Behavior of function field Gauss sums at ∞

Dinesh S. Thakur
(with an appendix by José Felipe Voloch)

Abstract

We describe the valuations of the function field Gauss sums at the infinite places, by relating them to Weierstrass gaps. This generalizes our previous results for $\mathbf{F}_q[T]$, in which case the valuations are all $1/(q-1)$, in direct analogy with the well-known classical result that all the absolute values of Gauss sums are $q^{1/2}$. We also investigate the sign of quadratic or higher order Gauss sums, giving results in the direction of Gauss' sign theorem and the work of Cassels and Matthews.

Introduction

An analogue of Gauss sums taking values in function fields over finite fields was introduced and studied in [**8**, **9**, **10**, **12**]. In [**8**, **9**], analogues of various classical results about Gauss sums such as Stickelberger factorization, Hasse-Davenport and Gross-Koblitz results were established, in the case of $\mathbf{F}_q[T]$. The general case turns out to be interestingly different, in view of the established analogies, and is discussed in [**10**, **12**]. More relevant to this paper is another well-known classical fact that the absolute value of Gauss sum at any infinite place is $q^{1/2}$. For $\mathbf{F}_q[T]$ analogue, it was shown in [**8**, **9**] that the valuation at any infinite place is $-1/(q-1)$. Here 2 and $q-1$ can be described as the cardinalities of $\mathbf{Z}^*$ and $\mathbf{F}_q[T]^*$ resp. or as the degrees of respective cyclotomic fields over their maximal 'totally real' subfields. We will see (theorem 1.8) that even though these analogies generalize, the valuation in the general case is closely related to Weierstrass gaps.

We only deal with the case where the infinite place is of degree one. It might be worthwhile to do the general case and the interested reader will find the relevant cyclotomic theory developed in [**5**]. For the general case, when the genus is zero, see [**10**, **12**].

Next we consider the question of sign of Gauss sums and establish (theorem 2.5) an analogue of Gauss' theorem on the sign of quadratic Gauss sums. Then we consider signs of m-th order Gauss sums, in spirit of the investigations of Cassels and Matthews (See [**7**]).

Acknowledgements: I am much obliged to José Felipe Voloch for his help (see the appendix) with some questions about the exceptional primes.

I would also like to thank Greg Anderson for asking me about the signs and directing me to papers of Matthews. He has also computed the valuation of Gauss sums for generic primes, by using his theory of Baker functions in characteristic p.

Section 0: Background

Notation:
$\mathbf{F}_q$: a finite field of characteristic p containing q elements
K : a function field of one variable with the field of constants $\mathbf{F}_q$
∞ : a place of K of degree one
H: maximal abelian unramified extension of K split at ∞
A : the ring of elements of K with no poles outside ∞
$\wp$: a prime of A of degree d
K_∞: the completion of K at ∞
Ω: the completion of an algebraic closure of K_∞
h : the class number of K
$\underline{g}$: the genus of K

Drinfeld modules, Gauss sums (See [**2**, **4**, **10**] for more details) :

0.1 Fix a local parameter t^{-1} at ∞. For $x \in K_\infty^*$, define $\deg(x) \in \mathbf{Z}$ and $\mathrm{sgn}(x) \in \mathbf{F}_q^*$ to be the exponent in the highest power of t and the coefficient of the highest power respectively, in the expansion of x as Laurent series in t^{-1}, with coefficients in $\mathbf{F}_q$.

0.2 Let L be a field containing A and let $L\{F\}$ denote the noncommutative ring generated by the elements of L and by a symbol F, with the commutation relation $Fl = l^q F$, for all $l \in L$. By a Drinfeld A-module ρ over L (in fact 'sgn-normalized, of rank one and generic characteristic', but we will drop these words) we will mean an injective homomorphism $\rho : A \to L\{F\}$ ($a \in A \mapsto \rho_a \in L\{F\}$) such that, for all $a \in A - \{0\}$,

$$\rho_a = \sum_{i=0}^{\deg(a)} \rho_{a,i} F^i, \quad \rho_{a,i} \in L \quad \rho_{a,0} = a, \quad \rho_{a,\deg(a)} = \mathrm{sgn}(a)$$

Two Drinfeld A-modules ρ, $\tilde{\rho}$ are considered isomorphic (say over $L' \supset L$) if there is a nonzero $l' \in L'$ such that $l'\rho_a = \tilde{\rho}_a l'$ for $a \in A$.

0.3 Minimal L such that Drinfeld A-module over L exists is H up to isomorphism. Note that the degree of the extension H of K is h. There are h nonisomorphic Drinfeld A-modules over H, Galois conjugates over K to each other.

0.4 For a Drinfeld module ρ over K_∞, define the exponential $e(z) = e_\rho(z)$ of ρ as the power series characterized by $e(az) = \rho_a(e(z))$, for all $a \in A$ and $e(z) = z+$higher order terms in z. Then $e(z)$ is an everywhere convergent in Ω, it has coefficients in H. The kernel of the function e is a rank one A-lattice in Ω and hence can be described as $\tilde{\pi}_{\mathcal{A}}\mathcal{A}$, for some $\tilde{\pi} = \tilde{\pi}_{\mathcal{A}} \in \Omega$ and an ideal $\mathcal{A}$ of A. The fundamental period $\tilde{\pi}$ (in fact it has been defined only upto multiplication by element in $\mathbf{F}_q^*$) of $e(z)$ can be thought of as an analogue of $2\pi i$ and is known to be transcendental [**13**]. We have $\tilde{\pi}^{q-1} \in K_\infty$, just as $(2\pi i)^2 \in \mathbf{R}$. The nonarchimedean nature of Ω then gives the product formula $e(z) = z\prod(1 + z/\lambda)$, where the product runs over the nonzero elements λ of the lattice $\tilde{\pi}\mathcal{A}$.

0.5 Let $\overline{L}$ be an algebraic closure of L. For $a \in A$, define 'a-torsion of ρ' as $\Lambda_a := \{u \in \overline{L} : \rho_a(u) = 0\}$. For an ideal I of A, we define 'I-torsion of ρ' as $\Lambda_I := \{u \in \overline{L} : \rho_i(u) = 0, \text{for all } i \in I\}$. It is an A-module under ρ. By adjoining Λ_I (I nonzero) to K, we get another type of cyclotomic extension of K. In analogy with the classical case, $K(\Lambda_I) = H(\Lambda_I)$ has Galois group $(A/I)^*$ over H and the decomposition (also inertia) group at an infinite place of H is $\mathbf{F}_q^* \subset (A/I)^*$. Hence the degree of $H(\Lambda_I)$ over its 'maximal totally real' subfield $H(\Lambda_I)^+$ is $q-1$.

0.6 Let $\wp$ be a prime of A of degree d. Choose an A-module isomorphism $\psi : A/\wp \to \Lambda_\wp$ (an analogue of additive character) and let χ_j ($j$mod d) be $\mathbf{F}_q$-homomorphisms $A/\wp \to L$ where L is a field containing $K(\Lambda_\wp)$, indexed so that $\chi_j^q = \chi_{j+1}$ (special multiplicative characters which are q^j-powers of 'Teichmüller character', say χ_0). Then we define the Gauss sums

$$g_j := g(\chi_j) := -\sum_{z \in (A/\wp)^*} \chi_j(z^{-1})\psi(z)$$

Section I: Valuations at ∞

1.1 Let ρ be a Drinfeld module over K_∞ with the corresponding lattice $\tilde{\pi}\mathcal{A}$. Let $\wp$ be a prime of A of degree d. Consider the Gauss sums as defined in 0.6. Note that $\Lambda_\wp = \{e(\tilde{\pi}r) : r \in \wp^{-1}\mathcal{A}\}$ and that $g_j \in \tilde{\pi}\mathbf{F}_{q^d}((t^{-1}))$.

1.2 **Theorem**: *The degree of the Gauss sum is same as the maximum possible degree of a $\wp$-torsion element*

Proof: Let $R \subset \wp^{-1}\mathcal{A}$ be a set of representatives modulo $\mathcal{A}$ of the lowest possible degrees. It is easy to see that there is a $\mathbf{F}_q$- basis $\{r_1, \cdots r_d\}$ of R such that $\{r_1 + r_2\theta_1 + \cdots + r_d\theta_d : \theta_i \in \mathbf{F}_q\}$ is exactly the subset of monic (i.e. of sgn 1) elements of R of maximal degree.

We can assume that the torsion points $\psi(r)$ are just $e(\tilde{\pi}r)$, for $r \in R$. The product formula in 0.4 shows that the degree of $\psi(r)$ is maximal, when the degree of r is maximal. Now ψ being additive, the maximal degree is degree of $\psi(r_1)$. It is enough to show that this top degree does not get cancelled in the summation. Since both ψ and χ_j are $\mathbf{F}_q$-linear, and $q-1=-1$ in characteristic p, we have $g_j = \sum \chi_j(z^{-1})\psi(z)$, where now the sum is taken over the monic representatives of $\wp^{-1}\mathcal{A}/\mathcal{A}$. If we note that $\chi_j(r_i)$ is a basis of $\mathbf{F}_{q^d}$ over $\mathbf{F}_q$, the theorem then follows from the following lemma.

1.3 **Lemma**: *If $f_1, \cdots, f_d$ is a basis of $\mathbf{F}_{q^d}$ over $\mathbf{F}_q$, then*

$$\sum := \sum_{\theta_i \in \mathbf{F}_q} \frac{1}{f_1 + f_2\theta_2 + \cdots + f_d\theta_d} \neq 0$$

Proof: Let

$$M(x_1, \cdots, x_k) := \prod_{j=1}^{k} \prod_{\theta_i \in \mathbf{F}_q} (x_j + x_{j+1}\theta_{j+1} + \cdots + x_k\theta_k)$$

Then with $P(t) := \prod(t + f_2\theta_2 + \cdots + f_d\theta_d)$, where the product is over all $\theta_i \in \mathbf{F}_q$, we have $\sum = P'(f_1)/P(f_1)$ and $P(f_1) = M(f_1, \cdots, f_d)/M(f_2, \cdots, f_d)$. As $P(t)$ is an $\mathbf{F}_q$-linear polynomial, $P'(t)$ is just the coefficient of t in $P(t)$ and hence equals $\prod(f_2\theta_2 + \cdots + f_d\theta_d)$, where now the product runs through $\theta_i \in \mathbf{F}_q$ not all zero. But this is just $(-1)^{d-1}M(f_2, \cdots, f_d)^{q-1}$, because $\prod_{\theta \in \mathbf{F}_q^*} \theta = -1$ and $(-1)^{(q^{d-1}-1)/(q-1)} = (-1)^{d-1}$. Hence $\sum = (-1)^{d-1}M(f_2, \cdots, f_d)^q/M(f_1, \cdots, f_d)$ is nonzero, as it is product of terms which are nonzero because f_i are linearly independent over $\mathbf{F}_q$. This finishes the proof of the lemma and of the theorem.

1.4 **Definition**: Let $0 \leq n_1 < n_2 \cdots < n_g$ be the integers n ('gaps of $\mathcal{A}$') so that there are no elements of $\mathcal{A}$ of degree n. (Here g is just the number of gaps. It is the genus $\underline{g}$ when $\mathcal{A} = A$, by the Riemann-Roch. Note $n_g - g$ is an ideal class invariant and hence when $g = 0$ we take $n_0 = -1$ to retain this property.) Call $\wp$ exceptional with respect to $\mathcal{A}$ (or rather its ideal class) if n_g is a gap for fractional ideal $\wp^{-1}\mathcal{A}$ (i.e. there is no element of degree n_g in $\wp^{-1}\mathcal{A}$.) We say that $\wp$ is exceptional, if it is exceptional with respect to some $\mathcal{A}$.

1.5 **Theorem**: *(1) Principal primes are not exceptional; (2) Primes of degree more than $\underline{g}$ are not exceptional. In particular, there are at most finitely many exceptional primes. (3) Primes of degree one which are not principal are exceptional.*

Proof: Let $\wp$ be a prime of degree d. Since n_g is the largest gap of $\mathcal{A}$, there is an element, say $e \in \mathcal{A}$ of degree $n_g + d$. If $\wp$ is principal, $\wp = (P)$ say, then $e/P \in \wp^{-1}\mathcal{A}$ has degree n_g and (1) follows. In general, given $\wp$, let d' be the degree of the smallest degree element in the smallest degree ideal $\overline{\wp}$ in the ideal class inverse to that of $\wp$. Counting the gaps of $\overline{\wp}$, we see that $d' \leq \deg\ \overline{\wp} + \underline{g}$. If $d > d' - \deg\ \overline{\wp}$, then $\wp^{-1}$ has an element of negative degree and just as above we see that $\wp$ in that case can not be exceptional. (2) follows. Now let $\wp$ be of degree one and not principal (equivalently $\underline{g} \neq 0$). Then 0 is a gap for $\wp$, but not for A. Hence the count of gaps shows that the largest gap for A is also the largest gap for $\wp$ and hence $\wp$ is exceptional for $\mathcal{A} = \wp$. This proves (3) and hence the theorem.

1.6 **Remarks**: (i) If $\wp$ is a non-principal prime of the lowest possible degree for A for an hyperelliptic K, then $\wp$ has $2\underline{g} - 1$ as a gap and hence is exceptional for $\mathcal{A} = \wp$.

(ii) When $\underline{g} = 1$, the theorem shows that the exceptional primes are exactly the primes of degree one and are hence $h - 1$ in number.

(ii) By 1.5, there are no exceptional primes when $h = 1$. (By [**6**], apart from $A = \mathbf{F}_q[T]$ (one for each q), there are only four such A's.) On the other hand, Voloch (see the appendix) has given a nice characterization of exceptional primes and proved that they do exist when $h > 1$.

1.7 **Lemma**: *If $\wp$ is (resp. is not) exceptional, the highest degree element in R has degree less than (resp. equal to) n_g.*

Proof: If $\wp$ is not exceptional, $\wp^{-1}\mathcal{A}$ has an element of degree n_g, which is not congruent to any element of lower degree modulo $\mathcal{A}$, since n_g is a gap for $\mathcal{A}$. On the other hand, any element of $\wp^{-1}\mathcal{A}$ of degree more than n_g is congruent modulo $\mathcal{A}$ to one of lower degree as can be seen by subtracting an element of same degree (which exists, as n_g is largest gap) and opposite sign.

Now we state the main theorem of this section.

1.8 **Theorem**: *Let ρ be a Drinfeld module over H. Let $i_k : H \hookrightarrow K_\infty$ be the embedding corresponding to a infinite place ∞_k of H and $\tilde{\pi}\mathcal{A}$ be the corresponding lattice. Then (with the notation as in 1.4) the degree of the Gauss sum is same at any prime above ∞_k and is less than or equal to $q^{n_g - g + 1}/(q-1)$, with equality if and only if $\wp$ is not exceptional with respect to $\mathcal{A}$.*

Proof: Let $n(i)$ be the number of monic elements of $\mathcal{A}$ of degree i. Then it is easy to see that $n(i)$ is q^{i-j}, if $n_j < i < n_{j+1}$, where for convenience we

take $n_{g+1} = \infty$. Then by [**11**] pg. 41, the degree of $\tilde{\pi}$ is (the sum is p-adic) $\sum(q-1)in(i) = \Sigma_1 + \Sigma_2$, where Σ_1 is the sum over $i \leq n_g$ and Σ_2 over $i > n_g$. Then

$$\Sigma_2 = (q-1)\sum_{k=1}^{\infty}(n_g+k)q^{n_g+k-g} = -(n_g+1)q^{n_g-g+1} + \frac{q^{n_g-g+2}}{q-1}$$

By 1.2 the degree of the Gauss sum is the degree of $e(\tilde{\pi}r_1) = \tilde{\pi}r_1\prod(1+r_1/a)$, where the product runs over nonzero $a \in \mathcal{A}$. Let us compute the degree of $r_1\prod(1+r_1/a)$. Note that there are no terms of negative degree in the product by the choice of R. It is clearly sufficient to consider only the case where $\wp$ is not exceptional. Then the degree is easily seen to be

$$n_g + \sum_{i\neq n_j, i\leq n_g}(n_g-i)(q-1)n(i) = n_g[1+\sum(q-1)n(i)] - \sum(q-1)in(i)$$

Now the sum in the bracket telescopes to q^{n_g-g+1} by the determination of $n(i)$ above. Combining with the formula for the degree of $\tilde{\pi}$, the degree of the Gauss sum then turns out to be $-q^{n_g-g+1}+q^{n_g-g+2}/(q-1) = q^{n_g-g+1}/(q-1)$ as claimed. This proves the theorem.

1.9 **Remark**: Let D be the degree of a non-principal prime of A of smallest possible degree. If the largest gap for A is smaller than $D + \underline{g} - 1$ (for example, $D > 1$ and A with gaps 1 to $\underline{g}$), then $\wp$ is not exceptional for $\mathcal{A} = \wp$ and hence for such A's, every prime has 'generic' infinite valuation for at least one ∞_k by the theorem. The situation when A has a gap $2\underline{g}-1$ gives another example of this, since then there are no exceptional primes for $\mathcal{A} = A$: The largest gap for $\wp^{h-1}$ is $\leq 2\underline{g} - 1 + (h-1)d$ and hence the largest gap for $\wp^{-1}$ is $\leq 2\underline{g} - 1 - d$. In fact, for general A, Voloch (see the appendix) shows how to find $\mathcal{A}$ with no exceptional primes with respect to it.

Section II: Sign of the Gauss sum

2.1 In this section, we restrict to the case $A = \mathbf{F}_q[T]$, with T of sgn one. Then $\rho_T = T + F$. We begin by explaining what m-th order Gauss sum, when m divides $q^d - 1$, means in our context. For $y \in \frac{1}{q^d-1}\mathbf{Z}/\mathbf{Z} - \{0\}$, let us write $0 < (q^d-1)y = \sum y_j q^j < q^d - 1$, with $0 \leq y_j < q$. Then we put $g(y) = \prod g_j^{y_j}$. Note that $g(q^j/(q^d-1)) = g_j$ corresponds to the multiplicative characters χ_j of order $q^d - 1$. Hence it is natural to consider the reduced denominator of y as the order of the Gauss sum. (For more explanation, see [**8**, **9**]). In particular, if $p \neq 2$, we can talk about the 'quadratic Gauss

sum' $g(1/2) = \prod g_j^{(q-1)/2}$. Also, $g(y)g(1-y) = \prod g_j^{q-1} = (-1)^d \wp$ (here and below $\wp$ will be assumed to be monic) can be thought of as an analogue of the well-known classical fact $g(\chi)g(\overline{\chi}) = \chi(-1)q$. (See [**8**]).

2.2 We can consider g_j as an element of $\tilde{\pi}K_\infty(\zeta_{q^d-1})$ and can talk about its 'sign' sgn. Carlitz [**1**] (but see [**11**] pg. 33 and 42 for our normalizations) gives a formula for $\tilde{\pi}$, which implies that $\tilde{\pi}^{q-1} \in K_\infty$ and $\mathrm{sgn}(\tilde{\pi}^{q-1}) = -1$. We write $\epsilon := \mathrm{sgn}(\tilde{\pi})$ and $t_j := \chi_j(T)$. Here j is considered modulo d. We first give a formula for $\mathrm{sgn}(g_j)$ in terms of ϵ and t_i's.

2.3 **Theorem**: *We have*

$$\mathrm{sgn}(g_j) = (-1)^{d-1}\epsilon \prod_{k=1}^{d-1} (t_k - t_0)^{-q^j}$$

Proof: Consider the $\mathbf{F}_q$-basis $r_i := T^{d-i}$, $0 < i \leq d$ for the representatives of $A/\wp$. Then 1.2 shows that $\mathrm{sgn}(g_j)$ is ϵ times $\chi_j(\sum)$, where $\sum := \sum_{\theta_i \in \mathbf{F}_q} (r_1 + r_2\theta_2 + \cdots + r_d\theta_d)^{-1}$. By [**1**], theorem 9.4 (there are some sign mistakes in the theorem and proof, but these are easily correctable), we have $\sum = (-1)^{d-1}/\prod(T^{q^k} - T)$ where k runs through $1 \leq k < d$. This proves the theorem.

2.4 Now in general, as can be easily seen from this theorem, the dependence of the $\mathrm{sgn}(g_j)$ or even $\mathrm{sgn}(g(1/m))$ on $\wp$ is quite complicated and not just through d. But when $m = 2$, i.e the case of quadratic Gauss sums, we have the following analogue of Gauss' theorem.

2.5 **Theorem**: *Let* $i := \epsilon^{(q-1)/2}$. *(Note* $i^2 = -1$.*) Then* $s_2 := \mathrm{sgn}(g(1/2))$ *depends only on the congruence class of* q *and* d *modulo* 4. *In fact, we have*

$$s_2 = (-i)^{d+2} \ \ (q \equiv 1 \bmod 4) \ \ \ s_2 = (-i)^{d^2+2} \ \ (q \equiv 3 \bmod 4)$$

In other words, s_2 *is* i, $(-1)^{(q-1)/2}$, $(-i)(-1)^{(q-1)/2}$ *or* -1 *according as* d *congruent to* $1, 2, 3$ *or* 4 *modulo* 4.

Proof: (We know by 2.1, $g(1/2)^2 = (-1)^d\wp$ and hence s_2 is a fourth root of unity, a priori). By the theorem 2.3 and the formula for $g(1/2)$ in 2.1, we see that $s_2 = i^d \prod (t_k - t_0)^{-(q^d-1)/2}$, with $0 < k < d$. Now $(q^d - 1)/2 = (q^{d-1} + \cdots + q + 1)(q-1)/2$. Since $t_k^{q^r} = t_{k+r}$, we have

$$\prod (t_k - t_0)^{q^{d-1}+\cdots+1} = \prod (t_j - t_i) = (-1)^{d(d-1)/2} \prod (t_j - t_i)^2 \qquad (**)$$

where $d > j \neq i \geq 0$ in the second product and $d > j > i \geq 0$ in the third. On the other hand,

$$\prod_{j>i}(t_j - t_i)^{q-1} = \frac{\prod_{j>i}(t_{j+1} - t_{i+1})}{\prod_{j>i}(t_j - t_i)} = (-1)^{d-1}$$

where the last equality follows from the fact that there are $d-1$ reversals of the sign, namely when $j = d-1$. (Another way: the 'discriminant' is square exactly when d is odd). Putting this together, we see $s_2 = i^d(-1)^{d(d-1)(q-1)/4}(-1)^{d-1}$, which is equivalent to the formulae claimed. This proves the theorem.

2.6 Now we turn to the question of sign, say s_m, of the m-th order Gauss sum $g(1/m)$, when $m > 2$. Theorem 2.3 provides a formula. Now, for the classical Gauss sums, Matthews [**7**] has given some interesting formulae when $m = 3$ or 4, in terms of '$1/m$-th residue set, factorials and 'torsion' values of elliptic functions. Theorems 2.7 and 2.10 provide rough analogues of these formulae, when m divides $q^2 - 1$. Note that $\mathbf{Q}(\zeta_3)$ and $\mathbf{Q}(\zeta_4)$ are quadratic cyclotomic extensions of $\mathbf{Q}$, whereas $K(\zeta_{q^2-1})$ is a quadratic cyclotomic extension of K. Results with weaker condition that m divides $q^d - 1$ would be more desirable. In our situation we do have 'complex multiplication' as in [**7**], and the exponential for $\mathbf{F}_{q^d}[T]$ seems to be a good function in the place of elliptic functions of [**7**], but we have not been able to make a stronger analogy. On the other hand, in the general case, our formulae can be considered to be in the spirit of Patterson's simplification (see [**7**]) of Matthews' formulae. For history of the subject, various analogies and comparison of complexities of different formulae, see [**7**].

Let S be a '$1/(q-1)$-th residue set modulo $\wp$', i.e. a set of representatives of $(A/\wp)^*/\mathbf{F}_q^*$. Define $\alpha(S) \in \mathbf{F}_{q^d}^*$ by $\alpha(S) \equiv \prod_{s\in S} s \bmod \wp$. Then by $\mathbf{F}_q$-linearity of $e(z)$, $\mu := \prod_{s\in S} e(s\tilde{\pi}/\wp)/\alpha(S)$ is independent of the choice of S. Then it is easy to see from the fact that product of all nonzero $\wp$-torsion points is $\wp$, that $g(1/(q-1))^{q-1} = (-1)^d\wp = -\mu^{q-1}$.

2.7 **Theorem** *We have*

$$s_{q-1} = (-1)^{d(d-1)/2}\epsilon^{-d}\mathrm{sgn}(\mu)^2$$

Proof: By theorem 2.3 and (**), we have $s_{q-1} = (-1)^{d(d-1)/2}\epsilon^d \prod(t_j - t_i)^{-2}$, where the product is over $d > j > i \geq 0$. Hence it is enough to show that $\mathrm{sgn}(\mu) = \epsilon^{(q^d-1)/(q-1)} \prod(t_j - t_i)^{-1}$. We can choose S to be the set of all monic elements of A of degree less than d. Let D_j denote the product

of all monic elements of A of degree j. Then it is enough to show that $\chi_0(D_{d-1}\cdots D_1 D_0) = \prod(t_j - t_i)$. Now $D_j = \prod_{i<j}(T^{q^j} - T^{q^i})$, by [**1**] pg. 140. The claim and the theorem now follow easily.

2.8 **Remark**: Let m divide $q-1$. Choose a set S_0 of representatives for $\mathbf{F}_q^*/ < \zeta_m >$ and let S' be $1/m$-th residue set. We can choose S' to consist of elements of degree less than d and with signs in S_0. Let μ' be defined in analogous fashion to μ with S' in place of S. Then $\mathrm{sgn}(\mu') = \mathrm{sgn}(\mu)^{(q-1)/m}$ and $s_m = s_{q-1}^{(q-1)/m}$. Hence the theorem provides a similar formula for s_m.

2.9 Now consider m dividing q^2-1. As in 2.8, it is enough to consider $m = q^2-1$. Let $\wp$ be such that the norm of $\wp$ (i.e. q^d) be congruent to one modulo m, so that d is even and $\wp$ splits in $B := \mathbf{F}_{q^2}[T]$ as say $\wp = \wp_1\wp_2$. We identify $(A/\wp)^*$ with $(B/\wp_1)^*$. By theorem 2.3, ignoring the explicit powers of -1 and ϵ, the interesting part of s_{q^2-1} is $\mathcal{S} := \prod(t_j - t_0)^{(q^d-1)/(q^2-1)}$. Let $\alpha_1 := \prod(t_j - t_i)$, where the product runs through $d > j > i \geq 0$ and let $\alpha_2 := \prod(t_j - t_i)$, where the product runs through $d > j > i \geq 0$ and i, j are even. Then α_1 and α_2 are $\alpha(S)$'s for S as in 2.6 for α_1; but for S corresponding to B and $\wp_1$ in place of A and $\wp$ for α_2.

2.10 **Theorem**: *We have* $\mathcal{S} = \alpha_2^{1-q}\alpha_1$.

Proof: It is easy to see that $\mathcal{S} = \prod(t_j - t_i)$ where i is even and $j \neq i$. Decomposing the product over $i > j$ and $i < j$, we see that $\mathcal{S} = \alpha_2 \prod(t_j - t_i)$, where now the product is over $j > i$ and at least one of i or j is even. But then this product is α_1/α_2^q and hence the theorem is established.

2.11 **Remark**: By [**1**] pg. 148, the sum $\sum$ in the proof of the theorem 2.3 can also be expressed as $(-1)^{d-1}\Pi(q^{d-1}-1)/\Pi(q^{d-1})$, where Π is Carlitz' factorial. (See [**1**], [**11**]). This gives a simple expression for the sign of Gauss sums in terms of Carlitz factorials.

References

[**1**] Carlitz L. - *On certain functions connected with polynomials in a Galois field*, Duke Math J. 1 (1935), 137-168.

[**2**] Drinfeld V. - *Elliptic modules*, (Translation), Math. Sbornik 23 (1974), 561-592.

[**3**] Gross B. and Koblitz N. - *Gauss sums and the p-adic* Γ *function*, Ann. Math. 109 (1979), 569-581.

[**4**] Hayes D. - *Explicit class field theory in global function fields*, Studies in Algebra and Number theory - Ed. G. C. Rota, Academic press (1979), 173-217.

[**5**] Hayes D. - *Stickelberger elements in function fields*, Compositio Math. 55 (1985), 209-239.

[**6**] Leitzel J., Madan M., Queen C. - *On congruence function fields of class number one*, J. Number theory 7 (1975), 11-27.

[**7**] Matthews C. R. - *Gauss sums and elliptic functions I , II*, Inv. Math. 52 (1979), 163-185 and 54 (1979), 23-52

[**8**] Thakur D. - *Gamma functions and Gauss sums for function fields and periods of Drinfeld modules*, Thesis, Harvard University, (1987).

[**9**] Thakur D. - *Gauss sums for* $\mathbf{F}_q[T]$, Invent. Math. 94 (1988), 105-112.

[**10**] Thakur D. - *Gauss sums for function fields*, J. Number theory 37 (1991), 242-252.

[**11**] Thakur D. - *Gamma functions for function fields and Drinfeld modules*, Ann. Math. 134 (1991), 25-64.

[**12**] Thakur D. - *Shtukas and Jacobi sums*, To appear in Inventiones Math.

[**13**] Yu J. - *Transcendence and Drinfeld modules*, Inv. Math 83 (1986), 507-517.

School of Mathematics, University of Minnesota, Minneapolis, MN 55455, U. S. A.

Appendix to Dinesh S. Thakur's 'Behavior of function field Gauss sums at ∞'

José Felipe Voloch

The notion of exceptional prime is introduced in [**15**], definition 1.4. We characterize exceptional primes, show that they always exist when the class number is bigger than one and make other remarks about them.

We shall use a more geometric language. Let X be an algebraic curve defined over a finite field and P a rational point of X, which will play the role of ∞ in [**15**]. Recall that there is a 1-1 correspondence between fractional ideals of the ring of functions on X holomorphic away from P and divisors on X with support disjoint from P. Proofs of results on orders of linear system used below can be found in [**14**].

Denote by, for a divisor D, $L(D) = \{x \in K : (x) + D \geq 0\}$ and by $l(D)$ its dimension over the field of constants. The gaps of an ideal defined by a divisor D are the integers for which L(nP - D) = L((n-1)P - D). Indeed, this means that any function on the ideal with degree at most n has degree at most n-1. Recall that a prime divisor P' is exceptional for D if the highest gap for D is also a gap for $D - P'$. Let K be a canonical divisor of X.

Theorem: *If D is a divisor of X, let m be the biggest integer for which $K + D$ is linearly equivalent to $mP + D'$ for some divisor $D' \geq 0$. Then the exceptional prime divisors for D are the prime divisors of D'.*

Proof: Let n be a gap for D and apply Riemann-Roch to the above equality, we get $l(K + D - (n-1)P) = l(K + D - nP) + 1$. That implies that $K + D$ is linearly equivalent to $(n-1)P + D'$ for some positive divisor D' which doesn't have P in its support. That means that $n - 1$ is an order at P for the linear system $|K + D|$. Conversely, if $n - 1$ is an order, n is a gap. Finally, if n is the largest gap then no prime factor of D' can move in a linear system, for otherwise we would find a linearly equivalent divisor passing through P and and $n-1$ wouldn't be the maximal order. Let's take n maximal and P' a prime divisor of D' and prove that P' is exceptional for the ideal generated by D. It suffices to show that n is a gap for $D - P'$. First, by maximality of n, $l(K + D - (n-1)P) = 1$. On the other hand

$$l(K + D - (n-1)P) \geq l(K + D - (n-1)P - P') \geq 1.$$

The last inequality is true since P' divides D'. Finally, $l(K+D-nP-P') \leq l(K + D - nP) = 0$, so n is a gap for $D - P'$, as desired.

Corollary 1: *The exceptional primes are the primes P' satisfying $dim|P'| = 0$.*

Proof: As remarked above $dim|P'| = 0$ if P' is exceptional. Conversely if Q is a prime divisor with $dim|Q| = 0$, take n large so that $nP + Q$ is linearly equivalent to $K + D$ for some positive D. It follows by reversing the above argument that Q is exceptional for the ideal defined by D.

We can now give a quick proof of theorem 1.5 of [**15**]. Note that by Riemann Roch, $\deg(D') \leq g$ above, which gives a proof that a prime of degree at least $g+1$ is not exceptional. Also, principal primes have positive dimension, so are not exceptional. Also, divisors of degree 1 have dimension zero unless principal, so are principal or exceptional.

On the same vein, a divisor of degree 2 on a curve of genus at least two has dimension zero unless the curve is hyperelliptic and the divisor is in the g^1_2 linear system, in which case it is principal if and only if the point at infinity is a Weierstrass point on the hyperelliptic curve.

Corollary 2: *If X has class number bigger than one, then it has exceptional primes.*

Proof: By the theorem, given a divisor D, it will fail to have an exceptional prime if and only if $D + K$ is linearly equivalent to mP for some m (i.e. $D' = 0$ in the proof of the theorem). If this is the case $D - \deg(D)P$ is linearly equivalent to $\deg(K)P - K$. If this happens for all D then X has class number 1, as desired.

Let m be large enough so that mP is linearly equivalent to $K + D$, for some positive D, then this D gives an example of a divisor that has no exceptional primes with respect to it.

References

[**14**] Stöhr, K.-O. and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc., **52** (1986) 1-19.

[**15**] Thakur, D. S., *Behavior of function field Gauss sums at ∞.*

IMPA, Est. D. Castorina, 110, Rio de Janeiro, Brazil.
(current)Dept. of Mathematics, Univ. of Texas at Austin, Austin, TX 78712, U.S.A..