Explicit lifts of quintic Jacobi sums and period polynomials for $\mathbf{F}_q$

By Akinari HOSHI

Department of Mathematics, School of Education, Waseda University, 1–6–1, Nishi-Waseda, Shinjuku-ku, Tokyo 169–8050, Japan

(Communicated by Heisuke HIRONAKA, M.J.A., Sept. 12, 2006)

Abstract: In this paper, we construct explicit lifts of quintic Jacobi sums for finite fields via integer solutions of Dickson's system. Namely we give a procedure to compute quintic Jacobi sums for extended field $\mathbf{F}_{p^{s+t}}$ by using quintic Jacobi sums for $\mathbf{F}_{p^s}$ and for $\mathbf{F}_{p^t}$. We also have the multiplication formula from $\mathbf{F}_{p^s}$ to $\mathbf{F}_{p^{ns}}$ as a special case. By the quintuplication formula, we obtain the explicit factorization of the quintic period polynomials for finite fields.

Key words: Jacobi sums; Gaussian periods; Dickson's system; Gauss sums.

1. Introduction. Let $e \geq 2$ be a positive integer and $q = p^r$ a prime power such that $q \equiv 1 \pmod{e}$. Write $q = ef + 1$. Let ζ_p be a p-th primitive root of unity, γ a fixed generator of $\mathbf{F}_q^*$. Gaussian periods $\eta_{0,r}, \ldots, \eta_{e-1,r}$ of degree e for $\mathbf{F}_q$ are defined by

$$\eta_{i,r} := \sum_{j=0}^{f-1} \zeta_p^{\mathrm{Tr}(\gamma^{ej+i})},$$

where Tr is the trace map $\mathrm{Tr} : \mathbf{F}_q \to \mathbf{F}_p$, and the period polynomial $P_{e,r}(X)$ of degree e for $\mathbf{F}_q$ is given by $P_{e,r}(X) := \prod_{i=0}^{e-1}(X - \eta_{i,r})$. We also use the reduced form $P_{e,r}^*(X) := \prod_{i=0}^{e-1}(X - \eta_{i,r}^*)$, where $\eta_{i,r}^* = e\,\eta_{i,r} + 1$, since the coefficient of X^{e-1} of $P_{e,r}^*(X)$ is vanished. In the classical case $q = p$, Gauss [7] showed that the period polynomial $P_{e,1}(X)$ is irreducible over $\mathbf{Q}$. However this is not always true for general $q = p^r$. In 1981, for $\delta = \gcd(e, (q-1)/(p-1))$, Myerson [15] showed that the period polynomial $P_{e,r}(X)$ splits over $\mathbf{Q}$ into δ factors

$$P_{e,r}(X) = \prod_{k=0}^{\delta-1} P_{e,r}^{(k)}(X),$$

where $P_{e,r}^{(k)}(X)$ is in $\mathbf{Z}[X]$ and irreducible or a power of an irreducible polynomial. Note that $P_{e,r}(X)$ is irreducible over $\mathbf{Q}$ if and only if $p \equiv 1 \pmod{e}$ and $(r, e) = 1$, i.e. $\delta = 1$, (see [15]). The explicit determination of the factors of $P_{e,r}(X)$, if reducible, is important because it is known that the (exponential) Gauss sum $g_r(e)$ is one of the roots of $P_{e,r}^*(X)$ (see [4]). Myerson [15] determined the factors $P_{e,r}^{(k)}(X)$ for $e = 2, 3, 4$. In 2004, Gurak [9] gave the factors $P_{e,r}^{(k)}(X)$ for the case $e \mid 8, 12$ (see also [8]). However it seems to be hard to determine the explicit factors $P_{e,r}^{(k)}(X)$ for general prime degree. In this paper, we shall give the factors $P_{e,r}^{(k)}(X)$ in the quintic case $e = 5$ by constructing explicit lifts of quintic Jacobi sums.

Here we describe briefly our construction of lifts of quintic Jacobi sums via Dickson's system. Let χ be a character of order e on $\mathbf{F}_q^*$ such that $\chi(\gamma) = \zeta_e$ and we extend it to $\mathbf{F}_q$ by $\chi(0) = 0$. The Jacobi sum $J_r(\chi^m, \chi^n)$ of degree e for $\mathbf{F}_q$, $q = p^r$, is defined by

$$J_r(\chi^m, \chi^n) := \sum_{\alpha \in \mathbf{F}_q} \chi^m(\alpha)\chi^n(1 - \alpha).$$

We now suppose that $e = 5$ and $p \equiv 1 \pmod{5}$, since the case $p \not\equiv 1 \pmod{5}$ is tractable (see Section 6). The following system of Diophantine equations is called Dickson's system:

$$\begin{cases} 16p^r = x^2 + 125w^2 + 50v^2 + 50u^2, \\ xw = v^2 - 4vu - u^2, \\ x \equiv -1 \pmod{5}. \end{cases}$$

It is known that there exist exactly four integer solutions of Dickson's system, related to p^r, which satisfy the condition $p \nmid x^2 - 125w^2$, and we denote them by $S(p,r)^U$. The crucial facts are that $S(p,r)^U$ gives the value of $J_r(\chi, \chi)$ and $P_{5,r}(X)$ can be described by using the value of $J_r(\chi, \chi)$. In Section 4, we shall make a lift of quintic Jacobi sums by using integer solutions of Dickson's system. This means that we

2000 Mathematics Subject Classiffcation. Primary 11E25, 11L05, 11T22, 11T24.

give the procedure of constructing four integer solutions $S(p,s+t)^U$ by using $S(p,s)^U$ and $S(p,t)^U$. This method gives us an algorithm for fast computation of quintic Jacobi sums for $\mathbf{F}_q$ (cf. [22]). In Section 5, we shall give the multiplication formula of the lift from $S(p,s)^U$ to $S(p,ns)^U$ explicitly. Let σ be a non-singular linear transformation of order four such that $\sigma(x,w,v,u)=(x,-w,-u,v)$. Using the quintuplication formula, we obtain the explicit factorization of the quintic period polynomial.

Theorem 1. *Let $p\equiv 1 \pmod 5$, $q=p^{5s}$ and $(x,w,v,u)\in S(p,s)^U$. The quintic reduced period polynomial $P^*_{5,5s}(X)$ for $\mathbf{F}_q$ splits over $\mathbf{Q}$ as follows*:

$$P^*_{5,5s}(X)=$$
$$\Big(X+\frac{p^s}{16}\big(x^3-25L\big)\Big)\prod_{i=0}^{3}\Big(X-\frac{p^s}{64}\sigma^i\big(x^3-25M\big)\Big),$$

where

$$\begin{aligned}L&=2x(v^2+u^2)+5w(11v^2-4vu-11u^2),\\ M&=2x^2u+7xv^2+20xvu-3xu^2+125w^3\\ &\quad+200w^2v-150w^2u+5wv^2-20wvu\\ &\quad-105wu^2-40v^3-60v^2u+120vu^2+20u^3.\end{aligned}$$

2. Review of the cyclotomic numbers. We review the method which gives the period polynomials using the Jacobi sums. The cyclotomic numbers $A_{i,j}$, $(i,j=0,\dots,e-1)$ of order e for $\mathbf{F}_q$ are defined by

$$A_{i,j}:=\#\left\{(v_1,v_2)\ \middle|\ \begin{array}{c}0\le v_1,v_2\le f-1\\ 1+\gamma^{ev_1+i}\equiv\gamma^{ev_2+j}\pmod q\end{array}\right\}.$$

Note that the cyclotomic numbers $A_{i,j}$ depend on a choice of γ. One can find the basic properties of $A_{i,j}$ in [4, 15]. Especially we can see the following relations of Gaussian periods.

$$\eta_{m,r}\,\eta_{m+i,r}=\sum_{j=0}^{e-1}\big(A_{i,j}-D_if\big)\,\eta_{m+j,r},$$

where $D_i=\delta_{0,i}$ (resp. $\delta_{\frac{e}{2},i}$), if pf is even (resp. odd) and $\delta_{i,j}$ is Kronecker's delta. It follows that Gaussian periods $\eta_{i,r}$ are eigenvalues of the $e\times e$ matrix $M:=[A_{i,j}-D_if]_{0\le i,j\le e-1}$. Hence we can obtain the period polynomial $P_{e,r}(X)$ as the characteristic polynomial of the matrix M. The crucial fact is that the cyclotomic numbers can be given by Jacobi sums when degree e is prime. Let l be an odd prime. In the case $e=l$ and $p\equiv 1 \pmod l$, by using Jacobi sums, Katre and Rajwade [14] determined cyclotomic numbers of order l for $\mathbf{F}_q$ without γ-ambiguity. Acharya and Katre [1] extended this result for order $2l$. One can find a detailed historical survey for the cyclotomic problem in [4] and [14], and we also can study recent topics for Jacobi sums and period polynomials in [2, 10, 11, 16–22].

3. Known results of the quintic case. We recall known results in the quintic case $e=5$ such that $p\equiv 1 \pmod 5$. The following system of Diophantine equations is called "Dickson's system" since the case $r=1$ was discovered by Dickson [5].

$$(1)\qquad \begin{cases}16p^r=x^2+125w^2+50v^2+50u^2,\\ xw=v^2-4vu-u^2,\\ x\equiv -1 \pmod 5.\end{cases}$$

We denote by $S(p,r)$ the set of all integer solutions of Dickson's system related to p^r. It is known that $\#S(p,r)=(r+1)^2$, (see [14, Section 2]). We define a non-singular linear transformation $\sigma:\mathbf{Z}^4\to\mathbf{Z}^4$ of order four by

$$\sigma:(x,w,v,u)\mapsto(x,-w,-u,v).$$

Note that if $(x,w,v,u)\in S(p,r)$ then $\sigma^i(x,w,v,u)\in S(p,r)$ for $i=1,2,3$. We denote by $\langle(x,w,v,u)\rangle$ the σ-orbit of a 4-tuple (x,w,v,u):

$$\langle(x,w,v,u)\rangle:=\Big\{\sigma^i(x,w,v,u)\ \Big|\ i=0,1,2,3\Big\}.$$

In [13], Katre and Rajwade gave the following result. The Dickson's system (1) has *exactly* four integer solutions $\langle(x,w,v,u)\rangle$ which satisfy the condition

$$(2)\qquad p\nmid x^2-125w^2.$$

For one of these four solutions satisfying

$$(3)\qquad \gamma^{(q-1)/5}\equiv\frac{X_1-10X_2}{X_1+10X_2}\pmod p,$$

where $X_1=x^2-125w^2$ and $X_2=2xu-xv-25vw$, the Jacobi sum $J_r(\chi,\chi)$ for $\mathbf{F}_q$ is given by

$$J_r(\chi,\chi)=\frac14\Big(C\zeta_5+\sigma^3(C)\zeta_5^2+\sigma(C)\zeta_5^3+\sigma^2(C)\zeta_5^4\Big),$$

where $C=x-5w-4v-2u$, and conversely for this value of $J_r(\chi,\chi)$, (x,w,v,u) gives the unique solution of Dickson's system which satisfies (2) and (3). Moreover the cyclotomic numbers of order five for $\mathbf{F}_{p^r}$, related to γ, are unambiguously given by

$$A_{0,0} = (p^r - 14 + 3x)/25,$$
$$A_{0,1} = (4p^r - 16 - 3x + 25w + 50v)/100,$$
$$A_{0,2} = \sigma^3(A_{0,1}),\ A_{0,3} = \sigma(A_{0,1}),\ A_{0,4} = \sigma^2(A_{0,1}),$$
$$A_{1,2} = (2p^r + 2 + x - 25w)/50,\ A_{1,3} = \sigma^2(A_{1,2}).$$

Using the above $A_{i,j}$, we have the quintic period polynomial $P_{5,r}(X)$ as the characteristic polynomial of the matrix $[A_{i,j} - D_i f]_{0\le i,j\le 4}$. Here we describe the reduced form of the quintic period polynomial:

$$\begin{aligned} P^*_{5,r}&(x,w,v,u;X) \\ &= X^5 - 10p^rX^3 + 5p^rxX^2 \\ &\quad + \frac{5p^r}{4}\big(4p^r - x^2 + 125w^2\big)X \\ &\quad + \frac{p^r}{8}\big(x^3 - 8p^rx - 625w(v^2-u^2)\big). \end{aligned} \tag{4}$$

Note that all coefficients of $P^*_{5,r}(X)$ are σ-invariants since $P^*_{5,r}(X)$ does not depend on a choice of γ. This representation, however, gives us no information about explicit factors of $P^*_{5,r}(X)$ when $r = 5s$.

Remark. From the equation

$$\sigma\big(J_r(\chi,\chi)\big) = J_r(\chi^2,\chi^2),$$

we see that if (x,w,v,u) gives the Jacobi sum $J(\chi,\chi)$ then the other solutions $\sigma(x,w,v,u)$, $\sigma^2(x,w,v,u)$, $\sigma^3(x,w,v,u)$ give $J_r(\chi^2,\chi^2)$, $J_r(\chi^4,\chi^4)$, $J_r(\chi^3,\chi^3)$ respectively.

4. Lift of Jacobi sums. As in Section 3, we suppose that $p \equiv 1 \pmod 5$. We shall construct a lift of Jacobi sums via Dickson's system.

Definition. Four integer solutions of Dickson's system which satisfy (2) are called *essentially unique* and we denote them by $S(p,r)^U$.

The aim of this section is to give the procedure to compute the set $S(p,s+t)^U$ by using $S(p,s)^U$ and $S(p,t)^U$. This is achieved by using certain quadratic forms which are called multiplicative on algebraic varieties in [12]. The following proposition, which can be given as a special case of [12, Theorem 4], plays a key role of our construction.

Proposition 2. *Let* $q(\mathbf{X}) = X_1^2 + 125X_2^2 + 50X_3^2 + 50X_4^2$ *and* V *a hypersurface defined by* $X_1X_2 = X_3^2 - 4X_3X_4 - X_4^2$. *There exists a bilinear map* $\varphi : \mathbf{Z}^4 \times \mathbf{Z}^4 \to \mathbf{Z}^4$ *such that* $\varphi(V\times V) \subset V$ *and* $q(\mathbf{v})q(\mathbf{w}) = q(\varphi(\mathbf{v},\mathbf{w}))$ *for any* $\mathbf{v},\mathbf{w} \in V$. *Moreover the bilinear map* φ *is given as follows*:

$$\begin{aligned} \varphi(\mathbf{X},\mathbf{Y}) = (&X_1Y_1 + 125X_2Y_2 + 50X_3Y_3 + 50X_4Y_4, \\ &X_2Y_1 + X_1Y_2 - 2X_3Y_3 + 4X_4Y_3 + 4X_3Y_4 + 2X_4Y_4, \\ &X_3Y_1 - 5X_3Y_2 + 10X_4Y_2 - X_1Y_3 + 5X_2Y_3 - 10X_2Y_4, \\ &X_4Y_1 + 10X_3Y_2 + 5X_4Y_2 - 10X_2Y_3 - X_1Y_4 - 5X_2Y_4). \end{aligned} \tag{5}$$

We have the following remarkable equation:

$$\varphi\big(\sigma(\mathbf{X}),\sigma(\mathbf{Y})\big) = \sigma\big(\varphi(\mathbf{X},\mathbf{Y})\big). \tag{6}$$

Using φ in (5), we can construct a lift of integer solutions of Dickson's system.

Proposition 3. *For* $\mathbf{s} = (x_s,w_s,v_s,u_s) \in S(p,s)$ *and* $\mathbf{t} = (x_t,w_t,v_t,u_t) \in S(p,t)$, *the sixteen 4-tuples* $\langle\varphi(\mathbf{s},\sigma^i(\mathbf{t}))/4\rangle$, $0 \le i \le 3$, *are integer solutions of Dickson's system related to* p^{s+t}.

Proof. It is known that an integer solution (x,w,v,u) of Dickson's system satisfies the following congruences (see [13, Lemma 1 (d)]).

$$\begin{cases} -x + w + 2u \equiv 0 \pmod 4, \\ -x - w + 2v \equiv 0 \pmod 4). \end{cases}$$

Using this, we can show that the sixteen 4-tuples $\varphi\big(\sigma^i(\mathbf{s}),\sigma^j(\mathbf{t})\big)/4, (0 \le i,j \le 3)$, are in $\mathbf{Z}^4$ (see also [12, Lemma 9]). From (6), they separate four σ-orbits. And we can easily check that they satisfy the conditions (1) from Proposition 2. □

Definition. For $\mathbf{s} = (x_s,w_s,v_s,u_s) \in S(p,s)$ and $\mathbf{t} = (x_t,w_t,v_t,u_t) \in S(p,t)$, we define 4-tuples of integers $\mathbf{s} \overset{i}{*} \mathbf{t}$, for $0 \le i \le 3$, by

$$\mathbf{s} \overset{i}{*} \mathbf{t} := \varphi\big(\mathbf{s},\sigma^i(\mathbf{t})\big)/4,$$

where φ is defined in (5).

We have that $\langle \mathbf{s} \overset{i}{*} \mathbf{t}\rangle \subset S(p,s+t)$ for $0 \le i \le 3$ from Proposition 3. Next we consider when there exists integer i such that $\langle \mathbf{s} \overset{i}{*} \mathbf{t}\rangle = S(p,s+t)^U$, i.e. which 4-tuples $\langle \mathbf{s} \overset{i}{*} \mathbf{t}\rangle$ correspond to the Jacobi sum $J_{s+t}(\chi,\chi)$ for $\mathbf{F}_{p^{s+t}}$. For $\mathbf{r} = (x,w,v,u) \in S(p,r)$, we put

$$g_1(\mathbf{r}) := x^2 - 125w^2, \qquad g_2(\mathbf{r}) := v^2 + vu - u^2,$$
$$g_3(\mathbf{r}) := 2xu - xv - 25wv, \quad g_4(\mathbf{r}) := g_3(\sigma(\mathbf{r})).$$

Lemma 4. *Let* $\mathbf{r} = (x,w,v,u) \in S(p,r)$. $p \nmid g_1(\mathbf{r})$ *if and only if* $p \nmid g_k(\mathbf{r})$ *for* $k = 2,3,4$.

Proof. See, for example, [13, Lemma 2]. □

The following proposition gives an explicit lift of quintic Jacobi sums by using essentially unique solutions of Dickson's system.

Theorem 5 (Addition formula)**.** *Let* $\mathbf{s} \in S(p,s)$ *and* $\mathbf{t} \in S(p,t)$. *There exists integer* i, $(0 \le i \le 3)$ *such that* $\langle \mathbf{s} \overset{i}{*} \mathbf{t} \rangle = S(p, s+t)^U$ *if and only if* $\langle \mathbf{s} \rangle = S(p,s)^U$ *and* $\langle \mathbf{t} \rangle = S(p,t)^U$.

Proof. We should show that $p \mid g_1\big(\mathbf{s} \overset{i}{*} \mathbf{t}\big)$ for $0 \le i \le 3$ if and only if $p \mid g_1(\mathbf{s})$ or $p \mid g_1(\mathbf{t})$. We can obtain the following remarkable equation:

$$\begin{aligned} 16\, g_1\big(\mathbf{s} \overset{0}{*} \mathbf{t}\big) &= g_1(\mathbf{s})g_1(\mathbf{t}) + 2000 g_2(\mathbf{s})g_2(\mathbf{t}) \\ &\quad + 20 g_3(\mathbf{s})g_3(\mathbf{t}) + 20 g_4(\mathbf{s})g_4(\mathbf{t}). \end{aligned}$$

We also have similar equations for $g_1\big(\mathbf{s} \overset{i}{*} \mathbf{t}\big), (i = 1,2,3)$ using $g_1(\sigma(\mathbf{t})) = g_1(\mathbf{t})$, $g_2(\sigma(\mathbf{t})) = -g_2(\mathbf{t})$, $g_3(\sigma(\mathbf{t})) = g_4(\mathbf{t})$, $g_4(\sigma(\mathbf{t})) = -g_3(\mathbf{t})$. If $p \mid g_1\big(\mathbf{s} \overset{i}{*} \mathbf{t}\big)$ for $0 \le i \le 3$ then p divides $\sum_{i=0}^{3}(-1)^i g_1(\mathbf{s} \overset{i}{*} \mathbf{t}) = 8000 g_2(\mathbf{s})g_2(\mathbf{t})$, and then $p \mid g_1(\mathbf{s})$ or $p \mid g_1(\mathbf{t})$ from Lemma 4. If $p \mid g_1(\mathbf{s})$ or $p \mid g_1(\mathbf{t})$ then it follows that $p \mid g_1\big(\mathbf{s} \overset{i}{*} \mathbf{t}\big)$ for $0 \le i \le 3$ from Lemma 4. □

Theorem 5 enables us to compute the value of quintic Jacobi sums for general $\mathbf{F}_q$ (cf. [22]). However we should choose the suitable integer i which depends on the first choice of $\mathbf{s}$ and $\mathbf{t}$. In the next section, we shall dissolve this ambiguity and give the multiplication formula explicitly.

5. Multiplication formula. First we consider the case $s = t$ in Theorem 5 in order to establish the duplication formula. For $\mathbf{s} = (x, w, v, u) \in S(p,s)^U$, we have the following equalities:

$$\begin{aligned} &\langle \mathbf{s} \overset{0}{*} \mathbf{s} \rangle = \big\{(4p^s, 0, 0, 0)\big\}, \\ &\langle \mathbf{s} \overset{1}{*} \mathbf{s} \rangle = \langle \mathbf{s} \overset{3}{*} \mathbf{s} \rangle = \Big\langle\Big(\frac{x^2 - 125w^2}{4}, v^2 + vu - u^2, \\ &\frac{-x(v+u) + 5w(v+3u)}{4}, \frac{x(v-u) + 5w(3v-u)}{4}\Big)\Big\rangle, \end{aligned} \tag{7}$$

$$\begin{aligned} \langle \mathbf{s} \overset{2}{*} \mathbf{s} \rangle = \Big\langle\Big(&\frac{-8p^s + x^2 + 125w^2}{2}, xw, \\ &\frac{xv - 5wv + 10wu}{2}, \frac{xu + 10wv + 5wu}{2}\Big)\Big\rangle. \end{aligned}$$

Hence if we have $S(p,s)^U$ then we can obtain nine (different) integral solutions of Dickson's system related to p^{2s}. This corresponds to the fact that Dickson's system related to p has four solutions and to p^2 nine solutions. The following formula gives us which above are essentially unique.

Proposition 6 (Duplication formula)**.** *For* $\mathbf{s} \in S(p,s)^U$, *we have* $S(p, 2s)^U = \langle \mathbf{s} \overset{2}{*} \mathbf{s} \rangle$ *as in* (7).

Proof. It remains to show that $\mathbf{s} \overset{2}{*} \mathbf{s}$ satisfy the condition (2). Write $(x_{2s}, w_{2s}, v_{2s}, u_{2s}) := \mathbf{s} \overset{2}{*} \mathbf{s}$. We have that $x_{2s} \equiv (x^2 + 125w^2)/2 \pmod{p^s}$ and

$$\Big(\frac{x^2 + 125w^2}{2}\Big)^2 - 125\Big(xw\Big)^2 = \frac{(x^2 - 125w^2)^2}{4}.$$

Hence we obtain

$$x_{2s}^2 - 125 w_{2s}^2 \equiv \frac{(x^2 - 125w^2)^2}{4} \pmod{p^s}.$$

Thus $p \nmid x_{2s}^2 - 125w_{2s}^2$ follows from $p \nmid x^2 - 125w^2$. □

From the direct computation, we see that the symbol $\overset{i}{*}$ satisfy the following law:

Lemma 7. *For* $\mathbf{s} \in S(p,s), \mathbf{t} \in S(p,t), \mathbf{u} \in S(p,u)$, *we have*

$$\begin{aligned} &\mathbf{s} \overset{2}{*} \mathbf{t} = \mathbf{t} \overset{2}{*} \mathbf{s}, \\ &(\mathbf{s} \overset{2}{*} \mathbf{t}) \overset{j}{*} \mathbf{u} = \mathbf{s} \overset{2}{*} (\mathbf{t} \overset{j}{*} \mathbf{u}), \quad j = 0,1,2,3. \end{aligned}$$

Remark. In general, we see that $\mathbf{s} \overset{i}{*} \mathbf{t} \ne \mathbf{t} \overset{i}{*} \mathbf{s}$ and $(\mathbf{s} \overset{i}{*} \mathbf{t}) \overset{j}{*} \mathbf{u} \ne \mathbf{s} \overset{i}{*} (\mathbf{t} \overset{j}{*} \mathbf{u})$, for $i = 0,1,3, j = 0,1,2,3$.

From Lemma 7, we can define the n-th power of the symbol $\overset{2}{*}$ as follows:

$$\mathbf{s}^{(n)} := \mathbf{s} \overset{2}{*} \mathbf{s} \overset{2}{*} \cdots \overset{2}{*} \mathbf{s}, \quad (n \text{ times}).$$

Using $\mathbf{s}^{(n)}$, we obtain the multiplication formula:

Theorem 8 (Multiplication formula)**.** *Suppose that* $\mathbf{s} \in S(p,s)^U$. *Then* $S(p, ns)^U = \langle \mathbf{s}^{(n)} \rangle$.

Proof. We should show that if $S(p, ns)^U = \langle \mathbf{s}^{(n)} \rangle$ then $S(p, (n+1)s)^U = \langle \mathbf{s}^{(n+1)} \rangle$. The case $n = 1$ follows from Proposition 6. Thus we assume that $S(p, ns)^U = \langle \mathbf{s}^{(n)} \rangle$. From Theorem 5, there exists an integer i such that $\mathbf{s}^{(n)} \overset{i}{*} \mathbf{s} \in S(p, (n+1)s)^U$. However the integer i must be 2 because we obtain that $\mathbf{s}^{(n-1)} \overset{2}{*} (\mathbf{s} \overset{i}{*} \mathbf{s}) \in S(p, (n+1)s)^U$ by Lemma 7 and hence $\mathbf{s} \overset{i}{*} \mathbf{s} \in S(p, 2)^U$ from Theorem 5. □

Here we describe the triplication, the quadruplication and the quintuplication formula which can be obtained by iterating the duplication formula.

$$\begin{aligned} \mathbf{s}^{(3)} = \Big(&\frac{x(-12p^s + x^2 + 375w^2)}{4}, \\ &\frac{w(-12p^s + 3x^2 + 125w^2)}{4}, \frac{\sigma(F)}{4}, \frac{F}{4}\Big), \end{aligned}$$

where

$$F = -4p^s u + x^2 u + 20xwv + 10xwu + 125w^2 u.$$

$$\mathbf{s}^{(4)} = \Bigl(\frac{G_1}{8}, \frac{xw(-8p^s + x^2 + 125w^2)}{2}, \frac{\sigma(G_2)}{8}, \frac{G_2}{8}\Bigr),$$

where $G_1 = 16p^s(2p^s - x^2 - 125w^2) + x^4 + 750x^2w^2 + 15625w^4$, $G_2 = -8p^s(xu + 10wv + 5wu) + x^3u + 30x^2wv + 15x^2wu + 375xw^2u + 1250w^3v + 625w^3u$.

$$\mathbf{s}^{(5)} = \Bigl(\frac{xH_1}{16}, \frac{5wH_2}{16}, \frac{\sigma(H_3)}{16}, \frac{H_3}{16}\Bigr), \tag{8}$$

where $H_1 = 20p^s(4p^s - x^2 - 375w^2) + x^4 + 1250x^2w^2 + 78125w^4$, $H_2 = 4p^s(4p^s - 3x^2 - 125w^2) + x^4 + 250x^2w^2 + 3125w^4$, $H_3 = 4p^s(4p^s u - 3x^2u - 60xwv - 30xwu - 375w^2u) + x^4u + 40x^3wv + 20x^3wu + 750x^2w^2u + 5000xw^3v + 2500xw^3u + 15625w^4u$.

Using (8), we can prove Theorem 1 which gives an explicit factorization of the reduced period polynomial $P^*_{5,5s}(X)$ for $\mathbf{F}_{p^{5s}}$.

Proof of Theorem 1. From (4), we have $P^*_{5,5s}(x_{5s}, w_{5s}, v_{5s}, u_{5s}; X)$ for $\mathbf{F}_q, (q = p^{5s})$, where $(x_{5s}, w_{5s}, v_{5s}, u_{5s}) \in S(p, 5s)^U$. Using (8), we have that $S(p, 5s)^U = \langle \mathbf{s}^{(5)} \rangle$ where $\mathbf{s} = (x, w, v, u) \in S(p, s)^U$. Since $P^*_{5,5s}(X)$ does not depend on a choice of γ, we obtain $P^*_{5,5s}(X)$ using not $(x_{5s}, w_{5s}, v_{5s}, u_{5s})$ but $\mathbf{s} = (x, w, v, u) \in S(p, s)^U$ as $P^*_{5,5s}(\mathbf{s}^{(5)}; X)$. And then the assertion can be checked by direct computation. □

Gauss sums $g_r(b, e)$, $(b \in \mathbf{F}_q)$ of degree e for $\mathbf{F}_q$ are defined by

$$g_r(b, e) := \sum_{\alpha \in \mathbf{F}_q} \zeta_p^{\mathrm{Tr}(b\alpha^e)},$$

(see, for example, [4]). We see that Gaussian periods and Gauss sums have the following relation

$$e\,\eta_{i,r} + 1 = g_r(\gamma^i, e), \quad \text{for} \quad i = 0, \ldots, e-1.$$

From the definition, we have $g_r(\gamma^i, e) = \eta^*_{i,r}$, for $0 \le i \le e-1$. Hence the Gauss sums $g_r(\gamma^i, e)$ are roots of $P^*_{e,r}(X)$. For $i = 0$, we write $g_r(e) := g_r(1, e) = g_r(\gamma^0, e)$. As a corollary of Theorem 1, we obtain the location of the quintic Gauss sums for $\mathbf{F}_{p^{5s}}$.

Corollary 9. *Let $p \equiv 1 \pmod 5, q = p^{5s}$. The Gauss sum $g_{5s}(5)$ for $\mathbf{F}_q$ is given by $g_{5s}(5) = p^s(-x^3 + 25L)/16$, where L is in Theorem 1.*

Proof. Since $g_{5s}(5)$ does not depend on a choice of γ, the assertion follows from $\sigma(-x^3 + 25L) = -x^3 + 25L$ and (6). □

Remark. It is not difficult to compute only the value of the Gauss sum $g_{5s}(5)$ above. Indeed it is known that $g_{5s}(5)$ can be given by using Eisenstein sums (see [4, Chapter 12]). By Theorem 1 and (4), we also see that $g_{5s}(5)$ is the product of $g_s(\gamma_s^i, 5)$, $0 \le i \le 4$, where γ_s is a generator of $\mathbf{F}^*_{p^s}$:

$$g_{5s}(5) = \prod_{i=0}^{4} g_s(\gamma_s^i, 5).$$

Example. For $p = 11$, we have that

$$\begin{aligned}
&S(11,1) = S(11,1)^U = \langle(-1, 1, 0, -1)\rangle,\\
&S(11,2)^U = \langle(19, -1, -5, -2)\rangle,\\
&S(11,3)^U = \langle(-61, -1, 5, -18)\rangle,\\
&S(11,4)^U = \langle(-241, -19, -50, 11)\rangle,\\
&S(11,5)^U = \langle(-396, -100, 150, -30)\rangle,\\
&P^*_{5,1}(X) = X^5 - 110X^3 - 55X^2 + 2310X + 979,\\
&P^*_{5,5}(X) = X^5 - 1610510X^3 - 318880980X^2\\
&\qquad + 349760093485X + 36198435398004\\
&= (X+99)(X+649)(X+979)(X-451)(X-1276).
\end{aligned}$$

And we also obtain that $g_5(5) = -979 = -11 \cdot 89$.

6. Appendix: tractable case. Let $e \ge 2$ be a positive integer and $q = p^r$ a prime power such that $q \equiv 1 \pmod e$. In this section, we assume that

$$-1 \text{ is a power of } p \pmod e.$$

It is known that this situation is more tractable. For example, Evans [6] showed that -1 is a power of $p \pmod e$ if and only if the Jacobi sum $J_r(\chi^s, \chi^t)$ is *pure* (i.e. some non-zero integral power of it is real) for all $s, t \in \mathbf{Z}$. The cyclotomic numbers $A_{i,j}$ of order e for $\mathbf{F}_q$ are called *uniform* if $A_{0,i} = A_{i,0} = A_{i,i}$ and $A_{i,j} = A_{1,2}$ $(i \ne j)$, for $1 \le i, j \le e-1$. And Gaussian periods $\eta_{i,r}$ of degree e for $\mathbf{F}_q$ are also called *uniform* if for some fixed c and η we have $\eta_{i,r} = \eta$ for $i \ne c$. Baumert, Mills and Ward [3] showed that the following conditions are equivalent for $e \ge 3$: (i) -1 is a power of $p \pmod e$, (ii) The cyclotomic numbers of order e for $\mathbf{F}_q$ are uniform, (iii) The Gaussian periods of degree e for $\mathbf{F}_q$ are uniform.

For $e = l$, where l is an odd prime, Anuradha and Katre [2] evaluated Jacobi sums and cyclotomic numbers of order l for $\mathbf{F}_q$ as follows. For a prime p such that $m = \mathrm{ord}\ p \pmod l$ is even, $q = p^r \equiv 1 \pmod l$, and $r = ms$, $(s \ge 1)$,

$$J_r(\chi, \chi^n) = (-1)^{s-1} p^{r/2}, \quad \text{for} \quad 1 \leq n \leq l-2,$$

(9)

$$l^2 A_{0,0} = q - 3l + 1 - (l-1)(l-2)(-1)^s q^{1/2},$$
$$l^2 A_{0,j} = q - l + 1 + (l-2)(-1)^s q^{1/2}, \text{ for } j \neq 0,$$
$$l^2 A_{i,j} = q + 1 - 2(-1)^s q^{1/2}, \text{ for } i, j, i-j \neq 0.$$

By (9), we can easily obtain the following lemma which includes the quintic case $l = 5$ such that $p \not\equiv 1 \pmod 5$.

Lemma 10. *Let l be an odd prime. Suppose $m = \operatorname{ord} p \pmod l$ is even and $q = p^{ms} \equiv 1 \pmod l$, $(s \geq 1)$. The reduced period polynomial $P^*_{l,ms}(X)$ of degree l for $\mathbf{F}_q$ splits over $\mathbf{Q}$ as follows*:

$$P^*_{l,ms}(X) = \begin{cases} (X - q^{1/2})^{l-1}(X + (l-1)q^{1/2}), & \text{if } s \text{ is even}, \\ (X + q^{1/2})^{l-1}(X - (l-1)q^{1/2}), & \text{if } s \text{ is odd}. \end{cases}$$

Proof. The period polynomial $P_{l,ms}(X)$ of degree l is given as the characteristic polynomials of the matrix $[A_{i,j} - \delta_{0,i} f]_{0 \leq i,j \leq l-1}$, since pf is even. It is easily verified that

$$P_{l,ms}(X) = (X - A_{0,1} + A_{1,2})^{l-2}\Big((X - A_{0,0} + f)\times (X - A_{0,1} - (l-2)A_{1,2}) + (l-1)A_{0,1}(f - A_{0,1})\Big),$$

because the cyclotomic numbers are uniform. Thus the assertion follows from (9). □

The calculations in this paper were carried out with Maple and Mathematica [23].

Acknowledgements. The author is grateful to the referee for pointing out a misunderstanding in the manuscript. Theorem 8 was improved by the referee's valuable comments. He is also grateful to Prof. Ki-ichiro Hashimoto who gave him helpful comments and various suggestions during this study.

References

[1] V. V. Acharya and S. A. Katre, Cyclotomic numbers of order $2l$, l an odd prime, Acta Arith. **69** (1995), 51–74.

[2] N. Anuradha and S. A. Katre, Number of points on the projective curves $aY^l = bX^l + cZ^l$ and $aY^{2l} = bX^{2l} + cZ^{2l}$ defined over finite fields, l an odd prime, J. Number Theory **77** (1999), 288–313.

[3] L. D. Baumert, W. H. Mills and R. L. Ward, Uniform cyclotomy, J. Number Theory **14** (1982), 67–82.

[4] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Wiley, New York, 1998.

[5] L. E. Dickson, Cyclotomy, higher congruences and Waring's problem, Amer. J. Math. **57** (1935), 391–424.

[6] R. J. Evans, Pure Gauss sums over finite fields, Mathematika. **28** (1981), 239–248.

[7] C. F. Gauss, *Disquisitiones Arithmeticae*, Section 358.

[8] S. Gurak, Period polynomials for F_{p^2} of fixed small degree, in *Finite fields and applications* (*Augsburg*, 1999) 196–207, Springer, Berlin.

[9] S. Gurak, Period polynomials for $\mathbf{F}_q$ of fixed small degree, in *Number theory*, 127–145, Amer. Math. Soc., Providence, 2004.

[10] K. Hashimoto and A. Hoshi, Families of cyclic polynomials obtained from geometric generalization of Gaussian period relations, Math. Comp. **74** (2005), 1519–1530.

[11] K. Hashimoto and A. Hoshi, Geometric generalization of Gaussian period relations with application to Noether's problem for meta-cyclic groups, Tokyo J. Math. **28** (2005), 13–32.

[12] A. Hoshi, Multiplicative quadratic forms on algebraic varieties, Proc. Japan Acad. Ser. A Math. Sci. **79** (2003), no.4, 71–75.

[13] S. A. Katre and A. R. Rajwade, Unique determination of cyclotomic numbers of order five, Manuscripta Math. **53** (1985), 65–75.

[14] S. A. Katre and A. R. Rajwade, Complete solution of the cyclotomic problem in $\mathbf{F}_q^*$ for any prime modulus l, $q = p^\alpha$, $p \equiv 1 \pmod l$, Acta Arith. **45** (1985), 183–199.

[15] G. Myerson, Period polynomials and Gauss sums for finite fields, Acta Arith. **39** (1981), 251–264.

[16] F. Thaine, Properties that characterize Gaussian periods and cyclotomic numbers, Proc. Amer. Math. Soc. **124** (1996), 35–45.

[17] F. Thaine, On the coefficients of Jacobi sums in prime cyclotomic fields, Trans. Amer. Math. Soc. **351** (1999), 4769–4790.

[18] F. Thaine, Families of irreducible polynomials of Gaussian periods and matrices of cyclotomic numbers, Math. Comp. **69** (2000), 1653–1666.

[19] F. Thaine, Jacobi sums and new families of irreducible polynomials of Gaussian periods, Math. Comp. **70** (2001), 1617–1640.

[20] F. Thaine, On Gaussian periods that are rational integers, Michigan Math. J. **50** (2002), 313–337.

[21] F. Thaine, Cyclic polynomials and the multiplication matrices of their roots, J. Pure Appl. Algebra **188** (2004), 247–286.

[22] P. V. Wamelen, Jacobi sums over finite fields, Acta Arith. **102** (2002), 1–20.

[23] S. Wolfram, *The Mathematica book*, Fourth ed., Wolfram Media, Inc., Cambridge Univ. Press, Cambridge-New York, 1999.