Poseidon2 测试验证数学规范

1 测试验证数学模型

1.1 测试用例定义

给定输入输出对集合：

$$\mathcal{T} = \left\{(x_i, y_i) \mid x_i \in \mathbb{F}_p^t, y_i = \text{Poseidon2}(x_i)\right\}_{i=1}^{k}$$

其中：

- $x_i = [x_{i0}, x_{i1}, x_{i2}]$（当 $t = 3$ 时）
- $y_i \in \mathbb{F}_p$ 为理论哈希值

2 见证验证过程

2.1 见证生成算法

对于每个测试用例 (x_i, y_i)，见证生成函数：

$$W(x_i) = w_i \in \mathbb{F}_p^m \quad \text{满足} \quad \Phi(x_i, w_i) = 0$$

其中 Φ 为 R1CS 约束系统：

$$\begin{cases} A \cdot s_i \circ B \cdot s_i = C \cdot s_i \\ s_i = (1, x_i, w_i) \in \mathbb{F}_p^{n+1} \end{cases}$$

2.2 正确性条件

$$\text{测试通过} \iff \forall i, (\text{Circuit}(x_i) = y_i) \wedge (\text{Verify}(\text{vk}, y_i, \pi_i) = 1)$$

3 自动化测试协议

Algorithm 1 测试验证流程

初始化测试集 $\mathcal{T} \leftarrow \{(x_1, y_1), \ldots, (x_k, y_k)\}$
for each $(x_i, y_i) \in \mathcal{T}$ **do**
    计算见证 $w_i \leftarrow \text{WitnessCalc}(x_i)$
    生成证明 $\pi_i \leftarrow \text{Groth16.Prove}(x_i, w_i)$
    电路输出 $y_i' \leftarrow \text{Circuit}(x_i)$
    if $y_i' \neq y_i$ **or** $\text{Verify}(vk, y_i', \pi_i) \neq 1$ **then**
        return " 测试失败"
    end if
end for
return " 所有测试通过"

4 安全性分析

4.1 完备性

$$\Pr\left[\text{测试通过} \mid \text{电路正确}\right] = 1$$

4.2 可靠性

对于错误电路：

$$\Pr\left[\text{测试通过} \mid \exists (x_i, y_i) \text{不匹配}\right] \leq \text{negl}(\lambda)$$

输入 x	预期输出 y（示例值）
$[0,0,0]$	$0x2a09e9...$
$[1,2,3]$	$0x1f3a8d...$
$[2^{32}-1,0,1]$	$0x7c4b21...$

表 1: Poseidon2 标准测试用例

5 Poseidon2 测试参数

5.1 标准测试向量

5.2 边界条件

$$\begin{aligned}&\text{空输入测试}: x = [] \ \text{（需填充为零值）}\\&\text{大整数测试}: x_i = p-1\\&\text{随机性测试}: x \xleftarrow{\$} \mathbb{F}_p^t\end{aligned}$$

6 实现验证

6.1 Wasm 见证生成

$$\text{Witness} = \begin{pmatrix}\text{输入层}\\ \text{S-box 中间值}\\ \text{线性层输出}\\ \text{最终哈希}\end{pmatrix} \in \mathbb{F}_p^{3t+R_F+R_P}$$

6.2 约束检查

对每个约束 $j \in [1, C_{\text{总}}]$ 验证：

$$\langle A_j, s\rangle \cdot \langle B_j, s\rangle \stackrel{?}{=} \langle C_j, s\rangle$$