

**ENTROPY, CHARACTER THEORY AND
CENTRALITY OF FINITE QUASIGROUPS**

By

Jonathan D.H. Smith

IMA Preprint Series # 416

April 1988

ENTROPY, CHARACTER THEORY AND CENTRALITY OF FINITE QUASIGROUPS

JONATHAN D.H. SMITH*

Abstract. The paper introduces concepts of entropy and asymptotic entropy for finite quasigroups. A quasigroup is abelian if and only if its entropy is maximal. It is a 3-quasigroup if and only if its asymptotic entropy is maximal.

1. Introduction. Let (X, S, μ) be a probability space with probability measure μ defined on the σ -field S . A (finite) partition $\xi = \{C_1, \dots, C_s\}$ of (X, S, μ) is a set of pairwise disjoint elements of S whose union is X . The entropy of the partition is

$$(1.1) \quad H(\xi) = - \sum_{i=1}^s \mu(C_i) \log \mu(C_i),$$

where the logarithms are taken to an appropriate fixed base (usually 2, 10, or e), and where $\mu(C_i) \log \mu(C_i) = 0$ if $\mu(C_i) = 0$. The entropy $H(\xi)$ satisfies the inequality

$$(1.2) \quad 0 \leq H(\xi) \leq \log s,$$

in which equality obtains on the left if and only if $\mu(C_i) = 1$ for some i , and equality obtains on the right if and only if $\mu(C_i) = 1/s$ for each i [CS, §10.6]. A second finite partition $\eta = \{D_1, \dots, D_t\}$ of (X, S, μ) is said to be a refinement of ξ , written $\xi \leq \eta$, if each D_j in η is contained in some C_i in ξ . Then

$$(1.3) \quad \xi \leq \eta \Rightarrow H(\xi) \leq H(\eta),$$

equality holding only if each D_j in η differs from \emptyset or some C_i in ξ by a set of measure 0. The concept of entropy in this form originated in information theory, and subsequently played an important role in ergodic theory [CS, Ch. 10]. It is also closely related to the classical entropy concept of statistical mechanics.

The intention of the current paper is to initiate the use of the entropy concept in combinatorial character theory. The probability spaces (X, S, μ) appearing will be finite sets X , on which the σ -field S is just the power set 2^X , and the measure $\mu(A)$ of a subset A of X is just the ratio $|A|/|X|$ of the cardinalities. To begin with, consider the case of a finite group G , partitioned by its set ξ of conjugacy classes. This partition associates an entropy $H(\xi)$ or $H(G)$ to each finite group G . Since a group has all its conjugacy classes being singletons precisely when it is abelian, the inequality (1.2) (together with its cases of equality) gives the following

*Department of Mathematics, Iowa State University, Ames, Iowa 50011, USA

PROPOSITION 1.1. Amongst all groups G of given finite order n , those of maximal entropy $\log n$ are precisely the abelian groups.

This paper is almost exclusively concerned with the maximisation of entropy. Nevertheless, in the opposite direction it is natural to make the following conjecture.

CONJECTURE 1.2. Let n be the order of a finite simple group G . Then $H(G)$ is a minimum for the set of entropies of groups of order n .

Now recall that a *quasigroup* Q or (Q, \cdot) is a set Q equipped with a binary multiplication denoted by \cdot or juxtaposition, for which knowledge of any two of x, y , or z in the equation $x \cdot y = z$ specifies the third uniquely. The *multiplication group* G or $\text{Mlt } Q$ of Q is the subgroup of the group $Q!$ of all bijections $Q \rightarrow Q$ generated by all the bijections $L(y) : Q \rightarrow Q; x \mapsto yx$ and $R(y) : Q \rightarrow Q; x \mapsto xy$ as y ranges over Q . The (*quasigroup*) *conjugacy classes* [J1, §2] of the quasigroup Q are the orbits under the diagonal action of G on $Q \times Q$. If Q is a group with identity element 1 and centre $Z(Q)$, then the multiplication group G of Q is given by the exact sequence

$$(1.4) \quad 1 \longrightarrow Z(Q) \xrightarrow{\Delta} Q \times Q \xrightarrow{T} G \longrightarrow 1,$$

in which $\Delta : Z(Q) \rightarrow Q \times Q; z \mapsto (z, z)$ and $T : Q \times Q \rightarrow G; (x, y) \mapsto L(x)^{-1}R(y)$. Each quasigroup conjugacy class C of Q is of the form $\{(x, cx) | c \in C', x \in Q\}$, for some (group) conjugacy class $C' = [C \cap (\{1\} \times Q)]\pi_2$. Thus one may define the entropy of a finite non-empty quasigroup in the following way as a generalization of the group entropy defined above.

DEFINITION 1.3. Let Q be a finite, non-empty quasigroup, with the set $\xi = \{C_1, \dots, C_s\}$ of quasigroup conjugacy classes. Then the *entropy* $H(Q)$ of Q is the entropy $H(\xi)$ of the partition ξ of $Q \times Q$.

A quasigroup is said to be *abelian* if it is both commutative and associative, and thus is either empty or an abelian group. A *rank 2 quasigroup* Q is a quasigroup with just 2 conjugacy classes, namely the relations of equality and inequality on Q [J2, §5]. One then has the following strengthening of Proposition 1.1.

PROPOSITION 1.4. Let Q be a quasigroup of finite positive order n . Then

$$\log n - (1 - n^{-1}) \log(n - 1) \leq H(Q) \leq \log n.$$

Equality obtains on the right if and only if Q is abelian. Equality obtains on the left if and only if Q has rank 2.

Proof. Since G is transitive on Q , there are at most n conjugacy classes. The right hand inequality follows by (1.2). Equality obtains there if and only if each element of Q

has trivial stabiliser in G . This is equivalent to Q being abelian (cf. [CP, Th. III. 6.4], [J3, Prop. 7.2(a)]). The left hand inequality follows by (1.3). \square

Quasigroups are interesting because they cover a much broader range of phenomena than groups, while still retaining many of the structural features that groups possess, possibly recast into new form. One example of such retention is the conjugacy class partition and its associated entropy. Another example is furnished by quasigroup character tables, which have much of the structure of group character tables [J1] - [J5], [S2, Ch.5]. In particular, quasigroup character tables encode the sizes of the conjugacy classes, so that the entropy of a quasigroup may be calculated from its character table. Indeed, the calculation is direct and numerical, merely involving rational functions and logarithms with character table entries [J1, Cor. 3.5][S2, Cor. 542]. This is why the present applications of the entropy concept are attributed above to combinatorial character theory.

An illustration of the phenomenal richness of quasigroups is provided by the way the abelian/non-abelian dichotomy for groups becomes a trichotomy for quasigroups. A quasigroup Q is said to be a $\mathfrak{3}$ -quasigroup if the diagonal $\hat{Q} = \{(x, x) | x \in Q\}$ is a normal subquasigroup of Q^2 , i.e. a congruence class for a congruence on Q^2 . Groups that are $\mathfrak{3}$ -quasigroups are just abelian groups. A quasigroup Q with an *identity* element 1 such that $1x = x = x1$ for all x in Q is called a *loop*. Then even loops that are $\mathfrak{3}$ -quasigroups are just abelian groups. But in the full generality of quasigroups, a wide gap opens up between abelian groups and $\mathfrak{3}$ -quasigroups. Many interesting examples, such as the projective geometries discussed in Example 2.2 below, are found in this gap. In general neither the entropy of a quasigroup Q , nor even its character table, can specify whether Q lies in the class $\mathfrak{3}$ or not [J3, Prop. 7.7 (b)]. The character table of Q^2 does determine whether Q lies in $\mathfrak{3}$ or not [J4, Th. 3.1], but the determination is indirect and non-numerical, requiring analysis of the structure of the congruence lattice of Q^2 (which by [J1, Th. 3.6] is encoded in the character table). One is thus led to the second main definition.

DEFINITION 1.5. For a finite non-empty quasigroup Q , the *asymptotic entropy* $h(Q)$ is defined to be $\limsup_{m \rightarrow \infty} \frac{1}{m} H(Q^m)$.

By Proposition 1.4, $0 < H(Q^m) \leq \log |Q^m|$, whence

$$(1.5) \quad 0 \leq h(Q) \leq \log |Q|.$$

If Q is a loop, $H(Q^m) = mH(Q)$, so the asymptotic entropy $h(Q)$ just coincides with the entropy $H(Q)$ of Definition 1.3. If Q is a non-abelian $\mathfrak{3}$ -quasigroup of positive order n , however, the sequence $H(Q^m)$ exhibits interesting behaviour. It begins by staying well below $m \log n$, and then tends asymptotically to $(m \log n) - k$ for a constant k . Thus $h(Q) = \log n$. From the point of view of hierarchical information theory [BCL][S3], the sequence of powers Q^m may be used to model processes in which a large degree of self-organisation is built up initially, only to decay ultimately to a small residual level. The entropic behaviour of

$\mathfrak{3}$ -quasigroups is examined in Section 2. The third section then presents the main Theorem 3.1 characterising finite non-empty $\mathfrak{3}$ -quasigroups Q by the property $h(Q) = \log |Q|$. This gives a direct, numerical method of recognising $\mathfrak{3}$ -quasigroups Q from character tables, at the price of requiring the character tables of the sequence of powers Q^m rather than just the character table of Q^2 needed for the indirect, non-numerical method of [J4, Th. 3.1]. Together, Proposition 1.4 and Theorem 3.1 show how the two numerical invariants, the entropy $H(Q)$ and asymptotic entropy $h(Q)$, may be used to locate quasigroups within the trichotomy. The entropy $H(Q)$ is maximised (at $\log |Q|$) precisely by the abelian quasigroups, while the asymptotic entropy $h(Q)$ is maximised (again at $\log |Q|$) precisely by the $\mathfrak{3}$ -quasigroups. The projective geometries $P(q)$ of Example 2.2 have the curious property of simultaneously minimising the entropy and maximising the asymptotic entropy.

2. Entropy of $\mathfrak{3}$ -quasigroups. The class $\mathfrak{3}$ was defined in the introduction to be the class of quasigroups Q for which the diagonal \hat{Q} is a normal subquasigroup of Q^2 , i.e. a congruence class for a congruence on Q^2 . In order to examine the entropic behaviour of $\mathfrak{3}$ -quasigroups, it is convenient to use the alternative characterisation of the class $\mathfrak{3}$ given by the Structure Theorem [S1, 418], [CP, Th. III.5.6]. This characterisation depends on some concepts of centrality theory [S1][CP, Ch. III]. To begin with, a congruence V on a congruence α on a quasigroup Q is said to *respect the equivalence* of α if the three conditions

$$(2.1) \quad \left\{ \begin{array}{l} (RR) \quad \forall x, y \in Q, (x, x)V(y, y); \\ (RS) \quad \forall (x_1, x_2), (y_1, y_2) \in \alpha, (x_1, x_2)V(y_1, y_2) \Rightarrow (x_2, x_1)V(y_2, y_1); \\ (RT) \quad \forall (x_1, x_2), (x_2, x_3), (y_1, y_2), (y_2, y_3) \in \alpha, \\ \quad (x_1, x_2)V(y_1, y_2) \text{ and } (x_2, x_3)V(y_2, y_3) \Rightarrow (x_1, x_3)V(y_1, y_3) \end{array} \right.$$

are satisfied. Then V is said to *centre* α if V respects the equivalence of α and

$$(2.2) \quad \forall (x, y) \in \alpha, \pi_1 : (x, y)^V \rightarrow Q; (z_1, z_2) \mapsto z_1 \text{ bijects.}$$

If V centres α , then \hat{Q} , being a V -class, is a normal subquasigroup of α . Conversely [CP, Prop. III. 3.5], if \hat{Q} is normal in α , then there is a congruence V centering α . A congruence α on Q with these properties is said to be *central*. Each quasigroup Q has a unique maximal central congruence [S1, 228][CP, Th. III.3.10] called the *centre congruence* $\zeta(Q)$. Thus Q is a $\mathfrak{3}$ -quasigroup if and only if $\zeta(Q) = Q^2$. This is the origin of the designation $\mathfrak{3}$: $\mathfrak{3}$ -quasigroups are “all centre” ($\mathfrak{3}$ entrum). If Q is a group or loop, then the centre $Z(Q)$ is the $\zeta(Q)$ -class containing the identity element.

From the standpoint of universal algebra, a quasigroup (Q, \cdot) is best defined as a set Q equipped with three binary operations (*multiplication* \cdot as before, *right division* $/$, and

left division \backslash) satisfying the identities

$$(2.3) \quad \begin{cases} (ER) & (x/y).y = x; \\ (UR) & (x.y)/y = x; \\ (EL) & x.(x\backslash y) = y; \\ (UL) & x\backslash(x.y) = y. \end{cases}$$

(For the equivalence of this definition with the one given in the introduction, see [S2, 117].) A quasigroup $(Q, \cdot, /, \backslash)$ is then said to be a *central isotope* of a second quasigroup $(P, \cdot, /, \backslash)$ if there is a bijection $\theta : Q \rightarrow P$, called a *central shift*, such that for each of the operations $\cdot, /, \backslash$, denoted by ω , there is an element $(p_\omega, \bar{p}_\omega)$ of $\zeta(P)$ such that

$$(2.4) \quad (p_\omega, \bar{p}_\omega)V(qq'\omega\theta, q\theta q'\theta\omega)$$

for each pair q, q' of elements of Q , V being a congruence centering $\zeta(P)$. Central isotopy is an equivalence relation [S1,412][CP,Th. III.4.5].

PROPOSITION 2.1. *If two finite, non-empty quasigroups P and Q are centrally isotopic, then they have the same entropy and the same asymptotic entropy.*

Proof. Two finite quasigroups A and B are centrally isotopic if and only if there is a finite quasigroup Z such that $Z \times A$ and $Z \times B$ are isomorphic [S1, 4.2]. Since P and Q are centrally isotopic, there is a finite quasigroup Z_1 with $Z_1 \times P$ and $Z_1 \times Q$ isomorphic. Suppose, as an induction hypothesis, that there is a finite quasigroup Z_r with $Z_r \times P^r \cong Z_r \times Q^r$. Then $(Z_1 \times Z_r) \times P^{r+1} \cong (Z_1 \times P) \times (Z_r \times P^r) \cong (Z_1 \times Q) \times (Z_r \times Q^r) \cong (Z_q \times Z_r) \times Q^{r+1}$. It follows that P^r is centrally isotopic to Q^r for each positive integer r . Now centrally isotopic quasigroups have similar multiplication group actions [CP, Th. III. 4.6], and accordingly have the same entropy. Thus $H(P^r) = H(Q^r)$ for each r (including $r = 1$, of course), whence $h(P) = h(Q)$. \square

An element e of a quasigroup Q is said to be an *idempotent* if $e.e = e$. For example, the identity elements of groups and loops are idempotents. A central shift $\theta : Q \rightarrow P$ mapping an idempotent of Q to an idempotent of P is an isomorphism [CP, Prop. III. 4.3]. The Structure Theorem for 3-quasigroups [S1, 418][CP, Th. III. 5.6] states that each non-empty 3-quasigroup Q is centrally isotopic to a 3-quasigroup P with idempotent 0, unique up to isomorphism. (Essentially, P with $\{0\}$ is Q^2/\hat{Q} with $\{\hat{Q}\}$.) By Proposition 2.1, the respective entropies and asymptotic entropies of (finite) P and Q coincide. Thus it suffices to examine the entropic behaviour of finite 3-quasigroups with idempotent. The Structure Theorem describes the structure of a 3-quasigroup $(P, \cdot, /, \backslash)$ with idempotent 0 as follows. Set $R = R(0)$ and $L = L(0)$. Then 0 is the zero of an abelian group $(P, +)$ on P having R and L as automorphisms. The multiplication on P is given by

$$(2.5) \quad x.y = xR + yL.$$

Conversely, any pair of automorphisms R, L of an abelian group $(P, +)$ gives a \mathfrak{J} -quasigroup via (2.5), having 0 as an idempotent. In the multiplication group of (P, \cdot) , the stabiliser of 0 is the subgroup generated by R and L , a subgroup of the group of automorphisms of $(P, +)$. To calculate the entropy of P , it is often more convenient to calculate it as the entropy of the partition of P given by the orbits of this stabiliser subgroup.

EXAMPLE 2.2. (Projective Geometries). Let P be a Galois field of order q . Let R and L both denote multiplication by a generator of the cyclic group P^* of non-zero elements of P . Define a quasigroup multiplication on the full set P via (2.5), giving a quasigroup denoted $P(q)$. The stabiliser of 0 in $\text{Mlt } P(q)$ is P^* . Since this stabiliser is transitive on P^* , the quasigroup $P(q)$ has rank 2, and thus minimal entropy by Proposition 1.4. Now consider $P(q)^m$, an m -dimensional vector space over P . Except for the singleton consisting of the origin, the orbits of P^* on $P(q)^m$ are the sets of non-origin elements of lines in $P(q)^m$ through the origin, i.e. the points of the $(m - 1)$ -dimensional projective space over P . There are $(q^m - 1)/(q - 1)$ of these, each of size $q - 1$. Thus

$$(2.6) \quad H(P(q)^m) = \log q^m - (1 - q^{-m}) \log(q - 1)$$

and

$$(2.7) \quad h(P(q)) = \lim_{m \rightarrow \infty} \left[\log q - \frac{(1 - q^{-m})}{m} \log(q - 1) \right] = \log q,$$

the maximum allowed by (1.5). \square

The behaviour $h(P(q)) = \log |P(q)|$ of projective geometries is typical for \mathfrak{J} -quasigroups:

PROPOSITION 2.3. *Let Q be a finite, non-empty \mathfrak{J} -quasigroup. Then $h(Q) = \log |Q|$.*

Proof. By Proposition 2.1 and the Structure Theorem for \mathfrak{J} -quasigroups, it suffices to consider the case of a finite \mathfrak{J} -quasigroup P with idempotent 0, centrally isotopic to Q . Let q be the order of P , and let r be the order of the stabiliser F of 0 in $\text{Mlt } P$. The stabiliser of $(0, \dots, 0)$ in $\text{Mlt } P^m$ is then $F_m = \{(f, \dots, f) | f \in F\}$, again of order r . The entropy of P^m (and hence of Q^m) is equal to the entropy of the partition of P^m given by the orbits of F_m . This entropy is

$$(2.8) \quad \sum_{j=1}^r n_j \frac{j}{q^m} \log \frac{q^m}{j},$$

where the non-negative integer n_j is the number of orbits of size j . The n_j satisfy

$$(2.9) \quad n_1 + 2n_2 + \dots + rn_r = q^m.$$

For non-negative real numbers x_1, \dots, x_r , consider the problem of minimising

$$(2.10) \quad \sum_{j=1}^r \frac{x_j}{q^m} \log \frac{q^m}{j} = \frac{1}{q^m} \left[\log q^m \left(\sum_{j=1}^r x_j \right) - \sum_{j=1}^r x_j \log j \right]$$

subject to

$$(2.11) \quad x_1 + x_2 + \dots + x_r = q^m.$$

In view of (2.11), the problem reduces to maximising $\sum_{j=1}^r x_j \log j$ subject to (2.11). The desired extremum is attained at $x_r = q^m$, $x_{r-1} = \dots = x_1 = 0$, which gives $\log q^m - \log r$ as the minimum value of (2.10). Setting $x_j = j n_j$ makes the value of (2.10) equal to (2.8). Thus

$$(2.12) \quad \log q^m \geq H(q^m) \geq \log q^m - \log r,$$

whence

$$(2.13) \quad h(Q) = \lim_{m \rightarrow \infty} \frac{1}{m} H(Q^m) = \log q$$

as required. \square

Comparing (2.7) and (2.13) with Definition 1.5 raises the following

PROBLEM 2.4. For which quasigroups Q does the limit $\lim_{m \rightarrow \infty} \frac{1}{m} H(Q^m)$ exist?

Finally, recall that a quasigroup (Q, \cdot) is said to be *entropic* (cf. [Et, (3)]) if

$$(2.14) \quad xy.zt = xz.yt$$

for all x, y, z, t in Q . For instance, the projective geometries $P(q)$ of Example 2.2 are entropic (by (2.5) and the commutativity of the group P^*).

COROLLARY 2.5. A finite, non-empty entropic quasigroup Q has maximal asymptotic entropy $\log |Q|$.

Proof. By (2.14), each subquasigroup of an entropic quasigroup is normal. In particular, the diagonal subquasigroup \hat{Q} of the entropic quasigroup Q^2 is normal. Thus Q is a $\mathfrak{3}$ -quasigroup, and the result follows by Proposition 2.3. \square

3. Asymptotic entropy. This section is devoted to the proof of the main

THEOREM 3.1. *A finite non-empty quasigroup Q is a \mathfrak{J} -quasigroup if and only if $h(Q) = \log |Q|$.*

The “only if” direction has been covered by Proposition 2.3. Let Q be a finite non-empty quasigroup not in the class \mathfrak{J} . It must be shown that $h(Q) < \log |Q|$. In fact, it will be shown that there are positive constants w and c such that

$$(3.1) \quad \frac{1}{m}H(Q^m) \leq \log |Q| - w \log 2 + \frac{\log 2c}{m}$$

for all sufficiently large m .

To begin with, fix an element e of Q . For any positive integer m , set $x = (e, \dots, e) \in Q^m$. Since Q is not a \mathfrak{J} -quasigroup, the diagonal \hat{Q} is not a normal subquasigroup of Q^2 . The first lemma gives a sufficient condition for normality of subquasigroups (cf. [Br,Th. I. 3C] for the loop case).

LEMMA 3.2. *Let P be a finite quasigroup with multiplication group G . Let h be an element of a subquasigroup H of P . Then H is a normal subquasigroup of P if it is invariant under the stabiliser G_h of h in G .*

Proof. It will be shown that the right cosets $H(h \setminus p)$ of H in P form a quasigroup P/H under complex multiplication. Indeed, for p and q in P , one has $H(h \setminus p) \cdot H(h \setminus q) = \{HR(h \setminus p)R(r(h \setminus q))R(h \setminus [p \cdot r(h \setminus q)])^{-1}R(h \setminus [p \cdot r(h \setminus q)]) \mid r \in H\} = \{HR(h \setminus [p \cdot r(h \setminus q)]) \mid r \in H\} = H(h \setminus [p \cdot H(h \setminus q)]) = H(h \setminus [HR(h \setminus q)L(p)R(h \setminus pq)]^{-1}R(h \setminus pq)) = H(h \setminus H(h \setminus pq)) = \{HR(h \setminus [r(h \setminus pq)]) \mid r \in H\} = \{HR(h \setminus r)R(h \setminus pq)R(h \setminus [r(h \setminus pq)])^{-1}R(h \setminus [r(h \setminus pq)]) \mid r \in H\} = H(h \setminus pq)$. The second equality holds since $R(h \setminus p)R(r(h \setminus q))R(h \setminus [p \cdot r(h \setminus q)])^{-1}$ fixes h . The fourth equality holds since $R(h \setminus q)L(p)R(h \setminus pq)^{-1}$ fixes h . The last equality holds since $R(h \setminus r)R(h \setminus pq)R(h \setminus [r(h \setminus pq)])^{-1}$ fixes h . Thus $P \rightarrow P/H; p \mapsto H(h \setminus p)$ is a quasigroup homomorphism, with H as the preimage of the coset H . \square

If F is the stabiliser of (e, e) in $\text{Mlt } Q^2$, Lemma 3.2 shows that $\hat{Q}F$ contains \hat{Q} properly. In particular,

$$(3.2) \quad \exists q \in Q. \exists (\alpha, \beta) \in \text{Mlt } Q^2. e\alpha = e\beta = e, qx = s \neq t = q\beta.$$

Consider a random element $y = (y_1, \dots, y_m)$ of Q^m . The probability that its i -th component y_i coincides with q is $1 - p = |Q|^{-1}$. The following lemma bounds the probability that y does not have even a certain small proportion u of its components coinciding with q . The lemma gives an appropriate and immediate version of the “Chernoff bound” of large deviation theory [Cr], [ES, §3], [Sp, Lectures 4,7].

LEMMA 3.3. For each p in the open unit interval $]0, 1[$, there are positive constants u, v , and c (with $c \geq 1$ and u irrational) such that

$$\sum_{k=0}^{\lfloor um \rfloor} \binom{m}{k} (1-p)^k p^{m-k} \leq c 2^{-vm}$$

for all non-negative integers m .

Proof. For given $0 < r < 1$, let Γ denote the circle of radius r centered on the origin in the complex plane. Then $\sum_{k=0}^{\lfloor um \rfloor} \binom{m}{k} (1-p)^k p^{m-k} = \frac{1}{2\pi i} \int_{\Gamma} [z(1-p) + p]^m [1 + z^{-1} + \dots + z^{-\lfloor um \rfloor}] z^{-1} dz = \frac{1}{2\pi i} \int_{\Gamma} \frac{[z(1-p) + p]^m}{z^{\lfloor um \rfloor}} \cdot \frac{z^{1+\lfloor um \rfloor} - 1}{z(z-1)} dz$. For z on Γ , one has the estimates

$$(3.3) \quad \left| \frac{z^{1+\lfloor um \rfloor} - 1}{z(z-1)} \right| \leq \frac{r^{1+\lfloor um \rfloor} + 1}{r(1-r)} < \frac{2}{r(1-r)}$$

and

$$(3.4) \quad \left| \frac{[z(1-p) + p]^m}{z^{\lfloor um \rfloor}} \right| \leq \frac{[r(1-p) + p]^m}{r^{\lfloor um \rfloor}} \leq \left[\frac{r(1-p) + p}{r^u} \right]^m,$$

whence $\sum_{k=0}^{\lfloor um \rfloor} \binom{m}{k} (1-p)^k p^{m-k} < \frac{2}{1-r} \left[\frac{r(1-p) + p}{r^u} \right]^m$. Now $r(1-p) + p < 1$, while $\lim_{u \rightarrow 0} r^u = 1$. The positive irrational constant u is thus chosen so small that $b = r^u / [r(1-p) + p] > 1$. The lemma follows, with $c = 2/(1-r) \geq 1$ and $v = \log_2 b$. \square

The irrationality of u in Lemma 3.3 is merely a technical convenience to separate the floor of um from its ceiling, regardless of the choice of the integer m .

An element $y = (y_1, \dots, y_m)$ of Q^m is called *good* if the number of its components coinciding with q exceeds um , the irrational constant u being associated by Lemma 3.3 with $p = (|Q| - 1)/|Q|$. A quasigroup conjugacy class of Q^m is called *good* if it contains a pair (x, y) with good y . If elements and classes are not good, they are called *bad*. By Lemma 3.3, there are at most $c|Q|^m \cdot 2^{-vm}$ bad elements y . Each bad class contains at least one pair (x, y) with bad y . Thus the number of bad classes is at most

$$(3.5) \quad c|Q|^m \cdot 2^{-vm}.$$

On the other hand, good classes are fairly large:

LEMMA 3.4. Each good quasigroup conjugacy class of Q^m contains at least

$$|Q|^m \cdot 2^{um}$$

elements, for all sufficiently large m .

Proof. Without loss of generality, one may consider the good class containing the pair (x, y) with $y = (q, \dots, q, y_{r+1}, \dots, y_m)$, where $r = \lceil um \rceil$. For each subset I of $\{1, \dots, r\}$, there is a certain element γ_I of the stabiliser of x in $\text{Mlt } Q^m$. This element γ_I is chosen to have the property that $y\gamma_I = (z_1, \dots, z_r, y'_{r+1}, \dots, y'_m)$ for some y'_i in Q , where $z_i = s$ for i in I , but $z_j = t$ for j not in I . Thus the i -th components of γ_I may be taken as the α of (3.2), while the j -th components may be taken as β . As I ranges over the 2^r different subsets of $\{1, \dots, r\}$, one obtains 2^r different elements $(x, y)(\gamma_I, \gamma_I) = (x, y\gamma_I)$ in the conjugacy class, each having x in its first half. The result follows. \square

Since $Q^m \times Q^m$ has $|Q|^{2m}$ elements, and each good quasigroup conjugacy class has at least $|Q|^m \cdot 2^{um}$ elements, there are at most

$$(3.6) \quad |Q|^m \cdot 2^{-um}$$

good classes. Let w be the minimum of the two positive constants u and v . Recall $c \geq 1$. Since each class is either good or bad, (3.5) and (3.6) show that the total number of classes is at most $|Q|^m(c \cdot 2^{-vm} + 2^{-um}) \leq 2c|Q|^m \cdot 2^{-wm}$. By (1.2), $H(Q^m) \leq \log |Q|^m - \log 2^{wm} + \log 2c$. The required inequality (3.1) follows.

REFERENCES

- [BCL] D.R. BROOKS, D.D. CUMMING AND P.H. LEBLOND, *Dollo's Law and The Second Law of Thermodynamics: analogy or extension?*, in *Entropy, Information and Evolution: New Perspectives on Physical and Biological Evolution*, B.H. Weber, D.J. Depew and J.D. Smith eds., M.I.T. Press, Cambridge, 1988, pp. 189–224.
- [Br] R.H. BRUCK, *Contributions to the theory of loops*, Trans. Amer. Math. Soc., 60 (1946), pp. 245–354.
- [CP] O. CHEIN, H. PFLUGFELDER AND J.D.H. SMITH (eds.), *Theory and Applications of Quasigroups and Loops*, Heldermann Verlag, Berlin, 1989.
- [Cr] H. CHERNOFF, *A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations*, Ann. Math. Stat., 23 (1952), pp. 493–509.
- [CS] I.P. CORNFELD, S.W. FOMIN AND YA. G. SINAI, *Ergodic Theory*, Springer, New York, 1982.
- [ES] P. ERDŐS AND J. SPENCER, *Probabilistic Methods in Combinatorics*, Academic Press, New York, 1974.
- [Et] I.M.H. ETHERINGTON, *Note on quasigroups and trees*, Proc. Edin. Math. Soc., 13 (1963), pp. 219–222.
- [J1] K.W. JOHNSON AND J.D.H. SMITH, *Characters of finite quasigroups*, Europ. J. Combinatorics, 5 (1984), pp. 43–50.
- [J2] K.W. JOHNSON AND J.D.H. SMITH, *Characters of finite quasigroups II: induced characters*, Europ. J. Combinatorics, 7 (1986), pp. 131–137.
- [J3] K.W. JOHNSON AND J.D.H. SMITH, *Characters of finite quasigroups III: quotients and fusion*, Europ. J. Combinatorics (to appear).

- [J4] K.W. JOHNSON AND J.D.H. SMITH, *Characters of finite quasigroups IV: products and superschemes*, Europ. J. Combinatorics (to appear).
- [J5] K.W. JOHNSON AND J.D.H. SMITH, *Characters of finite quasigroups V: linear characters*, preprint.
- [S1] J.D.H. SMITH, *Mal'cev Varieties*, Springer, Berlin, 1976.
- [S2] J.D.H. SMITH, *Representation Theory of Infinite Groups and Finite Quasigroups*, Université de Montréal, Montréal, 1986.
- [S3] J.D.H. SMITH, *A class of mathematical models for evolution and hierarchial information theory*, IMA preprint series # 396 (1988).
- [Sp] J. SPENCER, *Ten Lectures on the Probabilistic Method*, SIAM, Philadelphia (1987).