

PROOF OF LEMMA 1

DAVID BRUST AND JOHANNES J. BRUST

PROOF OF LEMMA 1 ($d = 2$, AND $q = p$ (PRIME))

Designs with $d = 2$ and $q = p$ (prime order), use modulus arithmetic and lines and may therefore be regarded to be simpler than more general polynomial constructions. Thus we provide a proof of Lemma 1 in this situation in order to motivate the underlying computations.

Similar like in the main text, suppose that $1 \leq k < p$ and let $j \neq i$. Select an arbitrary pair of samples $\{(x_i, y_{x_i}); (x_j, y_{x_j})\}$, computed using, say, a and b . Consider the different slope $\bar{a} \neq a$ and intercept $\underline{b} \neq b$. There are four possibilities to generate pools in PP, and consequently pairs of samples other than a base pair

Base: Slope and intercept given	a, b with $\{(x_i, y_{x_i}); (x_j, y_{x_j})\}$
Case 1: Slope differs	\bar{a}, b with $\{(x_i, \bar{y}_{x_i}); (x_j, \bar{y}_{x_j})\}$
Case 2: Intercept differs	a, \underline{b} with $\{(x_i, \underline{y}_{x_i}); (x_j, \underline{y}_{x_j})\}$
Case 3: Slope and intercept differ	\bar{a}, \underline{b} with $\{(x_i, \bar{\underline{y}}_i); (x_j, \bar{\underline{y}}_j)\}$
Case 4: Slope at infinity	$\bar{a} = q$ with $\{(x_i^\infty, y_i^\infty); (x_j^\infty, y_j^\infty)\}$

Next we analyze how the pairs in each of the four cases compare to the base pair $\{(x_i, y_{x_i}); (x_j, y_{x_j})\}$. We use $y^+ \in \{\bar{y}, \underline{y}, \bar{\underline{y}}\}$ to represent a y value from one of the Cases 1-3. Note that the conditions for having different pairs of samples in these cases are

$$(1) \quad \text{if } y_{x_i} = y_{x_i}^+ \text{ then } y_{x_j} \neq y_{x_j}^+, \quad \text{or} \quad \text{if } y_{x_j} = y_{x_j}^+ \text{ then } y_{x_i} \neq y_{x_i}^+$$

For $d = 2$ the lines $y = (ax+b) \bmod p$ generate the different pools, which we use to evaluate condition (1). Moreover, with $d = 2$, the indices simplify to $i_{d-1} = i_1 = i$ and $x_i = i, x_j = j$.

Proof. Case 1: Only the slope \bar{a} differs and we use the notation $y^+ = \bar{y}$. From the equation of a line and from (1)

$$y_{x_k} - \bar{y}_{x_k} = 0 \quad \text{implies} \quad ((a - \bar{a})x_k) \bmod p = 0 \quad \text{and} \quad x_k = 0, \quad k \in \{i, j\}$$

Since $x_k = k \neq x_t = t$ for $t \neq k \in \{i, j\}$ we see that

$$\text{if } y_{x_k} = \bar{y}_{x_k} \text{ then } x_k = 0, x_t > 0, \quad y_{x_t} - \bar{y}_{x_t} = ((a - \bar{a})x_t) \bmod p \neq 0 \quad t \neq k \in \{i, j\}$$

Therefore, we conclude that $y_{x_j} \neq \bar{y}_{x_j}$ when $y_{x_i} = \bar{y}_{x_i}$ and similarly for the reverse $y_{x_i} \neq \bar{y}_{x_i}$ when $y_{x_j} = \bar{y}_{x_j}$. This means that pairs of samples do not co-occur when pools are generated in case 1.

Case 2: Only the intercept \underline{b} differs and $y^+ = \underline{y}$. Note that

$$y_{x_k} - \underline{y}_{x_k} = (b - \underline{b}) \bmod p \neq 0, \quad k \in \{i, j\}$$

Therefore $y_{x_i} \neq \underline{y}_{x_i}$ and $y_{x_j} \neq \underline{y}_{x_j}$ and all samples and corresponding pairs are different in this case.

Case 3: Both slope \bar{a} and intercept \underline{b} differ and we denote $y^+ = \bar{y}$. Using condition (1) one finds that

$$y_{x_k} - \bar{y}_{x_k} = 0 \quad \text{implies} \quad ((a - \bar{a})x_k + (b - \underline{b})) \bmod p = 0, \quad k \in \{i, j\}$$

which means that

$$y_{x_k} - \bar{y}_{x_k} = 0 \quad \text{implies} \quad ((a - \bar{a})x_k) \bmod p = -(b - \underline{b}) \bmod p, \quad k \in \{i, j\}$$

Therefore, for $k = x_k \neq x_t = t$ when $t \neq k \in \{i, j\}$ it holds that

$$\begin{aligned} \text{if } y_{x_k} = \bar{y}_{x_k} \text{ then } y_{x_t} - \bar{y}_{x_t} &= ((a - \bar{a})x_t + (b - \underline{b})) \bmod p \\ &= ((a - \bar{a})x_t - (a - \bar{a})x_k) \bmod p \\ &= ((a - \bar{a})(x_t - x_k)) \bmod p \\ &\neq 0, \quad k \in \{i, j\} \end{aligned}$$

The final equality holds because $a \neq \bar{a}$ and $x_t \neq x_k$, $t \neq k \in \{i, j\}$ by definition.

Case 4: With slope of ‘‘infinity’’ $\in \mathbb{F}_p$ a pool of samples is computed with a special formula. Specifically, a pool (with $d = 2$) with this slope is defined to have $x_i^\infty = \sum_{l=2}^{2-1} p^{d-1-l} i_l + q^{2-2} b = b = x_j^\infty = b$ and

$$\{(x_i^\infty, y_i^\infty); (x_j^\infty, y_j^\infty)\} = \{(b, y_i^\infty); (b, y_j^\infty)\}.$$

Since $x_k \neq x_t$ for $k \neq t \in \{i, j\}$ (by definition) we note that if $x_k = b = x_k^\infty$ and $y_{x_k} = y_k^\infty$ then $x_t \neq x_t^\infty = x_k = b$. Thus no pairs occur more than once with the pools from slopes $a < q$ and $a = q$. Therefore, we conclude from the four cases that pairs occur jointly $d - 1 = 1$ times for all slopes $a \leq p$. \square