On the Crosscorrelation of Sequences with the Decimation Factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$ *

Z. Hu[1], X. Li[1], D. Mills[2], E. Müller[3], W. Sun[1], W. Willems[3], Y. Yang[1], and Z. Zhang[1]

[1] P.O.Box 126, Information Security Center
Beijing University of Posts and Telecomm.
Beijing, 1000876, China

[2] U.S. Army Research Laboratory
Aberdeen Proving Ground
Aberdeen, MD 21005

[3] Fakultät für Mathematik, IAG
Otto-von-Guericke-Universität
39106 Magdeburg, Germany

Abstract. Let p be a prime with $p \equiv 3 \pmod 4$, let n be an odd natural number and let $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$. Consider the crosscorrelation function $C_d(t) = \sum_{i=1}^{p^n-1} \zeta^{a_i - a_{di-t}}$ where $\zeta \neq 1$ is a complex p-th root of unity and (a_i) is a maximal linear shift register sequence. In [7] the bound $|1 + C_d(t)| \leq 2\sqrt{3^n}$ has been computed for $p = 3$. In this note we generalize this to $|1 + C_d(t)| \leq \frac{p+1}{2}\sqrt{p^n}$ for $p \geq 3$. Furthermore we give an upper bound for the probability of the crosscorrelation function achieving the maximum absolute value.

Let $(a_i)_{i\in\mathbb{N}}$ and $(b_i)_{i\in\mathbb{N}}$ be linear shift register sequences over $\mathbb{F}_p$ (p a prime) of order n. Suppose that (a_i) is maximal, i.e. (a_i) has length $p^n - 1$. If $1 \neq \zeta$ denotes a complex p-th root of unity, the crosscorrelation $C_{a,b}(t)$ of (a_i) with (b_i) is given by

$$C_{a,b}(t) = \sum_{i=1}^{p^n-1} \zeta^{a_i - b_{i-t}}.$$

Now let (b_i) be the sequence derived from (a_i) by decimation with factor d, i.e. $b_i = a_{di}$. As (a_i) is maximal we may assume that up to a cyclic shift $a_i = \mathrm{Tr}(\alpha^i)$ where α is a generator of the multiplicative group of $K = \mathbb{F}_{p^n}$ depending on the sequence (a_i) and Tr denotes the trace function from K

* This paper arose of two different notes, both with the same content. One was written by the authors from Beijing University of Posts and Telecommunications, and supported by the National Natural Science Foundation of China (No. 69802002, 69882002, 69772035) and by National "863" (No. 863-306-ZT05-05-2), the other by the remaining authors.

onto $\mathbb{F}_p$. Thus we obtain

$$\begin{aligned} C_{a,b}(t) &= \sum_{i=1}^{p^n-1} \zeta^{a_i - b_{i-t}} \\ &= -1 + \sum_{x \in \mathbb{F}_{p^n}} \zeta^{\mathrm{Tr}(x - \gamma x^d)} \end{aligned}$$

where $\gamma = \alpha^{-t}$ and we may write $C_d(t)$ instead of $C_{a,b}(t)$. For more details about crosscorrelation the reader is refered to [3].

Now let p be a prime with $p \equiv 3 \pmod 4$. If $n \in \mathbb{N}$ is odd what we always assume then

$$p^n + 1 = (p+1)(p^{n-1} - p^{n-2} + \ldots - p + 1).$$

Thus

$$d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2} \in \mathbb{Z}.$$

The condition $p \equiv 3 \pmod 4$ implies $4 \mid p+1 \mid p^n+1$ and we get

$$p^n - 1 = 2m \quad \text{with } m \text{ odd}\ . \tag{1}$$

Furthermore

$$\frac{p^n+1}{p+1} = p^{n-1} - p^{n-2} + \ldots - p + 1 \equiv n \pmod 4$$

since $p \equiv -1 \pmod 4$. Hence d is even as n is odd. Suppose that $2k$ divides $\gcd(d, p^n-1)$. By (1), k has to be odd and obviously k divides $\frac{p^n-1}{2}$ and $\frac{p^n+1}{p+1}$. Hence $k \mid p^n-1$ and $k \mid p^n+1$ which forces $k=1$. Thus we have shown

$$\gcd(d, p^n-1) = 2. \tag{2}$$

As a consequence the sequence $(b_i) = (a_{di})$ has period $\frac{p^n-1}{2}$ if (a_i) is maximal of order n. Now the aim of this note is to prove

Theorem 1. *Let p be a prime with $p \equiv 3 \pmod 4$ and let $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$ with $n \geq 3$ and n odd. Furthermore let (a_i) denote a maximal linear shift register sequence over $\mathbb{F}_p$ of order n. Then*

$$|1 + C_d(t)| \leq \frac{p+1}{2}\sqrt{p^n}.$$

For $p = 3$ this is Theorem 2 of [7]. In order to prove the Theorem for general $p \equiv 3 \pmod 4$ we need some preliminary results on quadratic forms of $K = \mathbb{F}_{p^n}$ regarded as a vector space over the prime field $\mathbb{F}_p$. Apart from this and the use of Gauss sums the proof follows the lines of [7].

Lemma 2. *Under the conditions stated we have*

a) $K^2 = K^{p+1}$.
b) $K = K^{p+1} \cup (-K^{p+1})$.

Proof. a) Let $x \in K$. Since $x^{p^n} = x$, we have $x^2 = x^{p^n+1} = (x^{\frac{p^n+1}{p+1}})^{p+1}$. Thus $K^2 \subseteq K^{p+1}$. Furthermore, as $\gcd(\frac{p^n+1}{p+1}, p^n - 1) = 1$, the map

$$x \longrightarrow x^{\frac{p^n+1}{p+1}}$$

is an automorphism of K^*, the multiplivative group of K. Hence $K^2 = K^{p+1}$.
b) By (1), the element -1 is a nonsquare in K. $\square$

Lemma 3. *Let $\beta, \gamma \in K$. If we regard K as a vector space over the prime field $\mathbb{F}_p$, then*

$$Q_{\beta,\gamma}(x) = \mathrm{Tr}(\beta x^{p+1} - \gamma x^2)$$

defines a quadratic form on K of rank $n, n-1$ or $n-2$ for $(\beta, \gamma) \neq (0,0)$.

Proof. For $\lambda \in \mathbb{F}_p$ we have $Q_{\beta,\gamma}(\lambda x) = \lambda^2 Q_{\beta,\gamma}(x)$. Furthermore, the polarization $B_{\beta,\gamma}(x,y) = Q_{\beta,\gamma}(x+y) - Q_{\beta,\gamma}(x) - Q_{\beta,\gamma}(y)$ is given by

$$B_{\beta,\gamma}(x,y) = \mathrm{Tr}(\beta(x^p y + x y^p) - 2\gamma xy)$$

which obviously defines a symmetric bilinear form on K over $\mathbb{F}_p$. Thus $Q_{\beta,\gamma}(x)$ is a quadratic form. To compute the rank we recall that $x \in K$ lies in the radical of $Q_{\beta,\gamma}$ if and only if

$$Q_{\beta,\gamma}(x+y) = Q_{\beta,\gamma}(y) \text{ for all } y \in K.$$

Now,

$$\begin{aligned}
0 &= Q_{\beta,\gamma}(x+y) - Q_{\beta,\gamma}(y) \\
&= \mathrm{Tr}(\beta[(x+y)^{p+1} - y^{p+1}] + \gamma[(x+y)^2 - y^2]) \\
&= \mathrm{Tr}(\beta[(x^p + y^p)(x+y) - y^{p+1}] + \gamma[(x+y)^2 - y^2]) \\
&= \mathrm{Tr}(\beta[x^p y + y^p x + x^{p+1}] - \gamma[x^2 + 2xy]) \\
&= \mathrm{Tr}(y^p[\beta^p x^{p^2} + \beta x - 2\gamma^p x^p] + \beta x^{p+1} - \gamma x^2),
\end{aligned}$$

where $\mathrm{Tr}(z) = \mathrm{Tr}(z^p)$ has been used to get the last equation. Thus x lies in the radical of $Q_{\beta,\gamma}$ if and only if x is a root of the polynomial

$$q_{\beta,\gamma}(x) = \beta^p x^{p^2} + \beta x - 2\gamma^p x^p.$$

As $q_{\beta,\gamma}(x)$ is a linearized polynomial of degree at most p^2 the roots form a vector space of dimension $0, 1$ or 2 over $\mathbb{F}_p$. This proves the assertion on the rank of the form. $\square$

Lemma 4. *For $\beta \neq 0$ we have*

$$2n - 2 \leq \operatorname{rank} Q_{\beta,\gamma} + \operatorname{rank} Q_{-\beta,\gamma}.$$

Proof. Recall that

$$\operatorname{rank} Q_{\beta,\gamma} = n - \log_p n_{\beta,\gamma}$$

where $n_{\beta,\gamma}$ denotes the number of roots of $q_{\beta,\gamma}$ in K counted with multiplicities. Thus it is sufficient to show that

$$\begin{aligned} q(x) &= q_{\beta,\gamma}(x) q_{-\beta,\gamma}(x) \\ &= -\beta^2 x^2 (x^{2p^2-2} + 2x^{p^2-1} - 4\beta^{-2}\gamma^{2p} x^{2p-2} + 1) \end{aligned}$$

has at most $p^2 + 1$ roots in K (counted again with multiplicities). To see this we put $u = x^{2p-2}$ and

$$h(u) = u^{p+1} + 2u^{\frac{p+1}{2}} - 4\beta^{-2}\gamma^{2p} u + 1.$$

With this notation we have $\frac{q(x)}{-\beta^2 x^2} = h(u)$. Since $\gcd(2p-2, p^n - 1) = p - 1$ by (1), to each root u of h there correspond only $p-1$ roots x of the polynomial q. Thus the polynomial $\frac{q(x)}{-\beta^2 x^2}$ has at most $(p+1)(p-1)$ roots (counted with multiplicities). Taking into account the double root 0 we find the upper bound $p^2 + 1$ for the number of roots of q. $\square$

For the reader's convenience we state the following well-known result on solutions of non-degenerate quadratic forms (see for instance [6], Chapter 6, Section 2).

Lemma 5. *Let V be a vector space of dimension n over $\mathbb{F}_p$ where p is an odd prime. Let Q be a non-degenerate quadratic form on V with determinant Δ and for $c \in \mathbb{F}_p$ let $N(c) = |\{v \in V : Q(v) = c\}|$. Then*

(i) for n odd the number of solution is

$$N(c) = \begin{cases} p^{n-1} & \text{for } c = 0 \\ p^{n-1} + p^{\frac{n-1}{2}} \left(\frac{(-1)^{\frac{n-1}{2}} \Delta}{p} \right) \left(\frac{c}{p} \right) & \text{for } c \neq 0 \end{cases}$$

(ii) and for n even

$$N(c) = p^{n-1} - p^{\frac{n-2}{2}} \left(\frac{(-1)^{\frac{n}{2}} \Delta}{p} \right) \delta(c)$$

where $(\frac{\cdot}{p})$ denotes the Legendre symbol and $\delta(c) = \begin{cases} -1 & \text{for } c \neq 0 \\ p - 1 & \text{for } c = 0. \end{cases}$

Finally, we need the following Lemma whose proof one can find in [6], Theorem 5.15 or [5].

Lemma 6. *If p is an odd prime and ζ is a complex primitive p-th root of unity, then*

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k = \begin{cases} \sqrt{p} & \text{for } p \equiv 1 \bmod 4 \\ \sqrt{-p} & \text{for } p \equiv 3 \bmod 4. \end{cases}$$

Now we have enough prepared to start with the proof of Theorem 1.

Proof. By Lemma 2 we have $K = K^{p+1} \cup (-K^{p+1})$ and since

$$x^{d(p+1)} = x^{p^n+1}(x^{p^n-1})^{\frac{p+1}{2}} = x^{p^n+1} = x^2$$

we obtain

$$\begin{aligned} 2(1+C_d(t)) &= \textstyle\sum_{x\in K} (\zeta^{\mathrm{Tr}(x^{p+1}-\gamma x^2)} + \zeta^{\mathrm{Tr}(-x^{p+1}-\gamma x^2)}) \\ &= \textstyle\sum_{c=0}^{p-1} (N_+(c) + N_-(c))\zeta^c \end{aligned} \tag{3}$$

where $N_\pm(c) = |\{x \in K : \mathrm{Tr}(\pm x^{p+1} - \gamma x^2) = c\}|$. Thus it remains to determine the values $N_\pm(c)$. If we write $K = U_\pm \oplus \operatorname{rad} Q_{\pm,\gamma}$, then

$$N_{\pm,\gamma}(c) = p^{n-rank\, Q_{\pm,\gamma}} |\{x \in U_\pm : Q_{\pm,\gamma}(x) = c\}|.$$

According to Lemma 4 there are four cases to consider. Let $\sigma_\pm$ denote a Legendre symbol, i.e. a sign, depending on the determinant and the rank of the underlying non-degenerate quadratic form.

Case 1. $\operatorname{rank} Q_{+,\gamma} = \operatorname{rank} Q_{-,\gamma} = n$.
Applying Lemma 5 and Lemma 6 we get by (3)

$$\begin{aligned} 2(1+C_d(t)) &= 2p^{n-1} + \sum_{i=1}^{p-1} (2p^{n-1} + p^{\frac{n-1}{2}}(\sigma_+ + \sigma_-)\left(\frac{i}{p}\right))\zeta^i \\ &= p^{\frac{n-1}{2}}(\sigma_+ + \sigma_-) \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \zeta^i. \end{aligned}$$

Thus

$$2|1+C_d(t)| = p^{\frac{n-1}{2}} |\sigma_+ + \sigma_-| |\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \zeta^i| \leq 2p^{\frac{n-1}{2}} \sqrt{p}$$

which proves $|1+C_d(t)| \leq \sqrt{p^n}$.

Case 2. $\operatorname{rank} Q_{+,\gamma} = \operatorname{rank} Q_{-,\gamma} = n-1$.
In this case we obtain

$$\begin{aligned}
2(1+C_d(t)) &= p(2p^{n-2} + (p-1)p^{\frac{n-3}{2}}(\sigma_+ + \sigma_-) \\
&\qquad + (2p^{n-2} - p^{\frac{n-3}{2}}(\sigma_+ + \sigma_-))\sum_{i=1}^{p-1}\zeta^i) \\
&= p((p-1)p^{\frac{n-3}{2}}(\sigma_+ + \sigma_-) + p^{\frac{n-3}{2}}(\sigma_+ + \sigma_-)) \\
&= p^{\frac{n+1}{2}}(\sigma_+ + \sigma_-)
\end{aligned}$$

which leads to $|1+C_d(t)| \le \sqrt{p^{n+1}} < \frac{p+1}{2}\sqrt{p^n}$.

Case 3. $\operatorname{rank} Q_{+,\gamma} = n$ and $\operatorname{rank} Q_{-,\gamma} = n-1$.
Now we get

$$\begin{aligned}
2(1+C_d(t)) &= 2p^{n-1} + (p-1)\sigma_- p^{\frac{n-1}{2}} \\
&\qquad + \sum_{i=0}^{p-1}(2p^{n-1} + p^{\frac{n-1}{2}}(\sigma_+\left(\frac{i}{p}\right) - \sigma_-))\zeta^i \\
&= \sigma_-(p-1)p^{\frac{n-1}{2}} + p^{\frac{n-1}{2}}\sum_{i=0}^{p-1}(\sigma_+\left(\frac{i}{p}\right) - \sigma_-))\zeta^i \\
&= \sigma_- p^{\frac{n+1}{2}} + \sigma_+ p^{\frac{n-1}{2}}\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)\zeta^i.
\end{aligned}$$

Thus $2|1+C_d(t)| \le p^{\frac{n+1}{2}} + p^{\frac{n-1}{2}}\sqrt{p} \le 2\sqrt{p^{n+1}}$ which implies the desired bound $|1+C_d(t)| \le \sqrt{p^{n+1}} < \frac{p+1}{2}\sqrt{p^n}$.

Case 4. $\operatorname{rank} Q_{+,\gamma} = n$ and $\operatorname{rank} Q_{-,\gamma} = n-2$.
In this last case we obtain

$$\begin{aligned}
2(1+C_d(t)) &= p^{n-1} + \sum_{i=1}^{p-1}(p^{n-1} + \sigma_+ p^{\frac{n-1}{2}}\left(\frac{i}{p}\right))\zeta^i \\
&\qquad + p^2(p^{n-3} + \sum_{i=1}^{p-1}(p^{n-3} + \sigma_- p^{\frac{n-3}{2}}\left(\frac{i}{p}\right))\zeta^i \\
&= 2p^{n-1} + \sum_{i=1}^{p-1}(2p^{n-1} + (\sigma_+ p^{\frac{n-1}{2}} + \sigma_- p^{\frac{n+1}{2}})\left(\frac{i}{p}\right))\zeta^i \\
&= (\sigma_+ p^{\frac{n-1}{2}} + \sigma_- p^{\frac{n+1}{2}})\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\zeta^i.
\end{aligned}$$

Hence $2|1+C_d(t)| \le p^{\frac{n-1}{2}}(1+p)\sqrt{p}$ which yields $|1+C_d(t)| \le \frac{p+1}{2}\sqrt{p^n}$.

Finally note that a change of the ranks in Cases 3 and 4 leads to the same bounds. □

Remarks. a) Let $f(x)$ be the polynomial $f(x) = q_{1,1}(x) = x^{p^2} + x - 2x^p$. Over $\mathbb{F}_p$ it has the factorization

$$f(x) = x \prod_{a \in \mathbb{F}_p^*} (x+a)(x^p - x + a).$$

Now, $x^p - x + a$ is irreducible over $\mathbb{F}_p$ (see [6], Corollary 3.79). Thus all roots of $x^p - x + a$ are in $\mathbb{F}_{p^p}$. Consequently, all roots of $f(x)$ are in $\mathbb{F}_{p^p}$ and Case 4 in the proof of the Theorem occurs with $n = p$, $\operatorname{rank} Q_{+,1} = p-2$ and $\operatorname{rank} Q_{-,1} = p$. In order to get $|1+C_d(0)| = \frac{p+1}{2}\sqrt{p^p}$ we have to prove that $\sigma_+ = \sigma_-$ or equivalently $\left(\frac{\Delta_+}{p}\right) = -\left(\frac{\Delta_-}{p}\right)$ since $\sigma_+ = \left(\frac{(-1)^{\frac{p-3}{2}}\Delta_+}{p}\right) = \left(\frac{\Delta_+}{p}\right)$, $\sigma_- = \left(\frac{(-1)^{\frac{p-1}{2}}\Delta_-}{p}\right) = -\left(\frac{\Delta_-}{p}\right)$. Unfortunately we don't see any way to prove this. For $p = n = 3$ (see [7]) and $p = n = 7$ we checked $\sigma_+ = \sigma_-$ with the computer. In the first case it turned out that $\sigma_+ = \sigma_- = -1$, in the second $\sigma_+ = \sigma_- = 1$.

b) Let p be odd and $d = \frac{p^n+1}{p+1}$. Then $d \cdot \frac{p^{n+1}+1}{2} \equiv 1 \pmod{(p^n-1)}$. Thus by Lemma 5.1 ad Theorem 5.5 in [3], the crosscorrelation $C_d(t)$ takes on exactly three values, namely -1 and $-1 \pm p^{\frac{n+1}{2}}$. This result was originally established in [8].

c) For n odd, $p = 2$ and $d = \frac{2^n+1}{3} = \frac{p^n+1}{p+1}$ the crosscorrelation $C_d(t)$ has exactly three values, namely -1 and $-1 \pm 2^{\frac{n+1}{2}}$. This can be seen as follows. Since $x \longrightarrow x^3$ is an automorphism of $K = \mathbb{F}_{2^n}$ we get

$$1 + C_d(t) = \sum_{x \in K} (-1)^{\operatorname{Tr}(x - \gamma x^d)} = \sum_{x \in K} (-1)^{\operatorname{Tr}(x^3 - \gamma x^2)}.$$

The form $Q(x) = \operatorname{Tr}(x^3 - \gamma x^2)$ has polarization $B(x,y) = \operatorname{Tr}(x^2 y + y^2 x) = \operatorname{Tr}(y^2(x^4 + x))$. Thus B is of rank $n-1$ since the roots of $x^4 + x$ in K are only 0 and 1. Consequently Q has rank n or $n-1$ depending on $\operatorname{Tr}(1-\gamma) \neq 0$ or $\operatorname{Tr}(1-\gamma) = 0$. Applying ([6], Theorem 6.32), one easily finds the three values above. Thus, by an unpublished result of Cusick [1], the power function $x \longrightarrow x^d$ is an APN function on K. Since

$$\left(\frac{2^n+1}{3}\right)(2^{n-1}+1) = 1 + 2\left(\frac{2^{n-2}+1}{3}\right)(2^n - 1) \tag{4}$$

the function $x \longrightarrow x^d$ is the inverse of the well-known APN function $x \longrightarrow x^{2^{n-1}+1}$ (see [4], Theorem 2, 2)).

Equation (4) provides another way to see that $C_d(t)$ takes the values $-1, -1 \pm 2^{\frac{n+1}{2}}$: Obviously, the inverse $\mod (2^n-1)$ of $d = \frac{2^n+1}{3}$ is $2^{n-1}+1$ by (4). Since d and d^{-1} lead to the same crosscorrelation spectrum, the result follows immediately from [2].

In the rest of the paper we show that for large p the probability of the crosscorrelation function achieving the maximum absolute value is very small. More precisely,

Theorem 7. *Under the condition of Theorem 1 we have*

$$\mathrm{P}\left(|1 + C_d(t)| = \frac{p+1}{2}\sqrt{p^n}\right) < \frac{2}{p^2-1}.$$

Proof. Let $K = \mathbb{F}_{p^n}$. Put

$$\begin{aligned} q_{+,\gamma}(x) &= x^{p^2} - 2\gamma^p x^p + x \\ q_{-,\gamma}(x) &= x^{p^2} + 2\gamma^p x^p + x \end{aligned}$$

and $\mathrm{R}(\pm,\gamma) = \{\, x \in K \mid q_{\pm,\gamma}(x) = 0\}$.

(1) We claim that $\mathrm{R}(+,\gamma_1) \cap \mathrm{R}(+,\gamma_2) = \{0\}$ and $\mathrm{R}(-,\gamma_1) \cap \mathrm{R}(-,\gamma_2) = \{0\}$ for $\gamma_1 \neq \gamma_2$ and $\gamma_i \neq 0$.
For if $x^{p^2} \mp 2\gamma_1^p x^p + x = 0$ and $x^{p^2} \mp 2\gamma_2^p x^p + x = 0$, then

$$2(\gamma_1^p - \gamma_2^p)x^p = 2(\gamma_1 - \gamma_2)^p x^p = 0,$$

which implies $x = 0$.

(2) Next we claim that for $z \in K^*$ there exists $\gamma_+, \gamma_- \in K^*$ such that $z \in \mathrm{R}(+,\gamma_+)$ and $\mathrm{R}(-,\gamma_-)$.
Let α be a primitive root of K. Then $\beta = \alpha^p$ is a primitive root of K as well. Thus z can be written as $z = \beta^i$. If we put

$$\gamma_\pm = \pm\frac{\beta^{ip} + \alpha^i}{2\beta^i},$$

then

$$\begin{aligned} g_{+,\gamma_+}(z) &= \beta^{ip^2} - 2\beta^{ip}\left(\tfrac{\beta^{ip}+\alpha^i}{2\beta^i}\right)^p + \beta^i \\ &= \beta^{ip^2} - \beta^{ip^2} - \alpha^{ip} + \beta^i = 0, \end{aligned}$$

hence $z \in \mathrm{R}(+,\gamma_+)$. Similary $g_{-,\gamma_-}(z) = 0$.

Now let $\mathrm{R}(\pm,\gamma)^* = \mathrm{R}(\pm,\gamma) - \{0\}$. By claim (1) and (2) we get

$$(*) \qquad \sum_{\gamma \in K^*} |\mathrm{R}(\pm,\gamma)^*| = p^n - 1.$$

Obviously, we also have

$$|\mathrm{R}(\pm,\gamma)^*| = 0, p-1 \text{ or } p^2-1,$$

since $g_{\pm,\gamma}$ is a linearized polynomial of degree p^2. Equation $(*)$ implies

$$s_{\pm,2} := |\{\, \gamma \in K^* \mid |\mathrm{R}(\pm,\gamma)| = p^2 - 1\}| \le \lfloor \frac{p^n-1}{p^2-1} \rfloor < \frac{p^n-1}{p^2-1},$$

where the last inequality holds since n is odd. Now, by the proof of Theorem 1, the maximal value $|1 + C_d(t)| = \frac{p+1}{2}\sqrt{p^n}$ occurs if and only if

$$\operatorname{rank} Q_{+,\gamma} = n,\ \operatorname{rank} Q_{-,\gamma} = n-2 \text{ or vice versa and } \sigma_+ = \sigma_-.$$

By the proof of Lemma 4 we have $\operatorname{rank} Q_{\pm,\gamma} = n, n-1$ or $n-2$ which is equivalent to $|\mathrm{R}(\pm,\gamma)^*| = 0, p-1$ or p^2-1. Thus $|1 + C_d(t)| = \frac{p+1}{2}\sqrt{p^n}$ requires $|\mathrm{R}(+,\gamma)^*| = 0$ and $|\mathrm{R}(-,\gamma)^*| = p^2 - 1$ or vice versa. This shows that

$$\mathrm{P}\left(|1 + C_d(t)| \le \frac{p+1}{2}\sqrt{p^n}\right) = \frac{s_{-,2} + s_{+,2}}{p^n - 1} < \frac{2}{p^2-1}.$$

References

1. T.W. Cusick, Constructing differentially uniform permutations via crosscorrelation functions, unpublished.
2. R. Gold, Maximal recursive sequences with three-valued recursive crosscorrelation function. IEEE Trans. Inform. Theory IT-14 (1968), 154-156.
3. T. Helleseth and P.V. Kumar, Sequences with low correlation. In Handbook of Coding Theory, Part II, Editors V.S. Pless and W.C.Huffman, Elsevier 1998, 1765-1853.
4. T. Helleseth, C. Rong and D. Sandberg, New families of almost perfect nonlinear power mappings, IEEE Trans. Inform. Theory 45 (1999), 475-485.
5. L. Hua, Introduction to number theory, Science Press, Beijing 1957.
6. R. Lidl and H. Niederreiter, Finite fields. Encyclopedia of Math. and Appl. 20, Cambridge Uni. Press, Second Edition 1997.
7. E.N. Müller, On the crosscorrelation of sequences over GF(p) with short periods. IEEE Trans. Inform. Theory 45 (1999), 289-295.
8. H.M. Trachtenberg, On the cross-correlation functions of maximal linear recurring sequences. PhD thesis, Faculty of the Graduate School, University of Southern California, Los Angeles, California, 1970.