Designs, Codes and Cryptogrphy 2 (1992), 315-323.

Optimal normal bases

Shuhong Gao and Hendrik W. Lenstra, Jr.

Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario
Canada N2L 3G1
E-mail: sgao@violet.waterloo.edu

Department of Mathematics
University of California
Berkeley, CA 94720
U. S. A.
E-mail: hwl@math.berkeley.edu

Abstract. Let $K \subset L$ be a finite Galois extension of fields, of degree n. Let G be the Galois group, and let $(\sigma\alpha)_{\sigma\in G}$ be a normal basis for L over K. An argument due to Mullin, Onyszchuk, Vanstone and Wilson (Discrete Appl. Math. **22** (1988/89), 149–161) shows that the matrix that describes the map $x \mapsto \alpha x$ on this basis has at least $2n-1$ non-zero entries. If it contains exactly $2n-1$ non-zero entries, then the normal basis is said to be optimal. In the present paper we determine all optimal normal bases. In the case that K is finite our result confirms a conjecture that was made by Mullin et al. on the basis of a computer search.

Key words: normal basis, Galois theory.

1991 Mathematics subject classification: 12F10.

Acknowledgements. The first author acknowledges his Ph. D. supervisor Ronald C. Mullin for his help and continuous encouragement; he received partial financial assistance from NSERC grant #OGP0003071. The second author is grateful to the Institute for Advanced Study in Princeton, the Institute for Computer Research at the University of Waterloo, and the Université de Franche-Comté in Besançon for providing hospitality and support while this work was being done; he was supported by NSF under Grant No. DMS 90-02939.

Let $K \subset L$ be a finite Galois extension of fields, n the degree of the extension, and G the Galois group. A basis of L over K is called a *normal basis* if it is of the form $(\sigma\alpha)_{\sigma\in G}$, with $\alpha \in L$. Let $(\sigma\alpha)_{\sigma\in G}$ be a normal basis for L over K, and let $d(\tau,\sigma) \in K$, for σ, $\tau \in G$, be such that

$$\alpha \cdot \sigma\alpha = \sum_{\tau\in G} d(\tau,\sigma)\tau\alpha \tag{1}$$

for each $\sigma \in G$. Summing this over σ we find that

$$\sum_{\sigma} d(1,\sigma) = \operatorname{Tr}\alpha,$$
$$\sum_{\sigma} d(\tau,\sigma) = 0 \qquad \text{for } \tau \in G,\ \tau \neq 1,$$

where $\operatorname{Tr}\alpha = \sum_\sigma \sigma\alpha \in K$ denotes the trace of α. Since α is a unit, the matrix $\big(d(\tau,\sigma)\big)$ is invertible, so for each τ there is at least one non-zero $d(\tau,\sigma)$. If $\tau \neq 1$, then by the above relations there are at least *two* non-zero $d(\tau,\sigma)$'s. Thus we find that

$$\#\{(\sigma,\tau) \in G \times G : d(\tau,\sigma) \neq 0\} \geq 2n-1.$$

The normal basis $(\sigma\alpha)_{\sigma\in G}$ is called *optimal* if we have equality here.

The argument just given and the notion of an optimal normal basis are due to Mullin, Onyszchuk, Vanstone and Wilson [2]. They give several examples of optimal normal bases, and they formulate a conjecture that describes all finite extensions of the field of two elements that admit an optimal normal basis. In [1] this conjecture is extended to all finite fields. In the present paper we confirm the conjecture, and we show that the constructions given in [2] exhaust all optimal normal bases, even for Galois extensions of general fields.

Our result is as follows. If F is a field, we denote by F^* the multiplicative group of non-zero elements of F, and by $\operatorname{char} F$ the characteristic of F.

Theorem. *Let $K \subset L$ be a finite Galois extension of fields, with Galois group G, and let $\alpha \in L$. Then $(\sigma\alpha)_{\sigma\in G}$ is an optimal normal basis for L over K if and only if there is a prime number p, a primitive pth root of unity ζ in some algebraic extension of L, and an element $c \in K^*$ such that one of* (i), (ii) *is true:*

(i) *the irreducible polynomial of ζ over K has degree $p-1$, and we have $L = K(\zeta)$ and $\alpha = c\zeta$;*

(ii) $\operatorname{char} K = 2$, *the irreducible polynomial of $\zeta + \zeta^{-1}$ over K has degree $(p-1)/2$, and we have $L = K(\zeta + \zeta^{-1})$ and $\alpha = c(\zeta + \zeta^{-1})$.*

In case (i), the degree of L over K is $p-1$, and G is isomorphic to $\mathbf{F}_p^*$, where $\mathbf{F}_p$ denotes the field of p elements. In case (ii), the prime number p is odd (because $\operatorname{char} K = 2$), the degree of L over K is $(p-1)/2$, and G is isomorphic to $\mathbf{F}_p^*/\{\pm 1\}$. In particular, we see from the theorem that the Galois group is cyclic if there is an optimal normal basis.

In case (i) the irreducible polynomial of ζ over K is clearly equal to $\sum_{i=0}^{p-1} X^i$. We remark that, when K is a field and p is a prime number, we can give a necessary and sufficient condition for the polynomial $\sum_{i=0}^{p-1} X^i$ to be irreducible over K. Namely, it is irreducible over the prime field K_0 of K if and only if either $\operatorname{char} K = 0$, or $\operatorname{char} K \neq 0$ and $\operatorname{char} K$ is a primitive root modulo p, or $\operatorname{char} K = p = 2$; and it is irreducible over K if and only if it is irreducible over K_0 and $K_0(\zeta) \cap K = K_0$, where ζ denotes a zero of the polynomial in an extension field of K.

The formula for the irreducible polynomial of $\zeta + \zeta^{-1}$ over K in case (ii) is a little more complicated. Let $a \prec b$, for non-negative integers a and b, mean that each digit of a in the binary system is less than or equal to the corresponding digit of b; so we have $a \prec b$ if and only if one can subtract a from b in binary without "borrowing". Further, write $n = (p-1)/2$. With this notation, the irreducible polynomial of $\zeta + \zeta^{-1}$ over K in case (ii) equals $\sum_i X^i$, where i ranges over those non-negative integers for which we have $2i \prec n+i$. To prove this, one first observes that, for any primitive pth root of unity ζ in any field, one has the polynomial identity

$$\prod_{j=1}^{n}(X - \zeta^j - \zeta^{-j}) = \sum_{j=0}^{[(n-1)/2]} (-1)^j \binom{n-1-j}{j} X^{n-(2j+1)} + \sum_{j=0}^{[n/2]} (-1)^j \binom{n-j}{j} X^{n-2j}.$$

Next one uses Lucas's theorem, which asserts that $a \prec b$ if and only if the binomial coefficient $\binom{b}{a}$ is odd. This leads to the formula stated above. Again, we can for any field K of characteristic 2 and for any odd prime number $p = 2n+1$ give a necessary and sufficient condition for the polynomial to be irreducible over K. Namely, the polynomial is irreducible over the prime field $\mathbf{F}_2$ of K if and only if the group $\mathbf{F}_p^*/\{\pm 1\}$ is generated by the image of $(2 \bmod p)$; and it is irreducible over K if and only if it is irreducible over $\mathbf{F}_2$ and $\mathbf{F}_2(\gamma) \cap K = \mathbf{F}_2$, where γ denotes a zero of the polynomial in an extension field of K.

We turn to the proof of the theorem. First we prove the "if" part. Let p be a prime number and ζ a primitive pth root of unity such that (i) or (ii) holds for some $c \in K^*$. Clearly, α gives rise to an optimal normal basis for L over K if and only if $c\alpha$ does. Hence without loss of generality we may assume that $c = 1$.

Let it now first be supposed that we are in case (i). Since ζ has degree $p-1$ over K, all primitive pth roots of unity ζ^i, $1 \le i \le p-1$, must be conjugate to ζ. Also, the elements ζ^i, $0 \le i \le p-2$, form a basis for L over K. Multiplying this basis by ζ, we see that the elements ζ^i, $1 \le i \le p-1$, form a basis for L over K as well, so this is a normal basis. Multiplication by ζ on this basis is given by

$$\zeta \cdot \zeta^i = \zeta^{i+1} \qquad (i \neq p-1),$$
$$\zeta \cdot \zeta^{p-1} = 1 = \sum_{i=1}^{p-1} -\zeta^i.$$

It follows that the normal basis is optimal.

Next suppose that we are in case (ii), so that $\operatorname{char} K = 2$ and $\alpha = \zeta + \zeta^{-1}$. If γ is conjugate to α over K, then a zero η of $X^2 - \gamma X + 1$ is conjugate to one of the zeroes ζ, ζ^{-1} of $X^2 - \alpha X + 1$ and is therefore a primitive pth root of unity. Then we have $\eta = \zeta^i$ for some integer i that is not divisible by p, so $\gamma = \eta + \eta^{-1} = \zeta^i + \zeta^{-i}$ for some integer i with $1 \le i \le (p-1)/2$. Since α has degree $(p-1)/2$, it follows that its conjugates over K are precisely the elements $\alpha_i = \zeta^i + \zeta^{-i}$ for $1 \le i \le (p-1)/2$. Note that for $0 < j < (p-1)/2$ we have $\alpha^j = (\zeta + \zeta^{-1})^j = \sum_{i=0}^{[(j-1)/2]} \binom{j}{i} \alpha_{j-2i}$, and that $\alpha^0 = 1 = \sum_{i=1}^{p-1} \zeta^i = \sum_{i=1}^{(p-1)/2} \alpha_i$. This shows that the K-vector space spanned by α^j, $0 \le j < (p-1)/2$, which is L, is contained in the K-vector space spanned by α_i, $1 \le i \le (p-1)/2$. By dimension considerations it follows that the elements α_i, $1 \le i \le (p-1)/2$, form a normal basis for L over K. Multiplication by α on this basis is given by

$$\begin{aligned} \alpha \cdot \alpha_i &= \alpha_{i-1} + \alpha_{i+1} \qquad (1 < i < (p-1)/2), \\ \alpha \cdot \alpha_1 &= \alpha^2 = \alpha_2, \\ \alpha \cdot \alpha_{(p-1)/2} &= \alpha_{(p-3)/2} + \alpha_{(p-1)/2}. \end{aligned}$$

It follows that the normal basis is optimal. This completes the proof of the "if" part of the theorem.

We begin the proof of the "only if" part with a few general remarks about normal bases. Let $K \subset L$ be a finite Galois extension of fields, with Galois group G, and let $\alpha \in L$ be such that $(\sigma\alpha)_{\sigma \in G}$ is a normal basis for L over K. Let $d(\tau, \sigma) \in K$, for σ, $\tau \in G$, be such that (1) holds for each $\sigma \in G$. Applying σ^{-1} to (1) we find that

(2) $$d(\tau, \sigma) = d(\sigma^{-1}\tau, \sigma^{-1}) \qquad \text{for all } \sigma,\ \tau \in G.$$

We now express multiplication by α in the dual basis. Let β be the unique element of L satisfying $\operatorname{Tr}(\beta \cdot \alpha) = 1$ and $\operatorname{Tr}(\beta \cdot \sigma\alpha) = 0$ for all $\sigma \in G$, $\sigma \ne 1$, where $\operatorname{Tr}\colon L \to K$ denotes the trace map. Then for σ, $\tau \in G$ we have $\operatorname{Tr}(\sigma\beta \cdot \tau\alpha) = 1$ or 0 according as $\sigma = \tau$ or $\sigma \ne \tau$. It follows that $(\sigma\beta)_{\sigma \in G}$ is also a normal basis for L over K; it is called the *dual basis* of $(\sigma\alpha)_{\sigma \in G}$. We claim that multiplication by α is expressed in this basis by

(3) $$\alpha \cdot \tau\beta = \sum_{\sigma \in G} d(\tau, \sigma) \sigma\beta \qquad \text{for all } \tau \in G.$$

To prove this, it suffices to observe that the coefficient of $\alpha\cdot\tau\beta$ at $\sigma\beta$ is given by

$$\mathrm{Tr}((\alpha\cdot\tau\beta)\cdot\sigma\alpha)=\mathrm{Tr}((\alpha\cdot\sigma\alpha)\cdot\tau\beta)=\mathrm{Tr}\Big(\sum_{\rho\in G}d(\rho,\sigma)\rho\alpha\cdot\tau\beta\Big)=d(\tau,\sigma).$$

Let it now be assumed that $(\sigma\alpha)_{\sigma\in G}$ is an optimal normal basis for L over K. As we saw at the beginning of this paper this means the following. First of all, for each $\tau\in G$, $\tau\neq 1$, there are exactly two elements $\sigma\in G$ for which $d(\tau,\sigma)$ is non-zero, and these two non-zero elements add up to zero. Secondly, there is exactly one element $\sigma\in G$ for which $d(1,\sigma)$ is non-zero, and denoting this element by μ we have $d(1,\mu)=\mathrm{Tr}\,\alpha$. By (3), we can express the first property by saying that

(4) for each $\tau\in G$, $\tau\neq 1$, the element $\alpha\cdot\tau\beta$ equals an element of K^* times the difference of two distinct conjugates of β.

Likewise, the second property is equivalent to $\alpha\cdot\beta=(\mathrm{Tr}\,\alpha)\mu\beta$, where $\mu\in G$. Replacing α by $c\alpha$ for $c=-1/\mathrm{Tr}\,\alpha$ we may, without loss of generality, assume that $\mathrm{Tr}\,\alpha=-1$. Then we have

$$\alpha\cdot\beta=-\mu\beta. \tag{5}$$

Also, from $(\mathrm{Tr}\,\alpha)(\mathrm{Tr}\,\beta)=\sum_{\sigma,\tau}\sigma\alpha\cdot\tau\beta=\sum_{\rho}\mathrm{Tr}(\alpha\cdot\rho\beta)=1$ we see that we have $\mathrm{Tr}\,\beta=-1$.

If $\mu=1$ then from (5) we see that $\alpha=-1$, so that $L=K$. Then we are in case (i) of the theorem, with $p=2$, if $\mathrm{char}\,K\neq 2$, and we are in case (ii) of the theorem, with $p=3$, if $\mathrm{char}\,K=2$. Let it henceforth be assumed that $\mu\neq 1$.

We first deal with the case that $\mu^2=1$. From (5) we see that $\alpha=-\mu\beta/\beta$, so $\mu\alpha=-\mu^2\beta/\mu\beta=-\beta/\mu\beta=1/\alpha$. Therefore we have

$$\alpha\cdot\mu\alpha=1=-\,\mathrm{Tr}\,\alpha=\sum_{\sigma\in G}-\sigma\alpha.$$

This shows that $d(\sigma,\mu)=-1$ for all $\sigma\in G$. By (3) and (4) this implies that for each $\sigma\neq 1$ there is a unique $\sigma^*\neq\mu$ such that

$$\alpha\cdot\sigma\beta=\sigma^*\beta-\mu\beta.$$

If $\sigma \neq \tau$ then $\alpha \cdot \sigma\beta \neq \alpha \cdot \tau\beta$, so $\sigma^* \neq \tau^*$. Therefore $\sigma \mapsto \sigma^*$ is a bijective map from $G - \{1\}$ to $G - \{\mu\}$. Hence each $\sigma^* \neq \mu$ occurs exactly once, and again using (3) we see that

$$\alpha \cdot \sigma^*\alpha = \sigma\alpha \quad \text{for } \sigma^* \neq \mu,$$
$$\alpha \cdot \mu\alpha = 1.$$

It follows that the set $\{1\} \cup \{\sigma\alpha : \sigma \in G\}$ is closed under multiplication by α. Since it is also closed under the action of G, we conclude that it is a multiplicative group of order $n+1$. This implies that $\alpha^{n+1} = 1$, and we also have $\alpha \neq 1$. Hence α is a zero of $X^n + \ldots + X + 1$. Since α has degree n over K, the polynomial $X^n + \ldots + X + 1$ is irreducible over K. Therefore $n+1$ is a prime number. This shows that we are in case (i) of the theorem.

For the rest of the proof we assume that $\mu^2 \neq 1$. By (5) we have $d(1, \sigma) = -1$ or 0 according as $\sigma = \mu$ or $\sigma \neq \mu$. Hence from (2) we find that

$$d(\sigma, \sigma) = \begin{cases} -1 & \text{if } \sigma = \mu^{-1}, \\ 0 & \text{if } \sigma \neq \mu^{-1}. \end{cases} \tag{6}$$

Therefore $\alpha \cdot \mu^{-1}\beta$ has a term $-\mu^{-1}\beta$, and from $\mu^{-1} \neq 1$ and (4) we see that there exists $\lambda \in G$ such that

$$\alpha \cdot \mu^{-1}\beta = \lambda\beta - \mu^{-1}\beta, \qquad \lambda \neq \mu^{-1}. \tag{7}$$

We shall prove that we have

$$\operatorname{char} K = 2, \tag{8}$$
$$\alpha \cdot \mu\beta = \lambda\mu\beta + \beta, \tag{9}$$
$$\lambda\mu = \mu\lambda. \tag{10}$$

Before we give the proof of these properties we show how they lead to a proof of the theorem.

Applying μ to (7) and comparing the result to (9) we find by (8) and (10) that $\mu\alpha \cdot \beta = \alpha \cdot \mu\beta$, which is the same as

$$\alpha/\beta = \mu(\alpha/\beta). \tag{11}$$

Multiplying (11) and (5) we find by (8) that $\alpha^2 = \mu\alpha$. By induction on k one deduces from this that $\mu^k\alpha = \alpha^{2^k}$ for every non-negative integer k. If we take for k the order of μ, then we find that $\alpha^{2^k} = \alpha$, which by the theory of finite fields means that α is algebraic of degree dividing k over the prime field $\mathbf{F}_2$ of K. Therefore we have $k = \operatorname{order}\mu \le \#G = [L : K] = [K(\alpha) : K] \le k$. We must have equality everywhere, so μ generates G. By (11), this implies that $\alpha/\beta \in K$, and since $\operatorname{Tr}\alpha = \operatorname{Tr}\beta = -1$ we have in fact $\alpha = \beta$. Thus from (1) and (3) we see that

$$(12) \qquad d(\sigma,\tau) = d(\tau,\sigma) \qquad \text{for all } \sigma,\, \tau \in G.$$

Let now ζ be a zero of $X^2 - \alpha X + 1$ in some algebraic extension of L, so that $\zeta + \zeta^{-1} = \alpha$. Since α is algebraic over $\mathbf{F}_2$, the same is true for ζ, so the multiplicative order of ζ is finite and odd; let it be $2m+1$. For each integer i, write $\gamma_i = \zeta^i + \zeta^{-i}$, so that $\gamma_0 = 0$ and $\gamma_1 = \alpha$. We have $\gamma_i = \gamma_j$ if and only if the zeroes ζ^i, ζ^{-i} of $X^2 - \gamma_i X + 1$ coincide with the zeroes ζ^j, ζ^{-j} of $X^2 - \gamma_j X + 1$, if and only if $i \equiv \pm j \bmod 2m+1$. Hence there are exactly m different non-zero elements among the γ_i, namely $\gamma_1, \gamma_2, \ldots, \gamma_m$. Each of the n conjugates of α is of the form $\mu^j\alpha = \alpha^{2^j} = \zeta^{2^j} + \zeta^{-2^j} = \gamma_{2^j}$ for some integer j, and therefore occurs among the γ_i. This implies that $n \le m$. We show that $n = m$ by proving that, conversely, every non-zero γ_i is a conjugate of α. This is done by induction on i. We have $\gamma_1 = \alpha$ and $\gamma_2 = \mu\alpha$, so it suffices to take $3 \le i \le m$. We have

$$\alpha \cdot \gamma_{i-2} = (\zeta + \zeta^{-1}) \cdot (\zeta^{i-2} + \zeta^{2-i}) = \gamma_{i-1} + \gamma_{i-3},$$

where by the induction hypothesis each of γ_{i-2}, γ_{i-1} is conjugate to α, and γ_{i-3} is either conjugate to α or equal to zero. Thus when $\alpha \cdot \gamma_{i-2}$ is expressed in the normal basis $(\sigma\alpha)_{\sigma\in G}$, then γ_{i-1} occurs with a coefficient 1. By (12), this implies that when $\alpha \cdot \gamma_{i-1}$ is expressed in the same basis, γ_{i-2} likewise occurs with a coefficient 1. Hence from (4) (with $\beta = \alpha$) and $\gamma_{i-1} \ne \alpha$ we see that $\alpha \cdot \gamma_{i-1}$ is equal to the sum of γ_{i-2} and some other conjugate of α. But since we have $\alpha \cdot \gamma_{i-1} = \gamma_{i-2} + \gamma_i$, that other conjugate of α must be γ_i. This completes the inductive proof that all non-zero γ_i are conjugate to α and that $n = m$.

From the fact that each non-zero γ_i equals a conjugate $\mu^j\alpha$ of α it follows that for each integer i that is not divisible by $2m+1$ there is an integer j such that $i \equiv \pm 2^j \bmod 2m+1$.

In particular, every integer i that is not divisible by $2m+1$ is relatively prime to $2m+1$, so $2m+1$ is a prime number. Thus with $p = 2m+1$ we see that all assertions of (ii) have been proved.

It remains to prove (8), (9), and (10). The hypotheses are that α gives rise to an optimal normal basis with $\operatorname{Tr}\alpha = -1$, that β gives rise to the corresponding dual basis, that μ and λ satisfy (5) and (7), and that $\mu^2 \neq 1$. The main technique of the proof is to use the obvious identity $\rho\alpha \cdot (\sigma\alpha \cdot \tau\beta) = \sigma\alpha \cdot (\rho\alpha \cdot \tau\beta)$ for several choices of ρ, σ, $\tau \in G$.

From (5) we see that

$$\mu\alpha \cdot (\alpha \cdot \beta) = \mu\alpha \cdot (-\mu\beta) = -\mu(\alpha \cdot \beta) = \mu^2\beta,$$

and from (7) we obtain

$$\alpha \cdot (\mu\alpha \cdot \beta) = \alpha \cdot \mu(\alpha \cdot \mu^{-1}\beta) = \alpha \cdot \mu(\lambda\beta - \mu^{-1}\beta) = \alpha \cdot \mu\lambda\beta - \alpha \cdot \beta = \alpha \cdot \mu\lambda\beta + \mu\beta.$$

Therefore we have

$$(13) \qquad \alpha \cdot \mu\lambda\beta = \mu^2\beta - \mu\beta.$$

From $\mu \neq \mu^{-1}$ and (6) we see that $d(\mu, \mu) = 0$, so (13) implies that

$$(14) \qquad \lambda \neq 1.$$

By (2) and (7) we have $d(\lambda^{-1}\mu^{-1}, \lambda^{-1}) = d(\mu^{-1}, \lambda) = 1$. Also, $\lambda^{-1}\mu^{-1} \neq 1$ by (7), so from (4) we obtain

$$(15) \qquad \alpha \cdot \lambda^{-1}\mu^{-1}\beta = \lambda^{-1}\beta - \kappa\beta \qquad \text{for some } \kappa \in G,\ \kappa \neq \lambda^{-1}.$$

We have $\lambda^{-1}\mu^{-1} \neq \mu^{-1}$ by (14), so (6) gives

$$(16) \qquad \kappa \neq \lambda^{-1}\mu^{-1}.$$

From (7) and (15) we obtain

$$\lambda\alpha \cdot (\alpha \cdot \mu^{-1}\beta) = \lambda\alpha \cdot (\lambda\beta - \mu^{-1}\beta) = \lambda(\alpha \cdot \beta - \alpha \cdot \lambda^{-1}\mu^{-1}\beta) = -\lambda\mu\beta - \beta + \lambda\kappa\beta,$$

and (15) gives

$$\alpha \cdot (\lambda\alpha \cdot \mu^{-1}\beta) = \alpha \cdot \lambda(\alpha \cdot \lambda^{-1}\mu^{-1}\beta) = \alpha \cdot (\beta - \lambda\kappa\beta) = -\mu\beta - \alpha \cdot \lambda\kappa\beta.$$

Therefore we have

$$\alpha \cdot \lambda\kappa\beta = -\mu\beta + \lambda\mu\beta + \beta - \lambda\kappa\beta. \tag{17}$$

By (16) we have $\lambda\kappa \neq \mu^{-1}$, so by (6) the term $-\lambda\kappa\beta$ does not appear in $\alpha \cdot \lambda\kappa\beta$. It must therefore be canceled by one of the other terms of (17). We have $\lambda\kappa \neq 1$ by (15), so it is not canceled by β. Therefore it is canceled either by $\lambda\mu\beta$ or by $-\mu\beta$. We shall derive a contradiction from the hypothesis that it is canceled by $\lambda\mu\beta$; this will prove that it is canceled by $-\mu\beta$.

Suppose therefore that $\lambda\kappa\beta = \lambda\mu\beta$. Then we have $\kappa = \mu$, so (17) gives

$$\alpha \cdot \lambda\mu\beta = \beta - \mu\beta. \tag{18}$$

By (2) and (18) we have $d(\mu^{-1}\lambda\mu, \mu^{-1}) = d(\lambda\mu, \mu) = -1$, and since by (14) we have $\mu^{-1}\lambda\mu \neq 1$ it follows that

$$\alpha \cdot \mu^{-1}\lambda\mu\beta = \nu\beta - \mu^{-1}\beta, \qquad \text{for some } \nu \in G,\ \nu \neq \mu^{-1}. \tag{19}$$

Now we have on the one hand

$$\alpha \cdot (\mu\alpha \cdot \lambda\mu\beta) = \alpha \cdot \mu(\alpha \cdot \mu^{-1}\lambda\mu\beta) = \alpha \cdot \mu(\nu\beta - \mu^{-1}\beta) = \alpha \cdot \mu\nu\beta + \mu\beta,$$

by (19), and on the other hand

$$\mu\alpha \cdot (\alpha \cdot \lambda\mu\beta) = \mu\alpha \cdot (\beta - \mu\beta) = \mu(\alpha \cdot \mu^{-1}\beta - \alpha \cdot \beta) = \mu\lambda\beta - \beta + \mu^2\beta,$$

by (18) and (7). This leads to

$$\alpha \cdot \mu\nu\beta = \mu\lambda\beta - \beta + \mu^2\beta - \mu\beta.$$

Since 1, μ, μ^2 are pairwise distinct, the term $\mu\lambda\beta$ must be canceled by one of the other three terms. Therefore $\mu\lambda \in \{1, \mu, \mu^2\}$, so λ belongs to the subgroup generated by μ, and therefore $\lambda\mu = \mu\lambda$. But then (13) and (18) give $\mu^2 = 1$, contradicting our hypothesis.

We conclude that the term $-\lambda\kappa\beta$ in (17) is canceled by $-\mu\beta$, that is, $-\mu\beta-\lambda\kappa\beta=0$. This implies that $\mu=\lambda\kappa$ and $2\mu\beta=0$. This proves (8), and (17) gives (9). From (15) we obtain

$$\alpha\cdot\lambda^{-1}\mu^{-1}\beta=\lambda^{-1}\beta+\lambda^{-1}\mu\beta. \tag{20}$$

Combining this with (2) we find that $d(\mu^{-2},\mu^{-1}\lambda)=d(\lambda^{-1}\mu^{-1},\lambda^{-1}\mu)=1$, and since $\mu^{-2}\neq 1$ this gives

$$\alpha\cdot\mu^{-2}\beta=\mu^{-1}\lambda\beta+\nu\beta\qquad\text{for some }\nu\in G.$$

This implies that

$$\lambda\alpha\cdot(\mu\alpha\cdot\mu^{-1}\beta)=\lambda\alpha\cdot\mu(\alpha\cdot\mu^{-2}\beta)=\lambda\alpha\cdot\mu(\mu^{-1}\lambda\beta+\nu\beta)=\lambda\mu\beta+\lambda\alpha\cdot\mu\nu\beta,$$

whereas (20) and (7) lead to

$$\begin{aligned}\mu\alpha\cdot(\lambda\alpha\cdot\mu^{-1}\beta)&=\mu\alpha\cdot\lambda(\alpha\cdot\lambda^{-1}\mu^{-1}\beta)=\mu\alpha\cdot\lambda(\lambda^{-1}\beta+\lambda^{-1}\mu\beta)\\&=\mu(\alpha\cdot\mu^{-1}\beta+\alpha\cdot\beta)=\mu(\lambda\beta+\mu^{-1}\beta+\mu\beta)=\mu\lambda\beta+\beta+\mu^2\beta.\end{aligned}$$

Therefore we have

$$\lambda\alpha\cdot\mu\nu\beta=\lambda\mu\beta+\mu\lambda\beta+\beta+\mu^2\beta.$$

This is conjugate to $\alpha\cdot\lambda^{-1}\mu\nu\beta$, so two terms on the right must cancel. From $1\notin\{\lambda\mu,\mu\lambda,\mu^2\}$ it follows that β does not cancel any of the other terms. Hence two of $\lambda\mu\beta$, $\mu\lambda\beta$, $\mu^2\beta$ must cancel, so that we have $\lambda\mu=\mu\lambda$, or $\mu\lambda=\mu^2$, or $\mu^2=\lambda\mu$. In each of the three cases λ and μ commute. This proves (10), which completes the proof of the theorem.

References

1. R. C. Mullin, *A characterization of the extremal distributions of optimal normal bases*, Proc. Marshall Hall Memorial Conference, Burlington, Vermont, 1990, to appear.
2. R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, R. M. Wilson, *Optimal normal bases in* GF(p^n), Discrete Appl. Math. **22** (1988/89), 149–161.