Reasoning About Programs

Week 3 Tutorial - Mathematical and Strong Induction

Sophia Drossopoulou and Mark Wheelhouse

Aims: To apply mathematical induction, the mathematical induction technique and strong induction. Moreover, to think about the choice of the appropriate induction principle to apply. Note also that some properties can be proven without the use of induction.

In the following, $\mathbb{N}$ stands for the natural numbers $\{0, 1, 2...\}$, $\mathbb{N}^+$ stands for the positive natural numbers $\{1, 2...\}$ and $\mathbb{Z}$ stands for the integers $\{..., -2, -1, 0, 1, 2, ...\}$.

0th Question:

Prove that

$$\forall n \in \mathbb{N}. \exists m \in \mathbb{N}.\ [\ 2^{2*n} = 3 * m + 1\ ]$$

A possible answer:

We will prove this assertion by mathematical induction over n.
Note: The main challenge in this exercise is the treatment of the existential quantifiers.

Base case:

To show: $\exists m \in \mathbb{N}.\ [\ 2^{2*0} = 3 * m + 1\ ]$

$$\begin{array}{lll} 2^{2*0} & & \\ \quad = & 2^0 & \text{by arithmetic} \\ \quad = & 1 & \text{by arithmetic} \\ \quad = & 3 * 0 + 1 & \text{by arithmetic} \end{array}$$

Therefore, taking $m = 0$, we obtain that $\exists m \in \mathbb{N}.\ [\ 2^{2*0} = 3 * m + 1\ ]$

Inductive Step:

Take an arbitrary $k \in \mathbb{N}$.

Inductive Hypothesis: $\exists m \in \mathbb{N}.\ [\ 2^{2*k} = 3 * m + 1\ ]$
To show: $\exists m \in \mathbb{N}.\ [\ 2^{2*(k+1)} = 3 * m + 1\ ]$

(Fact_1) From the induction hypothesis, we take $m1 \in \mathbb{N}$, such that $2^{2*k} = 3 * m1 + 1$.

$$\begin{array}{lll} 2^{2*(k+1)} & & \\ \quad = & 2^{2*k+2} & \text{by arithmetic} \\ \quad = & 2^{2*k} * 2^2 & \text{by arithmetic} \\ \quad = & 2^{2*k} * 4 & \text{by arithmetic} \\ \quad = & (3 * m1 + 1) * 4 & \text{by (Fact\_1)} \\ \quad = & 4 * 3 * m1 + 4 & \text{by arithmetic} \\ \quad = & 4 * 3 * m1 + 3 + 1 & \text{by arithmetic} \\ \quad = & 3 * (4 * m1 + 1) + 1 & \text{by arithmetic} \end{array}$$

Therefore, taking $m = 4 * m1 + 1$, we obtain that $\exists m \in \mathbb{N}.\ [\ 2^{2*(k+1)} = 3 * m + 1\ ]$

1st Question:

Given the following function definition:

```
squareList :: Int -> [Int]
squareList 1 = [1]
squareList n = (2*n + m - 1 : ms) where
   ms = squareList (n-1)
    m = head ms
```

(a) What is the value of `squareList` (-3)? What is the value of `squareList 0`?

(b) Consider the assertion:

$$(*)\quad \forall n \in \mathbb{N}^{+}.\ \texttt{head}\ (\texttt{squareList}\ n) = n^2.$$

Which induction principle will you use to prove $(*)$?
Write out this principle as it applies for $(*)$.

(c) Prove $(*)$.

A possible answer:

a Both `squareList` (-3) and `squareList 0` are undefined.

b We define $P \subseteq \mathbb{N}$ as $P(n) \longleftrightarrow (\texttt{head}\ (\texttt{squareList}\ n)\ = n^2\ )$.

The assertion (*) is equivalent to $\forall n \geq 1.\ P(n)$. Therefore the induction technique is applicable. This gives:

$$\texttt{head}\ (\texttt{squareList 1})\ = 1^2$$
$$\wedge$$
$$\forall k \geq 1\,[\,\texttt{head}\ (\texttt{squareList}\ k)\ = k^2\ \rightarrow\ \texttt{head}\ (\texttt{squareList}\ (k+1))\ = (k+1)^2\,]$$
$$\longrightarrow$$
$$\forall n \geq 1.\,\texttt{head}\ (\texttt{squareList}\ n)\ = n^2$$

c We prove $(*)$ by application of the induction technique as outlined in part (b).

Base case:

To show: `head` (`squareList 1`) $= 1^2$

$$\begin{aligned} &\texttt{head}\ (\texttt{squareList 1}) \\ &\quad = \ \texttt{head}\ [1] \quad \text{by definition of } \texttt{squareList} \\ &\quad = \ 1 \quad \text{by definition of } \texttt{head} \\ &\quad = \ 1^2 \quad \text{by arithmetic} \end{aligned}$$

Inductive Step:

Take an arbitrary $k \in \mathbb{N}$. Assume that $k \geq 1$.

Inductive Hypothesis: `head` (`squareList` k) $= k^2$

To show: `head` (`squareList` $(k+1)$) $= (k+1)^2$

$$
\begin{array}{lll}
\multicolumn{3}{l}{\texttt{head}\ (\texttt{squareList}\ (k+1))} \\
= & 2(k+1)+m-1 & \text{by function definition} \\
  &   & \text{where } m = \texttt{head}\ (\texttt{squareList}\ k) \\
= & 2(k+1)+k^2-1 & \text{by ind. hyp.} \\
= & k^2+2k+1 & \text{by arithmetic} \\
= & (k+1)^2 & \text{by arithmetic}
\end{array}
$$

2nd Question:

Consider the following program for calculating powers of 2:

```
powerTwo :: Int -> Int
powerTwo 0 = 1
powerTwo n = 2 * (powerTwo (n - 1))
```

(a) Consider the assertion:

$$(*)\quad \texttt{powerTwo}\ n < n! \qquad \text{for all } n \geq 4$$

Write out the induction principle that is applicable to $(*)$.

(b) Prove $(*)$.

(c) Consider the assertion:

$$(**)\quad \forall n \in \mathbb{N}.\ \texttt{powerTwo}\ (2*n) = (\texttt{powerTwo}\ n) * (\texttt{powerTwo}\ n)$$

Write out the mathematical induction principle that allows us to prove $(**)$.
Write out the strong induction principle that allows us to prove $(**)$.

(d) Prove $(**)$.

(e) Consider the following, more efficient, program for calculating powers of 2:

```
powerTwoMod :: Int -> Int
powerTwoMod 0 = 1
powerTwoMod n
      | (mod n 2) == 0
          = (powerTwoMod (div n 2))  * (powerTwoMod (div n 2))
      | otherwise
          = 2 * powerTwoMod (n - 1)
```

Remember that `mod` and `div` have the property that for all $\mathtt{x}, \mathtt{y} \in \mathbb{N}$:

(A) $(\texttt{div x y}) * \mathtt{y} + (\texttt{mod x y}) = \mathtt{x}$

(B) $\mathtt{y} \neq 1 \ \rightarrow\ \texttt{div x y} < \mathtt{x}$

(C) $\texttt{mod x y} < \mathtt{y}$

Prove that $\forall n \in \mathbb{N}.\ \texttt{powerTwoMod}\ n = \texttt{powerTwo}\ n.$

(f) Prove that $\texttt{powerTwoMod}\ n < n!$ for all $n \geq 4$.

A possible answer:

(a) Let $P \subseteq \mathbb{N}$ be defined as $P(n) \longleftrightarrow \texttt{powerTwo}\ n < n!$.
Then, the assertion (*) is equivalent with $\forall n \geq 4 . P(n)$.
Therefore the mathematical induction technique is applicable. This gives:

$$\begin{array}{l} \texttt{powerTwo}\ 4 < 4! \\ \wedge \\ \forall k \geq 4 .\ [\ \texttt{powerTwo}\ k < k! \rightarrow \texttt{powerTwo}\ (k+1) < (k+1)!\ ] \\ \longrightarrow \\ \forall n \geq 4 . \texttt{powerTwo}\ n < n! \end{array}$$

(b) Let $Q \subseteq \mathbb{N}$ be defined as $Q(n) \longleftrightarrow \texttt{powerTwo}\ n < n!$.
We can prove $\forall \texttt{n} \geq 4.\ Q(n)$ by the induction technique.

Base case:

To show: $\texttt{powerTwo}\ 4 < 4!$

$$\begin{array}{lll} \texttt{powerTwo}\ 4 & & \\ \quad = & 16 & \text{by definition of } \texttt{powerTwo} \\ \quad < & 24 & \text{by arithm.} \\ \quad = & 4 * 3 * 2 * 1 = 4! & \text{by def. of } ! \end{array}$$

Inductive Step:

Take an arbitrary $k \in \mathbb{N}$.
Assume that (Ass1) $k \geq 4$.
Inductive Hypothesis: $\texttt{powerTwo}\ k < k!$
To show: $\texttt{powerTwo}\ (k+1) < (k+1)!$

We obtain:
(Fact_1) $2 < k+1$ because of (Ass1).

We now calculate $\texttt{powerTwo}\ (k+1)$.

$$\begin{array}{lll} \texttt{powerTwo}\ (k+1) & & \\ \quad = & 2 * (\texttt{powerTwo}\ k) & \text{by definition of } \texttt{powerTwo} \\ \quad < & 2 * k! & \text{by induct. hyp.} \\ \quad < & (k+1) * k! & \text{because of (Fact\_1)} \\ \quad = & (k+1)! & \text{by definition of } ! \end{array}$$

Note that the use of (Ass1) was indispensable here.

(c) Let $R \subseteq \mathbb{N}$ be defined as $R(n) \longleftrightarrow \texttt{powerTwo}\ (2*n) = (\texttt{powerTwo}\ n) * (\texttt{powerTwo}\ n)$.
The mathematical induction principle gives

$$\begin{array}{l} \texttt{powerTwo}\ (2*0) = (\texttt{powerTwo}\ 0) * (\texttt{powerTwo}\ 0) \\ \wedge \\ \forall k \in \mathbb{N}\ [\ \texttt{powerTwo}\ (2*k) = (\texttt{powerTwo}\ k) * (\texttt{powerTwo}\ k) \\ \qquad\qquad \rightarrow \\ \qquad\qquad \texttt{powerTwo}\ (2*(k+1)) = (\texttt{powerTwo}\ (k+1)) * (\texttt{powerTwo}\ (k+1))\ ] \\ \longrightarrow \\ \forall n \in \mathbb{N} . \texttt{powerTwo}\ (2*n) = (\texttt{powerTwo}\ n) * (\texttt{powerTwo}\ n) \end{array}$$

The strong induction principle gives

$$\begin{array}{l}
\texttt{powerTwo}\ (2*0) = (\texttt{powerTwo}\ 0)*(\texttt{powerTwo}\ 0) \\
\wedge \\
\forall k \in \mathbb{N}\ [\ \forall j \leq k.\, \texttt{powerTwo}\ (2*j) = (\texttt{powerTwo}\ j)*(\texttt{powerTwo}\ j) \\
\qquad\qquad \rightarrow \\
\qquad\qquad \texttt{powerTwo}\ (2*(k+1)) = (\texttt{powerTwo}\ (k+1))*(\texttt{powerTwo}\ (k+1))\ ] \\
\longrightarrow \\
\forall n \in \mathbb{N}.\, \texttt{powerTwo}\ (2*n) = (\texttt{powerTwo}\ n)*(\texttt{powerTwo}\ n)
\end{array}$$

(d) We will prove $\forall \texttt{n} \in \mathbb{N}.\ R(n)$ by mathematical induction.

Base case:

To show: $\texttt{powerTwo}\ (2*0) = (\texttt{powerTwo}\ 0)*(\texttt{powerTwo}\ 0)$

$$\begin{array}{lll}
\multicolumn{3}{l}{\texttt{powerTwo}\ (2*0)} \\
= & \texttt{powerTwo}\ (0) & \text{by arithmetic} \\
= & 1 & \text{by def. of } \texttt{powerTwo} \\
= & 1*1 & \text{by arithmetic} \\
= & (\texttt{powerTwo}\ 0)*(\texttt{powerTwo}\ 0) &
\end{array}$$

Inductive Step

Take an arbitrary $k \in \mathbb{N}$.

Inductive Hypothesis: $\texttt{powerTwo}\ (2*k) = (\texttt{powerTwo}\ k)*(\texttt{powerTwo}\ k)$

To show: $\texttt{powerTwo}\ (2*(k+1)) = \texttt{powerTwo}\ (k+1)\ *\ \texttt{powerTwo}\ (k+1)$

$$\begin{array}{lll}
\multicolumn{3}{l}{\texttt{powerTwo}\ (2*(k+1))} \\
= & \texttt{powerTwo}\ (2*k+2) & \text{because } 2*(k+1) = 2*k+2 \\
= & 2*2*\texttt{powerTwo}\ (2*k) & \text{by definition of } \texttt{powerTwo}\text{, twice} \\
= & 2*2*(\texttt{powerTwo}\ k)*(\texttt{powerTwo}\ k) & \text{by inductive hypothesis} \\
= & 2*(\texttt{powerTwo}\ k)*2*(\texttt{powerTwo}\ k) & \text{by properties of } * \\
= & \texttt{powerTwo}\ (k+1)\ *\ \texttt{powerTwo}\ (k+1) & \text{by definition of } \texttt{powerTwo}\text{, twice}
\end{array}$$

(e) Let $S \subseteq \mathbb{N}$ be defined as $S(n) \longleftrightarrow \texttt{powerTwoMod}\ n = \texttt{powerTwo}\ n$.

We will prove $\forall n \in \mathbb{N}.\ S(n)$ by strong induction.

Note: It is not always obvious whether an assertion can be proven by mathematical induction or strong in induction. In the particular case of proving properties of `powerTwoMod _`*, the fact that* `powerTwoMod n` *is defined in terms of* `powerTwoMod (div n 2)`*, rather than in terms of* `powerTwoMod (n − 1)` *hints at the fact that we will need strong induction. Alternatively, you might have tried to develop the proof using mathematical induction, get stuck at the inductive step, and then realize that you need to apply strong induction.*

Base case:

To show: $\texttt{powerTwoMod}\ 0 = \texttt{powerTwo}\ 0$

$$\begin{array}{lll}
\multicolumn{3}{l}{\texttt{powerTwoMod}\ 0} \\
= & 1 & \text{by definition of } \texttt{powerTwoMod} \\
= & \texttt{powerTwo}\ 0 & \text{by definition of } \texttt{powerTwo}
\end{array}$$

Inductive Step:

Take an arbitrary $k \in \mathbb{N}$.
Inductive Hypothesis: $\forall j \leq k.\ \texttt{powerTwoMod}\ j = \texttt{powerTwo}\ j$
To show: $\texttt{powerTwoMod}\ (k+1) = \texttt{powerTwo}\ (k+1)$

1st Case: $\texttt{mod}\ (k+1)\ 2 = 0$.

Then, by application of **(A)** on the fact from above, we obtain:
$(\mathit{Fact\_2})\quad (\texttt{div}\ (k+1)\ 2) * 2 = (k+1)$

We use $\texttt{d}$ as a shorthand for $\texttt{div}\ (k+1)\ 2$.

then have:

$$\begin{array}{lll}
\multicolumn{3}{l}{\texttt{powerTwoMod}\ (k+1)} \\
= & (\texttt{powerTwoMod d})\ * (\texttt{powerTwoMod d}) & \text{by definition of } \texttt{powerTwoMod} \\
= & (\texttt{powerTwo d})\ * (\texttt{powerTwo d}) & \text{by inductive hypothesis} \\
 & & \text{NOTE: ind. hyp. applicable because} \\
 & & \texttt{d} < k+1 \text{ by (} \mathbf{B}\text{) , and therefore } \texttt{d} \leq k \\
= & \texttt{powerTwo}\ (2 * \texttt{d}) & \text{by part (c)} \\
= & \texttt{powerTwo}\ (k+1) & \text{by (Fact\_2), and definition of } d \\
 & & \text{which gives } 2 * \texttt{d} = k+1
\end{array}$$

2nd Case: $\texttt{mod}\ (k+1)\ 2\ \neq\ 0$.

$$\begin{array}{lll}
\multicolumn{3}{l}{\texttt{powerTwoMod}\ (k+1)} \\
= & 2\ * \texttt{powerTwoMod}\ k & \text{by definition of } \texttt{powerTwoMod} \\
= & 2\ * \texttt{powerTwo}\ k & \text{by inductive hypothesis} \\
= & \texttt{powerTwo}\ (k+1) & \text{by definition of } \texttt{powerTwo}
\end{array}$$

Note: While doing this proof we discover that we need an auxiliary lemma. Fortunately, this lemma has already been proven in part (c).

(f) This follows from the lemma shown in part (a) and the lemma shown in part (c).

3rd Question (challenge)

Consider *trominoes* which are three squares glued together in the form of an L-shape. The following assertion holds:

> $(*)$ In a square grid 2^n by 2^n there exists a single square, such that the rest of the grid can be tiled using trominoes.

Assume that in an m by m grid the rows and columns are enumerated from 1 to m, that is the coordinates of the squares are from the set $\{1, ...m\} \times \{1, ...m\}$, and that $i, j \in \{1, ...m\}$. In Figure 1 we see a an m by m grid, and the square at (i, j).

(a) Express $(*)$ formally, using an assertion $Q \subseteq \mathbb{N} \times \mathbb{N} \times \mathbb{N}$, where $Q(m, i, j)$ stands for

> In a m by m grid, if we choose a square at the co-ordinates (i, j) , we can tile the rest using trominoes.

(b) Apply the mathematical induction principle to your solution from part a).

(c) Prove the assertion from part a. *Hint:* You may need to prove a stronger assertion than the one in a.

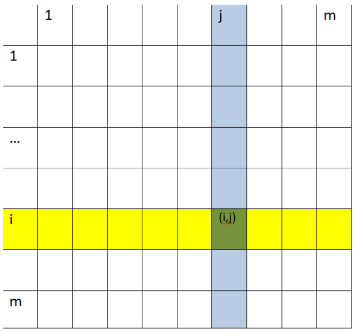


Figure 1: Trominoes, m by m grids, and a square at (i, j)

A possible answer:

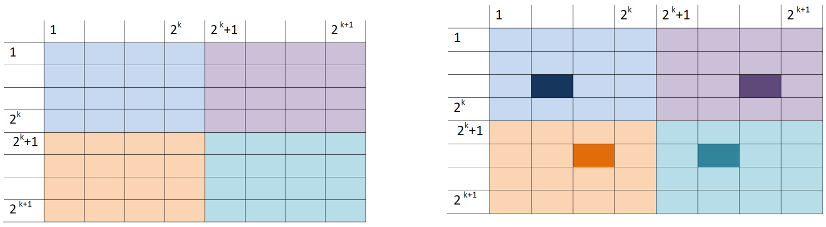
The answer is quite long, because it discusses alternatives and gives explanations – such discussions are not expected in exams.

a (**) $\quad \forall n : \mathbb{N}.\exists i, j : \mathbb{N}.[\ 1 \leq i, j \leq 2^n \ \wedge \ Q(2^n, i, j)\ ]$

b $\exists i, j : \mathbb{N}.[\,1 \leq i, j \leq 2^0 \wedge Q(2^0, i, j)\,]$
$\wedge$
$\forall k : \mathbb{N}.[\quad \exists i, j : \mathbb{N}.[\,1 \leq i, j \leq 2^k \wedge Q(2^k, i, j)\,]$
$\to$
$\exists i, j : \mathbb{N}.[\,1 \leq i, j \leq 2^{k+1} \wedge Q(2^{k+1}, i, j)\,] \quad]$
$\to$
$\forall n : \mathbb{N}.\exists i, j : \mathbb{N}.[\ 1 \leq i, j \leq 2^n \ \wedge \ Q(2^n, i, j)\ ]$

c We can try to prove $(**)$ by induction on n. The base case is straight-forward. In the inductive step, we need to think how we will be able to apply the induction hypothesis. For this, we note that $2^{k+1} = 2 * 2^k$ (by definition of x^y), and therefore, a 2^{k+1} by 2^{k+1} grid contains four 2^k by 2^k sub-grids. We can see this in Figure 2.a.

We can apply the inductive hypothesis to each subgrid, and obtain that in each of these we can pick one square, and tile the rest with trominoes. We can see this in Figure 2.b. But we are left with *four* squares, rather than just the *one* as requested in (**).



a: An 2^{k+1} by 2^{k+1} grid

b: Each subgrid has an empty square

Figure 2: 2^{k+1} by 2^{k+1} grid

But what if we were at liberty to chose *where* to place the square in three of the sub-grids? If indeed we had that liberty, then we could chose to place them in the middle of the larger grid, so as to build a shape that can be covered by a tromino. This is show in Fig. 3.

So, instead of (**), we will be proving a *stronger* assertion, which says that

(***) $\forall n : \mathbb{N}.\forall i, j : \mathbb{N}.[\, 1 \leq i, j \leq 2^n \to Q(2^n, i, j)\,]$

In words,

> $(***)$ In a square grid 2^n by 2^n pick any single square.
> The rest of the grid can be tiled using trominoes.

(As an exercise, prove that (***) implies (**)).

Applying the inductive principle on (***), we obtain:

$$
\begin{array}{l}
\forall i, j : \mathbb{N}.[\, 1 \leq i, j \leq 2^0 \to Q(2^0, i, j)\,] \\
\wedge \\
\forall k : \mathbb{N}.[\quad (\ \forall i, j : \mathbb{N}.[\, 1 \leq i, j \leq 2^k \to Q(2^k, i, j)\,]\ ) \\
\qquad\qquad\quad \to \\
\qquad\qquad\quad (\ \forall i, j : \mathbb{N}.[\, 1 \leq i, j \leq 2^{k+1} \to Q(2^{k+1}, i, j)\,]\ ) \quad] \\
\to \\
\forall n : \mathbb{N}.\forall i, j : \mathbb{N}.[\, 1 \leq i, j \leq 2^n \to Q(2^n, i, j)\,]
\end{array}
$$

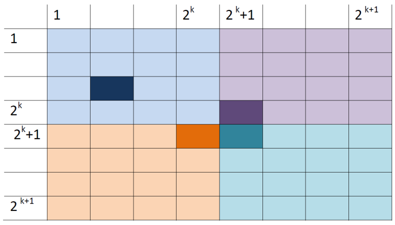


Figure 3: The 2^{k+1} by 2^{k+1} grid revisited

We now proceed with the proof:

Base case:

To show: $Q(1, 1, 1)$
(this is so because $2^0 = 1$, and because $1 \leq i \leq 1$ implies $i = 1$).
Now $Q(1, 1, 1)$ says that if we select a square at coordinates $(1, 1)$ in a 1 by 1 grid, the rest can be covered by trominoes. This holds trivially, because after selecting a square at coordinates $(1, 1)$ in a 1 by 1 grid, there is nothing left to cover.

Inductive Step:

Take an arbitrary $k \in \mathbb{N}$.

Inductive Hypothesis: $\forall i, j : \mathbb{N}.[\, 1 \leq i, j \leq 2^k \to Q(2^k, i, j)\,]$
To show: $\forall i, j : \mathbb{N}.[\, 1 \leq i, j \leq 2^{k+1} \to Q(2^{k+1}, i, j)\,]$

Take $i : \mathbb{N}, j : \mathbb{N}$. arbitrary.
Ass1: assume that $1 \leq i, j \leq 2^{k+1}$.

We want to show that $Q(2^{k+1}, i, j)$.

To be able to progress, we split the 2^{k+1} by 2^{k+1} grid into four sub-grids, and also need to find which of the four sub-grids contains the single square at (i, j). We can do this by case analysis.

Namely, from **Ass1** we know that
$1 \leq i, j \leq 2^k \quad \vee \quad 1 \leq j \leq 2^k < i \leq 2^{k+1} \quad \vee \quad 1 \leq i \leq 2^k < j \leq 2^{k+1} \quad \vee \quad 2^k < i, j \leq 2^{k+1}$

1st Case: $1 \leq i, j \leq 2^k$. That is the single square was selected in the left upper sub-grid. Then, by application of the induction hypothesis on this sub-grid, we know that we can cover the rest of it with trominoes, that is,
(A) All squares in $\{1, ..2^k\} \times \{1, ..2^k\} \setminus \{(i, j)\}$ can be covered with trominoes.

We apply the inductive hypothesis on the left lower sub-grid, and select our single square to be at its right-most upper-most part, ie at $2^k + 1$ and 2^k, that is,
(B) All squares in $\{2^k + 1, ..2^{k+1}\} \times \{1, ..2^k\} \setminus \{(2^k + 1, 2^k)\}$ can be covered with trominoes.

We then apply the inductive hypothesis on the right lower grid, and select our single square to be at the left-most upper-most part, ie at $2^k + 1$ and $2^k + 1$, that is,
(C) All squares in $\{2^k+1, ..2^{k+1}\} \times \{2^k+1, ..2^{k+1}\} \setminus \{(2^k+1, 2^k+1)\}$ can be covered with trominoes.

Finally, we apply the inductive hypothesis on the right upper grid, and select our single square to be at the left-most lower-most part, ie at 2^k and $2^k + 1$, that is,
(D) All squares in $\{1, ..2^k\} \times \{2^k + 1, ..2^{k+1}\} \setminus \{(2^k, 2^k + 1)\}$ can be covered with trominoes.

(E) The squares at $(2^k + 1, 2^k)$, $(2^k + 1, 2^k + 1)$, $(2^k, 2^k + 1)$ can be covered by a tromino.

Therefore, from **(A)** - **(E)** we obtain that the squares at $\{1, ..2^{k+1}\} \times \{1, ..2^{k+1}\} \setminus \{(i, j)\}$ can be covered with trominoes. That is, $Q(2^{k+1}, i, j)$ holds.

Note that we applied the induction hypothesis *four* times.

2nd Case: $1 \leq j \leq 2^k < i \leq 2^{k+1}$, similar to **1st Case**.

3rd Case: $1 \leq i \leq 2^k < j \leq 2^{k+1}$, similar to **1st Case**.

4th Case: $2^k < i, j \leq 2^{k+1}$, similar to **1st Case**.