CHAPTER VI

CONCLUSION

A. General criteria and criteria involving characters

1. Let S and T be nonempty subsets of $\mathbb{F}_q$ with the same number of elements, s, and $S(x) = \prod_{\alpha \in S}(x - \alpha)$. For $P(x) \in \mathbb{F}_q[x]$ and $k \in \mathbb{N}$, put

$$(P(x))^k = B_k(x)S(x) + A_k(x),$$

where $B_k(x)$ and $A_k(x) := a_{s-1,k}x^{s-1} + a_{s-2,k}x^{s-2} + \cdots + a_{1,k}x + a_{0,k} \in \mathbb{F}_q[x]$. Let

$$V_j = \sum_{b \in S} b^j \quad (j = 0, 1, \ldots, s-1)$$

and

$$\begin{aligned} T(x) = {} & sx^{q-1} + x^{q-2}(a_{s-1,1}V_{s-1} + a_{s-2,1}V_{s-2} + \cdots + a_{0,1}V_0) \\ & + x^{q-3}(a_{s-1,2}V_{s-1} + a_{s-2,2}V_{s-2} + \cdots + a_{0,2}V_0) + \cdots \\ & + x(a_{s-1,q-2}V_{s-1} + a_{s-2,q-2}V_{s-2} + \cdots + a_{0,q-2}V_0) \\ & + (a_{s-1,q-1}V_{s-1} + a_{s-2,q-1}V_{s-2} + \cdots + a_{0,q-1}V_0 - s). \end{aligned}$$

Then $P(x)$ is an (S,T)QPP if and only if

$$\gcd\left(T(x), x(x^{q-1} - 1)\right) = \prod_{\alpha \in \mathbb{F}_q \setminus T} (x - \alpha),$$

where the empty product is taken to be 1.

2. Let S and T be nonempty multiplicative (or additive) abelian subgroups of $\mathbb{F}_q$, and $f(x) \in \mathbb{F}_q[x]$ sending S onto T. Then $f(x)$ is an (S,T)QPP if and only if

$$\sum_{c \in S} \chi(f(c)) = 0$$

for each nontrivial character χ of S.

3. Let q be odd, $a \in \mathbb{F}_q$, H a nonempty multiplicative subgroup of $\mathbb{F}_q \setminus \{0\}$ of even order d, and $S = H \cup \{0\}$.

(i) If $a - 1 \in H = S \setminus \{0\}$ and $\eta_H(a^2 - 1) = 1$, then $f(x) = x^{1+d/2} + ax$ is an $(S, f(S))$QPP.

(ii) If $a + 1 \in S$ and $a - 1 \in H = S \setminus \{0\}$, then $f(x) = x^{1+d/2} + ax$ is an $(S, f(S))$QPP if and only if $\eta_H(a^2 - 1) = 1$.

B. Criteria for special forms of QPP's

1. Let S be an additive subgroup of $\mathbb{F}_{q^r}$, $T \subseteq \mathbb{F}_{q^r}$ with $0 \in T \subseteq \mathbb{F}_{q^r}$ and $|S| = |T| = s$. Let

$$L(x) = \sum_{i=0}^{r-1} a_i x^{q^i} \in \mathbb{F}_{q^r}[x]$$

be a linearized polynomial sending S into T. Then $L(x)$ is an (S,T)QPP if and only if $L(x)$ has exactly one root, namely 0, in S.

2. Let S be an additive subgroup of $\mathbb{F}_{q^r}$, $0 \in T \subseteq \mathbb{F}_{q^r}$, $|S| = |T|$. Assume that $S\mathbb{F}_q \subseteq S$ and set $d := \dim_{\mathbb{F}_q} S$, $r = kd$ $(k \in \mathbb{N})$. Let $\beta_0, \beta_1, \ldots, \beta_{d-1} \in S$ be linearly independent over $\mathbb{F}_q$ and put

$$\alpha_i := \beta_i + \beta_i^{q^d} + \beta_i^{q^{2d}} + \cdots + \beta_i^{q^{(k-1)d}} \quad (i = 0, 1, 2, \ldots, d-1).$$

Let $L : S \to T$ be a linearized polynomial of the form

$$L(x) = \sum_{i=0}^{r-1} a_i x^{q^i} \in \mathbb{F}_{q^r}[x], \text{ with } a_t = a_i \text{ whenever } t \equiv i \pmod{d}.$$

(i) Assume that $\alpha_0, \alpha_1, \ldots, \alpha_{d-1}$ are linearly independent over $\mathbb{F}_q$. Then $L(\beta_0), L(\beta_1), \ldots, L(\beta_{d-1})$ are linearly independent over $\mathbb{F}_q$ if and only if $\det A \neq 0$,

where

$$A = \begin{pmatrix} a_0 & a_{d-1}^{q} & a_{d-2}^{q^2} & \cdots & a_1^{q^{d-1}} \\ a_1 & a_0^{q} & a_{d-1}^{q^2} & \cdots & a_2^{q^{d-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{d-1} & a_{d-2}^{q} & a_{d-3}^{q^2} & \cdots & a_0^{q^{d-1}} \end{pmatrix}.$$

(ii) If $\alpha_0, \alpha_1, \ldots, \alpha_{d-1}$ are linearly dependent over $\mathbb{F}_q$, then $L(\beta_0)$, $L(\beta_1), \ldots, L(\beta_{d-1})$ are linearly dependent over $\mathbb{F}_q$, and $L(x)$ is not an (S,T)QPP.

3. Let $S \subseteq \mathbb{F}_{q^r}$, $|S| = s$, α a primitive element in $\mathbb{F}_{q^r}$, $\{\alpha_0, \alpha_1, \ldots, \alpha_{r-1}\}$ a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ and $\beta \in \mathbb{F}_{q^r} \setminus \{0\}$. If

$$f(x) = \sum_{k=0}^{r-1} \beta^{q^k} \left(\alpha_0 + \alpha^{q^k}\alpha_1 + \alpha^{2q^k}\alpha_2 + \cdots + \alpha^{(r-1)q^k}\alpha_{r-1}\right) x^{q^k} \in \mathbb{F}_{q^r}[x],$$

then $f(x)$ is an $(S, f(S))$QPP.

4. Let S be a nonempty additive subgroup of $\mathbb{F}_{q^r}$ and $U = \mathbb{F}_{q^r} - S^{(q^i-q^j)}$, $i > j \geq 0$, where $S^{(q^i-q^j)} = \{\beta^{q^i-q^j};\ \beta \in S \setminus \{0\}\}$. Then $f(x) = x^{q^i} - ax^{q^j}$ is an $(S, f(S))$QPP for all $a \in U \setminus \{0\}$.

5. Let d be a divisor of $q-1$. Assume that S is a cyclic multiplicative subgroup of $\mathbb{F}_q^*$ with $|S| = \frac{q-1}{d}$. Then $f(x) = x^m$ is an (S,S)QPP if and only if $\gcd\left(m, \frac{q-1}{d}\right) = 1$.

6. Let $0 \in S \subseteq \mathbb{F}_q$ and let $f(x) = x^i - ax^j$, where $i > j \geq 1$ and $a \in \mathbb{F}_q \setminus \{0\}$.

(i) If $a \in S^{(i-j)} := \{\alpha^{i-j}; \alpha \in S\}$, then $f(x)$ is not an $(S, f(S))$QPP.

(ii) $f(x)$ is an $(S, f(S))$QPP if and only if $a \notin \left\{\frac{y^i-z^i}{y^j-z^j}; y, z \in S, y \neq z\right\} =: S_2^{(i,j)}$.

(iii) Let $e = \gcd(i,j)$, $i' = i/e$, $j' = j/e$. If S is closed undermultiplication, then $f(x)$ is an $(S, f(S))$QPP if and only if $\gcd(e, q-1) = 1$ and $h(x) = x^{i'} - ax^{j'}$ is an $(S, h(S))$QPP.

C. Number of QPP's of fixed degrees

Let $S = \{\alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_s}\} \subseteq \mathbb{F}_q$ where $\mathbb{F}_q^* = \langle \alpha \rangle$ and

$$W := \begin{pmatrix} 1 & \alpha^{i_1} & (\alpha^{i_1})^2 & \cdots & (\alpha^{i_1})^{s-1} \\ 1 & \alpha^{i_2} & (\alpha^{i_2})^2 & \cdots & (\alpha^{i_2})^{s-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{i_s} & (\alpha^{i_s})^2 & \cdots & (\alpha^{i_s})^{s-1} \end{pmatrix}.$$

For $a \in \mathbb{F}_q^*$, let S_a denote the system of equations, in $x_1, x_2, \ldots, x_s$,

$$\begin{aligned} C_{1,d+1}x_1 + C_{2,d+1}x_2 + \cdots + C_{s,d+1}x_s &= a, \\ C_{1,d+2}x_1 + C_{2,d+2}x_2 + \cdots + C_{s,d+2}x_s &= 0, \\ &\vdots \\ C_{1,s}x_1 + C_{2,s}x_2 + \cdots + C_{s,s}x_s &= 0 \end{aligned}$$

where $C_{i,j} = (-1)^{i+j} \det(M_{i,j})$ is the (i,j)-cofactor of W and $M_{i,j}$ is its (i,j)-minor. Then

$$N_{S,T}(d) = \sum_{a \in \mathbb{F}_q^*} E_a,$$

where E_a denotes the number of solutions $(x_1, x_2, \ldots, x_s) \in T^s$ of S_a with $x_i \neq x_j$ for $i \neq j$.