RTZ(rtz\text{-}sqrt(x, n), m) = rtz\text{-}sqrt(x, m).$$

Proof The case $m = n$ follows from Lemmas 6.8 and 7.3. We proceed by induction on $n - m$. Let $1 < m \leq n$ and assume that $RTZ(rtz\text{-}sqrt(x, n), m) = rtz\text{-}sqrt(x, m)$. Then by Lemma 6.12,

$$\begin{aligned} RTZ(rtz\text{-}sqrt(x, n), m - 1) &= RTZ(RTZ(rtz\text{-}sqrt(x, n), m), m - 1) \\ &= RTZ(rtz\text{-}sqrt(x, m), m - 1), \end{aligned}$$

and we need only show that $RTZ(rtz\text{-}sqrt(x, m), m - 1) = rtz\text{-}sqrt(x, m - 1)$. Let $w = rtz\text{-}sqrt(x, m)$ and $z = rtz\text{-}sqrt(x, m - 1)$. If $w = z$, then w is $(n - 1)$-exact by Lemma 7.3 and $RTZ(w, n - 1) = w = z$ by Lemma 6.8. But otherwise, $w = z + 2^{-n}$, $2^{n-1}z \in \mathbb{Z}$ by Corollary 7.2, and hence, by Definition 6.1,

$$\begin{aligned} RTZ(w, n - 1) &= 2^{1-n}\lfloor 2^{n-1}w \rfloor \\ &= 2^{1-n}\lfloor 2^{n-1}(z + 2^{-n}) \rfloor \\ &= 2^{1-n}\lfloor 2^{n-1}z + 1 \rfloor \\ &= 2^{1-n}(2^{n-1}z) \\ &= z. \end{aligned}$$

□

7.2 Odd-Rounded Square Root

The name of the following function is motivated by the (once again unproven) observation that for $\frac{1}{4} \leq x < 1$,

$$rto\text{-}sqrt(x, n) = RTO(\sqrt{x}, n).$$

Definition 7.2 Let $x \in \mathbb{R}$ and $n \in \mathbb{Z}^+$, and let $z = rtz\text{-}sqrt(x, n - 1)$. Then

$$rto\text{-}sqrt(x, n) = \begin{cases} z & \text{if } x \leq z^2 \\ z + 2^{-n} & \text{if } x > z^2. \end{cases}$$

Lemma 7.7 *Let $x \in \mathbb{Q}$ and $n \in \mathbb{Z}^+$. If $x \geq \frac{1}{4}$, then*

$$\frac{1}{2} \leq rto\text{-}sqrt(x, n) \leq 1 - 2^{-n}.$$

Proof If $n = 1$, then $rto\text{-}sqrt(x, n) = \frac{1}{2}$ and the claim is trivial. Let $n > 1$ and $z = rtz\text{-}sqrt(x, n-1)$. By Lemma 7.1, $\frac{1}{2} \le z < 1$, which implies

$$\frac{1}{2} \le z \le rto\text{-}sqrt(x, n) \le z + 2^{-n} \le (1 - 2^{1-n}) + 2^{-n} = 1 - 2^{-n}.$$

□

Corollary 7.8 *Let $x \in \mathbb{Q}$ $n \in \mathbb{Z}^+$. If $x \ge \frac{1}{4}$, then $expo(rto\text{-}sqrt(x, n)) = -1$.*

Lemma 7.9 *Let $x \in \mathbb{Q}$ and $n \in \mathbb{Z}^+$. If $x \ge \frac{1}{4}$, then $rto\text{-}sqrt(x, n)$ is n-exact.*

Proof Let $z = rtz\text{-}sqrt(x, n-1)$ and $w = rto\text{-}sqrt(x, n)$. By Corollaries 7.2 and 7.8, $expo(z) = expo(w) = -1$. By Lemma 7.3, $2^{n-1}z \in \mathbb{Z}$. Consequently, since w is either z or $z + 2^{-n}$, $2^n w \in \mathbb{Z}$, i.e., w is n-exact. □

Lemma 7.10 *Let $x \in \mathbb{Q}$, $m \in \mathbb{Z}^+$, and $n \in \mathbb{N}$. Assume that $\frac{1}{4} \le x < 1$ and $2 \le n \le m$. Then*

$$rto(rto\text{-}sqrt(x, m), n) = rto\text{-}sqrt(x, n).$$

Proof We first consider the case $n = m - 1$. Let $z_1 = rtz\text{-}sqrt(x, m-2)$, $w_1 = rto\text{-}sqrt(x, m-1)$, $z_2 = rtz\text{-}sqrt(x, m-1)$, and $w_2 = rto\text{-}sqrt(x, m)$. We shall show that $rto(w_2, m-1) = w_1$. Note that by Lemmas 7.2, 7.6, and 7.4, $\frac{1}{2} \le z_1^2 \le z_2^2 \le x$.

Case 1: $z_1 = z_2$ and $z_2^2 < x$.

$z_1 = w_1 = z_2 = w_2$. Since w_2 is $(m-1)$-exact, Lemma 6.74 implies $rto(w_2, m-1) = w_2 = w_1$.

Case 2: $z_1 = z_2$ and $z_2^2 < x$.

Since w_1 is $(m-2)$-exact, Lemma 4.20 implies that $w_1 = z_1 + 2^{1-n}$ is not $(m-2)$-exact; similarly, since w_2 is $(m-1)$-exact, $w_2 = z_2 + 2^{-m}$ is not $(m-1)$-exact. Therefore,

$$rto(w_2, m-1) = RTZ(w_2, m-2) + 2^{1-n} = z_1 + 2^{1-m} = w_1.$$

Case 3: $z_1 < z_2$ and $z_2^2 = x$.

By Lemma 7.3, z_1 is $(m-1)$-exact and z_2 is $(m-2)$-exact. By Lemma 7.6, $z_1 = RTZ(z_2, m-2) < z_2$, and it follows from Lemma 6.9 that $z_2 = z_1 + 2^{1-m}$. Thus, $w_1 = z_2 = w_2$ and by Lemma 6.74, $rto(w_2, m-1) = w_2 = w_1$.

Case 4: $z_1 < z_2$ and $z_2^2 < x$.

In this case, $w_1 = z_2 = z_1 + 2^{1-m}$ and $w_2 = z_2 + 2^{-m} = z_1 + 2^{1-m} + 2^{-m}$, which is not $(m-2)$-exact. Thus,

$$rto(w_2, m-1) = RTZ(w_2, m-2) + 2^{1-m} = z_1 + 2^{1-m} = w_1.$$

The proof is completed by induction on m. If $m > n$, then by Lemma 6.81,

$$\begin{aligned} rto(rto\text{-}sqrt(x, m), n) &= rto(rto(rto\text{-}sqrt(x, m), m-1), n) \\ &= rto(rto\text{-}sqrt(x, m-1), n) \\ &= rto\text{-}sqrt(x, n). \square \end{aligned}$$

Lemma 7.11 *Let $x \in \mathbb{Q}$, $\ell \in \mathbb{Q}$,$h \in \mathbb{Q}$, and $n \in \mathbb{Z}^+$. Assume that $\frac{1}{4} \le x < 1$, $h > 0$, and $\ell^2 \le x \le h^2$. Then*

$$rto(\ell, n) \le rto\text{-}sqrt(x, n) \le rto(h, n).$$

Proof Let $z = rtz\text{-}sqrt(x, n-1)$ and $w = rto\text{-}sqrt(x, n)$. Suppose $z^2 = x$. Then $w = z$, $\ell^2 \le x = w^2$, and hence $\ell \le w$. By Lemmas 6.79, 6.74, and 7.3,

$$rto(l, n) \le rto(w, n) = w.$$

Thus, we may assume $z^2 < x$ and $w = z + 2^{-n}$. By Lemma 7.4, $\ell^2 \le x < w^2$, and hence $\ell < w = fp^+(z, n-1)$. It follows from Lemmas 6.3, 6.7, and 4.20 that $RTZ(\ell, n-1) \le z$. Therefore,

$$rto(\ell, n) \le RTZ(\ell, n-1) + 2^{1+expo(\ell)-n} \le z + 2^{-n} = w.$$

To prove the second inequality, we note that if $h \ge w$, then by Lemmas 6.79, 6.74, and 7.3,

$$rto(h, n) \ge rto(w, n) = w.$$

Therefore, we may assume that $h < w$. If $z^2 = x$, then $w = z$, $h^2 \ge x = w^2$, and $h \ge w$. Thus, by Lemma 7.4, $z^2 < x$ and $w = z + 2^{-n} = fp^+(z, n-1)$. Since $h^2 \ge x > z^2$, $h > z$. It follows from Lemma 6.9 that $RTZ(h, n-1) \ge a$. By Lemma 4.20, h is not n-exact, and hence

$$rto(h, n) = RTZ(h, n-1) + 2^{-n} \ge z + 2^{-n} = w. \square$$

Lemma 7.12 *Let $x \in \mathbb{Q}$, $q \in \mathbb{Q}$, and $n \in \mathbb{Z}^+$. Assume that $\frac{1}{4} \le x < 1$, $q > 0$, and q is $(n-1)$-exact. Then*

(a) $q^2 < x \Leftrightarrow q < rto\text{-}sqrt(x, n)$;
(b) $q^2 > x \Leftrightarrow q > rto\text{-}sqrt(x, n)$.

Proof Let $z = rtz\text{-}sqrt(x, n-1)$ and $w = rto\text{-}sqrt(x, n)$. If $q^2 > x$, then by Lemma 7.4, $q^2 > z^2$, so that $q > z$ and by Lemma 4.20,

$$q \ge z + 2^{1-n} > z + 2^{-n} \ge w.$$

We may assume, therefore, that $q^2 \le x < (z + 2^{-n})^2$, and hence $q < z + 2^{-n}$. We must show that $q < x^2$ iff $q < w$. By Lemma 4.20, $q \le z$. If $q < z$, then $q < x^2$ and $q < w$. If $q = z = x^2$, then $q = z = w$. Finally, if $q = z < x^2$, then $q = z < z + 2^{-n} = w$. □

7.3 IEEE-Rounded Square Root

The desired approximation function is a simple generalization of *rto-sqrt* to arbitrary positive rationals:

Definition 7.3 Let $x \in \mathbb{Q}$ and $n \in \mathbb{Z}^+$ with $x > 0$. Let $e = \left\lfloor \frac{expo(x)}{2} \right\rfloor + 1$. Then

$$\sqrt[(n)]{x} = 2^e \, rto\text{-}sqrt(2^{-2e}x, n).$$

Lemma 7.13 *Let $x \in \mathbb{Q}$, $x > 0$, $e = \left\lfloor \frac{expo(x)}{2} \right\rfloor + 1$, and $x' = 2^{-2e}x$. Then $\frac{1}{4} \le x' < 1$.*

Proof Since

$$\frac{expo(x)}{2} - 1 < \left\lfloor \frac{expo(x)}{2} \right\rfloor \le \frac{expo(x)}{2},$$

we have

$$expo(x) < 2 \left\lfloor \frac{expo(x)}{2} \right\rfloor + 2 = 2e$$

and

$$expo(x) \ge 2 \left\lfloor \frac{expo(x)}{2} \right\rfloor = 2e - 2.$$

By Lemma 4.6, $-2 \le expo(x') < 0$ and the lemma follows. □

Lemma 7.14 *Let $x \in \mathbb{Q}$ and $n \in \mathbb{Z}^+$. If $\frac{1}{4} \le x < 1$, then*

$$\sqrt[(n)]{x} = rto\text{-}sqrt(x, n).$$

Proof Since $expo(x) \in \{-2, -1\}$, $\left\lfloor \frac{expo(x)}{2} \right\rfloor = -1$ and $e = 0$. □

Lemma 7.15 *Let $x \in \mathbb{Q}$ and $n \in \mathbb{Z}^+$ with $x > 0$. For all $k \in \mathbb{Z}$,*

$$\sqrt[(n)]{2^{2k}x} = 2^k \sqrt[(n)]{x}.$$

Proof Let $x' = 2^{2k}x$, $e = \left\lfloor \frac{expo(x)}{2} \right\rfloor + 1$, and

$$e' = \left\lfloor \frac{expo(x')}{2} \right\rfloor + 1 = \left\lfloor \frac{expo(x)}{2} + k \right\rfloor + 1 = e + k.$$

Then

$$\begin{aligned} \sqrt[(n)]{x'} &= 2^{e'} rto\text{-}sqrt(2^{-2e'}x', n) \\ &= 2^{e+k} rto\text{-}sqrt(2^{-2(e+k)}2^{2k}x, n) \\ &= 2^k \left(2^e rto\text{-}sqrt(2^{2e}x, n)\right) \\ &= 2^k \sqrt[(n)]{x}. \square \end{aligned}$$

Lemma 7.16 *Let $x \in \mathbb{Q}$, $k \in \mathbb{N}$, $m_1 \in \mathbb{N}$, and $n_2 \in \mathbb{N}$ with $x > 0$ and $2 < k + 2 \leq m \leq n$ and let $\mathcal{R}$ be a common rounding mode. Then*

$$\mathcal{R}(\sqrt[(m)]{x}, k) = \mathcal{R}(\sqrt[(n)]{x}, k).$$

Proof Let $e = \left\lfloor \frac{expo(x)}{2} \right\rfloor + 1$. By Definition 7.3 and Lemmas 7.11 and 6.80,

$$\begin{aligned} \mathcal{R}(\sqrt[(m)]{x}, k) &= \mathcal{R}(2^e rto\text{-}sqrt(2^{-2e}x, m), k) \\ &= 2^e \mathcal{R}(rto\text{-}sqrt(2^{-2e}x, m), k) \\ &= 2^e \mathcal{R}(rto\text{-}sqrt(2^{-2e}x, n), k) \\ &= \mathcal{R}(2^e rto\text{-}sqrt(2^{-2e}x, n), k) \\ &= \mathcal{R}(\sqrt[(n)]{x}, k). \square \end{aligned}$$

The next lemma establishes the critical property of $\sqrt[(k)]{x}$ discussed at the beginning of this chapter.

Lemma 7.17 *Let $x \in \mathbb{Q}$, $\ell \in \mathbb{Q}$, $h \in \mathbb{Q}$ $n \in \mathbb{Z}^+$, and $k \in \mathbb{Z}^+$. Assume that $x > 0$ $h > 0$, $k \geq n + 2$, and $\ell^2 \leq x \leq h^2$. Let $\mathcal{R}$ be a common rounding mode. Then*

$$\mathcal{R}(\ell, n) \leq \mathcal{R}(\sqrt[(k)]{x}, n) \leq \mathcal{R}(h, n).$$

Proof Let $e = \left\lfloor \frac{expo(x)}{2} \right\rfloor + 1$, $x' = 2^{-2e}x$, $\ell' = 2^{-e}\ell$, and $h' = 2^{-e}h$. By Lemmas 7.13 and 7.11,

$$RTO(\ell', k) \leq rto\text{-}sqrt(x', k) \leq RTO(h', k),$$

or

$$RTO(2^{-k}\ell, k) \leq 2^{-k} \sqrt[(k)]{x} \leq RTO(2^{-k}h, k).$$

By Lemma 6.80,

$$RTO(\ell, k) \leq \sqrt[(k)]{x} \leq RTO(h, k),$$

and by Lemma 6.101,

$$\mathcal{R}(\ell, n) = \mathcal{R}(RTO(\ell, k), n) \leq \mathcal{R}(\sqrt[(k)]{x}, n) \leq \mathcal{R}(RTO(h, k), n) = \mathcal{R}(h, n). \square$$

Our final lemma, which is also required for the proof of Chap. 19, warrants some motivation. In practice, a typical implementation of a subtractive square root algorithm produces a final truncated approximation q of the square root and a remainder that provides a comparison between q^2 and the radicand x. A final rounded result r is derived from this approximation in accordance with a given rounding mode $\mathcal{R}$ and precision n. In order to apply (7.5), we would like to show that $r = \mathcal{R}(\sqrt[(k)]{x}, n)$ for some appropriate k. This may be done, for example, by invoking Lemma 6.104 with q and $\sqrt[(k)]{x}$ substituted for x and z, respectively. But this requires showing that $q = RTZ(\sqrt[(k)]{x}, n)$ and determining whether $q = \sqrt[(k)]{x}$. Thus, we require a means of converting inequalities relating q^2 and x to inequalities relating q and $\sqrt[(k)]{x}$. This is achieved by the following:

Lemma 7.18 *Let $x \in \mathbb{Q}$, $q \in \mathbb{Q}$, and $n \in \mathbb{N}$. Assume that $x > 0$, $q > 0$, $n > 1$, and q is $(n-1)$-exact. Then*

(a) $q^2 < x \Leftrightarrow q < \sqrt[(n)]{x}$;
(b) $q^2 > x \Leftrightarrow q > \sqrt[(n)]{x}$;
(c) $q^2 = x \Leftrightarrow q = \sqrt[(n)]{x}$.

Proof Let $e = \left\lfloor \frac{expo(x)}{2} \right\rfloor + 1$, $x' = 2^{-2e}x$, and $q' = 2^{-e}q$. Then $\frac{1}{4} \leq x' < 1$ and $\sqrt[(n)]{x} = 2^e rto\text{-}sqrt(x', n)$. By Lemma 7.12,

$$\begin{aligned} q^2 < x &\Leftrightarrow q'^2 < x' \\ &\Leftrightarrow q' < rto\text{-}sqrt(x', n) \\ &\Leftrightarrow 2^{-e}q < 2^{-e}\sqrt[(n)]{x} \\ &\Leftrightarrow q < \sqrt[(n)]{x}. \end{aligned}$$

The proof of (b) is similar, and (c) follows. $\square$

Corollary 7.19 *Let $x \in \mathbb{Q}$ and $n \in \mathbb{N}$ with $x > 0$ and $n > 1$. If $\sqrt[(n)]{x}$ is $(n-1)$-exact, then $(\sqrt[(n)]{x})^2 = x$.*

Proof Instantiate Lemma 7.18 with $q = \sqrt[(n)]{x}$. $\square$

Corollary 7.20 *Let $x \in \mathbb{Q}$, $k \in \mathbb{N}$, $n \in \mathbb{N}$, and $m \in \mathbb{N}$ with $x > 0$, $k > 1$, $n > k$, and $m > k$. If $\sqrt[(n)]{x}$ is $(n-1)$-exact, then $\sqrt[(m)]{x} = \sqrt[(n)]{x}$.*

Proof By Corollary 7.19, $({}^{(n)}\sqrt{x})^2 = x$. The corollary again follows from Lemma 7.18. □

Lemma 7.18 is also critical in the detection of floating-point precision exceptions. As described more fully in Sects. 12.5, 13.5, and 14.3, this exception is signaled when an instruction returns a rounded result r that differs from the precise mathematical value u of an operation. But in the case of the square root, the ACL2 formalization compares r to ${}^{(p+2)}\sqrt{x}$ rather than $u = \sqrt{x}$, where p is the target precision. This is justified by (c) above, from which it follows that $r = \sqrt{x}$ iff $r = {}^{(p+2)}\sqrt{x}$.