Generators for primary closures of Galois fields

Dirk Hachenberger

Institut für Mathematik der Universität Augsburg, Universitatsstr. 14, D-86135 Augsburg, Germany

Received 26 March 2002; accepted 23 September 2002

Abstract

We continue to study the existence of (norm- and) trace-compatible sequences of primitive normal bases for prime power extensions of finite fields, introduced by the author in Hachenberger (Finite Fields Appl. 5 (1999) 378–385; in: D. Jungnickel, H. Niederreiter (Eds.), Proceedings of the Fifth International Conference on Finite Fields and Applications, Augsburg, August 1999, Springer, Heidelberg, 2001, pp. 208–223), and improve on some aspects of these papers.

Keywords: Finite (Galois) field; Primitive element; Normal (free) element; Normal basis; Completely normal (completely free) element; Trace; Norm; Trace-compatible sequence; Norm-compatible sequence; Universal quadruple

1. Introduction

In [Ha2] we have introduced $\mathcal{T}$ as the set of all triples (q,k,e) (where $q>1$ is a prime power and $k,e\in\mathbb{N}^*$) such that the following condition holds for the corresponding tower $(\mathbb{F}_q,\mathbb{F}_{q^k},\mathbb{F}_{q^{kc}})$ of Galois fields: *for every* $a\in\mathbb{F}_{q^k}$ *which is normal (or free) over* $\mathbb{F}_q$ *there exists a primitive element* $w_a\in\mathbb{F}_{q^{kc}}$ *which is normal over* $\mathbb{F}_q$ *and whose* $(\mathbb{F}_{q^{kc}},\mathbb{F}_{q^k})$*-trace is equal to* a.

In [Ha3] a quadruple (q,k,l,n) (where $k,l,n\in\mathbb{N}^*$ with k and l dividing n) is called *universal*, provided the following condition holds for the quadruple $(\mathbb{F}_q,\mathbb{F}_{q^k},\mathbb{F}_{q^l},\mathbb{F}_{q^n})$ of Galois fields: *given any* $a\in\mathbb{F}_{q^k}$ *which is normal over* $\mathbb{F}_q$ *and any* $b\in\mathbb{F}_{q^l}$ *which is primitive, there exists a primitive element* $w_{a,b}\in\mathbb{F}_{q^n}$, *which is normal over* $\mathbb{F}_q$, *whose*

$(\mathbb{F}_{q^n}, \mathbb{F}_{q^k})$-*trace is equal to a and whose* $(\mathbb{F}_{q^n}, \mathbb{F}_{q^l})$-*norm is equal to b*. Let $\mathcal{Q}$ be the set of all universal quadruples.

By means of character theory and Gaussian sums, we have provided sufficient criteria for membership in $\mathcal{T}$ and $\mathcal{Q}$. For the case where k, l, e, n are powers of a prime r, the following assertions hold without any restriction on q (here, p is the characteristic of $\mathbb{F}_q$).

1. Theorem 5.1 in [Ha2]: $(q, r^a, r^b) \in \mathcal{T}$ for all $a \geqslant 0$ and all $b \geqslant 1$ provided $r \geqslant 5$ or $r = p$; $(q, 3^a, 3^b) \in \mathcal{T}$ for all $a \geqslant 0$ and all $b \geqslant 2$; $(q, 8 \cdot 2^a, 2^b) \in \mathcal{T}$ for all $a \geqslant 0$ and all $b \geqslant 2$.
2. Theorem 2.3′ in [Ha3]: $(q, r^a, r^b, r^c) \in \mathcal{Q}$ for all $a, b \geqslant 0$ and all $c > \max(a, b)$ provided $r \geqslant 7$.

In the present paper, we are going to prove the following results.

Theorem 1.1. *Let r be an odd prime which is distinct from the characteristic of the Galois field* $F = \mathbb{F}_q$. *Let s* (*a divisor of* $r - 1$) *be the order of q* modulo *r and assume that the order of q* modulo r^2 *is equal to sr. Then* $(q, r^a, r^b) \in \mathcal{T}$ *for all* $a \geqslant 0$ *and all* $b \geqslant 1$.

Theorem 1.2. *Let* $r \geqslant 5$ *be a prime. If r is distinct from the characteristic p of the Galois field* $F = \mathbb{F}_q$, *let s be the order of q* modulo *r and assume that the order of q* modulo r^2 *is equal to sr. Then* (q, r^a, r^b, r^c) *is a universal quadruple for all* $a, b \geqslant 0$ *and all* $c > \max(a, b)$.

When $r = 3$, the assertion of Theorem 1.1 is satisfied (and therefore yields an improvement over [Ha2, Theorem 5.1]) for all q such that $q \bmod 9 \in \{2, 4, 5, 7\}$ (which holds for 22 prime powers $q \leqslant 100$: 2, 4, 5, 7, 11, 13, 16, 23, 25, 29, 31, 32, 41, 43, 47, 49, 59, 61, 67, 79, 83, 97). It remains open for which q with $q \bmod 9 \in \{1, 8\}$ the triples $(q, 3^{n-1}, 3)$ are members of $\mathcal{T}$ where $n \geqslant 2$ (see [Ha2, Proposition 1.1] and observe that $(q, 1, e) \in \mathcal{T}$ for all q and all e by the Theorem on Primitive Normal Basis with Prescribed Trace of Cohen and Hachenberger [CoHa1]). More details on the latter problem are given in Section 4.

We remark that Theorem 1.1 generalizes Hachenberger [Ha4, Theorem 4.1], where the study of preimages of generalized trace-mappings lead to the conclusion of the above theorem under the additional assumption that $s = r - 1$ (whence q is a primitive root modulo r^l for all l). An application of Theorem 1.1 in combination with [Ha2, Theorem 5.1] yields $(2^t, r^a, r^b) \in \mathcal{T}$ for all primes r, all $a \in \mathbb{N}$ and all $b \in \mathbb{N}^*$, whenever t is not divisible by 3. Consequently, if $q = 2^t$ with $\gcd(t, 3) = 1$, then the following holds for any prime r: *there exists a sequence* $(y_l)_{l \in \mathbb{N}}$ *in the r-primary closure* $\mathbb{F}_{q^{r^\infty}}$ *over* $\mathbb{F}_q$ *such that* y_l *is primitive and normal in* $\mathbb{F}_{q^{r^l}}/\mathbb{F}_q$ *for all l, and such that the* $(\mathbb{F}_{q^{r^{l_2}}}, \mathbb{F}_{q^{r^{l_1}}})$-*trace of* y_{l_2} *is equal to* y_{l_1} *whenever* $l_1 \leqslant l_2$. The latter is an improvement of [Ha4, Theorem 5.1].

Unfortunately, an essential argument used in the proof of Theorem 1.1 does not apply to arbitrary extensions with degree a power of 2. However, as a consequence of [Ha4, Theorem 4.1] we note the following result (which is also incorporated in Section 2 of the present paper).

Theorem 1.3. $(q,2,2)\in\mathscr{T}$ *for all* $q\equiv 3 \bmod 4$.

Concerning universal quadruples, Theorem 1.2 extends [Ha3, Theorem 2.3′] when $r=5$ is the characteristic of $\mathbb{F}_q$, or when the order of q modulo 25 is divisible by 5. The latter holds when $q \bmod 25\in\{2,3,4,6,8,9,11,12,13,14,16,17,19,21,22,23\}$. According to [Ha3, Proposition 2.4] it remains open whether $(q,5^l,5^l,5^{l+1})$ is a universal quadruple for all $l\geqslant 1$ and all q satisfying $q \bmod 25\in\{1,7,18,24\}$ (observe that $(q,1,1,5)\in\mathscr{Q}$ by work of Cohen [Co2], which extends work of Hachenberger and Cohen [CoHa2]).

The proofs of Theorems 1.1 and 1.2 are given in Section 2. In Section 3 we discuss the consequences of Theorem 1.2 concerning *complete* universal quadruples.

2. Proofs of Theorems 1.1 and 1.2

The proofs rely on fundamental facts concerning the additive module structure of extensions of Galois fields, the details of which may be found in [Ha1]. We start with a characterization of normal elements by means of traces.

Theorem 2.1. *Let r be a prime and $l\in\mathbb{N}^*$. Assume that r is equal to the characteristic p of $\mathbb{F}_q$ or that $\mathrm{ord}_{r^2}(q)$ is divisible by r. Assume additionally that $l=2$ if $r=2\neq p$. Finally, let $E=\mathbb{F}_{q^{r^l}}$ and $K=\mathbb{F}_{q^{r^{l-1}}}$. Then the following two assertions are equivalent:*

1. *$w\in E$ is normal over $\mathbb{F}_q$;*
2. *$w\in E$ is normal over K and the (E,K)-trace of w is normal in $K/\mathbb{F}_q$.*

Proof. If r is the characteristic of F, then w is normal in E/F if and only if the (E,F)-trace of w is nonzero; moreover, any normal element of E/F is already completely normal (completely free) in E/F (see [Ha1, Theorem 5.7]). From that the assertion of the theorem easily follows.

Assume therefore that r is different from the characteristic of F. Let first r be odd and s the order of $q \bmod r$, and assume that the order of $q \bmod r^2$ is sr (which is equivalent to the fact that q^s-1 is not divisible by r). By elementary number theory (see e.g. [Ha1, Section 19]) the order of $q \bmod r^l$ is then equal to sr^{l-1} for every $l\in\mathbb{N}^*$. For a given $l\in\mathbb{N}^*$ let K and E be as in the assertion.

Consider the rth cyclotomic polynomial Φ_r. Over F it splits into $t:=(r-1)/s$ monic irreducible factors (of degree s, each), say $f_1,\ldots,f_t$. As s and r are relatively prime, the f_i remain irreducible when considered as polynomials over K. According

to the decomposition (over K) of

$$x^r - 1 = (x-1)\,\Phi_r = (x-1)\prod_{i=1}^{t} f_i,$$

any $w \in E$ can be written as

$$w = w_0 + w' = w_0 + \sum_{i=1}^{t} w_i,$$

such that $w_0 \in K$ and the $q^{r^{l-1}}$-order of any w_i divides f_i (see [Ha1, Section 8]). When considered over the field F, the q-order of w_0 divides $x^{r^{l-1}} - 1$ while the q-order of any w_i divides $f_i(x^{r^{l-1}})$. The latter corresponds to the decomposition (over F) of

$$x^{r^l} - 1 = (x^{r^{l-1}} - 1)\Phi_{r^l} = (x^{r^{l-1}} - 1)\prod_{i=1}^{t} f_i(x^{r^{l-1}}).$$

As $\mathrm{ord}_{r^l}(q) = sr^{l-1}$, the t polynomials $f_1(x^{r^{l-1}}), \ldots, f_t(x^{r^{l-1}})$ are irreducible over F and therefore give the (complete) decomposition of the r^lth cyclotomic polynomial Φ_{r^l}, which is equal to $\Phi_r(x^{r^{l-1}})$.

Now, $w_i \neq 0$ if and only if its q-order is $f_i(x^{r^{l-1}})$, and this holds if and only if its $q^{r^{l-1}}$-order is f_i. Moreover, w is normal in E/F if and only if w_0 is normal in K/F and $w_i \neq 0$ for all i. The normality of w_0 is equivalent to the normality of the (E,K)-trace of w over F (which is equal to the (E,K)-trace of w_0). As the (E,K)-trace of a normal element is always normal in K/F, the equivalence of the theorem holds.

If $r = 2 = l$, then $q \equiv 3 \bmod 4$, whence the fourth cyclotomic polynomial Φ_4 is irreducible over F. Now the assertion follows by a similar reasoning, as, under the assumption that $q \equiv 3 \bmod 4$, an element u has q-order Φ_4 if and only if it has q^2-order Φ_2. □

We remark that the proof of Theorem 2.1 is similar to that of Theorem 8 of Pincin [Pi], where *multiplicative* decompositions of normal basis generators are studied.

Proof of Theorem 1.1. Let r, s and q be as in the assertion of Theorem 1.1. For a given $l \in \mathbb{N}^*$, we let $E = \mathbb{F}_{q^{r^l}}$ and $K = \mathbb{F}_{q^{r^{l-1}}}$. Considering the extension E/K, the theorem of Cohen and Hachenberger on Primitive Normal Bases with Prescribed Trace [CoHa1] asserts that for any nonzero $a \in K$ there exists a primitive $w \in E$ which is normal over K and has (E,K)-trace equal to a (i.e., $(q^{r^{l-1}}, 1, r) \in \mathscr{T}$). Now, assume that a is chosen to be normal in K/F (where $F = \mathbb{F}_q$). Letting w as above, Theorem 2.1 implies that w is normal in E/F.

Altogether, this means $(q, r^{l-1}, r) \in \mathscr{T}$ for all $l \in \mathbb{N}^*$. The assertion of Theorem 1.1 follows now from [Ha1, Proposition 1.1], which states that $(q, \frac{k}{d}, ed) \in \mathscr{T}$ for every divisor d of k provided that $(q,k,e) \in \mathscr{T}$. □

We remark that the case $s = r - 1$ for odd r (as well as $r = 2 = l$, see [Ha4, Section 4]) gives rise to the irreducibility of the r^lth cyclotomic polynomial. In that situation it would suffice to require w to be primitive, which is guaranteed by Cohen's Theorem on Primitive Elements with Prescribed Trace [Co1].

Proof of Theorem 1.2. Let r, s and q be as in the assertion of Theorem 1.2. For a given $l \in \mathbb{N}^*$, we consider again the fields $E = \mathbb{F}_{q^{r^l}}$ and $K = \mathbb{F}_{q^{r^{l-1}}}$. By Cohen and Hachenberger [CoHa2] (for $r \geqslant 7$, essentially) and by Cohen [Co2] (for $r \geqslant 5$) the following is true for the field extension E/K: for any nonzero $a \in K$ and any primitive $b \in K$ there is a primitive w in E which is normal over K and has (E,K)-trace equal to a and (E,K)-norm equal to b (i.e., $(q^{r^{l-1}}, 1, 1, r) \in \mathcal{Q}$). If a in particular is chosen to be normal in K/F (where again $F = \mathbb{F}_q$), then w is normal in E/F, and this implies the universality of $(q, r^{l-1}, r^{l-1}, r^l)$ (for all $l \in \mathbb{N}^*$). The assertion of Theorem 1.2 follows now from [Ha3, Proposition 2.4], which states that $(q,k,l,n) \in \mathcal{Q}$ implies $(q,k',l',n) \in \mathcal{Q}$ for every divisor k' of k and every divisor l' of l. □

3. On complete universal quadruples

In [Ha3] a quadruple (q,k,l,n) (where $k,l,n \in \mathbb{N}^*$ with k and l dividing n) is called *completely universal* provided the following condition holds for the quadruple $(\mathbb{F}_q, \mathbb{F}_{q^k}, \mathbb{F}_{q^l}, \mathbb{F}_{q^n})$ of Galois fields: *given any* $a \in \mathbb{F}_{q^k}$ *which is completely normal (completely free) over* $\mathbb{F}_q$ *and any* $b \in \mathbb{F}_{q^l}$ *which is primitive, there exists a primitive element* $w_{a,b} \in \mathbb{F}_{q^n}$, *which is completely normal over* $\mathbb{F}_q$, *whose* $(\mathbb{F}_{q^n}, \mathbb{F}_{q^k})$*-trace is equal to* a *and whose* $(\mathbb{F}_{q^n}, \mathbb{F}_{q^l})$*-norm is equal to* b. Let $\mathcal{Q}^c$ be the set of all complete universal quadruples.

By Hachenberger [Ha3, Theorem 6.2′] we know that $(q, r^a, r^b, r^c) \in \mathcal{Q}^c$ for all $a,b \geqslant 0$ and all $c > \max(a,b)$ provided $r \geqslant 7$ (without any restriction on q). Combining the present Theorem 1.2 with [Ha3, Proposition 6.3] thus yields the following extension of [Ha3, Theorem 6.2′].

Theorem 3.1. *Let* $r \geqslant 5$ *be a prime. If* r *is distinct from the characteristic* p *of the Galois field* $F = \mathbb{F}_q$, *let* s *be the order of* q modulo r *and assume that the order of* q modulo r^2 *is equal to* sr. *Then* (q, r^a, r^b, r^c) *is a complete universal quadruple for all* $a,b \geqslant 0$ *and all* $c > \max(a,b)$.

We shall mention that the statement of [Ha3, Proposition 6.3] is as follows: Under the assumption that r is an odd prime which does not divide q, the quadruple (q, r^l, r^l, r^{l+1}) is completely universal provided that $(q^{r^\tau}, r^{l-\tau}, r^{l-\tau}, r^{l-1-\tau})$ is universal, where $\tau := \lfloor \beta/2 \rfloor$ and β is defined by $\mathrm{ord}_{r^{l+1}}(q) = \mathrm{ord}_r(q) \cdot r^\beta$. Furthermore, as mentioned in [Ha3, Section 6], $(q, r^l, r^l, r^{l+1}) \in \mathcal{Q}^c$ implies $(q, r^a, r^b, r^{l+1}) \in \mathcal{Q}^c$ for all $a,b \leqslant l$.

For the case where r equals the characteristic of $\mathbb{F}_q$, recall that any normal element of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$ is completely normal (see [Ha1, Theorem 5.7]).

4. Concluding remarks

In the present section we shall summarize some computational results. All computations have been performed with the computer algebra system *Maple* (in version 7.00).

The first two remarks concern triples $(q, 3^{n-1}, 3)$ for $q \bmod 9 \in \{1, 8\}$, which are not covered by Theorem 1.1. Remarks 3 and 4 concern triples $(q, k, 4)$ with $k \in \{2, 4\}$, which are not covered by [Ha2, Theorem 5.1].

Remark 1. Assume that $q \equiv 1 \bmod 9$. If $n \geqslant 5$, then an application of [Ha2, Proposition 4.3] (with $l = 300$) yields $(q, 3^{n-1}, 3) \in \mathscr{T}$ whenever $q \geqslant 65\,193$. Let $L := \{q \leqslant 65\,193 : q \equiv 1 \bmod 9\}$. Using the approach outlined in [Ha2, Section 5], one can show that $(q, 3^5, 3) \in \mathscr{T}$ for all $q \in L$ with four possible exceptions: $q \in \{1459, 2917, 17\,497, 21\,871\}$. Furthermore, $(q, 3^6, 3) \in \mathscr{T}$ for all $q \in L$ with two possible exceptions: $q \in \{17\,497, 21\,871\}$. Moreover, $(q, 3^a, 3) \in \mathscr{T}$ for all $q \in L$ and all $a \geqslant 7$. Consequently, for $q \equiv 1 \bmod 9$ it essentially remains open, whether $(q, 3^m, 3) \in \mathscr{T}$ for $m \in \{1, 2, 3, 4\}$.

Remark 2. Assume that $q \equiv -1 \bmod 9$. If $n \geqslant 4$, then an application of [Ha2, (4.5)] (with $d = 2$ and $l = 300$) gives $(q, 3^{n-1}, 3) \in \mathscr{T}$ whenever $q \geqslant 2130$. The approach of [Ha3, Section 5] yields $(q, 3^{n-1}, 3) \in \mathscr{T}$ for all $q \equiv -1 \bmod 9$ and all $n \geqslant 4$. So, for $q \equiv -1 \bmod 9$ it remains open, whether $(q, 3^m, 3) \in \mathscr{T}$ for $m \in \{1, 2\}$. If $m = 2$ and $q \geqslant 346\,794$, then $(q, 9, 3) \in \mathscr{T}$ by [Ha2, (4.5)] (with $d = 2$ and $l = 300$).

Remark 3. An application of [Ha2, Proposition 4.3] (with $l = 149$) shows $(q, 4, 4) \in \mathscr{T}$ for all $q \geqslant 3104$. If $q \leqslant 3104$, [Ha2, Proposition 3.1] yields $(q, 4, 4) \in \mathscr{T}$ with possibly five exceptions $q \in \{3, 5, 7, 9, 17\} =: L$. If $q \in L$ and $q \neq 3$, then $(q, 2, 8) \in \mathscr{T}$; hence $(q, 2, 8) \in \mathscr{T}$ for all q with only one possible exception, namely $q = 3$.

Remark 4. An application of [Ha2, Proposition 4.3] (with $l = 100$) shows $(q, 2, 4) \in \mathscr{T}$ for all $q \geqslant 70\,542$. If $q \leqslant 70\,542$, [Ha2, Proposition 3.1] yields $(q, 2, 4) \in \mathscr{T}$ with possibly 21 exceptions $q \in \{3, 5, 7, 9, 11, 13, 17, 19, 25, 27, 29, 31, 37, 41, 43, 49, 73, 83, 89, 137, 233\}$.

References

[Co1] S.D. Cohen, Primitive elements and polynomials with arbitrary trace, Discrete Math. 83 (1990) 1–7.

[Co2] S.D. Cohen, Gauss sums and a sieve for generators of Galois fields, Publ. Math. Debrecen 56 (2000) 293–312.

[CoHa1] S.D. Cohen, D. Hachenberger, Primitive normal bases with prescribed trace, Appl. Algebra Eng. Comm. Comput. 9 (1999) 383–403.

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

[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 Appl. 5 (1999) 378–385.

[Ha3] D. Hachenberger, Universal generators for primary closures of Galois fields, in: D. Jungnickel, H. Niederreiter (Eds.), Proceedings of the Fifth International Conference on Finite Fields and Applications, Augsburg, August 1999, Springer, Heidelberg, 2001, pp. 208–223.

[Ha4] D. Hachenberger, Characterizing normal bases via the trace map, Comm. Algebra (2003), to appear.

[Pi] A. Pincin, Bases for finite fields and a canonical decomposition for a normal basis generator, Comm. Algebra 17 (1989) 1337–1352.