Why and How zk-SNARK Works: Definitive Explanation

Maksym Petkus
maksym@petkus.info

Abstract

Despite the existence of multiple great resources on *zk-SNARK* construction, from original papers[1] to explainers[2], due to the sheer number of moving parts the subject remains a black box for many. While some pieces of the puzzle are given one can not see the full picture without the missing ones.

Hence the focus of this work is to shed light onto the topic with a straightforward and clean approach based on examples and answering many whys along the way so that more individuals can appreciate the state of the art technology, its innovators and ultimately the beauty of math.

Paper's contribution is a simplistic exposition with a sufficient and gradually increasing level of complexity, necessary to understand *zk-SNARK* without any prerequisite knowledge of the subject, cryptography or advanced math. The primary goal is not only to explain how it works but why it works and how it came to be this way.

Keywords: zero-knowledge proof, SNARK, privacy, verifiable computation.

[1] Bit+11; Par+13.
[2] Rei16; But16; But17; Gab17.

Contents

0 Preface

While initially planned as short, the work now spans several dozens of pages, nevertheless it requires very little pre-requisite knowledge, and one can freely skip familiar parts.

Do not worry if you are not acquainted with some of the used math symbols, there will be just a few, and they will be introduced gradually, one at a time.

1 Introduction

Zero-knowledge succinct non-interactive arguments of knowledge (*zk-SNARK*) is the truly ingenious method of proving that something is true without revealing any other information, however, why it is useful in the first place?

Zero-knowledge proofs are advantageous in a myriad of application, including:

- Proving statement on private data:
  - Person A has more than X in his bank account
  - In the last year, a bank did not transact with an entity Y
  - Matching DNA without revealing full DNA
  - One has a credit score higher than Z
- Anonymous authorization:
  - Proving that requester R has right to access web-site's restricted area without revealing its identity (e.g., login, password)
  - Prove that one is from the list of allowed countries/states without revealing from which one exactly
  - Prove that one owns a monthly pass to a subway/metro without revealing card's id
- Anonymous payments:
  - Payment with full detachment from any kind of identity[3]
  - Paying taxes without revealing one's earnings
- Outsourcing computation:
  - Outsource an expensive computation and validate that the result is correct without redoing the execution; it opens up a category of trustless computing
  - Changing a blockchain model from everyone computes the same to one party computes and everyone verifies

[3] Ben+14.

As great as it sounds on the surface the underlying method is a "marvel" of mathematics and cryptography and is being researched for the 4th decade since its introduction in 1985 in the principal work "The Knowledge Complexity of Interactive Proof-systems" [GMR85] with subsequent introduction of the non-interactive proofs [BFM88] which are especially essential in the context of blockchains.

In any *zero-knowledge proof* system, there is a *prover* who wants to convince a *verifier* that some *statement* is true without revealing any other information, e.g., *verifier* learns that the prover has more than X in his bank account but nothing else (i.e., the actual amount is not disclosed). A protocol should satisfy three properties:

- Completeness — if the *statement* is true then a *prover* can convince a *verifier*
- Soundness — a cheating *prover* can not convince a *verifier* of a false *statement*
- Zero-knowledge — the interaction only reveals if a *statement* is true and nothing else

The *zk-SNARK* term itself was introduced in [Bit+11], building on [Gro10] with following Pinocchio protocol [Gen+12; Par+13] making it applicable for general computing.

2 The Medium of a Proof

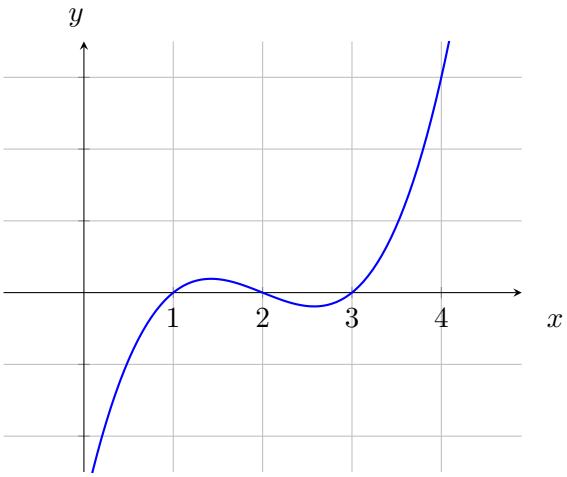
Let us start simple and try to prove something without worrying about the zero-knowledge, non-interactivity, its form, and applicability.

Imagine that we have an array of bits of length 10, and we want to prove to a verifier (e.g., program) that all those bits are set to 1, i.e., we *know* an array such that every element equals to 1.

$$b = [\ \boxed{?},\ \boxed{?},\ \boxed{?},\ \boxed{?},\ \boxed{?},\ \boxed{?},\ \boxed{?},\ \boxed{?},\ \boxed{?},\ \boxed{?}\ ]$$

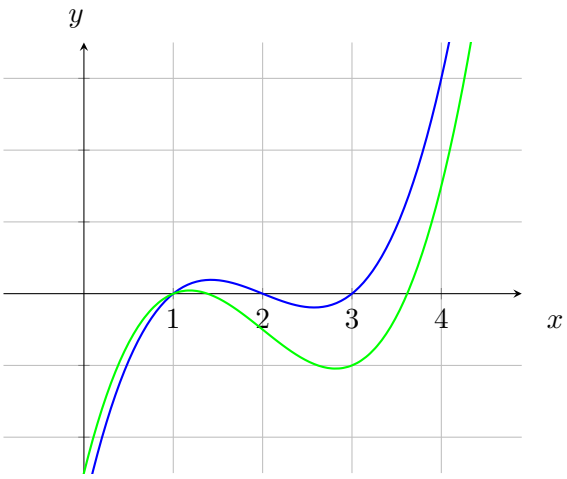
Verifier can only check (i.e., read) one element at a time. In order to verify the statement one can proceed by reading elements in some arbitrary order and checking if it is truly equal to 1 and if so the confidence in that statement after the first check is $\frac{1}{10} = 10\%$, or statement is invalidated altogether if the bit equals to 0. A verifier must proceed to the next round until he reaches sufficient confidence. In some cases, one may trust a prover and require only 50% confidence which means that 5 checks must be executed, in other cases where 95% confidence is needed all cells must be checked. It is clear that the downside of such a proving protocol is that one must do the number of checks proportionate to the number of elements, which is non-practical if we consider arrays of millions of elements.

Let us consider polynomials, which can be visualized as a curve on a graph, shaped by a mathematical equation:



The above curve corresponds to the polynomial: $f(x) = x^3 - 6x^2 + 11x - 6$. The degree of a polynomial is determined by its greatest exponent of x, which in this case is 3.

Polynomials have an advantageous property, namely, if we have two non-equal polynomials of degree at most d, they can intersect at no more than d points. For example, let us modify the original polynomial slightly $x^3 - 6x^2 + \mathbf{10}x - \mathbf{5}$ and visualize it in green:



Such a tiny change produces a dramatically different result. In fact, it is impossible to find two non-equal polynomials, which share a consecutive chunk of a curve[4].

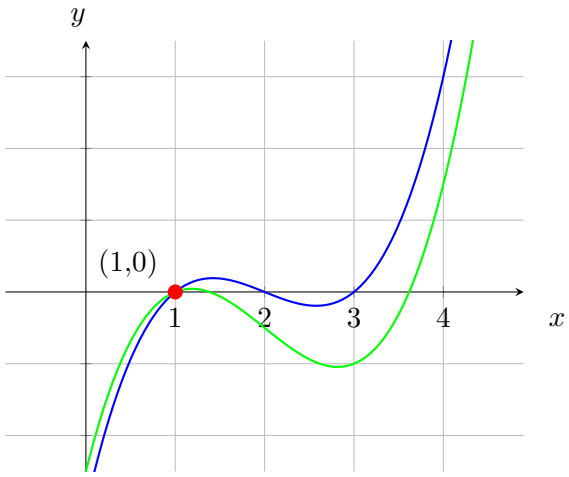
This property flows from the method of finding shared points. If we want to find intersections of two polynomials, we need to equate them. For example, to find where a polynomial crosses an x-axis (i.e., $f(x) = 0$), we equate $x^3 - 6x^2 + 11x - 6 = 0$, and solutions to such an equation will be those shared points: $x = 1$, $x = 2$ and $x = 3$, also you can clearly see that this is true on the previous graph, where the blue curve crosses the x-axis line.

Likewise, we can equate our original and modified version of polynomials to find their intersections.

$$x^3 - 6x^2 + 11x - 6 = x^3 - 6x^2 + \mathbf{10}x - \mathbf{5}$$
$$x - 1 = 0$$

[4]Excluding a single point chunk case

The resulting polynomial is of degree 1 with an obvious solution $x = 1$. Hence only one intersection:



The result of any such equation for arbitrary degree d polynomials is always another polynomial of degree at most d, since there is no multiplication to produce higher degrees. Example: $5x^3 + 7x^2 - x + 2 = 3x^3 - x^2 + 2x - 5$, which simplifies to $2x^3 + 8x^2 - 3x + 7 = 0$. And the Fundamental Theorem of Algebra tells us that a degree d polynomial can have at most d solutions[5], and therefore at most d shared points.

Hence we can conclude that evaluation[6] of any polynomial at an arbitrary point is akin to the representation of its unique identity. Let us evaluate our example polynomials at $x = 10$.

$$x^3 - 6x^2 + 11x - 6 = 504$$
$$x^3 - 6x^2 + 10x - 5 = 495$$

In fact out of all choices of x to evaluate, only at most 3 choices will have equal evaluations in those polynomials and all others will differ.

That is why if a prover claims to *know* some polynomial (no matter how large its degree is) that the verifier also knows, they can follow a simple protocol to verify the statement:

- Verifier chooses a random value for x and evaluates his polynomial locally
- Verifier gives x to the prover and asks to evaluate the polynomial in question
- Prover evaluates his polynomial at x and gives the result to the verifier
- Verifier checks if the local result is equal to the prover's result, and if so then the statement is proven with a high confidence

If we, for example, consider an integer range of x from 1 to 10^{77}, the number of points where evaluations are different is $10^{77} - d$. Henceforth the probability that x accidentally "hits" any of the d shared points is equal to $\frac{d}{10^{77}}$, which is considered negligible.

[5] More on this in section 3.2
[6] More on polynomial evaluation: [Pik13]

Note: the new protocol requires only one round and gives overwhelming confidence (almost 100% *assuming d is sufficiently smaller than the upper bound of the range) in the statement compared to the inefficient bit check protocol.*

That is why polynomials are at the very core of *zk-SNARK*, although it is likely that other proof mediums exist as well.

3 Non-Interactive Zero-Knowledge of a Polynomial

3.1 Proving Knowledge of a Polynomial

We start with a problem of proving the knowledge of a polynomial and make our way to a generic approach. We will discover many other properties of polynomials along the way.

The discussion so far has focused on a weak notion of a proof, where parties have to trust each other because there are no measures yet to enforce the rules of the protocol. For example, the prover is not required to know a polynomial, and he can use any other means available to him to come up with a correct result. Moreover, if the amplitude of the verifier's polynomial evaluations is not large, let us say 10, the verifier can guess a number, and there is a non-negligible probability that it will be accepted. We have to address such weakness of the protocol, but first what does it means to know a polynomial? A polynomial can be expressed in the form (where n is the degree of the polynomial):

$$c_n x^n + ... + c_1 x^1 + c_0 x^0$$

If one stated that he or she knows a polynomial of degree 1 (i.e., $c_1 x^1 + c_0$), that means that what one really *knows* is the coefficients c_0, c_1. Moreover, coefficients can have any value, including 0.

Let us say that the prover claims to know a degree 3 polynomial, such that $x = 1$ and $x = 2$ are two of all possible solutions. One of such valid polynomials is $x^3 - 3x^2 + 2x = 0$. For $x = 1$: $1 - 3 + 2 = 0$. For $x = 2$: $8 - 12 + 4 = 0$.

Let us first look more closely at the anatomy of the solution.

3.2 Factorization

The Fundamental Theorem of Algebra states that any polynomial can be factored into linear polynomials (i.e., a degree 1 polynomials representing a line), as long it is solvable. Consequently, we can represent any valid polynomial as a product of its factors:

$$(x - a_0)(x - a_1)...(x - a_n) = 0$$

Also, if any of these factors is zero then the whole equation is zero, henceforth all the a-s are the only solutions.

In fact, our example can be factored into the following polynomial:

$$x^3 - 3x^2 + 2x = (x - 0)(x - 1)(x - 2)$$

And the solutions are (values of x): $0, 1, 2$, you can check this easily on either form of the polynomial, but the factorized form has all the solutions (also called roots) on the surface.

Getting back to the prover's claim that he knows a polynomial of degree 3 with the roots 1 and 2, this means that his polynomial has the form:

$$(x-1)(x-2)\cdot\ldots$$

In other words $(x-1)$ and $(x-2)$ are the cofactors of the polynomial in question. Hence if the prover wants to prove that indeed his polynomial has those roots without disclosing the polynomial itself, he needs to prove that his polynomial $p(x)$ is the multiplication of those cofactors $t(x) = (x-1)(x-2)$, called *target polynomial*, and some arbitrary polynomial $h(x)$ (equals to $x-0$ in our example), i.e.:

$$p(x) = t(x) \cdot h(x)$$

In other words, there exists some polynomial $h(x)$ which makes $t(x)$ equal to $p(x)$, therefore $p(x)$ contains $t(x)$, consequently $p(x)$ has all roots of $t(x)$, the very thing to be proven.

A natural way to find $h(x)$ is through the division $h(x) = \frac{p(x)}{t(x)}$. If the prover cannot find such $h(x)$ that means that $p(x)$ does not have the necessary cofactors $t(x)$, in which case the polynomials division will have a remainder.

In our example if we divide $p(x) = x^3 - 3x^2 + 2x$ by the $t(x) = (x-1)(x-2) = x^2 - 3x + 2$:

$$\begin{array}{r|l} & x \\ \hline x^2 - 3x + 2 & x^3 - 3x^2 + 2x \\ & -x^3 + 3x^2 - 2x \\ \hline & 0 \end{array}$$

Note: the denominator is to the left, the result is to the top right, and the remainder is to the bottom[7].

We have got the result $h(x) = x$ without remainder.

Note: for simplicity, onwards we will use polynomial's letter variable to denote its evaluation, e.g., $p = p(r)$

Using our polynomial identity check protocol we can compare polynomials $p(x)$ and $t(x) \cdot h(x)$:

- Verifier samples a random value r, calculates $t = t(r)$ (i.e., evaluates) and gives r to the prover
- Prover calculates $h(x) = \frac{p(x)}{t(x)}$ and evaluates $p(r)$ and $h(r)$; the resulting values p, h are provided to the verifier
- Verifier then checks that $p = t \cdot h$, if so those polynomials are equal, meaning that $p(x)$ has $t(x)$ as a cofactor.

[7] Polynomial division explanation with examples is available at [Pik14]

To put this into practice, let us execute this protocol for our example:

$$p(x) = x^3 - 3x^2 + 2x$$
$$t(x) = (x-1)(x-2)$$

- Verifier samples a random value 23, calculates $t = t(23) = (23-1)(23-2) = 462$ and gives 23 to the prover
- Prover calculates $h(x) = \frac{p(x)}{t(x)} = x$, evaluates $p = p(23) = 10626$ and $h = h(23) = 23$ and provides p, h to the verifier
- Verifier then checks that $p = t \cdot h$: $10626 = 462 \cdot 23$, which is true, and therefore the statement is proven

On the contrary, if the prover uses a different $p'(x)$ which does not have the necessary cofactors, for example $p'(x) = 2x^3 - 3x^2 + 2x$, then:

$$\begin{array}{rl} h(x) \quad = & \qquad\qquad\qquad\qquad\qquad\quad 2x+3 \\ & \qquad\qquad\qquad x^2-3x+2\big) \quad 2x^3-3x^2+2x \\ & \qquad\qquad\qquad\qquad\quad -2x^3+6x^2-4x \\ & \qquad\qquad\qquad\qquad\qquad\quad\; 3x^2-2x \\ & \qquad\qquad\qquad\qquad\qquad\quad -3x^2+9x-6 \\ & \qquad\qquad\qquad\qquad\qquad\qquad\quad\; 7x-6 \end{array}$$

We will get $2x+3$ with the remainder $7x-6$, i.e.: $p(x) = t(x) \times (2x+3) + 7x - 6$. This means that the prover will have to divide the remainder by the $t(r)$ in order to evaluate $h(x) = 2x+3+\frac{7x-6}{t(x)}$. Therefore because of the random selection of x by the verifier, there is a low[8] probability that the evaluation of the remainder $7x-6$ will be evenly divisible by the evaluation of $t(x)$, henceforth if verifier will additionally check that p and h must be integers, such proofs will be rejected. However, the check requires the polynomial coefficients to be integers too, creating a significant limitation to the protocol.

That is the reason to introduce cryptographic primitives which make such division impossible, even if the raw evaluations happen to be divisible.

Note: although the author's chief objective is simplicity, including the set of math symbols in use, it would be detrimental for further sections to omit the ubiquitous symbol prime: $'$. Its essential purpose is to signify some transformation or derivation of the original variable or function, e.g., if we want to multiply v by 2 and assign it to a separate variable, we could use prime: $v' = 2 \cdot v$.

Remark 3.1 *Now we can check a polynomial for specific properties without learning the polynomial itself, so this already gives us some form of zero-knowledge and succinctness. Nonetheless, there are multiple issues with this construction:*

[8] But still non-negligible

- *Prover may not know the claimed polynomial $p(x)$ at all. He can calculate evaluation $t = t(r)$, select a random number h and set $p = t \cdot h$, which will be accepted by the verifier as valid, since equation holds.*
- *Because prover knows the random point $x = r$, he can construct any polynomial which has one shared point at r with $t(r) \cdot h(r)$.*
- *In the original statement, prover claims to know a polynomial of a particular degree, in the current protocol there is no enforcement of degree. Hence prover can cheat by using a polynomial of higher degree which also satisfies the cofactors check.*

We will address all of the issues in the following sections.

3.3 Obscure Evaluation

Two first issues of remark 3.1 are possible because values are presented at raw, prover knows r and $t(r)$. It would be ideal if those values would be given as a black box, so one cannot temper with the protocol, but still able to compute operations on those obscure values. Something similar to the hash function, such that when computed it is hard to go back to the original input.

3.3.1 Homomorphic Encryption

That is exactly what homomorphic encryption is designed for. Namely, it allows to encrypt a value and be able to apply arithmetic operations on such encryption. There are multiple ways to achieve homomorphic properties of encryption, and we will briefly introduce a simple one.

The general idea is that we choose a base[9] natural number g (say 5) and to encrypt a value we exponentiate g to the power of that value. For example, if we want to encrypt the number 3:

$$5^3 = 125$$

Where 125 is the encryption of 3. If we want to multiply this encrypted number by 2, we raise it to the exponent of 2:

$$125^2 = 15625 = \left(5^3\right)^2 = 5^{2\times 3} = 5^6$$

We were able to multiply an unknown value by 2 and keep it encrypted. We can also add two encrypted values through multiplication, for example, 3 + 2:

$$5^3 \cdot 5^2 = 5^{3+2} = 5^5 = 3125$$

Similarly, we can subtract encrypted numbers through division, for example, $5 - 3$:

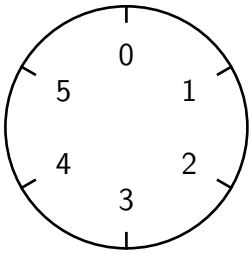
$$\frac{5^5}{5^3} = 5^5 \cdot 5^{-3} = 5^{5-3} = 5^2 = 25$$

[9]There are certain properties that base number needs to have

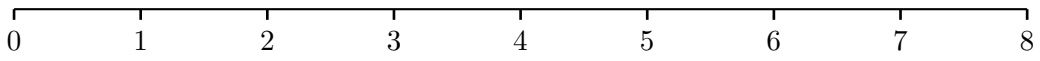
However, since the base 5 is public, it is quite easy to go back to the secret number, dividing encrypted by 5 until the result is 1. The number of steps is the secret number.

3.3.2 Modular Arithmetic

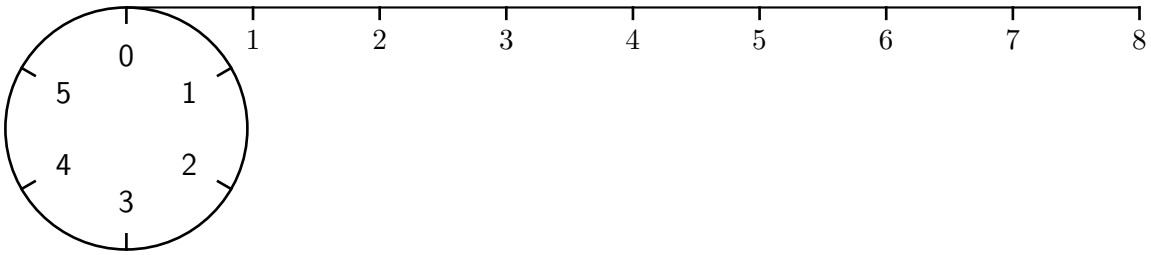
That is where the modular arithmetic comes into play. The idea of modular arithmetic is following: instead of having an infinite set of numbers we declare that we select only first n natural numbers, i.e., $0, 1, \ldots, n-1$, to work with, and if any given integer falls out of this range, we "wrap" it around. For example, let us choose six first numbers. To illustrate this, consider a circle with six ticks of equal units; this is our range[10].



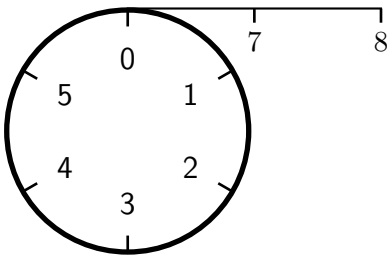
Now let us see where the number eight will land. As an analogy, we can think of it as a rope, the length of which is eight units:



If we attach the rope to the beginning of the circle

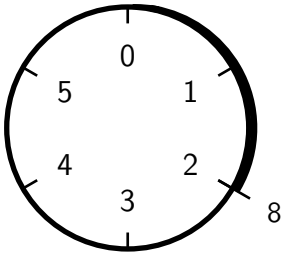


and start wrapping the rope around it, after one rotation we still have a portion of the rope left:



Therefore if we continue the process, the rope will end right at the tick #2.

[10] Usually referred to as finite field



It is the result of the modulo operation. No matter how long the rope is it will always stop at one of the circle's ticks. Therefore the modulo operation will keep it in certain bounds (in this case from 0 to 5). The 15-units rope will stop at 3, i.e., $6 + 6 + 3$ (two full circles with 3-units leftover). The negative numbers work the same way, and the only difference is that we wrap it in the opposite direction, for -8 the result will be 4.

Moreover, we can perform arithmetic operations, and the result will always be in the scope of n numbers. We will use the notation "mod n" for now on to denote the range of numbers. For example:

$$3 \times 5 = 3 \pmod 6$$
$$5 + 2 = 1 \pmod 6$$

Furthermore, the most important property is that the order of operations does not matter, e.g., we can perform all operations first and then apply modulo or apply modulo after every operation. For example $(2 \times 4 - 1) \times 3 = 3 \pmod 6$ is equivalent to:

$$2 \times 4 = 2 \pmod 6$$
$$2 - 1 = 1 \pmod 6$$
$$1 \times 3 = 3 \pmod 6$$

So why on earth is that helpful? It turns out that if we use modulo arithmetic, having a result of operation it is non-trivial to go back to the original numbers because many different combinations will have the same result:

$$5 \times 4 = 2 \pmod 6$$
$$4 \times 2 = 2 \pmod 6$$
$$2 \times 1 = 2 \pmod 6$$
$$\dots$$

Without the modular arithmetic, the size of the result gives a clue to its solution. This piece of information is hidden otherwise, while common arithmetic properties are preserved.

3.3.3 Strong Homomorphic Encryption

If we go back to the homomorphic encryption and use modular arithmetic, for example with modulo 7, we will get:

$$5^1 = 5 \pmod 7$$
$$5^2 = 4 \pmod 7$$
$$5^3 = 6 \pmod 7$$
$$\dots$$

And different exponents will have the same result:

$$5^5 = 3 \pmod 7$$
$$5^{11} = 3 \pmod 7$$
$$5^{17} = 3 \pmod 7$$
$$\dots$$

This is where it gets *hard* to find the exponent. In fact, if modulo is sufficiently large, it becomes infeasible to do so, and a good portion of the modern-day cryptography is based on the "hardness" of this problem.

All the homomorphic properties of the scheme are preserved in the modular realm:

$$\text{encryption}: \quad 5^3 = 6 \pmod 7$$
$$\text{multiplication}: \quad 6^2 = (5^3)^2 = 5^6 = 1 \pmod 7$$
$$\text{addition}: \quad 5^3 \cdot 5^2 = 5^5 = 3 \pmod 7$$

Note: modular division is a bit more complicated and out of the scope.

Let us explicitly state the encryption function: $E(v) = g^v \pmod n$, where v is the value we want to encrypt.

Remark 3.2 *There are limitations to this homomorphic encryption scheme while we can multiply an encrypted value by an unencrypted value, we cannot multiply (and divide) two encrypted values, as well as we cannot exponentiate an encrypted value. While unfortunate from the first impression, these properties will turn out to be the cornerstone of zk-SNARK. The limitations are addressed in section 3.6.1*

3.3.4 Encrypted Polynomial

Armed with such tools, we can now evaluate a polynomial with an encrypted random value of x and modify the *zero-knowledge* protocol accordingly.

Let us see how we can evaluate a polynomial $p(x) = x^3 - 3x^2 + 2x$. As we have established previously to know a polynomial is to know its coefficients, in this case those are: 1, -3, 2. Because homomorphic encryption does not allows to exponentiate an encrypted value, we've must been given encrypted values of powers of x from 1 to 3: $E(x), E(x^2), E(x^3)$, so that we

can evaluate the encrypted polynomial as follows:

$$E\left(x^3\right)^1 \cdot E\left(x^2\right)^{-3} \cdot E\left(x\right)^2 =$$
$$\left(g^{x^3}\right)^1 \cdot \left(g^{x^2}\right)^{-3} \cdot \left(g^{x}\right)^2 =$$
$$g^{1x^3} \cdot g^{-3x^2} \cdot g^{2x} =$$
$$g^{x^3-3x^2+2x}$$

As the result of such operations, we have an encrypted evaluation of our polynomial at some unknown to us x. This is quite a powerful mechanism, and because of the homomorphic property, the encrypted evaluations of the same polynomials are always the same in encrypted space.

We can now update the previous version of the protocol, for a polynomial of degree d:

- Verifier
  - samples a random value s, i.e., secret
  - calculates encryptions of s for all powers i in $0, 1, ..., d$, i.e.: $E(s^i) = g^{s^i}$
  - evaluates unencrypted *target polynomial* with s: $t(s)$
  - encrypted powers of s are provided to the prover: $E(s^0), E(s^1), ..., E(s^d)$
- Prover
  - calculates polynomial $h(x) = \frac{p(x)}{t(x)}$
  - using encrypted powers $g^{s^0}, g^{s^1}, \ldots, g^{s^d}$ and coefficients $c_0, c_1, \ldots, c_n$ evaluates $E\left(p(s)\right) = g^{p(s)} = \left(g^{s^d}\right)^{c_d} \cdots \left(g^{s^1}\right)^{c_1} \cdot \left(g^{s^0}\right)^{c_0}$ and similarly $E\left(h(s)\right) = g^{h(s)}$
  - the resulting g^p and g^h are provided to the verifier
- Verifier
  - The last step for the verifier is to checks that $p = t(s) \cdot h$ in encrypted space: $g^p = \left(g^h\right)^{t(s)} \quad \Rightarrow \quad g^p = g^{t(s)\cdot h}$

Note: because the prover does not know anything about s, it makes it hard to come up with non-legitimate but still matching evaluations.

While in such protocol the prover's agility is limited he still can use any other means to forge a proof without actually using the provided encryptions of powers of s, for example, if the prover claims to have a satisfactory polynomial using only 2 powers s^3 and s^1, that is not possible to verify in the current protocol.

3.4 Restricting a Polynomial

The knowledge of a polynomial is the knowledge of its coefficients $c_0, c_1, \ldots, c_i$ and the way we "assign" those coefficients in the protocol is through exponentiation of the corresponding encrypted powers of the secret value s (i.e., $E\left(s^i\right)^{c_i} = g^{c_i \cdot s^i}$). We do already restrict a prover in the selection of encrypted powers of s, but such restriction is not enforced, e.g., one could use any possible means to find some arbitrary values z_p and z_h which satisfy equation $z_p = (z_h)^{t(s)}$ and provide them to the verifier instead of g^p and g^h. For example, for some random r $z_h = g^r$ and $z_p = \left(g^{t(s)}\right)^r$, where $g^{t(s)}$ can be computed from the provided encrypted powers of s. That is why verifier needs the proof that only supplied encryptions of powers of s were used to calculate g^p and g^h and nothing else.

Let us consider an elementary example of a degree 1 polynomial with one variable and one coefficient $f(x) = c \cdot x$ and correspondingly the encryption of the s is provided $E(s) = g^s$. What we are looking for is to make sure that only encryption of s, i.e., g^s, was homomorphically "multiplied" by some arbitrary coefficient c and nothing else. So the result must always be of the form $(g^s)^c$ for some arbitrary c.

A way to do this is to require to perform the same operation on another *shifted* encrypted value alongside with the original one, acting as an arithmetic analog of "checksum", ensuring that the result is exponentiation of the original value.

This is achieved through the Knowledge-of-Exponent Assumption (or KEA), introduced in [Dam91], more precisely:

- Alice has a value a, that she wants Bob to exponentiate to any power[11], the single requirement is that only this a can be exponentiated and nothing else, to ensure this she:
  - chooses a random α
  - calculates $a' = a^\alpha \pmod n$
  - provides the tuple (a, a') to Bob and asks to perform same arbitrary exponentiation of each value and reply with the resulting tuple (b, b') where the exponent "α-shift" remains the same, i.e., $b^\alpha = b' \pmod n$
- because Bob cannot extract α from the tuple (a, a') other then through a brute-force[12] which is infeasible, it is conjectured that the only way Bob can produce a valid response is through the procedure:
  - chose some value c
  - calculate $b = (a)^c \pmod n$ and $b' = (a')^c \pmod n$
  - reply with (b, b')

[11] Where a is a generator of a finite field group used

[12] The proof is provided in the original paper

- having the response and α, Alice checks the equality:

  $(b)^\alpha = b'$

  $(a^c)^\alpha = (a')^c$

  $a^{c\cdot\alpha} = (a^\alpha)^c$

- conclusions:
  - Bob has applied the same exponent (i.e., c) to both values of the tuple
  - Bob could only use the original Alice's tuple to maintain the α relationship
  - Bob *knows* the applied exponent c, because the only way to produce valid (b, b') is to use the same exponent
  - Alice has not learned c for the same reason Bob cannot learn α[13]

Ultimately such protocol provides a proof to Alice that Bob indeed exponentiated a by some value known to him, and he could not do any other operation, e.g., multiplication, addition, since this would erase the α-shift relationship.

In the homomorphic encryption context, exponentiation is the multiplication of the encrypted value. We can apply the same construction in the case with the simple one-coefficient polynomial $f(x) = c \cdot x$:

- Verifier chooses random s, α and provides evaluation for $x = s$ for power 1 and its "shift": $(g^s, g^{\alpha\cdot s})$
- Prover applies the coefficient c: $((g^s)^c, (g^{\alpha\cdot s})^c) = (g^{c\cdot s}, g^{\alpha\cdot c\cdot s})$
- Verifier checks: $(g^{c\cdot s})^\alpha = g^{\alpha\cdot c\cdot s}$

Such construction *restricts* the prover to use only the encrypted s provided, therefore prover could have assigned coefficient c only to the polynomial provided by the verifier. We can now scale such one-term polynomial[14] approach to a multi-term polynomial because the coefficient assignment of each term is calculated separately and then homomorphically "added" together (this approach was introduced by Jens Groth in [Gro10]). So if the prover is given encrypted exponentiations of s alongside with their *shifted* values he can evaluate original and shifted polynomial, where the same check must hold. In particular, for a degree d polynomial:

- Verifier provides encrypted powers $g^{s^0}, g^{s^1}, \ldots, g^{s^d}$ and their shifts $g^{\alpha s^0}, g^{\alpha s^1}, \ldots, g^{\alpha s^d}$
- Prover:
  - evaluates encrypted polynomial with provided powers of s: $g^{p(s)} = \left(g^{s^0}\right)^{c_0} \cdot \left(g^{s^1}\right)^{c_1} \cdot \ldots \cdot \left(g^{s^d}\right)^{c_d} = g^{c_0 s^0 + c_1 s^1 + \ldots + c_d s^d}$

[13] Although the c is *encrypted* its range of possible values might not be sufficient to preserve *zero-knowledge* property which will be addressed in the section 3.5.

[14] Monomial

- evaluates encrypted "shifted" polynomial with the corresponding α-shifts of the powers of s:
  $g^{\alpha p(s)} = \left(g^{\alpha s^0}\right)^{c_0} \cdot \left(g^{\alpha s^1}\right)^{c_1} \cdot \ldots \cdot \left(g^{\alpha s^d}\right)^{c_d} = g^{c_0 \alpha s^0 + c_1 \alpha s^1 + \ldots + c_d \alpha s^d} = g^{\alpha(c_0 s^0 + c_1 s^1 + \ldots + c_d s^d)}$
- provides the result as $g^p, g^{p'}$ to the verifier

- Verifier checks: $(g^p)^\alpha = g^{p'}$

For our previous example polynomial $p(x) = x^3 - 3x^2 + 2x$ this would be:

- Verifier provides $E(s^3), E(s^2), E(s)$ and their shifts $E(\alpha s^3), E(\alpha s^2), E(\alpha s)$
- Prover evaluates:
  $g^p = g^{p(s)} = \left(g^{s^3}\right)^1 \cdot \left(g^{s^2}\right)^{-3} \cdot \left(g^s\right)^2 = g^{s^3} \cdot g^{-3s^2} \cdot g^{2s} = g^{s^3 - 3s^2 + 2s}$
  $g^{p'} = g^{\alpha p(s)} = \left(g^{\alpha s^3}\right)^1 \cdot \left(g^{\alpha s^2}\right)^{-3} \cdot \left(g^{\alpha s}\right)^2 = g^{\alpha s^3} \cdot g^{-3\alpha s^2} \cdot g^{2\alpha s} = g^{\alpha(s^3 - 3s^2 + 2s)}$
- Verifier checks $(g^p)^\alpha = g^{p'}$:
  $\left(g^{s^3 - 3s^2 + 2s}\right)^\alpha = g^{\alpha(s^3 - 3s^2 + 2s)}$
  $g^{\alpha(s^3 - 3s^2 + 2s)} = g^{\alpha(s^3 - 3s^2 + 2s)}$

Now we can be sure that the prover did not use anything else other than the provided by verifier polynomial, since there is no other way to preserve the α-shift. Also if a verifier would want to ensure exclusion of some power(s) of s in a prover's polynomial, e.g., j, he will not provide encryption g^{s^j} and its *shift* $g^{\alpha s^j}$.

Compared to what we have started with, we now have a robust protocol. However there is still a significant drawback to the *zero-knowledge* property, regardless of encryption: while theoretically polynomial coefficients c_i can have a vast range of values, in reality, it might be quite limited (6 in the previous example), which means that the verifier could brute-force limited range of coefficients combinations until the result is equal to the prover's answer. For instance if we consider the range of 100 values for each coefficient, the degree 2 polynomial would total to 1 million of distinct combinations, which considering brute-force would require less than 1 million iterations. Moreover, the secure protocol should be secure even in cases where there is only one coefficient, and its value is 1.

3.5 Zero-Knowledge

Because verifier can extract knowledge about the unknown polynomial $p(x)$ only from the data sent by the prover, let us consider those provided values (the proof): $g^p, g^{p'}, g^h$. They participate in the following checks:

$$g^p = \left(g^h\right)^{t(s)} \qquad \text{(polynomial } p(x) \text{ has roots of } t(x)\text{)}$$
$$(g^p)^\alpha = g^{p'} \qquad \text{(polynomial of a correct form is used)}$$

The question is how do we alter the proof such that the checks still hold, but no knowledge can be extracted? One answer can be derived from the previous section: we can "shift" those values by some random number δ (delta), e.g., $(g^p)^\delta$. Now, in order to extract the knowledge, one

first needs to find δ which is considered infeasible. Moreover, such randomization is statistically indistinguishable from random.

To maintain relationships let us examine the verifier's checks. One of the prover's values is on each side of the equations. Therefore if we "shift" each of them with the same δ the equations must remain balanced.

Concretely, prover samples a random δ and exponentiates his proof values with it $\left(g^{p(s)}\right)^{\delta}$, $\left(g^{h(s)}\right)^{\delta}$, $\left(g^{\alpha p(s)}\right)^{\delta}$ and provides to the verifier for verification:

$$(g^{p})^{\delta} = \left(\left(g^{h}\right)^{\delta}\right)^{t(s)}$$
$$\left((g^{p})^{\delta}\right)^{\alpha} = \left(g^{p'}\right)^{\delta}$$

After consolidation we can observe that the check still holds:

$$g^{\delta \cdot p} = g^{\delta \cdot t(s) h}$$
$$g^{\delta \cdot \alpha p} = g^{\delta \cdot p'}$$

Note: how easily the zero-knowledge is woven into the construction, this is often referred to as "free" zero-knowledge.

3.6 Non-Interactivity

Till this point, we had an *interactive zero-knowledge* scheme. Why is that the case? Because the proof is only valid for the original verifier, nobody else (other verifiers) can trust the same proof since:

- the verifier could collude with the prover and disclose those secret parameters s, α which allows to fake the proof, as mentioned in remark 3.1
- the verifier can generate fake proofs himself for the same reason
- verifier have to store α and $t(s)$ until all relevant proofs are verified, which allows an extra attack surface with possible leakage of secret parameters

Therefore a separate interaction with every verifier is required in order for a statement (knowledge of polynomial in this case) to be proven.

While interactive proof system has its use cases, for example when a prover wants to convince only a dedicated verifier (called designated verifier[15]) such that the proof cannot be re-used to prove same statement to others, it is quite inefficient when one needs to convince many parties simultaneously (e.g., in distributed systems such as blockchain) or permanently. Prover would be required to stay online at all times and perform the same computation for every verifier.

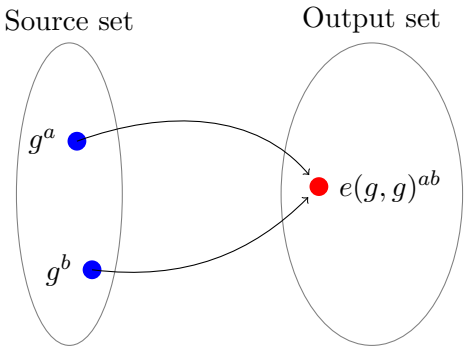
Hence, we need the secret parameters to be reusable, public, trustworthy and infeasible to abuse.

[15] More on designated verifier in [JSI96]

Let us first consider how would we secure the secrets $(t(s), \alpha)$ after they are produced. We can encrypt them the same way verifier encrypts powers of s before sending to the prover. However as mentioned in the remark 3.2, the homomorphic encryption we use does not support the multiplication of two encrypted values, which is necessary for both verification checks to multiply encryptions of $t(s)$ and h as well as p and α. This is where cryptographic pairings fit in.

3.6.1 Multiplication of Encrypted Values

Cryptographic pairings (bilinear map) is a mathematical construction, denoted as a function $e(g^*, g^*)$, which given two encrypted inputs (e.g., g^a, g^b) from one set of numbers allows to map them deterministically to their multiplied representation in a different output set of numbers, i.e., $e(g^a, g^b) = e(g, g)^{ab}$:



.

Because the source and output number sets[16] are different the result of the pairing is not usable as an input for another pairing operation. We can look at the output set (also called "target set") as being from a "different universe." Therefore we cannot multiply the result by another encrypted value and suggested by the name itself we can only multiply two encrypted values at a time.

In some sense, it resembles a hash function, which maps all possible input values to an element in the set of possible output values and it is not trivially reversible.

Note: from first glance, such limitation must only impede a dependent functionality, ironically in the zk-SNARK case it is a paramount property on which security of the scheme holds, see remark 3.3.

A rudimentary (and technically incorrect) mathematical analogy for pairing function $e(g^*, g^*)$ would be to state that there is a way to "swap" each input's base and exponent, such that base g is modified in the process of transformation into exponent, e.g., $g^a \rightarrow a^{\mathbf{g}}$. Both "swapped" inputs are then multiplied together, such that raw a and b values get multiplied under the same exponent, e.g.:

$$e(g^a, g^b) = a^{\mathbf{g}} \cdot b^{\mathbf{g}} = (ab)^{\mathbf{g}}$$

[16] Usually referred to as a group.

Therefore because the base gets altered during the "swap" using the result $(ab)^{\mathbf{g}}$ in another pairing (e.g., $e\left((ab)^{\mathbf{g}}, g^c\right)$) would not produce desired encrypted multiplication abc.

The core properties of pairings can be expressed in the equations:

$$e(g^a, g^b) = e(g^b, g^a) = e(g^{ab}, g^1) = e(g^1, g^{ab}) = e(g^1, g^a)^b = e(g^1, g^1)^{ab} = \dots$$

Technically the result of a pairing is an encrypted product of raw values under a different generator $\mathbf{g}$ of the target set, i.e., $e(g^a, g^b) = \mathbf{g}^{ab}$. Therefore it has properties of the homomorphic encryption, e.g., we can add the encrypted products of multiple pairings together:

$$e(g^a, g^b) \cdot e(g^c, g^d) = \mathbf{g}^{ab} \cdot \mathbf{g}^{cd} = \mathbf{g}^{ab+cd} = e(g, g)^{ab+cd}$$

Note: cryptographic pairing is leveraging elliptic curves to achieve these properties, therefore from now on notation g^n will represent a generator point on a curve added to itself n times instead of a multiplicative group generator which we have used in previous sections.

The survey [DBS04] provides a starting point for exploration of the cryptographic pairings.

3.6.2 Trusted Party Setup

Having cryptographic pairings, we are now ready to set up secure public and reusable parameters. Let us assume that we trust a single honest party to generate secrets s and α. As soon as α and all necessary powers of s with corresponding α-shifts are encrypted ($g^{\alpha}, g^{s^i}, g^{\alpha s^i}$ for i in $0, 1, \dots, d$), the raw values must be deleted.

These parameters are usually referred to as *common reference string* or CRS. After CRS is generated any prover and any verifier can use it in order to conduct non-interactive zero-knowledge proof protocol. While non-crucial, the optimized version of CRS will include encrypted evaluation of the *target polynomial* $g^{t(s)}$.

Moreover CRS is divided into two groups (for i in $0, 1, \dots, d$):

- Proving key[17]: $(g^{s^i}, g^{\alpha s^i})$
- Verification key: $(g^{t(s)}, g^{\alpha})$

Being able to multiply encrypted values the verifier can check the polynomials in the last step of the protocol:

- Having verification key verifier processes received encrypted polynomial evaluations $g^p, g^h, g^{p'}$ from the prover:
  - checks that $p = t \cdot h$ in encrypted space:

    $e\left(g^p, g^1\right) = e\left(g^t, g^h\right)$ which is equivalent to $e\left(g, g\right)^p = e\left(g, g\right)^{t \cdot h}$
  - checks polynomial restriction:
    $e\left(g^p, g^{\alpha}\right) = e\left(g^{p'}, g\right)$

[17] Also called *evaluation key*

3.6.3 Trusting One out of Many

While the trusted setup is efficient, it is not effective since multiple users of CRS will have to trust that one deleted α and s, since currently there is no way to prove that[18]. Hence it is necessary to minimize or eliminate that trust. Otherwise, a dishonest party would be able to produce fake proofs without being detected.

One way to achieve that is by generating a *composite* CRS by multiple parties employing mathematical tools introduced in previous sections, such that neither of those parties knows the secret. Here is an approach, let us consider three participants Alice, Bob and Carol with corresponding indices A, B and C, for i in $1, 2, \ldots, d$:

- Alice samples her random s_A and α_A and publishes her CRS:
  $\left(g^{s_A^i}, g^{\alpha_A}, g^{\alpha_A s_A^i}\right)$
- Bob samples his s_B and α_B and augments Alice's encrypted CRS through homomorphic multiplication:
  $\left(\left(g^{s_A^i}\right)^{s_B^i}, (g^{\alpha_A})^{\alpha_B}, \left(g^{\alpha_A s_A^i}\right)^{\alpha_B s_B^i}\right) = \left(g^{(s_A s_B)^i}, g^{\alpha_A \alpha_B}, g^{\alpha_A \alpha_B (s_A s_B)^i}\right)$
  and publishes the resulting two-party Alice-Bob CRS:
  $\left(g^{s_{\mathsf{AB}}^i}, g^{\alpha_{\mathsf{AB}}}, g^{\alpha_{\mathsf{AB}}\, s_{\mathsf{AB}}^i}\right)$
- So does Carol with her s_C and α_C:
  $\left(\left(g^{s_{\mathsf{AB}}^i}\right)^{s_C^i}, \left(g^{\alpha_{\mathsf{AB}}}\right)^{\alpha_C}, \left(g^{\alpha_{\mathsf{AB}}\, s_{\mathsf{AB}}^i}\right)^{\alpha_C s_C^i}\right) = \left(g^{(s_A s_B s_C)^i}, g^{\alpha_A \alpha_B \alpha_C}, g^{\alpha_A \alpha_B \alpha_C (s_A s_B s_C)^i}\right)$
  and publishes Alice-Bob-Carol CRS:
  $\left(g^{s_{\mathsf{ABC}}^i}, g^{\alpha_{\mathsf{ABC}}}, g^{\alpha_{\mathsf{ABC}}\, s_{\mathsf{ABC}}^i}\right)$

As the result of such protocol, we have composite $s^i = s_A^i s_B^i s_C^i$, and $\alpha = \alpha_A \alpha_B \alpha_C$ and no participant learns secret parameters of other participants unless they are colluding. In fact, in order to learn s and α, one must collude with every other participant. Therefore even if one out of all is honest, it will be infeasible to produce fake proofs.

Note: this process can be repeated for as many participants as necessary.

The question one might have is how to verify that participant have been consistent with every value of CRS, because an adversary can sample multiple different $s_1, s_2, \ldots$ and $\alpha_1, \alpha_2, \ldots$, and use those randomly for different powers of s (or provide random numbers as an augmented common reference string), rendering CRS invalid and unusable.

Luckily, because we can multiply encrypted values using pairings, we are able to perform consistency check, starting with the first parameter and ensuring that every next is derived from it. Every published CRS by participants can be checked as follows:

- We take power 1 of s as canonical value and check every other power for consistency with it:

[18] Proof of ignorance is an area of active research [DK18]

$e\left(g^{s^i}, g\right) = e\left(g^{s^1}, g^{s^{i-1}}\right)\Big|_{i\in\{2,\ldots,d\}}$
for example:

- Power 2: $e\left(g^{s^2}, g\right) = e\left(g^{s^1}, g^{s^1}\right) \Rightarrow e(g,g)^{s^2} = e(g,g)^{s^{1+1}}$
- Power 3: $e\left(g^{s^3}, g\right) = e\left(g^{s^1}, g^{s^2}\right) \Rightarrow e(g,g)^{s^3} = e(g,g)^{s^{1+2}}$, etc.

- We now check if the α-shift of values in the previous step is correct:
  $e\left(g^{s^i}, g^{\alpha}\right) = e\left(g^{\alpha s^i}, g\right)\Big|_{i\in[d]}$
  for example:
  - Power 3: $e\left(g^{s^3}, g^{\alpha}\right) = e\left(g^{\alpha s^3}, g\right) \Rightarrow e(g,g)^{s^3\cdot\alpha} = e(g,g)^{\alpha s^3}$, etc.

  where $i \in \{2,\ldots,d\}$ is a shortened form of "i is in $2,3,\ldots,d$" and $[d]$ is a shortened form of $1,2,\ldots,d$, which is the more convenient notation for the next sections

Notice that while we verify that every participant is consistent with their secret parameters, the requirement to use previously published CRS is not enforced for every next party (Bob and Carol in our example). Hence if an adversary is the last in the chain he can ignore the previous CRS and construct valid parameters from scratch, as if he was the first in the chain, therefore being the only one who knows secret s and α.

We can address this by additionally requiring every participant except the first one to encrypt and publish his secret parameters, for example, Bob also publishes:

$$\left(g^{s_B^i}, g^{\alpha_B}, g^{\alpha_B s_B^i}\right)\Big|_{i\in[d]}$$

This allows to validate that Bob's CRS is a proper multiple of Alice's parameters, for i in $1,2,\ldots,d$:

- $e\left(g^{s_{\mathsf{AB}}^i}, g\right) = e\left(g^{s_A^i}, g^{s_B^i}\right)$
- $e\left(g^{\alpha_{\mathsf{AB}}}, g\right) = e\left(g^{\alpha_A}, g^{\alpha_B}\right)$
- $e\left(g^{\alpha_{\mathsf{AB}}\, s_{\mathsf{AB}}^i}, g\right) = e\left(g^{\alpha_A s_A^i}, g^{\alpha_B s_B^i}\right)$

Similarly Carol will have to prove that her CRS is a proper multiple of Alice-Bob's CRS.

This is a robust CRS setup scheme which does not rely entirely on any single party. In fact, it is sufficient if only one party is honest and deletes and never shares its secret parameters, even if all other parties have colluded. So the more there are unrelated participants in CRS setup[19] the faintest the possibility of fake proofs, the probability becomes negligible if competing parties are participating. The scheme allows involving other untrusted parties who are in doubt about the legibility of the setup because verification step ensures they are not sabotaging (which also includes usage of weak α and s) the final common reference string.

[19] Sometimes called ceremony [Wil16]

3.7 Succinct Non-Interactive Argument of Knowledge of Polynomial

We are now ready to consolidate the evolved *zk-SNARKOP* protocol. Being formal, for brevity, we will be using curly brackets to denote a set of elements populated by the subscript next to it, for example $\left\{s^i\right\}_{i\in[d]}$ denotes a set $s^1, s^2, \ldots, s^d$.

Having agreed upon *target polynomial* $t(x)$ and degree d of the prover's polynomial:

- Setup
  - sample random values s, α
  - calculate encryptions g^α and $\left\{g^{s^i}\right\}_{i\in[d]}, \left\{g^{\alpha s^i}\right\}_{i\in\{0,\ldots,d\}}$
  - proving key: $\left(\left\{g^{s^i}\right\}_{i\in[d]}, \left\{g^{\alpha s^i}\right\}_{i\in\{0,\ldots,d\}}\right)$
  - verification key: $\left(g^\alpha, g^{t(s)}\right)$
- Proving
  - assign coefficients $\{c_i\}_{i\in\{0,\ldots,d\}}$ (i.e., knowledge), $p(x) = c_d x^d + \cdots + c_1 x^1 + c_0 x^0$
  - calculate polynomial $h(x) = \frac{p(x)}{t(x)}$
  - evaluate encrypted polynomials $g^{p(s)}$ and $g^{h(s)}$ using $\left\{g^{s^i}\right\}_{i\in[d]}$
  - evaluate encrypted shifted polynomial $g^{\alpha p(s)}$ using $\left\{g^{\alpha s^i}\right\}_{i\in\{0,\ldots,d\}}$
  - sample random δ
  - set the randomized proof $\pi = \left(g^{\delta p(s)}, g^{\delta h(s)}, g^{\delta\alpha p(s)}\right)$
- Verification
  - parse proof π as $\left(g^p, g^h, g^{p'}\right)$
  - check polynomial restriction $\quad e\left(g^{p'}, g\right) = e\left(g^p, g^\alpha\right)$
  - check polynomial cofactors $\; e\left(g^p, g\right) = e\left(g^{t(s)}, g^h\right)$

Remark 3.3 *If it would be possible to reuse result of pairing for another multiplication such protocol would be completely insecure because the prover can assign* $g^{p'} = e\left(g^p, g^\alpha\right)$ *which would then pass the "polynomial restriction" check:*

$$e\left(e\left(g^p, g^\alpha\right), g\right) = e\left(g^p, g^\alpha\right)$$

3.7.1 Conclusions

We came to the zero-knowledge succinct non-interactive arguments of knowledge protocol for the knowledge of a polynomial problem, which is a niche use-case. While one can claim that a prover can easily construct such polynomial $p(x)$ just by multiplying $t(x)$ by another bounded polynomial to make it pass the test, the construction is still useful.

Verifier knows that the prover has a valid polynomial but not which particular one. We could add additional proofs of other properties of the polynomial such as: divides by multiple polynomials, is a square of a polynomial. There could be a service which accepts, stores and rewards all the attested polynomials, or there is a need in an encrypted evaluation of unknown polynomials of a necessary form. However, having universal scheme would allow for a myriad of applications.

4 General-Purpose Zero-Knowledge Proofs

We have paved our way with a simple yet sufficient example involving most of the *zk-SNARK* machinery, and it is now possible to advance the scheme to execute zero-knowledge programs.

4.1 Computation

Let us consider a simple program in pseudocode:

Algorithm 1 Operation depends on an input

```
function calc(w, a, b)
    if w then
        return a × b
    else
        return a + b
    end if
end function
```

From a high-level view, it is quite unrelated to polynomials, which we have the protocol for. Therefore we need to find a way to convert a program into the polynomial form. The first step then is to translate the program into the language of math, which is relatively easy, the same statement can be expressed as following (assuming w is either 0 or 1):

$$f(w, a, b) = w(a \times b) + (1 - w)(a + b)$$

Executing calc(1, 4, 2) and evaluating $f(1, 4, 2)$ will yield the same result: 8. Conversely calc(0, 4, 2) and $f(0, 4, 2)$ would both be resolved to 6. We can express any kind of finite program in such a way.

What we need to prove then (in this example), is that for the input $(1, 4, 2)$ of expression $f(w, a, b)$ the output is 8, in other words, we check the equality:

$$w(a \times b) + (1 - w)(a + b) = 8$$

4.2 Single Operation

We now have a general computation expressed in a mathematical language, but we still need to translate it into the realm of polynomials. Let us have a closer look at what computation is

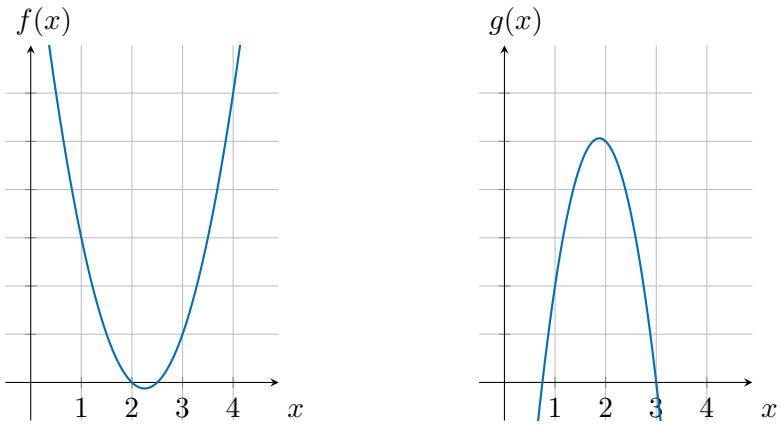
in a nutshell. Any computation at it is core consists of elemental operations of the form:

left operand **operator** right operand = output

Two operands (i.e., values) are being operated upon by an operator (e.g., $+, -, \times, \div$). For example for operands 2 and 3 and operator "multiplication" these will resolve to $2 \times 3 = 6$. Because any complex computation (or a program) is just a series of operations, firstly we need to find out how single such operation can be represented by a polynomial.

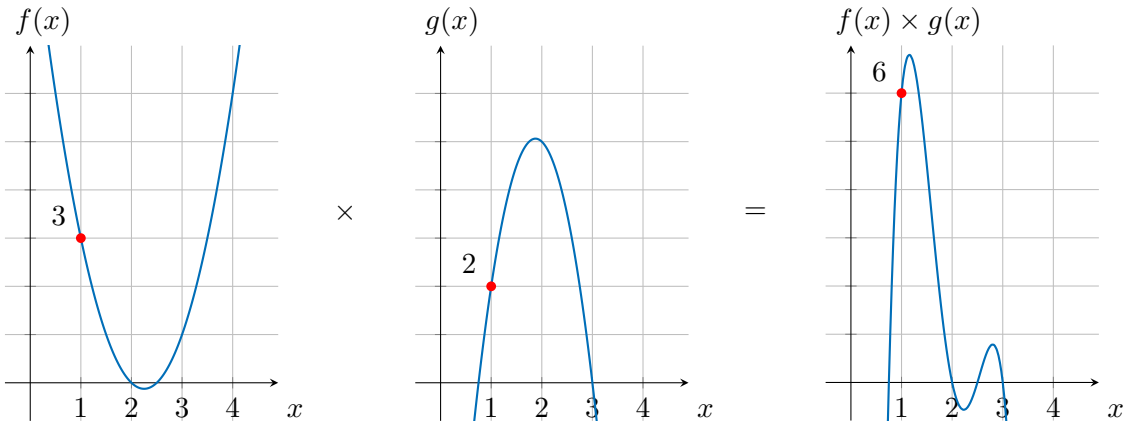
4.2.1 Arithmetic Properties of Polynomials

Let us see how polynomials are related to arithmetic operations. If you take two polynomials $f(x)$ and $g(x)$ and try, for example, to multiply them $h(x) = f(x) \times g(x)$, the result of evaluation of $h(x)$ at any $x = r$ will be the multiplication of results of evaluations of $f(r)$ and $g(r)$. Let us consider two following polynomials: $f(x) = 2x^2 - 9x + 10$ and $g(x) = -4x^2 + 15x - 9$. Visualized in the form of graph:



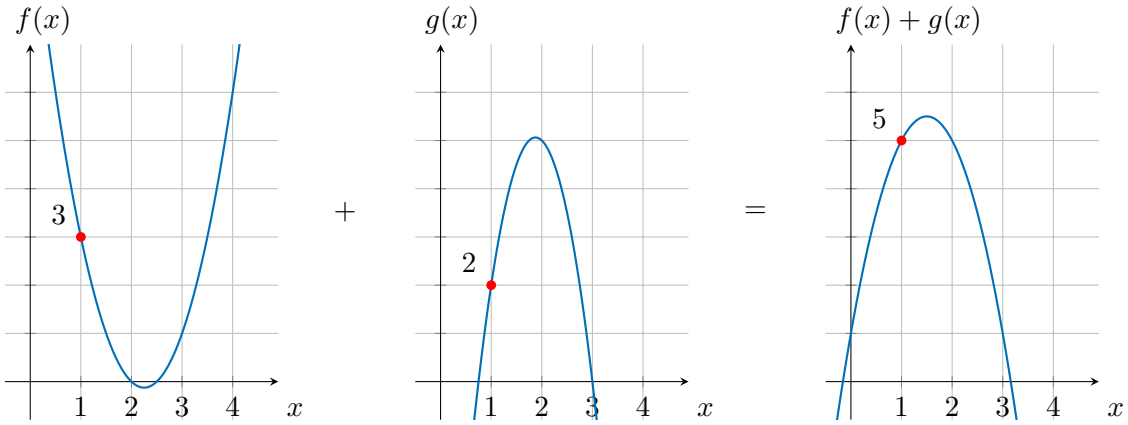
For $x = 1$ these will evaluate to: $f(1) = 2 - 9 + 10 = 3$, $g(1) = -4 + 15 - 9 = 2$.

Let us multiply the polynomials: $h(x) = f(x) \times g(x) = -8x^4 + 66x^3 - 193x^2 + 231x - 90$. Visually multiplication can be seen as:



If we examine evaluations at $x = 1$ on the resulting polynomial $f(x) \times g(x)$ we will get: $h(1) = -8 + 66 - 193 + 231 - 90 = 6$, hence the values at $x = 1$ of $f(x)$ and $g(x)$ has multiplied, and respectively at every other x.

Likewise if we add $f(x)$ and $g(x)$ we will get $-2x^2+6x+1$ which evaluates to 5 at $x=1$.



Note: evaluations at other x-s were also added together, e.g., examine $x=2, x=3$.

If we can represent operand values as polynomials (and we indeed can as outlined) then through the arithmetic properties, we will be able to get the result of an operation imposed by an operand.

4.3 Enforcing Operation

If a prover claims to have the result of multiplication of two numbers how does verifier checks that? To prove the correctness of a single operation, we must enforce the correctness of the output (result) for the operands provided. If we look again at the form of operation:

left operand **operator** right operand = output

The same can be represented as an *operation polynomial*:

$$l(x) \textbf{ operator } r(x) = o(x)$$

where for some chosen a:

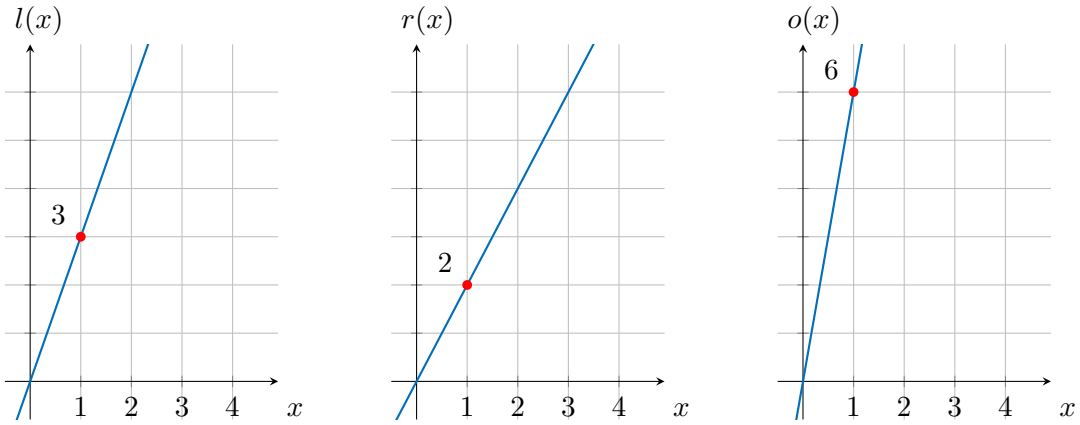
- $l(x)$ - at a represents (evaluates to) the value of the left operand
- $r(x)$ - at a represents the value of the right operand
- $o(x)$ - at a represents the result (output) of the operation

Therefore if the operands and the output are represented correctly for the operation by those polynomials, then the evaluation of $l(a)$ **operator** $r(a) = o(a)$ should hold. And moving *output polynomial* $o(x)$ to the left side of the equation $l(a)$ **operator** $r(a) - o(a) = 0$ is surfacing the fact that the *operation polynomial* $l(x)$ **operator** $r(x) - o(x) = 0$ has to evaluate to 0 at a, if the value represented by the *output polynomial* $o(x)$ is the correct result produced by the **operator** on the values represented by *operand polynomials* $l(x)$ and $r(x)$. Henceforth *operation polynomial* must have the root a if it is valid, and consequently, it must contain cofactor $(x-a)$ as we have established previously (see factorization, section 3.2), which is the *target polynomial* we prove against, i.e., $t(x) = x - a$.

For example, let us consider operation:

$$3 \times 2 = 6$$

It can be represented by simple polynomials $l(x) = 3x$, $r(x) = 2x$, $o(x) = 6x$, which evaluate to the corresponding values for $a = 1$, i.e., $l(1) = 3;\ r(1) = 2;\ o(1) = 6$.

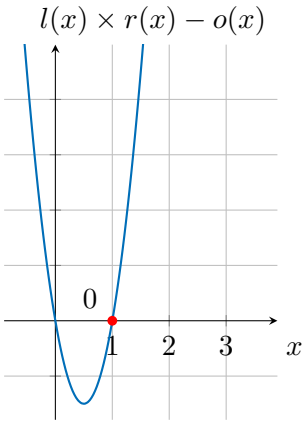


Note: The value of a can be arbitrary.

The operation polynomial then will be:

$$l(x) \times r(x) = o(x)$$
$$3x \times 2x = 6x$$
$$6x^2 - 6x = 0$$

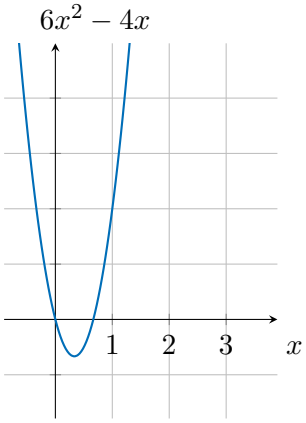
Which is visualised as:



It is noticeable that the operation polynomial has $(x - 1)$ as a co-factor:

$$6x^2 - 6x = 6x(x - 1)$$

Therefore if the prover provides such polynomials $l(x), r(x), o(x)$ instead of former $p(x)$ then the verifier will accept it as valid, since it is divisible by $t(x)$. On the contrary if the prover tries to cheat and substitutes output value with 4, e.g., $o(x) = 4x$, then the *operation polynomial* will be $6x^2 - 4x = 0$:



Which is not have a solution $x = 1$, henceforth $l(x) \times r(x) - o(x)$ is not divisible by $t(x)$ without remainder:

$$h(x) = \begin{array}{r|l} & 6x + 2 \\ \hline x - 1 & 6x^2 - 4x \\ & -6x^2 + 6x \\ \hline & 2x \\ & -2x + 2 \\ \hline & 2 \end{array} \quad \Rightarrow \quad h(x) = 6x + 2 + \frac{2}{x-1}$$

Hence such *inconsistent operation* will not be accepted by the verifier[20].

4.4 Proof of Operation

Let us modify our latest protocol to support a single multiplication operation proof. Recall that previously we had proof of knowledge of polynomial $p(x)$, but now we deal with three $l(x), r(x), o(x)$. While we could define $p(x) = l(x) \times r(x) - o(x)$ there are two counterargument. Firstly, in our protocol, the multiplication of encrypted values (i.e., $l(s) \times r(s)$) is not possible in the proving stage, since pairings can only be used once and it is required for the "polynomial restriction" check. Secondly, this would leave an opportunity for the prover to modify the structure of polynomial at will but still maintain a valid cofactor $t(x)$, for example $p(x) = l(x)$ or $p(x) = l(x) - r(x)$ or even $p(x) = l(x) \times r(x) + o(x)$, as long as $p(x)$ has root a. Such modification effectively means that the proof is about a different statement, which is certainly not desired.

That is why the evaluations of polynomials $l(s)$, $r(s)$, $o(s)$ have to be provided separately by the prover. This means that the *knowledge of polynomial* must be adjusted. In essence what a verifier needs to check in encrypted space is that $l(s) \times r(s) - o(s) = t(s)h(s)$. While a verifier can perform multiplication using cryptographic pairings, the subtraction $(-o(x))$ is an expensive operation[21] that is why we move $o(x)$ to the right side of the equation: $l(x)r(x) = t(x)h(x) + o(x)$.

[20] As described in section 3.2

[21] Would require to find inverse of $g^{o(s)}$

In encrypted space verifier's check translates to:

$$e\left(g^{l(s)}, g^{r(s)}\right) = e\left(g^{t(s)}, g^{h(s)}\right) \cdot e\left(g^{o(s)}, g\right)$$
$$e(g,g)^{l(s)r(s)} = e(g,g)^{t(s)h(s)} \cdot e(g,g)^{o(s)}$$
$$e(g,g)^{l(s)r(s)} = e(g,g)^{t(s)h(s)+o(s)}$$

Note: recall that the result of cryptographic pairings supports encrypted addition through multiplication, see section 3.6.1.

While the *setup* stage stays unchanged, here is the updated protocol:

- Proving
  - assign corresponding coefficients to the $l(x)$, $r(x)$, $o(x)$
  - calculate polynomial $h(x) = \frac{l(x) \times r(x) - o(x)}{t(x)}$
  - evaluate encrypted polynomials $g^{l(s)}$, $g^{r(s)}$, $g^{o(s)}$ and $g^{h(s)}$ using $\left\{g^{s^i}\right\}_{i \in [d]}$
  - evaluate encrypted shifted polynomials $g^{\alpha l(s)}$, $g^{\alpha r(s)}$, $g^{\alpha o(s)}$ using $\left\{g^{\alpha s^i}\right\}_{i \in \{0,\ldots,d\}}$
  - set proof $\pi = \left(g^{l(s)}, g^{r(s)}, g^{o(s)}, g^{h(s)}, g^{\alpha l(s)}, g^{\alpha r(s)}, g^{\alpha o(s)}\right)$
- Verification
  - parse proof π as $\left(g^{l}, g^{r}, g^{o}, g^{h}, g^{l'}, g^{r'}, g^{o'}\right)$
  - polynomial restrictions check:
    $e(g^{l'}, g) = e(g^{l}, g^{\alpha})$
    $e(g^{r'}, g) = e(g^{r}, g^{\alpha})$
    $e(g^{o'}, g) = e(g^{o}, g^{\alpha})$
  - valid operation check: $e\left(g^{l}, g^{r}\right) = e\left(g^{t(s)}, g^{h}\right) \cdot e\left(g^{o}, g\right)$

Such protocol allows to prove that the result of multiplication of two values is computed correctly.

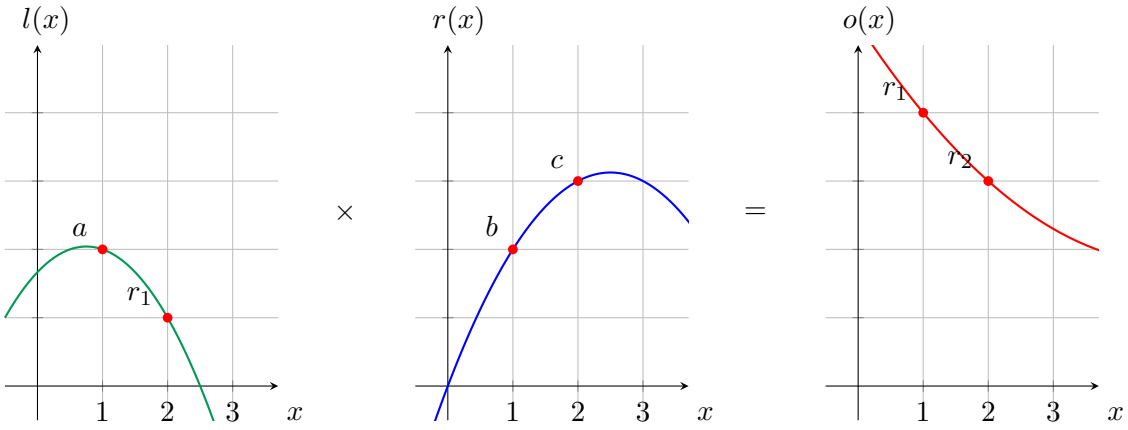
One might notice that in the updated protocol we had to let go of the *zero-knowledge* component. The reason for this is to make the transition simpler. We will get back to it in a later section.

4.5 Multiple Operations

We can prove a single operation, but how do we scale to prove multiple operations (which is our ultimate goal)? Let us try to add just one another operation. Consider the need to compute the product: $a \times b \times c$. In the elemental operation model this would mean two operations:

$$a \times b = r_1$$
$$r_1 \times c = r_2$$

As discussed previously we can represent one such operation by making operand polynomials evaluate to a corresponding value at some arbitrary x, for example 1. Having this the properties of polynomials does not restrict us in representing other values at different x, for example 2, e.g.:



Such independence allows us to *execute* two operations at once without "mixing" them together, i.e., no interfering. The result of such polynomial arithmetic will be:

Where it is visible that the operation polynomial has roots $x = 1$ and $x = 2$. Therefore both operations are *executed* correctly.

Let us have a look at example of 3 multiplications $2 \times 1 \times 3 \times 2$, which can be executed as follows:

$$\begin{aligned} 2 \times 1 &= 2 \\ 2 \times 3 &= 6 \\ 6 \times 2 &= 12 \end{aligned}$$

We need to represent those as operand polynomials, such that for operations represented by $x \in \{1, 2, 3\}$ the $l(x)$ pass correspondingly through $2, 2$ and 6, i.e., through points $(1, 2), (2, 2), (3, 6)$, and similarly $r(x) \ni (1, 1), (2, 3), (3, 2)$ and $o(x) \ni (1, 2), (2, 6), (3, 12)$.

However, how do we find such polynomials which passes through those points? For any case where we have more than one point, a particular mathematical method has to be used.

4.5.1 Polynomial Interpolation

In order to construct *operand* and *output polynomials* we need a method which given a set of points produces a *curved* polynomial in such a way that it passes through all those points, it is called *interpolation* There are different ways available:

- Set of equations with unknowns
- Newton polynomial
- Neville's algorithm
- Lagrange polynomials
- Fast Fourier transform

Let us use the former for example. The idea of such method is that there exists a unique polynomial of degree at most n with yet *unknown coefficients* which pass through given $n+1$ points such that for each point $\{(x_i, y_i)\}_{i\in[n+1]}$ the polynomial evaluated at x_i should be equal to y_i. In our case for three points it will be polynomial of degree 2 of the form:

$$ax^2 + bx + c = y$$

Let us *equalize* the evaluated polynomial for each point of the *left operand polynomial* (green) and solve the system of equations by expressing each coefficient in terms of others:

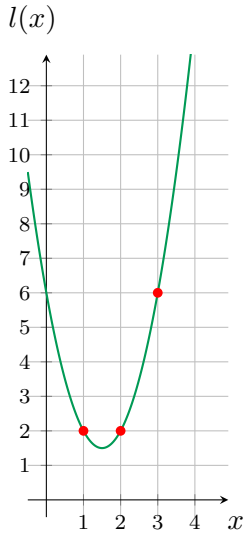
$$\begin{cases} l(1) = 2 \\ l(2) = 2 \\ l(3) = 6 \end{cases} \Rightarrow \begin{cases} a(1)^2 + b\cdot 1 + c = 2 \\ a(2)^2 + b\cdot 2 + c = 2 \\ a(3)^2 + b\cdot 3 + c = 6 \end{cases} \Rightarrow \begin{cases} a + b + c = 2 \\ 4a + 2b + c = 2 \\ 9a + 3b + c = 6 \end{cases} \Rightarrow \begin{cases} a = 2 - b - c \\ 2b = 2 - 4(2 - b - c) - c \\ c = 6 - 9(2 - b - c) - 3b \end{cases}$$

$$\Rightarrow \begin{cases} a = 2 - b - c \\ b = \frac{6-3c}{2} \\ c = -12 + 6b + 9c \end{cases} \Rightarrow \begin{cases} a = 2 - b - c \\ b = \frac{6-3c}{2} \\ c = -12 + 6(\frac{6-3c}{2}) + 9c \end{cases} \Rightarrow \begin{cases} a = 2 \\ b = -6 \\ c = 6 \end{cases}$$

Therefore the *left operand polynomial* is:

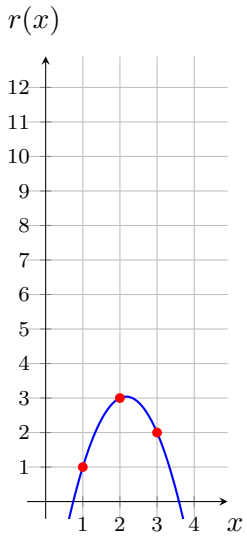
$$l(x) = 2x^2 - 6x + 6$$

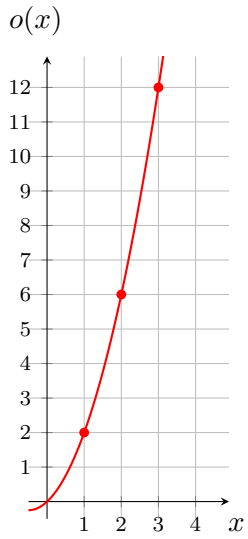
Which corresponds to the following graph:



We can find $r(x)$ and $o(x)$ in the same way:

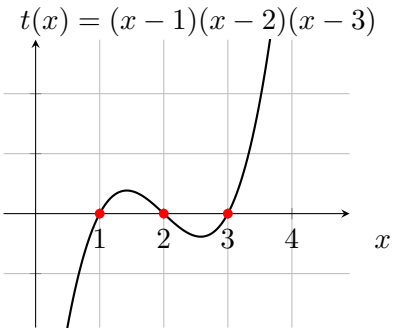
$$r(x) = \frac{-3x^2 + 13x - 8}{2}; \quad o(x) = x^2 + x$$



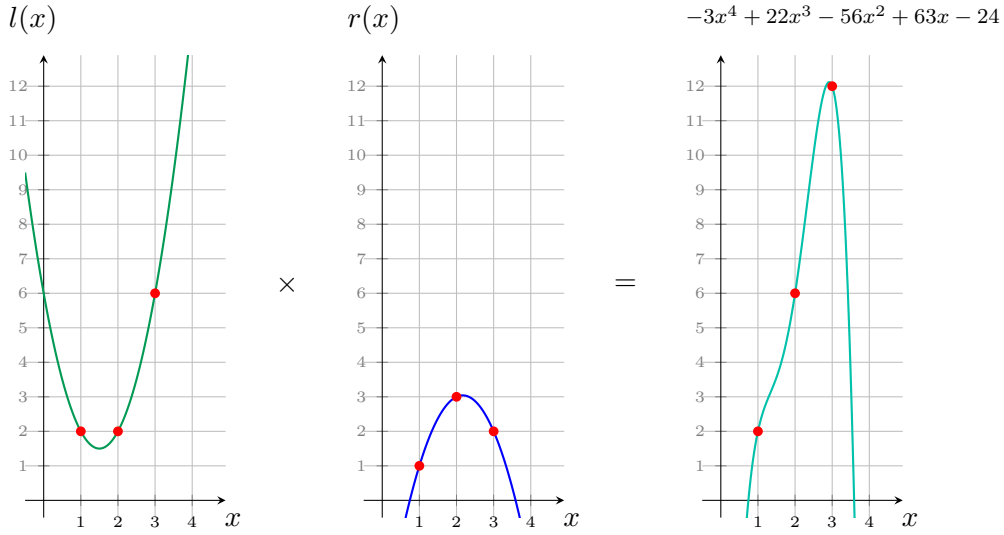


4.5.2 Multi-Operation Polynomials

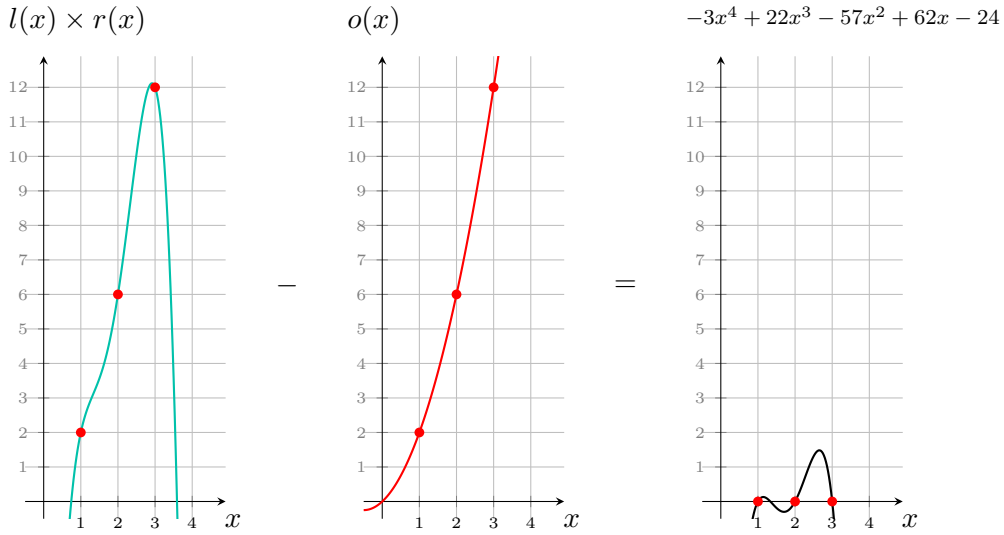
Now we have operand polynomials which represent three operations, let us see step-by-step how the correctness of each operation is verified. Recall that a verifier is looking for equality $l(x) \times r(x) - o(x) = t(x)h(x)$. In this case, because the operations are represented at points $x \in \{1, 2, 3\}$ the target polynomial has to evaluate to 0 at those x-s, in other words, the roots of the $t(x)$ must be 1, 2 and 3, which in elementary form is:



Firstly, $l(x)$ and $r(x)$ are multiplied which results in:



Secondly, the $o(x)$ is subtracted from the result of $l(x) \times r(x)$:



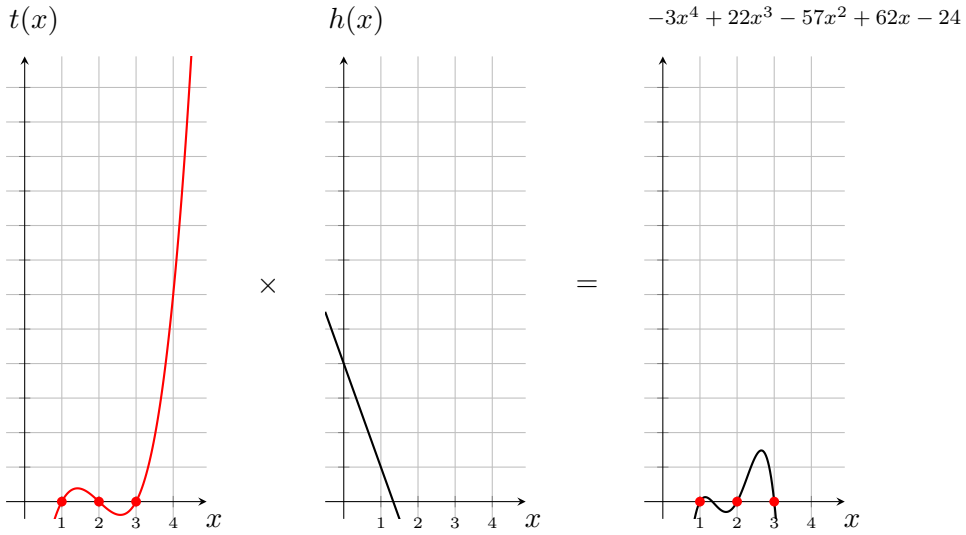
Where it is already visible that every operands multiplication corresponds to a correct result. For the last step a *prover* needs to present a valid cofactor:

$$h(x) = \frac{l(x) \times r(x) - o(x)}{t(x)} = \frac{-3x^4 + 22x^3 - 57x^2 + 62x - 24}{(x-1)(x-2)(x-3)}$$

Using long division we get:

$$
\begin{array}{rr}
h(x) = & \qquad\qquad\qquad\qquad -3x \;\; +4 \\
\hline
x^3 - 6x^2 + 11x - 6 \big) & -3x^4 + 22x^3 - 57x^2 + 62x - 24 \\
& \;\; 3x^4 - 18x^3 + 33x^2 - 18x \\
\hline
& \qquad\quad 4x^3 - 24x^2 + 44x - 24 \\
& \qquad\quad -4x^3 + 24x^2 - 44x + 24 \\
\hline
& \qquad\qquad\qquad\qquad 0
\end{array}
$$

With $h(x) = -3x + 4$ a *verifier* can compute $t(x)h(x)$:



It is now evident that $l(x) \times r(x) - o(x) = t(x)h(x)$ which is what had to be proven.

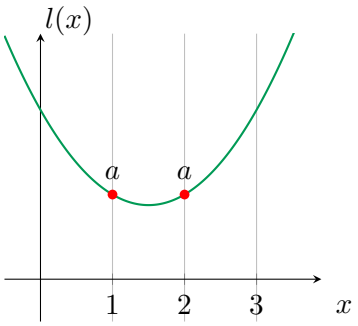
4.6 Variable Polynomials

With such an approach, we can prove many operations at once (e.g., millions and more), but there is a critical downside to it.

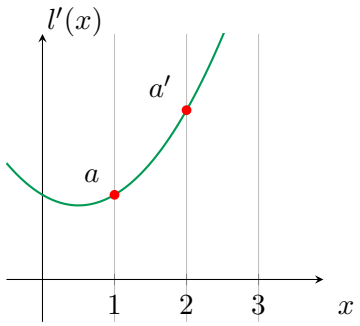
If the "program," execution for which is being proved, uses the same *variable*, either as an operand or as output, in different operations, for example:

$$
\begin{aligned}
a \times b &= r_1 \\
a \times c &= r_2
\end{aligned}
$$

The a will have to be represented in the *left operand polynomial* for both operations as:



Nevertheless, because our protocol allows prover to set any coefficients to a polynomial, he is not restricted from setting different values of a for different operations (i.e., represented by some x), e.g.:



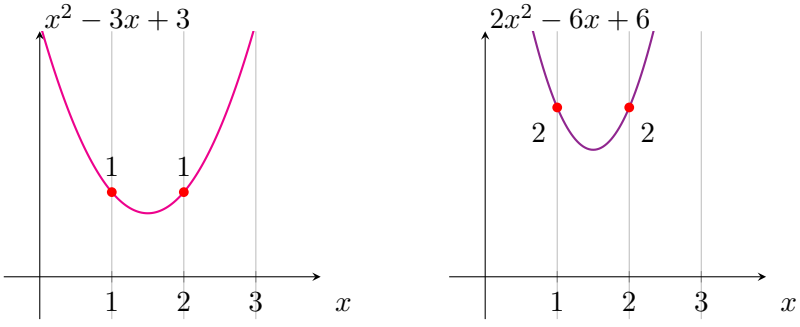
This freedom breaks consistency and allows prover to prove the execution of some other program which is not what verifier is interested in. Therefore we must ensure that any variable can only have a single value across every operation it is used in.

Note: variable in this context differs from the regular computer science definition in a sense that it is immutable and is only assigned once per execution.

4.6.1 Single-Variable Operand Polynomial

Let us consider a simple case (as with the current example) where we have only one variable (e.g., a) used in all left operands represented by the *left operand polynomial* $l(x)$. We have to find out if it is possible to ensure that this polynomial represents the same values of a for every operation. The reason why a prover can set different values is that he has control over each coefficient for every exponentiation of x. Therefore if those coefficients were constant, that would solve the variability problem.

May us have a closer look at polynomials containing equal values. For example examine two polynomials representing equal values for the two operations correspondingly (i.e., at $x = 1$ and $x = 2$), where the first polynomial contains value 1 and the second contains value 2:



Notice that the corresponding coefficients are proportional in each polynomial, such that coefficients in the second are twice as large as in the first, i.e.:

$$2x^2 - 6x + 6 = 2 \times (x^2 - 3x + 3)$$

Therefore when we want to change all the values simultaneously in a polynomial we need to change its proportion, this is due to arithmetic properties of polynomials, if we multiply a polynomial by a number, evaluations at every possible x will also be multiplied (i.e., scaled). To verify, try to multiply the first polynomial by 3 or any other number.

Consequently, if a verifier needs to enforce the prover to set the same value in all operations, then it should only be possible to modify the proportion and not the individual coefficients.

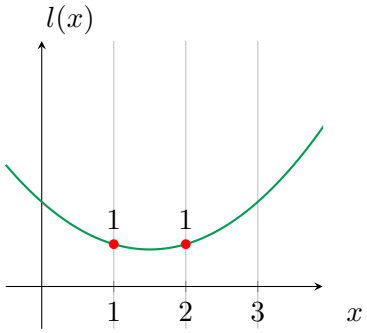
So how coefficients proportion can be preserved? We can start by considering what is provided as proof for the *left operand polynomial*. It is an encrypted evaluation of $l(x)$ at some secret s: $g^{l(s)}$, i.e., it is an encrypted number. We already know from section 3.4 how to restrict a verifier to use only the provided exponents of s through an α-shift, such that homomorphic multiplication is the single operation available.

Similarly to restricting a single exponent, the verifier can restrict the whole polynomial at once. Instead of providing separate encryptions $g^{s^1}, g^{s^2}, \ldots, g^{s^d}$ and their α-shifts $g^{\alpha s^1}, g^{\alpha s^2}, \ldots, g^{\alpha s^d}$ the protocol proceeds:

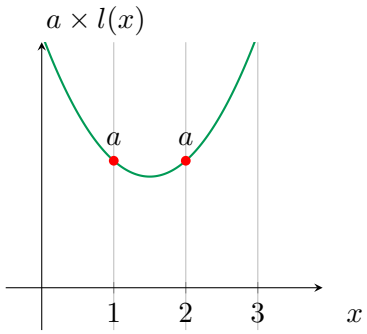
- Setup
  - construct the respective *operand polynomial* $l(x)$ with corresponding coefficients
  - sample random α and s
  - set proving key with encrypted $l(s)$ and it is "shifted" pair: $\left(g^{l(s)}, g^{\alpha l(s)}\right)$
  - set verification key: (g^{α})
- Proving
  - having operand's value v
    - multiply *operand polynomial*: $\left(g^{l(s)}\right)^v$
    - multiply shifted *operand polynomial*: $\left(g^{\alpha l(s)}\right)^v$
  - provide *operand polynomial* multiplication proof: $\left(g^{v\, l(s)}, g^{v\, \alpha l(s)}\right)$
- Verification
  - parse the proof as $\left(g^{l}, g^{l'}\right)$
  - verify proportion: $e\left(g^{l'}, g\right) = e\left(g^{l}, g^{\alpha}\right)$

Prover needs to respond with the same α-shift and because he cannot recover α from the proving key the only way to maintain the shift is to multiply both encryptions $g^{l(s)}$ and $g^{\alpha l(s)}$ by the same value. Therefore prover cannot modify individual coefficients of $l(x)$, for example if $l(x) = ax^2 + bx + c$ he can only multiply the whole polynomial at once by some value v: $v(ax^2 + bx + c) = vax^2 + vbx + vc$. Multiplication by another polynomial is not available since *pairings*, and α-shifts of individual exponents of s are not available. Prover cannot add or subtract either since $g^{\alpha(l(x)+a'x^2+c')} \neq g^{\alpha l(x)} \cdot g^{a'x^2} \cdot g^{c'}$ (this, again, requires the knowledge of unencrypted α).

We now have the protocol, but how *operand polynomial* $l(x)$ should be constructed? Since any integer can be derived by multiplying 1, the polynomial should evaluate to 1 for every corresponding operation, e.g.:



This allows a prover to *assign* the value of a:



Remark 4.1 *Since verification key contains g^{α} it is possible to add (or subtract) an arbitrary value v' to the polynomial, i.e.:*

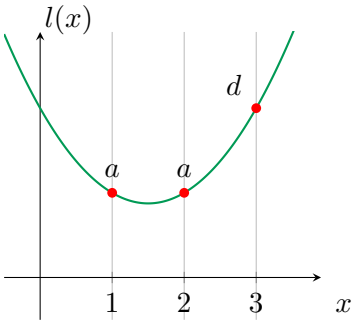
$$g^{vl(s)} \cdot g^{v'} = g^{vl(s)+v'}$$
$$g^{\alpha vl(s)} \cdot (g^{\alpha})^{v'} = g^{\alpha(vl(s)+v')}$$
$$e\left(g^{\alpha(vl(s)+v')}, g\right) = e\left(g^{vl(s)+v'}, g^{\alpha}\right)$$

Therefore it is possible to modify the polynomial beyond what is intended by the verifier and prove a different statement. We will address this shortcoming in section 4.9.3.

4.6.2 Multi-Variable Operand Polynomial

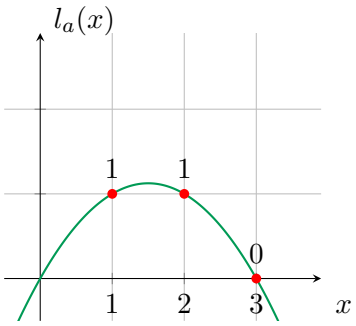
We are now able to singularly set value only if all left operands use the same variable. What if we add another one d:

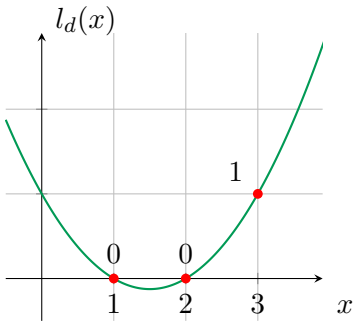
$$
\begin{aligned}
a \times b &= r_1 \\
a \times c &= r_2 \\
d \times c &= r_3
\end{aligned}
$$



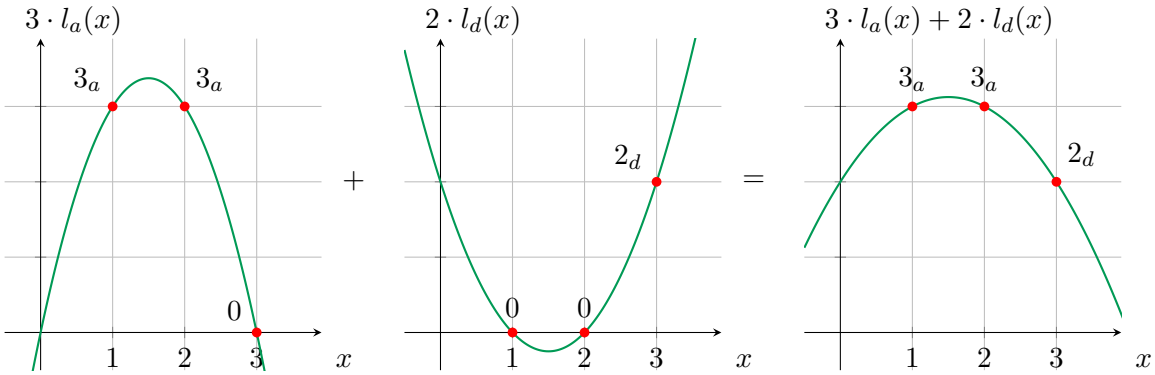
If we have used the same approach we would not be able to set the value separately for each variable, and every distinct variable will be multiplied altogether. Hence such restricted polynomial can support only one *variable*. If we examine properties of polynomials, we will see that adding polynomials together adds distinct evaluations of those polynomials. Therefore we can separate the *operand polynomial* $l(x)$ into *operand variable polynomials* $l_a(x)$ and $l_d(x)$ (note the subscripts) such that *variables* a and d are *assigned* and restricted separately similarly to the previous section and then added together to represent variables of all left operands. Because we add *operand variable polynomials* together, we need to ensure that only one of all the *variables* is represented for each operation by the operand polynomial.

Using the arithmetic properties we can construct each *operand variable polynomial* such that if *variable* is used as an operand in the corresponding operation then it evaluates to 1, otherwise to 0. Consecutively 0 multiplied by any value will remain zero and when added together it will be ignored. For our example $l_a(x)$ must conform to evaluations $l_a(1) = 1$, $l_a(2) = 1$ and $l_a(3) = 0$ and $l_d(x)$ is zero at 1 and 2 but 1 at $x = 3$:





Consequently we can set the value of each variable separately and just add them together to get the operand polynomial, for example if $a = 3$ and $d = 2$:



Note: we are using subscript next to a value to indicate which variable it represents, e.g., 3_a *is a variable* a *instantiated with value* 3*.*

Let us denote such composite *operand polynomial* with an upper-case letter from now on, e.g., $L(x) = a\,l_a(x) + d\,l_d(x)$, and its evaluation value as L, i.e., $L = L(s)$. This construction will only be effective if each *operand variable polynomial* is restricted by the verifier, the interaction concerning left operand shall be altered accordingly:

- Setup
  - construct $l_a(x)$, $l_d(x)$ such that it passes through 1 at "operation x" where it is used and through 0 in all other operations
  - sample random s, α
  - evaluate and encrypt *unassigned variable polynomials*:
    $g^{l_a(s)}, g^{l_d(s)}$
  - calculate *shifts* of these polynomials:
    $g^{\alpha l_a(s)}, g^{\alpha l_d(s)}$
  - set proving key:
    $\left(g^{l_a(s)}, g^{l_d(s)}, g^{\alpha l_a(s)}, g^{\alpha l_d(s)}\right)$
  - set verification key:
    (g^{α})
- Proving
  - *assign* values a and d to the variable polynomials:
    $\left(g^{l_a(s)}\right)^a, \left(g^{l_d(s)}\right)^d$
  - *assign* same values to the *shifted* polynomials:
    $\left(g^{\alpha l_a(s)}\right)^a, \left(g^{\alpha l_d(s)}\right)^d$
  - add all *assigned* variable polynomials to form an *operand polynomial*:
    $g^{L(s)} = g^{a l_a(s)} \cdot g^{d l_d(s)} = g^{a l_a(s) + d l_d(s)}$
  - add *shifted assigned variable polynomials* to form a *shifted operand polynomial*:
    $g^{\alpha L(s)} = g^{a\alpha l_a(s)} \cdot g^{d\alpha l_d(s)} = g^{\alpha(a l_a(s) + d l_d(s))}$
  - provide proof of valid assignment of *left operand*:
    $\left(g^{L(s)}, g^{\alpha L(s)}\right)$
- Verification
  - parse proof as $\left(g^{L}, g^{L'}\right)$
  - check that provided polynomials is a sum of multiples of originally provided *unassigned variable polynomials*:
    $e\left(g^{L'}, g\right) = e\left(g^{L}, g^{\alpha}\right)$ which checks that
    $\alpha\, a l_a(s) + \alpha\, d l_d(s) = \alpha \times (a l_a(s) + d l_d(s))$

Note: $L(s)$ and $\alpha L(s)$ represent all variable polynomials at once and since α is used only in evaluation of variable polynomials, the prover has no option but to use provided evaluations and assign same coefficients to original and shifted variable polynomials.

As a consequence the prover:

- is not able to modify provided *variable polynomials* by changing their coefficients, except "assigning" values, because prover is presented only with encrypted evaluations of these polynomials, and because necessary encrypted powers of s are unavailable separately with their α-shifts
- is not able to add another polynomial to the provided ones because the α-ratio will be broken
- is not able to modify operand polynomials through multiplication by some other polynomial $u(x)$, which could disproportionately modify the values because encrypted multiplication is not possible in pre-pairings space

Note: if we add (or subtract) one polynomial, e.g., $l_a(x)$, to the other, e.g., $l'_d(x) = c_d \cdot l_d(x) + c'_a \cdot l_a(x)$, that is not really a modification of the polynomial $l_d(x)$, but rather changing of the resulting coefficient of the $l_a(x)$, because they are summed up in the end:

$$L(x) = c_a \cdot l_a(x) + l'_d(x) = (c_a + c'_a) \cdot l_a(x) + c_d \cdot l_d(x)$$

While the prover restricts the use of polynomials, there is still some freedoms which are not necessary to counteract:

- it is acceptable if the prover decides not to add some of the assigned variable polynomials $l_i(x)$ to form the operand polynomial $L(x)$ because it is the same as to assign the value 0: $g^{al_a(x)} = g^{al_a(x)+0l_d(x)}$
- it is acceptable if the prover adds same variable polynomials multiple times because it is the same as to assign the multiple of that value once, e.g., $g^{al_a(x)} \cdot g^{al_a(x)} \cdot g^{al_a(x)} = g^{3al_a(x)}$

This approach is applied similarly to the right operand and output polynomials $R(x)$, $O(x)$.

4.7 Construction Properties

There are multiple additional useful properties which are acquired as a side-effect of such modification.

4.7.1 Constant Coefficients

In the above construction, we have been using evaluations of *unassigned variable polynomials* 1 or 0 as a means to signify if the variable is *used* in operation or *not*. Naturally, there is nothing that stops us from using other coefficients as well, including negative ones, because

we can *interpolate* polynomials through any necessary points[22]. Examples of such operations are:

$$2a \times 1b = 3r$$
$$-3a \times 1b = -2r$$

Therefore our program can now use constant coefficients, for example:

Algorithm 2 Constant coefficients

```
function calc(w, a, b)
    if w then
        return 3a × b
    else
        return 5a × 2b
    end if
end function
```

These coefficients will be "hardwired" during the setup stage and similarly to 1 or 0 will be immutable. We can modify the form of operation accordingly:

$$c_a \cdot a \times c_b \cdot b = c_r \cdot r$$

Or more formally, for variables $v_i \in \{v_1, v_2, ..., v_n\}$:

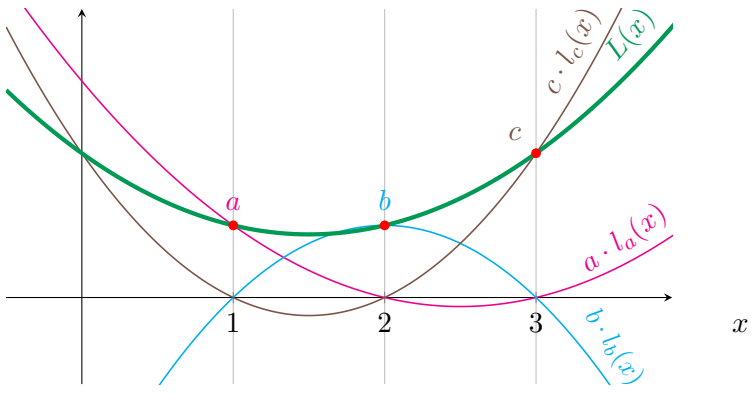
$$c_l \cdot v_l \times c_r \cdot v_r = c_o \cdot v_o$$

where l, r, o are indices of a variable used in operation.

Note: constant coefficient for the same variable can be different in different operations and operands/outputs.

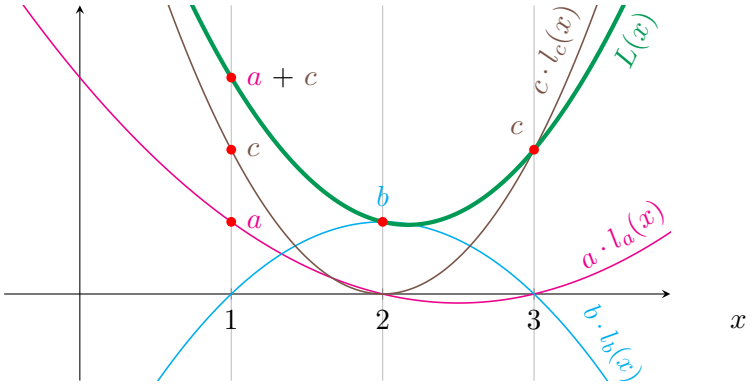
4.7.2 Addition for Free

Considering the updated construction, it is apparent that in polynomial representation every *operand* expressed by some distinct x is a sum of all *operand variable polynomials* such that only single *used* variable can have a non-zero value and all others are zero. The graph demonstrates it best:



[22]Provided that no two operations occupy same x

We can take advantage of such construction and allow to add any number of necessary *variables* for each operand in operation. For example in the first operation, we can add $a + c$ first and only then multiply it by some other operand, e.g., $(a + c) \times b = r$, this can be represented as:



Therefore it is possible to add any number of present variables in a single *operand*, using arbitrary coefficients for each of them, to produce an operand value which will be used in a corresponding operation, as needed in a respective program. Such property effectively allows changing the operation construction to:

$$(c_{\mathrm{l},a} \cdot a + c_{\mathrm{l},b} \cdot b + \ldots) \times (c_{\mathrm{r},a} \cdot a + c_{\mathrm{r},b} \cdot b + \ldots) = (c_{\mathrm{o},a} \cdot a + c_{\mathrm{o},b} \cdot b + \ldots)$$

Or more formally, for variables $v_i \in \{v_1, v_2, ..., v_n\}$ and operand variable coefficients $c_{\mathrm{l},i} \in \{c_{\mathrm{l},1}, c_{\mathrm{l},2}, ..., c_{\mathrm{r},n}\}$, $c_{\mathrm{r},i} \in \{c_{\mathrm{r},1}, c_{\mathrm{r},2}, ..., c_{\mathrm{r},n}\}$, $c_{\mathrm{o},i} \in \{c_{\mathrm{o},1}, c_{\mathrm{o},2}, ..., c_{\mathrm{o},n}\}$:

$$\sum_{i=1}^{n} c_{\mathrm{l},i} \cdot v_i \times \sum_{i=1}^{n} c_{\mathrm{r},i} \cdot v_i = \sum_{i=1}^{n} c_{\mathrm{o},i} \cdot v_i$$

Note: each operation's operand has its own set of coefficients c.

4.7.3 Addition, Subtraction and Division

We have been focusing on multiplication operation primarily until now. However, in order to be able to execute general computations, a real-life program will also require addition, division, and subtraction.

Addition In previous section we have established that we can add variables in context of a single operand, which is then multiplied by another operand, e.g., $(3a + b) \times d = r$, but what if we need just addition without multiplication, for example, if a program needs to compute a + b, we can express this as:

$$(a + b) \times 1 = r$$

Note: because our construction requires both a constant coefficient and a variable $(c \cdot v)$ for every operand, the value of 1 is expressed as $c_{\mathrm{one}} \cdot v_{\mathrm{one}}$, and while $c_{\mathrm{one}} = 1$ can be "hardwired" into a corresponding polynomial, the v_{one} is a variable and can be assigned any value, therefore we must enforce the value of v_{one} through constraints as explained in section 4.10.

Subtraction Subtraction is almost identical to addition, the only difference is a negative coefficient, e.g., for a − b:

$$(a + -1 \cdot b) \quad \times \quad 1 \quad = \quad r$$

Division If we examine the division operation $\frac{\mathsf{factor}}{\mathsf{divisor}} = \mathsf{result}$ we would see that the result of the division is the number we need to multiply divisor by to produce the factor. Therefore we can express the same meaning through multiplication: $\mathsf{divisor} \times \mathsf{result} = \mathsf{factor}$. Consequently, if we want to prove the division operation $\frac{\mathrm{a}}{\mathrm{b}} = \mathrm{r}$, it can be expressed as:

$$b \quad \times \quad r \quad = \quad a$$

Note: the operation's construction is also called "constraint" because the operation represented by polynomial construction does not compute results per se, but rather checks that the prover already knows variables (including result), and they are valid *for the operation, i.e., the prover is constrained to provide consistent values no matter what they are.*

Note: all those arithmetic operations were already present; therefore modification of the operation's construction is not needed.

4.8 Example Computation

Having the general operation's construction, we can convert our original algorithm 1 into a set of operations and further into polynomial form. Let us consider the mathematical form of the algorithm (we will use variable v to capture the result of evaluation):

$$w \times (a \times b) + (1 - w) \times (a + b) = v$$

It has three multiplications, and because the operation construction supports only one, there will be at least 3 operations. However, we can simplify the equation:

$$w \times (a \times b) + a + b - w \times (a + b) = v$$
$$w \times (a \times b - a - b) = v - a - b$$

Now it requires two multiplications while maintaining same relationships. In complete form the operations are:

$$1: \qquad 1 \cdot a \quad \times \quad 1 \cdot b \quad = \quad 1 \cdot m$$
$$2: \qquad 1 \cdot w \quad \times \quad 1 \cdot m \; + \; -1 \cdot a \; + \; -1 \cdot b \quad = \quad 1 \cdot v \; + \; -1 \cdot a \; + \; -1 \cdot b$$

We can also add a constraint that requires w to be binary, otherwise a prover can use any value for w rendering computation incorrect:

$$3: \qquad 1 \cdot w \quad \times \quad 1 \cdot w \quad = \quad 1 \cdot w$$

To see why w can only be 0 or 1, we can represent the equation as $w^2 - w = 0$ and further as $(w - 0)(w - 1) = 0$ where 0 and 1 are the only solutions.

These totals to 5 variables, with 2 in the left operand, 4 in the right operand and 5 in the output. The operand polynomials are:

$$L(x) = a \cdot l_a(x) + w \cdot l_w(x)$$
$$R(x) = m \cdot r_m(x) + a \cdot r_a(x) + b \cdot r_b(x) + w \cdot r_w(x)$$
$$O(x) = m \cdot o_m(x) + v \cdot o_v(x) + a \cdot o_a(x) + b \cdot o_b(x) + w \cdot o_w(x)$$

where each *variable polynomial* must evaluate to a corresponding coefficient for each of 3 operations or to 0 if the variable isn't present in the operation's operand or output:

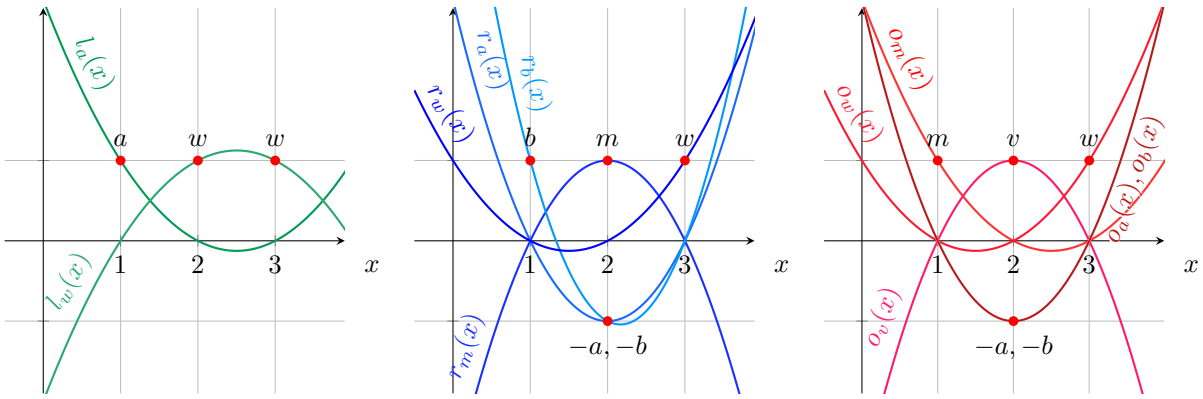
$$l_a(1) = 1;\ l_a(2) = 0;\ l_a(3) = 0;\ r_m(1) = 0;\ r_m(2) = 1;\ r_m(3) = 0;\ o_m(1) = 1;\ o_m(2) = 0;\ o_m(3) = 0;$$
$$l_w(1) = 0;\ l_w(2) = 1;\ l_w(3) = 1;\ r_a(1) = 0;\ r_a(2) = -1;\ r_a(3) = 0;\ o_v(1) = 0;\ o_v(2) = 1;\ o_v(3) = 0;$$
$$r_b(1) = 1;\ r_b(2) = -1;\ r_b(3) = 0;\ o_a(1) = 0;\ o_a(2) = -1;\ o_a(3) = 0;$$
$$r_w(1) = 0;\ r_w(2) = 0;\ r_w(3) = 1;\ o_b(1) = 0;\ o_b(2) = -1;\ o_b(3) = 0;$$
$$o_w(1) = 0;\ o_w(2) = 0;\ o_w(3) = 1;$$

Consequently the cofactor polynomial is $t(x) = (x-1)(x-2)(x-3)$, which will ensure that all three operations are computed correctly.

Next we leverage polynomial interpolation to find each *variable polynomial*:

$$l_a(x) = \frac{1}{2}x^2 - \frac{5}{2}x + 3; \qquad r_m(x) = -x^2 + 4x - 3; \qquad o_m(x) = \frac{1}{2}x^2 - \frac{5}{2}x + 3;$$
$$l_w(x) = -\frac{1}{2}x^2 + \frac{5}{2}x - 2; \qquad r_a(x) = x^2 - 4x + 3; \qquad o_v(x) = -x^2 + 4x - 3;$$
$$r_b(x) = \frac{3}{2}x^2 - \frac{13}{2}x + 6; \qquad o_a(x) = x^2 - 4x + 3;$$
$$r_w(x) = \frac{1}{2}x^2 - \frac{3}{2}x + 1; \qquad o_b(x) = x^2 - 4x + 3;$$
$$o_w(x) = \frac{1}{2}x^2 - \frac{3}{2}x + 1;$$

Which are plotted as:



We are ready to prove computation through polynomials. Firstly, let us choose input values for the function, for example $w = 1, a = 3, b = 2$. Secondly, calculate values of intermediary

variables from operations:

$$m = a \times b = 6$$

$$v = w(m - a - b) + a + b = 6$$

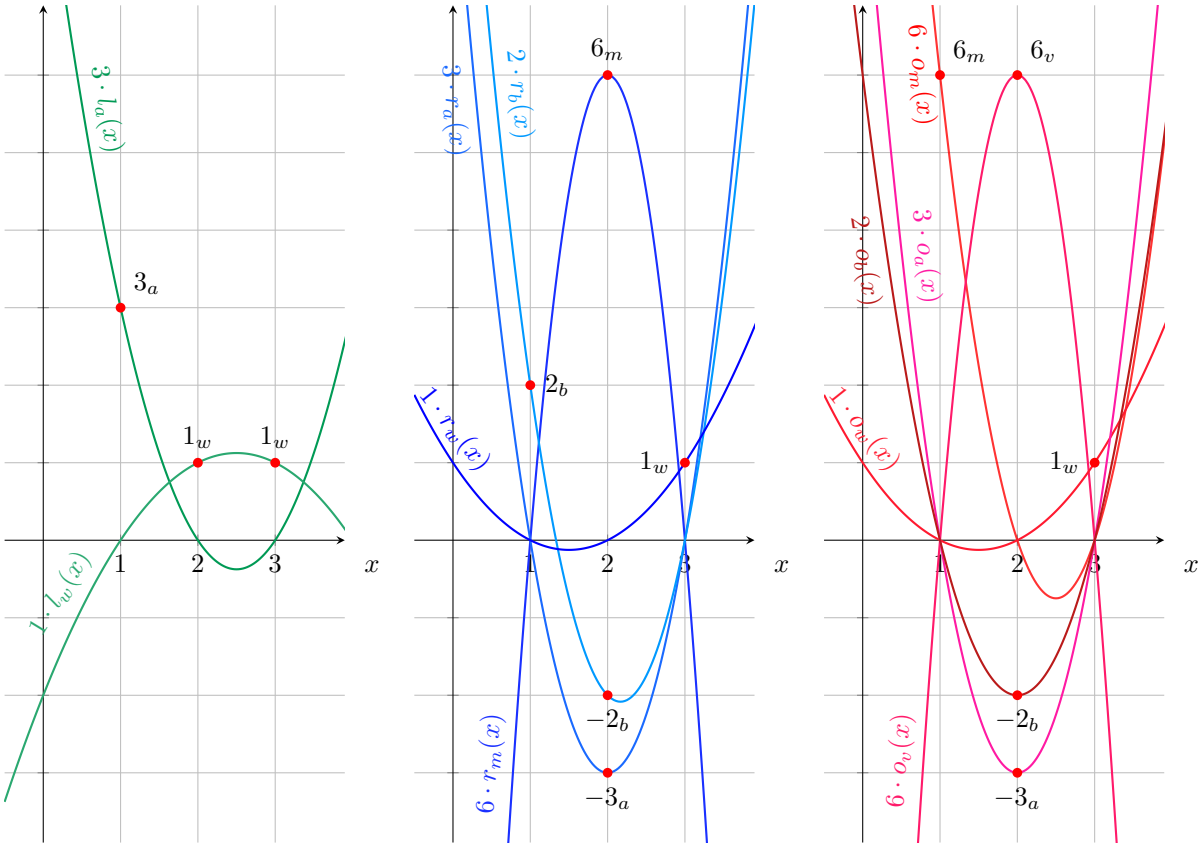
After, we assign all values involved in the computation of the result to the corresponding *variable polynomials* and sum them up to form operand and output polynomials:

$$L(x) = 3 \cdot l_a(x) + 1 \cdot l_w(x) = x^2 - 5x + 7$$

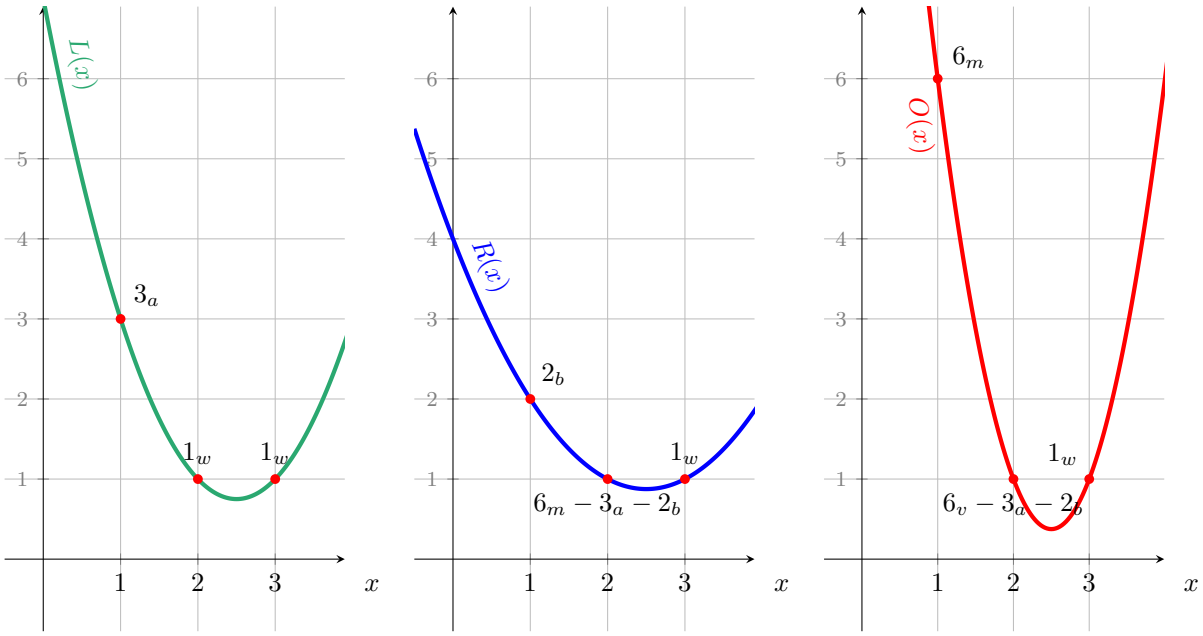
$$R(x) = 6 \cdot r_m(x) + 3 \cdot r_a(x) + 2 \cdot r_b(x) + 1 \cdot r_w(x) = \frac{1}{2}x^2 - 2\frac{1}{2}x + 4$$

$$O(x) = 6 \cdot o_m(x) + 6 \cdot o_v(x) + 3 \cdot o_a(x) + 2 \cdot o_b(x) + 1 \cdot o_w(x) = 2\frac{1}{2}x^2 - 12\frac{1}{2}x + 16$$

and in the graph form these are:



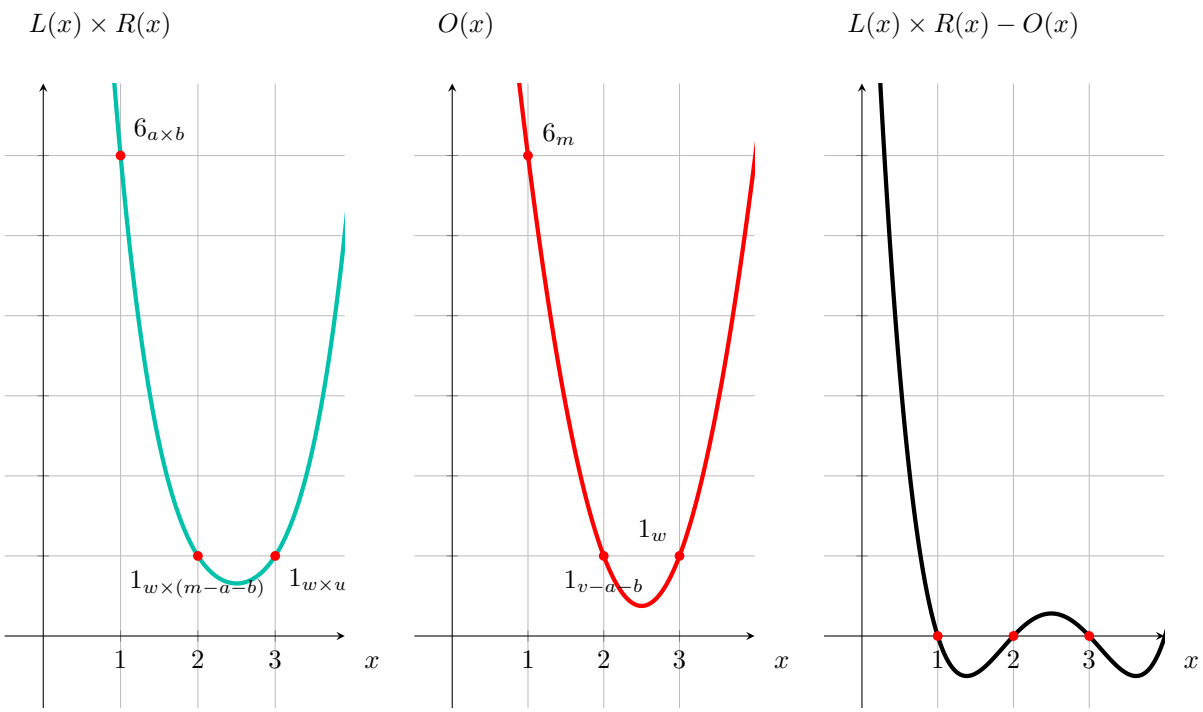
Summed up to represent operand and output values in corresponding operations:



We need to prove that $L(x) \times R(x) - O(x) = t(x)\,h(x)$, therefore we find $h(x)$:

$$h(x) = \frac{L(x) \times R(x) - O(x)}{t(x)} = \frac{\frac{1}{2}x^4 - 5x^3 + \frac{35}{2}x^2 - 25x + 12}{(x-1)(x-2)(x-3)} = \frac{1}{2}x - 2$$

In a graph form it is represented as:



Where it's visible that polynomial $L(x) \times R(x) - O(x)$ has solutions $x = 1$, $x = 2$ and $x = 3$, and therefore $t(x)$ is its cofactor, which would not be the case if we used inconsistent values of variables.

That is how the knowledge of variable values for a correct computation execution is proven on the level of polynomials. A prover is then proceeding with a cryptographic portion of the protocol.

4.9 Verifiable Computation Protocol

We went through many important modifications of the knowledge of polynomial protocol (section 3.7) to make it general-purpose, so let us see how it is defined now. Assuming agreed upon function $f(*)$ the result of computation of which is the subject of the proof, with the number of operations d, the number of variables n and corresponding to them coefficients $\{c_{\mathrm{L},i,j}, c_{\mathrm{R},i,j}, c_{\mathrm{O},i,j}\}_{i\in\{1,\dots,n\},j\in\{1,\dots,d\}}$:

- Setup
  - construct *variable polynomials* for left operand $\{l_i(x)\}_{i\in\{1,\dots,n\}}$ such that for all operations $j \in \{1,\dots,d\}$ they evaluate to corresponding coefficients, i.e., $l_i(j) = c_{\mathrm{L},i,j}$, and similarly for right operand and output
  - sample random s, α
  - calculate $t(x) = (x-1)(x-2)\dots(x-d)$ and its evaluation $g^{t(s)}$
  - compute proving key: $\left(\left\{g^{s^k}\right\}_{k\in[d]}, \left\{g^{l_i(s)}, g^{r_i(s)}, g^{o_i(s)}, g^{\alpha l_i(s)}, g^{\alpha r_i(s)}, g^{\alpha o_i(s)}\right\}_{i\in\{1,\dots,n\}} \right)$
  - compute verification key: $\left(g^{t(s)}, g^{\alpha}\right)$
- Proving
  - compute function $f(*)$ and therefore corresponding variables values $\{v_i\}_{i\in\{1,\dots,n\}}$
  - calculate $h(x) = \frac{L(x)\times R(x) - O(x)}{t(x)}$, where $L(x) = \sum_{i=1}^{n} v_i \cdot l_i(x)$, and similarly $R(x), O(x)$
  - assign variable values and *sum up* to get operand polynomials:
$$g^{L(s)} = \left(g^{l_1(s)}\right)^{v_1} \cdots \left(g^{l_n(s)}\right)^{v_n}, \quad g^{R(s)} = \prod_{i=1}^{n} \left(g^{r_i(s)}\right)^{v_i}, \quad g^{O(s)} = \prod_{i=1}^{n} \left(g^{o_i(s)}\right)^{v_i}$$
  - assign variable values to the shifted polynomials:
$$g^{\alpha L(s)} = \prod_{i=1}^{n} \left(g^{\alpha l_i(s)}\right)^{v_i}, \quad g^{\alpha R(s)} = \prod_{i=1}^{n} \left(g^{\alpha r_i(s)}\right)^{v_i}, \quad g^{\alpha O(s)} = \prod_{i=1}^{n} \left(g^{\alpha o_i(s)}\right)^{v_i}$$
  - calculate encrypted evaluation $g^{h(s)}$ using provided powers of s: $\left\{g^{s^k}\right\}_{k\in[d]}$
  - set proof: $\left(g^{L(s)}, g^{R(s)}, g^{O(s)}, g^{\alpha L(s)}, g^{\alpha R(s)}, g^{\alpha O(s)}, g^{h(s)}\right)$
- Verification
  - parse proof as $\left(g^{L}, g^{R}, g^{O}, g^{L'}, g^{R'}, g^{O'}, g^{h}\right)$
  - variable polynomials restriction check:
$e(g^L, g^\alpha) = e(g^{L'}, g), \quad e(g^R, g^\alpha) = e(g^{R'}, g), \quad e(g^O, g^\alpha) = e(g^{O'}, g)$
  - valid operations check:
$e(g^L, g^R) = e(g^t, g^h) \cdot e(g^O, g)$

Note: using symbol $\prod$ allows for a concise way to express product of multiple elements, i.e., $\prod_{i=1}^{n} v_i = v_1 \cdot v_2 \cdot \ldots \cdot v_n$.

The set of all the variable polynomials $\{l_i(x), r_i(x), o_i(x)\}_{i\in\{1,\dots,n\}}$ and the target polynomial $t(x)$ is called a *quadratic arithmetic program* (QAP[23]).

While the protocol is sufficiently robust to allow a general computation verification, there are two security considerations that must be addressed.

4.9.1 Non-Interchangeability of Operands and Output

Because we use the same α for all the operands of *variable polynomials restriction* there is nothing that prevents prover from:

- using variable polynomials from other operands, e.g., $L'(s) = o_1(s) + r_1(s) + r_5(s) + \dots$
- swapping *operand polynomials* completely, e.g., $O(s)$ with $L(s)$ will result in operation $O(s) \times R(s) = L(s)$
- re-using same operand polynomials e.g., $L(s) \times L(s) = O(s)$

This interchangeability means that the prover can alter the execution and effectively prove some other computation. The obvious way to prevent such behavior is to use different α-s for the different operands, concretely we modify:

- Setup
  - $\dots$
  - sample random $\alpha_l, \alpha_r, \alpha_o$ instead of α
  - calculate corresponding "shifts" $\left\{g^{\alpha_l l_i(s)}, g^{\alpha_r r_i(s)}, g^{\alpha_o o_i(s)}\right\}_{i\in\{1\dots n\}}$
  - proving key: $\left(\left\{g^{s^k}\right\}_{k\in[d]}, \left\{g^{l_i(s)}, g^{r_i(s)}, g^{o_i(s)}, g^{\alpha_l l_i(s)}, g^{\alpha_r r_i(s)}, g^{\alpha_o o_i(s)}\right\}_{i\in\{1\dots n\}}\right)$
  - verification key: $\left(g^{t(s)}, g^{\alpha_l}, g^{\alpha_r}, g^{\alpha_o}\right)$
- Proving
  - $\dots$
  - assign variables to the "shifted" polynomials
    $g^{\alpha_l L(s)} = \prod_{i=1}^{n}\left(g^{\alpha_l l_i(s)}\right)^{v_i}$, $g^{\alpha_r R(s)} = \prod_{i=1}^{n}\left(g^{\alpha_r r_i(s)}\right)^{v_i}$, $g^{\alpha_o O(s)} = \prod_{i=1}^{n}\left(g^{\alpha_o o_i(s)}\right)^{v_i}$
  - set proof: $\left(g^{L(s)}, g^{R(s)}, g^{O(s)}, g^{\alpha_l L(s)}, g^{\alpha_r R(s)}, g^{\alpha_o O(s)}, g^{h(s)}\right)$
- Verification
  - $\dots$
  - variable polynomials restriction check:
    $e\left(g^{L}, g^{\alpha_l}\right) = e\left(g^{L'}, g\right)$, $e\left(g^{R}, g^{\alpha_r}\right) = e\left(g^{R'}, g\right)$, $e\left(g^{O}, g^{\alpha_o}\right) = e\left(g^{O'}, g\right)$

[23] Gen+12.

It is now not possible to use variable polynomials from other operands since $\alpha_l, \alpha_r, \alpha_o$ are not known to the prover.

4.9.2 Variable Consistency Across Operands

For any variable v_i we have to *assign* its value to a *variable polynomial* for each corresponding operand, i.e., $\left(g^{l_i(s)}\right)^{v_i}, \left(g^{r_i(s)}\right)^{v_i}, \left(g^{o_i(s)}\right)^{v_i}$. Because the validity of each of the *operand polynomials* is checked separately, no enforcement requires to use same variable values in the corresponding *variable polynomials*. This means that the value of variable v_1 in left operand can differ from variable v_1 in the right operand or the output.

We can enforce equality of a variable value across operands through already familiar approach of restricting a polynomial (as we did with variable polynomials). If we can create a "shifted checksum" variable polynomial across all operands, that would restrain prover such that he can assign only same value. A verifier can combine polynomials for each variable into one, e.g., $g^{l_i(s)+r_i(s)+o_i(s)}$, and shift it by some other random value β, i.e., $g^{\beta(l_i(s)+r_i(s)+o_i(s))}$. This shifted polynomials are provided to the prover to assign values of the variables alongside with variable polynomials:

$$\left(g^{l_i(s)}\right)^{v_{\mathrm{L},i}}, \left(g^{r_i(s)}\right)^{v_{\mathrm{R},i}}, \left(g^{o_i(s)}\right)^{v_{\mathrm{O},i}}, \left(g^{\beta(l_i(s)+r_i(s)+o_i(s))}\right)^{v_{\beta,i}}$$

And the β is encrypted and added to the verification key g^{β}. Now, if the values of all v_i were the same (i.e., $v_{\mathrm{L},i} = v_{\mathrm{R},i} = v_{\mathrm{O},i} = v_{\beta,i}$ for $i \in \{1, \ldots, n\}$), the equation shall hold:

$$e\left(g^{v_{\mathrm{L},i} \cdot l_i(s)} \cdot g^{v_{\mathrm{R},i} \cdot r_i(s)} \cdot g^{v_{\mathrm{O},i} \cdot o_i(s)}, g^{\beta}\right) = e\left(g^{v_{\beta,i} \cdot \beta(l_i(s)+r_i(s)+o_i(s))}, g\right)$$

While this is a useful consistency check, due to the non-negligible probability that at least two of $l(s), r(s), o(s)$ could either have same evaluation value or one polynomial is divisible by another etc., this would allow the prover to factor values $v_{\mathrm{L},i}, v_{\mathrm{R},i}, v_{\mathrm{O},i}, v_{\beta,i}$ such that at least two of them are non-equal but the equation holds, rendering the check ineffective:

$$(v_{\mathrm{L},i} \cdot l_i(s) + v_{\mathrm{R},i} \cdot r_i(s) + v_{\mathrm{O},i} \cdot o_i(s)) \cdot \beta = v_{\beta,i} \cdot \beta \cdot (l_i(s) + r_i(s) + o_i(s))$$

For example, let us consider a single operation, where it is the case that $l(x) = r(x)$. We will denote evaluation of those two as $w = l(s) = r(s)$ and $y = o(x)$. The equation then will look as:

$$\beta(v_{\mathrm{L}}\, w + v_{\mathrm{R}}\, w + v_{\mathrm{O}}\, y) = v_{\beta} \cdot \beta(w + w + y)$$

Such form allows, for some arbitrary v_{R} and v_{O}, to set $v_{\beta} = v_{\mathrm{O}}$, $v_{\mathrm{L}} = 2v_{\mathrm{O}} - v_{\mathrm{R}}$, which will translate into:

$$\beta(2v_{\mathrm{O}}\, w - v_{\mathrm{R}}\, w + v_{\mathrm{R}}\, w + v_{\mathrm{O}}\, y) = v_{\mathrm{O}} \cdot \beta(2w + y)$$

Hence such consistency strategy is not effective. A way to mitigate this is to use different β for each operand, ensuring that operand's *variable polynomials* will have unpredictable values. Following are the protocol modifications:

- Setup
  - ... sample random $\beta_l, \beta_r, \beta_o$

  - calculate, encrypt and add to the proving key the *variable consistency polynomials*: $\left\{g^{\beta_l l_i(s)+\beta_r r_i(s)+\beta_o o_i(s)}\right\}_{i\in\{1,\dots,n\}}$
  - encrypt β-s and add to the verification key: $\left(g^{\beta_l}, g^{\beta_r}, g^{\beta_o}\right)$

- Proving
  - ... assign variable values to the *variable consistency polynomials*: $g^{z_i(s)} = \left(g^{\beta_l l_i(s)+\beta_r r_i(s)+\beta_o o_i(s)}\right)^{v_i} \quad \text{for } i \in \{1,\dots,n\}$
  - add assigned polynomials in encrypted space: $g^{Z(s)} = \prod_{i=1}^{n} g^{z_i(s)} = g^{\beta_l L(s)+\beta_r R(s)+\beta_o O(s)}$
  - add to the proof: $g^{Z(s)}$

- Verification
  - ... check the consistency between provided *operand polynomials* and the "checksum" polynomial: $e\left(g^L, g^{\beta_l}\right) \cdot e\left(g^R, g^{\beta_r}\right) \cdot e\left(g^O, g^{\beta_o}\right) = e\left(g^Z, g\right)$ which is equivalent to: $e\left(g, g\right)^{\beta_l L+\beta_r R+\beta_o O} = e\left(g, g\right)^{Z}$

Same variable values tempering technique will fail in such construction because different β-s makes the same polynomials incompatible for manipulation. There is however a flaw similar to the one in remark 4.1, concretely because the terms $g^{\beta_l}, g^{\beta_r}, g^{\beta_o}$ are publicly available an adversary can modify the zero-index coefficient of any of the variable polynomials since it does not rely on s, i.e., $g^{\beta_l s^0} = g^{\beta_l}$.

4.9.3 Non-malleability of Variable and Variable Consistency Polynomials

Malleability of Variable Polynomials

Let us exemplify remark 4.1 with the following two operations:

$$\begin{aligned} a \quad &\times \quad 1 \quad = \quad b \\ 3a \quad &\times \quad 1 \quad = \quad c \end{aligned}$$

The expected result is $b = a$ and $c = 3a$, with clear relationship $c = 3b$. This implies that the *left operand's variable* polynomial has evaluations $l_a(1) = 1$ and $l_a(2) = 3$. Regardless of the form of $l_a(x)$, a prover can unproportionately assign the value of a, by providing modified polynomial $l'_a(x) = a l_a(x) + 1$. Therefore evaluations will be $l'_a(1) = a + 1$ and $l'_a(2) = 3a + 1$, hence the results $b = a + 1$ and $c = 3a + 1$ where $c \neq 3b$, effectively meaning that the value of a is different for different operations.

Because the prover has access to g^{α_l} and g^{β_l} he can satisfy both the *correct operand polynomials* and *variable values consistency* checks:

- ... proving:
  - form left operand polynomial by unproportionately assigning variable a: $L(x) = a \cdot l_a(x) + 1$
  - form right operand and output polynomials as usual: $R(x) = r_1(x)$, $O(x) = b \cdot o_b(x) + c \cdot o_c(x)$
  - calculate the remainder $h(x) = \frac{L(x) \cdot R(x) - O(x)}{t(x)}$
  - compute encryption: $g^{L(s)} = \left(g^{l_a(s)}\right)^a \cdot g^1$ and as usual for $g^{R(s)}, g^{O(s)}$
  - compute α-shifts: $g^{\alpha L(s)} = \left(g^{\alpha l_a(s)}\right)^a \cdot g^\alpha$ and as usual for $g^{\alpha R(s)}, g^{\alpha O(s)}$
  - compute variable consistency polynomials: $g^{Z(s)} = \prod_{i \in \{1,a,b,c\}} \left(g^{\beta_l l_i(s) + \beta_r r_i(s) + \beta_o o_i(s)}\right)^i \cdot g^{\beta_l} = g^{\beta_l(L(s)+1) + \beta_r R(s) + \beta_o O(s)}$

    where the subscript $_i$ represents symbol of the corresponding variable while the exponent ^{i} represents the value of variable; moreover undefined *variable polynomials* are equal to zero.
  - set proof: $\left(g^{L(s)}, g^{R(s)}, g^{O(s)}, g^{\alpha_l L(s)}, g^{\alpha_r R(s)}, g^{\alpha_o O(s)}, g^{Z(s)} g^{h(s)}\right)$
- verification:
  - variable polynomials restriction check: $e\left(g^{L'}, g\right) = e\left(g^L, g^\alpha\right) \Rightarrow e\left(g^{\alpha a \cdot l_a(s) + \alpha}, g\right) = e\left(g^{a l_a(s) + 1}, g^\alpha\right)$ and as usually for $g^{R'}, g^{O'}$
  - variable values consistency check $e\left(g^L, g^{\beta_l}\right) \cdot e\left(g^R, g^{\beta_r}\right) \cdot e\left(g^O, g^{\beta_o}\right) = e\left(g^Z, g\right) \Rightarrow$ $e\left(g, g\right)^{(a \cdot l_a + 1)\beta_l + R\beta_r + O\beta_o} = e\left(g, g\right)^{\beta_l(L+1) + \beta_r R + \beta_o O}$
  - valid operations check $e(g^L, g^R) = e(g^t, g^h) \cdot e(g^O, g)$

Malleability of Variable Consistency Polynomials

Moreover the availability of $g^{\beta_l}, g^{\beta_r}, g^{\beta_o}$ allows to use different values of same variable in different operands. For example, if we have an operation:

$$a \quad \times \quad a \quad = \quad b$$

Which can be represented by the variable polynomials:

$$l_a(x) = x, \quad r_a(x) = x, \quad o_a(x) = 0$$
$$l_b(x) = 0, \quad r_b(x) = 0, \quad o_b(x) = x$$

While the expected output is $b = a^2$, we can set different values of a, for example $a = 2$, $a = 5$ as following:

- proving:
  - ... form left operand polynomial with $a = 2$: $L(x) = 2l_a(x) + 10l_b(x)$

  - form right operand polynomial with $a = 5$: $R(x) = 2r_a(x) + 3 + 10r_b(x)$
  - form output polynomial with $b = 10$: $O(x) = 2o_a(x) + 10o_b(x)$
  - ... compute encryptions:
    $g^{L(s)} = \left(g^{l_a(s)}\right)^2 \cdot \left(g^{l_b(s)}\right)^{10} = g^{2l_a(s)+10l_b(s)}$
    $g^{R(s)} = \left(g^{r_a(s)}\right)^2 \cdot (g)^3 \cdot \left(g^{r_b(s)}\right)^{10} = g^{2r_a(s)+3+10r_b(s)}$
    $g^{O(s)} = \left(g^{o_a(s)}\right)^2 \cdot \left(g^{o_b(s)}\right)^{10} = g^{2o_a(s)+10o_b(s)}$
  - compute variable consistency polynomial:
    $g^{Z(s)} = \left(g^{\beta_l l_a(s)+\beta_r r_a(s)+\beta_o o_a(s)}\right)^2 \cdot \left(g^{\beta_r}\right)^3 \cdot \left(g^{\beta_l l_b(s)+\beta_r r_b(s)+\beta_o o_b(s)}\right)^{10} =$
    $g^{\beta_l(2l_a(s)+10l_b(s)) \; + \; \beta_r(2r_a(s)+3+10r_b(s)) \; + \; \beta_o(2o_a(s)+10o_b(s))}$

- verification
  - ... variable values consistency check, should hold:
    $e\left(g^L, g^{\beta_l}\right) \cdot e\left(g^R, g^{\beta_r}\right) \cdot e\left(g^O, g^{\beta_o}\right) = e\left(g^Z, g\right)$

Note: polynomials $o_a(x), l_b(x), r_b(x)$ can actually be disregarded since they are evaluating to 0 for any x, however we preserve those for completeness.

Such ability sabotages the *soundness* of proof. It is clear that encrypted β-s should not be available to a prover.

Non-Malleability

One way to address malleability is to make g^{β_l}, g^{β_r}, g^{β_o} from verification key incompatible with $g^{Z(s)}$ by multiplying them in encrypted space by a random secret γ (gamma) during setup stage: $g^{\beta_l\gamma}$, $g^{\beta_r\gamma}$, $g^{\beta_o\gamma}$. Consecutively such masked encryptions does not allow feasibility to modify $g^{Z(s)}$ in a meaningful way since $Z(s)$ is not a multiple of γ, e.g., $g^{Z(s)} \cdot g^{v' \cdot \beta_l\gamma} = g^{\beta_l(L(s)+ v'\gamma)+\beta_r R(s)+\beta_o O(s)}$. Because a prover does not know the γ the alteration will be random. The modification requires us to balance the variable values consistency check equation in the protocol multiplying $Z(s)$ by γ:

- setup
  - ... sample random $\beta_l, \beta_r, \beta_o, \gamma$
  - ... set verification key: $\left(\ldots, g^{\beta_l\gamma}, g^{\beta_r\gamma}, g^{\beta_o\gamma}, g^{\gamma}\right)$
- proving ...
- verification
  - ... variable values consistency check should hold:
    $e\left(g^L, g^{\beta_l\gamma}\right) \cdot e\left(g^R, g^{\beta_r\gamma}\right) \cdot e\left(g^O, g^{\beta_o\gamma}\right) = e\left(g^Z, g^{\gamma}\right)$

It is important to note that we exclude the case when variable polynomials are of 0-degree (e.g., $l_1(x) = 1x^0$), which otherwise would allow to expose encryptions of β in variable consistency polynomials of proving key $\left\{g^{\beta_l l_i(s)+\beta_r r_i(s)+\beta_o o_i(s)}\right\}_{i\in\{1,\ldots,n\}}$ in case when any two of operands / output is zero, e.g., for $l_1(x) = 1, r_1(s) = 0, o_1(s) = 0$ this will result in $g^{\beta_l l_1(s)+\beta_r r_1(s)+\beta_o o_1(s)} = g^{\beta_l}$.

We could also similarly *mask* the α-s to address the malleability of *variable polynomials*. However it is not necessary since any modification of a *variable polynomial* needs to be reflected in *variable consistency polynomials* which are not possible to modify.

4.9.4 Optimization of Variable Values Consistency Check

The *variable values consistency* check is effective now, but it adds 4 expensive pairing operations and 4 new terms to the verification key. The Pinocchio protocol [Par+13] uses a clever selection of the generators g for each operand *ingraining* the "shifts":

- Setup
  - ... sample random $\beta, \gamma, \rho_l, \rho_r$ and set $\rho_o = \rho_l \cdot \rho_r$
  - set generators $g_l = g^{\rho_l}, g_r = g^{\rho_r}, g_o = g^{\rho_o}$
  - set proving key:
    $\left(\left\{g^{s^k}\right\}_{k\in[d]}, \left\{g_l^{l_i(s)}, g_r^{r_i(s)}, g_o^{o_i(s)}, g_l^{\alpha_l l_i(s)}, g_r^{\alpha_r r_i(s)}, g_o^{\alpha_o o_i(s)}, g_l^{\beta l_i(s)} \cdot g_r^{\beta r_i(s)} \cdot g_o^{\beta o_i(s)}\right\}\right)$
  - set verification key: $\left(g_o^{t(s)}, g^{\alpha_l}, g^{\alpha_r}, g^{\alpha_o}, g^{\beta\gamma}, g^{\gamma}\right)$
- Proving
  - ... assign variable values
    $g^{Z(s)} = \prod_{i=1}^{n} \left(g_l^{\beta l_i(s)} \cdot g_r^{\beta r_i(s)} \cdot g_o^{\beta o_i(s)}\right)^{v_i}$
- Verification
  - ... variable polynomials restriction check:
    $e\left(g_l^{L'}, g\right) = e\left(g_l^{L}, g^{\alpha_l}\right)$, and similarly for g_r^R, g_o^O
  - variable values consistency check:
    $e\left(g_l^L \cdot g_r^R \cdot g_o^O, g^{\beta\gamma}\right) = e\left(g^Z, g^{\gamma}\right)$
  - valid operations check:
    $e\left(g_l^L \cdot g_r^R\right) = e\left(g_o^t, g^h\right) e\left(g_o^O, g\right) \Rightarrow$
    $e\left(g, g\right)^{\rho_l\rho_r LR} = e\left(g, g\right)^{\rho_l\rho_r th+\rho_l\rho_r O}$

Such randomization of the generators further adds to the security making *variable polynomials* malleability, described in remark 4.1, ineffective because for intended change it must be a multiple of either ρ_l, ρ_r or ρ_o, raw or encrypted versions of which are not available (assuming, as

stated previously that we're not dealing with 0-degree variable polynomials which could expose encrypted versions).

The optimization makes verification key two elements smaller and eliminates two pairing operations from the verification step.

Note: there are further protocol improvements in the Jens Groth's 2016 paper [Gro16].

4.10 Constraints

Our analysis has been primarily focusing on the notion of operation. However, the protocol is not actually "computing" but rather is checking that the output value is the correct result of an operation for the operand's values. That is why it is called a constraint, i.e., a verifier is constraining a prover to provide valid values for the predefined "program" no matter what are they. A multitude of constraints is called a *constraint system* (in our case it is a rank 1 constraint system or R1CS).

Note: This implies that one way to find all correct solutions is to perform a brute-force of all possible combinations of values and select only "valid" ones, or use more sophisticated techniques of constraint satisfaction [con18].

Therefore we can also use constraints to ensure other relationships. For example, if we want to make sure that the value of the variable a can only be 0 or 1 (i.e., binary), we can do it with the simple constraint:

$$a \times a = a$$

We can also constrain a to only be 2:

$$(a-2) \times 1 = 0$$

A more complex example is ensuring that number a is a 4-bit number[24], in other words it is possible to represent a with 4 bits. We can also call it "ensuring number range" since a 4-bit number can represent 2^4 combinations, therefore 16 numbers in the range from 0 to 15. In the decimal number system any number can be represented as a sum of powers of the base 10 (as the number of fingers on our hands) with corresponding coefficients, for example, $123 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$. Similarly a binary number can be represented as a sum of powers of base 2 with corresponding coefficients, for example, 1011 (binary) $= 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 =$ 11 (decimal).

Therefore if a is a 4-bit number, then $a = b_3 \cdot 2^3 + b_2 \cdot 2^2 + b_1 \cdot 2^1 + b_0 \cdot 2^0$ for some boolean b_0, b_1, b_2, b_3. The constraint can be following:

$$1: \qquad a \times 1 = 8 \cdot b_3 + 4 \cdot b_2 + 2 \cdot b_1 + 1 \cdot b_0$$

and to ensure that b_0, b_1, b_2, b_3 can only be binary we need to add:

[24] **Also called nibble**.

$$
\begin{aligned}
2: \quad & b_0 \times b_0 = b_0 \\
3: \quad & b_1 \times b_1 = b_1 \\
4: \quad & b_2 \times b_2 = b_2 \\
5: \quad & b_3 \times b_3 = b_3
\end{aligned}
$$

Quite sophisticated constraints can be applied this way, ensuring that the values used are complying with the rules. It is important to note that the above constraint 1 is not possible in the current operation's construction:

$$
\sum_{i=1}^{n} c_{\mathrm{l},i} \cdot v_i \quad \times \quad \sum_{i=1}^{n} c_{\mathrm{r},i} \cdot v_i \quad = \quad \sum_{i=1}^{n} c_{\mathrm{o},i} \cdot v_i
$$

Because the value 1 (and 2 from the previous constraint) has to be expressed through $c \cdot v_{\mathrm{one}}$, where c can be ingrained into the proving key, but the v_{one} may have any value because the prover supplies it. While we can enforce the $c \cdot v$ to be 0 by setting $c = 0$, it is hard to find a constraint to enforce v_{one} to be 1 in the construction we are limited by. Therefore there should be a way for a verifier to set the value of v_{one}.

4.11 Public Inputs and One

The proofs would have limited usability if it were not possible to check them against the verifier's inputs, e.g., knowing that the prover has multiplied two values without knowing what was the result and/or values. While it is possible to "hardwire" the values to check against (e.g., the result of multiplication must always be 12) in the proving key, this would require to generate separate pair of keys for each desired "verifier's input."

Therefore it would be universal if the verifier could specify some of the values (inputs or/and outputs) for the computation, including the v_{one}, instead of the prover.

First, let us consider the proof values $g^{L(s)}, g^{R(s)}, g^{O(s)}$. Because we are using the homomorphic encryption it is possible to augment these values, for example, we can add another encrypted polynomial evaluation $g^{L(s)} \cdot g^{l_v(s)} = g^{L(s)+l_v(s)}$, which means that the verifier could add other variable polynomials to the already provided ones. Therefore if we could exclude necessary variable polynomials from the ones available to the prover, the verifier would be able to set his values on those variables, while the computation check should still match.

It is easy to achieve since the verifier is already constraining the prover in the choice of polynomials he can use empolying the α-shift. Therefore those variable polynomials can be moved from the proving key to the verification key while eliminating its α-s and β checksum counterparts.

The necessary protocol update:

- Setup
  - ...separate all n variable polynomials into two groups:

* verifier's $m+1$:
  $L_v(x) = l_0(x) + l_1(x) + \ldots + l_m$, and alike for $R_v(x)$ and $O_v(x)$,
  where index 0 is reserved for the value of $v_{\text{one}} = 1$

* prover's $n-m$:
  $L_p(x) = l_{m+1}(x) + \ldots + l_n(x)$, and alike for $R_p(x)$ and $O_p(x)$

– set proving key:
$\left(\left\{ g^{s^k} \right\}_{k \in [d]}, \left\{ g_l^{l_i(s)}, g_r^{r_i(s)}, g_o^{o_i(s)}, g_l^{\alpha_l l_i(s)}, g_r^{\alpha_r r_i(s)}, g_o^{\alpha_o o_i(s)}, g_l^{\beta l_i(s)} \cdot g_r^{\beta r_i(s)} \cdot g_o^{\beta o_i(s)} \right\}_{i \in \{m+1,\ldots,n\}} \right)$

– add to the verification key:
$\left(\ldots, \left\{ g_l^{l_i(s)}, g_r^{r_i(s)}, g_o^{o_i(s)} \right\}_{i \in \{0,\ldots,m\}} \right)$

- Proving

  – ... calculate $h(x)$ accounting for the verifier's polynomials: $h(x) = \dfrac{L(x) \cdot R(x) - O(x)}{t(x)}$,
  where $L(x) = L_v(x) + L_p(x)$, and similarly for $R(x), O(x)$

  – provide the proof:
  $\left(g_l^{L_p(s)}, g_r^{R_p(s)}, g_o^{O_p(s)}, g_l^{\alpha_l L_p(s)}, g_r^{\alpha_r R_p(s)}, g_o^{\alpha_o O_p(s)}, g^{Z(s)}, g^{h(s)} \right)$

- Verification

  – assign verifier's variable polynomial values and add to 1:
  $g_l^{L_v(s)} = g_l^{l_0(s)} \cdot \prod_{i=1}^{m} \left(g_l^{l_i(s)} \right)^{v_i}$

  and similarly for $g_r^{R_v(s)}$ and $g_o^{O_v(s)}$

  – variable polynomials restriction check:
  $e\left(g_l^{L_p}, g^{\alpha_l} \right) = e\left(g_l^{L'_p}, g \right)$ and similarly for $g_r^{R_p}$ and $g_o^{O_p}$

  – variable values consistency check:
  $e\left(g_l^{L_p} g_r^{R_p} g_o^{O_p}, g^{\beta\gamma} \right) = e\left(g^Z, g^\gamma \right)$

  – valid operations check:
  $e\left(g_l^{L_v(s)} g_l^{L_p}, g_r^{R_v(s)} g_r^{R_p} \right) = e\left(g_o^t, g^h \right) \cdot e\left(g_o^{O_v(s)} g_o^{O_p}, g \right)$

Note: following from the protocol properties (section 4.6.1) the 1 *represented by polynomials* $l_0(x), r_0(x), o_0(x)$ *already have appropriate values at the corresponding operations and therefore needs no assignment.*

Note: verifier will have to do extra work on the verification step, which is proportionate to the number of variables he assigns.

Effectively this is taking some variables from the prover into the hands of verifier while still preserving the balance of the equation. Therefore the *valid operations* check should still hold, but only if the prover has used the same values that the verifier used for his input.

The value of 1 is essential and allows to derive any number[25] through multiplication by a constant term, for example, to multiply a by 123:

$$1 \cdot a \quad \times \quad 123 \cdot v_{\text{one}} \quad = \quad 1 \cdot r$$

4.12 Zero-Knowledge Proof of Computation

Since the introduction of the general-purpose computation protocol (section 4.4 proof of operation) we had to let go of the *zero-knowledge* property, to make the transition simpler. Until this point, we have constructed a verifiable computation protocol.

Previously to make a proof of polynomial *zero-knowledge* we have used the random δ-shift, which makes the proof indistinguishable from random (section 3.5):

$$\delta p(s) = t(s) \cdot \delta h(s)$$

With the computation we are proving instead that:

$$L(s) \cdot R(s) - O(s) = t(s)h(s)$$

While we could just adapt this approach to the multiple polynomials using same δ, i.e., supplying randomized values $\delta L(s), \delta R(s), \delta^2 O(s), \delta^2 h(s)$, which would satisfy the valid operations check through pairings:

$$e\left(g,g\right)^{\delta^2 L(s)R(s)} = e(g,g)^{\delta^2(t(s)h(s)+O(s))}$$

The issue is that having same δ hinders security, because we provide those values separately in the proof:

- one could easily identify if two different polynomial evaluations have same value (e.g., $g^{\delta L(s)} = g^{\delta R(s)}$, etc.), i.e., learning some knowledge
- potential insignificance of differences of values between $L(s)$ and $R(s)$ could allow factoring of those differences through brute-force, for example if $L(s) = 5R(s)$, iterating check $g^{L(s)} = \left(g^{R(s)}\right)^i$, for $i \in \{1...N\}$ would reveal the $5\times$ difference in just 5 steps. Same brute-force can be performed on encrypted addition operation, e.g., $g^{L(s)} = g^{R(s)+5}$
- other correlations between elements of the proof may be discovered, e.g., if $e(g^{\delta L(s)}, g^{\delta R(s)}) = e(g^{\delta^2 O(s)}, g)$ then $L(x) \cdot R(x) = O(x)$, etc.

Note: the optimization 4.9.4 makes such data mining harder but still allows to discover relationships, apart from the fact that verifier can choose ρ_l, ρ_r in a particular way that can facilitate revealing of knowledge[26].

Consequently, we need to have different randomness (δ-s) for each polynomial evaluation, e.g.:

$$\delta_l L(s) \cdot \delta_r R(s) - \delta_o O(s) = t(s) \cdot (\Delta \oslash h(s))$$

To resolve inequality on the right side, we can only modify the proof's value $h(s)$, without alteration of the protocol which would be preferable. Delta (Δ) here represents the difference we

[25] In the chosen finite field

[26] As long as it is not a diversified setup

need to apply to $h(s)$ in order to counterbalance the randomness on the other side of the equation and ⍰ represents either multiplication or addition operation (which in turn accommodates division and subtraction). If we chose to apply Δ through multiplication ($⍰ = \times$) this would mean that it is impossible to find Δ with overwhelming probability, because of randomization:

$$\Delta = \frac{\delta_l L(s) \cdot \delta_r R(s) - \delta_o O(s)}{t(s)h(s)}$$

We could set $\delta_o = \delta_l \cdot \delta_r$, which transforms into:

$$\Delta = \frac{\delta_l \delta_r (L(s) \cdot R(s) - O(s))}{t(s)h(s)} = \delta_l \delta_r$$

However, as noted previously this hinders the zero-knowledge property, and even more importantly such construction will not accommodate the verifier's input polynomials since they must be multiples of the corresponding δ-s, which would require an interaction.

We can try adding randomness to the evaluations:

$$(L(s) + \delta_l) \cdot (R(s) + \delta_r) - (O(s) + \delta_o) = t(s) \cdot (\Delta \times h(s))$$

$$\Delta = \frac{\overbrace{L(s)R(s) - O(s)}^{t(s)h(s)} + \delta_r L(s) + \delta_l R(s) + \delta_l \delta_r - \delta_o}{t(s)h(s)} = 1 + \frac{\delta_r L(s) + \delta_l R(s) + \delta_l \delta_r - \delta_o}{t(s)h(s)}$$

However due to randomness it is non-divisible. Even if we address this by multiplying each δ with $t(s)h(s)$, because we apply Δ through multiplication of $h(s)$, and Δ will consist of encrypted evaluations (i.e., $g^{L(s)}$, etc.) it will not be possible to compute $g^{\Delta h(s)}$ without use of pairings (result of which is in another number space). Likewise computation is not possible through encrypted evaluation of $\Delta h(x)$ using encrypted powers $\left\{g^{s^i}\right\}_{i \in [d]}$, because the degree of $h(x)$ and Δ is d, hence the degree of $\Delta h(x)$ is up to $2d$. Moreover, it is not possible to compute such randomized operand polynomial evaluation $g^{L(s)+\delta_l t(s)h(s)}$ for the same reason.

Therefore we should try applying Δ through addition ($⍰ = +$), since it is available for homomorphically encrypted values.

$$(L(s) + \delta_l) \cdot (R(s) + \delta_r) - (O(s) + \delta_o) = t(s) \cdot (\Delta + h(s))$$

$$\Delta = \frac{L(s)R(s) - O(s) + \delta_r L(s) + \delta_l R(s) + \delta_l \delta_r - \delta_o - t(s)h(s)}{t(s)} \Rightarrow$$

$$\Delta = \frac{\delta_r L(s) + \delta_l R(s) + \delta_l \delta_r - \delta_o}{t(s)}$$

Every term in the numerator is a multiple of a δ, therefore we can make it divisible by multiplying each δ with $t(s)$:

$$(L(s) + \delta_l t(s)) \cdot (R(s) + \delta_r t(s)) - (O(s) + \delta_o t(s)) = t(s) \cdot (\Delta + h(s))$$

$$\cancel{L(s)R(s) - O(s)} + t(s)(\delta_r L(s) + \delta_l R(s) + \delta_l \delta_r t(s) - \delta_o) = t(s)\Delta + \cancel{t(s)h(s)}$$

$$\Delta = \delta_r L(s) + \delta_l R(s) + \delta_l \delta_r t(s) - \delta_o$$

Which we can efficiently compute in the encrypted space:

$$g^{L(s)+\delta_l t(s)} = g^{L(s)} \cdot \left(g^{t(s)}\right)^{\delta_l} \quad , \quad \text{etc.}$$

$$g^{\Delta} = \left(g^{L(s)}\right)^{\delta_r} \cdot \left(g^{R(s)}\right)^{\delta_l} \cdot \left(g^{t(s)}\right)^{\delta_l \delta_r} g^{-\delta_o}$$

This leads to passing of *valid operations* check while concealing the encrypted values.

$$L \cdot R - O + t(\delta_r L + \delta_l R + \delta_l \delta_r t - \delta_o) = t(s)h + t(s)(\delta_r L + \delta_l R + \delta_l \delta_r t - \delta_o)$$

The construction is statistically *zero-knowledge* due to addition of uniformly random multiples of $\delta_l, \delta_r, \delta_o$ (see theorem 13 of [Gen+12]).

Note: this approach is also consistent with the verifier's operands, e.g., $g_l^{L_p+\delta_l t} \cdot g_l^{L_v} = g_l^{L_p+L_v+\delta_l t}$*, therefore the valid operations check holds but still only if the prover have used verifier's values to construct the proof (i.e.,* $\Delta = \delta_r(L_p + L_v) + \delta_l(R_p + R_v) + \delta_l \delta_r t - \delta_o$*), see next section for more details.*

To make the "variable polynomials restriction" and "variable values consistency" checks coherent with the *zero-knowledge* alterations, it is necessary to add the following parameters to the proving key:

$$g_l^{t(s)}, g_r^{t(s)}, g_o^{t(s)}, g_l^{\alpha_l t(s)}, g_r^{\alpha_r t(s)}, g_o^{\alpha_o t(s)}, g_l^{\beta t(s)}, g_r^{\beta t(s)}, g_o^{\beta t(s)}$$

It is quite curious that the original Pinocchio protocol [Par+13] was concerned primarily with the verifiable computation and less with the *zero-knowledge* property, which is a minor modification and comes almost *for free*.

4.13 zk-SNARK Protocol

Considering all the gradual improvements the final zero-knowledge succinct non-interactive arguments of knowledge protocol is (the *zero-knowledge* components are optional and highlighted with a different color):

- Setup
  - select a generator g and a cryptographic pairing e
  - for a function $f(u) = y$ with n total variables of which m are input/output variables, convert into the polynomial form[27] $\left(\{l_i(x), r_i(x), o_i(x)\}_{i\in\{0,\dots,n\}}, t(x)\right)$ of degree d (equal to the number of operations) and size $n+1$
  - sample random $s, \rho_l, \rho_r, \alpha_l, \alpha_r, \alpha_o, \beta, \gamma$
  - set $\rho_o = \rho_l \cdot \rho_r$ and the operand generators $g_l = g^{\rho_l}, g_r = g^{\rho_r}, g_o = g^{\rho_o}$

[27] A quadratic arithmetic program

- set the proving key:

$$\Bigg(\left\{g^{s^k}\right\}_{k\in[d]}, \left\{g_l^{l_i(s)}, g_r^{r_i(s)}, g_o^{o_i(s)}\right\}_{i\in\{0,\ldots,n\}},$$
$$\left\{g_l^{\alpha_l l_i(s)}, g_r^{\alpha_r r_i(s)}, g_o^{\alpha_o o_i(s)}, g_l^{\beta l_i(s)} g_r^{\beta r_i(s)} g_o^{\beta o_i(s)}\right\}_{i\in\{m+1,\ldots,n\}},$$
$$g_l^{t(s)}, g_r^{t(s)}, g_o^{t(s)}, g_l^{\alpha_l t(s)}, g_r^{\alpha_r t(s)}, g_o^{\alpha_o t(s)}, g_l^{\beta t(s)}, g_r^{\beta t(s)}, g_o^{\beta t(s)} \Bigg)$$

- set the verification key:

$$\left(g^1, g_o^{t(s)}, \left\{g_l^{l_i(s)}, g_r^{r_i(s)}, g_o^{o_i(s)}\right\}_{i\in\{0,\ldots,m\}}, g^{\alpha_l}, g^{\alpha_r}, g^{\alpha_o}, g^{\gamma}, g^{\beta\gamma}\right)$$

- Proving
  - for the input u, execute the computation of $f(u)$ obtaining values $\{v_i\}_{i\in\{m+1,\ldots,n\}}$ for all the itermediary variables
  - assign all values to the unencrypted variable polynomials $L(x) = l_0(x) + \sum_{i=1}^{n} v_i \cdot l_i(x)$ and similarly $R(x), O(x)$
  - sample random δ_l, δ_r and δ_o
  - find $h(x) = \dfrac{L(x)R(x) - O(x)}{t(x)} + \delta_r L(x) + \delta_l R(x) + \delta_l\delta_r t(x) - \delta_o$
  - assign the prover's variable values to the encrypted variable polynomials and apply *zero-knowledge* δ-shift $g_l^{L_p(s)} = \left(g_l^{t(s)}\right)^{\delta_l} \cdot \prod_{i=m+1}^{n} \left(g_l^{l_i(s)}\right)^{v_i}$ and similarly $g_r^{R_p(s)}$, $g_o^{O_p(s)}$
  - assign its α-shifted pairs $g_l^{L'_p(s)} = \left(g_l^{\alpha_l t(s)}\right)^{\delta_l} \cdot \prod_{i=m+1}^{n} \left(g_l^{\alpha_l l_i(s)}\right)^{v_i}$ and similarly $g_r^{R'_p(s)}$, $g_o^{O'_p(s)}$
  - assign the variable values consistency polynomials

$$g^{Z(s)} = \left(g_l^{\beta t(s)}\right)^{\delta_l} \left(g_r^{\beta t(s)}\right)^{\delta_r} \left(g_o^{\beta t(s)}\right)^{\delta_o} \cdot \prod_{i=m+1}^{n} \left(g_l^{\beta l_i(s)} g_r^{\beta r_i(s)} g_o^{\beta o_i(s)}\right)^{v_i}$$

  - compute the proof $\left(g_l^{L_p(s)}, g_r^{R_p(s)}, g_o^{O_p(s)}, g^{h(s)}, g_l^{L'_p(s)}, g_r^{R'_p(s)}, g_o^{O'_p(s)}, g^{Z(s)}\right)$
- Verification
  - parse a provided proof as $\left(g_l^{L_p}, g_r^{R_p}, g_o^{O_p}, g^h, g_l^{L'_p}, g_r^{R'_p}, g_o^{O'_p}, g^Z\right)$
  - assign input/output values to verifier's encrypted polynomials and add to 1: $g_l^{L_v(s)} = g_l^{l_0(s)} \cdot \prod_{i=1}^{m} \left(g_l^{l_i(s)}\right)^{v_i}$ and similarly for $g_r^{R_v(s)}$ and $g_o^{O_v(s)}$
  - variable polynomials restriction check : $e\left(g_l^{L_p}, g^{\alpha_l}\right) = e\left(g_l^{L'_p}, g\right)$ and similarly for $g_r^{R_p}$ and $g_o^{O_p}$
  - variable values consistency check: $e\left(g_l^{L_p} g_r^{R_p} g_o^{O_p}, g^{\beta\gamma}\right) = e\left(g^Z, g^{\gamma}\right)$

– valid operations check:
$e\left(g_l^{L_p} g_l^{L_v(s)}, g_r^{R_p} g_r^{R_v(s)}\right) = e\left(g_o^{t(s)}, g^h\right) \cdot e\left(g_o^{O_p} g_o^{O_v(s)}, g\right)$

5 Conclusions

We ended up with an effective protocol which allows proving computation:

- succinctly — independently from the amount of computation the proof is of constant, small size
- non-interactively — as soon as the proof is computed it can be used to convince any number of verifiers without direct interaction with the prover
- with argumented knowledge — the statement is correct with non-negligible probability, i.e., fake proofs are infeasible to construct
- in *zero-knowledge* — it is "hard" to extract any knowledge from the proof, i.e., it is indistinguishable from random

It was possible to achieve primary due to unique properties of polynomials, modular arithmetic, homomorphic encryption, elliptic curve cryptography, cryptographic pairings and ingenuity of the inventors.

This protocol proves computation of a unique finite execution machine which in one operation can add together almost any number of variables but may only perform one multiplication. Therefore there is an opportunity to both optimize programs to leverage this specificity efficiently as well as use constructions which minimize the number of operations.

It is essential that verifier does not have to know any secret data in order to verify a proof so that properly constructed verification key can be published and used by anyone in a non-interactive manner. Which is contrary to the "designated verifier" schemes where the proof will convince only one party, therefore it is non-transferable. In *zk-SNARK* context, we can achieve this property if untrustworthy or a single party generates the keypair.

The field of zero-knowledge proof constructions is continuously evolving, introducing optimizations ([Ben+13; Gro16; GM17]), improvements such as updatable proving and verification keys ([Gro+18]), and new constructions (Bulletproofs [Bün+17], ZK-STARK [Ben+18], Sonic [Mal+19]).

6 Disclaimer

This work does not focus on exhaustive formal security proofs which can be found in original papers (see references).

The explanation is opinionated by the author and is the result of his best guess which may not reflect the exact true story of the protocol.

7 References

[Bit+11] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer. *From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again*. Cryptology ePrint Archive, Report 2011/443. `https://eprint.iacr.org/2011/443`. 2011.

[Par+13] Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova. *Pinocchio: Nearly Practical Verifiable Computation*. Cryptology ePrint Archive, Report 2013/279. `https://eprint.iacr.org/2013/279`. 2013.

[Rei16] Christian Reitwiessner. *zkSNARKs in a Nutshell*. 2016. URL: `https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/` (visited on 2018-05-01).

[But16] Vitalik Buterin. *Quadratic Arithmetic Programs: from Zero to Hero*. 2016. URL: `https://medium.com/@VitalikButerin/quadratic-arithmetic-programs-from-zero-to-hero-f6d558cea649` (visited on 2018-05-01).

[But17] Vitalik Buterin. *zk-SNARKs: Under the Hood*. 2017. URL: `https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6` (visited on 2018-05-01).

[Gab17] Ariel Gabizon. *Explaining SNARKs*. 2017. URL: `https://z.cash/blog/snark-explain/` (visited on 2018-05-01).

[Ben+14] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. *Zerocash: Decentralized Anonymous Payments from Bitcoin*. Cryptology ePrint Archive, Report 2014/349. `https://eprint.iacr.org/2014/349`. 2014.

[GMR85] S Goldwasser, S Micali, and C Rackoff. "The Knowledge Complexity of Interactive Proof-systems". In: *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*. STOC '85. Providence, Rhode Island, USA: ACM, 1985, pp. 291–304. ISBN: 0-89791-151-2. DOI: `10.1145/22145.22178`. URL: `http://doi.acm.org/10.1145/22145.22178`.

[BFM88] Manuel Blum, Paul Feldman, and Silvio Micali. "Non-interactive Zero-knowledge and Its Applications". In: *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. STOC '88. Chicago, Illinois, USA: ACM, 1988, pp. 103–112. ISBN: 0-89791-264-0. DOI: `10.1145/62212.62222`. URL: `http://doi.acm.org/10.1145/62212.62222`.

[Gro10] Jens Groth. "Short pairing-based non-interactive zero-knowledge arguments". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2010, pp. 321–340.

[Gen+12] Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. *Quadratic Span Programs and Succinct NIZKs without PCPs*. Cryptology ePrint Archive, Report 2012/215. `https://eprint.iacr.org/2012/215`. 2012.

[Pik13] Scott Pike. *Evaluating Polynomial Functions*. 2013. URL: `http://www.mesacc.edu/~scotz47781/mat120/notes/polynomials/evaluating/evaluating.html` (visited on 2018-05-01).

[Pik14] Scott Pike. *Dividing by a Polynomial*. 2014. URL: http://www.mesacc.edu/~scotz47781/mat120/notes/divide_poly/long_division/long_division.html (visited on 2018-05-01).

[Dam91] Ivan Damgård. "Towards practical public key systems secure against chosen ciphertext attacks". In: *Annual International Cryptology Conference*. Springer. 1991, pp. 445–456.

[JSI96] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. "Designated verifier proofs and their applications". In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 1996, pp. 143–154.

[DBS04] Ratna Dutta, Rana Barua, and Palash Sarkar. *Pairing-Based Cryptographic Protocols: A Survey*. Cryptology ePrint Archive, Report 2004/064. https://eprint.iacr.org/2004/064. 2004.

[DK18] Apoorvaa Deshpande and Yael Kalai. *Proofs of Ignorance and Applications to 2-Message Witness Hiding*. Cryptology ePrint Archive, Report 2018/896. https://eprint.iacr.org/2018/896. 2018.

[Wil16] Zooko Wilcox. *The Design of the Ceremony*. 2016. URL: https://z.cash/blog/the-design-of-the-ceremony/ (visited on 2018-05-01).

[Gro16] Jens Groth. *On the Size of Pairing-based Non-interactive Arguments*. Cryptology ePrint Archive, Report 2016/260. https://eprint.iacr.org/2016/260. 2016.

[con18] Wikipedia contributors. *Constraint satisfaction*. Wikipedia, The Free Encyclopedia. 2018. (Visited on 2018-08-05).

[Ben+13] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. *Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture*. Cryptology ePrint Archive, Report 2013/879. https://eprint.iacr.org/2013/879. 2013.

[GM17] Jens Groth and Mary Maller. *Snarky Signatures: Minimal Signatures of Knowledge from Simulation-Extractable SNARKs*. Cryptology ePrint Archive, Report 2017/540. https://eprint.iacr.org/2017/540. 2017.

[Gro+18] Jens Groth, Markulf Kohlweiss, Mary Maller, Sarah Meiklejohn, and Ian Miers. *Updatable and Universal Common Reference Strings with Applications to zk-SNARKs*. Cryptology ePrint Archive, Report 2018/280. https://eprint.iacr.org/2018/280. 2018.

[Bün+17] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. *Bulletproofs: Short Proofs for Confidential Transactions and More*. Cryptology ePrint Archive, Report 2017/1066. https://eprint.iacr.org/2017/1066. 2017.

[Ben+18] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. *Scalable, transparent, and post-quantum secure computational integrity*. Cryptology ePrint Archive, Report 2018/046. https://eprint.iacr.org/2018/046. 2018.

[Mal+19] Mary Maller, Sean Bowe, Markulf Kohlweiss, and Sarah Meiklejohn. *Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updateable Structured Reference Strings*. Cryptology ePrint Archive, Report 2019/099. https://eprint.iacr.org/2019/099. 2019.