Universal Generators for Primary Closures of Galois Fields

Dirk Hachenberger

Institut für Mathematik der Universität Augsburg
D-86135 Augsburg
Germany
e-mail: hachenberger@math.uni-augsburg.de

Dedicated to Heinz Lüneburg on the occasion of his 65th birthday.

Abstract If $\bar{F}$ is an algebraic closure of a Galois field F, then for each integer $n \geq 1$ there is exactly one subfield E_n of $\bar{F}$ containing F and having degree n over F. For a prime number r, we consider the r-primary closure $\bar{F}_r := \bigcup_{m \geq 0} E_{r^m}$ over F and prove, under the assumption that $r \geq 7$, but without any restriction on the cardinality q of F, the existence of a *universal generator* for $\bar{F}_r$ over F: this is a sequence $w = (w_{r^m})_{m \geq 0}$ in $\bar{F}_r$ which satisfies all the following properties:

(1) w_{r^m} is a primitive element of E_{r^m} (for all $m \geq 0$),
(2) w_{r^m} generates a normal basis for E_{r^m} over F (for all $m \geq 0$),
(3) w is norm-compatible,
(4) w is trace compatible.

We prove furthermore that (2) can be strengthened to

(2^c) w_{r^m} is completely free in E_{r^m} over F (for all $m \geq 0$),

which means that w_{r^m} simultaneously generates a normal basis for E_{r^m} over E_{r^i} for all $i = 0, 1, ..., m$, whence w is called a *complete universal generator* for $\bar{F}_r$ over F. The results establish a (complete) primitive normal basis theorem for $\bar{F}_r$ over F.

1 (Complete) Universal Generators

It is well-known that the multiplicative group E^* of a Galois field E is cyclic, i.e., free on one generator as a module over the ring of integers. If $u \in E$ is a generator of E^*, then u is called *primitive in E*.

A further classical result is the *normal basis theorem*: for every extension E/F of Galois fields, there exists $v \in E$ such that v generates the additive group of E as a module over the group algebra FG, i.e., $v^G = \{v^g | g \in G\}$ is a basis of E as F-vector space (here, G denotes the (cyclic) Galois group of E/F); v is called *free* or *normal in E over F*. (Unfortunately, the terminology is not consistent. Since we also work with the norm-mapping, we shall here use the term *free*.) In this generality the normal basis theorem for finite fields was first proved by Hensel [He] in 1888.

Besides their theoretical importance, primitive and free elements are interesting for some practical purposes as well, because they allow presentations of Galois fields, which are useful for applications where the arithmetic in the underlying fields has to be performed efficiently (such as the decoding for error-correcting codes, the encryption and key-exchange in public-key-cryptosystems, or the generation of pseudorandom numbers). For the basic theory, applications and the arithmetic of finite fields we refer to Jungnickel [Ju] and Lidl and Niederreiter [LiNi]. For the early history of Galois fields we refer to Lüneburg [Lü]. For the theory of normal bases we refer to Hachenberger [Ha1].

It is natural to ask, whether, for a Galois field extension E/F, there exists a primitive element of E which is additionally free over F. Completing previous work of Carlitz [Ca] and Davenport [Da], the final answer was only given in 1987, when Lenstra and Schoof [LeSc] proved the *primitive normal basis theorem*, which states that this is indeed the case for every extension E/F.

In the present paper we are concerned with an (infinite) version of the primitive normal basis theorem for the r-primary closure $\bar{F}_r$ of a Galois field F. Before stating our main results, Theorem 1.2 and its *complete* version Theorem 1.2^c, we have to introduce some terminology.

Working in an algebraic closure $\bar{F}$ of a Galois field F, for a nonempty set N of positive integers, we denote by E_N the set $\{E_n | n \in N\}$ of extensions over F (where E_n is as in the abstract). Let $w = (w_n)_{n \in N}$ be a sequence in $\bar{F}$ such that $w_n \in E_n$ for each n. Then w is called *norm-compatible*, if for all $l, n \in N$ with l dividing n, the (E_n, E_l)-norm $\prod_{\gamma \in G_{n,l}} w_n^\gamma$ of w_n is equal to w_l (here $G_{n,l}$ denotes the Galois group of E_n over E_l). Thus, norm-compatibility just means that w belongs to the (multiplicative) projective limit of E_N with respect to the norm-mappings of the extensions associated with N. Similarly, w is called *trace-compatible*, if for all $l, n \in N$ with l dividing n, the (E_n, E_l)-trace $\sum_{\gamma \in G_{n,l}} w_n^\gamma$ of w_n is equal to w_l, i.e., w is a member of the (additive) projective limit of E_N with respect to the trace-mappings of the extensions associated with N.

A sequence $w = (w_n)_{n \in N}$ is called a *generator for* E_N, if for all $n \in N$, $F(w_n)$, the field obtained by adjoining w_n to F, is equal to E_n. A generator w is called *primitive for* E_N, if for each $n \in N$, w_n is primitive in E_n. Finally, a generator w is called *free for* E_N *over* F, if for each $n \in N$, w_n is free in E_n over F.

Definition 1.1. Let N be a non-empty set of positive integers, F a Galois field and E_N the set of finite extensions of F (in $\bar{F}$) corresponding to N. A generator w of E_N which is primitive and free over F as well as norm- and trace-compatible is called a *universal generator for* E_N *over* F. □

From an algebraic point of view the most interesting sets N are those for which $F_N := \cup_{n \in N} E_n$ is a subfield of $\bar{F}$ (infinite, if N is infinite): a norm-compatible primitive sequence can then be seen as a primitive element of F_N, while a trace-compatible free sequence can be interpreted as a free element for F_N over F (we refer to Lenstra [Le] for a rigorous justification of the latter statement, see also Scheerhorn [Sche]). It holds that F_N is a field if and only if for all $n, m \in N$ there exists an $l \in N$ such that n and m divide l. The latter is in particular the case, when N is *closed*, i.e., if for any two members n and m of N, *every* divisor of the least common multiple of n and m is again a member of N. Hence, for a closed set N, a generator for E_N contains information for *every* finite subfield of F_N.

It is not known at all for which closed sets there exist universal generators. In the present contribution, however, we prove the existence of such an interesting object for certain *infinite* closed sets. For a prime r, let N_r be the closed set $\{r^m | m \geq 0\}$, whence E_{N_r} is a tower of extensions over F and $F_{N_r} = \bar{F}_r$ is the r-primary closure of F (in $\bar{F}$).

Theorem 1.2. *Let F be any Galois field and let $r \geq 7$ be any prime. Then there exists a universal generator for E_{N_r} over F.*

We shall be able to strengthen the assertion of Theorem 1.2 even further by requiring that all members w_{r^m} of the universal generator w are completely free over F (an element v of E_n is called *completely free over F* if v is simultaneously free over E_d for every divisor d of n).

Definition 1.3. Let N be a non-empty set of positive integers and F a Galois field. A generator w for E_N is called *completely free for E_N over F*, if for each $n \in N$, w_n is completely free in E_n over F. A universal generator for E_N over F which is completely free is called a *complete universal generator for E_N over F.* □

Theorem 1.2^c. *Let F be any Galois field and let $r \geq 7$ be any prime. Then there exists a complete universal generator for E_{N_r} over F.*

We give an outline of the content of the present paper.

The basic technique for proving Theorem 1.2 is by induction (on the exponent m of r). In order to accomplish the induction step (see Section 2) we consider a problem which is interesting in itself, namely, whether for a quadruple (F, K, L, E) of Galois fields (E an extension of F and K, L intermediate fields of E/F) and given elements $a \in K$ (free over F) and $b \in L$ (primitive) there exists an element $w_{a,b} \in E$ which is primitive and free over F, whose (E, K)-trace is equal to a and whose (E, L)-norm is equal to b. In this context, our main result is Theorem 2.3 (from which Theorem 1.2 immediately follows). Observe that Theorem 2.3 asserts more than is necessary for proving Theorem 1.2, because we show that (for all m) *every* universal generator for $E_{\{1,r,r^2,\ldots,r^m\}}$ can be *extended* to one of E_{N_r}.

In order to prove Theorem 2.3, a sufficient criterion for the existence of an element $w_{a,b}$ as above is derived in Section 3 by means of characters and Gauss sums for E/F (see Proposition 3.1). The proof of Theorem 2.3 is completed in Section 4 by applying concrete versions of that criterion to the case where E/F has prime power degree and $K = L$ is the unique maximal intermediate field of that extension (see Section 4).

We have assumed that $r \geq 7$, because we seeked to obtain a result which holds independently from the cardinality q of the ground field F. Our criterion is less effective when $r = 5$: in that case it yields only the *asymptotic* existence of universal generators, i.e., as long as q is large enough. If $r = 2$ or $r = 3$ the criterion does not work at all with $K = L$ being the maximal intermediate field. However, when seeking for results with $r = 2, 3, 5$, unrestricted in q, one can study towers with relative degrees $8, 9, 25$, i.e., with larger gaps in the relative degrees. We shall not work out the latter here.[1]

In Section 6, we shall prove Theorem 1.2^c. We postpone a more detailed discussion of completeness to Section 5.

Finally, in Section 7 we conclude with some remarks.

2 Universal Quadruples

Let (q, k, l, n) be a quadruple of nonnegative integers, where $q > 1$ is a prime power and k, l are proper divisors of n, and let (F, K, L, E) be the corresponding quadruple of Galois fields, i.e., $F = \mathrm{GF}(q)$, and, in a fixed algebraic closure $\bar{F}$ of F, $K = E_k$, $L = E_l$ and $E = E_n$.

Definition 2.1. (q, k, l, n) is called *universal*, if for the corresponding quadruple (F, K, L, E) it holds that for **every** $b \in L$ which is primitive in L and for **every** $a \in K$ which is free in K over F, there exists an element $w = w_{a,b}$ in E which satisfies all the following properties:

(1) w is primitive in E,
(2) w is free in E over F,
(3) $\mathrm{N}_{E,L}(w)$, the (E, L)-norm of w, is equal to b,
(4) $\mathrm{Tr}_{E,K}(w)$, the (E, K)-trace of w, is equal to a. □

As norms of primitive elements are primitive and traces of free elements are free, the assumptions on $a \in K$ and $b \in L$ are necessary.

So far, the universality of quadruples has only been considered for the case where $k = l = 1$, which in view of Proposition 2.4 is the easiest instance of the problem. (In this case $K = L = F$, a is any nonzero element of F and b is any primitive element of F.) First, in [CoHa], Cohen and Hachenberger have proved that, for $n \geq 9$, $(q, 1, 1, n)$ is universal for every prime power q; moreover, for $n = 7, 8$ the universality of $(q, 1, 1, n)$ is proved except for 8 values of q.[2] The main tool in [CoHa] is Proposition 3.1 of the present

[1] We refer to Hachenberger [Ha2]; in that paper, a similar problem is studied, namely the existence of trace-compatible primitive free generators for E_{N_r} over F.

[2] In [CoHa], (q, n) is called a *PFNT-pair*, if, in the present notation, $(q, 1, 1, n)$ is universal.

paper, applied to the case $k = l = 1$ (the corresponding result is not proved in [CoHa] and neither is proved a character sum formulation, which, for the general case is carried out in Section 3 of the present paper). By improving the estimates for Gauss sums and by developing a sieving technique (both are available for the case $K = L = F$, only), Cohen [Co] was able to prove the universality of $(q,1,1,n)$ for all $n \in \{5,6,7,8\}$ and all q, whence altogether the following holds.

Theorem 2.2. *If $n \geq 5$ then $(q,1,1,n)$ is universal for all prime powers $q \geq 2$.* □

Since we want to prove the existence of universal generators for primary closures of Galois fields, we consider here the case where the degree of E/F is a power of a prime. The main result in this direction is the following theorem (which is proved in Section 3 and Section 4).

Theorem 2.3. *Assume that $r \geq 7$ is a prime. Let $q > 1$ be any prime power and $m \geq 0$ be any integer. Then (q, r^m, r^m, r^{m+1}) is universal.*

Observe that the case $m = 0$ is covered by Theorem 2.2, and we therefore restrict our attention to the case $m \geq 1$, later. Now, Theorem 1.2 follows at once by induction from Theorem 2.3.

Proof of Theorem 1.2. If $w_1 \in F$ is primitive, then, trivially, $(w_n)_{n\in\{1\}}$ is a universal generator for E_1 over F. For $m \geq 0$ assume that $(w_n)_{n\in\{1,r,\ldots,r^m\}}$ is a universal generator for $E_{\{1,r,\ldots,r^m\}}$ over F. As (q, r^m, r^m, r^{m+1}) is universal, there exists $v = w_{m+1} \in E = E_{r^{m+1}}$ which is primitive in E, free over F and satisfies $\mathrm{Tr}_{E,E_{r^m}}(v) = w_m = \mathrm{N}_{E,E_{r^m}}(v)$. The transitivity of the trace- and norm-mappings now implies that $(w_n)_{n\in\{1,r,\ldots,r^{m+1}\}}$ is a universal generator for $E_{\{1,r,\ldots,r^{m+1}\}}$ over F, and everything is proved. □

We finally mention that Theorem 2.3 can be strengthened as follows.

Theorem 2.3'. *Assume that $r \geq 7$ is a prime. Let $q > 1$ be any prime power. Then $(q, r^\alpha, r^\beta, r^\gamma)$ is universal for all $\alpha, \beta \geq 0$ and all $\gamma > max\{\alpha, \beta\}$.* □

The latter is an immediate consequence of the following proposition.

Proposition 2.4. *Assume that (q,k,l,n) is universal. Let k' be a divisor of k and l' a divisor of l. Then (q,k',l',n) likewise is universal.*

Proof. If $a' \in E_{k'}$ is free over $F = \mathrm{GF}(q)$, then there exists an element a in E_k, free over F, whose $(E_k, E_{k'})$-trace is equal to a'. Analogously, if $b' \in E_{l'}$ is primitive, then there exists a primitive $b \in E_l$ such that the $(E_l, E_{l'})$-norm of b is equal to b'. Since (q,k,l,n) is universal by assumption, the result follows using the transitivity of the norm- and trace-mappings. □

3 Character Sum Formulation and a Sufficient Criterion

In the present section we shall prove a sufficient criterion for a quadruple (q,k,l,n) to be universal (see Proposition 3.1). We have to introduce some notation. Let $P = P(q,n,l)$ be the largest divisor of $q^n - 1$ which is relatively prime to $q^l - 1$ and let $\omega = \omega(P)$ be the number of distinct prime divisors of P. Let $t = t(q,n,k)$ be the largest monic divisor of $x^n - 1$ which is relatively prime to $x^k - 1$ and let $\Omega = \Omega(q,n,k)$ be the number of distinct monic irreducible F-divisors of t.

Proposition 3.1. *Assume that (q,k,l,n) is as at the beginning of Section 2. If*

$$\frac{q^{\frac{n}{2}}}{q^k(q^l-1)} > \left(2^{\Omega} - \frac{1}{q^k}\right) \cdot \left(2^{\omega} - \frac{1}{q^l-1}\right), \tag{3.1}$$

then (q,k,l,n) is universal.

The proof of Proposition 3.1 is based on the character-sum formulation of the four conditions in Definition 2.1 and on an estimate for Gauss sums. We let (F,K,L,E) be the quadruple of fields corresponding to (q,k,l,n), throughout.

We first investigate *the multiplicative part* which comprises the primitivity and the condition of prescribed (E,L)-norm, i.e., (1) and (3) in Definition 2.1. For simplicity let N denote the (E,L)-norm mapping.

For a divisor d of $q^n - 1$ let C_d be the unique (cyclic) subgroup of the multiplicative group of E^* having cardinality d. Let furthermore D denote the cofactor of P in $q^n - 1$ and let δ be the cofactor of $q^l - 1$ in D. Thus, L^* is a subgroup of C_D, and, as D and P are relatively prime, E^* decomposes into the direct product of C_D with C_P. This decomposition is crucial for the subsequent characterization of primitive elements in E having (E,L)-norm equal to b.

Since, for $x \in E$, $N(x) = x^{\delta P}$, $C_{\delta P}$ is the kernel of N. Restricting N onto C_D induces an epimorphism onto L^* with kernel equal to C_δ. Now, with φ denoting the Euler totient function, it holds that C_D has exactly $\varphi(D) = \varphi(q^l-1)\cdot\delta$ generators (i.e., elements of E whose multiplicative order is equal to D), whence for a primitive b of L^*, the entire preimage of b under N in C_D consists of generators of the group C_D. Consequently, if $w \in E^*$ with $N(w) = b$, letting $w = w_D w_P$ (with $w_D \in C_D$ and $w_P \in C_P$), we have $b = N(w_D)$, and the above argument yields that w_D is a generator of C_D. We have proved the following.

Lemma 3.2. *An element $w \in E$ is primitive in E if and only if the (E,L)-norm of w is primitive in L and the multiplicative order of w is divisible by P.* □

From Cohen and Hachenberger [CoHa1] (or Carlitz [Ca], Davenport [Da], Lenstra and Schoof [LeSc]) we know that the function M_P in (3.2) is the characteristic function of the set of elements of E^* whose multiplicative order is divisible by P.

$$M_P(w) = \frac{\varphi(P)}{P} \sum_{d|P} \frac{\mu(d)}{\varphi(d)} \sum_{(\eta,d)} \eta(w), \qquad w \in E^* \tag{3.2}$$

(μ denotes the Möbius function and the first sum runs over all positive divisors of P, while the second one runs over all $\varphi(d)$ multiplicative characters $\eta \in E^*$ whose multiplicative order is equal to d).

The set of elements $w \in E^*$ having (E, L)-norm equal to b can be described by its characteristic function N_b which in (3.3) is given in terms of the group $\hat{L}^*$ of multiplicative characters of L.

$$N_b(w) := \frac{1}{q^l - 1} \sum_{\nu \in \hat{L}^*} \nu(N(w)b^{-1}), \qquad w \in E^*. \tag{3.3}$$

Thus, combining (3.2) with (3.3), we conclude that $w \in E^*$ satisfies the conditions (1) and (3) of Definition 2.1 if and only if $M_P(w)N_b(w) = 1$.

We next investigate *the additive part*, comprising the freeness and the prescribed (E, K)-trace, i.e., the conditions (2) and (4) of Definition 2.1. For simplicity, let T denote the (E, K)-trace mapping. Then, with $\hat{K}$ being the group of additive characters of K, the mapping T_a in (3.4) is the characteristic function of the set of all $w \in E$ such that $T(w) = a$.

$$T_a(w) := \frac{1}{q^k} \sum_{\lambda \in \hat{K}} \lambda(T(w) - a), \qquad w \in E. \tag{3.4}$$

In order to cope with the freeness, we have to recall that the additive group of E is equipped with a module structure over the polynomial ring $F[x]$ by defining $f \circ w := f(\sigma)(w)$ (for $w \in E$ and $f \in F[x]$), where σ is a generator of the Galois group of E/F, the Frobenius automorphism for instance. The *F-order* of $w \in E$ is the monic polynomial $f \in F[x]$ of least degree such that $f \circ w = 0$. The group $\hat{E}$ of additive characters of E likewise carries the structure of an $F[x]$-module by defining $(f \circ \chi)(w) := \chi(f \circ w)$ (where $\chi \in \hat{E}$, and f, w are as above). Similarly, the F-order of $\chi \in \hat{E}$ is defined to be the monic polynomial $f \in F[x]$ of least degree such that $f \circ \chi = \chi_0$, the trivial additive character. As $\hat{E}$ and the additive group of E are isomorphic as $F[x]$-modules (namely free on one generator with minimal polynomial $x^n - 1$), for each monic divisor $g \in F[x]$ of $x^n - 1$ there are exactly $\phi_q(g)$ characters $\chi \in \hat{E}$ whose F-order is equal to g, where $\phi_q(g)$ is the number of units in the ring $F[x]/gF[x]$ (i.e., ϕ_q is the q-analogue of the Euler totient function).

Now, compare again with [CoHa1] (or [Ca], [Da], [LeSc]), with t as in Proposition 3.1, it holds that A_t in (3.5) is the characteristic function of the set of elements in E whose F-order is divisible by t.

$$A_t(w) := \frac{\phi_q(t)}{q^{\deg t}} \sum_{g|t} \frac{\mu_q(g)}{\phi_q(g)} \sum_{(\chi,g)} \chi(w), \tag{3.5}$$

where, the first sum runs over all monic F-divisors of t and the symbol (χ, g) indicates that the second sum runs over all additive characters of E having F-order equal to g.

The following is the additive analogue of Lemma 3.2. It implies that $w \in E$ satisfies (2) and (4) of Definition 2.1 if and only if $A_t(w)T_a(w) = 1$.[3]

Lemma 3.3. *An element $w \in E$ is free in E over F if and only if its (E, K)-trace is free in K over F and its F-order is divisible by t.*

Proof. Let p be the characteristic of F and let π be the largest power of p dividing n/k. Then t is equal to $(x^n - 1)/(x^{k\pi} - 1)$ (which is relatively prime to $x^k - 1$). This leads to a decomposition of the additive group of E into the direct sum $\tilde{K} \oplus \mathcal{T}$, where $\tilde{K}$ is the extension of degree $k\pi$ over F, and where $\mathcal{T}$ is the kernel of the $(E, \tilde{K})$-trace mapping. For $w \in E$, let $w_{\tilde{K}} + w_{\mathcal{T}}$ be the decomposition of w corresponding to that of E. By Theorem 8.6 in Hachenberger [Ha1], it holds that w is free over F if and only if $w_{\tilde{K}}$ is free in $\tilde{K}$ over F and the F-order of $w_{\mathcal{T}}$ is equal to t (the latter means that $w_{\mathcal{T}}$ is a generator of $\mathcal{T}$ as $F[x]$-module). An application of Lemma 7.4 of [Ha1] shows that the F-order of the $(E, \tilde{K})$-trace of w and the F-order of $w_{\tilde{K}}$ are equal. Finally, since $\tilde{K}/K$ has degree a power of p, an application of Theorem 10.5 in [Ha1] gives that $u \in \tilde{K}$ is free over F if and only if the $(\tilde{K}, K)$-trace of u is free in K over F. From all that the assertion follows. □

Combining *the multiplicative and the additive part*, we obtain that the total number Y of elements in E which are primitive and free over F with $N(w) = b$ and $T(w) = a$, i.e., satisfying all conditions in Definition 2.1, is equal to

$$Y = \sum_{w \in E} M_P(w) N_b(w) A_t(w) T_a(w). \tag{3.6}$$

(As usual, we let $\eta(0) := 0$ if η is a nontrivial multiplicative character, and $\eta_0(0) := 1$ for the trivial multiplicative character η_0.) Letting

$$\theta := \frac{\varphi(P)}{P}, \quad \Theta_q := \frac{\phi_q(t)}{q^{\deg t}},$$

and using (3.2)-(3.5), we have

[3] Lemma 3.2 is therefore also crucial for proving Proposition 3.1 in [Ha2].

$$\frac{q^k \cdot (q^l - 1)}{\theta\Theta_q} \cdot Y = \sum_{d|P} \sum_{g|t} \frac{\mu(d)}{\varphi(d)} \frac{\mu_q(g)}{\phi_q(g)} \sum_{(\eta,d)} \sum_{(\chi,g)} \sum_{\nu \in \hat{L}^*} \sum_{\lambda \in \hat{K}} \frac{G_{a,b}(\eta\hat{\nu}, \chi\hat{\lambda})}{\nu(b)\lambda(a)}, \tag{3.7}$$

where $G_{a,b}(\eta\hat{\nu}, \chi\hat{\lambda})$ denotes the *Gauss sum*

$$G_{a,b}(\eta\hat{\nu}, \chi\hat{\lambda}) = \sum_{w \in E} (\eta\hat{\nu})(w)(\chi\hat{\lambda})(w), \tag{3.8}$$

and where $\hat{\nu} \in \hat{E}^*$ and $\hat{\lambda} \in \hat{E}$ denote the lifted characters of $\nu \in \hat{L}^*$ and $\lambda \in \hat{K}$, respectively, i.e,

$$\hat{\nu}(w) := \nu(N(w)), \quad \hat{\lambda}(w) := \lambda(T(w)), \quad w \in E.$$

The decompositions of E^* and E in Lemma 3.2 and Lemma 3.3, respectively, yield corresponding decompositions of the character groups $\hat{E}^*$ and $\hat{E}$. These are crucial for the analysis of (3.7), because $\eta\hat{\nu}$ is trivial if and only if η and $\hat{\nu}$ are both trivial, and similarly, $\chi\hat{\lambda}$ is trivial if and only if χ and $\hat{\lambda}$ are both trivial. We are now able to complete the proof of Proposition 3.1.[4]

Proof of Proposition 3.1. If $\eta\hat{\nu}$ and $\chi\hat{\lambda}$ are both trivial, then

$$G_{a,b}(\eta\hat{\nu}, \chi\hat{\lambda}) = q^n.$$

If either $\eta\hat{\nu}$ or $\chi\hat{\lambda}$ is trivial, then $G_{a,b}(\eta\hat{\nu}, \chi\hat{\lambda}) = 0$. Finally, if both $\eta\hat{\nu}$ and $\chi\hat{\lambda}$ are nontrivial, then the absolute value of $G_{a,b}(\eta\hat{\nu}, \chi\hat{\lambda})$ is equal to $q^{n/2}$.

Now, using properties of the Möbius functions as well as the triangle inequality in combination with the absolute values of the Gauss sums, we obtain

$$\left| \frac{q^k \cdot (q^l - 1) \cdot Y}{\theta\Theta_q} - q^n \right| \leq q^{\frac{n}{2}} \cdot (U + V + W + X),$$

where $U = (2^\omega - 1)(q^l - 1)(2^\Omega - 1)q^k$, $V = (2^\omega - 1)(q^l - 1)(q^k - 1)$, $W = (q^l - 2)(2^\Omega - 1)q^k$ and $X = (q^l - 2)(q^k - 1)$. Thus, $Y = 0$ implies

$$\frac{q^{n/2}}{q^k \cdot (q^l - 1)} \leq (2^\Omega - \frac{1}{q^k}) \cdot (2^\omega - \frac{1}{q^l - 1}),$$

and everything is proved. □

[4] For the basic properties of Gauss sums we refer to Section 5.2 of Lidl and Niederreiter [LiNi] or Section 7.2 of Jungnickel [Ju].

4 Proof of Theorem 2.3

In the present section, in order to complete the proof of Theorem 2.3, we analyse the sufficient condition in Proposition 3.1 for quadruples (q, r^m, r^m, r^{m+1}), where $r \geq 7$ is a prime number and where $m \geq 1$ (recall that $m = 0$ is covered by Theorem 2.2). Using the notation of the previous section, we have $t = 1$ if $r = p$ is the characteristic of $F =$GF(q), whereas $t = \Phi_{r^{m+1}}$ is the r^{m+1}st cyclotomic polynomial if $r \neq p$. In the following, $|\Lambda|$ denotes the cardinality of the set Λ.

Proposition 4.1. *Let $q > 1$ be a prime power and r a prime. Let $\lambda \geq 1$ be an integer, Λ a set of primes $s < \lambda$ such that each prime divisor of P which is less than λ is contained in Λ, and let $L(\Lambda) = \prod_{s \in \Lambda} s$ (being equal to 1 if Λ is empty). Finally, if $r \neq p$, let $\delta = \mathrm{ord}_{r^{m+1}}(q)$; if $r = p$, let $\delta = \varphi(r^{m+1})$. If*

$$\left(\frac{r-4}{\log 4} - \frac{r-1}{\log \lambda}\right) \cdot \log q \geq \frac{r-1}{\delta} + \frac{1}{r^m} \cdot \left(|\Lambda| - \frac{\log L(\Lambda)}{\log \lambda}\right), \tag{4.1}$$

then (q, r^m, r^m, r^{m+1}) is universal.

Proof. With ω as in Section 3, it follows from Lemma 2.6 of Lenstra and Schoof [LeSc] that

$$\omega \leq \frac{\log P - \log L(\Lambda)}{\log \lambda} + |\Lambda|.$$

Furthermore, $\Omega = 1$ if $r = p$ and

$$\Omega = \varphi(r^{m+1})/\mathrm{ord}_{r^{m+1}}(q) \leq (r-1)r^m$$

if $r \neq p$, where $\mathrm{ord}_{r^{m+1}}(q)$ denotes the order of q modulo r^{m+1}. Using these upper bounds, an easy calculation shows that the validity of (4.1) implies that of (3.1) (with $k = l = r^m$), whence everything is proved. □

We next return to the case $r \geq 7$. In that case, a choice of $\lambda \geq 17$ asserts that the factor

$$N(r, \lambda) := \frac{r-4}{\log 4} - \frac{r-1}{\log \lambda} \tag{4.2}$$

of $\log q$ in the left hand side of (4.1) is greater than zero. In what follows, we have always chosen $\lambda = 300$. For $r \neq p$, we let $\alpha(q, r, m, \lambda, \Lambda)$ denote the right hand side of (4.1), and for $r = p$, let $\beta(r, m, \lambda, \Lambda)$ be the right hand side of (4.1). For an integer $d \geq 1$, let

$$\gamma(r,m,d,\lambda,\Lambda) := \frac{r-1}{d} + \frac{1}{r^m}\cdot\left(|\Lambda| - \frac{\log L(\Lambda)}{\log\lambda}\right). \tag{4.3}$$

Step 1. Assume first that $q-1$ is divisible by r.

Then, independently from m, each prime divisor s of P is congruent to 1 modulo $2r$, whence Proposition 4.1 is applicable with Λ being the set of all primes $s < \lambda$ such that $s-1$ is divisible by $2r$. Now, $\log q < \gamma(r,1,1,\lambda,\Lambda)/N(r,\lambda)$ implies $q \le 267$ if $r = 7$; $q \le 21$ if $r = 11$ and $q \le 13$ if $r \ge 13$. Since $\gamma(r,1,1,\lambda,\Lambda)$ is an upper bound for $\alpha(q,r,m,\lambda,\Lambda)$ for all $m \ge 1$, we are therefore left with the cases where $r = 7$ and $q \in \{8,29,43,64,71,113,127,169,197,211,239\}$. For each q of the latter set we apply Proposition 4.1 with $\Lambda = \Lambda_\lambda(q,7^\infty)$ being the set of all primes $s < \lambda$ such that $\mathrm{ord}_s(q)$ is a power of 7: we obtain that (4.1) is satisfied for all these q with $m = 1$, except when $q = 197$. But (4.1) is satisfied for $q = 197$ and $m = 2$. Now, it is important to observe that

$$\alpha(q,r,m,\lambda,\Lambda_\lambda(q,7^\infty)) \ge \alpha(q,r,M,\lambda,\Lambda_\lambda(q,7^\infty)), \quad \text{if } M \le m. \tag{4.4}$$

Since the left side of (4.1) is independent of m, it therefore remains to show that $(197,7,7,49)$ is universal. We apply Proposition 3.1: P has only one prime divisor which is smaller than 10000 (namely 1373), whence $\omega \le 29$; since $\Omega = 42$, (3.1) is valid for $(197,7,7,49)$. Altogether, we have shown that (q,r^m,r^m,r^{m+1}) is universal for all $m \ge 1$, all $r \ge 7$ and all q such that $q-1$ is divisible by r.

Step 2. Assume that $q-1$ is not divisible by r, that $r \ne p$ and that $q \ge 4$ if $r \ge 17$.

Independently from m, we first choose Λ to be the set of all odd primes $s < \lambda$ (recall that P is odd). Here, $\gamma(r,1,2,\lambda,\Lambda)$ is an upper bound for $\alpha(q,r,m,\lambda,\Lambda)$ for all $m \ge 1$, and $\log q < \gamma(r,1,2,\lambda,\Lambda)/N(r,\lambda)$ implies $q \le 74$ if $r = 7$, $q \le 6$ if $r = 11$, $q \le 4$ if $r = 13$ and $q \le 3$ if $r \ge 17$. For the remaining values for q and r, we apply Proposition 4.1 with $\Lambda = \Lambda_\lambda(q,r^\infty)$ (see Step 1). Here, (4.1) is satisfied for all the remaining cases with $m = 1$, and thus, using again (4.4), we conclude that (q,r^m,r^m,r^{m+1}) is universal for all $m \ge 1$, all $r \ge 7$ and all q as in the assumption.

Step 3. Assume that $q = 2$ or $q = 3$ and that $r \ge 17$.

In either case for q, and independently from m, we first take Λ to be the set of odd primes $s < \lambda$ different from p. As $r \ge 17$, we have $\mathrm{ord}_r(q) \ge 5$, whence $\gamma(r,1,5,\lambda,\Lambda)$ is an upper bound for $\alpha(q,r,m,\lambda,\Lambda)$ for all $m \ge 1$. Since $\log q \ge \gamma(r,5,1,\lambda,\Lambda)/N(r,\lambda)$ for all $r \ge 17$ and $q \in \{2,3\}$, Proposition 4.1 yields the universality of (q,r^m,r^m,r^{m+1}) for all quadruples under consideration.

Step 4. Assume finally that $r = p \ge 7$.

We take Λ to be the set of odd primes $s < \lambda$. Now, $\beta(q,r,1,\lambda,\Lambda)$ is an upper bound for the right hand side of (4.1) for all $m \ge 1$. Since $\log r \ge$

$\beta(r, 1, \lambda, \Lambda)/N(r, \lambda)$, for all r, (4.1) is always satisfied, and this completes the proof of Theorem 2.3. □

5 Completeness

When considering a finite dimensional Galois extension E/F, then $v \in E$ is called *completely free in* E *over* F [5], if for each intermediate field K of E/F it holds that $\{v^g | g \in G_K\}$ is a K-(normal) basis of E over K (where G_K denotes the Galois group of E/K). Completely free elements were first studied in 1957 by Faith [Fa]; he proved their existence whenever F has infinite cardinality. For finite fields the corresponding result was only proved in 1986 by Blessenohl and Johnsen [BlJo]: the *complete normal basis theorem* states that for every extension E/F of Galois fields, there exists an element in E which is completely free over F. (For an extensive treatment of the structure of completely free elements we refer to the monograph Hachenberger [Ha1].)

It is natural to ask, whether, for a Galois field extension E/F, there exists a primitive element of E which is additionally *completely* free over F. By means of a computer search, Morgan and Mullen [MoMu] have determined primitive completely free elements for all extensions $\mathrm{GF}(q^n)/\mathrm{GF}(q)$ where $q \leq 97$ and $n \leq 9$; they have therefore conjectured that such elements do always exist (i.e., for all extensions of Galois fields). A considerable step towards proving the *primitive complete normal basis theorem* is provided in Hachenberger [Ha2], where the existence is shown for a (large) class of so-called *regular extensions*. The precise formulation is given in Theorem 5.1.

Theorem 5.1. *Consider the extension* $\mathrm{GF}(q^n)/\mathrm{GF}(q)$ *of Galois fields. Let* n' *be the largest divisor of* n *which is relatively prime to* q *and let* $\nu(n')$ *be the square-free part of* n'. *Assume that* $\mathrm{ord}_{\nu(n')}(q)$ *and* n *are relatively prime. Assume further that* $q \equiv 1 \bmod 4$ *if* n' *is even. Then there exists a primitive element in* $\mathrm{GF}(q^n)$ *which is completely free over* $\mathrm{GF}(q)$.

Observe that the assumption in Theorem 5.1 is satisfied whenever n is an odd prime power, say $n = r^k$ with r being a prime. If $r \geq 7$, then for the latter class of extensions, Theorem 1.2^c is an improvement of Theorem 5.1. The proof of Theorem 1.2^c is the aim of the following section.

6 Proof of Theorem 1.2^c

Analogously to Theorem 2.1, the proof of Theorem 1.2^c is established via induction. We first have to formulate a complete version of Definition 2.1.

[5] Again, the terminology is not consistent; such elements are also called *completely normal*.

Definition 6.1. A quadruple (q,k,l,n) is called *completely universal*, if for the corresponding quadruple (F,K,L,E) of Galois fields it holds that for **every** $b \in L$ which is primitive in L and for **every** $a \in K$ which is completely free in K over F, there exists an element $w = w_{a,b}$ in E which satisfies (1), (3) and (4) in Definition 2.1 as well as

(2^c) w is completely free in E over F. □

As the trace of a completely free element is again completely free, the assumption on a is necessary.

Now, Theorem 1.2^c is an immediate consequence of Theorem 6.2.

Theorem 6.2. *Assume that $r \geq 7$ is a prime. Let $q > 1$ be any prime power and $m \geq 0$ be any integer. Then the quadruple (q, r^m, r^m, r^{m+1}) is completely universal.*

For the proof of Theorem 6.2 we shall use Theorem 2.3 in combination with the characterization of completely free elements in prime power extensions over finite fields as given in Section 17 of Hachenberger [Ha1]. Throughout, let E be the r^{m+1}-dimensional extension over the Galois field F.

First, the assertion of Theorem 6.2 is valid if r is equal to the characteristic p of F, in which case $w \in E$ is completely free over F if and only if w is free over F (see Theorem 5.7 in [Ha1]). We may therefore assume that $r \neq p$. But then the situation is totally different, because for every q there exists a free element in E over F which is not free over $\mathrm{GF}(q^r)$ as long as m exceeds a certain bound depending on q and r (see the proof of Theorem 14.5 in [Ha1] or the discussion in Section 2 of Hachenberger [Ha3]). However, as we will see below, Theorem 2.3 can nevertheless be used, when changing the ground field F to an appropriate intermediate field of E/F.

The multiplicative order of q modulo r^{m+1} is of the form

$$\mathrm{ord}_{r^{m+1}}(q) = \mathrm{ord}_r(q) \cdot r^{\alpha}, \tag{6.1}$$

where $\mathrm{ord}_r(q)$ divides $r-1$ and where $\alpha = \alpha(q,r,m) \leq m$. We define a parameter $\tau = \tau(q,r,m+1)$ as follows:

$$\tau := \lfloor \frac{\alpha}{2} \rfloor. \tag{6.2}$$

Then $\tau < m$, whence $M := E_{r^\tau}$ is a proper subfield of E containing F. Now, in combination with Theorem 2.3, Theorem 6.2 is an immediate consequence of the following proposition.

Proposition 6.3. *Let $q \geq 2$ be a prime power, r an odd prime number not dividing q, and let $m \geq 0$. Letting τ be as in (6.2) it holds that (q, r^m, r^m, r^{m+1}) is completely universal, if $(q^{r^\tau}, r^{m-\tau}, r^{m-\tau}, r^{m+1-\tau})$ is universal.*

Proof. Consider the quadruple (M, K, L, E) corresponding to $(q^{r^\tau}, r^{m-\tau}, r^{m-\tau}, r^{m+1-\tau})$. Let $a \in K = E_{r^m}$ be completely free over F (hence free over M) and let $b \in L = K$ be primitive. Assuming the universality of $(q^{r^\tau}, r^{m-\tau}, r^{m-\tau}, r^{m+1-\tau})$, there exists a primitive element $w \in E$ which is free over M such that $\mathrm{Tr}_{E,K}(w) = a$ and $\mathrm{N}_{E,L}(w) = b$. We claim that these conditions already suffice for w to be completely free in E over F, whence everything is proved.

Let $\mathcal{T}$ be the kernel of the (E, K)-trace mapping. Then, similar to the proof of Lemma 3.3 (with $K = \tilde{K}$), $K \oplus \mathcal{T}$ is a decomposition of the additive group of E as $F[x]$-module with respect to a generator σ of the Galois group G of E over F. The decomposition likewise respects the action of $M[x]$ with respect to $\psi := \sigma^{r^\tau}$, which is a generator of the Galois group of E over M (in the latter context the scalar multiplication is given by $g \star u := g(\psi)(u)$ for $g \in M[x]$ and $u \in E$). In terms of this decomposition, we have the following characterization of completely free elements for E over F (see Section 17 in [Hal]): $v = v_K + v_{\mathcal{T}}$ $(v_K \in K, v_{\mathcal{T}} \in \mathcal{T})$ is completely free in E over F if and only if v_K is completely free in K over F and the M-order of $v_{\mathcal{T}}$ (i.e., the monic polynomial g of least degree in $M[x]$ such that $g \star v_{\mathcal{T}} = 0$) is equal to $\Phi_{r^{m+1-\tau}}$, the $r^{m+1-\tau}$th cyclotomic polynomial.

It therefore remains to verify the latter two conditions for the element w given above. With $w = w_K + w_{\mathcal{T}}$ we have (by assumption) that $a = \mathrm{Tr}_{E,K}(w) = rw_K$. Hence, w_K is completely free in K over F, as a satisfies this property by assumption. We also have chosen w to be free in E over M. Consequently, an application of Theorem 8.6 of [Hal] shows that the components w_K and $w_{\mathcal{T}}$ are generators of the $M[x]$-modules K and $\mathcal{T}$, respectively. But for $w_{\mathcal{T}}$ this just means that the M-order of $w_{\mathcal{T}}$ is equal to $\Phi_{r^{m+1-\tau}}$, which is the minimal polynomial of $\mathcal{T}$ with respect to ψ over M. Thus, everything is proved. □

We finally remark that in general it is not known, whether the intermediate trace of a completely free element can be prescribed, wherefore a complete version of Proposition 2.4 is not (yet) available (see the proof of Proposition 2.4). The latter is however the case, when E/F is of prime power degree (for more details on this problem see Section 26 in [Hal]). We therefore have the following strengthening of Theorem 6.2.

Theorem 6.2'. *Assume that $r \geq 7$ is a prime. Let $q > 1$ be any prime power. Then $(q, r^\alpha, r^\beta, r^\gamma)$ is completely universal for all $\alpha, \beta \geq 0$ and all $\gamma > max\{\alpha, \beta\}$.* □

7 Concluding Remarks

We would finally like to remark that universal generators might be interesting in view of representing finite fields and their arithmetic in Computer Algebra systems.

It was suggested by J. H. Conway to use norm-compatible primitive generators for describing field extensions. The reason is that, as far as the multiplicative structure is concerned, such presentations include information on the embeddings of the various subfields. This concept is used in the computer algebra system *Magma.*

Analogously, as pointed out in Scheerhorn [Sche] (see also [CiD]), computationally simple embeddings relying on a normal-basis representation consist of trace-compatible free generators. This additive presentation is used in the computer algebra system *Axiom.*

It seems therefore to be of interest to have (complete) universal generators: they yield a *dynamic* data structure for presenting finite fields. It seems also that for finite sets E_N of small degree over small fields F the existence of these objects can only be decided experimentally. When searching for such generators one should assume that the relative degrees of the fields are at least three.

References

[BlJo] *D. Blessenohl* and *K. Johnsen*, Eine Verschärfung des Satzes von der Normalbasis, J. Algebra **103** (1986), 141-159.

[Ca] *L. Carlitz*, Primitive roots in a finite field. Trans. Am. Math. Soc. **73** (1952), 373-382.

[CiD] Computeralgebra in Deutschland (Bestandsaufnahme, Möglichkeiten, Perspektiven), Herausgegeben von der Fachgruppe Computeralgebra der GI, DMV, GAMM, Passau und Heidelberg (1993).

[Co] *S. D. Cohen*, Gauss sums and a sieve for generators of Galois fields, Publ. Math. Debrecen, **56** (2000), to appear.

[CoHa1] *S. D. Cohen* and *D. Hachenberger*, Primitive normal bases with prescribed trace, Applic. Alg. Engin. Comm. Comp. **9** (1999), 383-403.

[CoHa2] *S. D. Cohen* and *D. Hachenberger*, Primitivity, freeness, norm and trace, Discrete Mathematics **214** (2000), 135-144.

[Da] *H. Davenport*, Bases for finite fields. J. London Math. Soc. **43** (1968), 21-49.

[Fa] *C. C. Faith*, Extensions of normal bases and completely basic fields, Trans. Am. Math. Soc. **85** (1957), 406-427.

[Ha1] *D. Hachenberger*, "Finite Fields: Normal Bases and Completely Free Elements", Kluwer Academic Publishers, Boston, 1997.

[Ha2] *D. Hachenberger*, Primitive normal bases for towers of field extensions, Finite Fields and their Applications **5** (1999), 378-385.

[Ha3] *D. Hachenberger*, Primitive complete normal bases for regular extensions, Glasgow Journal Math., to appear.

[He] *K. Hensel*, Über die Darstellungen der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor, J. reine angew. Math. **103** (1888), 230-237.

[Ju] *D. Jungnickel*, "Finite Fields. Structure and Arithmetic", Bibliographisches Institut, Mannheim, 1993.

[Le] *H.W. Lenstra, Jr.*, A normal basis theorem for infinite Galois extensions, Nederl. Akad. Wetensch. Indag. Math **47** (1985), no. 2, 221-228.

[LeSc] *H. W. Lenstra, Jr.* and *R. J. Schoof*, Primitive normal bases for finite fields, Math. Comp. **48** (1987), 217-231.

[LiNi] *R. Lidl* and *H. Niederreiter*, "Finite Fields", Addison-Wesley, Reading, Massachusetts, 1983.

[Lü] *H. Lüneburg*, On the early history of Galois fields, in: D. Jungnickel and H. Niederreiter (eds.), Proceedings of the Fifth International Conference on Finite Fields and Applications, Augsburg, August 1999, this volume.

[Sche] *A. Scheerhorn*, Trace- and norm-compatible extensions of finite fields, AAECC **3** (1992), 199-209.