Totally Symmetric Quasigroups of Order 16

Hy Ginsberg

Abstract

We present the number of totally symmetric quasigroups (equivalently, totally symmetric Latin squares) of order 16, as well as the number of isomorphism classes of such objects. Totally symmetric quasigroups of orders up to and including 16 that are (respectively) medial, idempotent, and unipotent are also enumerated.

Suppose $xy = z$ for some elements x, y, z in a quasigroup Q of order n. We say that Q is *totally symmetric* if this implies all six permutations of the symbols x, y, and z in this equation: $xz = y$, $yx = z$, $yz = x$, $zx = y$, and $zy = x$ (along with the hypothesized $xy = z$).

In [Bai79a, Bai79b] Rosemary Bailey enumerated the totally symmetric quasigroups of orders up to and including $n = 10$; these results were extended by Brendan McKay and Ian Wanless through $n = 15$ in [MW22]. The main purpose of this paper is to announce the results for $n = 16$, which are as follows:

Theorem 1. *There are*

91,361,407,076,595,590,705,971,200

totally symmetric quasigroups of order 16; these are divided into

4,366,600,209,354

isomorphism classes.

A brief overview of the algorithm used to calculate this result is given at the end of this document.

Returning to our totally symmetric quasigroup Q of order n, if

$$w(x(yz)) = y(x(wz)$$

for all $w, x, y, z \in Q$, then Q is said to be *medial*. This property can also be expressed as $(wx)(yz) = (wy)(xz)$, and has been referred to by various authors as *abelian* [Mur41, Bru44, Sch95] or *entropic* [Eth65]; *medial* appears to be the most modernly accepted term [Mar97, Shc05, SV16, You21], and so has been adopted for this paper.

The interest in medial totally symmetric quasigroups arises naturally in the study of elliptic curves, where one can define an addition for points on a curve by fixing a point p (generally taken to be the projective point at infinity) and defining

$$x + y = p(xy).$$

Under this definition, if Q is totally symmetric, then p is the additive identity, $-x = px$, and the addition thus defined is associative *if and only if* Q is medial (see the beautiful exercise 1.11 in [ST15], which inspired the author's investigation into these objects). This addition enjoys the useful property that the sum of any two rational points on an elliptic curve $\mathcal{C}$ is itself a rational point on $\mathcal{C}$.

Recent results of Benjamin Young [You21] establish that the number of medial totally symmetric quasigroups of order n is precisely the number of "labeled" abelian groups of order n (i.e. counting isomorphic but non-identical groups separately); this is sequence A034382 in the *On-Line Encyclopedia of Integer Sequences* [OEI]. Furthermore, J. Schwenk [Sch95] gives a formula for the number of isomorphism classes of medial totally symmetric quasigroups: If 3 does not divide n, it is precisely the number of isomorphism classes of abelian groups of order n; otherwise each abelian group of order n contributes one more than the number of non-isomorphic cyclic 3-groups in its invariant factor decomposition (for $n \leq 16$ with n divisible by 3, each abelian group of order n has a single such factor, so for the quasigroups considered in this paper there are in this case twice as many isomorphism classes of medial totally symmetric quasigroups as there are isomorphism classes of abelian groups).

Our data on totally symmetric quasigroups and medial totally symmetric quasigroups is presented in Table 1, below.

Table 1: Totally Symmetric Quasigroups

	Totally Symmetric Quasigroups		Medial	
Order	Number	Classes	Number	Classes
1	1	1	1	1
2	2	1	2	1
3	3	2	3	2
4	16	2	16	2
5	30	1	30	1
6	480	3	360	2
7	1290	3	840	1
8	163,200	13	15,360	3
9	471,240	12	68,040	4
10	386,400,000	139	907,200	1
11	2,269,270,080	65	3,991,680	1
12	12,238,171,545,600	25,894	159,667,200	4
13	149,648,961,369,600	24,316	518,918,400	1
14	8,089,070,513,113,497,600	92,798,256	14,529,715,200	1
15	160,650,421,233,958,656,000	122,859,802	163,459,296,000	2
16	91,361,407,076,595,590,705,971,200	4,366,600,209,354	4,250,979,532,800	5

We include as well (in Table 2) the numbers of *idempotent* and *unipotent* totally symmetric quasigroups and classes, where a quasigroup is *idempotent* if $xx = x$ for all $x \in Q$, and *unipotent* if $xx = k$ for all $x \in Q$ and some fixed $k \in Q$. These properties are closely related; McKay and Wanless prove that there is a bijective correspondence between isomorphism classes of idempotent totally symmetric quasigroups of order n and isomorphism classes of unipotent totally symmetric quasigroups of order $n + 1$ [MW22, Theorem 5.2]. We strengthen this theorem slightly:

Theorem 2. *The number of unipotent totally symmetric quasigroups of order $n + 1$ is precisely $n + 1$ times the number of idempotent totally symmetric quasigroups of order n.*

Table 2: Unipotent and Idempotent Totally Symmetric Quasigroups

	Idempotent		Unipotent	
Order	Number	Classes	Number	Classes
1	1	1	1	1
2	0	0	2	1
3	1	1	0	0
4	0	0	4	1
5	0	0	0	0
6	0	0	0	0
7	30	1	0	0
8	0	0	240	1
9	840	1	0	0
10	0	0	8,400	1
11	0	0	0	0
12	0	0	0	0
13	1,197,504,000	2	0	0
14	0	0	16,765,056,000	2
15	60,281,712,691,200	80	0	0
16	0	0	964,507,403,059,200	80

Proof. We demonstrate how to construct $n+1$ distinct unipotent totally symmetric quasigroups of order $n+1$ from any given idempotent totally symmetric quasigroup of order n; this procedure can then be reversed to complete the proof.

Let $(Q, *)$ be an idempotent totally symmetric quasigroup of order n, and let $Q' = Q \cup \{a\}$ where $a \notin Q$. If x and y are distinct elements of $Q' - \{a\}$, define $x *' y = x * y$. Otherwise, for every $x \in Q$, define $x *' x = a$, so $x*'a = a*'x = x$ by total symmetry. Setting $a*'a = a$ completes the definition of $(Q', *')$, and it is immediately apparent that $(Q', *')$ is both unipotent and totally symmetric. There are $n+1$ quasigroups isomorphic to $(Q', *')$, one for each of the possible choices of element along the diagonal; these are obtained by applying the transposition $(x\, a)$ (in cycle notation) to the rows, columns, and symbols of the multiplication table for Q' (equivalently, to the corresponding Latin square).

To reverse this procedure, let $(Q', *')$ be any unipotent totally symmetric quasigroup of order $n+1$, and assume once again that $Q' = Q \cup \{a\}$ with $a \notin Q$. Then if $x *' x = k$ for all $x \in Q'$, we may construct the quasigroup $(Q, *)$ of order n by first applying the transposition $(k\, a)$ to the rows, columns, and symbols of the associated multiplication table (Latin square), so that $x *' x = a$ for all x in the result. Removing the a^{th} row and column, setting $x * x = x$ for all $x \in Q$, and otherwise letting $x * y = x *' y$ results in a quasigroup Q that is clearly both idempotent and totally symmetric; moreover, each of the $n+1$ unipotent quasigroups Q' described in the preceding paragraph generate precisely this quasigroup.

Finally, observe that since $x *' y = x * y$ for all distinct $x, y \in Q$, the $n+1$ unipotent quasigroups Q' of order $n+1$ corresponding to a given idempotent quasigroup Q of order n are the *only* unipotent quasigroups corresponding to Q in this manner; any other unipotent quasigroup of order $n+1$ must correspond (in the same manner) to a different idempotent quasigroup of order n. □

The results of Bailey, McKay and Wanless, Young, and Schwenk all provide independent confirmation of the correctness of the results reported in Theorem 1, as the software used to establish that theorem reproduces a great many of the results computed and predicted by these authors. Specifically, the software gives:

- the number of totally symmetric quasigroups, as well as the number of isomorphism classes of totally symmetric quasigroups, computed by McKay and Wanless for sets of order $n \leq 15$ (agreeing, of course, with Bailey's results for $n \leq 10$);

- the number of medial totally symmetric quasigroups of order n for all $n \leq 16$ predicted by Young;

- the number of isomorphism classes of medial totally symmetric quasigroups of order n for all $n \leq 16$ predicted by Schwenk;

- the number of idempotent totally symmetric quasigroups, as well as the number of isomorphism classes of idempotent totally symmetric quasigroups computed by McKay and Wanless for those orders $n < 16$ that have such objects ($n = 3, 7, 9, 13, 15$).

It is worth noting that this last observation provides corresponding results for $n = 16$ (namely that there are 80 isomorphism classes of unipotent totally symmetric quasigroups of this order), which the software corroborates.

Finally, we offer a slight strengthening of an observation from Bruck [Bru44, Lemma 10]:

Theorem 3. *A totally symmetric quasigroup is a group if and only if it is an elementary abelian 2-group. When this occurs the quasigroup is both medial and unipotent.*

Proof. That an elementary abelian 2-group is a medial, unipotent, totally symmetric quasigroup is clear.

To establish the converse, let Q be a totally symmetric quasigroup, and assume Q is a group. Let $x \in Q$ and suppose $xx = y$. It follows by total symmetry that $xy = x$, so

$$x(xy) = (xx)y = y.$$

Hence xx is the identity for every $x \in Q$. Since every nonidentity element has order 2, Q is an elementary abelian 2-group. □

Procedural Summary

Viewing a totally symmetric quasigroup as a Latin square, or, equivalently, as being represented by its Cayley table, the entries along the main diagonal are of precisely two types – those for which $xx = x$ (i.e. idempotent elements) and those for which this is not the case. In [Bai79a] Rosemary Bailey presented criteria constraining the quantity of each type of diagonal entry based on the order n of the quasigroup, and further described a procedure for constructing directed graphs for each permissible configuration of the diagonal. The software developed to enumerate quasigroups for this paper begins by constructing these "Bailey graphs;" for $n = 16$ there are 980 distinct, non-isomorphic Bailey graphs: 901 with one idempotent element, 77 with 4 idempotent elements, and 2 with 7 idempotent elements. These correspond to 980 starting configurations, each with a distinct, non-isomorphic arrangement of the elements on the diagonal, and – in deference to the magnitude of the problem – each is processed separately, with the results recorded and ultimately combined.

The fundamental process amounts to constructing totally symmetric quasigroups (by building their Cayley tables) and then checking completed instances for isomorphism to quasigroups already constructed. In [MW22] McKay and Wanless describe a technique for extending a Bailey graph to a directed graph that completely describes the quasigroup; this we do, allowing us to use the `nauty` graph automorphism software [MP14] to test for isomorphism.

A great deal of technical sleight-of-hand is required to make the algorithm workable in practice... Although there is a wide range of complexity among the starting configurations, a fairly typical example might have approximately 25 billion isomorphism classes and 500 sextillion quasigroups. Maintaining data structures for individual quasigroups is thankfully not necessary, but maintaining 25 billion isomorphism classes – with enough information to distinguish them from each other – is a daunting task, and in fact cannot be done within any reasonable limit on the amount of computer memory. The McKay-Wanless graph for $n = 16$ requires 408 bytes to represent in `nauty`; using compression to approximately halve this amount still results in an isomorphism class structure that requires roughly 240 bytes. This amounts to over 6 *terabytes* of memory just to store the isomorphism classes; naturally there are other memory requirements as well, making the prospect unfeasible for even the most powerful of today's readily available consumer computers. This limitation is addressed by maintaining a large hash table of isomorphism classes, and, when an appropriate memory threshold is reached, flushing sections of the hash table to disk for storage and later processing. As the process is ongoing, this then requires further flushing of newly constructed isomorphism classes to disk, should they happen to belong to already flushed sections of the hash table. In some of the more challenging configurations the available disk space proves to be insufficient for the task, leaving no option but to discard some of the flushed sections of the hash table; when this occurs subsequent iterations through the entire process are required to recover the abandoned data.

Regarding hardware, the project was completed on a pair of Dell Precision 5810 workstations (running Fedora Linux at runlevel 3); both computers were equipped with 256 GB of RAM and 12 terabytes of hard drive space (comprised of three 4 terabyte drives, configured in a RAID0 array). One of the computers had an additional 1 TB solid state drive; that computer was outfitted with an Intel Xeon E5-2699A v4 22-core 2.4 GHz processor;

the other had an Intel Xeon E5-2697A v4 16-core 2.6 GHz processor. (These specifications reflect the ultimate configurations of the two systems; there was initially only one, and much upgrading of components – including CPUs, memory, and disk drives – was performed while the project was ongoing.) The final results reported herein were obtained after approximately 12 months of computing.

Acknowledgments

This paper was greatly improved through correspondence with Benjamin Young, who brought to my attention Schwenk's results on the number of isomorphism classes of medial totally symmetric quasigroups, thereby disembarrassing me of a simpler (and incorrect) conjecture that I would otherwise have submitted for publication. Much obliged, Ben.

Heartfelt thanks to Jeff Robbins of LiveData Inc., who generously shared his unparalleled knowledge of modern computing platforms and techniques, helping design the fantasy system for which the funding unfortunately never materialized... My remarkable brother-in-law, Robert Edelstein, a writer with no advanced mathematical training, somehow managed to beat me to the discovery of a body of published research on these objects... His continued sincere interest provided a much needed outlet for my frequent, detailed, elaborate bursts of obsessive enthusiasm; thank you, Rob. Thanks as well to the brilliant Matthew Welz – my "mathematical brother" – for his assistance during the early stages of the work, and to our "mathematical father," Richard Foote, without whom, as far as I am concerned, there would be no mathematics – as far as I am concerned, Richard said "Let $\epsilon > 0$ be given," and there was *light*...

References

[Bai79a] R. A. Bailey, *Enumeration of totally symmetric Latin squares*, Util. Math. **15** (1979), 193–216.

[Bai79b] _____, *Corrigendum to enumeration of totally symmetric Latin squares*, Util. Math. **16** (1979), 302.

[Bru44] R. H. Bruck, *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. **55** (1944), 19–52.

[Eth65] I. M. H. Etherington, *Quasigroups and cubic curves*, Proc. Edinburgh Math. Soc. **14** (1965), 273–291.

[Mar97] A. W. Marczak, *On nondistributive Steiner quasigroups*, Colloq. Math. **74** (1997), no. 1, 135–145.

[MP14] B. D. Mckay and A. Piperno, *Practical graph isomorphism II*, J. Symbolic Comput. **60** (2014), 94–112.

[Mur41] D. C. Murdoch, *Structure of abelian quasigroups*, Trans. Amer. Math. Soc. **47** (1941), 134–138.

[MW22] B. D. Mckay and I. M. Wanless, *Enumeration of Latin squares with conjugate symmetry*, J. Combin. Des. **30** (2022), 105–130.

[OEI] *The on-line encyclopedia of integer sequences*, published electronically at https://oeis.org, OEIS Foundation, Inc.

[Sch95] J. Schwenk, *A classification of abelian quasigroups*, Rend. Mat. Appl. **15** (1995), 161–172.

[Shc05] V. A. Shcherbacov, *On the structure of finite medial quasigroups*, Bul. Acad. Ştiinţe Repub. Mold. Mat. **47** (2005), no. 1, 11–18.

[ST15] J. H. Silverman and J. T. Tate, *Rational points on elliptic curves*, second ed., Undergraduate Texts in Mathematics, Springer, 2015.

[SV16] D. Stanovsky and P. Vojtechovsky, *Central and medial quasigroups of small order*, Bul. Acad. Ştiinţe Repub. Mold. Mat. **80** (2016), no. 1, 24–40.

[You21] B. Young, *Totally symmetric and medial quasigroups and their applications*, Master's thesis, Case Western Reserve University, May 2021.