Let $p \equiv 1 \bmod 3$. Let $F(X) = X^{\frac{p+1}{2}} + aX^{\frac{p+5}{6}} + bX$ be a polynomial over $\mathbb{F}_p$. Let α be a primitive root in $\mathbb{F}_p$.
Notice that $F(X) = X(X^{\frac{p-1}{2}} + aX^{\frac{p-1}{6}} + b)$. We will use the approach of considering the $\alpha^{6k+r}, r = 0, ..., 5$. This divides $F(X)$ into 6 classes:

- $F(\alpha^{6k}) = \alpha^{6k}(1 + a + b)$
- $F(\alpha^{6k+1}) = \alpha^{6k+1}(-1 + a\alpha^{\frac{p-1}{6}} + b)$
- $F(\alpha^{6k+2}) = \alpha^{6k+2}(1 + a\alpha^{\frac{p-1}{3}} + b)$
- $F(\alpha^{6k+3}) = \alpha^{6k+3}(-1 - a + b)$
- $F(\alpha^{6k+4}) = \alpha^{6k+4}(1 + a\alpha^{2\frac{p-1}{3}} + b)$
- $F(\alpha^{6k+5}) = \alpha^{6k+5}(-1 + a\alpha^{5\frac{p-1}{6}} + b)$

1 Lemas for PP

Note that in order for $F(X)$ to be a PP, these 6 "classes" should be disjoint. This is $F(\alpha^{6k+r}) \neq F(\alpha^{6l+s})$ where $k, l < \frac{p-1}{6}$, $r, s < 6$, and $r \neq s$. We want to find the necessary conditions on a and b such that this occurs.

Lemma 1 (Lemma 1:). *Let $F(X)$ be defined as above. In order for $F(X)$ to be a Permutation Polynomial, a and b can NOT satisfy any of the following equalities:*

Class $6k$

- Class $6l + 1$

  $\alpha^{6k}(1 + a + b) = \alpha^{6l+1}(-1 + a\alpha^{\frac{p-1}{6}} + b)$

  $\alpha^{6(k-l)}(1 + a + b) = \alpha(-1 + a\alpha^{\frac{p-1}{6}} + b)$

  $\alpha^{6(k-l)} = \alpha\frac{(-1+a\alpha^{\frac{p-1}{6}}+b)}{(1+a+b)}$

  From this we know that a and b must satisfy $\alpha^{6m} \neq \alpha\frac{(-1+a\alpha^{\frac{p-1}{6}}+b)}{(1+a+b)}$

- Class $6l+2$

  $\alpha^{6k}(1+a+b) = \alpha^{6l+2}(1+a\alpha^{\frac{p-1}{3}}+b)$

  $\alpha^{6(k-l)}(1+a+b) = \alpha^{2}(1+a\alpha^{\frac{p-1}{3}}+b)$

  $\alpha^{6(k-l)} = \alpha^{2}\frac{(1+a\alpha^{\frac{p-1}{3}}+b)}{(1+a+b)}$

  From this we know that a and b must satisfy $\alpha^{6m} \neq \alpha^{2}\frac{(1+a\alpha^{\frac{p-1}{3}}+b)}{(1+a+b)}$

- Class $6l+3$

  $\alpha^{6k}(1+a+b) = \alpha^{6l+3}(-1-a+b)$

  $\alpha^{6(k-l)}(1+a+b) = \alpha^{3}(-1-a+b)$

  $\alpha^{6(k-l)} = \alpha^{3}\frac{(-1-a+b)}{(1+a+b)}$

  From this we know that a and b must satisfy $\alpha^{6m} \neq \alpha^{3}\frac{(-1-a+b)}{(1+a+b)}$

- Class $6l+4$

  $\alpha^{6k}(1+a+b) = \alpha^{6l+4}(1+a\alpha^{2\frac{p-1}{3}}+b)$

  $\alpha^{6(k-l)}(1+a+b) = \alpha^{4}(1+a\alpha^{2\frac{p-1}{3}}+b)$

  $\alpha^{6(k-l)} = \alpha^{4}\frac{(1+a\alpha^{2\frac{p-1}{3}}+b)}{(1+a+b)}$

  From this we know that a and b must satisfy $\alpha^{6m} \neq \alpha^{4}\frac{(1+a\alpha^{2\frac{p-1}{3}}+b)}{(1+a+b)}$

- Class $6l+5$

  $\alpha^{6k}(1+a+b) = \alpha^{6l+5}(-1+a\alpha^{5\frac{p-1}{6}}+b)$

  $\alpha^{6(k-l)}(1+a+b) = \alpha^{5}(-1+a\alpha^{5\frac{p-1}{6}}+b)$

  $\alpha^{6(k-l)} = \alpha^{5}\frac{(-1+a\alpha^{5\frac{p-1}{6}}+b)}{(1+a+b)}$

From this we know that a and b must satisfy $\alpha^{6m} \neq \alpha^{5}\frac{(-1+a\alpha^{5\frac{p-1}{6}}+b)}{(1+a+b)}$

2 No zeros

Recall that for any polynomial to be a permutation polynomial it can only have 1 root. This provides another necessary condition for $F(X)$ to be PP. These 6 classes cannot be equal to 0. This is because $\alpha^n \neq 0$ for all n. We find necessary conditions on a and b by equating our partitions to 0.

Lemma 2 (Lemma 1:). *Let $F(X)$ be defined as above. We get the following conditions on a and b by contradiction:*

- $F(\alpha^{6k}) = 0 \to [a, -1-a]$ is not a possible combination.
- $F(\alpha^{6k+1}) = 0 \to [a, 1-a\alpha^{\frac{p-1}{6}}]$ is not a possible combination.
- $F(\alpha^{6k+2}) = 0 \to [a, -1-a\alpha^{\frac{p-1}{3}}]$ is not a possible combination.
- $F(\alpha^{6k+3}) = 0 \to [a, 1+a]$ is not a possible combination.
- $F(\alpha^{6k+4}) = 0 \to [a, -1-a\alpha^{2*\frac{p-1}{3}}]$ is not a possible combination.
- $F(\alpha^{6k+5}) = 0 \to [a, 1-a\alpha^{5*\frac{p-1}{6}}]$ is not a possible combination.