arXiv:1603.00426v1 [math.QA] 1 Mar 2016

FINITE NONCOMMUTATIVE GEOMETRIES RELATED TO $\mathbb{F}_p[x]$

M.E. BASSETT & S. MAJID

Abstract. It is known that irreducible noncommutative differential structures over $\mathbb{F}_p[x]$ are classified by irreducible monics m. We show that the cohomology $H^0(\mathbb{F}_p[x];m)=\mathbb{F}_p[g_d]$ if and only if $\mathrm{Trace}(m)\neq 0$, where $g_d=x^{p^d}-x$ and d is the degree of m. This implies that there are $\frac{p-1}{pd}\sum_{k|d,p\nmid k}\mu_M(k)p^{\frac{d}{k}}$ such 'regular' m (μ_M the Möbius function). Motivated by killing this zero'th cohomology, we study the directed system of finite-dimensional Hopf algebras $A_d=\mathbb{F}_p[x]/(g_d)$ as well as their inherited bicovariant differential calculi $\Omega(A_d;m)$. We show that $A_d=C_d\otimes_\chi A_1$ a cocycle extension where $C_d=A_d^\psi$ is the subalgebra of elements fixed under $\psi(x)=x+1$. We also have a Frobenius-fixed subalgebra B_d of dimension $\frac{1}{d}\sum_{k|d}\phi(k)p^{\frac{d}{k}}$ (ϕ the Euler totient function), generalising Boolean algebras when $p=2$. We note that $A_1\cong\mathbb{F}_p(\mathbb{Z}/p\mathbb{Z})$ the algebra of functions on the finite group $\mathbb{Z}/p\mathbb{Z}$ and we describe its differential calculus and Fourier theory. We show dually that $\mathbb{F}_p\mathbb{Z}/p\mathbb{Z}\cong\mathbb{F}_p[L]/(L^p)$ for a 'lie algebra' generator L with e^L group-like, using a truncated exponential. We show that A_2 over $\mathbb{F}_2$ is a 1-dimensional extension of the Boolean algebra on 3 elements and we study its noncommutative differentials, metrics and Levi-Civita connections within bimodule noncommutative geometry.

1. Introduction

This article is motivated by a fundamental issue in characteristic $p>0$ geometry visible even for polynomials $\mathbb{F}_p[x]$ in one variable over the finite field of order p, namely the failure of differential calculus to provide an effective tool. Specifically, on any connected manifold the only functions killed by the exterior derivative are the constant functions, i.e. the zeroth cohomology H^0 is spanned by 1. By contrast, the classical differential calculus on $\mathbb{F}_p[x]$ has a large kernel for d, namely all polynomials in x^p. One approach is to quoient out this kernel to give the Hopf algebra $\mathbb{F}_p[x]/(x^p)$ and one will then have that the inherited calculus on this is now connected. On the other hand, this Hopf algebra is rather too small to serve as an approximation of $\mathbb{F}_p[x]$. We ask if we we can do rather better by looking not at the usual differential calculus but a noncommutative one.

A differential structure in noncommutative geometry can be expressed as a differential bimodule (Ω^1,d) of '1-forms' with d obeying the Leibniz rule. This is more general than classical in that we do not assume that differentials commute with 1-forms, i.e. we allow $(\mathrm{d}x)x\neq x\mathrm{d}x$. In this more general setting it is known that irreducible calculi on $\mathbb{F}_p[x]$ are classified by monic irreducibles m [12, 9]. We study

2000 *Mathematics Subject Classification.* Primary 81R50, 58B32, 83C57.

Key words and phrases. Noncommutative geometry, finite field, prime number, Hopf algebra, quantum group, bimodule Riemannian geometry, Galois extension, cocycle, boolean algebra.

the zeroth cohomology $H^0(\mathbb{F}_p[x];m)$ and find that again there is a kernel but that in the 'regular' case with m of degree d, it consists of polynomials in $g_d = x^{p^d} - x$. We also show that this applies precisely when the trace of m is nonzero, see our main Theorem 3.4 in Section 3. Following the same philosophy as before, we are led to introduce and study the Hopf algebras

$$A_d = \mathbb{F}_p[x]/(g_d)$$

again with their inherited calculus, which we show now has $H^0(A_d;m) = \mathbb{F}_p 1$. The generating polynomial g_d here is well-known to be the product of all monic irreducibles of degree dividing d, from which it follows that if $m|n$ then there is a canonical homomorphism $A_n \to A_m$. This forms a directed system of Hopf algebras ordered by divisibility so that one has an inverse limit

$$\widehat{\mathbb{F}_p[x]} = \lim_{\leftarrow} A_d$$

projecting on to every A_d, as well as a map $\mathbb{F}_p[x] \to \widehat{\mathbb{F}_p[x]}$ through which the quotienting maps $\mathbb{F}_p[x] \to A_d$ necessarily factor. Since each monic gives a field extension, it is clear that $A_d \cong \prod_{k|d} \mathbb{F}_{p^d}^{N_k}$ and that

$$\widehat{\mathbb{F}_p[x]} = \prod_m \frac{\mathbb{F}_p[x]}{(m)} \cong \prod_k \mathbb{F}_{p^k}^{N_k}$$

as rings, where N_k is the number of monic irreducibles of degree k; this does not, however, take account of their possible geometric and Hopf structures. The first expression here can be thought of as the product over all prime ideals in $\mathbb{F}_p[x]$, as an example of a more general construction. From that point of view it is natural to think of it as a quotient mod each (m) of $\prod_m \mathbb{F}_p[x]_m$ where $\mathbb{F}_p[x]_m = \lim_{\leftarrow k} \mathbb{F}_p[x]/(m)^k$ in analogy with $\prod_p \mathbb{F}_p$ as a quotient of $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. The inverse limit is a topic for further study and at present we focus on the structure and geometry of the A_d individually while thinking of them loosely as increasingly good approximations of $\mathbb{F}_p[x]$.

In Section 4, we show that the A_d are cocycle extensions $A_d = C_d \otimes_\chi A_1$ where C_d is a polynomial algebra in g_1 with a single relation related to the trace map. In fact this result arises uniformly from $\mathbb{F}_p[x] = \mathbb{F}_p[g_1] \otimes_\chi A_1$ where the cocycle amounts to projection-like identities for the canonical 'delta-functions' $\delta_i(x) = -g_1/(x-i)$, namely

$$\delta_i\delta_i = \delta_i + g_1 \sum_{k=1}^{p-1} \frac{\delta_{i+k}}{k}, \quad \delta_i\delta_j + g_1 \frac{\delta_i - \delta_j}{i-j} = 0, \quad \forall i \neq j$$

as we show in Theorem 4.6. Here g_1 is invariant under $x \to x+1$ while the δ_i shift their index. This also implies that the A_d are (cleft) Hopf-Galois extensions or trivial quantum principal bundles from a geometric point of view. Here A_1 is easily seen to be isomorphic to $\mathbb{F}_p(\mathbb{Z}/p\mathbb{Z})$, so this is a version of an Artin-Schreier covering. We also compute the dimension of the subalgebra of elements of A_d fixed under the Frobenius automorphism.

In Section 5.1 we look at the Hopf algebra Fourier theory from A_1 to its dual, the group algebra $\mathbb{F}_p\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p[t](t^p - 1)$, and we show in Lemma 5.1 that the latter is isomorphic to $\mathbb{F}_p[L]/(L^p)$ by $t = e^L$, using the truncated exponential. This is more complicated than the more obvious $t = 1 + L$ but allows the Fourier transform to have a classical form, see Corollary 5.2, as well as an interesting coproduct on L. We also show that the Fourier transform is compatible with the regular noncommutative differential structures on A_1 and plays the same role as classically.

Finally, Section 5.2 studies the noncommutative Riemannian geometry of A_2 over $\mathbb{F}_2$. This is an application of the concrete 'quantum group' approach to noncommutative geometry developed by many authors but particularly in the bimodule approach in [5, 6, 1] and elsewhere. This approach works for the most part over any field and also particularly applies to finite geometries even though our algebras are commutative (the differentials are not, as we have explained above). There is a unique regular m leading to just one inherited differential calculus on A_2 and for it we find exactly 3 translation-invariant metrics $\eta \in \Omega^1 \otimes_{A_2} \Omega^1$, and for each of these we find exactly two Levi-Civita (i.e. torsion free and metric compatible) bimodule connections. One of these is the obvious 'zero' connection on the basic 1-forms and in each case there is a second flat connection. We present this as an example of what we would like to call 'digital geometry', where we work over $\mathbb{F}_2 = \{0, 1\}$ but retain a geometrical point of view. We believe that this could be of wider interest if it leads to the transfer of geometric ideas to computer science.

Our results demonstrate that one can usefully carry over geometrical concepts to a finite setting over $\mathbb{F}_p$, sometimes even in the extreme case $p = 2$, with the help of Hopf algebras and noncommutative differentials. A more in-depth study of the noncommutative geometry of the general A_d and the possibility of geometry on the inverse limit, as well as its more general context, are some specific topics for future work.

2. Preliminaries

Let A be an algebra over a field k. We think if this as like the coordinate algebra of an algebraic variety (it need not be) and we require enough differentiable structure so as to have an associative 'differential graded algebra' (DGA) of differential forms, namely an exterior algebra $\Omega(A) = \oplus_n \Omega^n$ where $\Omega^0 = A$, equipped with a graded-derivation $\mathrm{d} : \Omega^i \to \Omega^{i+1}$ with respect to the product $\wedge$ and obeying $\mathrm{d}^2 = 0$. We are interested in the standard case where Ω^1 is spanned by elements of the form $a\mathrm{d}b$ for $a, b \in A$ and Ω is generated by degrees 0,1 over A. The cohomology $H^{\cdot}$ of this complex is sometimes called the noncommutative de Rham complex of the DGA. It is worth noting that $H^0 = \ker \mathrm{d} \subseteq A$ is obviously a subalgebra in view of the Leibniz rule and $k.1 \subseteq H^0$. We say that the DGA is *connected* if $k.1 = H^0$, this being the case in classical differential geometry for a connected manifold. In noncommutative differential geometry we are often interested in the case when the calculus in inner, i.e. when there is $\theta \in \Omega^1$ such that $[\theta, a] = \mathrm{d}a$ for all $a \in A$ (and normally also on higher degrees by graded commutator). We refer to [9] for an introduction. This approach to differentials is common to most approaches to noncommutative geometry, including [4], but in our case it is a starting point.

Working with algebraic differential forms, by 'metric' we mean an element $\eta \in \Omega^1 \otimes_A \Omega^1$ which is quantum symmetric in the sense $\wedge(\eta) = 0$ and invertible in the sense of existence of a bimodule map $(\ , \ ) : \Omega^1 \otimes_A \Omega^1 \to A$ such that $(\omega, \eta^1)\eta^2 = \omega = \eta^1(\eta^2, \omega)$ for all $\omega \in \Omega^1$. Here $\eta = \eta^1 \otimes \eta^2$ (a sum of such terms understood) is a notation. One can show[1] that such an η is necessarily central. By a 'left connection', in our case on Ω^1, we mean $\nabla : \Omega^1 \to \Omega^1 \otimes_A \Omega^1$ such that $\nabla(a\omega) = a\nabla\omega + \mathrm{d}a \otimes \nabla\omega$ for all $a \in A$ and $\omega \in \Omega^1$. By a 'bimodule connection' we mean a left connection such that in addition $\nabla(\omega a) = (\nabla\omega)a + \sigma(\omega \otimes \mathrm{d}a)$ for some bimodule map $\sigma : \Omega^1 \otimes_A \Omega^1 \to \Omega^1 \otimes_A \Omega^1$. If a left connection admits such a σ then the latter is unique, hence this is a property of ∇ and not further data. In this case one has the notion of metric compatible connection $\nabla\eta = 0$ where ∇ acts on each tensor factor Ω^1 and σ is used to correctly position its output when acting on the second tensor factor. Finally, the torsion of a connection on Ω^1 is $T = \wedge\nabla - \mathrm{d} : \Omega^1 \to \Omega^2$ and in noncommutative Riemannian geometry we are ideally interested in finding a 'Levi-Civita' bimodule connection defined as metric compatible and torsion free. In the inner case it is shown in [13] that the construction of a bimodule connection is equivalent to bimodule maps σ as above and $\alpha : \Omega^1 \to \Omega^1 \otimes_A \Omega^1$. This is torsion free if and only if

$$\wedge\,\alpha = 0, \quad \wedge\sigma = -\wedge \tag{2.1}$$

and metric compatible if and only if

$$\theta \otimes \eta + (\alpha \otimes \mathrm{id})\eta + \sigma_{12}(\mathrm{id} \otimes (\alpha - \sigma_\theta))\eta = 0. \tag{2.2}$$

We will use these equations in Section 5.

Now let A be augmented by a unital algebra hom $\epsilon : A \to k$ (so $\epsilon(1) = 1$). We think of ϵ as defining a 'point' and the following construction as a step towards its 'connected component'. If A is a Hopf algebra we take counit as the augmentation (corresponding in the classical case to the group identity).

Proposition 2.1. *Let (A, ϵ) be an augmented algebra, $\Omega(A)$ a DGA and $H^0(A)$ its degree zero cohomology. We define $A_c = A/\langle H^0(A) \cap \ker\epsilon\rangle$ with its inherited differential calculus. If A is a Hopf algebra and $\Omega(A)$ bicovariant then $H^0(A)$ is a sub-Hopf algebra, A_c is a quotient Hopf algebra and $\Omega(A_c)$ is bicovariant.*

Proof. Clearly $J = H^0(A) \cap \ker\epsilon$ is a subalgebra by the Leibniz rule and we quotient by the ideal it generates intersected with the ideal A^+. More generally, we define $\Omega(A_c) = \Omega(A)/\langle H^0(A) \cap \ker\epsilon\rangle$ where we quotient by the ideal generated in the exterior algebra. The map d descends to this quotient since by definition $\mathrm{d}(ga) = (\mathrm{d}g)a + g\mathrm{d}a = g\mathrm{d}a$ for all $g \in J$.

For the second part, by assumption there exist left and right coactions Δ_L, Δ_R commuting with d. Hence if $a \in \ker\mathrm{d} = H^0$ it follows that $(\mathrm{d} \otimes \mathrm{id})\Delta a = \Delta_L \mathrm{d}a = 0$ and $(\mathrm{id} \otimes \mathrm{d})\Delta a = \Delta_R \mathrm{d}a = 0$. Hence $\Delta a \in H^0 \otimes H^0$ and we have a sub-Hopf algebra. It follows that $J = H^{0+}$ is a coideal (here if $a \in J$ then $\Delta a = a_{(1)} \otimes (a_{(2)} - 1\epsilon(a_{(2)})) + a \otimes 1 \in A \otimes J + J \otimes A$). In this case $I = \langle A \rangle$ the ideal it generates is a Hopf ideal and $A_c = A/I$ is a Hopf algebra. Employing the construction above, the assumed $\Delta_{L,R}$ descend to A_c since these are part of Hopf module structures, eg $\Delta_L(\omega a) = (\Delta_L\omega)\Delta a \subseteq AJ \otimes \Omega^1 + A \otimes \Omega^1 J$ for $a \in J$ and $\omega \in \Omega^1$. Hence $\Omega^1(A_c)$ is bicovariant. The higher order calculi will be generated by Ω^1, A_c with the inherited relations and since the latter are bicovariant, the higher forms will be too. Equivalently, $\Omega(A)$ is a super-Hopf algebra with $\Delta_L + \Delta_R$ in degree 1 and we can view J as a super-coideal. $\square$

It is not clear that the quotient DGA now has $H^0(A_c) = k1$ but this is a step in the right direction and could be iterated. However, in our application this construction will do the job in one step.

The other ingredient in the paper is the construction in [12, 9] whereby irreducible bicovariant calculi on $k[x]$ correspond to monic irreducible m. The latter defines a field extension $K = k[\mu]/(m(\mu))$ and $\Omega^1(k[x]; m) = K[x]$ as a left $k[x]$-module in the obvious way and

$$v \cdot f(x) = f(x+\mu)v, \quad \mathrm{d}f = (f(x+\mu) - f(x))\mu^{-1}, \quad \forall f \in k[x],\ v \in K$$

in terms of the algebra $K[x]$ and provided $\mu \in K^*$; this is understood as the classical calculus when $\mu = 0$. The non-classical case is inner with $\theta = \mu^{-1}$. The entire exterior algebra is of the form $\Omega = \Lambda[x]$ where $\Lambda = \Lambda(K)$ is the usual exterior algebra of K as a vector space over k and in the inner case has $\mathrm{d} = [\theta, \ \}$ given by graded-commutator. Note that if $k \subseteq K$ is a field extension and $\mu \in K$ then there is a possibly non-surjective translation-invariant calculus $\Omega^1_{\mu,K}(k[x]) = K[x]$ as a left $k[x]$-module and the description above, which is an actual calculus if K is generated by k, μ. Conversely, every translation-invariant calculus on $k[x]$ is of this form with K given by adjoining μ subject to a relation $m(\mu) = 0$. The calculus depends on μ and hence on m.

Lemma 2.2. *Suppose that $H^0(k[x]; m) \neq k.1$ and let $g \in H^0$ have minimal positive degree. Then $H^0(k[x]; m) = k[g]$.*

Proof. Let $f \in H^0$ and let $f = f_1 g + r_1$ where $\deg r_1 < \deg g$. Then $\mathrm{d}r_1 + (\mathrm{d}f_1)g = 0$ as $\mathrm{d}g = 0$. Viewing this in the ring $K[x]$ we have the first term degree $< \deg g$ and the 2nd term degree $\geq \deg g$, hence both terms vanish and since g had minimal degree among non-constants in H^0 we conclude that r_1 is a constant, $\mathrm{d}f_1 = 0$. Iterating, we conclude that f is a polynomial in g. □

3. Structure of $H^0(\mathbb{F}_p[x]; m)$

We consider $A = \mathbb{F}_p[x]$ and calculi defined by monic irreducible m of degree d and let P denote the linear subspace of $\mathbb{F}_p[x]$ involving only power-p exponents (we will explain later that P is the set of primitive elements of A as a Hopf algebra). If $f \in P$ then f is additive and hence, when $\mu \neq 0$,

$$\mathrm{d}f = f(\mu)\mu^{-1} \in \mathbb{F}_{p^d}, \quad [v, f] = f(\mu)v, \quad \forall v \in \mathbb{F}_{p^d}$$

where $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^d}[x]$ is the subspace of left-invariant 1-form in the calculus. Thus $f \in H^0 \cap P$ are characterised by $f(\mu) = 0$, while general $f \in H^0$ are characterised by $f(x+\mu) = f(x)$ which implies $f(\mu) = f(0)$ or $f(\mu) = 0$ for $f \in H^0 \cap \ker\epsilon$ as a necessary condition.

The case $d = 1$ is easy enough to analyse in full detail and includes the case where $\mu = 0$. Here monic irreducibles have the form $m(x) = x - \mu$, for some $\mu \in \mathbb{F}_p$. This gives a 1-dimensional calculus and of course no actual extension of the field. The field extension defined by m would have generator set equal to μ, which is why we have denoted this as the constant to fit with our previous notation. The case $\mu = 0$ also leads to a calculus which we understand as the classical one. We let

$$g_1(x) = x^p - x = x(x^{p-1} - 1) = x(x-1)(x-2)\cdots(x-(p-1)) \in P.$$

Proposition 3.1. *For $d = 1$, $H^0(\mathbb{F}_p[x]; m) = \begin{cases} \mathbb{F}_p[x^p] & \text{if } \mu = 0 \\ \mathbb{F}_p[g_1] & \text{if } \mu \neq 0 \end{cases}$.*

Proof. If $\mu = 0$ we have the classical calculus where $\mathrm{d}x^m = mx^{m-1}\mathrm{d}x = 0$ when $m = p$, and clearly any non-constant polynomial of lower degree will not be in the kernel by looking at its top degree. We then use Lemma 2.2. When $\mu \neq 0$ we manifestly have $g_1(x + \mu) = g_1(x)$ (from the form of g_1) and we show that its degree p is the minimal degree of non-constant elements of H^0. Thus, let f be monic of degree $t < p$ so $f = x^t + cx^{t-1} + \cdots$ for some $c \in \mathbb{F}_p$. We have $f(x+\mu) = x^t + \mu t x^{t-1} + cx^{t-1} + \cdots$ where we indicate further terms of degree $< t$. For this to equal f we need $\mu t = 0 \bmod p$, which requires $t = 0$ as $t < p$. Hence $f = 1$. We then use Lemma 2.2. □

More generally, we let

$$g_n(x) = x^{p^n} - x \in P. \tag{3.1}$$

which is well-known to be the product of all irreducible monics in $\mathbb{F}_p[x]$ of degree dividing n. We are interested in a fixed monic m of degree d defining our differential calculus and associated $\mathbb{F}_{p^d} = \mathbb{F}_p[\mu]/(m)$.

Lemma 3.2. *For m of degree d other than $m = x$ (or $\mu = 0$) already covered, we have $H^0(\mathbb{F}_p[x]; m) \supseteq \mathbb{F}_p[g_d]$ and $g_i \notin H^0(\mathbb{F}_p[x]; m)$ for $i = 1, 2, \cdots, d-1$.*

Proof. Clearly m is a factor of g_d so $g_d(\mu) = 0$. This is also immediate from $\mu^{p^d-1} = 1$ in $\mathbb{F}_{p^d}$. Hence excluding the special case $\mu = 0$, we have $g_d \in H^0(\mathbb{F}_p[x]; m)$ and hence (by the Leibniz rule) that all polynomials of it are contained in the cohomology. If $g_i(\mu) = 0$ for some $i < d$ then μ is a zero of some irreducible monic of degree dividing i and hence of degree $< d$. This would have to be divisible by m, which is a contradiction. Hence $\mathrm{d}g_i \neq 0$ for $1 \leq i < d$. □

We say that m of degree d is *regular* if $H^0(\mathbb{F}_p[x]; m) = \mathbb{F}_p[g_d]$. We have seen that this happens for $d = 1$ precisely when $\mu \neq 0$. We will also be interested in

$$h_d = x^{p^{d-1}} + x^{p^{d-2}} + \cdots + x \in P \tag{3.2}$$

where h_d is the trace for the field extension when viewed as a map $\mathbb{F}_{p^d} = \mathbb{F}_p[\mu]/(m) \to \mathbb{F}_p$.

Lemma 3.3. *If $h_d(\mu) = 0$ then m of degree d is not regular, and $H^0(\mathbb{F}_p[x]; m) \supseteq \mathbb{F}_p[h_d]$ when $d > 1$.*

Proof. If $d = 1$ and $h_1(\mu) = 0$ then $\mu = 0$ and we know that this case is not regular by the above. If $d > 1$ and $h_d(\mu) = 0$ then $h_d \in H^0$ by the above remarks and hence so is the subalgebra $\mathbb{F}_p[h_1]$ by the Leibniz rule. We also have

$$g_d = h_d(h_d^{p-1} - 1) \tag{3.3}$$

so that $\mathbb{F}_p[g_d] \subsetneq \mathbb{F}_p[h_d]$ and this is strict as h_d has lower degree and clearly can't be written as a polynomial in g_d. Hence if $h_d(\mu) = 0$ then m cannot be regular. □

Theorem 3.4. *m of degree d has $H^0(\mathbb{F}_p[x]; m) = \mathbb{F}_p[g_d]$, i.e. is regular, if and only if $h_d(\mu) \neq 0$.*

Proof. $d = 1$ was already covered so we fix $d \geq 2$ and prove the assertion for $h_d(\mu) \neq 0$ by induction. Thus, suppose for some n in the range $1 \leq n \leq d$ that if f is of degree $< p^{n-1}$ and $f(x+\mu) - f(x) = c\mu^{p^i}$ for some constant $c \in \mathbb{F}_p$ and some $i = 1, \cdots, d-1$ then $f(x) = f(0)$ and $c = 0$. We note that if f has degree $< p$ and obeys the condition stated then the argument in the proof of Proposition 3.1 is unaffected when we look at powers of $x > 1$ and similarly allows us to conclude that $f(x) = f(0) + c\mu^{p^i - 1}x$. We write this as $(f(x) - f(0))\mu = c\mu^{p^i}x$ and apply the Trace to both sides, so $(f(x) - f(0) - cx)h_d(\mu) = 0$ (using invariance of the Trace under the Frobenius) and hence $f(x) = f(0) + cx$. Putting in this information, we have $g_i cx = 0$ and hence $c = 0$ using the second part of Lemma 3.1. Thus the hypothesis holds for f of degree $< p$.

Now consider f of degree $< p^n$ and write this as $f = \sum_{k=0}^{p-1} x^{p^{n-1}k} f_k(x)$ where f_k have degree $< p^{n-1}$. We also write

$$\begin{aligned}
f(x+\mu) &= \sum_{k=0}^{p-1} (x^{p^{n-1}} + \mu^{p^{n-1}})^k f_k(x) + \sum_{k=0}^{p-1} (x^{p^{n-1}} + \mu^{p^{n-1}})^k (f_k(x+\mu) - f_k(x)) \\
&= f(x) + A_{p-1}(x) \\
A_m(x) &= \sum_{k=0}^{m} x^{p^{n-1}k}(f_k(x+\mu) - f_k(x)) + \sum_{k=0}^{m}\sum_{s=0}^{k-1} \mu^{p^{n-1}(k-s)} x^{p^{n-1}s} \binom{k}{s} f_k(x+\mu) \\
&= x^{p^{n-1}m}(f_m(x+\mu) - f_m(x)) + \sum_{s=0}^{m-1} \mu^{p^{n-1}(m-s)} x^{p^{n-1}s} \binom{m}{s} f_m(x+\mu) + A_{m-1}
\end{aligned}$$

Now suppose that $f(x+\mu) = f(x) + c\mu^{p^i}x$ for some c and some $i < d$, i.e. $A_{p-1}(x) = c\mu^{p^i}$. We prove by induction that this implies that $c = 0$ and f is constant. Indeed, suppose $A_m(x) = c\mu^{p^i}$. From the second expression for $A_m(x)$, only the first term has powers of degree $\geq p^{n-1}m$ and $A_m(x) = c\mu^{p^i}$ tells us that $f_m(x+\mu) - f_m(x) = 0$ and hence by our inductive assumption, $f_m(x) = f_m(0)$ is a constant. Putting in this information gives us

$$\sum_{s=0}^{m-1} \mu^{p^{n-1}(m-s)} x^{p^{n-1}s} \binom{m}{s} f_m(0) + A_{m-1}(x) = c\mu^{p^i}$$

We now pick off the $\geq p^{n-1}(m-1)$ degrees to find

$$f_{m-1}(x+\mu) - f_{m-1}(x) + m\mu^{p^{n-1}} f_m(0) = 0$$

and our induction hypothesis allows us to conclude that $f_m(0) = 0$ and hence that $A_{m-1}(x) = c\mu^{p^i}$. Starting at $m = p-1$ we now iterate this argument to conclude that $f_{p-1} = 0, \cdots, f_1 = 0$ and $A_0(x) = c\mu^{p^i}$, and hence that $f = f_0 \in H^0$ has degree $< p^{n-1}$. We then conclude by our overall induction hypothesis that f is a constant and $c = 0$. Proceeding inductively, we have proven our hypothesis for all f of degree $< p^d$.

In particular, we apply this result with $c = 0$ to conclude that H^0 contains no nonconstant elements of degree $< p^d$. Hence the degree p^d of g_d is minimal among nonconstants in H^0. We then use Lemma 2.2. Lemma 3.3 provides the other direction when $h_d(\mu) = 0$. $\square$

Corollary 3.5. *$h_d(\mu) \neq 0$ iff m of degree d has a nonzero coefficient in degree $d-1$. Moreover, there are*

$$\frac{p-1}{pd} \sum_{k|d; p\nmid k} \mu_{M\ddot{o}b}(k) p^{\frac{d}{k}}$$

such m, where $\mu_{M\ddot{o}b}$ is the Möbius function.

Proof. Here $h_1(\mu) = \mathrm{Trace}(\mu)$ is the trace for $\mathbb{F}_p[\mu]/(m) \to \mathbb{F}_p$ and it is a fact from number theory[7] that $\mathrm{Trace}(\mu) = -m_{d-1}$ where $m(x) = x^d + m_{d-1}x^{d-1} + \cdots + m_0$ is the minimal polynomial of μ, which is our case by construction. Hence $h_1(\mu) \neq 0$ if and only $m_{d-1} \neq 0$. Next, the number of monic irreducibles in $\mathbb{F}_p[x]$ with a fixed non-zero value of this coefficient was found by Carlitz[2] and more recently in the form we use in [15]. As we required only a non-zero value, we multiply this by the $p-1$ possible values to give the expression stated. □

This gives an easy criterion to tell if a given m is regular. The number of such should be compared with Gauss' formula for the number N_d of all irreducible m of degree d, $N_d = \frac{1}{d}\sum_{k|d} \mu_{\mathrm{M\ddot{o}b}}(k) p^{\frac{d}{k}}$. Thus a good fraction of m are regular. The formula gives $p-1$ regular m as it should for $d=1$ by Proposition 3.1.

Also note that the factorisation (3.3) means that either $h_d(\mu) = 0$ (the non-regular case) or m divides $(h_d - 1)(1 + h_d + \cdots h_d^{p-2})$ (the regular case) according to our theorem. Meanwhile, Lemma 3.3 suggests a similar result for the cohomology for the flip side when $h_d(\mu) = 0$:

Conjecture 3.6. *m of degree $d > 1$ has $H^0(\mathbb{F}_p[x]; m) = \mathbb{F}_p[h_d]$ if and only if $h_d(\mu) = 0$.*

It is not clear that this can be proven by similar methods to those of our main theorem. We also note in passing that as well as the Trace there is a norm map $N : \mathbb{F}_{p^d} \to \mathbb{F}_p$ defined as

$$N(x) = x x^p \cdots x^{p^{d-1}} = x^{1+p+p^2+\cdots p^{d-1}} = x^{[d]_p}, \quad [d]_p = \frac{p^d - 1}{p-1}$$

and $N(\mu) = (-1)^d m_0 \neq 0$ as m is irreducible. Hence $N \notin H^0(\mathbb{F}_p[x]; m)$.

Example 3.7. By computer computations (checked at least to polynomial degree 100) we have for $p = 2$ and $d \leq 4$,

(1) $H^0(\mathbb{F}_2[x]; \mu^2 + \mu + 1) = \mathbb{F}_2[x^4 + x] = \mathbb{F}_2[g_2]$
(2) $H^0(\mathbb{F}_2[x]; \mu^3 + \mu^2 + 1) = \mathbb{F}_2[x^8 + x] = \mathbb{F}_2[g_3]$
(3) $H^0(\mathbb{F}_2[x]; \mu^3 + \mu + 1) = \mathbb{F}_2[x^4 + x^2 + x] = \mathbb{F}_2[h_3]$
(4) $H^0(\mathbb{F}_2[x]; \mu^4 + \mu^3 + \mu^2 + \mu + 1) = \mathbb{F}_2[x^{16} + x] = \mathbb{F}_2[g_4]$
(5) $H^0(\mathbb{F}_2[x]; \mu^4 + \mu^3 + 1) = \mathbb{F}_2[x^{16} + x] = \mathbb{F}_2[g_4]$
(6) $H^0(\mathbb{F}_2[x]; \mu^4 + \mu + 1) = \mathbb{F}_2[x^8 + x^4 + x^2 + x] = \mathbb{F}_2[h_4]$

One can also see here that the regular m are precisely the factors of degree d in $h_d + 1$, as per the general theory when $p = 2$. We also see the right number of regular ones as per the formula.

4. The Hopf algebras A_d

Motivated by the above cohomology computations, for each $d \in \mathbb{N}$ and each regular m of degree d we define

$$A_d := \mathbb{F}_p[x]/(g_d) = \mathbb{F}_p[x]/(x^{p^d} - x), \quad \Omega(A_d; m) = \Omega(\mathbb{F}_p[x]; m)/\langle g_d \rangle$$

Here $J = H^0 \cap \ker\epsilon = \mathrm{span}\{g_d^m \mid m > 0\} = \mathbb{F}_p[g_d]^+$ where the $+$ denotes functions with no constant term. Hence $\mathbb{F}_p[x]J = (g_d)$ is the ideal that we quotient out by to define A_d.

We think of the algebra A_d as defining a 'space' at a topological level in some sense, and in this regard we note that A_d as defined depends only on the degree of the field extension. We think of m as adding to this data a differentiable structure inherited from the one on $\mathbb{F}_p[x]$.

Corollary 4.1. *$H^0(A_d; m) = \mathbb{F}_p 1$ for the inherited differential structure from any regular monic irreducible m of degree d.*

Proof. This is immediate from Theorem 3.4 and we use the notations there. Suppose that $f(x + \mu) - f(x) \in (g_d)$ in $\mathbb{F}_{p^d}[x]$, i.e. products of g_d with polynomials that include powers of μ in their coefficients. In $\mathbb{F}_p[x]$ we let $f = hg_d + r$ where either $r = 0$ (so $f = 0$ in A_d) or the degree of r is less than p^d. Then $h(x+\mu)g_d(x+\mu) + r(x+\mu) - h(x)g_d(x) - r(x) = (h(x+\mu) - h(x))g_d(x) + r(x+\mu) - r(x) \in (g_d)$ since $g_d(x+\mu) = g_d(x)$ as g_d is additive and $g_d(\mu) = 0$. Hence $r(x+\mu) - r(x) \in (g_d)$. But since every nonzero element of (g_d) has degree $\geq p^d$ we conclude that $r(x+\mu) - r(x) = 0$ and hence by Theorem 3.4 that r is a constant, hence f is a multiple of the identity in A_d. . □

This means that we achieved our goal of having finite-dimensional quotients of $\mathbb{F}_p[x]$ equipped now with (a moduli space of) connected differential calculi. We now turn to the algebraic structure of the A_d.

Corollary 4.2. *A_d is a p^d-dimensional Hopf algebra and $\Omega(A_d)$ is bicovariant. Moreover, the primitive elements of A_d are spanned by the set $\{x^{p^i} : 0 \leq i < d\}$*

Proof. As x is primitive, we have

$$\Delta x^n = \sum_{k=0}^{n} \binom{n}{k} x^k \otimes x^{n-k}$$

By Lucas' theorem, $\binom{n}{k} = 0 \mod p$ iff a base p digit of k is greater than the corresponding digit of n. Hence x^n is primitive if $n = p^i$ for some i. Conversely, if n is not a power of p, then there exist some $k \neq 0, n$ for which $\binom{n}{k} \neq 0 \mod p$, and so x^n is not primitive. It then follows easily that the primitive elements of $\mathbb{F}_p[x]$ are precisely spanned by the p-power exponents. In particular, g_d is primitive and hence A_d is a Hopf algebra. Its primitives have the same form but restricted to degree $< p^d$. Here $\mathbb{F}_p[g_d]$ is a Hopf algebra with g_d primitive and in this way a sub-Hopf algebra of $\mathbb{F}_p[x]$ as per the general theory in Section 2. The latter also implies bicovariance. □

Next, A_d carries the Frobenius automorphism $F(x) = x^p$ and hence always contains a Frobenius-fixed subalgebra $B_d = A_d^F$ every element equals its p-power. For $p = 2$ this means that B_d is a Boolean subalgebra.

Proposition 4.3. *dim* $B_d = \frac{1}{d}\sum_{k|d}\phi(k)p^{\frac{d}{k}}$, *the number of irreducible factors of* g_d. *Here* ϕ *is the Euler totient function.*

Proof. The Frobenius automorphism has order d and permutes the set $\{1, x, x^2, \ldots, x^{p^d-1}\}$. Write this permutation in its decomposition as cycles $\sigma_1, \ldots \sigma_b$. When a polynomial f is the sum of monomials from an orbit of a σ_i it is fixed by the endomorphism. The set of such polynomials (with all coefficients 1) is linearly independent and generates B_d. Now let $C_s = \{sp^j \mod p^d - 1 : 0 \le j \le d-1\}$ be the cyclotomic coset of p modulo $p^d - 1$ containing s. Note that each C_s and C_r are either disjoint or equal. Let $\mathcal{C} \subset \mathbb{Z}/(p^d-1)\mathbb{Z}$ be such that

$$\bigcup_{s\in\mathcal{C}} C_s = \mathbb{Z}/(p^d-1)\mathbb{Z}$$

and each pair C_s and C_r are disjoint for $s, r \in \mathcal{C},\ s \neq r$. $\mathcal{C}$ is in bijection with the set of orbits of the permutation cycles define above, excluded the singleton orbit $\{x^{p^d-1}\}$, which comes from the additional factor of x in the polynomial modulus: let $s \in \mathcal{C}$, if $x^s \in \mathrm{orb}\sigma_i$, then $\mathrm{orb}\sigma_i = \{x^{sp^j} \mod x^{p^d} - x : 0 \le j \le d-1\}$.

Let $\alpha \in \mathbb{F}_{p^d}$ be a generator for the multiplicative group $\mathbb{F}_{p^d}^\times$. It is well known [8] that

$$x^{p^d-1} - 1 = \prod_{s\in\mathcal{C}} m_s(x)$$

for $m_s(x) = \prod_{a\in C_s}(x - \alpha^a)$, hence the set of orbits of the permutation, and thus the basis we've given, is in bijective correspondence with irreducible factors of $x^{p^d} - x$. □

Also note that g_i has a factor g_j whenever j divides i since it includes all irreducibles of degree that divide j. Hence we have a directed system of Hopf algebras

$$\{A_j \to A_i \mid i \text{ divides } j\}$$

ordered by divisibility. The full system will be studied elsewhere while here we focus on the canonical Hopf algebra maps $\pi : A_d \to A_1$, since 1 divides every integer. To find the kernel of this map we consider the canonical automorphism of the algebra A_d given by the order p periodicity map $\psi(x) = x+1$. Here $g_i(x+1) = (x+1)^{p^i} - (x+1) = g_i(x)$ working over $\mathbb{F}_p$, so these give invariant elements of A_d for $i = 1, \cdots, d-1$. We will be interested in the invariant subalgebra $C_d = A_d^\psi$ of A_d.

Proposition 4.4. $C_d = \mathbb{F}_p[g_1]/(h_d(g_1))$ *for all* $d \in \mathbb{N}$ *is a Hopf algebra of dimension* p^{d-1} *and*

$$C_d \hookrightarrow A_d \twoheadrightarrow A_1$$

is an extension of Hopf algebras.

Proof. We start with $\mathbb{F}_p[x]^\psi = \mathbb{F}_p[g_1]$. This is a well-known fact from Artin-Schreier theory but for completeness we include an elementary proof from [14]. If $f(x+1) = f(x)$ and f has degree $< p$ then the proof of Proposition 3.1 with $\mu = 1$ applies and allows us to conclude that $f(x)$ is a constant. More generally let $f(x) = g_1h(x)+r(x)$ where r has degree $< p$. Then $g_1(h(x+1)-h(x)) = -(r(x+1)-r(x))$ which by degrees requires both h and r to be invariant. Thus r is a constant and h is an invariant of lower degree, leading to the result. Also clearly, the $\{g_i^i\}$ are linearly independent over $\mathbb{F}_p$ (by looking at the top degree of a polynomial relation). Also in $\mathbb{F}_p[x]$ we have $h_i(g_1) = g_1+g_1^p+\cdots g_1^{p^{i-1}} = x^p-x+(x^p-x)^p+\cdots+(x^p-x)^{p^{i-1}} = x^p - x + x^{p^2} - x^p + \cdots x^{p^i} - x^{p^{i-1}} = g_i$ on cancellation. In particular, $h_d(g_1) = g_d$, and if a polynomial in g_1 of degree $< p^{d-1}$ is divisible by g_d then, by degrees, it must separately vanish. Hence polynomials in g_1 up to degree $< p^{d-1}$ viewed in A_d form a p^{d-1}-dimensional subalgebra. Finally, if $f \in \mathbb{F}_p[x]$ has degree $< p^d$ and $f(x+1) - f(x)$ is divisible by g_d then by degrees is must separately vanish, hence $C_d = \mathbb{F}_p[g_1]/(g_d) = \mathbb{F}_p[g_1]/(h_d(g_1))$. This inclusion $i : C_d \hookrightarrow A_d$ makes C_d a sub-Hopf algebra as g_1 is primitive. The Hopf algebra map $\pi : A_d \to A_1$ where we quotient by (g_1) clearly obeys $\pi \circ i = 1\epsilon$ since it is 1 on $1 \in C_d$ and vanishes on C_d^+. It follows from general arguments since the Hopf algebras involved are finite dimensional, see [16, Cor 3.2.2], that this gives an exact sequence of Hopf algebras in the technical (cleft) sense provided only that the dimensions match. This is our case as we have seen that $\dim(A_1)\dim(C_d) = \dim(A_d)$. $\square$

It follows from the theory of such extensions of Hopf algebras that A_d is a cocycle bicrossproduct of C_d and A_1[10]. We will give this explicitly and in fact the extension result applies for $\mathbb{F}_p[x]$ as well, not only the finite-dimensional quotients. We first define

$$\delta_i(x) = -\frac{g_1}{x-i} = -\prod_{j\neq i}(x-j) \in \mathbb{F}_p[x], \quad i = 0, \cdots, p-1$$

which clearly obey $\psi(\delta_i) = \delta_{i-1}$. Hence $\sum_i \delta_i$ is ψ-invariant and has degree $p-1$ hence is a constant. Evaluating at zero, only $\delta_0(0) = -(p-1)! = 1$ is non-zero, we have

$$\sum_i \delta_i = 1.$$

The following is well-known in the context of Mahler's theorem or Artin-Schreier theory but we include a short proof as a model for the proof of the theorem:

Lemma 4.5. *$A_1 \cong \mathbb{F}_p(\mathbb{Z}/p\mathbb{Z})$ the Hopf algebra of functions on the finite group $\mathbb{Z}/p\mathbb{Z}$.*

Proof. We identify the Kronecker delta-function at $i \in \mathbb{Z}/p\mathbb{Z}$ with $\delta_i \in A_1$ i.e. viewed mod g_1. Clearly in A_1 we have $\delta_i(x-i) = 0$ and hence $\delta_i\delta_j = 0$ in A_1 for $i \neq j$, so that $\delta_i\delta_i = \delta_i$ in A_1 from $\sum \delta_i = 1$. Hence this is an isomorphism of algebras. For the coproduct we note that the image of the coproduct of $\mathbb{F}_p[x]$ has the property of invariance under $\psi\otimes\psi^{-1}$ acting in the two factors (this clear for Δx and therefore applies on any polynomial). Since $\{\delta_i\}$ by the above relations form a basis of A_1, we let $\Delta\delta_k = \sum_{i,j} c_{ij}^k \delta_i \otimes \delta_j$ for some $c_{ij}^k \in \mathbb{F}_p$. Then invariance implies that ${c^k}_{i,j} = c_{0,i+j}^k$. However, $\epsilon(\delta_i) = \delta_{i,0}$ and the counity axiom then implies that $c_{0,i}^k = \delta_{k,i}$. Hence $\Delta\delta_i = \sum_{j=0}^{p-1} \delta_{i-j} \otimes \delta_j$ as for $\mathbb{F}_p(\mathbb{Z}/p\mathbb{Z})$. $\square$

Theorem 4.6. *Let $p>2$. $\mathbb{F}_p[x]=\mathbb{F}_p[g_1]\otimes_\chi A_1$ is a cocycle cleft extension by A_1 coacting via ψ and with cocycle*

$$\chi: A_1\otimes A_1\to \mathbb{F}_p[g_1],\quad \chi(\delta_i\otimes\delta_j)=\begin{cases}1 & \text{if } i=j=0\\ \frac{g_1}{j} & \text{if } i=0,\ j\neq 0\\ \frac{g_1}{i} & \text{if } i\neq 0,\ j=0\\ -\frac{g_1}{i} & \text{if } i=j\neq 0\\ 0 & \text{else}\end{cases}.$$

This amounts to the new identities for δ-functions in $\mathbb{F}_p[x]$,

$$\delta_i\delta_i=\delta_i+g_1\sum_{k=1}^{p-1}\frac{\delta_{i+k}}{k},\quad \delta_i\delta_j=-g_1\frac{\delta_i-\delta_j}{i-j}$$

for all $i,j\in\mathbb{F}_p$ and $i\neq j$. The coproduct of $\mathbb{F}_p[x]$ becomes

$$\Delta\delta_i=\sum_{j=0}^{p-1}\delta_{i-j}\otimes\delta_j,\quad \Delta g_1=g_1\otimes 1+1\otimes g_1,\quad \epsilon\delta_i=\delta_{i,0},\quad \epsilon g_1=0$$

so that A_1 is a subcoalgebra. These formulae descend to $A_d=C_d\otimes_\chi A_1$ for all $d\geq 1$.

Proof. In view of Lemma 4.5, the action of $\mathbb{Z}/p\mathbb{Z}$ via ψ on $\mathbb{F}_p[x]$ becomes a right coaction $\Delta_R f=\sum\psi^i(f)\otimes\delta_i$ of A_1. Clearly $\Delta_R(\delta_i)=\sum_j\delta_{i-j}\otimes\delta_j$ viewed in $\mathbb{F}_p[x]\otimes A_1$. Then $j:A_1\to\mathbb{F}_p[x]$ sending $j(\delta_i)=\delta_i$ is a right comodule map. It is also convolution-invertible with $j^{-1}(\delta_j)=\delta_{-j}$ as

$$\sum_j\delta_j\delta_{j-i}=\delta_{i,0}$$

This is because the sum is ψ-invariant hence by degrees is at most linear in g_1. The constant value is $\delta_{i,0}$ since only $\delta_0(0)=1$ is non-zero, while

$$\delta_0^2=1+O(x^2),\quad \delta_0\delta_j=-\frac{1}{j}x+O(x^2),\quad \delta_i\delta_j=O(x^2)$$

for all $i,j\neq 0$. Using that $\sum_{i=1}^{p-1}1/i=0$ which is equivalent to $\sum_{i\in\mathbb{F}_p}i=0$ mod p valid for $p>2$, one has that $\sum_j\delta_j\delta_{j-i}$ has zero coefficient in degree 1, so there is no g_1 term. Hence we have a cleft extension and $\mathbb{F}_p[x]\cong\mathbb{F}_p[g_1]\otimes_\chi A_1$ for some cocycle $\chi:A_1\otimes A_1\to\mathbb{F}_p[g_1]$ which we compute from

$$\chi(\delta_i\otimes\delta_j)=\sum_k j(\delta_{i-k})j(\delta_{j-k})j^{-1}(\delta_k)=\sum_k\delta_{i+k}\delta_{j+k}\delta_k.$$

This is again ψ-invariant and has at degree at most $(p-1)^3$, so is at most quadratic in g_1. Looking to degree 2, we have

$$\delta_i\delta_j\delta_k=O(x^3),\quad \delta_i\delta_j\delta_0=\frac{x^2}{ij}+O(x^3),\quad \delta_i\delta_0^2=-\frac{x}{i}-\frac{x^2}{i^2}+O(x^3),\quad \delta_0^3=1+O(x^3)$$

where we used that $\sum_{i=1}^{p-1}1/i^2=0$ mod p for $p>3$, which is equivalent to a power-sum identity $\sum_{i\in\mathbb{F}_p}i^2=0$ mod p for $p>3$ (this is well-known to hold for all powers not divisible by $p-1$, see [3]). From this one can see that χ has no x^2 coefficient and hence is at most constant plus linear in g_1. We then use our previous properties to match the coefficient of x, to give the form stated. From the theory of extensions, see [10], we will be able to recover the product of $\mathbb{F}_p[x]$ from

$$(c\otimes\delta_i)(c'\otimes\delta_j)=cc'\sum_k\chi(\delta_{i-k}\otimes\delta_{j-k})\otimes\delta_k,\quad\forall c,c'\in\mathbb{F}_p[g_1]$$

which implies in particular that

$$\delta_i\delta_j=\sum_{k=0}^{p-1}\chi(\delta_{i-k}\otimes\delta_{j-k})\delta_k$$

holds in $\mathbb{F}_p[x]$. This provides the identities stated. Finally, we look at the coproduct. Since its image in $\mathbb{F}_p[x]\otimes\mathbb{F}_p[x]$ is invariant under $\psi\otimes\psi^{-1}$ and we take a general form of this given the factorisation as algebras, namely $\Delta\delta_i=\sum_{j,k}\delta_j c^i_{j,k}\delta_k$ for $c^i_{j,k}\in\mathbb{F}_p[g_1]\otimes\mathbb{F}_p[g_1]$. The same arguments as in the proof of Lemma 4.5 apply and tell us that $\Delta\delta_i=\sum_{j,k}\delta_j c^i_{0,j+k}\delta_k$. Writing $c^i_{0,j}=\delta_{i,j}+g_1\otimes 1b^i{}_j+1\otimes g_1 b'^i{}_j+(g_1\otimes g_1)c'^i{}_j$ where b,b' are constants, the counit axiom $(\mathrm{id}\otimes\epsilon)\Delta\delta_i=(\epsilon\otimes\mathrm{id})\Delta\delta_i=\delta_i$ tells us that $b=b'=0$ (and also fixed the first term as $\delta_{i,j}$). Now, Δ does not change the total degree so the total degree of

$$\Delta\delta_i=\sum_j\delta_{i-j}\otimes\delta_j+(g_1\otimes g_1)\sum_{j,k}\delta_j c'^i{}_{j+k}\delta_k$$

has to be $p-1$. The first term has total degree at most $<2p$ while the second term has leading power $(x^p\otimes x^p)\sum_{j,k}\delta_j c'^i_{j+k}\delta_k$, hence his second term must separately vanish. This means that we have a tensor product as coalgebras, so that A_1 appears as a subcoalgebra. These assertions can all be verified directly for small p as a check.

Clearly, these results are not changed modulo g_d as higher powers of g_1 were not involved. Hence $A_d=C_d\otimes_\chi A_1$ also by identifying the δ-functions. $\square$

The same form of result applies for $p=2$ but the formulae are different due to failure of the power-sum identities in this case; we cover this case later. Such cleft extensions may also be regarded as trivial quantum principal bundles or Hopf-Galois extensions of a certain trivial type, which are indeed classified by cocycles as explained in detail in [11]. Indeed, the above implies that they are of the quantum homogeneous space type with $\Delta_R=(\mathrm{id}\otimes\pi)\Delta$.

5. Noncommutative geometry of A_1 and A_2

In this section we study A_1, A_2 in more detail, focussing on their noncommutative differential geometry and Fourier theory in the case of A_1. There are no significant proofs in this section but we rather we develop a geometric point of view on our finite-dimensional algebras.

5.1. Geometry and Fourier transform on $\mathbb{F}_p(\mathbb{Z}/p\mathbb{Z})$. Here we focus on

$$A_1=\mathbb{F}_p[x]/(x^p-x).$$

This is isomorphic to $\mathbb{F}_p^p$ as a ring, so the functions on p points, and indeed we have already remarked in Lemma 4.5 that it is isomorphic to $\mathbb{F}_p(\mathbb{Z}/p\mathbb{Z})$ where the Kronecker delta-functions on the latter are mapped to the $\delta_i(x)$ for $i=0,\cdots,p-1$.

From the projector relations among the δ_i in A_1 and the evaluations $\delta_i(j) = \delta_{i,j}$ which follow from the definition of $\delta_i(x)$, it is easy to see that

$$\delta_i(x)f(x) = f(i)\delta_i(x), \quad \forall f(x) \in A_1. \tag{5.1}$$

Thus, if $f(x) \in A_1$ then the values $f(i)$ for $i \in \mathbb{Z}/p\mathbb{Z}$ provide the corresponding function on the group while conversely $f(x) = \sum_i \delta_i(x)f(i)$. We also recall that finite-dimensional Hopf algebras have unique translation-invariant integration up to normalisation. In our case we have up to normalisation

$$\int x^n = \begin{cases} 1 & n = p-1 \\ 0 & \text{else} \end{cases}, \tag{5.2}$$

which is equivalent via the isomorphism to $\int f = \sum_{i=0}^{p-1} f(i)$ for $f \in \mathbb{F}_p(\mathbb{Z}/p\mathbb{Z})$. From this or from the coefficient of x^{p-1} in δ_i being 1, we clearly have $\int \delta_i(x) = 1$.

Next, the dual Hopf algebra to $\mathbb{F}_p(\mathbb{Z}/p\mathbb{Z})$ is the group Hopf algebra of $\mathbb{Z}/p\mathbb{Z}$,

$$H_1 = \mathbb{F}_p\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p[t]/(t^p - 1), \quad \Delta t = t \otimes t$$

and has the unique normalised translation-invariant integral

$$\int t^n = \begin{cases} 1 & n = 0 \\ 0 & \text{else} \end{cases}. \tag{5.3}$$

We can view this Hopf algebra as dual to A_1 via the Hopf algebra duality pairing

$$A_1 \otimes H_1 \to \mathbb{F}_p, \quad \langle f(x), t^j \rangle = f(j), \quad \forall f(x) \in A_1. \tag{5.4}$$

As our Hopf algebras are finite-dimensional, there is necessarily a canonical coevaluation which we denote $\exp \in H_1 \otimes A_1$. We recall that for any finite dimensional Hopf algebra and specified integral on it, we have a Fourier transform $\mathcal{F} : A_1 \to H_1$ given by integration against one factor of exp, see [10] for an exposition. In our case it is immediate from (5.4) that $\exp = \sum_{i=0}^{p-1} t^i \otimes \delta_i(x)$ leading to the canonical Hopf algebra Fourier transform

$$\mathcal{F}(f) = \sum_{i=0}^{p-1} t^i f(i), \quad \mathcal{F}^{-1}(t^i) = \delta_i(x) \quad \forall f(x) \in A_1, \ i \in 0, \cdots, p-1. \tag{5.5}$$

Note that $(\int \otimes \int) \exp = 1$ so this is the 'volume' (analogous to 2π) in the general Fourier theory[10]. This completes our review of the standard Fourier theory on $\mathbb{Z}/p\mathbb{Z}$.

Next, in the same way as we have described the functions on the finite group as a quotient of the affine line $\mathbb{F}_p[x]$, namely A_1, we can do the adjoint thing on the dual side. Thus, $\mathbb{F}_p\mathbb{Z}/p\mathbb{Z}$ already looks like an algebraic group with group-like generator t but we can go further and write this as like the enveloping algebra of a Lie algebra with infinitesimal generator L, say.

Lemma 5.1. *Let $p > 2$.*

$$H_1 = \mathbb{F}_p[L]/(L^p)$$

as a Hopf algebra via the identification

$$t = e^L := \sum_{i=0}^{p-1} \frac{L^i}{i!}, \quad L = \ln(t) := -\sum_{i=1}^{p-1} \frac{t^i}{i} \in H_1^+,$$

in terms of a 'truncated exponential' $e^{(\ )}$ *and 'truncated logarithm'* $\ln(\ )$. *We have*

$$\int L^i = \begin{cases} 1 & \text{if } i = 0, p-1 \\ 0 & \text{else} \end{cases}$$

as equivalent to (5.3).

Proof. First we note that given $t^p = 1$ and L defined as stated, $L^p = -\sum_{i\neq 0} 1/i = 0$ and

$$iL = i\ln(t) = \ln(t^i)$$

for all integers i mod p. Conversely, given L with $L^p = 0$, we define $t = e^L$ and clearly $t^p = \sum_{i=0}^{p-1} (L^i)^p/i! = 1$. More generally it follows from $L^p = 0$ that

$$e^{iL}e^{jL} = \sum_{k=0}^{p-1}\sum_{s=0}^{p-1} \frac{i^k j^s}{k!s!} L^{k+s} = \sum_{m=0}^{p-1}\sum_{k=0}^{m} \binom{m}{k} \frac{L^m}{m!} i^k j^{m-k} = e^{(i+j)L}$$

which implies in particular that $t^i = e^{iL}$ and hence

$$\ln(e^L) = -\sum_{i=1}^{p-1} \frac{e^{iL}}{i} = -\sum_{i=1}^{p-1} \frac{1}{i}\sum_{j=0}^{p-1} i^j \frac{L^j}{j!} = -\sum_{j=0}^{p-1} \frac{L^j}{j!}\sum_{i=1}^{p-1} i^{j-1} = -L(p-1) = L$$

using the power-sum identity so that the sum over i contributes only for $j = 1$. Hence the algebra map $\mathbb{F}_p[L]/(L^p) \to H_1$ sending L to $\ln(t)$ is injective (by applying the algebra map going the other way that sends t to e^L) and hence by dimensions an isomorphism. Next, given L, for t to be group-like we need

$$\Delta L = \ln(e^L \otimes e^L), \quad \epsilon L = 0$$

With this coalgebra, the two Hopf algebras are isomorphic. We then convert over the integral as stated. □

We remark that the coproduct can be written more explicitly as

$$\Delta L = L \otimes 1 + 1 \otimes L - \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} L^i \otimes L^{p-i} \tag{5.6}$$

which makes sense as p divides the binomial coefficient. We have verified this by computer for small primes. The coproduct can also be written as a multiplicative correction

$$\Delta L = \left(1 - \sum_{i=1}^{p-2} a_i L^i \otimes L^{p-1-i}\right)(L \otimes 1 + 1 \otimes L) \tag{5.7}$$

where

$$a_i = \frac{\binom{p-1}{i} - (-1)^i}{p}$$

also make sense and obey $a_i = a_{p-1-i}$, $a_1 = 1$, $a_2 = (p-3)/2$ etc, with middle value $i = (p-1)/2$ giving the so-called 'swinging Wilson quotients'[17]. Also note that if we took L primitive then we would again have a Hopf algebra on $\mathbb{F}_p[L]/(L^p)$ but now dually paired with $\mathbb{F}_p[x]/(x^p)$. One could view this pair as a kind of linearisation of our Hopf algebras, no longer isomorphic to group algebras and group function algebras respectively. Compared to these, A_1 has a modified algebra relation and dually H_1 has a modified coproduct.

Corollary 5.2. *The coevaluation and the canonical Hopf algebra Fourier transform in terms of x, L take the form*

$$\exp = e^{L\otimes x} \in H_1 \otimes A_1$$

$$\mathcal{F} : A_1 \to H_1, \quad \mathcal{F}(f) = \int e^{L\otimes x} f(x), \quad \mathcal{F}^{-1}(f) = \int f(L) e^{-L\otimes x}.$$

Proof. We deduce this as

$$\exp = \sum_{i=0}^{p-1} (e^L)^i \otimes \delta_i(x) = \sum_{m=0}^{p-1} \frac{L^m}{m!} \otimes \sum_{i=0}^{p-1} \delta_i(x) i^m = e^{L\otimes x}$$

using $x^m = \sum_i \delta_i(x) i^m$. This in turn gives the Fourier transform as stated. In principle, one can also find from (5.4) that $\langle x^i, L\rangle = -\sum_{k=1}^{p-1} \frac{k^i}{k} = -\sum_{k=1}^{p-1} k^{i-1} = 1$ if $i = 1 \mod p-1$ and zero otherwise, to eventually find exp from this. $\square$

We now turn to differentials. We recall that the regular $d = 1$ monics are of the form $m = x - \mu$ for $\mu \in \mathbb{F}_p^*$ and necessarily descend to A_1. The classical calculus on $\mathbb{F}_p[x]$ given by $\mu = 0$, aside from not being regular, implies $\mathrm{d}x = \mathrm{d}x^p = 0$ and hence gives the zero calculus on A_1; we exclude it for this reason also.

Proposition 5.3. *For any $\mu \in \mathbb{F}_p^*$, the inherited calculus $\Omega(A_1)$ has $\Omega^i = 0$ for $i > 1$ and $\Omega^1 = A_1 \mathrm{d}x$ with relations*

$$[\mathrm{d}x, f] = \mu \mathrm{d}f$$

Moreover, $H^0(A_1) = \mathbb{F}_p$, $H^1(A_1) = \mathbb{F}_p$, spanned by 1 and $x^{p-1}\mathrm{d}x$ respectively.

Proof. The inherited calculus has the form stated, with $\mathrm{d}f = (\partial f)\mathrm{d}x$ where

$$\partial f = \frac{f(x+\mu) - f(x)}{\mu}, \quad \forall f \in A_1.$$

We already know H^0 from Corollary 4.1 but we can also see this directly. If $\partial f = 0$ then $f(x+\mu) = f(x)$. But $n\mu = \lambda \mod p$ has a solution n for all λ so by iteration $f(x+\lambda) = f(x)$ for all λ. By (5.1), $f(x)$ is determined by its values and we see that these are constant, hence f is a multiple of 1. For H^1, all 1-forms are closed and if $f\mathrm{d}x = \mathrm{d}h$ for some $h(x)$ then $f = \partial h = (h(x+\mu) - h(x))/\mu$. Clearly this cannot happen for f of degree $p-1$ since h would need degree p which is not possible. For smaller degree one can iteratively solve to find h by calculations that are the same as for the trivial 1st cohomology of $\mathbb{F}_p[x]$ with its 1-dimensional calculi. The calculus is manifestly inner with $\theta = \mu^{-1}\mathrm{d}x$. $\square$

Note that calculi on finite sets correspond to directed graphs and the above calculi correspond to the Cayley graph on $\mathbb{Z}/p\mathbb{Z}$ generated by singleton sets $\{\mu\} \subset \mathbb{Z}/p\mathbb{Z}$. The directed graph here has edges of the form $i \xrightarrow{\mu} i + \mu$ corresponding to a finite difference by a single step size μ on $\mathbb{Z}/p\mathbb{Z}$. It is easy to see from (5.5) by a change of variables (shifting by μ) in $\mathcal{F}$ that

$$\mathcal{F}\partial f = \left(\frac{t^\mu - 1}{\mu}\right)\mathcal{F},$$

which is the fundamental identity of Fourier theory from a practical point of view (that differentiation becomes multiplication by an element of the dual space coordinate algebra).

One can also ask on the dual side about the calculus on $H_1 = \mathbb{F}_p[t]/\langle t^p - 1\rangle$. Usually in the abelian case the problem reverts to calculi on the dual group but that is not possible in our case where the order of the group is the characteristic. However, it remains in any characteristic that translation invariant calculi on group algebras are classified by group 1-cocycles. In our case there is a natural choice in which the values of the cocycle are in $\mathbb{F}_p$ with trivial group action. In that case a group cocycle means a group homomorphism from $\mathbb{Z}/pZ$ to itself, which since p is prime can only be trivial or the identity. We therefore have a unique 1-dimensional calculus from this point of view, namely

$$\Omega^1(H_1) = H_1 v, \quad v = t^{-1}\mathrm{d}t, \quad \mathrm{d}t^i = it\, v, \quad [\mathrm{d}t, t] = 0$$

and $\Omega^2 = 0$. We see that this is the classical calculus on the algebraic circle $\mathbb{F}_p[t, t^{-1}]$ descended to H_1. Writing $\mathrm{d}f(t) = (\partial f)(t)v$, we have $\partial t^m = mt^m$, the degree operator. From (5.5) one easily finds

$$\mathcal{F}^{-1}\partial = x\mathcal{F}^{-1}$$

so that differentiation on H_1 again becomes multiplication in A_1 under Fourier transform. In terms of L, we have

$$v = e^{-L}\mathrm{d}e^{L} = e^{-L}\sum_{i=1}^{p-1}\frac{L^{i-1}}{(i-1)!}\mathrm{d}L = (1 + L^{p-1})\mathrm{d}L.$$

The calculus here descends from the classical calculus on $\mathbb{F}_p[L]$ but v and not $\mathrm{d}L$ is the basic translation-invariant differential form, because this property depends on the coproduct on L and this was modified from the additive one. Consequently, we have

$$\partial L = 1 - L^{p-1}, \quad \partial L^i = iL^{i-1}, \quad \forall i > 1$$

for the left-invariant derivative.

5.2. **Finite Riemannian geometry of A_2.** Here the Hopf algebra

$$A_2 = \mathbb{F}_2[x]/(x^{p^2} - x)$$

is $\mathbb{F}_p^p \times \mathbb{F}_{p^2}^{\frac{p(p-1)}{2}}$ as ring, so we do not have functions on a finite group. We focus on $p = 2$. The Hopf algebra Fourier theory can be computed as for A_1 but is not particularly illuminating, while the geometry is now more interesting.

First, we look at the algebraic structure. The fixed subalgebra B_2 then has dimension 3 according to Proposition 4.3, so this is the Boolean algebra on 3 elements.

Proposition 5.4. *A_2 is reduced and every element obeys $a^4 = a$ for all $a \in A_2$. Moreover, $A_2 \cong \mathbb{F}_2 x \oplus B_2$ as a vector space and contains B_2 as a subalgebra. The Hopf algebra structure of A_2 in this form is*

$$e_ie_j = e_i\delta_{ij}, \quad \sum_i e_i = 1, \quad x^2 = x + e_1, \quad e_1x = e_2 + x, \quad e_2x = e_2, \quad e_3x = 0$$

$$\epsilon x = \epsilon e_1 = \epsilon e_2 = 0, \quad \epsilon e_3 = 1, \quad \Delta x = x\otimes 1 + 1\otimes x, \quad \Delta e_1 = e_1\otimes 1 + 1\otimes e_1$$

$$\Delta e_2 = e_2\otimes 1 + 1\otimes e_2 + e_1\otimes x + x\otimes e_1, \quad \Delta e_3 = 1\otimes 1 + e_3\otimes 1 + 1\otimes e_3 + e_1\otimes x + x\otimes e_1$$

Proof. By writing $a = \alpha + \beta x + \gamma x^2 + \delta x^3$ we see that $a^2 = \alpha + \beta x^2 + \gamma x + \delta x^3$ and $a^4 = a$. This is also clear from the ring structure. The coefficients here are $0, 1$ and in this case $a^n = 0$ is not possible for any $n > 0$ unless $a = 0$. The boolean elements (meaning $a^2 = a$) are of the form $\alpha + \beta(x + x^2) + \delta x^3$ and these form a subalgebra. Here $1, e_1 = x^2 + x, e_3 = x^3 + 1$ obey $e_1 e_3 = 0$ so with $e_2 = 1 - e_1 - e_3$ are a complete set of idempotents for this subalgebra. So $A_2 \cong \mathbb{F}_2.x \oplus B_2$. We easily work out the Hopf algebra structure as stated. The antipode is the identity map. $\square$

We also know from Proposition 4.4 that A_2 is a cocycle extension, as is $\mathbb{F}_2[x]$, but the formulae were not covered before. Here

$$\delta_0(x) = 1 + x, \quad \delta_1(x) = x$$

and $\mathbb{F}_2[x]^\psi = \mathbb{F}_2[g_1]$ where $g_1 = x^2 + x$.

Corollary 5.5. *$\mathbb{F}_2[x] = \mathbb{F}_2[g_1] \otimes_\chi A_1$ where $\chi(\delta_i \otimes \delta_j) = \delta_{i,0}\delta_{j,0} + g_1$ so that*

$$\delta_0^2 = \delta_0 + g_1, \quad \delta_1^2 = \delta_1 + g_1, \quad \delta_0\delta_1 = g_1$$

hold in $\mathbb{F}_2[x]$. Here g_1 is primitive while A_1 appears as a subcoalgebra via identification of δ-functions. Moreover, $A_2 \cong A_1 \otimes_\chi A_1$.

Proof. Here it is easier to compute the delta-function products in $\mathbb{F}_2[x]$ giving the result stated and from which one may readily deduce the cocycle. The new ingredient is that $C_2 = \mathbb{F}_2[g_1]/(g_1^2 + g_1) \cong A_1$. $\square$

This says equivalently that A_2 is a cocycle extension $\mathbb{F}_2(\mathbb{Z}/2\mathbb{Z}) \otimes_\chi \mathbb{F}_2(\mathbb{Z}_2/2\mathbb{Z})$. The dual Hopf algebra is most easily computed from this. We now turn to the inherited structure of $\Omega(A_2)$ and its geometry.

Proposition 5.6. *The quotient $\Omega(A_2)$ is 2-dimensional in degree 1 with basis $\mathrm{d}x, \mu$ and relations*

$$[\mathrm{d}x, x] = \mu, \quad [\mu, x] = \mathrm{d}x + \mu$$

Moreover, the calculus is bicovariant, inner with $\theta = \mathrm{d}x + \mu$ and connected with Poincare duality in the sense

$$H^0(A_2) = \mathbb{F}_2, \quad H^1(A_2) = \mathbb{F}_2^2, \quad H^2(A_2) = \mathbb{F}_2.$$

These are spanned by $1, \{x\mathrm{d}x, \mu x^2\}$ and $x^3\mathrm{d}x \wedge \mu$ respectively.

Proof. We work in the $\mathbb{F}_4[x]$ description but we write $\mathrm{d}x = 1 \in \mathbb{F}_4[x]$ to avoid confusion with $1 \in A_2$. Thus $\mathrm{d}x.x = (x + \mu) = x.1 + \mu = \mathrm{d}x + \mu$. Similarly, $\mu x = (x + \mu)\mu = x\mu + (1 + \mu) = \mathrm{d}x + (x + 1)\mu$ as stated. These are the same basis and relations as for $\mathbb{F}_2[x]$, just adopted for our quotent algebra. Note also that the calculus necessarily remains inner with $\theta = \mu^{-1} = \mathrm{d}x + \mu \in \Omega^1$. It necessarily remains bicovariant, but this can also be verified directly. If we let d_n denote the restriction of the derivative to n-th component of the graded exterior algebra and write $\mathrm{d}_0 f = \partial_1 f \mathrm{d}x + \partial_2 f \mu$ for $f \in A$, then $\mathrm{d}_1(f_1\mathrm{d}x + f_2\mu) = (\partial_1 f_2 - \partial_2 f_1)\mathrm{d}x \wedge \mu$ for $f_1\mathrm{d}x + f_2\mu \in \Omega^1$. We already know H^0 by Corollary 4.1 but it is also easy to verify directly. Brute-force calculation shows that $\mathrm{Im}(\mathrm{d}_0)$ is spanned over $\mathbb{F}_2$ by $\{\mathrm{d}x, \mu, x^2\mathrm{d}x + x\mu\}$, $\ker(\mathrm{d}_1)$ is spanned by $\{\mathrm{d}x, \mu, x\mathrm{d}x, x^2\mathrm{d}x + x\mu, x^2\mu\}$, and finally that $\mathrm{Im}(\mathrm{d}_1)$ is spanned by $\{1, x, x^2\}\mathrm{d}x \wedge \mu$. The dimensions and bases of the cohomologies follow. Note that over $\mathbb{F}_2$ the exterior algebra is both commutative and anticommutative and symmetric combinations of the basic 1-forms are in the kernel of $\wedge$. □

By contrast, these features do not hold for the universal calculus on A_2 which is necessarily acyclic and hence cannot obey Poincaré duality, and has weaker relations

$$[\mathrm{d}x, x] = \mu, \quad [\mu, x] = \theta, \quad [\theta, x] = \mathrm{d}x$$

where θ is an independent 1-form. It is clear that $\Omega(A_2)$ in Proposition 5.6 is the quotient of this by the further relation $\theta = \mathrm{d}x + \mu$ which respects the coaction and therefore remains bicovariant. Finally, we turn to the Riemannian geometry of this inherited 2-dimensional calculus. Note that in noncommutative geometry a metric, when it exists, need not admit a 'Levi-Civita' connection (in the sense of torsion free and metric compatible) and if it does, the connection need not be unique. In the Hopf algebra case it is natural to consider left-invariant metrics, i.e. ones that are constant in the basic 1-forms, in our case $\mathrm{d}x, \mu$.

Proposition 5.7. *Central $\eta \in \Omega^1 \otimes_{A_2} \Omega^1$ with $\wedge(\eta) = 0$ have the form*

$$\eta = \alpha(\mu \otimes \mu + \theta \otimes \theta) + \beta(\mathrm{d}x \otimes \mathrm{d}x + \theta \otimes \theta), \quad \alpha, \beta \in A_2.$$

$\nabla \mathrm{d}x = \nabla\mu = 0$, $\sigma = \mathrm{flip}$ *on the generators is a torsion free metric compatible bimodule connection if $\alpha, \beta \in \mathbb{F}_2$. Each of the three nonzero metrics in this case has a second torsion free metric compatible bimodule connection:*

$$\text{(i)} \quad \eta = \mathrm{d}x \otimes \mathrm{d}x + \mu \otimes \mu; \quad \nabla \mathrm{d}x = \nabla\mu = \theta \otimes \theta$$
$$\sigma(\mathrm{d}x \otimes \mathrm{d}x) = \mu \otimes \mu, \quad \sigma(\mu \otimes \mu) = \mathrm{d}x \otimes \mathrm{d}x$$
$$\sigma(\mathrm{d}x \otimes \mu) = \mathrm{d}x \otimes \mu, \quad \sigma(\mu \otimes \mathrm{d}x) = \mu \otimes \mathrm{d}x$$
$$\text{(ii)} \quad \eta = \mathrm{d}x \otimes \mathrm{d}x + \theta \otimes \theta; \quad \nabla \mathrm{d}x = \mathrm{d}x \otimes \mu + \mu \otimes \mathrm{d}x, \quad \nabla\mu = \mu \otimes \mu$$
$$\sigma(\mathrm{d}x \otimes \mathrm{d}x) = \theta \otimes \theta, \quad \sigma(\mu \otimes \mu) = \mu \otimes \mu$$
$$\sigma(\mathrm{d}x \otimes \mu) = \mu \otimes \theta, \quad \sigma(\mu \otimes \mathrm{d}x) = \theta \otimes \mu$$
$$\text{(iii)} \quad \eta = \mu \otimes \mu + \theta \otimes \theta; \quad \nabla \mathrm{d}x = \mathrm{d}x \otimes \mathrm{d}x, \quad \nabla\mu = \mathrm{d}x \otimes \mu + \mu \otimes \mathrm{d}x$$
$$\sigma(\mathrm{d}x \otimes \mathrm{d}x) = \mathrm{d}x \otimes \mathrm{d}x, \quad \sigma(\mu \otimes \mu) = \theta \otimes \theta$$
$$\sigma(\mathrm{d}x \otimes \mu) = \theta \otimes \mathrm{d}x, \quad \sigma(\mu \otimes \mathrm{d}x) = \mathrm{d}x \otimes \theta$$

and all four connections are flat.

Proof. We let $f = \mathrm{d}x \otimes \mu + \mu \otimes \mathrm{d}x$ and $h = \mathrm{d}x \otimes \mathrm{d}x + \mu \otimes \mu$ and compute

$$[\mathrm{d}x \otimes \mathrm{d}x, x] = f = [\mu \otimes \mu, x], \quad [\mathrm{d}x \otimes \mu, x] = \mathrm{d}x \otimes \mu + h, \quad [\mu \otimes \mathrm{d}x, x] = \mu \otimes \mathrm{d}x + h$$

from which it follows that central combinations must be of the form

$$\eta = \alpha \mathrm{d}x \otimes \mathrm{d}x + \beta\mu \otimes \mu + (\alpha + \beta) f$$

which can also be written as stated.

Next, we look for bimodule connections. By [13], since the calculus is inner, these take the form $\nabla\omega = \theta \otimes \omega - \sigma(\omega \otimes \theta) + \alpha\omega$ for bimodule maps σ, α and for this to have zero torsion, we need (2.1). Thus, if we suppose

$$\alpha(\mathrm{d}x) = a\mathrm{d}x \otimes \mathrm{d}x + b\theta \otimes \theta + cf$$

then

$$\alpha(\mu) = \alpha([\mathrm{d}x, x]) = [\alpha(\mathrm{d}x), x] = (a+b+c)f$$

using $[f, x] = f$ and the above. Then

$$a\mathrm{d}x \otimes \mathrm{d}x + b\mu \otimes \mu + (a+b)f = \alpha(\mathrm{d}x + \mu) = \alpha([\mu, x]) = [\alpha(\mu), x] = (a+b+c)f$$

requires $a, b, c = 0$. Hence there are no non-zero module maps α with the required symmetry. We therefore drop the bimodule map α henceforth (so there is no conflict with our other notation α, β as the metric parameters). Similarly, let

$$\sigma(\mathrm{d}x \otimes \mathrm{d}x) = a\mathrm{d}x \otimes \mathrm{d}x + b\mu \otimes \mu + cf$$

$$\sigma(\mu \otimes \mu) = A\mathrm{d}x \otimes \mathrm{d}x + B\mu \otimes \mu + Cf$$

$$\sigma(\mathrm{d}x \otimes \mu) = a'\mathrm{d}x \otimes \mathrm{d}x + b'\mu \otimes \mu + c'f + \mu \otimes \mathrm{d}x$$

as dictated by $\wedge\sigma = -\wedge$. Then

$$\sigma(f) = \sigma([\mathrm{d}x \otimes \mathrm{d}x, x]) = [\sigma(\mathrm{d}x \otimes \mathrm{d}x), x] = (a+b+c)f = (A+B+C)f$$

(by $f = [\mu \otimes \mu, x]$ for the second version) so that

$$a + b + c = A + B + C.$$

Similarly $\sigma([\mathrm{d}x \otimes \mu, x]) = [\sigma(\mathrm{d}x \otimes \mu), x]$ gives us two further equations

$$a' = 1 + a + A, \quad b' = 1 + b + B$$

This leaves us parameters a, b, c, A, B, c' for σ with the required symmetry. Then writing $\sigma_\theta = \sigma(\ ,\theta)$ we have

$$\sigma_\theta(\mathrm{d}x) = (1+A)\mathrm{d}x \otimes \mathrm{d}x + (1+B)\mu \otimes \mu + (c+c')f + \mu \otimes \mathrm{d}x,$$

$$\sigma_\theta(\mu) = (1+a)\mathrm{d}x \otimes \mathrm{d}x + (1+b)\mu \otimes \mu + (A+B+c')f + \mu \otimes \mathrm{d}x$$

For simplicity we assume that all our functions are constants. Then

$$\nabla\mathrm{d}x = A\mathrm{d}x \otimes \mathrm{d}x + (1+B)\mu \otimes \mu + (c+c')f,$$

$$\nabla\mu = (1+a)\mathrm{d}x \otimes \mathrm{d}x + b\mu \otimes \mu + (1+A+B+c')f$$

and

$$\begin{aligned}(\mathrm{id} \otimes \sigma_\theta)\eta = {}& \mathrm{d}x^{\otimes 2}\left((\alpha(a+A) + \beta(1+a))\mathrm{d}x + (\alpha(A+B+c) + \beta(A+B+c'))\mu\right) \\ & + \mu^{\otimes 2}\left((\alpha(1+c+c') + \beta(A+B+c))\mathrm{d}x + (\alpha(1+B) + \beta(b+B))\mu\right) \\ & + \mathrm{d}x \otimes \mu\left((\alpha(A+B+c) + \beta(1+A+B+c'))\mathrm{d}x + (\alpha(b+B) + \beta(1+b))\mu\right) \\ & + \mu \otimes \mathrm{d}x\left((\alpha(1+A) + \beta(a+A))\mathrm{d}x + ((\alpha(c+c') + \beta(A+B+c))\mu\right)\end{aligned}$$

Applying $\sigma\otimes\mathrm{id}$ and equating to $\theta\otimes\eta$ so as to solve the metric compatibility equation (2.2) we obtain a system of quadratic equations for our 6 parameters. Over $\mathbb{F}_2$, we try all 64 parameter values for each of the three non-zero cases of α, β, finding two solutions in each case. These are the unique nontrivial connections stated and one common connection which is zero on the basic forms and for which σ flips the generators as is the case classically. One may then verify metric compatibility directly as a check. That all four connections have zero curvature is obvious for the trivial one and, otherwise for case (i)

$$R_\nabla \mathrm{d}x = (\mathrm{d} \otimes \mathrm{id} - \wedge(\mathrm{id} \otimes \nabla))\nabla\mathrm{d}x = -\wedge(\mathrm{id} \otimes \nabla)(\theta \otimes \theta) = -\theta \wedge \nabla\theta = 0$$

and $R_\nabla\mu$ is the same as $\nabla\mu = \nabla\mathrm{d}x$. For case (ii) we have

$$R_\nabla \mathrm{d}x = -\mathrm{d}x \wedge \nabla\mu - \mu \wedge \nabla\mathrm{d}x = -\mathrm{d}x \wedge \mu \otimes \mu - \mu \wedge \mathrm{d}x \otimes \mu - \mu \wedge \mu \otimes \mathrm{d}x = 0$$

and $R_\nabla \mu = -\mu \nabla \mu = -\mu \wedge \mu \otimes \mu = 0$. Case (iii) is similar.

□

The trivial connection here can still be nonzero since $\nabla(a\mathrm{d}x + b\mu) = \mathrm{d}a \otimes \mathrm{d}x + \mathrm{d}b \otimes \mu$ for all $a, b \in A_2$, and corresponds geometrically to what we might expect on an affine line. The other connections are more unexpected and it is remarkable that for each metric we find a unique nontrivial one. The existence of a second 'nonclassical' quantum Levi-Civita connection was also a feature in the concrete model in [1]. The general case of nonconstant α, β in Proposition 5.7 is much harder but can in principle be analysed in the same way with additional $\mathrm{d}\alpha, \mathrm{d}\beta$ terms entering.

References

[1] E.J. Beggs & S. Majid, Gravity induced from quantum spacetime, Class. Quantum. Grav. 31 (2014) 035020 (39pp)

[2] L. Carlitz, A theorem of Dickson on irreducible polynomials, Proc. AMS. 3 (1952) 693–700

[3] L. Carlitz, The Staudt-Clausen Theorem, Math. Mag. 34 (1961) 131–146.

[4] A. Connes, *Noncommutative Geometry*, Academic Press (1994).

[5] M. Dubois-Violette & T. Masson, On the first-order operators in bimodules, Lett. Math. Phys. 37 (1996) 467–474.

[6] M. Dubois-Violette & P.W. Michor, Connections on central bimodules in noncommutative differential geometry, J. Geom. Phys. 20 (1996) 218 –232

[7] S. Lang, *Algebra*, 3rd Ed. (1993) Addison-Wesley.

[8] S. Ling & C. Xing, *Coding Theory: A First Course*, Cambridge University Press (2004)

[9] S. Majid, *A Quantum Groups Primer*, L.M.S. Lect. Notes 292 (2002) 179 pp

[10] S. Majid, *Foundations of Quantum Group Theory*, Cambridge Univ Press (2000), paperback ed.

[11] S. Majid, Cross product quantisation, nonAbelian cohomology and twisting of Hopf algebras, in *Proc. Generalised Symmetries*, Clausthal, Germany, July, 1993. World Sci.

[12] S. Majid, Quantum geometry of field extensions, J. Math. Phys. 40 (1999) 2311-2323.

[13] S. Majid, Noncommutative Riemannian geometry of graphs, J. Geom. Phys. 69 (2013) 74–93

[14] A. Rojas-Leon, Exponential sums with large automorphism group, Contemp. Math. 566 (2012) 43–64

[15] F. Ruskey, C.R. Miers & J. Sadawa, The number of irreducibles and Lyndon words with a given trace, Siam. J. Discrete 14 (2001) 240–245

[16] P. Schauenburg, Hopf algebra extensions and monoidal categories, in *New Directions in Hopf Algebras*, MSRI publications 43 (2002) 321–381.

[17] Swinging Wilson quotients, entry https://oeis.org/A163210 (P. Luschny), in *The Online Encyclopedia of Integer Sequences*

Queen Mary, University of London, School of Mathematics, Mile End Rd, London E1 4NS, UK

E-mail address: `s.majid@qmul.ac.uk`