Formalising Groth16 in Lean 4

Daniel Rogozin, for Yatima Inc

August 14, 2022*

In this document, we describe the Groth16 soundness formalisation in Lean 4. The text contains the protocol description as well as some comments to its implementation.

1 Preliminary definitions

We have a fixed finite field F, and $F[X]$ stands for the ring of polynomials over F as usual. The corresponding listing:

```
variable {F : Type u} [field : Field F]
```

In Groth16, we have random values $\alpha, \beta, \gamma, \delta \in F$ that we introduce separately as an inductive data type:

```
inductive Vars : Type
  | alpha : Vars
  | beta : Vars
  | gamma : Vars
  | delta : Vars
```

We also introduce the following parameters:

- $n_{stmt} \in \mathbb{N}$ — the statement size;
- $n_{wit} \in \mathbb{N}$ — the witness size;
- $n_{var} \in \mathbb{N}$ — the number of variables.

In Lean 4, we introduce those parameters as variables in the following way:

```
variable {n_stmt n_wit n_var : Nat}
```

We also define several finite collections of polynomials:

- $u_{stmt} = \{f_i \in F[X] \mid i < n_{stmt}\}$
- $u_{wit} = \{f_i \in F[X] \mid i < n_{wit}\}$
- $v_{stmt} = \{f_i \in F[X] \mid i < n_{stmt}\}$
- $v_{wit} = \{f_i \in F[X] \mid i < n_{wit}\}$
- $w_{stmt} = \{f_i \in F[X] \mid i < n_{stmt}\}$
- $w_{wit} = \{f_i \in F[X] \mid i < n_{wit}\}$

We introduce those collections in Lean 4 as variables as well:

*This document may be updated frequently.

```
variable {u_stmt : Fin n_stmt -> F[X]}
variable {u_wit : Fin n_wit -> F[X]}
variable {v_stmt : Fin n_stmt -> F[X]}
variable {v_wit : Fin n_wit -> F[X]}
variable {w_stmt : Fin n_stmt -> F[X]}
variable {w_wit : Fin n_wit -> F[X]}
```

Let $(r_i)_{i<n_{wit}}$ be a collection of elements of F (that is, each $r_i \in F$) parametrised by elements of n_{wit}. Define a polynomial $t \in F[X]$ as:

$$t = \prod_{i \in n_{wit}} (x - r_i).$$

Crearly, these r_i's are roots of t. The definition in Lean 4:

```
variable (r : Fin n_wit -> F)

def t : F[X] := Pi i in finRange n_wit,
  (x : F[X]) - Polynomial.c (r i)
```

2 Properties of t

The polynomial t has the following properties:

Lemma 1.

1. *$deg(t) = n_{wit}$;*
2. *t is monic, that is, its leading coefficient is equal to 0;*
3. *If $n_{wit} > 0$, then $deg(t) > 0$.*

We formalise these statements as follows (but we drop proofs):

```
lemma nat_degree_t : (t r).natDegree = n_wit
lemma monic_t : Polynomial.Monic (t r)
lemma degree_t_pos (hm : 0 < n_wit) : 0 < (t r).degree
```