Some new large sets of geometric designs of type \(LS[3][2, 3, 2^8]\)

Michael R. Hurley, Bal K. Khadka, Spyros S. Magliveras

Abstract: Let \(V\) be an \(n\)-dimensional vector space over \(\mathbb{F}_q\). By a geometric \(t\)-design over \(\mathbb{F}_q\), we mean a collection \(D\) of \(k\)-dimensional subspaces of \(V\), called blocks, such that every \(t\)-dimensional subspace \(T\) of \(V\) appears in exactly \(\lambda\) blocks in \(D\). A large set, \(LS[N][t, k, \lambda]\), of geometric designs, is a collection of \(N\) \(t\)-designs of \(\mathbb{F}_q\), with \(t\)-designs which partitions the collection \(\binom{V}{t}\) of all \(t\)-dimensional subspaces of \(V\). Prior to recent article [4] only large sets of geometric 1-designs were known to exist. However in [4] M. Braun, A. Kohnert, P. Östergard, and A. Wasserman constructed the world’s first large set of geometric 2-designs, namely an \(LS[3][2, 3, 2^8]\), invariant under a Singer subgroup in \(GL_8(2)\). In this work we construct an additional 9 distinct, large sets \(LS[3][2, 3, 2^8]\), with the help of lattice basis-reduction.

2010 MSC: 05B25, 05B40, 05E18

Keywords: Geometric \(t\)-designs, Large sets of geometric \(t\)-designs, \(t\)-designs over \(GF(q)\), Parallelisms, Lattice basis reduction, LLL algorithm.

1. Introduction

In this article we deal with large sets of geometric \(t\)-designs. By a geometric \(t\)-design we mean what earlier authors have called \(t\)-designs over a finite field, or designs on vector spaces. Geometric \(t\)-designs are the \(\mathbb{F}_q\)-analogs of ordinary \((v, k, \lambda)\) designs. The earliest mention of \(t\)-designs, although not using our terminology or notation, was by P.J. Cameron in 1974 [5, 6] and P. Delsarte in 1976 [7]. In 1987, S. Thomas [20] exhibited the first simple geometric 2-design, and in the 1990’s H. Suzuki [19], M. Miyakawa et al. [17], and T. Itoh [10] constructed new geometric 2-designs and families of such designs. In 1994, D.K. Ray-Chaudhuri and E.J. Schram [18] studied and constructed geometric \(t\)-designs from quadratic forms, allowing repeated blocks. For the first time, the latter authors also studied large sets of geometric \(t\)-designs.
M. Braun, A. Kerber and R. Laue [3] constructed in 2005 the first simple geometric 3-design. In 2013, Braun et al. [2] constructed the first example of a $q$-Steiner system, that is a simple, geometric $t$-design with $\lambda = 1$, namely a $2\cdot[2^{13}, 3, 1]$ design.

In a short recent arXiv preprint [8], and based on a probabilistic existence theorem of G. Kuperberg, S. Lovett and R. Peled in preprint [14], A. Fazeli, S. Lovett, and A. Vardy, appear to have proved the remarkable theorem that simple geometric $t$-designs exist for all values of $t$. This would be a $q$-analog of the famous theorem of L. Tierlinck for ordinary $t$-designs. It should be noted however, that the result in [8] is purely existential and there is no known efficient algorithm which can produce $t\cdot[q^n, k, \lambda]$ designs for $t > 3$. The authors present the following challenge:

**Problem 1.1.** Design an efficient algorithm to produce simple, non-trivial $t\cdot[q^n, k, \lambda]$ designs for large $t$, (say $t \geq 4$).

Of course, finding large sets of geometric $t$-designs is even harder than just finding geometric $t$-designs. Prior to recent article [4] only large sets of geometric 1-designs were known to exist. However in [4] M. Braun, A. Kohnert, P. Östergard, and A. Wasserman constructed the world’s first large set of geometric 2-designs, namely an LS$[3][2,3,2^8]$, invariant under a Singer subgroup in GL$(2)$.

In this paper we construct 9 distinct large sets LS$[3][2,3,2^8]$, all different from the large set constructed in [4]. The computation involved our APL package knuth for group theoretic matters, and various LLL variants in the NTL library, augmented by certain optimization techniques for parallel lattice basis reduction.

It should be noted that some of the recent work on geometric $t$-designs has been motivated by present day coding theoretic applications as discussed in [9] and [11].

2. Preliminaries

Let $V$ be an $n$-dimensional vector space over the field $\mathbb{F}_q$. If $U$ is a $j$-dimensional subspace of $V$, we say that $U$ is a $j$-subspace of $V$. If $X$ is a set and $0 \leq s \leq |X|$, $\binom{X}{s}$ denotes the collection of all subsets of cardinality $s$ of $X$.

A geometric $t\cdot[q^n, k, \lambda]$ design is a pair $(V, B)$ where $B$ is a multiset of $k$-subspaces of $V$, called blocks, such that any $t$-subspace $T$ of $V$ is contained in exactly $\lambda$ blocks. $(V, B)$ is said to be simple if $B$ is a set, i.e. if there are no repeated blocks.

In this paper we deal only with simple geometric designs, and the square brackets of the symbol $t\cdot[q^n, k, \lambda]$ will imply “geometric” in contrast to the round parentheses for an ordinary $t\cdot(v, k, \lambda)$ design.

We denote the collection of all $k$-subspaces of $V$ by $[v]_k$ and note that $|[v]_n| = \binom{n}{k}$, where $\binom{n}{k}_q$ is the well known Gaussian binomial coefficient, given by:

$$\binom{n}{k}_q = \frac{[n]_q!}{[k]_q![n-k]_q!}$$  \hspace{1cm} (1)

where for positive integer $r$,

$$[r]_q! := [1]_q[2]_q \cdots [r]_q, \text{ and } [j]_q := (1 + q + \cdots + q^{j-1}).$$  \hspace{1cm} (2)

Analogously to the case of ordinary $t\cdot(v, k, \lambda)$ designs, a geometric $t\cdot[q^n, k, \lambda]$ design $(V, B)$ is also an $s\cdot[q^n, k, \lambda]$ design for every $0 \leq s \leq t$ with:

$$\lambda_s = \lambda \binom{n-s}{t-s}_q \binom{k-s}{t-s}_q,$$  \hspace{1cm} (3)
Thus, a necessary condition for the existence of a \( t-[q^n,k,\lambda] \) design is that the \( \lambda_s \) given by the equations (3) must be integral for all \( 0 \leq s \leq t \).

By a *large set* \( LS[N][t,k,q^n] \) we mean a collection \( \mathcal{L} = \{(V,B_i)\}_{i=1}^N \) of simple \( t-[q^n,k,\lambda] \) designs where \( \{B_i\}_{i=1}^N \) is a partition of \( \binom{V}{k} \). We can immediately see that for a given large set \( LS[N][t,k,q^n] \), \( N \) can be expressed in terms of the other parameters as:

\[
N = \left\lfloor \frac{n-t}{k-t} \right\rfloor_q / \lambda, \tag{4}
\]

Two \( t-[q^n,k,\lambda] \) designs \( \mathcal{D} = (V,\mathcal{B}) \) and \( \mathcal{D}' = (V,\mathcal{B}') \) are said to be isomorphic if there exists \( \alpha \in GL_n(q) \) such that \( \mathcal{B}' = \mathcal{B}^\alpha \), that is, \( B^a \in B' \) for all \( B \in \mathcal{B} \), in which case we also write \( \mathcal{D}' = \mathcal{D}^\alpha \). If \( \mathcal{D}' = \mathcal{D} \), then \( \alpha \) is said to be an automorphism of \( \mathcal{D} \). The group of all automorphisms of \( \mathcal{D} \) is denoted by \( Aut(\mathcal{D}) \).

Let \( \mathcal{B} = \{B_i\}_{i=1}^N \) be the collection of designs in a large set \( \mathcal{L} \). A group \( G \leq GL_n(q) \) is said to be an automorphism group of \( \mathcal{L} \) if \( \mathcal{B}^g = \mathcal{B} \) for all \( g \in G \), that is, if \( B_i^g \in \mathcal{B} \) for all \( B_i \in \mathcal{B} \) and \( g \in G \). Equivalently, we say that a large set with this property is \( G \)-invariant. The group of all automorphisms of \( \mathcal{L} \) is denoted by \( \text{Aut}(\mathcal{L}) \). If the stronger condition holds, that \( \mathcal{B}^g = \mathcal{B} \) for all \( B_i \in \mathcal{B} \) and \( g \in G \), we say that the large set \( \mathcal{L} \) is \([G]\)-invariant.

In 1976, E.S. Kramer and D.M. Mesner [12] presented a theorem which provides necessary and sufficient conditions for the existence of an ordinary \( G \)-invariant \( t-(v,k,\lambda) \) design. Beginning with a given group action \( G[X] \), the authors define certain integer matrices, presently known as the Kramer-Mesner (KM) matrices. Roughly speaking such a matrix \( A_{t,k} \) is the result of fusing under \( G \) the incidence matrix between \( \binom{\mathcal{B}}{v} \) and \( \binom{\mathcal{B}}{k} \) where incidence is set inclusion (fused R.Wilson matrix). These matrices extend naturally to the case of a group \( G \leq GL_n(q) \) acting on \( AG_n(q) \) or \( PG_{n-1}(q) \), and provide necessary and sufficient conditions for the existence of geometric, \( G \)-invariant \( t-[q^n,k,\lambda] \) designs. We proceed to define these matrices in the context of geometric \( t \)-designs, and state the analog of the Kramer-Mesner theorem.

Let \( V \) be an \( n \)-dimensional vector space over \( \mathbb{F}_q \), and \( G \leq GL_n(q) \). Suppose that \( t \) and \( k \) are integers, \( 0 \leq t < k \leq n \), and consider the actions of \( G \) on \( \binom{V}{t} \) and \( \binom{V}{k} \) respectively, with corresponding \( G \)-orbit decompositions:

\[
\binom{V}{t} = \Delta_1 + \Delta_2 + \cdots + \Delta_{\rho(t)}, \tag{5}
\]

and

\[
\binom{V}{k} = \Gamma_1 + \Gamma_2 + \cdots + \Gamma_{\rho(k)}, \tag{6}
\]

where \( \rho(s) \) denotes the number of \( G \)-orbits on \( \binom{\mathcal{B}}{s} \). Just as in [12], it can be shown that for any fixed \( t \)-subspaces \( T, T' \in \Delta_1 \), we have that

\[
|\{K \in \Gamma_j : T \leq K\}| = |\{K \in \Gamma_j : T' \leq K\}|, \tag{7}
\]

that is, the number \( a_{t,k}(i,j) = |\{K \in \Gamma_j : T \leq K\}| \) is independent of the choice of a fixed \( T \in \Delta_1 \). The Kramer-Mesner matrix \( A_{t,k} \) is then defined as the \( \rho(t) \times \rho(k) \) matrix:

\[
A_{t,k} = (a_{t,k}(i,j)) \tag{8}
\]

Dually, for \( K \) fixed in \( \Gamma_j \), let \( b_{t,k}(i,j) := |\{T \in \Delta_1 : T \leq K\}| \), and define the dual KM matrix \( B_{t,k} \) by:

\[
B_{t,k} = (b_{t,k}(i,j)) \tag{9}
\]

In the following Lemma we state without proof geometric analogs of some properties of the \( A_{t,k} \) and \( B_{t,k} \) as included for the ordinary \( t \)-design context in [13].

**Lemma 2.1.** Let \( A_{t,k} \) and \( B_{t,k}, \Delta_i, \Gamma_j \) be as defined above.
(i) If \( t \leq s \leq k \leq n \), then 
\[
[k-t]_{k-s} q \cdot A_{t,k} = A_{t,s} \cdot A_{s,k}
\]

(ii) \( A_{t,k} \) has constant row sums 
\[
[s-t]_{k-t} q
\]

(iii) \( |\Delta_i| \cdot A_{t,k}(i,j) = |\Gamma_j| \cdot B_{t,k}(i,j) \)

Keeping in mind that we are only interested in simple geometric \( t \)-designs, we now state, without proof, the Kramer-Mesner theorem for geometric \( t \)-designs:

**Theorem 2.2.** If \( G \leq GL_n(q) \), there is a \( G \)-invariant (simple) \( t \)-design if and only if there is a \( \rho(k) \times 1 \)-vector \( v \) which is solution of the matrix equation

\[
A_{t,k} v = \lambda J
\]

where \( J \) is the \( \rho(t) \times 1 \)-vector of all 1’s.

Here, the 1’s in a solution \( v \) select the \( G \)-orbits of \( V_k \) whose union will constitute the design. The following corollary follows immediately:

**Corollary 2.3.** There is a \( G \)-invariant large set \( LS[N][t,k,q^n] \) of geometric designs if and only if there exist \( N \) distinct solutions, \( u_1, \ldots, u_N \), to the matrix equation (10), whose sum is the \( \rho(k) \times 1 \) all 1’s vector.

3. Main result

It is well known that \( GL_n(q) \) has a cyclic subgroup of order \( q^n - 1 \), called a Singer subgroup, acting regularly on the non-zero vectors of \( V = F^n_q \). It is also known that all Singer subgroups are conjugate in \( GL_n(q) \). A Singer subgroup \( G \) of \( \Gamma = GL_8(2) \) is the centralizer of a Sylow-17 subgroup of \( \Gamma \) and its normalizer \( N \) in \( \Gamma \) is a split extension of \( G \) by its Frobenius group \( \Phi_8 \), thus \( |N| = 2040 \). In particular, for the rest of the paper we adopt the notation \( V = F_8^8 \), \( \Gamma = GL_8(2) \), and \( G = \langle \alpha \rangle \), where \( \alpha \) is the same Singer cycle as the one used in [4], that is:

\[
\alpha = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{bmatrix}
\]

We will presently construct 9 distinct large sets of geometric 2 - \( [2^8,3,21] \) designs which are \( [G] \)-invariant under Singer subgroup \( G \) of \( \Gamma \). We have used the exact same Singer subgroup \( G = \langle \alpha \rangle \) as in [4] so that it will be easy to check that our large sets are different from the one constructed in [4].

3.1. Computing and presenting \( A_{2,3} \)

Members of \( V_2 \) are Klein 4-groups, and those of \( V_3 \) elementary abelian groups of order 8. Viewed projectively, the 2- and 3-spaces can be seen as collinear triples and Fano planes respectively. There are in all 10795 2-spaces, and 97155 3-spaces.

We begin by computing the \( G \)-orbits on \( V_2 \) and \( V_3 \), where \( G = \langle \alpha \rangle \). There are exactly 43 \( G \)-orbits on \( V_2 \), all of which have length 255, except for one which has length 85. The short orbit is explained by
the fact that the cyclic subgroup of order 3 in $G$ fixes a collinear triple. There are 381 $G$-orbits on $\mathbb{F}_3^n$ all of length 255.

The vectors of $V = \mathbb{F}_3^n$ are represented by the radix-2 representation of integers in $\mathbb{Z}_{256}$. Orbits of 2- and 3-spaces are represented by the lexically smallest basis among all members of the orbit, but since $G$ is transitive on the non-zero vectors, each such basis will consist of the vector $1 \leftrightarrow 00000001$, and one (or two) elements of $\mathbb{Z}_{256} - \{1\}$. Hence, to represent $(\alpha)$-orbits of 2-spaces, it suffices to specify the second vector in the lexically minimal basis over all 2-spaces for that orbit. Thus, the $(\alpha)$-orbits of 2-spaces are represented by the following 43 integers:

$$2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 24, 28, 30, 32, 34, 36, 38, 40, 42, 44, 50, 54, 56, 58$$

$$60, 62, 70, 74, 76, 78, 80, 86, 88, 96, 100, 106, 114, 128, 136, 146, 164, 210, 218.$$ 

Similarly, orbit representatives of the 381 orbits of 3-spaces are given by the pair of integers in $\mathbb{Z}_{256}$ which together with 1, form the lexically minimal basis among the members of the orbit of 3-spaces. The pairs $x, y \in \mathbb{Z}_{256}$ representing the $G$-orbits on 3-spaces will appear in our display of the KM-matrix $A_{2,3}$ below.

To compute $A_{2,3}$, we found it easier to first compute matrix $B_{2,3}$ and then compute the $A_{2,3}(i,j)$ entries, using Lemma 2.1, equation (iii):

$$A_{2,3}(i,j) = \frac{|\Gamma_i|}{|\Delta_i|} B_{2,3}(i,j).$$

Almost all ratios $\frac{|\Gamma_i|}{|\Delta_i|}$ are 1, that is all, except for those involving the short orbit $\Delta_{43}$ of length 85, in which case the ratio is 3. For any particular Fano plane $F$ in orbit $\Gamma_j$, it is easy to determine how the 7 lines of $F$ are distributed among the orbits $\{\Delta_i\}$, thus computation of $B_{2,3}$ is straightforward.

In an effort to overcome the difficulty of presenting in this article the $43 \times 381$ matrix $A_{2,3}$, the next two pages display a coded version of $A_{2,3}$.

**Example:**

1. The row sums of $A_{2,3}$ are all 63, as expected.
2. The vector of column sums of $A_{2,3}$ is of type $7^{360} 9^{21}$.
3. The row vectors of the long orbits of 2-spaces are all of type $0^{32} 1^{60} 3^{1}$.
4. The row vectors for the short orbit of 2-spaces is of type $0^{360} 3^{21}$. 

**Remark 3.1.** In passing, we present some properties of $A_{2,3}$ which may be used to establish still unknown features of designs and large sets related to $A_{2,3}$. We say that a vector with integer entries has type $x_1^{x_1} x_2^{x_2} \cdots x_m^{x_m}$ if the value $x_i$ appears $\lambda_i$ times in the vector, for $1 \leq i \leq m$.

(i) The row sums of $A_{2,3}$ are all 63, as expected.
(ii) The vector of column sums of $A_{2,3}$ is of type $7^{360} 9^{21}$.
(iii) The row vectors of the long orbits of 2-spaces are all of type $0^{32} 1^{60} 3^{1}$.
(iv) The row vectors for the short orbit of 2-spaces is of type $0^{360} 3^{21}$. 

169
<table>
<thead>
<tr>
<th>Column</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>3k0000000010004</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>24</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>28</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>32</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>36</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>40</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>44</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>52</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>56</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>60</td>
</tr>
<tr>
<td>16</td>
<td>2</td>
<td>64</td>
</tr>
<tr>
<td>17</td>
<td>2</td>
<td>68</td>
</tr>
<tr>
<td>18</td>
<td>2</td>
<td>72</td>
</tr>
<tr>
<td>19</td>
<td>2</td>
<td>76</td>
</tr>
<tr>
<td>20</td>
<td>2</td>
<td>80</td>
</tr>
<tr>
<td>21</td>
<td>2</td>
<td>84</td>
</tr>
<tr>
<td>22</td>
<td>2</td>
<td>88</td>
</tr>
<tr>
<td>23</td>
<td>2</td>
<td>92</td>
</tr>
<tr>
<td>24</td>
<td>2</td>
<td>96</td>
</tr>
<tr>
<td>25</td>
<td>2</td>
<td>100</td>
</tr>
<tr>
<td>26</td>
<td>2</td>
<td>104</td>
</tr>
<tr>
<td>27</td>
<td>2</td>
<td>108</td>
</tr>
<tr>
<td>28</td>
<td>2</td>
<td>112</td>
</tr>
<tr>
<td>29</td>
<td>2</td>
<td>116</td>
</tr>
<tr>
<td>30</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>31</td>
<td>2</td>
<td>124</td>
</tr>
<tr>
<td>32</td>
<td>2</td>
<td>128</td>
</tr>
<tr>
<td>33</td>
<td>2</td>
<td>132</td>
</tr>
<tr>
<td>34</td>
<td>2</td>
<td>136</td>
</tr>
<tr>
<td>35</td>
<td>2</td>
<td>140</td>
</tr>
<tr>
<td>36</td>
<td>2</td>
<td>144</td>
</tr>
<tr>
<td>37</td>
<td>2</td>
<td>148</td>
</tr>
<tr>
<td>38</td>
<td>2</td>
<td>152</td>
</tr>
<tr>
<td>39</td>
<td>2</td>
<td>156</td>
</tr>
<tr>
<td>40</td>
<td>2</td>
<td>160</td>
</tr>
<tr>
<td>41</td>
<td>2</td>
<td>164</td>
</tr>
<tr>
<td>42</td>
<td>2</td>
<td>168</td>
</tr>
<tr>
<td>43</td>
<td>2</td>
<td>172</td>
</tr>
<tr>
<td>44</td>
<td>2</td>
<td>176</td>
</tr>
<tr>
<td>45</td>
<td>2</td>
<td>180</td>
</tr>
<tr>
<td>46</td>
<td>2</td>
<td>184</td>
</tr>
<tr>
<td>47</td>
<td>2</td>
<td>192</td>
</tr>
<tr>
<td>48</td>
<td>2</td>
<td>196</td>
</tr>
<tr>
<td>49</td>
<td>2</td>
<td>200</td>
</tr>
<tr>
<td>50</td>
<td>2</td>
<td>204</td>
</tr>
<tr>
<td>51</td>
<td>2</td>
<td>212</td>
</tr>
<tr>
<td>52</td>
<td>2</td>
<td>216</td>
</tr>
<tr>
<td>53</td>
<td>2</td>
<td>220</td>
</tr>
<tr>
<td>54</td>
<td>2</td>
<td>224</td>
</tr>
<tr>
<td>55</td>
<td>2</td>
<td>228</td>
</tr>
<tr>
<td>56</td>
<td>2</td>
<td>232</td>
</tr>
<tr>
<td>57</td>
<td>2</td>
<td>236</td>
</tr>
<tr>
<td>58</td>
<td>2</td>
<td>240</td>
</tr>
<tr>
<td>59</td>
<td>2</td>
<td>244</td>
</tr>
<tr>
<td>60</td>
<td>2</td>
<td>248</td>
</tr>
<tr>
<td>61</td>
<td>2</td>
<td>252</td>
</tr>
<tr>
<td>62</td>
<td>2</td>
<td>256</td>
</tr>
<tr>
<td>63</td>
<td>2</td>
<td>260</td>
</tr>
<tr>
<td>64</td>
<td>2</td>
<td>264</td>
</tr>
</tbody>
</table>
(vi) Since all $G$-orbits on 3-spaces have length 255, each of the three constituent designs of any $[G]$-invariant large set $LS[3][2,3,2]$ will be comprised of 127 $G$-orbits of 3-spaces.

In particular, properties (v) d.) and (vi) imply that a large set $LS[3][2,3,2]$ whose automorphism group contains a Singer subgroup as a normal subgroup, cannot have a group of automorphisms transitive on the 3 2-[2$^3$,3,21] designs.

a.) 320 columns of type $0^{36}1^7$
b.) 40 columns of type $0^{31}1^3$3
c.) 20 columns of type $0^{36}1^3$
d.) a single column of type $0^{40}3^1$
3.2. Constructing and presenting the designs and large sets

As the number of columns of \( A_{2,3} \) is rather large, a backtrack, depth-first search or similar algorithm would be hopeless in finding solutions to equation (10). Instead, we use lattice basis reduction to seek solutions. This technique is nicely described in [15], pages 277-300. For each of the 9 large sets of 2-[2⁸, 3, 21] designs we proceed using the following non-deterministic procedure, which, in general, is not guaranteed to terminate.

Procedure 3.2.

(i) Determine a 0-1 solution \( u_1 \) to equation \( A_{2,3}u_1 = 21J \), thus extracting a 2-[2⁸, 3, 21] design \( D_1 \) as the union of 127 \( G \)-orbits of 3-spaces. If this step succeeds, proceed to step (ii), otherwise stop.

(ii) Remove from \( A_{2,3} \) the 127 columns corresponding to design \( D_1 \) to obtain a 43 \( \times \) 254 matrix \( C_{2,3} \), and find a 0-1 solution \( u_2 \) to equation \( C_{2,3}u_2 = 21J \), thus extracting a second design \( D_2 \) consisting of 127 \( G \)-orbits among the orbits corresponding to the columns of \( C_{2,3} \). If this step succeeds, proceed to step (iii), otherwise stop.

(iii) Remove the 127 columns constituting \( D_2 \) from \( C_{2,3} \). The remaining 127 columns of \( C_{2,3} \) correspond to orbits whose union is a third design \( D_3 \), and \( L = \{ D_1, D_2, D_3 \} \) is a \( LS[3][2, 3, 2] \) large set. If steps (i) and (ii) are successful, so is (iii) and we have a successful termination with output large set \( L \).

Thus, the procedure of finding \( u_1 \) and \( u_2 \) becomes a matter of solving systems of integer equations through lattice basis reduction [15]. The following procedure describes briefly how the problems are set up so that lattice basis reduction can be used.

Procedure 3.3. First we construct a matrix that will constitute a basis for an integral lattice \( \Lambda_1 \) by adjoining the identity matrix of order 381 above KM matrix \( A_{2,3} \). To the right of the 424 \( \times \) 381 matrix just formed we adjoin a 424 \( \times \) 1 column vector which has zeros in the first 381 positions and \(-21\)'s in the remaining 43 positions. Let \( M_1 \) denote the 424 \( \times \) 382 matrix just formed.

\[
M_1 = \begin{bmatrix}
I \\
A_{2,3} \\
0 \\
-21J
\end{bmatrix}, \quad M_2 = \begin{bmatrix}
I \\
C_{2,3} \\
J
\end{bmatrix}
\]

If basis reduction produces a short enough basis \( M'_1 \) for \( \Lambda_1 \) which contains a short vector \( v_1 \) with \( 0 \)'s and \( 1 \)'s (or \( 0 \)'s and \(-1 \)'s) in the first 381 positions and all \( 0 \)'s below, then the projection \( u_1 \) of \( v_1 \) (or \(-v_1 \)) to the first 381 coordinates is likely to be a solution to \( A_{2,3}u_1 = 21J \) (see [15].) The weight of \( u_1 \) will be 127, and the union of orbits of 3-spaces corresponding to the \( 1 \)'s in \( u_1 \) will form a 2-[2⁸, 3, 21] design \( D_1 \).

If a solution \( u_1 \) is found, then replacing \( A_{2,3} \) by \( C_{2,3} \) yields a 297 \( \times \) 255 matrix \( M_2 \) which spans a lattice \( \Lambda_2 \), and by the same process as above, \( M_2 \) can yield a solution to \( C_{2,3}u_2 = 21J \), that is, a design \( D_2 \) disjoint from \( D_1 \).

It is now clear that when the 127 columns corresponding to the orbits forming \( D_2 \) are removed from \( C_{2,3} \), the remaining 127 orbits will form a 2-[2⁸, 3, 21] design \( D_3 \), and that \( \{ D_1, D_2, D_3 \} \) will be a large set.

However, the above procedure is not guaranteed to find a solution at first try, so if the basis reduction algorithm was unable to find a column in reduced basis \( M'_1 \) that met the conditions in Procedure 3.2.2, we would repeat the process, twiking the order of the columns of \( M_1 \), and the same later for \( M_2 \). The above procedure was repeated a number of times and we successfully constructed 9 distinct large sets \( \{ L_1, \ldots, L_9 \} \) which we exhibit below.

3.3. Reconstruction of the large sets

We briefly describe the display, to enable the reader to reconstruct the large sets and related designs. The first column is the index of the \( G \)-orbits on 3-spaces. There are 9 additional columns, each corresponding to one of the large sets. Each column has 127 \( 1 \)'s, 127 \( 2 \)'s and 127 \( 3 \)'s in it, which select the orbits contained in \( D_1 \), \( D_2 \) and \( D_3 \) respectively, for each large set. Since the orbits can be computed from the representative bases in the presentation of \( A_{2,3} \), the reader can readily reconstruct the 9 large sets and the designs involved.

Direct computation shows that indeed the 9 large sets are different from each other and different from the large set \( L_0 \) constructed in [4]. However, a peculiar visual symmetry is observed in the structure of our 9 large sets.
Figure 1. The 10 large sets \( \{L_0, \ldots, L_9\} \)

which is perhaps only related to our search method. The 9 large sets can be divided into 3 clusters of 3 large sets per cluster. The large sets of each cluster share a common 2-[2^8, 3, 21] design forming a triad of large sets, with a central design and three peripheral pairs of designs as illustrated in Figure 1. The three centers are different from each other, and the 18 peripheral designs are also different from each other and the 3 centers. Actually, there are no elements of \( \Gamma \) permuting non-trivially the 3 clusters of large sets, nor elements of order 3 permuting the 3 designs of any one of the large sets.

Checking the list of maximal subgroups of \( \Gamma = GL_8(2) \) shows that \( N = N_\Gamma(G) \) is not maximal in \( \Gamma \). Let \( \Phi_8 = \langle \zeta \rangle \leq N \), \( \zeta : \alpha \to \alpha^2 \) be the Frobenius subgroup normalizing \( G \). We have checked that \( \Phi_8 \) does not fix any of the 9 large sets, and does not move any one of the 9 large sets to any other.

Let \( L_0 \) be the \( LS[3][2, 3, 2^8] \) discovered by the authors of [4], and let \( S = \{L_i : 0 \leq i \leq 9\} \). We already know that \( G \leq \text{Aut}(L_i) \) for each \( i \in \{0, \ldots, 9\} \). It is conceivable that the automorphism groups of the 10 large sets in \( S \) are not all identical, but we think this is very unlikely and we conjecture that in fact \( \text{Aut}(L_i) \) are all identical, and equal to the Singer subgroup \( G \).

\[
\zeta = \begin{bmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1
\end{bmatrix}
\]

We presently rephrase, in the context of our notation, a very useful theorem of A. Betten, R. Laue, and A. Wassermann in [1]. This will immediately yield a corollary concerning the question of isomorphism between the 10 large sets in \( S = \{L_0, L_1, \ldots, L_9\} \).

**Theorem 3.4. (Theorem 3.1 in [1])** Let \( G \) be a finite group acting on a set \( X \). Suppose that \( x_1, x_2 \in X \) and \( g \in G \) such that \( x_1^g = x_2 \). Moreover, suppose that a Sylow subgroup \( P \) of \( G \) is contained in the stabilizers \( G_{x_1} \) and \( G_{x_2} \). Then, \( x_1^n = x_2 \) for some \( n \in N_G(P) \).
Corollary 3.5. The ten Large Sets in $S = \{L_0, L_1, \ldots, L_9\}$ are pairwise non-isomorphic.

Proof. Let $\mathcal{L}$ be the collection all large sets of type $LS[3][2, 3, 2^9]$, and $G = \langle \alpha \rangle$ be the Singer subgroup as defined earlier. Then, $\Gamma$ acts on $\mathcal{L}$, and for any $\lambda \in \mathcal{L}$ the stabilizer $\Gamma_\lambda$ is the full automorphism group of $\lambda$. In particular, for each $\lambda \in S$ we have that $P < G \leq \Gamma_\lambda$ where $P$ is the Sylow-17 subgroup of $G$. Let $\beta, \gamma \in S$, $\beta \neq \gamma$, and suppose there is $g \in \Gamma$ such that $\beta^g = \gamma$. Then, by Theorem 3.4, there would exist an element $n \in N_{\Gamma}(P) = N_{\Gamma}(G)$ such that $\beta^n = \gamma$. But we know, by direct checking, that no element of the Frobenius group $\Phi_8$, and therefore no element of $N_{\Gamma}(G) = G \cdot \Phi_8$ sends $\beta$ to $\gamma$, a contradiction.

3.4. Conclusions

Until 2014, the only large sets of geometric $t$-$[q^n, k, \lambda]$ designs known were for $t = 1$. In finite geometry, $LS[N]-t,k,q^n$ large sets with $t = 1$, are known as $(k-1)$-parallelisms of $(k-1)$-spreads in $PG(n - 1, q)$. The first large set $L_0$ of geometric 2-designs, a $LS[3]-[2, 3, 2^9]$, was constructed by the authors of [4]. In this paper we construct an additional nine pairwise different large sets $L_1, \ldots, L_9$ which are also different from $L_0$. All these large sets are $[G]$-invariant, under the same Singer subgroup $G$ of order 255. In fact, the large sets $\{L_0, \ldots, L_9\}$ are pairwise non-isomorphic.

3.5. Possible future work

The necessary conditions for the existence of a $LS[3]-[3, 4, 2^9]$ are satisfied and we are close to settling the question of existence of a $LS[3]-[3, 4, 2^9]$.

Acknowledgment: The authors would like to express their thanks to Dr. Igor Kliakhandler whose generous support made possible a most significant conference on Algebraic Combinatorics and Applications at Michigan Technical University, in August, 2015. The authors also wish to thank Prof. Vladimir Tonchev for putting together a superbly organized conference.

References