STEINER QUADRUPLE SYSTEMS WITH MINIMUM COLOURABLE DERIVED DESIGNS AT THE ORDERS 38, 44, 62, 74, 86 AND 92

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. A Steiner quadruple system SQS(v) has *minimum colourable derived designs* — it is an mcDSQS(v), in the terminology of Tan and Zhou — when the derived Steiner triple system at *every* one of its v points partitions into the least possible number of partial parallel classes. For $v \equiv 2 \pmod 6$ that number is $v/2$, and the existence of an mcDSQS(n) for all $n \equiv 2 \pmod 6$, $n \geq 20$, is Conjecture 2 of Shi, Xia and Krotov, where it is equivalent to a statement about diameter perfect constant-weight codes. The published orders are 20, 26, 32 and $2 \cdot 9^m + 2$; Tan and Zhou ask, as the first of their open problems, for an mcDSQS(38). We construct an mcDSQS(v) for

$$v \ = \ 38,\ 44,\ 62,\ 74,\ 86,\ 92,$$

two designs at each order, and prove the defining property for all v points of each. Every design is cyclic, and no novelty is claimed on the design side: the cyclic SQS(v) spectrum below 100 is settled in the literature apart from $v = 94$. The new content is the colouring. Order 74 is the value at $n = 1$ of the family $18 \cdot 4^n + 2$, for which Tan and Zhou pose a separate open problem. The colourings were found by an encoding that makes explicit a second exact cover hidden in the problem: since each point of an STS($n-1$) is missed by exactly one class of a minimum colouring, a minimum colouring is a pair of coupled exact covers, and every earlier method we tried left the second one implicit. Making it explicit turns instances on which a local search of 1.2 million moves stalls into instances a SAT solver closes in seconds, and removes the need for any symmetry restriction at all. We also record two structural consequences: none of the minimum colourings found here has the "Hanani" class-size profile, and at orders 38 and 74 two of our designs realise *different* profiles, so the profile is not an invariant of the order. All statements are machine-checked in Lean 4.

1. Introduction

The objects. A *Steiner quadruple system* of order v, written SQS(v), is a 3-design $S(3,4,v)$: a collection of 4-subsets (*blocks*) of a v-set in which every 3-subset lies in exactly one block. Such a system has $\binom{v}{3}/4 = v(v-1)(v-2)/24$ blocks, and Hanani [7] proved that one exists precisely when $v \equiv 2$ or $4 \pmod 6$ (or $v \leq 1$). The *derived design* of an SQS(v) at a point x is

$$\{\, B \setminus \{x\} \ : \ x \in B \,\},$$

a Steiner triple system STS($v-1$) on the remaining $v-1$ points.

A *partial parallel class* of a triple system is a set of pairwise disjoint blocks, and an *r-colouring* is a partition of the block set into r partial parallel classes. The least r for which *some* STS(v) admits an r-colouring is the *chromatic index* $\chi'(v)$ (the quantity Shi, Xia and Krotov call the chromatic number of the system); an STS(v) attaining it is *minimum colourable*, an mcSTS(v). A simple count gives $\chi'(v) \geq (v+1)/2$ for $v \equiv 1 \pmod 6$, and Hanani triple systems — Steiner triple systems of order $v \equiv 1 \pmod 6$ with $(v-1)/2$ pairwise disjoint almost parallel classes, the triples left over forming one further partial parallel class, constructed by Vanstone, Stinson, Schellenberg, Rosa, Rees, Colbourn, Carter and Carter [15] for every such v except $v \in \{7, 13\}$ — show the bound is attained in $(v-1)/2 + 1$ classes. Hence

$$\chi'(v) \ = \ \tfrac{v+1}{2} \qquad \text{for } v \equiv 1 \pmod 6,\ v \notin \{7, 13\}. \tag{1}$$

What [15] proves is the existence theorem; (1) is the consequence drawn from it. It is printed in that form by Grannell, Griggs and Rosa [6], who state it for $v \equiv 1 \pmod 6$ with $v \geq 19$ and note that it follows from results of Ray-Chaudhuri and Wilson and of "Vanstone et al. … on the existence of Hanani triple systems for $v \equiv 1 \pmod 6$, $v \geq 19$", and again by Tan and Zhou [14], who write (1) with the exceptions displayed and cite [15] for it. The two exceptions are Colbourn's [3] values $\chi'(7) = 7$ and $\chi'(13) = 8$, and they are exactly why the conjecture below starts at $n \geq 20$.

Tan and Zhou [14] introduced the following strengthening, which asks for minimum colourability not at one point but at all of them at once.

Definition 1.1. An mcDSQS(v) is an SQS(v) whose derived design at *every* point is minimum colourable.

For $v \equiv 2 \pmod 6$ the derived designs are STS($v-1$) with $v - 1 \equiv 1 \pmod 6$, so by (1) an mcDSQS(v) with $v \geq 20$ is an SQS(v) all v of whose derived designs partition into $v/2$ partial parallel classes. The condition is a real strengthening of (1): that identity says that *some* STS($v-1$) attains $(v+1)/2$ colours, not that any particular one does, and Rosa's conjecture — that for $v \neq 7$ the chromatic index of an individual system lies in $\{m(v), m(v)+1, m(v)+2\}$, where $m(v)$ is the counting lower bound, as recorded by Bryant, Colbourn, Horsley and Wanless [1] — allows an individual STS(v) with $v \equiv 1 \pmod 6$ to need $(v+1)/2$, $(v+3)/2$ or $(v+5)/2$ colours. Requiring all v derived designs of one quadruple system to attain the minimum simultaneously does not follow from (1) at all, and that is the whole content of the problem.

The open questions. Shi, Xia and Krotov [12], studying diameter perfect constant-weight codes, close with the following, quoted verbatim.

Conjecture 1.2 ([12, Conjecture 2])**.** If $20 \leq n \equiv 2 \bmod 6$, then there is an SQS($n$) such that all its derived STS have chromatic number $n/2$, i.e., can be partitioned into $n/2$ partial parallel classes (equivalently, $q_0'(3, 4, n) = n/2 + 1$).

In the vocabulary of Definition 1.1 this is "an mcDSQS(n) exists for every $n \equiv 2 \pmod 6$ with $n \geq 20$". Tan and Zhou [14] prove the existence of an mcDSQS(v) for $v = 20, 26, 32$ and, by a recursive construction, for $v = 2 \cdot 9^m + 2$; the latter family is $20, 164, 1460, 13124, \ldots$, so the published set of settled orders is

$$\{20,\ 26,\ 32\} \ \cup\ \{\, 2 \cdot 9^m + 2 \ :\ m \geq 1 \,\}. \tag{2}$$

Their remaining families are conditional on auxiliary designs whose construction they pose as open problems, so (2) is the list of settled orders. Their first open problem reads, verbatim:

Problem 1.3 ([14, §4, Problem (1)])**.** Find more examples of mcDSQS(v)s, for example, an mcDSQS(38) and an RDSQS(52) (the smallest unknown mcDSQS($6n+2$)s and the smallest unknown RDSQS($6n+4$)s, respectively).

Their third open problem asks for auxiliary designs from which, as they put it, "the existence of an mcDSQS($18 \cdot 4^n + 2$) would be obtained by filling with an mcDSQS(20)". At $n = 1$ that family gives 74.

Results. We settle Conjecture 1.2 at six orders.

Theorem 1.4 (Main theorem)**.** *An* mcDSQS(v) *exists for* $v = 38$*,* 44*,* 62*,* 74*,* 86 *and* 92*. At each of the six orders two designs are exhibited, both of them cyclic* SQS(v)*s, and for each the defining property is verified at all v points. The first design at each order additionally carries the nontrivial multiplier recorded in Table 1.*

Together with (2), Conjecture 1.2 is now known at

$$20,\ 26,\ 32,\ 38,\ 44,\ 62,\ 74,\ 86,\ 92 \quad \text{and} \quad 2 \cdot 9^m + 2.$$

Order 38 answers the mcDSQS half of Problem 1.3 and was the smallest order at which Conjecture 1.2 was open; order 74 is the value at $n = 1$ of the family for which [14, §4, Problem (3)] asks by a different route. On the equivalence stated inside Conjecture 1.2, these constructions also fix the

v	blocks	derived STS	its blocks	colours	multiplier	class sizes
38	2109	STS(37)	222	19	$\langle 7\rangle$, order 3	$12^{15}\,11^{3}\,9$
44	3311	STS(43)	301	22	$\langle 5\rangle$, order 5	$14^{20}\,11\,10$
62	9455	STS(61)	610	31	$\langle 33\rangle$, order 5	$20^{26}\,18^{5}$
74	16206	STS(73)	876	37	$\langle 27\rangle$, order 6	$24^{31}\,22^{6}$
86	25585	STS(85)	1190	43	$\langle 11\rangle$, order 7	$28^{36}\,26^{7}$
92	31395	STS(91)	1365	46	$\langle 9\rangle$, order 11	$30^{44}\,23\,22$

TABLE 1. The six orders. "Multiplier" is the subgroup of $(\mathbb{Z}/v)^*$ under which the first design at that order is invariant; "class sizes" is the profile of the exhibited colouring of the derived design at the point 0.

constant-weight code quantity $q_0'(3,4,n) = n/2+1$ at these six orders; that reduction is the authors' own and is reported here, not re-derived.

Table 1 collects the numerical shape of the six orders. The proofs are, in each case, a design and one colouring: every design is invariant under $x \mapsto x+1$ on $\mathbb{Z}_v$, hence point-transitive, so its v derived designs are translates of one another and a single colouring settles all of them.

What is not new. The design side is not claimed as new at any order. Kiermaier, Krčadinac and Wassermann [8] record that the existence question for cyclic SQS(v) is settled in the literature for every $v < 100$ except $v = 94$, crediting the spectrum to Feng and Chang [5]; Chang, Fan, Feng, Holt and Östergård [2] write that "for $v \le 100$, the only open case is currently $v = 94$", crediting the same source, and name $v = 40$, 44, 50 as "the next orders to consider in a search for isomorphic multiplier inequivalent" cyclic systems. We did not consult [5] itself; the spectrum is taken here on the authority of [8] and [2], which agree. Our designs are constructed here only because the colouring search needs *many* of them and because no explicit block list was obtainable at most of these orders; that they exist is known. Likewise (1) is known, and the values $\chi'(37)$, $\chi'(43)$, $\chi'(61)$, $\chi'(73)$, $\chi'(85)$, $\chi'(91)$ are not new. No proof below uses (1): the lower bound we use is always the elementary count of Lemma 2.1, proved for every input, and the upper bound is always an exhibited colouring. Equation (1) enters only to say what the number $v/2$ of Definition 1.1 amounts to at these orders.

Method, and the methodological point. The colouring step, not the design step, is the whole difficulty, and it defeated five distinct methods over an earlier round of work at orders 62 and 74 (§6). The fix was not a larger budget but a different encoding, and we state it as the methodological contribution of the paper. In a minimum colouring of an STS($n-1$) with $n/2$ classes, each point lies in $n/2-1$ pairwise meeting triples, hence is *covered* by $n/2-1$ classes and *missed* by exactly one. So a minimum colouring is a pair of coupled exact covers, blocks to classes and points to "the class that misses me", and every method we had tried left the second cover implicit. Making it explicit — variables for the miss relation, tied to the block variables in both directions, together with the constraint that a class of deficiency e misses exactly $1+3e$ points — closes in seconds instances that a local search of 1.2 million moves per restart cannot close, and it removes the need for any symmetry restriction at all (§5).

Layout. Section 2 fixes notation, proves the counting bound and derives the deficiency identity that the encoding uses. Section 3 records the designs and their orbit arithmetic, Section 4 the colourings and the main theorems. Section 5 describes the encoding and the calibration experiments that justify it, and Section 6 explains what equivariance buys and where it is fatal — including a proof that the method is dead at order 50. Section 7 treats the class-size profiles, Section 8 the near-linear test for the Steiner condition that made orders 86 and 92 affordable, and Section 9 the published material that was transcribed and re-verified. Section 11 describes the formal verification.

2. Preliminaries

2.1. **Blocks, systems, colourings.** Throughout, points are the integers $0, 1, \ldots, v-1$, identified with $\mathbb{Z}_v$ when a cyclic structure is in play, and a block is a strictly increasing list of them. We write B for a block list, $D_x(B)$ for the derived design at x, and $P = (C_1, \ldots, C_r)$ for a colouring. Formally: B is an $\mathrm{SQS}(v)$ when every member is a 4-subset of $[0, v)$ and the multiset of 3-subsets covered by the members of B is exactly the set of all 3-subsets of $[0, v)$; P is an r-colouring of D when each C_i is a partial parallel class and the C_i partition D as a multiset.

2.2. **The counting bound.** The only inequality we ever use for a lower bound is the following, and it holds for every triple system, with no design data entering.

Lemma 2.1. *Let D be a list of triples drawn from $[0, n)$ and let P be a colouring of D into partial parallel classes. Then $|D| \le |P| \cdot \lfloor n/3 \rfloor$.*

Proof. A partial parallel class of triples on n points is a set of pairwise disjoint 3-sets inside an n-set, so it has at most $\lfloor n/3 \rfloor$ members. Summing over the classes and using that they partition D gives the bound. □

Applied to a derived design of an $\mathrm{SQS}(v)$ with $v \equiv 2 \pmod 6$, Lemma 2.1 forces the number of colours immediately. The derived design lives on $v-1$ points, but we state the bound with the ambient v, which is harmless and avoids a relabelling: $v \equiv 2 \pmod 3$ gives $\lfloor v/3 \rfloor = \lfloor (v-1)/3 \rfloor$ at all orders considered here.

Proposition 2.2. *Let B be an $\mathrm{SQS}(v)$ and x a point. Then every colouring of $D_x(B)$ uses at least $v/2$ classes, for $v = 26, 38, 44, 62, 74, 86, 92$. Explicitly:*

$$\begin{array}{llll} v = 26: & 12 \cdot 8 = 96 < 100, & v = 38: & 18 \cdot 12 = 216 < 222, \\ v = 44: & 21 \cdot 14 = 294 < 301, & v = 62: & 30 \cdot 20 = 600 < 610, \\ v = 74: & 36 \cdot 24 = 864 < 876, & v = 86: & 42 \cdot 28 = 1176 < 1190, \\ v = 92: & 45 \cdot 30 = 1350 < 1365. & & \end{array}$$

Proof. The derived design of an $\mathrm{SQS}(v)$ has $(v-1)(v-2)/6$ blocks, which is the right-hand number in each line; the left-hand product is $(v/2-1)\lfloor v/3 \rfloor$. By Lemma 2.1 a colouring with $v/2-1$ classes could cover at most the left-hand number of blocks. □

Since the colourings of §4 attain $v/2$ at each of these orders, they are minimum colourings, and no appeal to (1) is needed anywhere.

Remark 2.3. The notion of minimum colourability used throughout, and formalised, is the certified one: a triple system D on v points is *minimum colourable with r colours* when it has an r-colouring *and* $r-1$ colours are excluded by the bound of Lemma 2.1, i.e. $|D| > (r-1)\lfloor v/3 \rfloor$. At every order treated here the counting bound is tight, so this coincides with minimality; stating it this way is what stops the property from being satisfiable by an arbitrary colouring, and the second conjunct is checked to be load-bearing (Proposition 9.4).

At order 44 this also re-proves a known value of the chromatic index from scratch.

Proposition 2.4. $\chi'(43) = 22$*. The lower bound is Lemma 2.1 applied to an* $\mathrm{STS}(43)$*, which has* 301 *blocks on* 43 *points:* $21 \cdot \lfloor 43/3 \rfloor = 294 < 301$*. The upper bound is the* 22*-colouring of Theorem 4.2.*

2.3. **Cyclic systems and multipliers.** A block list B over $\mathbb{Z}_v$ is *cyclic* when $x \mapsto x+1$ permutes it, and an integer m prime to v is a *multiplier* when $x \mapsto mx$ permutes it as well. All designs below are obtained by *developing* a list of base blocks: taking all v translates of each and discarding duplicates. Cyclicity is the load-bearing property of the whole construction, for a reason worth stating separately.

Lemma 2.5. *Let B be a cyclic* $\mathrm{SQS}(v)$ *and let P be an r-colouring of $D_0(B)$. Then the translate of P by x is an r-colouring of $D_x(B)$, for every point x. In particular B is an* $\mathrm{mcDSQS}(v)$ *as soon as $D_0(B)$ has a colouring of the size forced by Proposition 2.2.*

Proof. Translation by x is an automorphism of B carrying $D_0(B)$ onto $D_x(B)$ bijectively, and it preserves disjointness of triples, so it carries partial parallel classes to partial parallel classes and partitions to partitions. □

In the formal development the conclusion of Lemma 2.5 is not taken on trust: the translated colouring is checked, as a partition into partial parallel classes, at each of the v points separately. The lemma explains why one colouring suffices; the verification does not use it.

If m is a multiplier and $m \cdot 0 = 0$, then $\sigma \colon x \mapsto mx$ restricts to an automorphism of $D_0(B)$, and one may look for colourings whose classes σ permutes. This is the *equivariant* restriction; §6 says what it costs and what it buys.

2.4. **Holes and the deficiency identity.** The following identity is elementary and is the whole reason the encoding of §5 works. Write $n \equiv 2 \pmod 6$ and consider a colouring of an $\mathrm{STS}(n-1)$ into exactly $n/2$ classes, with class sizes $s_1, \ldots, s_{n/2}$.

Lemma 2.6. *Each point of the* $\mathrm{STS}(n-1)$ *is missed by exactly one class, a class of size s misses exactly $(n-1) - 3s$ points, and writing $s_c = \lfloor (n-1)/3 \rfloor - e_c$ one has*

$$\sum_c \bigl(1 + 3e_c\bigr) \;=\; n-1 \qquad \textit{and} \qquad \sum_c e_c \;=\; \frac{n-2}{6}.$$

Proof. A point of an $\mathrm{STS}(n-1)$ lies in $(n-2)/2 = n/2 - 1$ blocks, and those blocks pairwise meet, so they lie in $n/2 - 1$ distinct classes: the point is missed by exactly one of the $n/2$ classes. A class of s pairwise disjoint triples covers $3s$ of the $n-1$ points and misses the rest; summing the missed counts over classes counts each point once, giving $\sum_c \bigl((n-1) - 3s_c\bigr) = n-1$. Writing $n = 6m+2$ we have $\lfloor (n-1)/3 \rfloor = 2m$ and $n/2 = 3m+1$, so $\sum_c s_c = (n-1)(n-2)/6 = m(6m+1)$ gives $\sum_c e_c = (3m+1) \cdot 2m - m(6m+1) = m = (n-2)/6$. Substituting $s_c = 2m - e_c$ into the missed-count identity gives the first display. □

We call $(e_c)_c$, as a partition of $(n-2)/6$, the *deficiency profile* of the colouring. The single partition $(n-2)/6 = (n-2)/6$ — all classes full except one — is what a *Hanani triple system* would give: $n/2 - 1$ almost parallel classes of $\lfloor (n-1)/3 \rfloor$ triples together with one short class. Section 7 shows it is not what happens.

3. The designs

All designs in this paper are cyclic and are given by base blocks over $\mathbb{Z}_v$. Under $x \mapsto x+1$ a quadruple of $\mathbb{Z}_v$ has orbit length $v/|S|$ where S is its setwise stabiliser, a subgroup of $\mathbb{Z}_v$ of order dividing 4; counting blocks then constrains the orbit structure before any search begins, and the constraint was used both as a search restriction and as a check on the implementation.

Proposition 3.1 (Orbit arithmetic)**.** *Let B be a cyclic* $\mathrm{SQS}(v)$ *with k orbits of length v, h of length $v/2$ and q of length $v/4$ (the last only when $4 \mid v$). Then:*

(1) $v = 44$*: $44k + 22h + 11q = 3311$ with $q \le 1$ forces $q = 1$, so $\{0, 11, 22, 33\}$ is a block of every cyclic* $\mathrm{SQS}(44)$*, and h is even.*
(2) $v = 62$*: $62k + 31h = 9455$ forces h odd, so a block $\{a, a+31, b, b+31\}$ is present.*
(3) $v = 74$*: $74k + 37h = 16206$ forces h even.*
(4) $v = 86$*: $86k + 43h = 25585$, i.e. $2k + h = 595$, forces h odd.*
(5) $v = 92$*: $92k + 46h + 23q = 31395$, i.e. $4k + 2h + q = 1365$, forces q odd, so a quarter orbit $\{a, a+23, a+46, a+69\}$ is present.*

Proof. Each is a parity or divisibility statement about the displayed linear equation, whose right-hand side is $v(v-1)(v-2)/24$. The classification of possible orbit lengths — which is the step that identifies the shapes $\{a, a+v/2, b, b+v/2\}$ and $\{a, a+v/4, a+v/2, a+3v/4\}$ — is a computation over $\mathbb{Z}_v$ carried out outside the formal development; what is proved formally is the arithmetic it feeds. ☐

Order 92 is the first order in this campaign at which $\mathbb{Z}_v$ has a subgroup of order 4, so it is the first at which a quarter orbit exists; that it is then *forced* has a visible consequence in the colouring, namely that the derived design at 0 contains the triple $\{23, 46, 69\}$, which is the unique block fixed by the multiplier.

The designs themselves were produced by dancing-links search on the exact cover whose columns are the translation orbits of triples and whose rows are the orbits of quadruples, restricted to rows invariant under a chosen multiplier. Restricting to a multiplier collapses the cover dramatically and is what makes the design side cheap; the restriction is a search device only, and every claim below is verified of the resulting block list itself.

Proposition 3.2. blocks$_{44}$*, the development of* 81 *base blocks over* $\mathbb{Z}_{44}$*, is a cyclic* SQS(44) *with* 3311 *blocks;* $x \mapsto 5x$*, of order* 5 *in* $(\mathbb{Z}/44)^*$ *with* $\langle 5\rangle = \{1, 5, 9, 25, 37\}$*, is a multiplier, and* $x \mapsto 3x$*, of order* 10*, is not.*

Remark 3.3. Outside the formal development, an exhaustive dancing-links search over the cover restricted to designs invariant under a multiplier of order 10 terminates with no solution in 23 search nodes: no cyclic SQS(44) admits such a multiplier. This is a complete search, but it is a complete search of a program's state space rather than a kernel-checked exhaustion, and it is recorded here as a measurement. It matters only because it shows $\langle 5\rangle$ is the largest usable multiplier group at this order, so the recipe that worked at order 38 — where $x \mapsto 7x$ has order 3 — does not transport unchanged.

Proposition 3.4. (1) blocks$_{50}$*, developed from* 98 *base blocks, is a cyclic* SQS(50) *with* 4900 *blocks and multiplier* $x \mapsto 11x$ *of order* 5*; its derived designs are* STS(49)*s with* 392 *blocks, and* 25 *colours are forced.*

(2) blocks$_{62}$*, developed from* 155 *base blocks (*150 *orbits of length* 62 *and* 5 *of length* 31*), is a cyclic* SQS(62) *with* 9455 *blocks and multiplier group* $\langle 33\rangle = \{1, 33, 35, 39, 47\}$ *of order* 5*; its derived designs are* STS(61)*s with* 610 *blocks, and* 31 *colours are forced.*

(3) blocks$_{74}$*, developed from* 219 *base blocks (all orbits of full length), is a cyclic* SQS(74) *with* 16206 *blocks and multiplier group* $\langle 27\rangle$ *of order* 6*; its derived designs are* STS(73)*s with* 876 *blocks, and* 37 *colours are forced.*

Proof. In each case the block count, the Steiner condition, the invariance under $x \mapsto x+1$ and the invariance under the stated multiplier are finite checks on an explicit block list and were carried out by compiled evaluation inside the proof assistant; the derived-design block counts are a further finite check at all v points; the forced number of colours is Proposition 2.2, which has no data in it. Negative controls accompany each: at order 62 the map $x \mapsto 5x$ of order 3 is checked *not* to be a multiplier, and at order 74 the map $x \mapsto 5x$ likewise, so the multiplier group is the stated one and not all of $(\mathbb{Z}/v)^*$. ☐

The designs at orders 86 and 92 are new to this development but, as explained in §1, not to the literature; they are stated together with their colourings in Theorems 4.5 and 4.6.

4. The main theorems

Each theorem in this section has the same shape: an explicit cyclic SQS(v), an explicit colouring of its derived design at the point 0 into $v/2$ partial parallel classes, and the verification that the translate of that colouring colours the derived design at each of the v points. Proposition 2.2 supplies minimality, with no data and no appeal to (1). We describe the searches in §5; the theorems themselves rest on the exhibited objects, not on the searches that produced them.

Theorem 4.1. *An* mcDSQS(38) *exists. Specifically, the cyclic* SQS(38) *published as the entry* $C(38, 4, 3)$ *of the La Jolla Covering Repository* [9] *and shipped in Sage* [11] *has a* 19*-colouring of its derived* STS(37) *at every one of its* 38 *points, and* 19 *is the least possible. This answers the* mcDSQS(38) *half of Problem 1.3, and settles the smallest order at which Conjecture 1.2 was open. A second* mcDSQS(38)*, on a design searched out here rather than taken from a repository, is exhibited alongside it.*

Theorem 4.2. *An* mcDSQS(44) *exists. The design* blocks_{44} *of Proposition 3.2 has a* 22*-colouring of its derived* STS(43) *at every one of its* 44 *points, with class sizes* $14^{20}\,11\,10$*, and* 22 *is the least possible. A second* mcDSQS(44) *on an independently searched cyclic* SQS(44) *is exhibited alongside it.*

Theorem 4.3. *An* mcDSQS(62) *exists. The design* blocks_{62} *of Proposition 3.4 has a* 31*-colouring of its derived* STS(61) *at every one of its* 62 *points, with class sizes* $20^{26}\,18^{5}$*, and* 31 *is the least possible. A second* mcDSQS(62) *is exhibited on an independently searched cyclic* SQS(62)*, whose colouring has the same class sizes.*

Theorem 4.4. *An* mcDSQS(74) *exists. The design* blocks_{74} *of Proposition 3.4 has a* 37*-colouring of its derived* STS(73) *at every one of its* 74 *points, with class sizes* $24^{31}\,22^{6}$*, and* 37 *is the least possible. A second* mcDSQS(74) *is exhibited on an independently searched cyclic* SQS(74)*; its colouring has class sizes* $24^{31}\,23^{3}\,21^{3}$*.*

Theorem 4.5. *An* mcDSQS(86) *exists. The development* blocks_{86} *of* 301 *base blocks over* $\mathbb{Z}_{86}$ *—* 294 *orbits of length* 86 *and* 7 *of length* 43*, the odd number of short orbits forced by Proposition 3.1 — is a cyclic* SQS(86) *with* 25585 *blocks, invariant under the multiplier group* $\langle 11\rangle = \{1, 11, 21, 35, 41, 47, 59\}$ *of order* 7*, and it has a* 43*-colouring of its derived* STS(85) *at every one of its* 86 *points, with class sizes* $28^{36}\,26^{7}$*.* 43 *is the least possible. A second* mcDSQS(86) *is exhibited alongside it.*

Theorem 4.6. *An* mcDSQS(92) *exists. The development* blocks_{92} *of* 342 *base blocks over* $\mathbb{Z}_{92}$ *—* 341 *orbits of length* 92 *and one of length* 23*, a quarter orbit forced by Proposition 3.1 — is a cyclic* SQS(92) *with* 31395 *blocks, invariant under the multiplier group* $\langle 9\rangle$ *of order* 11*, and it has a* 46*-colouring of its derived* STS(91) *at every one of its* 92 *points, with class sizes* $30^{44}\,23\,22$*.* 46 *is the least possible. A second* mcDSQS(92) *is exhibited alongside it.*

Proof of Theorems 4.1–4.6, and of Theorem 1.4. For each order, the following are finite checks on explicit block lists and were performed by compiled evaluation inside the proof assistant. (i) Every member of the block list is a 4-subset of $[0, v)$ and the multiset of covered triples is exactly the set of all $\binom{v}{3}$ triples — so the list is an SQS(v); the numbers of covered triples are 8436, 13244, 37820, 64824, 102340 and 125580 at $v = 38, 44, 62, 74, 86, 92$. At orders 86 and 92 this check goes through the near-linear route of Theorem 8.1 rather than through the sorting predicate directly. (ii) The list is invariant under $x \mapsto x + 1$ and under the stated multiplier. (iii) The derived design at each of the v points has $(v-1)(v-2)/6$ blocks. (iv) Each class of the exhibited colouring is a partial parallel class, and for each of the v points, the translate of the colouring by that point is a partition of the derived design there into partial parallel classes of triples inside $[0, v)$. Minimality of the number of classes is Proposition 2.2, which is proved for arbitrary input. The two designs at each order are proved distinct by exhibiting a block that lies in one and not in the other.

The finite searches behind the data are described in §5; nothing in the proofs depends on them. What the proofs do depend on exhaustively is item (iv), which is a check at all v points — $62 + 74 + 86 + 92 = 314$ point checks for the first designs at the four largest orders alone, and as many again for the second designs. □

Remark 4.7. The two designs at each order are genuinely different objects, not relabellings. Beyond the exhibited distinguishing block, which is what the formal development checks, a direct comparison outside it gives the number of shared blocks: 0 of 9455 at order 62 — the two designs at that order have no block in common at all — against 76 of 2109 at 38, 1111 of 3311 at 44, 2220 of 16206 at 74, 602 of 25585 at 86 and 1035 of 31395 at 92. Order 38 carries a third design, the further cyclic SQS(38) of Proposition 9.2, and it too shares exactly 76 blocks with the published one; the three designs are pairwise distinct and have no block common to all three. The same comparison shows that the second design at each of the orders 62, 74, 86 and 92 is invariant under the multiplier group of Table 1, as the search that produced it forced. Inside the formal development that invariance is checked for both designs at orders 38 and 44 but only for the first design at 62, 74, 86 and 92; the second designs at those four orders are checked to be cyclic, which is all any proof below uses.

5. The encoding

This section describes how the colourings were found. It is the part of the work we expect to transfer, and the reason is that the difficulty at orders 62 and 74 turned out to be an artefact of how the problem was written down rather than a property of the problem.

5.1. **The state before.** An earlier round of work settled the design half at orders 62 and 74 and recorded the colouring half as an open, measured search failure. The search log is unambiguous and is worth reproducing, because it is what makes the fix interesting:

- At order 62: sixty distinct cyclic SQS(62)s, each searched by a multiplier-equivariant insertion walk — Stinson's hill-climbing move for triple systems [13], adapted so that every colour class stays a partial parallel class throughout — at 1.2×10^6 moves and 10 restarts. *None solved.* Forty-seven stalled with two orbits of blocks unplaced out of 122, thirteen with one. The thirteen near misses, re-run with many more seeds at a larger budget, still did not close.
- The same instances by dancing links on a block-to-class exact cover, by a plain SAT encoding, by a clause-weighting variant of the walk, and by a hybrid that drops equivariance after a first phase and then repairs at the level of individual blocks: the hybrid got closest, leaving 4 blocks of 610 unplaced over 46 runs, and none closed.
- At order 74: three seeds at 2×10^6 moves and 20 restarts, not solved.
- A derived symmetry break pinning six items, cutting the space by a factor of about 1.1×10^7, gave no improvement — the expected behaviour for local search, which loses freedom without gaining information.

Five distinct methods stalling in the same place is evidence that the move is wrong rather than that the budget is small, and none of these negatives was ever read as a non-existence proof.

5.2. **The hole partition, made explicit.** Lemma 2.6 says that a minimum colouring carries a second combinatorial structure alongside the assignment of blocks to classes: the map sending each point to the unique class that misses it. Call it the *hole partition*. Its parts are the missed sets, of sizes $1 + 3e_c$, and they partition the $n - 1$ points.

Every method listed above represents only the block-to-class assignment and lets the hole partition emerge. A local search then cannot see it: its objective counts unplaced blocks, and two assignments with the same number of unplaced blocks are indistinguishable to it even when one has a hole structure that can be completed and the other has not. That is a plateau, not a budget problem, and indeed the identical stall signature appears on instances that are *satisfiable* — the STS(37) at 19 colours, where a solution provably exists by Theorem 4.1, stalls the same way.

The encoding used here adds Boolean variables miss$[c][x]$ for "class c misses point x", tied to the block variables in both directions, together with

- every point is missed by exactly one class, and
- class c misses exactly $1 + 3e_c$ points, over an enumerated deficiency profile $(e_c)_c$ of $(n-2)/6$ as in Lemma 2.6.

The profile enumeration is what makes the constraint usable: the number of partitions of $(n-2)/6$ is small at these orders (10, 12, 14, 15 have 42, 77, 135 and 176 partitions respectively, and admissibility conditions cut this much further), so one may branch over profiles and give the solver a fully determined hole structure in each branch.

5.3. **What it measures.** The figures in this subsection are the solve times recorded in the search log, on one machine and without repetition; they are reported, not re-measured. The driver scripts of those runs were not completely archived alongside the witness data — the script that enumerates candidate block sets from a hole partition was overwritten before it could be preserved — so the searches are not replayable from the artefacts as they stand, and the times below should be read as orders of magnitude rather than benchmarks. What does not depend on them is the mathematics: the witnesses themselves were re-verified in full, twice and independently (§11), and no theorem in this paper rests on a search. With that said, the instance that sixty designs at 1.2×10^6 moves each could not close is closed by a SAT solver on this encoding in 23 seconds, and the calibration runs that make this more than an anecdote are:

- **A positive control at a settled order.** Order 44, whose colouring is known (Theorem 4.2), is solved in 0.84 seconds, and six deficiency profiles are refuted along the way.
- **A negative control at an order that is provably blocked.** Order 50 returns unsatisfiable on all twelve admissible profiles, in agreement with Theorem 6.2 below, which was proved independently.
- **The calibration that matters.** A 19-colouring of an STS(37) is found *with no symmetry restriction at all* in 16 seconds — on the instance where a tabu colouring heuristic, a pairwise SAT encoding and exact-cover dancing links had all failed, and which previously required restricting to colourings invariant under the multiplier. Equivariance is therefore now optional rather than necessary.
- Twelve further cyclic SQS(62)s were coloured in 2 to 17 seconds each; order 74 took 66 seconds, order 86 about 30, order 92 about 132.

The conclusion we draw is narrow and, we think, safe: the negative results recorded at orders 62 and 74 were about an encoding, not about the objects, and the objects were there the whole time. The same reading applies retrospectively at order 38, where the first attempt at the colouring failed on generic colouring heuristics and succeeded only after two changes of move — and where the present encoding needs neither.

6. Equivariance: what it buys, and where it is fatal

Restricting a colouring search to colourings that the multiplier permutes is a smaller search, and a smaller search that still contains a solution is strictly better. It can also contain none, and at one order it provably does. This section records both, because the negative result is a real theorem about the method and because it is the control that the encoding of §5 is calibrated against.

Fix a cyclic SQS(n) with a multiplier m and put $\sigma\colon x \mapsto mx$, an automorphism of the derived design at 0. Let F be the number of σ-fixed points of that derived design and K the number of σ-fixed blocks. If σ has prime order $p \geq 5$ then a σ-fixed block is a triple of fixed points, since a 3-set orbit has size dividing both p and 3. A σ-fixed colour class then misses a σ-invariant set of points, and one counts as follows.

Proposition 6.1. *With the notation above and σ of prime order $p \geq 5$, let f be the number of σ-fixed colour classes in a σ-equivariant minimum colouring, and let the i-th of them contain k_i of the K fixed blocks. Then $F \cdot f = F + 3K$, i.e. $f = 1 + 3K/F$.*

Proof. A class containing a block orbit of size p that met a fixed point would put that point in all p blocks of the orbit, contradicting disjointness; so a σ-fixed class sees fixed points only through σ-fixed blocks, and one containing k_i of them misses exactly $F - 3k_i$ fixed points. Every fixed point is missed by exactly one class, and the class missing it is itself σ-fixed, so $\sum_i(F-3k_i)=F$, i.e. $Ff-3K=F$. □

Theorem 6.2. *No σ-equivariant minimum colouring of a derived design of an $\langle 11\rangle$-invariant cyclic* SQS(50) *exists.*

Proof. $(\mathbb{Z}/50)^*$ is cyclic of order 20, so $\langle 11\rangle$ of order 5 is its only subgroup of odd prime order, and $\sigma\colon x\mapsto 11x$ fixes the subgroup $H=\{0,5,10,\dots,45\}$ of order 10. In the multiplier-restricted exact cover, of the rows meeting a column whose triples lie inside H, all 19 have their quadruple inside H and none does not — so every such design contains a sub-SQS(10) on H, and its derived design at 0 has exactly $K=12$ fixed blocks, forming an STS(9) on the $F=9$ fixed points. (This last statement is verified of the exhibited design; the forcing step is the cover computation, done outside the formal development, and confirmed on 40 of 40 sampled designs.) Proposition 6.1 gives $f=5$. A fixed class holding k_i fixed blocks has $k_i\le 3$, misses $9-3k_i$ fixed points, and its missed set has size $1+3e_i$ with $1+3e_i\equiv 9-3k_i \pmod 5$ and $9-3k_i\le 1+3e_i$; case analysis on $k_i\in\{0,1,2,3\}$ gives $e_i\ge 6-k_i$ in every case. Summing over the five fixed classes,

$$\sum_i e_i \;\ge\; 6\cdot 5-\sum_i k_i \;=\; 30-12 \;=\; 18,$$

against the total budget $\sum_c e_c=(50-2)/6=8$ of Lemma 2.6. The gap is more than a factor of two and does not depend on how the twelve fixed blocks are distributed. □

Theorem 6.2 rules out the equivariant *search* at order 50, not an mcDSQS(50): a colouring that σ does not permute is untouched by it, as is any non-cyclic design. The culprit it names is cheap to test in advance — $\gcd(m-1,n)$ large enough that the fixed set carries a subsystem — and the same test passes comfortably at the orders settled here.

Proposition 6.3. *At $n=62$ with $\sigma\colon x\mapsto 33x$ one has $F=1$: the fixed set of σ in $\mathbb{Z}_{62}$ is $\{0,31\}$, so the derived design at 0 has the single fixed point 31. Hence $K=0$ is forced with no design data, since a fixed block would be a triple of fixed points and there is only one; and $f=1$ with forced total deficiency 0, against a budget of $(62-2)/6=10$. In particular the obstruction of Theorem 6.2 cannot occur at this order: the fixed set has two points and no sub-*SQS *has fewer than four.*

At $n=74$ the relevant multiplier acts on the derived design with order 3, so Proposition 6.1 does not apply — its derivation needs prime order at least 5, and at $p=3$ the formula would give the wrong answer, namely $f=37$. We record, as an unformalised remark, that the correct conclusion $f=1$ still holds by a different argument: no block through the fixed point 37 is σ-fixed, so the 36 blocks through it fall into 12 orbits of length 3 permuted in 3-cycles, leaving exactly the class that misses 37 fixed. Unlike Propositions 6.1 and 6.3, this argument is not part of the formal development; nothing else in the paper depends on it.

So both open orders passed the method's own criterion, and both nevertheless resisted the equivariant search. That is precisely the discrepancy the encoding of §5 resolves, and it is worth stating plainly what it means for the record: the criterion is a genuine necessary condition for the equivariant route, and it is not a predictor of search difficulty.

7. Deficiency profiles

Lemma 2.6 says the deficiencies of a minimum colouring form a partition of $(n-2)/6$. It is natural to guess that the extremal partition — all classes full but one, the Hanani profile — is the one to aim at, both because Hanani triple systems are how the upper bound (1) is proved in the first place and because the resulting structure is the most rigid. The evidence here says otherwise, in two independent ways.

Proposition 7.1. *The colourings exhibited in Theorems 4.1–4.6 realise the deficiency profiles*

$$\begin{aligned}
n = 38:&\quad 6 = 3+1+1+1 \ \textit{ and } \ 6 = 2+2+2,\\
n = 44:&\quad 7 = 4+3 \quad (\textit{both designs}),\\
n = 62:&\quad 10 = 2+2+2+2+2 \quad (\textit{both designs}),\\
n = 74:&\quad 12 = 2+2+2+2+2+2 \ \textit{ and } \ 12 = 1+1+1+3+3+3,\\
n = 86:&\quad 14 = 2+2+2+2+2+2+2 \quad (\textit{both designs}),\\
n = 92:&\quad 15 = 7+8 \quad (\textit{both designs}).
\end{aligned}$$

None of them is the Hanani profile $(n-2)/6 = (n-2)/6$, and at each of $n = 38$ and $n = 74$ two designs of the same order realise two different partitions.

Proof. The class sizes are read off the exhibited colourings, and the identity $s_c = \lfloor (n-1)/3 \rfloor - e_c$ of Lemma 2.6 converts them into deficiencies. The class-size lists are finite data; eleven of the twelve are verified by kernel evaluation in the formal development, and the twelfth, that of the second design at order 44, is read off its exhibited colouring, which the development carries in full. □

The pattern is not new with these orders. The minimum colourings printed in the literature are also non-Hanani: the derived STS(19) of the cyclic SQS(20) printed in [12, §4.3] has sizes $6^8\,5\,4$, deficiency profile $3 = 1+2$; and the derived STS(25) and STS(31) of the mcDSQS(26) and mcDSQS(32) printed in [14, Appendix B] have sizes $8^{11}\,6^2$ and $10^{13}\,9\,8^2$, profiles $4 = 2+2$ and $5 = 1+2+2$. These three lists were counted off the printed partitions in the sources; the block totals 57, 100 and 155 and the deficiency sums 3, 4 and 5 all check, and for the STS(25) the sizes agree with the transcribed data of Proposition 9.1.

So “minimum colourable” and “has a Hanani profile” are different properties, and aiming a search at the Hanani profile aims at the wrong object. It is worth adding what the right prior about minimum colourability itself is: the chromatic index of *every* Steiner triple system of order 19 is known [4], and all but 4077 of the 11 084 874 829 of them attain $\chi'(19) = 10$. Minimum colourable triple systems are common; what is hard is finding a quadruple system whose v derived designs are minimum colourable simultaneously, and — as §5 argues — knowing how to look. Whether any derived design occurring here admits a Hanani-profile minimum colouring at all is open; the question was probed at order 38 and the probe separated nothing, since at the same budget the unrestricted instance — which is satisfiable — also failed.

8. A near-linear test for the Steiner condition

The verification of item (i) in the proof of Theorems 4.1–4.6 is a multiset equality between the $\binom{v}{3}$ triples covered by the blocks and the $\binom{v}{3}$ triples of $[0, v)$. Comparing them by sorting with an algorithm that a proof kernel can evaluate is quadratic in $\binom{v}{3}$, and $\binom{v}{3}$ grows fast: from 13244 at $v = 44$ to 125580 at $v = 92$. Measured, that check took about two minutes at order 44 and about half an hour at each of orders 62 and 74; the same cost model priced it at roughly 80 minutes at order 86 and two hours at order 92, which is what made those orders unaffordable. The following removes the obstacle.

For $t = [a_1, \ldots, a_k]$ a list of points in $[0, v)$ write $\mathrm{key}_v(t)$ for its value in base-v positional notation, $\mathrm{key}_v(t) = \sum_i a_i v^{k-i}$.

Theorem 8.1. *Let B be a list of blocks such that every member is a 4-subset of $[0, v)$, and suppose the sorted list of base-v keys of the triples covered by B equals the sorted list of base-v keys of all triples of $[0, v)$. Then B is an* SQS(v).

Proof. Three steps. First, key_v is injective on lists of one fixed length with entries below v: base-v digits are recovered by division, which is proved from the recursion $\mathrm{key}_v(a :: t) = a \cdot v^{|t|} + \mathrm{key}_v(t)$ and the bound $\mathrm{key}_v(t) < v^{|t|}$ for such t. Second, insertion sort by key produces a list that is pairwise ordered by key. Third, therefore, sorting by key is a canonical form on lists of fixed-length bounded entries: two such lists that are permutations of each other have equal sorted forms, because one may map both sorted outputs to their key lists, identify those two sorted lists of naturals by antisymmetry of $\leq$, and pull back along injectivity. The hypothesis gives the permutation, via the fact that a merge sort of a list is a permutation of it; the members of the triples covered by B and the members of the list of all triples are 3-subsets of $[0, v)$, which is what feeds injectivity. □

The point of Theorem 8.1 is that its conclusion is the unmodified Steiner condition: only the decision procedure changes, from a quadratic insertion sort to one merge sort on each side, and the soundness argument is a piece of ordinary mathematics carrying no evaluation of its own. It was calibrated against the two orders that had already been checked the slow way, re-deriving the Steiner condition for the order-62 and order-74 designs through the new route and comparing the two development procedures directly; four negative controls accompany it — a design with a block deleted, a design with a base block corrupted, and a design tested against the wrong ambient order are all rejected. The measured effect is that the two calibration checks together, plus the controls, cost about six minutes where the two old checks alone cost about sixty-three; orders 86 and 92 then cost under seven minutes between them.

9. Published material, transcribed and re-verified

The following are not new results. They are recorded because the constructions above rest on some of them as data, and because transcription of block lists from papers, repositories and library code is exactly where silent errors enter.

Proposition 9.1. *The* 27 *base blocks and* 13 *colour classes printed by Tan and Zhou* [14] *do what they are said to do: the base blocks develop over* $\mathbb{Z}_{26}$ *to a cyclic* SQS(26) *with* 650 *blocks; the* 13 *classes, translated, colour its derived* STS(25) *at every one of the* 26 *points; and* 13 *is optimal by Proposition 2.2. Four of the base blocks lie in short orbits of length* 13*, as the paper's notation indicates.*

Proposition 9.2. *The* SQS(38) *hard-coded in Sage* [11] *as* `_SQS38`*, sourced there from the entry* $C(38, 4, 3)$ *of the La Jolla Covering Repository* [9]*, is a Steiner quadruple system with* 2109 *blocks, and it is* cyclic*, with* $x \mapsto 7x$ *(of order* 3*) a multiplier; neither source records this. Its affine automorphism group therefore has order at least* 114*. A second cyclic* SQS(38)*, searched out independently, is verified alongside it and is a different design.*

Cyclicity here is the load-bearing observation of Theorem 4.1: it is what makes the 38 derived designs translates of one another, so that one colouring settles all of them. We note in passing that the Sage docstring for this design describes it as being "on 14 points"; the data is correct and the docstring is not.

Proposition 9.3. *Every* SQS(38) *needs at least* 19 *colours on each of its derived designs (Proposition 2.2), and the published design of Proposition 9.2 has a* 20*-colouring of its derived* STS(37) *at every one of the* 38 *points. These two bracket its derived chromatic index to* $\{19, 20\}$*; the* 19*-colouring of Theorem 4.1 closes the bracket at* 19*.*

Proposition 9.4. *The Steiner predicate used throughout is validated by kernel evaluation alone, with no compiled evaluation in the trusted path, on the two smallest nontrivial Steiner quadruple systems* SQS(8) *(the affine geometry* $AG(3, 2)$*,* 14 *blocks) and* SQS(10) *(*30 *blocks). Negative controls refute a claim that is too strong (no* 18*-colouring at order* 38*, no* 12*-colouring at order* 26*) and one that is too weak (a colouring into* 20 *classes does not certify minimality; and dropping the disjointness requirement lets a single class containing all* 100 *triples pass the partition test, so that one colour would suffice). Corrupted base blocks and neighbouring ambient orders are rejected. Separately, the predicate is proved equivalent to the statement about multisets that the literature makes.*

Proposition 9.4 is the reason one predicate serves both the small kernel-evaluated cases and the large compiled ones: the predicate that compiled evaluation runs at orders 26 to 92 is itself validated by the kernel at orders 8 and 10.

10. Further directions

Three of them are concrete.

First, the other half of Problem 1.3 — an RDSQS(52), an SQS(52) all of whose derived designs are *resolvable* — is untouched here, and it is the harder half. Its derived designs are STS(51)s with 425 blocks, a partial parallel class there holds at most 17 triples, and $425 = 25 \cdot 17$: a resolution has exactly 25 parallel classes with no slack at all, where every minimum colouring above has $(n-2)/6$ units of slack to spend.

Second, two designs with few point orbits are already in print at orders this paper touches, and testing them is cheap for the same reason cyclicity is cheap here. Lu [10, Example 5.4] gives base blocks for an SQS(44) obtained as the orbit of $\{\infty, 0, 1, 37\}$ under $\mathrm{PSL}(2, 43)$ acting on the projective line $\mathbb{F}_{43} \cup \{\infty\}$, the classical construction of Carmichael; since $\mathrm{PSL}(2, 43)$ is 2-transitive on that line and preserves the design, the design is point-transitive, so all 44 of its derived designs are isomorphic and testing it costs a single chromatic-index computation. Kiermaier, Krčadinac and Wassermann [8, Theorem 2.2] construct a rotational SQS(92): their point set is $\mathbb{Z}_{91} \cup \{\infty\}$ and their design is a union of orbits of the group generated by $x \mapsto x + 1$ and $x \mapsto 4x$ on $\mathbb{Z}_{91}$, a group of order 546 isomorphic to $C_{91} \rtimes C_6$ that fixes ∞ and is transitive on $\mathbb{Z}_{91}$. Its two point orbits are $\{\infty\}$ and $\mathbb{Z}_{91}$, so testing that design costs two chromatic-index computations. Either would give a witness on a *published* design.

Third, the binding constraint has moved. With the test of Theorem 8.1 the verification cost is near-linear in $\binom{v}{3}$, and at the measured rate order 98 should cost about 1.2 times order 92; the design side is not in the way below 100 either [8]. What limits the campaign now is the colouring search. We also leave open, as at order 38, whether any derived design occurring here admits a minimum colouring with the Hanani profile at all.

11. Verification

Every statement in this paper has been formally verified in Lean 4 (toolchain `v4.32.0`) against *Mathlib*; the development is free of `sorry`. The archival reference for the development and for the witness data, together with acknowledgements and funding statements, is to be supplied at submission. The division of labour between reasoning and computation is as follows, and is deliberate.

The general mathematics carries no computational axiom at all: the counting bound (Lemma 2.1) and the forced colour counts (Proposition 2.2), the orbit arithmetic (Proposition 3.1), the equivariance criterion and the order-50 obstruction (Proposition 6.1, Theorem 6.2, Proposition 6.3), and the entire soundness argument for the near-linear Steiner test (Theorem 8.1) depend on no axioms beyond `propext`, `Classical.choice` and `Quot.sound` — several of them on strictly fewer. In particular, the near-linear test is a theorem about arbitrary inputs, so the new decision procedure introduces no new trusted component; only its *inputs* are evaluated.

What is delegated to compiled evaluation, through Lean's `native_decide`, is exactly the finite checks on explicit data listed in the proof of Theorems 4.1–4.6. At orders 86 and 92 the entire computational base of the main theorem is five evaluations: that the blocks are 4-subsets of the right range; that the covered-triple keys match those of all triples; that the translated colouring colours the derived design at all v points; that the derived designs have the right size; and that the translated classes consist of triples inside the range. At orders 62 and 74 the Steiner condition is instead checked by the older sorting predicate, which is kernel-validated at orders 8 and 10 (Proposition 9.4). The class-size lists behind Proposition 7.1 are checked by kernel evaluation, with no compiled step, at every order except for the second design at order 44, whose colouring the development carries but whose class sizes it does not separately state.

Independently of the proof assistant, the witness data for orders 62, 74, 86 and 92 — 19 design-and-colouring pairs — was re-checked by a separate implementation that develops each design from its base blocks, verifies the Steiner condition, and then at *every* point translates the colour classes and verifies that they are pairwise disjoint triples partitioning the derived design exactly. That implementation shares no code with the formal predicates. Every long data literal in the formal development was generated from the witness files by script and then parsed back out of the source and compared against them, so no block list or colour class was transcribed by hand. The two designs already present at orders 62 and 74 were confirmed identical, block for block and in the same order, to the corresponding witness files.

Orders 38 and 44 carry independent re-checks of the same kind, which additionally parse the base blocks and colour classes back out of the formal source text rather than out of the witness files.

The seven source files added for orders 62, 74, 86 and 92 took about 33 minutes of wall time in total on a 20-core machine under heavy competing load, at a peak resident size of about 4.1 gigabytes — essentially all of which is the cost of importing the library, the marginal cost of the largest file being about half a gigabyte.

References

[1] D. Bryant, C. J. Colbourn, D. Horsley and I. M. Wanless, *Steiner triple systems with high chromatic index*, SIAM J. Discrete Math. **31**(4) (2017) 2603–2611, doi `10.1137/17M1114338`; arXiv:1702.00521.

[2] Y. Chang, B. Fan, T. Feng, D. F. Holt and P. R. J. Östergård, *Classification of cyclic Steiner quadruple systems*, J. Combin. Des. **25**(3) (2017) 103–121, doi `10.1002/jcd.21530`.

[3] C. J. Colbourn, *Computing the chromatic index of Steiner triple systems*, Comput. J. **25** (1982) 338–339.

[4] C. J. Colbourn, A. D. Forbes, M. J. Grannell, T. S. Griggs, P. Kaski, P. R. J. Östergård, D. A. Pike and O. Pottonen, *Properties of the Steiner triple systems of order 19*, Electron. J. Combin. **17**(1) (2010), #R98.

[5] T. Feng and Y. Chang, *Constructions for cyclic 3-designs and improved results on cyclic Steiner quadruple systems*, J. Combin. Des. **19**(3) (2011) 178–201, doi `10.1002/jcd.20264`.

[6] M. J. Grannell, T. S. Griggs and A. Rosa, *Three-line chromatic indices of Steiner triple systems*, Australas. J. Combin. **21** (2000) 67–84.

[7] H. Hanani, *On quadruple systems*, Canad. J. Math. **12** (1960) 145–157.

[8] M. Kiermaier, V. Krčadinac and A. Wassermann, *Steiner 3-designs as extensions*, arXiv:2509.23483v1 (2025). No journal publication is recorded for this e-print; the theorem number cited in §10 is that of v1.

[9] La Jolla Covering Repository, entry $C(38, 4, 3)$, credited to Colin Barker, method "Steiner Quadruple System". The live site is no longer resolvable; the page survives in the Internet Archive (snapshot of 2021-10-21) and the repository has a permanent archive at `https://zenodo.org/doi/10.5281/zenodo.10779736`.

[10] X.-N. Lu, *Completely (quasi-)uniform nested Boolean Steiner quadruple systems*, J. Combin. Des. **34**(3) (2026) 139–156, doi `10.1002/jcd.22016`; arXiv:2509.06663. The example cited in §10 is Example 5.4 of v3 of the e-print; the same example is numbered 6.3 in v1.

[11] The Sage Developers, *SageMath*, module `sage/combinat/designs/steiner_quadruple_systems.py`, function `_SQS38` (retrieved 2026-08-22).

[12] M. Shi, Y. Xia and D. S. Krotov, *A family of diameter perfect constant-weight codes from Steiner systems*, J. Combin. Theory Ser. A **200** (2023) 105790, doi `10.1016/j.jcta.2023.105790`; arXiv:2212.00048.

[13] D. R. Stinson, *Hill-climbing algorithms for the construction of combinatorial designs*, in: C. J. Colbourn and M. J. Colbourn (eds.), *Algorithms in Combinatorial Design Theory*, Ann. Discrete Math. **26** (North-Holland Math. Stud. 114), North-Holland, Amsterdam, 1985, pp. 321–334, doi `10.1016/S0304-0208(08)72988-8`.

[14] Y. Tan and J. Zhou, *Steiner quadruple systems with minimum colorable derived designs: constructions and applications*, Des. Codes Cryptogr. **93**(10) (2025) 4117–4140, doi `10.1007/s10623-025-01677-x`; arXiv:2503.11934.

[15] S. A. Vanstone, D. R. Stinson, P. J. Schellenberg, A. Rosa, R. Rees, C. J. Colbourn, M. W. Carter and J. E. Carter, *Hanani triple systems*, Israel J. Math. **83** (1993) 305–319, doi `10.1007/BF02784058`.