THE CALCULUS OF COMPUTATION:
Decision Procedures with
Applications to Verification

by
Aaron Bradley
Zohar Manna

Springer 2007

Part II: Algorithm Reasoning

7. Quantified Linear Arithmetic

Quantifier Elimination (QE) — algorithm for elmiination of all quantifiers of formula F until quantifier-free formula G that is equivalent to F remains

Note: Could be enough F is equisatisfiable to F', that is F is satisfiable iff F' is satisfiable

A theory T admits quantifier elimination if there is an algorithm that given Σ-formula returns a quantifier-free Σ-formula G that is T-equivalent

Example

For $\Sigma_{\mathbb{Q}}$-formula

$F: \exists x.\ 2x = y,$

quantifier-free $T_{\mathbb{Q}}$-equivalent $\Sigma_{\mathbb{Q}}$-formula is

$G: \top$

For $\Sigma_{\mathbb{Z}}$-formula

$F: \exists x.\ 2x = y,$

there is no quantifier-free $T_{\mathbb{Z}}$-equivalent $\Sigma_{\mathbb{Z}}$-formula.

Let $T_{\widehat{\mathbb{Z}}}$ be $T_{\mathbb{Z}}$ with divisibility predicates.
For $\Sigma_{\widehat{\mathbb{Z}}}$-formula

$F: \exists x.\ 2x = y,$

a quantifier-free $T_{\widehat{\mathbb{Z}}}$-equivalent $\Sigma_{\widehat{\mathbb{Z}}}$-formula is

$G: 2 \mid y.$

In developing a QE algorithm for theory T, we need only consider formulae of the form

$\exists x.\ F$

for quantifier-free F

Example: For Σ-formula

$$G_1\colon \exists x.\ \forall y.\ \underbrace{\exists z.\ F_1[x,y,z]}_{F_2[x,y]}$$
$$G_2\colon \exists x.\ \forall y.\ F_2[x,y]$$
$$G_3\colon \exists x.\ \neg \underbrace{\exists y.\ \neg F_2[x,y]}_{F_3[x]}$$
$$G_4\colon \underbrace{\exists x.\ \neg F_3[x]}_{F_4}$$
$$G_5\colon F_4$$

G_5 is quantifier-free and T-equivalent to G_1

Quantifier Elimination for $T_{\mathbb{Z}}$

$\Sigma_{\mathbb{Z}}$: $\{\ldots, -2, -1, 0,\ 1,\ 2,\ \ldots, -3\cdot, -2\cdot, 2\cdot,\ 3\cdot,\ \ldots,\ +,\ -,\ =,\ <\}$

Lemma:

Given quantifier-free $\Sigma_{\mathbb{Z}}$-formula F s.t. free$(F) = \{y\}$.
F represents the set of integers

S : $\{n \in \mathbb{Z}\ :\ F\{y\ \mapsto\ n\}$ is $T_{\mathbb{Z}}$-valid$\}$.

Either $S \cap \mathbb{Z}^+$ or $\mathbb{Z}^+ \setminus S$ is finite.
where $\mathbb{Z}^+$ is the set of positive integers

Example: $\Sigma_{\mathbb{Z}}$-formula $\quad F$: $\exists x.\ 2x = y$

S: even integers

$S \cap \mathbb{Z}^+$: positive even integers — infinite
$\mathbb{Z}^+ \setminus S$: positive odd integers — infinite

Therefore, by the lemma, there is no quantifier-free $T_{\mathbb{Z}}$-formula that is $T_{\mathbb{Z}}$-equivalent to F.

Thus, $T_{\mathbb{Z}}$ does not admit QE.

Augmented theory $\widehat{T_{\mathbb{Z}}}$

$\widehat{\Sigma_{\mathbb{Z}}}$: $\Sigma_{\mathbb{Z}}$ with countable number of unary divisibility predicates

$k \mid \cdot \quad$ for $k \in \mathbb{Z}^+$

Intended interpretations:

$k \mid x$ holds iff k divides x without any remainder

Example:

$x > 1\ \wedge\ y > 1\ \wedge\ 2 \mid x + y$

is satisfiable (choose $x = 2, y = 2$).

$\neg(2 \mid x)\ \wedge\ 4 \mid x$

is not satisfiable.

Axioms of $\widehat{T_{\mathbb{Z}}}$: axioms of $T_{\mathbb{Z}}$ with additional countable set of axioms

$$\forall x.\ k \mid x\ \leftrightarrow\ \exists y.\ x = ky \quad \text{for } k \in \mathbb{Z}^+$$

$\widehat{T_{\mathbb{Z}}}$ admits QE (Cooper's method)

Algorithm: Given $\widehat{\Sigma_{\mathbb{Z}}}$-formula $\exists x.\ F[x]$, where F is quantifier-free
Construct quantifier-free $\widehat{\Sigma_{\mathbb{Z}}}$-formula that is equivalent to $\exists x.\ F[x]$.

Step 1

Put $F[x]$ in NNF $F_1[x]$, that is,
$\exists x.\ F_1[x]$ has negations only in literals (only $\wedge$, $\vee$)
and $\widehat{T_{\mathbb{Z}}}$-equivalent to $\exists x.\ F[x]$

Step 2

Replace (left to right)

$$\begin{aligned} s = t &\ \Leftrightarrow\ s < t+1\ \wedge\ t < s+1 \\ \neg(s = t) &\ \Leftrightarrow\ s < t\ \vee\ t < s \\ \neg(s < t) &\ \Leftrightarrow\ t < s+1 \end{aligned}$$

The output $\exists x.\ F_2[x]$ contains only literals of form

$$s < t\ , \quad k \mid t\ , \quad \text{or} \quad \neg(k \mid t)\ ,$$

where s, t are $\widehat{T_{\mathbb{Z}}}$-terms and $k \in \mathbb{Z}^+$.

Example:

$$\neg(x < y) \ \wedge \ \neg(x = y + 3)$$
$$\Downarrow$$
$$y < x + 1 \ \wedge \ (x < y + 3 \ \vee \ y + 3 < x)$$

Step 3

Collect terms containing x so that literals have the form

$$hx < t \ , \quad t < hx \ , \quad k \mid hx + t \ , \quad \text{or} \quad \neg(k \mid hx + t) \ ,$$

where t is a term and $h, k \in \mathbb{Z}^+$. The output is the formula $\exists x.\ F_3[x]$, which is $\widehat{T_{\mathbb{Z}}}$-equivalent to $\exists x.\ F[x]$.

Example:

$$x + x + y < z + 3z + 2y - 4x$$
$$\Downarrow$$
$$6x < 4z + y$$

Step 4

Let

$$\delta' = \text{lcm}\{h \ : \ h \text{ is a coefficient of } x \text{ in } F_3[x]\} \ ,$$

where lcm is the least common multiple. Multiply atoms in $F_3[x]$ by constants so that δ' is the coefficient of x everywhere:

$$\begin{array}{rcll} hx < t & \Leftrightarrow & \delta' x < h' t & \text{where} \quad h'h = \delta' \\ t < hx & \Leftrightarrow & h' t < \delta' x & \text{where} \quad h'h = \delta' \\ k \mid hx + t & \Leftrightarrow & h'k \mid \delta' x + h' t & \text{where} \quad h'h = \delta' \\ \neg(k \mid hx + t) & \Leftrightarrow & \neg(h'k \mid \delta' x + h' t) & \text{where} \quad h'h = \delta' \end{array}$$

The result $\exists x.\ F_3'[x]$, in which all occurrences of x in $F_3'[x]$ are in terms $\delta' x$.

Replace $\delta' x$ terms in F_3' with a fresh variable x' to form

$$F_3'' \ : \ F_3\{\delta' x \mapsto x'\}$$

Finally, construct

$$\exists x'.\ \underbrace{F_3''[x'] \ \wedge \ \delta' \mid x'}_{F_4[x']}$$

$\exists x'.F_4[x']$ is equivalent to $\exists x.\ F[x]$ and each literal of $F_4[x']$ has one of the forms:

(A) $x' < a$

(B) $b < x'$

(C) $h \mid x' + c$

(D) $\neg(k \mid x' + d)$

where a, b, c, d are terms that do not contain x, and $h, k \in \mathbb{Z}^+$.

Example: $\widehat{T_{\mathbb{Z}}}$-formula

$$\exists x.\ \underbrace{3x + 1 > y \ \wedge \ 2x - 6 < z \ \wedge \ 4 \mid 5x + 1}_{F[x]}$$

after step 3

$$\exists x.\ \underbrace{2x < z + 6 \ \wedge \ y - 1 < 3x \ \wedge \ 4 \mid 5x + 1}_{F_3[x]}$$

Collecting coefficients of x (step 4),

$$\delta' = \text{lcm}(2, 3, 5) = 30$$

Multiply when necessary

$$\exists x.\ 30x < 15z + 90 \ \wedge \ 10y - 10 < 30x \ \wedge \ 24 \mid 30x + 6$$

Replacing $30x$ with fresh x'

$$\exists x'.\ \underbrace{x' < 15z + 90 \ \wedge \ 10y - 10 < x' \ \wedge \ 24 \mid x' + 6 \ \wedge \ 30 \mid x'}_{F_4[x']}$$

$\exists x'.\ F_4[x']$ is equivalent to $\exists x.\ F[x]$

Step 5 (trickiest part):

Construct

left infinite projection $F_{-\infty}[x']$

of $F_4[x']$ by

(A) replacing literals $x' < a$ by $\top$

(B) replacing literals $b < x'$ by $\bot$

idea: very small numbers satisfy (A) literals but not (B) literals

Let

$$\delta = \text{lcm} \left\{ \begin{array}{l} h \text{ of (C) literals } h \mid x' + c \\ k \text{ of (D) literals } \neg(k \mid x' + d) \end{array} \right\}$$

and B be the set of b terms appearing in (B) literals. Construct

$$F_5 : \bigvee_{j=1}^{\delta} F_{-\infty}[j] \ \vee \ \bigvee_{j=1}^{\delta} \bigvee_{b \in B} F_4[b+j] \ .$$

F_5 is quantifier-free and $\widehat{T_{\mathbb{Z}}}$-equivalent to F.

Intuition

Property (Periodicity)

if $k \mid \delta$

then $k \mid n$ iff $k \mid n + \lambda\delta$ for all $\lambda \in \mathbb{Z}$

That is, $k \mid \cdot$ cannot distinguish between $k \mid n$ and $k \mid n + \lambda\delta$.

By the choice of δ (lcm of the h's and k's) — no $\mid$ literal in F_5 can distinguish between n and $n + \delta$.

$$F_5 : \bigvee_{j=1}^{\delta} F_{-\infty}[j] \ \vee \ \bigvee_{j=1}^{\delta} \bigvee_{b \in B} F_4[b+j]$$

left disjunct $\bigvee_{j=1}^{\delta} F_{-\infty}[j]$:

Contains only $\mid$ literals

Asserts: no least $n \in \mathbb{Z}$ s.t. $F[n]$.

For if there exists n satisfying $F_{-\infty}$,

then every $n - \lambda\delta$, for $\lambda \in \mathbb{Z}^+$, also satisfies $F_{-\infty}$

right disjunct $\bigvee_{j=1}^{\delta} \bigvee_{b \in B} F_4[b+j]$:

Asserts: There is least $n \in \mathbb{Z}$ s.t. $F[n]$.

For let b^* be the largest b in (B).

If $n \in \mathbb{Z}$ is s.t. $F[n]$,

then

$\exists j(1 \le j \le \delta).\ b^* + j \le n \ \wedge \ F[b^* + j]$

In other words,

if there is a solution,

then one must appear in δ interval to the right of b^*

Example (cont):

$$\exists x.\ \underbrace{3x+1 > y \ \wedge \ 2x-6 < z \ \wedge \ 4 \mid 5x+1}_{F[x]}$$

$$\Downarrow$$

$$\exists x'.\ \underbrace{x' < 15z+90 \ \wedge \ 10y-10 < x' \ \wedge \ 24 \mid x'+6 \ \wedge \ 30 \mid x'}_{F_4[x']}$$

By step 5,

$$F_{-\infty}[x] : \ \top \ \wedge \ \bot \ \wedge \ 24 \mid x'+6 \ \wedge \ 30 \mid x' \ ,$$

which simplifies to $\bot$. Compute

$$\delta = \text{lcm}\{24, 30\} = 120 \quad \text{and} \quad B = \{10y - 10\} \ .$$

Then replacing x' by $10y - 10 + j$ in $F_4[x']$ produces

$$F_5 : \bigvee_{j=1}^{120} \left[\begin{array}{l} 10y-10+j < 15z+90 \ \wedge \ 10y-10 < 10y-10+j \\ \wedge \ 24 \mid 10y-10+j+6 \ \wedge \ 30 \mid 10y-10+j \end{array} \right]$$

which simplifies to

$$F_5 : \bigvee_{j=1}^{120} \left[\begin{array}{l} 10y+j < 15z+100 \ \wedge \ 0 < j \\ \wedge \ 24 \mid 10y+j-4 \ \wedge \ 30 \mid 10y-10+j \end{array} \right] .$$

F_5 is quantifier-free and $\widehat{T_{\mathbb{Z}}}$-equivalent to F.

Example:

$$\underbrace{\exists x.\ (3x+1<10\ \vee\ 7x-6>7)\ \wedge\ 2\mid x}_{F[x]}$$

Isolate x terms

$$\exists x.\ (3x<9\ \vee\ 13<7x)\ \wedge\ 2\mid x\ ,$$

so

$$\delta' = \mathrm{lcm}\{3,7\} = 21\ .$$

After multiplying coefficients by proper constants,

$$\exists x.\ (21x<63\ \vee\ 39<21x)\ \wedge\ 42\mid 21x\ ,$$

we replace $21x$ by x':

$$\exists x'.\ \underbrace{(x'<63\ \vee\ 39<x')\ \wedge\ 42\mid x'\ \wedge\ 21\mid x'}_{F_4[x']}\ .$$

Then

$$F_{-\infty}[x']:\ (\top\ \vee\ \bot)\ \wedge\ 42\mid x'\ \wedge\ 21\mid x'\ ,$$

or, simplifying,

$$F_{-\infty}[x']:\ 42\mid x'\ \wedge\ 21\mid x'\ .$$

Finally,

$$\delta = \mathrm{lcm}\{21,42\} = 42 \quad \text{and} \quad B = \{39\}\ ,$$

so

$$F_5:\ \bigvee_{j=1}^{42}(42\mid j\ \wedge\ 21\mid j)\ \vee\ \bigvee_{j=1}^{42}((39+j<63\ \vee\ 39<39+j)\ \wedge\ 42\mid 39+j\ \wedge\ 21\mid 39+j)\ .$$

Since $42\mid 42$ and $21\mid 42$, the left main disjunct simplifies to $\top$, so that F is $\widehat{T_{\mathbb{Z}}}$-equivalent to $\top$. Thus, F is $\widehat{T_{\mathbb{Z}}}$-valid.

Example:

$$\exists x.\ \underbrace{2x=y}_{F[x]}$$

Rewriting

$$\exists x.\ \underbrace{y-1<2x\ \wedge\ 2x<y+1}_{F_3[x]}$$

Then

$$\delta' = \mathrm{lcm}\{2,2\} = 2\ ,$$

so by Step 4

$$\exists x'.\ \underbrace{y-1<x'\ \wedge\ x'<y+1\ \wedge\ 2\mid x'}_{F_4[x']}$$

$F_{-\infty}$ produces $\bot$.

However,

$$\delta = \mathrm{lcm}\{2\} = 2 \quad \text{and} \quad B = \{y-1\}\ ,$$

so

$$F_5:\ \bigvee_{j=1}^{2}(y-1<y-1+j\ \wedge\ y-1+j<y+1\ \wedge\ 2\mid y-1+j)$$

Simplifying,

$$F_5:\ \bigvee_{j=1}^{2}(0<j\ \wedge\ j<2\ \wedge\ 2\mid y-1+j)$$

and then

$$F_5:\ 2\mid y\ ,$$

which is quantifier-free and $\widehat{T_{\mathbb{Z}}}$-equivalent to F.

Two Improvements:

A. Symmetric Elimination

In step 5, if there are fewer

(A) literals $x' < a$

than

(B) literals $b < x'$.

Construct the right infinite projection $F_{+\infty}[x']$ from $F_4[x']$ by replacing

each (A) literal $x' < a$ by $\bot$

and

each (B) literal $b < x'$ by $\top$.

Then right elimination.

$$F_5 : \bigvee_{j=1}^{\delta} F_{+\infty}[-j] \ \vee \ \bigvee_{j=1}^{\delta} \bigvee_{a \in A} F_4[a-j] \ .$$

B. Eliminating Blocks of Quantifiers

$$\exists x_1. \ \cdots \exists x_n. \ F[x_1, \ldots, x_n]$$

where F quantifier-free.

Eliminating x_n (left elimination) produces

$$G_1 : \ \exists x_1. \ \cdots \exists x_{n-1}. \ \bigvee_{j=1}^{\delta} F_{-\infty}[x_1, \ldots, x_{n-1}, j] \ \vee \ \bigvee_{j=1}^{\delta} \bigvee_{b \in B} F_4[x_1, \ldots, x_{n-1}, b+j]$$

which is equivalent to

$$G_2 : \ \bigvee_{j=1}^{\delta} \exists x_1. \ \cdots \exists x_{n-1}. \ F_{-\infty}[x_1, \ldots, x_{n-1}, j] \ \vee \ \bigvee_{j=1}^{\delta} \bigvee_{b \in B} \exists x_1. \ \cdots \exists x_{n-1}. \ F_4[x_1, \ldots, x_{n-1}, b+j]$$

Treat j as a free variable and examine only $1 + |B|$ formulae

- $\exists x_1. \ \cdots \exists x_{n-1}. \ F_{-\infty}[x_1, \ldots, x_{n-1}, j]$
- $\exists x_1. \ \cdots \exists x_{n-1}. \ F_4[x_1, \ldots, x_{n-1}, b+j]$ for each $b \in B$

Example:

$$F : \ \exists y. \ \exists x. \ x < -2 \ \wedge \ 1 - 5y < x \ \wedge \ 1 + y < 13x$$

Since $\delta' = \mathrm{lcm}\{1, 13\} = 13$

$$\exists y. \ \exists x. \ 13x < -26 \ \wedge \ 13 - 65y < 13x \ \wedge \ 1 + y < 13x$$

Then

$$\exists y. \ \exists x'. \ x' < -26 \ \wedge \ 13 - 65y < x' \ \wedge \ 1 + y < x' \ \wedge \ 13 \mid x'$$

There is one (A) literal $x' < \ldots$ and two (B) literals $\ldots < x'$, we use right elimination.

$F_{+\infty} = \bot \qquad \delta = \{13\} = 13 \qquad A = \{-26\}$

$$\exists y. \ \bigvee_{j=1}^{13} \left[\begin{array}{c} -26 - j < -26 \ \wedge \ 13 - 65y < -26 - j \\ \wedge \ 1 + y < -26 - j \ \wedge \ 13 \mid -26 - j \end{array} \right]$$

Commute

$$G : \ \bigvee_{j=1}^{13} \exists y. \ j > 0 \ \wedge \ 39 + j < 65y \ \wedge \ y < -27 - j \ \wedge \ 13 \mid -26 - j$$

Apply QE (treating j as free variable)

$$H : \ \exists y. \ j > 0 \ \wedge \ 39 + j < 65y \ \wedge \ y < -27 - j \ \wedge \ 13 \mid -26 - j$$

Simplify

$$H' : \ \bigvee_{k=1}^{65} (k < -1794 - 66j \ \wedge \ 13 \mid -26 - j \ \wedge \ 65 \mid 39 + j + k)$$

Replace H with H' in G

$$\bigvee_{j=1}^{13} \bigvee_{k=1}^{65} (k < -1794 - 66j \ \wedge \ 13 \mid -26 - j \ \wedge \ 65 \mid 39 + j + k)$$

This formula is $\widehat{T_{\mathbb{Z}}}$-equivalent to F.

Quantifier Elimination over Rationals

$$\Sigma_{\mathbb{Q}}: \{0,\ 1,\ +,\ -,\ =,\ \geq\}$$

we use $>$ instead of $\geq$, as

$$x \geq y \ \Leftrightarrow\ x > y \ \vee\ x = y \qquad x > y \ \Leftrightarrow\ x \geq y \ \wedge\ \neg(x = y)\ .$$

Ferrante and Rackoff's Method

Given a $\Sigma_{\mathbb{Q}}$-formula $\exists x.\ F[x]$, where $F[x]$ is quantifier-free

Generate quantifier-free formula F_4 (four steps) s.t.

F_4 is $\Sigma_{\mathbb{Q}}$-equivalent to $\exists x.\ F[x]$.

Step 1: Put $F[x]$ in NNF. The result is $\exists x.\ F_1[x]$.

Step 2: Replace literals (left to right)

$$\begin{array}{lcl} \neg(s < t) & \Leftrightarrow & t < s \ \vee\ t = s \\ \neg(s = t) & \Leftrightarrow & t < s \ \vee\ t > s \end{array}$$

The result $\exists x.\ F_2[x]$ does not contain negations.

Step 3: Solve for x in each atom of $F_2[x]$, e.g.,

$$t < cx \qquad \Rightarrow \qquad \frac{t}{c} < x$$

where $c \in \mathbb{Z} - \{0\}$.

All atoms in the result $\exists x.\ F_3[x]$ have form

(A) $x < a$

(B) $b < x$

(C) $x = c$

where a, b, c are terms that do not contain x.

Step 4: Construct from $F_3[x]$

- left infinite projection $F_{-\infty}$ by replacing
  (A) atoms $x < a$ by $\top$
  (B) atoms $b < x$ by $\bot$
  (C) atoms $x = c$ by $\bot$
- right infinite projection $F_{+\infty}$ by replacing
  (A) atoms $x < a$ by $\bot$
  (B) atoms $b < x$ by $\top$
  (C) atoms $x = c$ by $\bot$

Let S be the set of a, b, c terms from (A), (B), (C) atoms.
Construct the final

$$F_4:\ F_{-\infty}\ \vee\ F_{+\infty}\ \vee\ \bigvee_{s,t \in S} F_3\left[\frac{s+t}{2}\right]\ ,$$

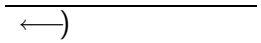
which is $T_{\mathbb{Q}}$-equivalent to $\exists x.\ F[x]$.

- $F_{-\infty}$ captures the case when small $n \in \mathbb{Q}$ satisfy $F_3[n]$
- $F_{+\infty}$ captures the case when large $n \in \mathbb{Q}$ satisfy $F_3[n]$
- last disjunct: for $s, t \in S$
  if $s \equiv t$, check whether $s \in S$ satisfies $F_4[s]$
  if $s \not\equiv t$, $\frac{s+t}{2}$ represents the whole interval (s, t), so check $F_4[\frac{s+t}{2}]$

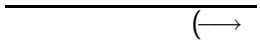
Intuition

Step 4 says that four cases are possible:

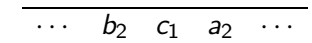
1. There is a left open interval s.t. all elements satisfy $F(x)$.



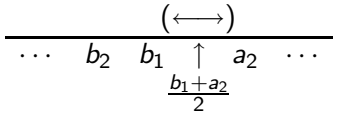
2. There is a right open interval s.t. all elements satisfy $F(x)$.



3. Some a_i, b_i, or c_i satisfies $F(x)$.



4. There is an open interval between two a_i, b_i, or c_i terms s.t. every element satisfies $F(x)$.



Example: $\Sigma_{\mathbb{Q}}$-formula

$$\exists x.\ \underbrace{3x+1<10\ \wedge\ 7x-6>7}_{F[x]}$$

Solving for x

$$\exists x.\ \underbrace{x<3\ \wedge\ x>\frac{13}{7}}_{F_3[x]}$$

Step 4: $x < 3$ in (A) $\Rightarrow$ $F_{-\infty} = \bot$
$x > \frac{13}{7}$ in (B) $\Rightarrow$ $F_{+\infty} = \bot$

$$F_4:\ \bigvee_{s,t\in S} \underbrace{\left(\frac{s+t}{2}<3\ \wedge\ \frac{s+t}{2}>\frac{13}{7}\right)}_{F_3[\frac{s+t}{2}]}$$

$S = \{3, \frac{13}{7}\}$ $\Rightarrow$

$$F_3\left[\frac{3+3}{2}\right] = \bot \qquad F_3\left[\frac{\frac{13}{7}+\frac{13}{7}}{2}\right] = \bot$$

$$F_3\left[\frac{\frac{13}{7}+3}{2}\right]:\ \frac{\frac{13}{7}+3}{2}<3\ \wedge\ \frac{\frac{13}{7}+3}{2}>\frac{13}{7}$$

simplifies to $\top$.

Thus, $F_4 : \top$ is $T_{\mathbb{Q}}$-equivalent to $\exists x.\ F[x]$,
so $\exists x.\ F[x]$ is $T_{\mathbb{Q}}$-valid.