6 What does it mean to prove theorems?

We already saw many examples of different proofs in this course. Let us pause for a second and think about various approaches and techniques that can be used for proofs. It is quite difficult to come up with a logical and algorithmic proof theory and hence most of my explanations will be relying on some "common sense" and intuitive understanding of what we call "a convincing explanation."

6.1 Statements and truth tables

Proof is an explanation of why a statement is true. Therefore, I start with a very brief discussion of what a statement is and how to determine whether a complicated statement is true or false.

A *statement* is a sentence which is either true or false (in this case one of the alternatives must be fulfilled, no statement is allowed to be true and false at the same time, and this is, hopefully, in accordance with our intuition). For example, the statement "2 is an integer" is definitely true, whereas "1/2 is an integer" is false. We know this because we are well aware of the commonly acknowledged definition of being an integer.

I can make new statements out of the old ones using the operations of negation (not), conjunction (and), disjunction (or), or implication (if...then). Let me start with the simplest operation.

The negation of statement A is the statement (again, according to our intuition and common sense), which is true when A is false and is false when A is true. I can write this in the form of a *truth table*:

A	not A
T	F
F	T

The conjunction of two statement A and B is the statement "A and B," and here is the truth table for it:

A	B	A and B
T	T	T
T	F	F
F	T	F
F	F	F

The disjunction of two statement A and B is the statement "A or B," and here is the truth table for it:

A	B	A or B
T	T	T
T	F	T
F	T	T
F	F	F

note that A or B is true if both A and B are true.

Finally, the truth table for the implication "if A then B" has the form

A	B	if A then B
T	T	T
T	F	F
F	T	T
F	F	T

This truth table is probably the least intuitive out of the considered four. To convince yourself that the values of the statements are chosen in accordance with our usual intuition consider the conditional statement "if x is divisible by four then x is divisible by 2." Note that this is not a statement by the definition above because we cannot say whether it is true or false without assigning a specific value to x. However, our experience from arithmetics tells us that this statement is true irrespective of what x is. Now take $x = 4$ then x is divisible by 4 and x is divisible by 2 are both true and so is the statement. Take $x = 2$, now x is divisible by 4 is false and x is divisible by 2 is true, and the whole statement is still true. Finally $x = 3$ gives us the motivation to call "if false then false" a true statement.

There are various ways to say if A then B. Very often the notation $A \implies B$ is used. Sometimes people say "B if A" to mean $A \implies B$. Less obvious, "A only if B" means the same $A \implies B$ (think this out).

Two statements are called *equivalent* if the truth tables made from their inputs and outputs are the same. It should be clear, for example, that the statement not not A is equivalent to A (make a truth table if you are not convinced). Using the notion of equivalent statements we can study how negation acts on other statement.

I claim that "not (A and B)" is the same (equivalent) to "not A or not B." To check this built a truth table. Similarly, "not (A or B)" is the same as "not A and not B." What is the negation of an implication? (Think how would you negate, e.g., "if it rains then I will take an umbrella".) I will give you just the result: "not (if A then B)" is equivalent to "A and not B" (it will rain and I will not take an umbrella). Indeed

A	B	not B	if A then B	A and not B
T	T	F	T	F
T	F	T	F	T
F	T	F	T	F
F	F	T	T	F

So remember that the negation of an implication is not an implication.

With the implication I can identify several other statements. The *inverse* of the implication "if A then B" is "if not A then not B." The inverse is not logically equivalent to the original statement (think carefully about the statement "if you are a mathematician then you are intelligent").

The *converse* of "if A then B" is "if B then A." As it can be simply checked the converse is not equivalent to the original statement. However, sometimes it happens that both $A \implies B$ and $B \implies A$ are true, and in this case we say that A and B are logically equivalent and write $A \Leftrightarrow B$. Another common abbreviation is to say that A if and only if B. Keep in mind that this kind of statement always has hidden two statements, which both must be analyzed in a proof. Yet another language used is "A is a necessary and sufficient condition for B." This literally mean that $A \implies B$ (A is sufficient for B, B is true if A is true) and $B \implies A$ (A is necessary for B, B is true only if A is true).

A *contrapositive* of an implication is "not B implies not A." By building a truth table, one can see that contrapositive is equivalent to the implication, and therefore in the proofs we can always replace the statement "A only if B" with "not B only if A" as we already did several times.

Finally, in mathematics we often mean two different things about x if we hear something like "x is an odd number." We may mean that "for all x, x is an odd number" or "there is an x, such that x is an odd number." Both of these expressions are called *quantifier*, the former is *the universal quantifier* and the latter is *the existential quantifier*. In some sentences people use more than one, e.g., "for any x there is an y such that $y > x$." Clearly the last statement is true. What about "there is y such that for any x $y > x$"? This is of cause false, and hence the take-home-message: be careful with the order of the quantifiers. Convince yourself that if you negate a universal quantifier you get an existential one and vice versa.

Now we are ready to talk about various proof techniques.

6.2 Proof techniques

Let us first set up the terminology. *Definition* is an explanation of the mathematical meaning of the word. *Theorem, proposition, lemma* are used to denote true statements (more important is theorem, less important is proposition, a statement that is used in proving other facts is lemma). *Corollary* is a true statement that is a simple deduction of another true statement. *Proof* is a (convincing) explanation why something is true. *Conjecture* is a statement believed to be true, but for which we have no proof. Finally, *axiom* is a basic assumption that does not require proof.

6.2.1 Direct proof

The vast majority of the statements to be proved can be broken into smaller statements of the form "if A then B." The idea of a direct proof is to find a sequence of implications $A \implies C_1$, $C_1 \implies C_2$, $C_2 \implies C_3, \dots, C_k \implies B$, where all the steps are almost obvious. In many cases you will need to use the definitions and already proved results to supply the arguments for the intermediate steps.

Proposition 6.1. *Let $\boldsymbol{A}_{m\times p}, \boldsymbol{B}_{p\times n}$ be upper triangular matrices. Then $\boldsymbol{AB}$ is an upper triangular matrix.*

Remark 6.2. To prove this fact we actually will need only a solid grasp of the definitions of upper triangular matrix and matrix multiplication. Nothing else. Therefore the proof here is simply expanding the definitions (in many undergraduate courses this is a very common way to find a proof, especially when you just start a new topic and did not proceed too far yet). Recall that a matrix is called upper triangular if all the elements below the main diagonal are zero. Mathematically, $\boldsymbol{A}$ is upper triangular means that $a_{ij} = 0$ if $i > j$. Recall also that the i, j element of the product of two matrices is the dot product of the i-th row of the first matrix and the j-th column of the second one. Now I need to take the element $(\boldsymbol{AB})_{ij}$ for $i > j$ and show that it is zero. This can be done by counting the number of zero elements in both the row and the column that we multiply. Here is a formal argument.

Proof. Let $\boldsymbol{a} = (a_{i1}, \dots, a_{ip})$ be the i-th row of $\boldsymbol{A}$ and $\boldsymbol{b} = (b_{1j}, \dots, b_{pj})^\top$ be column j of $\boldsymbol{B}$. Since both $\boldsymbol{A}, \boldsymbol{B}$ are upper triangular, I have that row i of $\boldsymbol{A}$ has first $i-1$ zeros and $p-i+1$ potentially non-zero elements; column j of $\boldsymbol{B}$ has j non-zero and $p-j$ zero entries. Since for $i > j$ I have that $i - 1 \geq j$ and hence

$$(\boldsymbol{AB})_{ij} = (\text{zero entries of } \boldsymbol{a}) \cdot (\text{non-zeroes of } \boldsymbol{b}) + (\text{zeros or non-zeroes of } \boldsymbol{a}) \cdot (\text{zero elements of } \boldsymbol{b}) = 0.$$

■

Here is another example from your homework.

Proposition 6.3. *Let $\boldsymbol{A}$ be an invertible matrix. Then $(\boldsymbol{A}^\top)^{-1} = (\boldsymbol{A}^{-1})^\top$.*

Remark 6.4. Here I am given that $\boldsymbol{A}$ is invertible. This means, by definition, that there is matrix $\boldsymbol{A}^{-1}$ such that $\boldsymbol{A}\boldsymbol{A}^{-1} = \boldsymbol{A}^{-1}\boldsymbol{A} = \boldsymbol{I}$. I must show that this fact implies that $\boldsymbol{A}^\top(\boldsymbol{A}^{-1})^\top = (\boldsymbol{A}^{-1})^\top\boldsymbol{A}^\top = \boldsymbol{I}$. The last expression gives me a hint that I must look how the transposition acts on the product. A little experimenting yields a conjecture that $(\boldsymbol{A}\boldsymbol{B})^\top = \boldsymbol{B}^\top\boldsymbol{A}^\top$. If I am able to show this, I immediately see that my claim will be proved. So I recall that $\boldsymbol{A}^\top = [a_{ij}^\top] = [a_{ji}]$ by definition and also recall the definition of a product of two matrices. Now I can carefully write everything down.

Proof. First, $(\boldsymbol{A}\boldsymbol{B})^\top = \boldsymbol{B}^\top\boldsymbol{A}^\top$. Indeed, the left hand side is

$$[\sum_{p=1}^{n} a_{ip}b_{pj}]^\top = [\sum_{p=1}^{n} a_{jp}b_{pi}].$$

The right hand side is

$$\boldsymbol{B}^\top\boldsymbol{A}^\top = [b_{ij}^\top][a_{ij}^\top] = [\sum_{p=1}^{n} b_{ip}^\top a_{pj}^\top] = [\sum_{p=1}^{n} b_{pi}a_{jp}],$$

and hence they are equal.

Now, using $\boldsymbol{A}\boldsymbol{A}^{-1} = \boldsymbol{I}$ and the fact that $\boldsymbol{I}^\top = \boldsymbol{I}$ I get

$$(\boldsymbol{A}\boldsymbol{A}^{-1})^\top = \boldsymbol{I}^\top \implies (\boldsymbol{A}^{-1})^\top\boldsymbol{A}^\top = \boldsymbol{I}.$$

Using $\boldsymbol{A}^{-1}\boldsymbol{A} = \boldsymbol{I}$ I get the second required equality, which finishes the proof. ■

Remark 6.5. Note that I initially worked backward to get an idea how to prove the statement. However, the proof itself is written in the forward direction. Remember, that proofs are always written in the forward direction.

Here is one more important example.

Theorem 6.6. *Let $\boldsymbol{A}$ be a square matrix that has either a left inverse or a right inverse, a matrix $\boldsymbol{B}$ such that either $\boldsymbol{B}\boldsymbol{A} = \boldsymbol{I}$ or $\boldsymbol{A}\boldsymbol{B} = \boldsymbol{I}$. Then $\boldsymbol{A}$ is invertible and $\boldsymbol{B}$ its inverse.*

Proof. Assume that $\boldsymbol{A}\boldsymbol{B} = \boldsymbol{I}$. I can always row reduce matrix $\boldsymbol{A}$ by multiplying with elementary matrices from the left:

$$\boldsymbol{A'}\boldsymbol{B} = \boldsymbol{P}, \quad \boldsymbol{A'} = \boldsymbol{P}\boldsymbol{A} = \boldsymbol{E}_1 \dots \boldsymbol{E}_k\boldsymbol{A}, \quad \boldsymbol{P} = \boldsymbol{E}_1 \dots \boldsymbol{E}_k.$$

Matrix $\boldsymbol{P}$, as a product of invertible matrices, is invertible, and hence cannot have a row of zeros. Therefore the product $\boldsymbol{A'}\boldsymbol{B}$ cannot have a row of zeros, and hence, by the definition of matrix multiplication, $\boldsymbol{A'}$ cannot have a row of zeros. This means that $\boldsymbol{A'}$ is an identity matrix, that is $\boldsymbol{P}$ is the left inverse of $\boldsymbol{A}$. Now, using

$$\boldsymbol{B} = \boldsymbol{P}\boldsymbol{A}\boldsymbol{B} = \boldsymbol{P}(\boldsymbol{A}\boldsymbol{B}) = \boldsymbol{P},$$

I see that my left inverse coincides with the right inverse.

Now assume that $\boldsymbol{B}\boldsymbol{A} = \boldsymbol{I}$. From the previous I get that $\boldsymbol{A}$ is also a left inverse for $\boldsymbol{B}$, and hence $\boldsymbol{A}\boldsymbol{B} = \boldsymbol{I}$, which concludes the proof. ■

6.2.2 Cases

A proof by cases is very similar to the direct proof. The only difference is that we can assume that the whole statement, which we want to prove, can be broken into smaller statements, which we can tackle individually. Here is a problem from one of the homeworks, which I will prove using two cases.

Proposition 6.7. *Let $\boldsymbol{A}$ be a square matrix. Consider the block-triangular matrix*

$$\boldsymbol{B} = \begin{bmatrix} \boldsymbol{I} & * \\ \boldsymbol{0} & \boldsymbol{A} \end{bmatrix},$$

where $*$ denotes anything. Then $\det \boldsymbol{A} = \det \boldsymbol{B}$.

Remark 6.8. First of all I note that using the cofactor expansion formula for the determinant gives the answer immediately, if an expansion with respect to the first column is used. I, however, would like to provide a proof, which relies on the properties of the determinant. It is quite plausible that using the row reduction on $\boldsymbol{B}$ I can transform it to a triangular form and get the desired answer. While this is almost obvious I still need a rigorous way to write this down. To be able to do it I note two things. First, if I take another block triangular matrix,

$$\hat{\boldsymbol{E}} = \begin{bmatrix} \boldsymbol{I} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{E} \end{bmatrix},$$

where $\boldsymbol{E}$ is an elementary matrix, then, using the formula for the product of block matrices I get

$$\hat{\boldsymbol{E}}\boldsymbol{B} = \begin{bmatrix} \boldsymbol{I} & * \\ \boldsymbol{0} & \boldsymbol{E}\boldsymbol{A} \end{bmatrix}.$$

Second, using the fact that $\hat{\boldsymbol{E}}$ is also an elementary matrix if $\boldsymbol{E}$ is, I clearly see that $\det \hat{\boldsymbol{E}} = \det \boldsymbol{E}$. Now I am very close to give a proof of my proposition.

Proof. Consider two cases: $\boldsymbol{A}$ is invertible and not invertible. Assume first that $\boldsymbol{A}$ is invertible. Then it can be represented as a product of elementary matrices $\boldsymbol{A} = \boldsymbol{E}_k \dots \boldsymbol{E}_1$. Since

$$\boldsymbol{B} = \hat{\boldsymbol{E}}_k \dots \hat{\boldsymbol{E}}_1 \begin{bmatrix} \boldsymbol{I} & * \\ \boldsymbol{0} & \boldsymbol{I} \end{bmatrix},$$

where

$$\hat{\boldsymbol{E}}_j = \begin{bmatrix} \boldsymbol{I} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{E}_j \end{bmatrix},$$

$$\det \hat{\boldsymbol{E}}_j = \det \boldsymbol{E}_j,$$

and $\det(\boldsymbol{A}_1 \dots \boldsymbol{A}_k) = \det \boldsymbol{A}_1 \dots \det \boldsymbol{A}_k$, I get that $\det \boldsymbol{B} = \det \boldsymbol{A}$.

Now, if $\boldsymbol{A}$ is not invertible, $\det \boldsymbol{A} = 0$ and $\boldsymbol{A} = \boldsymbol{E}_k \dots \boldsymbol{E}_1 \boldsymbol{A}'$, where $\boldsymbol{A}'$ is in row reduced echelon form and has a row of zeros. Using the same reasonings as above I find that

$$\det \boldsymbol{B} = \det \boldsymbol{E}_k \dots \det \boldsymbol{E}_1 \det \begin{bmatrix} \boldsymbol{I} & * \\ \boldsymbol{0} & \boldsymbol{A'} \end{bmatrix} = 0,$$

since the last matrix is in triangular form with zero on the main diagonal. Hence $\det \boldsymbol{B} = \det \boldsymbol{A}$ as required. ■

6.2.3 Contrapositive

You should recall that the implication $A \implies B$ is equivalent to its contrapositive not $B \implies$ not A. Quite often the contrapositive is easier to prove. This is especially true if the statement to be proved is negative. The negations in contrapositive will take care of this negation, since double negation is equivalent to the statement itself.

Proposition 6.9. *Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be two square matrices. If $\boldsymbol{B}$ is not invertible then $\boldsymbol{AB}$ is not invertible.*

Remark 6.10. Note that the contrapositive has no negations in it: If $\boldsymbol{AB}$ is invertible then $\boldsymbol{B}$ is invertible, which seems to be easier to prove.

Proof. Assume that $\boldsymbol{AB}$ is invertible. This means that there is matrix $\boldsymbol{C}$ such that $\boldsymbol{CAB} = \boldsymbol{I}$. Using the associativity of matrix multiplication it implies that $(\boldsymbol{CA})\boldsymbol{B} = \boldsymbol{I}$, that is, matrix $\boldsymbol{B}$ has a left inverse. Using the earlier result it means that $\boldsymbol{B}$ has the same right inverse, and hence is invertible. ■

6.2.4 If and only if

Recall that every time you are asked to prove something of the form "if and only if" you have to deal with two statements: if part and only if part.

Proposition 6.11. *Let $\boldsymbol{A}$ be a square matrix. Then it is invertible if and only if* $\det \boldsymbol{A} \neq 0$.

Proof. (only if part) $\boldsymbol{A}$ is invertible only if $\det \boldsymbol{A} \neq 0$. In other words, if $\boldsymbol{A}$ is invertible then $\det \boldsymbol{A} \neq 0$. We know that if $\boldsymbol{A}$ is invertible its row reduced echelon form is the identity matrix. Using only the elementary operations of the first and third type I can row reduce $\boldsymbol{A}$ to a diagonal form, with all the diagonal elements not zero. Hence, the determinant is not zero.

(if part) $\boldsymbol{A}$ is invertible if $\det \boldsymbol{A} \neq 0$. In other words, if $\det \boldsymbol{A} \neq 0$ then $\boldsymbol{A}$ is invertible. To prove it, consider contrapositive "if $\boldsymbol{A}$ is not invertible then $\det \boldsymbol{A} = 0$." If $\boldsymbol{A}$ is not invertible then its row reduced echelon form has a row of zeros. This means that using the first and third type elementary row operations I can put $\boldsymbol{A}$ into diagonal form with a zero on the main diagonal. Hence $\det \boldsymbol{A} = 0$. ■

6.2.5 Contradiction

I know that a given sentence is either true or false, and I need to actually show that it is true. I can assume that this statement is false and see what consequences I can deduce from it. If I am able logically obtain that my assumption of something being false implies something clearly wrong, then it implies that my assumption cannot be false, and therefore must be true. This is called a *proof by contradiction.*

Example 6.12. Suppose that $\boldsymbol{A}$ is a 2×1 matrix and $\boldsymbol{B}$ is a 1×2 matrix. Show that $\boldsymbol{C} = \boldsymbol{AB}$ is not invertible. I will prove it by contradiction. So, let

$$\boldsymbol{A} = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}, \quad \boldsymbol{B} = [b_1 \ b_2], \quad \boldsymbol{AB} = \begin{bmatrix} a_1b_1 & a_1b_2 \\ a_2b_1 & a_2b_2 \end{bmatrix}.$$

Assume that my matrix *is* invertible. This means that there is matrix $\boldsymbol{D}$ such that

$$\begin{bmatrix} a_1b_1 & a_1b_2 \\ a_2b_1 & a_2b_2 \end{bmatrix} \begin{bmatrix} d_1 & d_3 \\ d_2 & d_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

This means that I must have

$$a_1b_1d_1 + a_1b_2d_2 = 1,$$
$$a_2b_1d_1 + a_2b_2d_2 = 0.$$

I have that $a_2 \neq 0$ (otherwise I would have a row of zeros and my matrix would not be invertible), hence $b_1d_1 + b_2d_2 = 0$ from the second equation. Plugging this into the first equation yields

$$a_1 0 = 1,$$

which cannot be true for any a_1. Therefore my assumption is false and $\boldsymbol{AB}$ is not invertible.

Here is a nice generalization of the previous example:

Proposition 6.13. *Let $\boldsymbol{A}$ be an $m \times n$ matrix and $\boldsymbol{B}$ be $n \times m$ matrix, $n < m$. Then $\boldsymbol{AB}$ is not invertible.*

I am tempted to use the same strategy, but I will be soon lost into various index notations. Let me show a much simpler direct proof.

Proof. Since $n < m$ I know that the system $\boldsymbol{Bx} = \boldsymbol{0}$ has a nontrivial solution. This implies that $\boldsymbol{A}(\boldsymbol{Bx}) = (\boldsymbol{AB})\boldsymbol{x} = \boldsymbol{0}$ has (the same) nontrivial solution. We know that the conditions $\boldsymbol{Cx} = \boldsymbol{0}$ has only a trivial solution and $\boldsymbol{C}$ is invertible are equivalent. Hence $\boldsymbol{AB}$ is not invertible. ■

6.2.6 Induction

Finally consider a proof by induction. In this case we usually need to check that some property, call it D, holds for all natural numbers $\{0, 1, 2, 3, \ldots\}$ (it is not necessary to start with 0, I can always start with 1 or 2, or 55). Proof by induction consists of two steps: First, we need to check that $D(0)$ holds (or $D(1)$, or $D(2)$, or $D(55)$). Second, *assuming* that $D(n)$ is true we need to show that $D(n+1)$ is true. Clearly, if we are able to show these two facts, this would imply that property D holds for any n from my set. Here is a simple example.

Example 6.14. Find the formula for

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}^n.$$

I perform several computations

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 3 & 6 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}^4 = \begin{bmatrix} 1 & 4 & 10 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}, \ldots$$

It looks like the general answer is

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n & n(n+1)/2 \\ 0 & 1 & n \\ 0 & 0 & 1 \end{bmatrix},$$

but how to prove it? Let me use the induction.

Clearly, my formula holds for $n = 1$ and this is my base step. Now I assume that

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n & n(n+1)/2 \\ 0 & 1 & n \\ 0 & 0 & 1 \end{bmatrix}$$

and will show that this assumption implies that my formula is true for $n + 1$. I have

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}^{n+1} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}^n \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n & n(n+1)/2 \\ 0 & 1 & n \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n+1 & (n+1)(n+2)/2 \\ 0 & 1 & n+1 \\ 0 & 0 & 1 \end{bmatrix},$$

and I am done.

Exercise 1. Prove by induction that there are exactly $n!$ permutations.

Theorem 6.15. *The row reduced echelon form (r.r.e.f.) is unique.*

Proof. I will use the induction on the number of columns.

Consider the base case $n = 1$. If matrix $\boldsymbol{A}$ has just one column and has all zero entries then its r.r.e.f. is the matrix itself. If it has nonzero entries then its r.r.e.f. is $(1, 0, \ldots, 0)^\top$ and hence unique.

Now assume that it is true for $n > 1$, and let $\boldsymbol{A}$ be an $m \times n + 1$ matrix. Denote $\boldsymbol{A'}$ is the $m \times n$ matrix obtained from $\boldsymbol{A}$ by removing the last column. Let $\boldsymbol{B}$ and $\boldsymbol{C}$ be r.r.e.f. of $\boldsymbol{A}$. By the definition of r.r.e.f. $\boldsymbol{B'}$ and $\boldsymbol{C'}$ are in r.r.e.f., and by the induction assumption, $\boldsymbol{A'} = \boldsymbol{B'} = \boldsymbol{C'}$. Now, assume that $\boldsymbol{B} \neq \boldsymbol{C}$. By the reasoning above this can be true only if there is i such that $b_{i,n+1} \neq c_{i,n+1}$. Now, let $\boldsymbol{x} = (x_1, \ldots, x_{n+1})$ be a solution to $\boldsymbol{Bx} = 0$. Since $\boldsymbol{B}$ can be obtained from $\boldsymbol{C}$ by elementary row operations, it implies that $\boldsymbol{Cx} = 0$ as well. Therefore, $(\boldsymbol{B} - \boldsymbol{C})\boldsymbol{x} = 0$. Since $\boldsymbol{B'} = \boldsymbol{C'}$, this implies that $x_{n+1} = 0$, in other words, x_{n+1} cannot be a free variable, and therefore the last column of both $\boldsymbol{B}$ and $\boldsymbol{C}$ must contain pivot 1 and have all the other entries zero, moreover, this 1 must belong to the first zero row of both $\boldsymbol{B'}$ and $\boldsymbol{C'}$ and hence $\boldsymbol{B} = \boldsymbol{C}$. ■