SKEW BRACES OF SQUAREFREE ORDER

ALI A. ALABDALI AND NIGEL P. BYOTT

Abstract. Let $n \geq 1$ be a squarefree integer, and let M, A be two groups of order n. Using our previous results on the enumeration of Hopf-Galois structures on Galois extensions of fields of squarefree degree, we determine the number of skew braces (up to isomorphism) with multiplicative group M and additive group A. As an application, we enumerate skew braces whose order is the product of three distinct primes, in particular proving a conjecture of Bardakov, Neshchadim and Yadav on the number of skew braces of order $2pq$ for primes $q > p \geq 3$.

1. Introduction

Since the seminal work of Drinfeld [Dri92] on quantum groups, there has been a great deal of interest in algebraic systems which give rise to set-theoretic solutions of the quantum Yang-Baxter equation (QYBE). Etingof, Schedler and Soloviev [ESS99] defined the structure group attached to a set-theoretic solution of QYBE, and studied many of its properties. Subsequently, Rump showed how set-theoretic solutions arise from cycle sets [Rum05] and radical rings [Rum07a], and in the latter paper he also introduced braces as a generalisation of radical rings. Braces give rise to nondegenerate involutive set-theoretic solutions of QYBE, and have recently been studied intensively [Bac15, CJO16, LV16, CGIS18]. Several generalisations of braces have been investigated, including skew braces [GV17], which give noninvolutive solutions to QYBE, and semi-braces [CCS17], which give degenerate solutions.

Another area of algebra in which radical rings have found application is the study of Hopf-Galois structures on field extensions. If L/K is a finite Galois extension of fields with Galois group Γ, then L/K may admit many Hopf-Galois structures, and these can be described in group-theoretic terms. In particular, the Hopf algebra H acting

Date: March 24, 2020.

2010 *Mathematics Subject Classification.* 16T25, 16Y99, 12F10.

Key words and phrases. Skew braces; quantum Yang-Baxter equation; groups of squarefree order.

on L/K in any Hopf-Galois structure is a twisted form of the group algebra $K[G]$, where G is a group acting regularly on Γ. The Hopf-Galois structures can then be partitioned according to the isomorphism type of G. We refer to the isomorphism type of G as the *type* of the Hopf-Galois structure. Using the connection found in [CDVS06] between radical rings and abelian regular subgroups of the affine group of a field, Featherstonhaugh, Caranti and Childs [FCC12] studied the possible abelian types of Hopf-Galois structures on an abelian extension of prime-power degree.

Given the role of radical rings in these two situations, it is perhaps not surprising that there should be a deep connection between braces and Hopf-Galois structures. This connection was first mentioned explicitly in [Bac16], and was clarified and extended to the setting of skew braces in the appendix to [SV18]. Several papers and preprints have exploited this connection [Chi18, Chi19, NZ19].

In this paper, we make further use of the connection between skew braces and Hopf-Galois structures in order to study skew braces of squarefree order. Given a squarefree number $n \geq 1$ and two groups M, A of order n, we determine the number $b(M, A)$ of skew braces $(B, +, *)$ (up to isomorphism) with multiplicative group $(B, *)$ isomorphic to M and additive group $(B, +)$ isomorphic to A. To do so, we build upon our work in [AB] where, for any two groups Γ, G of squarefree order n, we determined the number $e(\Gamma, G)$ of Hopf-Galois structures of type G on a Galois extension with Galois group Γ. The special case where Γ is cyclic was previously treated in [AB18]. In the final two sections of this paper, we give some examples, in particular treating in full the case where n is the product of three primes.

For comparison with our work here, we note that the braces with finite cyclic additive group are determined in [Rum07b], and the braces of order p^3 for p prime are classified in [Bac15]. The skew braces whose additive group is the Heisenberg group of order p^3 for $p > 3$ are enumerated in [NZ19]. Further results on skew braces of order p^3 can be found in [NZ18]. Computational results for the total number of skew braces of order n are given in the papers [GV17, Ven19, BNY] for most $n \leq 868$. Our results are consistent with these computations, and allow us to prove a formula conjectured in [BNY] for the number of skew braces of order $2pq$ for primes $q > p \geq 3$.

2. Statement of Main Result

Before stating our main result, we must first describe the groups of squarefree order. Specialising the characterisation in [MM84] of finite groups in which every Sylow subgroup is cyclic, we obtain the following classification, cf. [AB18, Lemma 3.2].

Lemma 2.1. *Let $n \geq 1$ be squarefree. Then any group of order n has the form*

$$G(d,e,k) = \langle \sigma, \tau \colon \sigma^e = \tau^d = 1, \tau\sigma\tau^{-1} = \sigma^k \rangle$$

where $n = de$, $\gcd(d,e) = 1$ and $\operatorname{ord}_e(k) = d$. Conversely, any choice of d, e and k satisfying these conditions gives a group $G(d,e,k)$ of order n. Moreover, two such groups $G(d,e,k)$ and $G(d',e',k')$ are isomorphic if and only if $d = d'$, $e = e'$, and k, k' generate the same cyclic subgroup of $\mathbb{Z}_e^\times$.

Here, for a natural number m, we write $\mathbb{Z}_m$ for the ring of integers modulo m, and $\mathbb{Z}_m^\times$ for its group of units. Also, for $a \in \mathbb{Z}$ with $\gcd(a,m) = 1$, we denote by $\operatorname{ord}_m(a)$ the order of a in $\mathbb{Z}_m^\times$.

We now fix a squarefree number n, and two groups of order n:

$$A = G(d,e,k), \qquad M = G(\delta, \epsilon, \kappa). \tag{2.1}$$

(Our notation is chosen to be consistent with [AB], except that A, M correspond respectively to G, Γ in that paper.) We then define

$$z = \gcd(k-1,e), \quad g = e/z, \quad \zeta = \gcd(\kappa - 1, \epsilon), \quad \gamma = \epsilon/\zeta. \tag{2.2}$$

Thus z, g depend only on A, and ζ, γ depend only on M. Note that we have

$$n = de = dgz = \delta\epsilon = \delta\gamma\zeta. \tag{2.3}$$

We also set

$$w = \varphi(\gcd(\delta, d)),$$

which depends on both A and M. Here φ is the Euler totient function.

We can now state our main result. Recall that $\omega(g)$ denotes the number of (distinct) prime factors of the squarefree integer g.

Theorem 2.2. *Let M and A be groups of squarefree order n. Then, with the above notation, the number $b(M,A)$ of isomorphism classes of skew braces with multiplicative group isomorphic to M and additive group isomorphic to A is given by*

$$b(M,A) = \begin{cases} 2^{\omega(g)} w & \text{if } \gamma \mid e, \\ 0 & \text{if } \gamma \nmid e. \end{cases}$$

3. Skew Braces and Hopf-Galois Structures

For the convenience of the reader, we review in this section the necessary background on skew braces and Hopf-Galois structures, emphasising the connection between the corresponding enumeration problems.

A skew left brace $(B,+,*)$ is a set B with two binary operations such that $(B,+)$ and $(B,*)$ are groups, and $a*(b+c)=(a*b)+(-a)+(a*c)$ for all a, b, $c \in B$, where $-a$ is the inverse of a under $+$. We call $(B,+)$ the additive group of B and $(B,*)$ the multiplicative group. If $(B,+)$ is abelian, then $(B,+,*)$ is a left brace. Right skew braces and right braces are defined analogously, but we will not need these concepts in this paper. We therefore omit the adjective "left" from now on.

An isomorphism between two skew braces is a bijection between their underlying sets which is an isomorphism of both the additive groups and the multiplicative groups. For groups M, A of the same order, we write $b(M,A)$ for the number of isomorphism types of skew braces $(B,+,*)$ with $(B,*)\cong M$ and $(B,+)\cong A$.

Let $(B,+,*)$ be a skew brace. There is a homomorphism of groups

$$\lambda : (B,*) \to \mathrm{Aut}(B,+), \qquad b \mapsto \lambda_b \text{ with } \lambda_b(a) = -b + b * a.$$

Thus $(B,*)$ acts on $(B,+)$. Moreover, the identity map on B induces a bijection $i : (B,*) \to (B,+)$ which satisfies the 1-cocycle identity with respect to this action:

$$i(b*c) = i(b) + \lambda_b(i(c)) \text{ for all } b, c \in B.$$

Now consider the holomorph $\mathrm{Hol}(B,+) = (B,+) \rtimes \mathrm{Aut}(B,+)$ of the group $(B,+)$. We view $\mathrm{Hol}(B,+)$ as a subgroup of the group $\mathrm{Perm}(B)$ of permutations of the underlying set B, with the normal subgroup $(B,+)$ of $\mathrm{Hol}(B,+)$ acting as left translations. The map $(i,\lambda) : (B,*) \to \mathrm{Hol}(B,+)$ is a group homomorphism whose image is regular on B. (Recall that a subgroup $G \subset \mathrm{Perm}(X)$ is regular on X if it is transitive and the stabiliser of any point in X is the trivial group. When G is finite, this implies that $|G| = |X|$.) Thus the skew brace $(B,+,*)$ gives rise to a regular embedding of $(B,*)$ into the holomorph of $(B,+)$.

We can reverse this construction: for abstract finite groups M and A, a regular embedding $\beta : M \to \mathrm{Hol}(A)$ gives rise to a homomorphism $\lambda : M \to \mathrm{Aut}(A)$, and so to an action of M on A, together with a bijective cocycle $i : M \to A$ with respect to this action. Letting $(B,*) = M$, and defining a new operation $+$ on B by pulling back the group operation of A via i, we obtain a skew brace $(B,+,*)$ with $(B,*)\cong M$ and $(B,+)\cong A$. We may compose β (on the right) with any element of $\mathrm{Aut}(M)$, and this does not change the isomorphism type of B. An automorphism ψ of A induces an automorphism of $\mathrm{Hol}(A)$, which is given by conjugation with ψ in $\mathrm{Hol}(A)$. Composing β (on the left) with this automorphism again does not change the isomorphism type of B. Thus $b(M, A)$ is just the number of $\mathrm{Aut}(A) \times \mathrm{Aut}(M)$-orbits of regular embeddings $M \to \mathrm{Hol}(A)$, where the action of $\mathrm{Aut}(M)$ on regular embeddings is by composition, and that of $\mathrm{Aut}(A)$ by conjugation. Since two regular embeddings β have the same image if and only if they are in the same $\mathrm{Aut}(M)$-orbit, $b(M, A)$ is also number of $\mathrm{Aut}(A)$-orbits of regular subgroups in $\mathrm{Hol}(A)$ isomorphic to M.

We note that the groups $\mathrm{Aut}(A)$ and $\mathrm{Aut}(M)$ each act without fixed points on the set of regular embeddings $\beta : M \to \mathrm{Hol}(A)$, but their product $\mathrm{Aut}(A) \times \mathrm{Aut}(M)$ does not. Thus the orbits of $\mathrm{Aut}(A) \times \mathrm{Aut}(M)$ on this set of regular embeddings, or, equivalently, the orbits of $\mathrm{Aut}(A)$ on the set of regular subgroups of $\mathrm{Hol}(A)$ isomorphic to M, are in general not all of the same size.

We now turn to Hopf-Galois structures. A Hopf-Galois structure on a finite extension of fields L/K consists of a cocommutative K-Hopf algebra H and an action of H on L making L/K into an H-Galois extension in the sense of Chase and Sweedler [CS69]. The motivating example is when L/K is a Galois extension in the classical sense, and H is the group algebra $H = K[\Gamma]$ for $\Gamma = \mathrm{Gal}(L/K)$, with the natural action of H on L. The Galois extension L/K may also admit other (non-classical) Hopf-Galois structures. Greither and Pareigis [GP87] showed that the Hopf-Galois structures on L/K correspond bijectively to the regular subgroups $G \subset \mathrm{Perm}(\Gamma)$ which are normalised by the group $\lambda(\Gamma)$ of left translations by Γ. This shows that the number of such Hopf-Galois structures can be obtained by a purely group-theoretic calculation. The Hopf algebra occurring in the Hopf-Galois structure given by the regular subgroup G is $L[G]^\Gamma$, the Hopf algebra of Γ-fixed points in the group algebra $L[G]$, where Γ acts simultaneously on L as field automorphisms and on $G \subset \mathrm{Perm}(\Gamma)$ as conjugation with left translations. We refer to the isomorphism type of G as the *type* of this Hopf-Galois structure. We write $e(\Gamma, G)$ for the number of Hopf-Galois structures of type G on a Galois extension L/K with $\mathrm{Gal}(L/K) \cong \Gamma$.

We change notation to facilitate comparison between the enumeration problems for skew braces and for Hopf-Galois structures. Let M and A be two abstract finite groups of the same order. Then $e(M, A)$ is the number of regular subgroups in $\mathrm{Perm}(M)$ isomorphic to A and normalised by $\lambda(M)$. Equivalently, $e(M, A)$ is the number of $\mathrm{Aut}(A)$-orbits of regular embeddings $\alpha : A \to \mathrm{Perm}(M)$ with image normalised by $\lambda(M)$. There is a canonical bijection between regular embeddings

$\alpha : A \to \mathrm{Perm}(M)$ and regular embeddings $\beta : M \to \mathrm{Perm}(A)$, under which $\alpha(A)$ is normalised by $\lambda(M)$ if and only if $\beta(M) \subset \mathrm{Hol}(A)$. Thus $e(M, A)$ is the number of $\mathrm{Aut}(A)$-orbits of regular embeddings $\beta : M \to \mathrm{Hol}(A)$. Since the $\mathrm{Aut}(M)$-orbits of such β correspond to the regular subgroups of $\mathrm{Hol}(A)$ isomorphic to M, we may in practice evaluate $e(M, A)$ by first determining the number $e'(M, A)$ of these subgroups. We then have

$$e(M, A) = \frac{|\mathrm{Aut}(M)|}{|\mathrm{Aut}(A)|}\, e'(M, A).$$

This is often simpler than working directly with regular subgroups of $\mathrm{Perm}(M)$, as $\mathrm{Hol}(A)$ is usually much smaller than $\mathrm{Perm}(M)$.

In summary, $b(M, A)$ is the number of $\mathrm{Aut}(A)$-orbits on the set of regular subgroups of $\mathrm{Hol}(A)$ isomorphic to M, whereas $e'(M, A)$ is just the number of such subgroups. Once we have determined all such subgroups, we can easily find the number $e(M, A)$ of Hopf-Galois structures, but, as the $\mathrm{Aut}(A)$-orbits on these subgroups can be of different sizes, obtaining the number $b(M, A)$ of skew braces may require significant further calculation.

Remark 3.1. For Galois extensions of squarefree degree, the formula for $e(\Gamma, G)$ we obtained in [AB, Theorem 2.2] is much more complex than the formula for the number of skew braces in Theorem 2.2 of this paper. This is because the number of Hopf-Galois structures depends in an intricate way on the interplay of the structures of the two groups Γ, G. We are not aware, however, of any approach to proving Theorem 2.2 of this paper which avoids the detailed analysis of regular subgroups at the heart of our enumeration of the Hopf-Galois structures.

4. Regular subgroups in Hol(A)

Let M and A be two groups of squarefree order n, as in Theorem 2.2. In this section, we recall some results from [AB], and in particular we determine in Lemma 4.4 explicit generators for all regular subgroups of $\mathrm{Hol}(A)$ isomorphic to M. We will keep to the notation of [AB] except that we write A, M in place of G, Γ.

From (2.1) and Lemma 2.1, we have the presentations

$$A = \langle \sigma, \tau \colon \sigma^e = \tau^d = 1, \tau\sigma\tau^{-1} = \sigma^k \rangle,$$

$$M = \langle s, t \colon s^\epsilon = t^\delta = 1, tst^{-1} = s^\kappa \rangle.$$

Recall that g, z, γ, ζ were defined in (2.2).

By [AB18, Lemma 4.1], $\mathrm{Aut}(A) \cong \mathbb{Z}_g \rtimes \mathbb{Z}_e^\times$ and is generated by the automorphism θ, and automorphisms ϕ_s for $s \in \mathbb{Z}_e^\times$ where

$$\theta(\sigma) = \sigma, \quad \theta(\tau) = \sigma^z\tau; \qquad \phi_s(\sigma) = \sigma^s, \quad \phi_s(\tau) = \tau.$$

We write elements of $\mathrm{Hol}(A) = A \rtimes \mathrm{Aut}(A)$ as $[x, \alpha]$, where $x \in A$ and $\alpha \in \mathrm{Aut}(A)$. An arbitrary element of $\mathrm{Hol}(A)$ therefore has the form $[\sigma^u\tau^f, \theta^v\phi_t]$ for $u \in \mathbb{Z}_g$, $f \in \mathbb{Z}_d$, $v \in \mathbb{Z}_g$ and $t \in \mathbb{Z}_e^\times$. The group operation in $\mathrm{Hol}(A)$, and the action of $\mathrm{Hol}(A)$ on A, are given by

$$[x, \alpha][y, \beta] = [x\alpha(y), \alpha\beta], \qquad [x, \alpha] \cdot y = x\alpha(y). \tag{4.1}$$

We modify the above presentation of M. Setting $X = s^\zeta$ and $Y = ts^\gamma$, we have the alternative presentation

$$\Gamma = \langle X, Y \colon X^\gamma = Y^{\zeta\delta} = 1, YXY^{-1} = X^\kappa\rangle. \tag{4.2}$$

Proposition 4.1. [AB, Proposition 5.2] *If* $\mathrm{Hol}(A)$ *contains a regular subgroup* $M^* \cong M$ *then* $\gamma \mid e$. *Moreover, if* X *and* Y *are generators of* M^* *satisfying the relations in (4.2) then the subgroup* $\langle X, Y^d\rangle$ *of* M *of order* e *acts regularly on the subset* $\{\sigma^m : m \in \mathbb{Z}\}$ *of* A.

If $\gamma \nmid e$ then Proposition 4.1, together with the discussion in §3, shows that there are no skew braces $(B, +, *)$ with $(B, *) \cong M$ and $(B, +) \cong A$. This already proves the second case of Theorem 2.2.

We can replace Y by some power Y^f to ensure that Y has the form $Y = [\sigma^u\tau, \theta^v\phi_t]$ (so τ occurs in Y with exponent 1), but in doing so we replace κ by κ^f. To allow for this, we consider the action of the group

$$\Delta := \{m \in \mathbb{Z}_\delta^\times : m \equiv 1 \pmod{\gcd(\delta, d)}\}$$

on the set

$$\mathcal{K} = \{\kappa^r : r \in \mathbb{Z}_\delta^\times\}.$$

The index of Δ in $\mathbb{Z}_\delta^\times$ is $w = \varphi(\gcd(\delta, d))$. We choose a system $\kappa_1, \ldots, \kappa_w$ of orbit representatives of Δ on $\mathcal{K}$.

Lemma 4.2. [AB, Lemma 5.5] *Let* $M^* \cong M$ *be a regular subgroup of* $\mathrm{Hol}(A)$. *Then there is a unique* h *with* $1 \leq h \leq w$ *such that* M^* *is generated by a pair of elements* X, Y *of the form*

$$X = [\sigma^a, \theta^c], \qquad Y = [\sigma^u\tau, \theta^v\phi_t]. \tag{4.3}$$

which satisfy the relations

$$X^\gamma = Y^{\zeta\delta} = 1, \qquad YXY^{-1} = X^{\kappa_h}. \tag{4.4}$$

Indeed, M^* *contains exactly* $\gamma\varphi(e)w/\varphi(\delta)$ *such pairs of generators.*

The relations in (4.4) are the same as those in (4.2), except that κ is replaced by one of the coset representatives κ_h. Lemma 4.2 shows that the regular subgroups of $\mathrm{Hol}(A)$ isomorphic to M fall into w disjoint families $\mathcal{F}_1, \ldots, \mathcal{F}_w$ corresponding to the orbits of Δ on $\mathcal{K}$.

Not every pair X, Y satisfying (4.3) and (4.4) generate a regular subgroup. To identify those which do, we let

$$\mathcal{N}_h \subset \mathbb{Z}_e^\times \times \mathbb{Z}_e \times \mathbb{Z}_g \times \mathbb{Z}_e \times \mathbb{Z}_g$$

be the set of quintuples (t, a, c, u, v) such that the corresponding elements X, Y satisfy (4.4) for the orbit representative κ_h and generate a *regular* subgroup $M^* = \langle X, Y \rangle \in \mathcal{F}_h$.

It follows from Lemma 4.2 that the number $e'(M, A)$ of regular subgroups of $\mathrm{Hol}(A)$ isomorphic to M is given by

$$e'(M, A) = \sum_{h=1}^{w} |\mathcal{F}_h| = \frac{\varphi(\delta)}{\gamma\varphi(e)w} \sum_{h=1}^{w} |\mathcal{N}_h|.$$

We recall from [AB, Lemma 4.3] a formula for powers of the element Y.

Lemma 4.3. *For Y as in (4.3) and $j \geq 0$, we have*

$$Y^j = [\sigma^{A(j)}\tau^j, \theta^{vS(t,j)}\phi_{tj}],$$

where $A(j) = uS(tk, j) + vzkT(k, t, j)$, with

$$S(m, j) = \sum_{i=0}^{j-1} m^i. \tag{4.5}$$

and

$$T(k, t, j) = \sum_{h=0}^{j-1} S(t, h)k^{h-1} \text{ for } j \geq 1, \qquad T(k, t, 0) = 0. \tag{4.6}$$

For each prime $q \mid e$ (respectively, $q \mid \epsilon$), we set $r_q = \mathrm{ord}_q(k)$ (respectively, $\rho_q = \mathrm{ord}_\epsilon(\kappa)$). We then divide the set of primes $q \mid e$ into six subsets (any of which may be empty) as follows.

$$P = \{\text{primes } q \mid \gcd(\gamma, z)\};$$

$$Q = \{\text{primes } q \mid \gcd(\zeta\delta, z)\};$$

$$R = \{\text{primes } q \mid \gcd(\gamma, g) : \rho_q \neq r_q\};$$

$$S = \{\text{primes } q \mid \gcd(\gamma, g) : \rho_q = r_q > 2\};$$

$$T = \{\text{primes } q \mid \gcd(\gamma, g) : \rho_q = r_q = 2\};$$

$$U = \{\text{primes } q \mid \gcd(\zeta\delta, g)\}.$$

Moreover, for each $h \in \{1, \ldots, w\}$, we define

$$S_h^+ = \{q \in S : \kappa_h \equiv k \pmod{q}\},$$
$$S_h^- = \{q \in S : \kappa_h \equiv k^{-1} \pmod{q}\},$$

and set

$$S_h = S_h^+ \cup S_h^-, \qquad S_h' = S \backslash S_h.$$

We also set

$$\lambda = z^{-1}(k-1) \in \mathbb{Z}_g^\times. \qquad \mu = k^{-1}z^{-1}(k-1) \in \mathbb{Z}_g^\times.$$

The following result is [AB, Lemma 6.12].

Lemma 4.4. *A quintuple $(t, a, c, u, v) \in \mathbb{Z}_e^\times \times \mathbb{Z}_e \times \mathbb{Z}_g \times \mathbb{Z}_e \times \mathbb{Z}_g$ belongs to $\mathcal{N}_h$ if and only if, for each prime $q \mid e$, its entries satisfy the conditions mod q shown in Table 1.*

Primes q	t	a	u	c	v
$q \in P$	κ	$\not\equiv 0$	arb.		
$q \in Q$	1	0	$\not\equiv 0$		
$q \in R \cup S_h'$	κ	$\not\equiv 0$	arb.	λa	arb.
	κk^{-1}	$\not\equiv 0$	arb.	0	arb.
$q \in S_h^+$	$\kappa k^{-1} \equiv 1$	$\not\equiv 0$	arb.	0	0
	κ	$\not\equiv 0$	arb.	λa	arb.
$q \in S_h^-$	κ	$\not\equiv 0$	arb.	λa	μu
	$\kappa k^{-1} \equiv \kappa^2$	$\not\equiv 0$	arb.	0	arb.
$q \in T$	$\kappa \equiv -1$	$\not\equiv 0$	arb.	λa	μu
	$\kappa k^{-1} \equiv 1$	$\not\equiv 0$	arb.	0	0
$q \in U$	1	0	arb.	0	$\not\equiv 0$
	k^{-1}	0	arb.	0	$\not\equiv \mu u$

Table 1. Conditions for membership of $\mathcal{N}_h$.

In Table 1 and the discussion below, we write κ in place of κ_h to simplify notation. Moreover, all congruences are modulo the relevant prime q unless otherwise indicated. The parameters t, a, u are defined mod e, and hence (via the Chinese Remainder Theorem) are determined by their residue classes at all primes $q \mid e$ (that is, all $q \in P \cup Q \cup R \cup S \cup T \cup U$). The parameters c and v are defined mod g, and hence are determined by their residue classes at only those $q \in R \cup S \cup T \cup U$. Thus the entries in Table 1 for c and v at primes $q \in P \cup Q$ are left blank.

To illustrate how to interpret Table 1, suppose that $q \in S_h^+$, so that $\kappa \equiv k$. There are two possibilities for t mod q. Either $t \equiv 1$, and then

$a \not\equiv 0$, $c \equiv v \equiv 0$, and u may be chosen arbitrarily, or else $t \equiv \kappa$, and again $a \not\equiv 0$ and u may be chosen arbitrarily, but now v may also be chosen arbitrarily and $c \equiv \lambda a$.

Finally, from [AB, Corollary 6.10, Proposition 6.11] we have the following congruence information on the exponents $A(j)$ in Lemma 4.3 when j is a multiple of d:

Lemma 4.5. *For $i \geq 0$, we have the following congruences mod q.*

(i) *If $q \in Q$ then $A(di) \equiv udi$.*

(ii) *If $q \in U$ with $t \equiv 1$ then*

$$A(di) \equiv \frac{vzdi}{k-1}.$$

(iii) *If $q \in U$ with $t \equiv k^{-1}$ then*

$$A(di) \equiv \frac{zk}{k-1}(v - \mu u)di.$$

(iv) *If $q \mid \gamma$ then $A(di) \equiv 0$ for all $i \equiv 0 \pmod{\gcd(\delta, e)}$.*

5. Counting Skew Braces

Lemma 4.4 enables us to find all regular subgroups of $\mathrm{Hol}(A)$ isomorphic to M. Indeed, given $h \in \{1, \ldots, w\}$ and a quintuple $(t, a, c, u, v) \in \mathcal{N}_h$, we have the corresponding regular subgroup $M^* = \langle X, Y \rangle$ where X, Y are defined in (4.3). By Lemma 4.2, every regular subgroup M^* arises this way from $\gamma\varphi(e)w/\varphi(\delta)$ quintuples in $\mathcal{N}_h$. The number $b(M, A)$ of skew braces with multiplicative group M and additive group A is the number of $\mathrm{Aut}(A)$-orbits of these regular subgroups, where $\mathrm{Aut}(A)$ acts on $\mathrm{Hol}(A)$ by conjugation.

Let $I_h(t, a, c, u, v)$ be the size of the orbit of the subgroup M^*. Then $I_h(t, a, c, u, v)$ is the index in $\mathrm{Aut}(A)$ of the stabiliser of M^*. To count the skew braces, we need to count the subgroup M^* with weight $I_h(t, a, c, u, v)^{-1}$. Thus we have the following formula for $b(M, A)$:

$$b(M, A) = \frac{\varphi(\delta)}{\gamma\varphi(e)w} \sum_{h=1}^{w} \sum_{(t,a,c,u,v) \in \mathcal{N}_h} \frac{1}{I_h(t, a, c, u, v)}. \tag{5.1}$$

It remains to determine $I_h(t, a, c, u, v)$. An element of $\mathrm{Aut}(A)$ has the form $\alpha = \theta^r \phi_s$ for $r \in \mathbb{Z}_g$ and $s \in \mathbb{Z}_e^\times$.

Lemma 5.1. *Suppose that $\gamma \mid e$, let $1 \leq h \leq w$, and let $M^* = \langle X, Y \rangle$ be the regular subgroup in* $\mathrm{Hol}(A)$ *corresponding to $(t, a, c, u, v) \in \mathcal{N}_h$ as above. Let $\alpha = \theta^r \phi_s \in \mathrm{Aut}(A)$. Then $\alpha M^* \alpha^{-1} = M^*$ in* $\mathrm{Hol}(A)$

if and only if there exist $i \in \mathbb{Z}_{\zeta\delta/d}$ and $j \in \mathbb{Z}_\gamma$ satisfying the following three conditions:

$$t^{di} \equiv 1 \pmod{e}; \tag{5.2}$$

$$cj + vS(t, di) \equiv v(s-1) - (t-1)r \pmod{g}; \tag{5.3}$$

$$aj + A(di) \equiv (u - zv)(s-1) + ztr \pmod{e}. \tag{5.4}$$

Moreover, (5.2) is equivalent to

$$i \equiv 0 \pmod{\gcd(\delta, e)}; \tag{5.5}$$

Proof. Using (4.1) to calculate in $\mathrm{Hol}(A)$, we have

$$\begin{aligned} \alpha X \alpha^{-1} &= [1, \theta^r \phi_s][\sigma^a, \theta^c][1, \phi_s^{-1}\theta^{-r}] \\ &= [\sigma^{as}, \theta^r \phi_s \theta^c \phi_s^{-1} \theta^{-r}] \\ &= [\sigma^{as}, \theta^{r+cs-r}] \\ &= X^s, \end{aligned}$$

and

$$\begin{aligned} \alpha Y \alpha^{-1} &= [1, \theta^r \phi_s][\sigma^u \tau, \theta^v \phi_t][1, \phi_s^{-1}\theta^{-r}] \\ &= [\sigma^{us+rz}\tau, \theta^r \phi_s \theta^v \phi_t \phi_s^{-1} \theta^{-r}] \\ &= [\sigma^{us+rz}\tau, \theta^{r+vs} \phi_t \theta^{-r}] \\ &= [\sigma^{us+rz}\tau, \theta^{r+vs-rt} \phi_t]. \end{aligned}$$

Also

$$Y^{-1} = [\phi_t^{-1}\theta^{-v}(\tau^{-1}\sigma^{-u}), \phi_t^{-1}\theta^{-v}],$$

so that

$$\begin{aligned} (\alpha Y \alpha^{-1}) Y^{-1} &= [\sigma^{us+rz}\tau, \theta^{r+vs-rt}\phi_t][\phi_t^{-1}\theta^{-v}(\tau^{-1}\sigma^{-u}), \phi_t^{-1}\theta^{-v}] \\ &= [\sigma^{us+rz}\tau \cdot \theta^{r+vs-rt-v}(\tau^{-1}\sigma^{-u}), \theta^{r+vs-rt-v}] \\ &= [\sigma^{us+rz}\tau \cdot \tau^{-1}\sigma^{-z(r+vs-rt-v)-u}, \theta^{r+vs-rt-v}] \end{aligned}$$

Thus

$$(\alpha Y \alpha^{-1}) Y^{-1} = [\sigma^{(u-zv)(s-1)+ztr}, \theta^{v(s-1)-r(t-1)}]. \tag{5.6}$$

We then have

$$\begin{aligned} \alpha M^* \alpha^{-1} = M^* &\Leftrightarrow \langle X^s, \alpha Y \alpha^{-1} \rangle = \langle X, Y \rangle \\ &\Leftrightarrow \langle X, \alpha Y \alpha^{-1} \rangle = \langle X, Y \rangle \\ &\Leftrightarrow (\alpha Y \alpha^{-1}) Y^{-1} \in \langle X, Y \rangle. \end{aligned}$$

But $(\alpha Y \alpha^{-1})Y^{-1}$ does not involve τ, so this element takes 1_A to σ^m for some $m \in \mathbb{Z}$. Since M^* is regular on A, it follows from Proposition 4.1 that

$$\alpha M^* \alpha^{-1} = M^* \Leftrightarrow (\alpha Y \alpha^{-1})Y^{-1} \in \langle X, Y^d \rangle.$$

Thus $\alpha M^* \alpha^{-1} = M^*$ if and only if there exist $i \in \mathbb{Z}_{\zeta\delta/d}$ and $j \in \mathbb{Z}_\gamma$ such that

$$(\alpha Y \alpha^{-1})Y^{-1} = X^j Y^{di} = [\sigma^{aj+A(di)}, \theta^{cj+vS(t,di)}\phi_{t^{di}}],$$

where the last equality comes from Lemma 4.3. Comparing with (5.6), this is equivalent to (5.2), (5.3) and (5.4).

We show that (5.2) is equivalent to (5.5). Suppose (5.2) holds. Since $k^d \equiv 1 \pmod{e}$, it follows from the values of t shown in Table 1 that $\kappa^{di} \equiv 1 \pmod{\gamma}$. As $\kappa \equiv 1 \pmod{\zeta}$, we then have $\kappa^{di} \equiv 1 \pmod{\epsilon}$, so $\delta \mid di$. Thus $p \mid i$ for every prime $p \mid \delta$ with $p \nmid d$. This implies (5.5). Conversely, if (5.5) holds then $\kappa^{di} \equiv 1 \pmod{\epsilon}$. Since also $k^{di} \equiv 1 \pmod{e}$, it follows from Table 1 that (5.2) holds. □

To calculate $I_h(t, a, c, u, v)$, we must find the proportion of pairs r, s for which (5.3)–(5.5) can be solved for i and j. If (5.5) holds then, at each prime $q \mid e$, (5.3) and (5.4) reduce to congruences which are linear in i (as well as in j, r and s). Indeed, using Lemma 4.5, we can replace $A(di)$ by a multiple of di (by 0 if $q \mid \gamma$). Also, as $t^{di} \equiv 1$, we have $S(t, di) \equiv 0$ if $t \not\equiv 1$ and $S(t, di) \equiv di$ if $t \equiv 1$. By the Chinese Remainder Theorem, this linearity, together with the obvious linearity of (5.5), means that solutions to (5.3)–(5.5) exist if and only if solutions exist mod q for each prime $q \mid e$, and that the existence of solutions mod q depends only on the residue classes of r, s mod q. Thus we can decompose $I_h(t, a, c, u, v)$ into contributions for each q:

$$I_h(t, a, c, u, v) = \prod_{q \mid e} I_q.$$

(We suppress the dependence of I_q on h and (t, a, c, u, v) from the notation.)

In order to calculate the I_q, we need to subdivide the set of primes $q \mid e$ more finely than we did in Lemma 4.4. We define

$$Q' = \{\text{primes } q \mid \gcd(\delta, z)\},$$
$$Q'' = \{\text{primes } q \mid \gcd(\zeta, z)\},$$
$$U' = \{\text{primes } q \mid \gcd(\delta, g)\},$$
$$U'' = \{\text{primes } q \mid \gcd(\zeta, g)\},$$
$$S^+_{h,1} = \{q \in S^+_h : t \equiv 1\},$$
$$S^+_{h,2} = \{q \in S^+_h : t \equiv \kappa\},$$

$$S^-_{h,1} = \{q \in S^-_h : t \equiv \kappa\},$$
$$S^-_{h,2} = \{q \in S^-_h : t \equiv \kappa k^{-1}\}.$$

Thus we have (disjoint) unions

$$Q = Q' \cup Q'', \qquad U = U' \cup U'', \qquad S^+_h = S^+_{h,1} \cup S^+_{h,2}, \qquad S^-_h = S^-_{h,1} \cup S^-_{h,2}.$$

Lemma 5.2. *Let M^* correspond to $(t, a, c, u, v) \in \mathcal{N}_h$ as before. For each prime $q \mid e$, the q-part I_q of the index of the stabiliser of M^* in* Aut(A) *is as shown in Table 2. (For ease of reference, we repeat in Table 2 the possible values of t, a, c, u, v mod q as given in Table 1. We also show the number N_q of such quintuples mod q.)*

Primes q	t	a	u	c	v	Index I_q	Number N_q
$q \in P$	κ	$\not\equiv 0$	arb.			1	$q(q-1)$
$q \in Q'$	1	0	$\not\equiv 0$			$q-1$	$q-1$
$q \in Q''$	1	0	$\not\equiv 0$			1	$q-1$
$q \in R \cup S'_h$	κ κk^{-1}	$\not\equiv 0$ $\not\equiv 0$	arb. arb.	λa 0	arb. arb.	q	$2q^2(q-1)$
$q \in S^+_{h,1}$	$\kappa k^{-1} \equiv 1$	$\not\equiv 0$	arb.	0	0	1	$q(q-1)$
$q \in S^+_{h,2}$	κ	$\not\equiv 0$	arb.	λa	arb.	q	$q^2(q-1)$
$q \in S^-_{h,1}$	κ	$\not\equiv 0$	arb.	λa	μu	1	$q(q-1)$
$q \in S^-_{h,2}$	κk^{-1}	$\not\equiv 0$	arb.	0	arb.	q	$q^2(q-1)$
$q \in T$	$\kappa \equiv -1$ $\kappa k^{-1} \equiv 1$	$\not\equiv 0$ $\not\equiv 0$	arb. arb.	λa 0	μa 0	1	$2q(q-1)$
$q \in U'$	1 k^{-1}	0 0	arb. arb.	0 0	$\not\equiv 0$ $\not\equiv \mu u$	$q(q-1)$	$2q(q-1)$
$q \in U''$	1 k^{-1}	0 0	arb. arb.	0 0	$\not\equiv 0$ $\not\equiv \mu u$	q	$2q(q-1)$

Table 2. q-parts of index of stabiliser and number of quintuples.

Proof. We suppose that (5.5) holds. Then, by Lemma 4.5(iv), $A(di) \equiv 0 \pmod{q}$ for each $q \mid \gamma$. To find I_q for a given q, we divide the number of pairs $r \in \mathbb{Z}_q$, $s \in \mathbb{Z}_q^\times$ by the number of such pairs for which (5.3), (5.4) can be solved mod q for i, j with i also satisfying (5.5). We omit any of r, i, j which are not defined mod q. We distinguish four cases.

(i) Suppose $q \mid z$. Then (5.3) gives no condition at q and (5.4) becomes

$$aj + A(di) \equiv u(s-1). \tag{5.7}$$

Also, r is not determined mod q.

If $q \mid \gamma$, so $q \in P$, then $a \not\equiv 0$ and $A(di) \equiv 0$ for any choice of i mod q. We can choose s arbitrarily and solve (5.7) for j. Thus the existence of solutions i, j mod q imposes no restriction on s, and $I_q = 1$ for $q \in P$.

If $q \mid \zeta\delta$, so $q \in Q$, then $t \equiv 1$, $a \equiv 0$ and $u \not\equiv 0$, and $A(di) \equiv udi$. Then (5.7) becomes $di \equiv s - 1$. When $q \mid \delta$, so $q \in Q'$, we have $i \equiv 0$ by (5.5) so $s \equiv 1$. Thus only one of the $q - 1$ possibilities for $s \in \mathbb{Z}_q^\times$ can occur, and $I_q = q - 1$ for $q \in Q'$. If $q \mid \zeta$, so $q \in Q''$, there is no restriction on i from (5.5), so we may choose s arbitrarily and solve for i. Thus $I_q = 1$ for $q \in Q''$.

(ii) If $q \mid \gcd(\gamma, g)$, so that $q \in R \cup S \cup T$, then $a \not\equiv 0$ and $A(di) \equiv 0$. We consider two subcases.

(a) If $t \equiv \kappa$ then $c \equiv \lambda a \not\equiv 0$ and $S(t, di) \equiv 0$. Thus (5.3) and (5.4) become

$$\lambda aj \equiv v(s-1) - (t-1)r, \tag{5.8}$$

$$aj \equiv (u - zv)(s-1) + ztr, \tag{5.9}$$

so that

$$\lambda(u - zv)(s-1) + \lambda ztr \equiv \lambda aj \equiv v(s-1) - (t-1)r.$$

Using $1 + \lambda z = k$, this simplifies to

$$(kv - \lambda u)(s-1) \equiv (kt-1)r. \tag{5.10}$$

It suffices to determine when (5.9) and (5.10) have solutions.

If $t \equiv \kappa \not\equiv k^{-1}$, we may choose s arbitrarily, and then r (and j) are determined. Thus $I_q = q$. This accounts for $q \in R \cup S'_h$ with $t \equiv \kappa$, and also for $q \in S^+_{h,2}$.

If however $t \equiv \kappa \equiv k^{-1}$, so either $q \in S^-_{h,1}$ or $q \in T$ with $t \equiv -1$, then $v \equiv \mu u$, and, since $k\mu = \lambda$, (5.10) gives no condition on r and s. We may then choose r, s arbitrarily and solve (5.9) for j, so $I_q = 1$ in these cases.

(b) If $t \equiv \kappa k^{-1}$ then $c \equiv 0$ and (5.3) becomes

$$vS(t, di) \equiv v(s-1) - (t-1)r, \tag{5.11}$$

while (5.4) again simplifies to (5.9).

If $t \equiv \kappa k^{-1} \not\equiv 1$, then $S(t, di) \equiv 0$ and (5.11) determines r once s is chosen. We can then solve (5.9) for j. Thus $I_q = q$. This accounts for the $q \in R \cup S'_h$ with $t \equiv \kappa k^{-1}$ and also for $q \in S^-_{h,2}$.

If however $t \equiv \kappa k^{-1} \equiv 1$, so $q \in S^+_{h,1}$ or $q \in T$ with $t \equiv 1$, then $v = 0$, so (5.11) gives no restriction on r and s, and (5.9) can be solved for j. Hence $I_q = 1$.

(iii) Let $q \mid g$ and $q \mid \delta$, so $q \in U'$. Then $i \equiv 0$ by (5.5), and $a \equiv c \equiv 0$. Thus (5.3) and (5.4) become

$$v(s-1) \equiv (t-1)r, \qquad (u-zv)(s-1)+ztr \equiv 0. \tag{5.12}$$

We have two possibilities for t. If $t \equiv 1$ then $v \not\equiv 0$. Then the first congruence of (5.12) forces $s \equiv 1$ and the second $r \equiv 0$. If $t \equiv k^{-1}$, we have $v \not\equiv \mu u$. Eliminating r between the two congruences of (5.12) and simplifying, we obtain

$$(v-\mu u)(s-1) \equiv 0,$$

so that again $s \equiv 1$ and $r \equiv 0$. Thus, in both cases, we get $I_q = q(q-1)$.
(iv) Let $q \mid g$ and $q \mid \zeta$, so $q \in U''$. Then $a \equiv c \equiv 0$, and (5.3) and (5.4) become

$$vS(t,di) \equiv v(s-1)+(t-1)r, \qquad A(di) \equiv (u-zv)(s-1)+ztr. \tag{5.13}$$

Again, there are two possibilities for t. If $t \equiv 1$ then $v \not\equiv 0$, $S(t,di) \equiv di$ and $A(di) \equiv vzdi/(k-1)$. Thus we have

$$vdi \equiv v(s-1), \qquad \frac{vzdi}{k-1} \equiv (u-zv)(s-1)+zr.$$

Given s, we may solve the first of these for i, and r is determined by second. Thus $I_q = q$. If $t \equiv k^{-1}$ then $v \not\equiv \mu u$, and we have

$$v(s-1)+(t-1)r \equiv 0, \qquad A(di) \equiv (u-zv)(s-1)+ztr.$$

Again, we may choose s and the first congruence determines r. The second can then be solved for i. Thus again $I_q = q$. □

In order to sum over all quintuples $(t,a,c,u,v) \in \mathcal{N}_h$, we must allow for the fact that the partition of S_h^+ as $S_{h,1}^+ \cup S_{h,2}^+$ depends on the choice of quintuple: in choosing a quintuple, we must in particular choose which primes $q \in S_h^+$ to allocate to $S_{h,1}^+$, so that $t \equiv 1 \pmod q$, and which to allocate to $S_{h,2}^+$, so that $t \equiv \kappa k^{-1} \pmod q$. Similarly, we must choose how to allocate the primes $q \in S_h^-$ between $S_{h,1}^-$ and $S_{h,2}^-$. The remaining sets of primes listed in Table 2, viz. P, Q', Q'', R, S_h', T, U', U'', are all independent of the choice of quintuple.

Let $I \subseteq S_h^+$ and $J \subseteq S_h^-$. The number $N_h(I,J)$ of quintuples $(t,a,c,u,v) \in \mathcal{N}_h$ with $S_{h,1}^+ = I$ and $S_{h,1}^- = J$ is then given by

$$N_h(I,J) = \prod_{q \mid e} N_q,$$

where the N_q are as in Table 2, and with $N_q = q(q-1)$ if $q \in I$ or $q \in J$, and $N_q = q^2(q-1)$ if $q \in S_h^+ \backslash I$ or $q \in S_h^- \backslash J$. For all these quintuples, $I_h(t,a,c,u,v)$ takes the same value. Denoting this value by $I_h(I,J)$, we may rewrite (5.1) as

$$b(M,A) = \frac{\varphi(\delta)}{\gamma\varphi(e)w} \sum_{h=1}^{w} \sum_{I,J} \frac{N_h(I,J)}{I_h(I,J)}, \tag{5.14}$$

where

$$\begin{aligned}
\frac{N_h(I,J)}{I_h(I,J)} &= \prod_{q|e} \frac{N_q}{I_q} \\
&= \left(\prod_{q\in P} q(q-1)\right)\left(\prod_{q\in Q''}(q-1)\right)\left(\prod_{q\in R\cup S'_h\cup T} 2q(q-1)\right) \\
&\qquad \times \left(\prod_{q\in S_h^+\cup S_h^-} q(q-1)\right)\left(\prod_{q\in U'} 2\right)\left(\prod_{q\in U''} 2(q-1)\right) \\
&= \left(\prod_{q\in P\cup R\cup S\cup T} q(q-1)\right)\left(\prod_{q\in Q''\cup U''}(q-1)\right)\left(\prod_{q\in R\cup S'_h\cup T\cup U} 2\right) \\
&= \left(\prod_{q|\gamma} q(q-1)\right)\left(\prod_{q|\gcd(\zeta,e)}(q-1)\right)\left[\left(\prod_{q|g} 2\right)\left(\prod_{q\in S_h^+\cup S'_h} 2^{-1}\right)\right] \\
&= (\gamma\varphi(\gamma))\varphi(\gcd(\zeta,e))\left[2^{\omega(g)}2^{-|S_h^+\cup S_h^-|}\right].
\end{aligned}$$

This expression is independent of I and J since $N_q/I_q = q(q-1)$ for all $q \in S_h^+ \cup S_h^-$. As there are $2^{|S_h^+|}$ possible sets I, and $2^{|S_h^-|}$ possible sets J, summing over I and J introduces a factor $2^{|S_h^+\cup S_h^-|}$. Thus we have

$$\begin{aligned}
b(M,A) &= \frac{\varphi(\delta)}{\gamma\varphi(e)w} \sum_{h=1}^{w} \gamma\varphi(\gamma)\varphi(\gcd(\zeta,e))2^{\omega(g)} \\
&= \frac{\varphi(\delta)}{\gamma\varphi(e)w} \cdot w \cdot \gamma\varphi(\gamma)\varphi(\gcd(\zeta,e))2^{\omega(g)}.
\end{aligned}$$

Recalling (2.3), that $\gamma \mid e$, and that γ, ζ and δ are pairwise coprime, we have

$$\varphi(e) = \varphi(\gamma)\varphi(\gcd(\zeta,e))\varphi(\gcd(\delta,e)),$$

so the previous expression simplifies to

$$\begin{aligned} b(M,A) &= \frac{2^{\omega(g)}\varphi(\delta)}{\varphi(\gcd(\delta,e))} \\ &= \frac{2^{\omega(g)}\varphi(\gcd(\delta,e))\varphi(\gcd(\delta,d))}{\varphi(\gcd(\delta,e))} \\ &= 2^{\omega(g)}w. \end{aligned}$$

This completes the proof of Theorem 2.2.

6. An example where n has 7 prime factors

In [AB, §8], we considered four groups of order

$$n = 2\cdot 3\cdot 7\cdot 43\cdot 127\cdot 211\cdot 337 = 16\ 309\ 243\ 734,$$

each with

$$g = 43\cdot 127\cdot 211\cdot 337.$$

The values of d, z and the r_q for primes $q \mid g$ are as shown in Table 3. (We omit the values of k.)

	r_{43}	r_{127}	r_{211}	r_{337}	d	z
G_1	2	3	7	21	42	1
G_2	2	3	7	21	42	1
G_3	42	21	14	7	42	1
G_4	2	7	7	14	14	3

Table 3. Parameters for some groups of order n.

No two of these groups are isomorphic. Although the parameters shown in Table 3 are the same for G_1 and G_2, the (omitted) values of k are different and do not generate the same subgroup of $\mathbb{Z}_e^\times$. In [AB], we took $\Gamma = G_1$ and, for $1 \le i \le 4$, we calculated the number $e(\Gamma, G_i)$ of Hopf-Galois structures of type G_i on a Galois extension with Galois group isomorphic to Γ. We obtained a different answer for each i. In particular $e(G_1, G_1) \neq e(G_1, G_2)$, since the formula in [AB, Theorem 2.2] for the number of Hopf-Galois structures depends on the sets $S_h = S_h^+ \cup S_h^-$ and not just on the r_q.

When we calculate the number of skew braces $b(G_i, G_j)$, the non-isomorphic groups G_1, G_2, G_3 behave identically, since the formula in Theorem 2.2 of this paper only depends on the parameters g, d, γ and δ. In all these cases we have $\gamma = g$, so that $\gamma \mid e$. If i, $j \in \{1,2,3\}$, we have $d = \delta = 42$ and $w = 12$, whereas if $i = 4$ or $j = 4$ then $\gcd(\delta, d) = 14$ and $w = 6$. We can then read off from Theorem 2.2 that

$$b(G_i, G_j) = \begin{cases} 192 & \text{if } i, j \in \{1, 2, 3\}, \\ 96 & \text{if } i = 4 \text{ or } j = 4. \end{cases}$$

7. Special Cases

In this final section, we use Theorem 2.2 to calculate $b(M, A)$ for the various special cases considered in [AB, §9], and we compare our results to the computational results in [Ven19, BNY]. Throughout this section, $A = G(d, e, k)$ and $M = G(\delta, \epsilon, \kappa)$ are two groups of squarefree order $n = de = \delta\epsilon$, and g, z, γ, ζ, w are as defined before the statement of Theorem 2.2.

7.1. When M or A is cyclic or dihedral.

Corollary 7.1.

(i) *If M is cyclic and A is an arbitrary group of order n, then $b(M, A) = 2^{\omega(g)}$.*

(ii) *If A is cyclic and M is an arbitrary group of order n, then $b(M, A) = 1$.*

(iii) *If M is dihedral of order $n = 2m$ with m odd and squarefree, and A is an arbitrary group of order n, then*

$$b(M, A) = \begin{cases} 2^{\omega(g)} & \textit{if } d = 1 \textit{ or } 2, \\ 0 & \textit{if } d > 2 \end{cases}.$$

(iv) *If A is dihedral of order $n = 2m$ with m odd and squarefree, and M is an arbitrary group of order n, then $b(M, A) = 2^{\omega(m)}$.*

Proof. (i) We have $\gamma = 1$ so $w = 1$ and $b(M, A) = 2^{\omega(g)}w = 2^{\omega(g)}$.
(ii) We have $d = g = 1$, and $e = n$ so $\gamma \mid e$. Again, $w = 1$. Thus $b(M, A) = 1$.
(iii) We have $\delta = 2$ and $\gamma = m$. If $d > 2$ then $\gamma \nmid e$, so $b(M, A) = 0$. If $d \leq 2$ then $w = 1$ and $b(M, A) = 2^{\omega(g)}$.
(iv) We have $d = 2$, $g = m$ and $z = 1$. As $2 \nmid \gamma$ (cf. [AB, Remark 6.1]), we necessarily have $\gamma \mid e$. Again $w = 1$, so $b(M, A) = 2^{\omega(m)}$. □

Remark 7.2. In [Rum07b], Rump determines all braces whose multiplicative group is a finite cyclic group (not necessarily of squarefree order). Since he treats only braces, not skew braces, the additive group is always abelian. As any abelian group of squarefree order is necessarily cyclic, the only case covered by both Rump's result and ours is when M and A are both cyclic of squarefree order, so $b(M, A) = 1$.

7.2. **When n is the product of two primes.** Let $n = pq$ for prime numbers $p > q$. If $p \not\equiv 1 \pmod{q}$ then any group of order pq is cyclic and $b(M, A) = 1$ by Corollary 7.1(i). We therefore suppose that $p \equiv 1 \pmod{q}$. There are then two groups of order n, the cyclic group C_n (for which $g = d = 1$ and $z = pq$) and the nonabelian group $C_p \rtimes C_q$ (for which $g = p$, $d = q$, $z = 1$). We easily obtain the values of $b(M, A)$ from Theorem 2.2.

	$A = C_n$	$A = C_p \rtimes C_q$
$M = C_n$	1	2
$M = C_p \rtimes C_q$	1	$2(q-1)$

Table 4. Skew braces for two primes.

Corollary 7.3. *If $n = pq$ where p, q are primes with $p \equiv 1 \pmod{q}$, and M, A are groups of order pq, then the number $b(M, A)$ of skew braces with multiplicative group M and additive group A is as shown in Table 4. In particular, there are in total $2q + 2$ skew braces of order pq.*

Remark 7.4. This case was recently considered by Acri and Bonatto [AB20], and our results agree with theirs.

7.3. **When n is the product of three primes.** Let $n = p_1p_2p_3$ where $p_1 < p_2 < p_3$ are primes. Subject to certain congruence conditions between p_1, p_2 and p_3, there are 6 possible factorisations $n = dgz$ which give rise to groups of order n. We label these factorisations 1–6 as in Table 5. The last column shows the number of isomorphism types of group for each factorisation, as explained in [AB, §9.3].

Applying Theorem 2.2 to each combination of M and A, we obtain the following result:

Factorisation	d	g	z	Condition	# groups
1	1	1	$p_1p_2p_3$		1
2	p_1	p_2	p_3	$p_2 \equiv 1 \pmod{p_1}$	1
3	p_1	p_3	p_2	$p_3 \equiv 1 \pmod{p_1}$	1
4	p_1	p_2p_3	1	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	$p_1 - 1$
5	p_2	p_3	p_1	$p_3 \equiv 1 \pmod{p_2}$	1
6	p_1p_2	p_3	1	$p_3 \equiv 1 \pmod{p_1p_2}$	1

Table 5. Isomorphism types for groups of order $n = p_1p_2p_3$.

$\downarrow M \quad A \rightarrow$	1	2	3	4	5	6
1	1	2	2	4	2	2
2	1	$2(p_1-1)$	$2(p_1-1)$	$4(p_1-1)$	0	0
3	1	$2(p_1-1)$	$2(p_1-1)$	$4(p_1-1)$	2	$2(p_1-1)$
4	1	$2(p_1-1)$	$2(p_1-1)$	$4(p_1-1)$	0	0
5	1	2	2	4	$2(p_2-1)$	$2(p_2-1)$
6	1	$2(p_1-1)$	$2(p_1-1)$	$4(p_1-1)$	$2(p_2-1)$	$2(p_1-1)(p_2-1)$

TABLE 6. Numbers of skew braces for $n = p_1p_2p_3$.

Theorem 7.5. *Let $n = p_1p_2p_3$, where p_1, p_2, p_3 are primes satisfying the conditions $p_i \equiv 1 \pmod{p_j}$ for $i > j$. Let M and A be groups of order n. Then the number $b(M, A)$ of skew braces with multiplicative group M and additive group A is as shown in Table 6, where the rows (respectively, columns) correspond to the factorisations of n giving rise to M (respectively A) as in Table 5.*

Remark 7.6. One can easily obtain analogous results when the congruences $p_i \equiv 1 \pmod{p_j}$ do not all hold, simply by omitting from Table 6 the rows and columns for which the necessary congruences (as shown in Table 5) are not satisfied.

Corollary 7.7. *Let $n = p_1p_2p_3$ be as in Theorem 7.5.*

(i) *For any group M of order n, the number $b(M, \cdot)$ of skew braces (up to isomorphism) with multiplicative group M is as shown in Table 7.*

(ii) *For any group A of order n, the number $b(\cdot, A)$ of skew braces (up to isomorphism) with additive group A is as shown in Table 8.*

(iii) *The total number of skew braces of order n (up to isomorphism) is*

$$4p_1^3 + 4p_1^2 + 2p_1p_2 + p_1 + 4p_2 + 4.$$

(The rows in Tables 7, 8 correspond the factorisations of n giving M or A, as in Table 5.)

Proof. For each factorisation for M, the values of $b(M, \cdot)$ are obtained by adding the entries $b(M, A)$ in the corresponding row of Table 6, where the entry for A with Factorisation 4 is multiplied by $p_1 - 1$ since there are $p_1 - 1$ isomorphism types. The values of $b(\cdot, A)$ are obtained similarly from the columns of Table 6. The total number of skew braces

Factorisation for M	$b(M, \cdot)$
1	$4p_1 + 5$
2	$4p_1^2 - 4p_1 + 1$
3	$4p_1^2 - 2p_1 + 1$
4	$4p_1^2 - 4p_1 + 1$
5	$4p_1 + 4p_2 - 3$
6	$4p_1^2 + 2p_1p_2 - 6p_1 + 1$

Table 7. Number of skew braces with multiplicative group M.

Factorisation for A	$b(\cdot, A)$
1	$p_1 + 4$
2	$2p_1^2 + 2p_1$
3	$2p_1^2 + 2p_1$
4	$4p_1^2 + 4p_1$
5	$4p_2$
6	$2p_1p_2$

Table 8. Number of skew braces with additive group A.

of order n is obtained by adding the values of $b(M, \cdot)$, or of $b(\cdot, A)$, again with the value for Factorisation 4 multiplied by $p_1 - 1$. □

7.4. **Comparison with computational results.** For $n \geq 1$, let $b(n)$ (respectively, $s(n)$) be the number of braces (respectively, skew braces) of order n, up to isomorphism. If b is squarefree, the additive group of every brace of order n is cyclic, so by Corollary 7.1(ii), $b(n)$ is just the number of isomorphism classes of groups of order n. In particular, if $b(n) = 1$ then every group of order n is cyclic and $s(n) = 1$ as well; this holds for example if n is prime.

Results of computer calculations of $b(n)$ for most $n \leq 120$ and of $s(n)$ for all $n \leq 30$ are given in [GV17, Tables 5.3, 5.1]. These tables were extended to most $n \leq 168$ in [Ven19, Table 2.2] and extended again, using an improved algorithm, in [BNY]. The papers [Ven19] and [BNY] together give $b(n)$ and $s(n)$ for all $n \leq 868$ except for certain multiples of 2^4 and 3^4. On the basis of this wealth of numerical evidence, the authors of [BNY] formulate several conjectures on $b(n)$ and $s(n)$ for values of n with prime factorisations of particular forms. We now show how one of these conjectures follows from §7.3.

Theorem 7.8 ([BNY], Conjecture 4.4)**.** *Let p and q be prime numbers such that $q > p \geq 3$. Then*

$$b(2pq) = \begin{cases} 4 & \text{if } p \nmid (q-1) \\ 6 & \text{if } p \mid (q-1) \end{cases}$$

and

$$s(2pq) = \begin{cases} 36 & \text{if } p \nmid (q-1) \\ 8p+54 & \text{if } p \mid (q-1). \end{cases}$$

Proof. In the notation of §7.3, we have $p_1 = 2$, $p_2 = p$, $p_3 = q$ and $n = 2pq$. (Note that, in contrast to §7.2, we now have $q > p$ for consistency with the notation of [BNY].)

First suppose that $p \nmid (q-1)$, so $p_2 \equiv p_3 \equiv 1 \pmod{p_1}$ but $p_3 \not\equiv 1 \pmod{p_2}$. Thus only Factorisations 1–4 in Table 5 occur. Moreover, as $p_1 - 1 = 1$, each of these corresponds to a single isomorphism class. Hence there are 4 isomorphism classes of groups of order n, so $b(n) = 4$. To find $s(n)$, delete from Table 6 the rows and columns for Factorisations 5 and 6 and add all the remaining entries in the body of the table. Again noting that $p_1 - 1 = 1$, this gives $s(n) = 36$.

Now suppose that $p \mid (q-1)$, so $p_2 \equiv p_3 \equiv 1 \pmod{p_1}$ and $p_3 \not\equiv 1 \pmod{p_2}$. All 6 factorisations in Table 5 now occur, so $b(n) = 6$. Taking $p_1 = 2$, $p_2 = p$ in the formula of Corollary 7.7(iii) gives $s(n) = 8p + 54$. □

Remark 7.9. In a similar way, we can use the results of §7.2, §7.3, together with the above observation that $b(n) = s(n) = 1$ when n is prime, to calculate $b(n)$ and $s(n)$ for all squarefree $n \leq 868$ except for the 12 values $n = 210$, 330, 390, 462, 510, 546, 570, 690, 714, 770, 798, 858 (each of which is the product of 4 primes). We obtain the same values as in [Ven19, BNY] with one exception: [Ven19, Table 2.2] erroneously records $s(57)$ as 2, rather than 8.

References

[AB] Ali A. Alabdali and Nigel P. Byott, *Hopf-Galois structures of squarefree degree*, Preprint, arXiv:1910.07811.

[AB18] ———, *Counting Hopf-Galois structures on cyclic field extensions of squarefree degree*, J. Algebra **493** (2018), 1–19. MR 3715201

[AB20] E. Acri and M. Bonatto, *Skew braces of size pq*, Communications in Algebra (2020), to appear.

[Bac15] David Bachiller, *Classification of braces of order p^3*, J. Pure Appl. Algebra **219** (2015), no. 8, 3568–3603. MR 3320237

[Bac16] ———, *Counterexample to a conjecture about braces*, J. Algebra **453** (2016), 160–176. MR 3465351

[BNY] Valeriy G. Bardakov, Mikhail V. Neshchadim, and Manoj K. Yadav, *Computing skew left braces of small orders*, Internat. J. Algebra Comput., to appear.

[CCS17] Francesco Catino, Ilaria Colazzo, and Paola Stefanelli, *Semi-braces and the Yang-Baxter equation*, J. Algebra **483** (2017), 163–187. MR 3649817

[CDVS06] A. Caranti, F. Dalla Volta, and M. Sala, *Abelian regular subgroups of the affine group and radical rings*, Publ. Math. Debrecen **69** (2006), no. 3, 297–308. MR 2273982

[CGIS18] Ferran Cedó, Tatiana Gateva-Ivanova, and Agata Smoktunowicz, *Braces and symmetric groups with special conditions*, J. Pure Appl. Algebra **222** (2018), no. 12, 3877–3890. MR 3818285

[Chi18] Lindsay N. Childs, *Skew braces and the Galois correspondence for Hopf Galois structures*, J. Algebra **511** (2018), 270–291. MR 3834774

[Chi19] ———, *Bi-skew braces and Hopf Galois structures*, New York J. Math. **25** (2019), 574–588. MR 3982254

[CJO16] Ferran Cedó, Eric Jespers, and Jan Okniński, *Nilpotent groups of class three and braces*, Publ. Mat. **60** (2016), no. 1, 55–79. MR 3447734

[CS69] Stephen U. Chase and Moss E. Sweedler, *Hopf algebras and Galois theory*, Lecture Notes in Mathematics, Vol. 97, Springer-Verlag, Berlin-New York, 1969. MR 0260724

[Dri92] V. G. Drinfeld, *On some unsolved problems in quantum group theory*, Quantum groups (Leningrad, 1990), Lecture Notes in Math., vol. 1510, Springer, Berlin, 1992, pp. 1–8. MR 1183474

[ESS99] Pavel Etingof, Travis Schedler, and Alexandre Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. **100** (1999), no. 2, 169–209. MR 1722951

[FCC12] S. C. Featherstonhaugh, A. Caranti, and L. N. Childs, *Abelian Hopf Galois structures on prime-power Galois field extensions*, Trans. Amer. Math. Soc. **364** (2012), no. 7, 3675–3684. MR 2901229

[GP87] Cornelius Greither and Bodo Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), no. 1, 239–258. MR 878476

[GV17] L. Guarnieri and L. Vendramin, *Skew braces and the Yang-Baxter equation*, Math. Comp. **86** (2017), no. 307, 2519–2534. MR 3647970

[LV16] Victoria Lebed and Leandro Vendramin, *Cohomology and extensions of braces*, Pacific J. Math. **284** (2016), no. 1, 191–212. MR 3530867

[MM84] M. Ram Murty and V. Kumar Murty, *On groups of squarefree order*, Math. Ann. **267** (1984), no. 3, 299–309. MR 738255

[NZ18] Kayvan Nejabati Zenouz, *On Hopf-Galois structures and skew braces of order p^3*, Ph.D. thesis, University of Exeter, 2018.

[NZ19] ———, *Skew braces and Hopf-Galois structures of Heisenberg type*, J. Algebra **524** (2019), 187–225. MR 3905210

[Rum05] Wolfgang Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation*, Adv. Math. **193** (2005), no. 1, 40–55. MR 2132760

[Rum07a] ———, *Braces, radical rings, and the quantum Yang-Baxter equation*, J. Algebra **307** (2007), no. 1, 153–170. MR 2278047

[Rum07b] ———, *Classification of cyclic braces*, J. Pure Appl. Algebra **209** (2007), no. 3, 671–685. MR 2298848

[SV18] Agata Smoktunowicz and Leandro Vendramin, *On skew braces (with an appendix by N. Byott and L. Vendramin)*, J. Comb. Algebra **2** (2018), no. 1, 47–86. MR 3763907

[Ven19] Leandro Vendramin, *Problems on skew left braces*, Adv. Group Theory Appl. **7** (2019), 15–37. MR 3974481

(A. Alabdali) Department of Mathematics, College of Education for Pure Science, University of Mosul, Mosul, Iraq.
Email address: `ali.alabdali@uomosul.edu.iq`

(N. Byott) Department of Mathematics, College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter EX4 4QF U.K.
Email address: `N.P.Byott@exeter.ac.uk`