Advances in Mathematics of Communications
Volume 13, No. 1, 2019, 165–170
doi:10.3934/amc.2019010

NEW 2-DESIGNS OVER FINITE FIELDS FROM DERIVED AND RESIDUAL DESIGNS

Michael Braun*

Faculty of Computer Science
University of Applied Sciences Darmstadt
Schoefferstr. 8b, 64295 Darmstadt, Germany

Michael Kiermaier and Reinhard Laue

Mathematisches Institut
Universität Bayreuth
95447 Bayreuth, Germany
and
Institut für Informatik
Universität Bayreuth
95447 Bayreuth, Germany

(Communicated by Sihem Mesnager)

Abstract. Based on the existence of designs for the derived and residual parameters of admissible parameter sets of designs over finite fields we obtain a new infinite series of designs over finite fields for arbitrary prime powers q with parameters 2-$(8,4,\frac{(q^6-1)(q^3-1)}{(q^2-1)(q-1)};q)$ as well as designs with parameters 2-$(10,4,85\lambda;2)$, 2-$(10,5,765\lambda;2)$, 2-$(11,5,6205\lambda;2)$, 2-$(11,5,502605\lambda;2)$, and 2-$(12,6,423181\lambda;2)$ for $\lambda = 7, 12, 19, 21, 22, 24, 31, 36, 42, 43, 48, 49, 55, 60, 63$.

1. Introduction

A *design over a finite field* with parameters t-$(n,k,\lambda;q)$ is a pair $(V,\mathcal{B})$ consisting of an n-dimensional vector space V over the finite field $\mathbb{F}_q$ with q elements and a set $\mathcal{B}$ of k-dimensional subspaces of V such that each t-dimensional subspace of V is contained in λ elements of $\mathcal{B}$.

Designs over finite fields are also called q-analogs of combinatorial designs or subspace designs [8, 9].

Since the first non-trivial t-$(n,k,\lambda;q)$ designs for $t>1$ were introduced in 1987 [18] the interest in these objects has increased. Several results on parameter sets of new constructed designs over finite fields have been published [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 17], whereas until now only two infinite series for arbitrary field size q are known:

- In [17] a series of 2-$(n,3,\frac{q^3-1}{q-1};q)$ designs constructed for all integers $n \geq 7$ with $n \equiv \pm 1 \bmod 6$ and all prime powers q admitting the normalizer of a Singer cycle group as a group of automorphisms.

2010 *Mathematics Subject Classification:* Primary: 51E20; Secondary: 05B05, 05B25.
Key words and phrases: q-analog, designs over finite fields, residual design, derived design.
* Corresponding author: Michael Braun.

- In [10] a series of 2-$(\ell m, 3, q^3\frac{q^{\ell-5}-1}{q-1}; q)$ designs is given for all $m \geq 3$ and $\ell \geq 7$ with $\ell \equiv 5 \bmod 6(q-1)$ admitting the special linear group $\mathrm{SL}(m, q^\ell)$ as a group of automorphisms.

In this paper we present a new infinite series of designs over finite fields for arbitrary field size. Furthermore, we use parameter sets for which designs over the binary field can be constructed using a computer aided approach to deduce new parameters by considering reduced designs over finite fields.

2. Preliminaries

In the following by $\begin{bmatrix} V \\ k \end{bmatrix}$ we denote the set of k-dimensional subspaces of V—its cardinality is given by the q-binomial coefficient

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}.$$

Given a t-$(n,k,\lambda;q)$ design $(V,\mathcal{B})$ the existence of designs with new parameters can be derived from a result by Suzuki [16].

Lemma 2.1. *Let $(V,\mathcal{B})$ be a t-$(n,k,\lambda;q)$ design, i and j non-zero integers with $i+j \leq t$, $P \in \begin{bmatrix} V \\ i \end{bmatrix}$, and $H \in \begin{bmatrix} V \\ n-j \end{bmatrix}$. Then the following equation holds:*

$$|\{B \in \mathcal{B} \mid P \subseteq B \subseteq H\}| = \lambda \frac{\begin{bmatrix} n-j-i \\ k-i \end{bmatrix}_q}{\begin{bmatrix} n-t \\ k-t \end{bmatrix}_q}.$$

Plugging different values for i and j into this lemma immediately yields the existence of designs for new parameters:

- By setting $i = t-1$ and $j = 0$ the pair $(V,\mathcal{B})$ defines a design for *reduced* parameters
$$\mathrm{red}[t\text{-}(n,k,\lambda;q)] := (t-1)\text{-}(n,k,\lambda\tfrac{q^{n-t+1}-1}{q^{k-t+1}-1};q).$$
- If $K^\perp := \{x \in V \mid \langle x,y\rangle = 0\, \forall y \in K\}$ denotes the dual space for some non-singular bilinear form $\langle -,-\rangle$ by setting $i = 0$ and $j = t$ the pair $(V, \{K^\perp \mid K \in \mathcal{B}\})$ defines a design for the *dual* parameters
$$\mathrm{dual}[t\text{-}(n,k,\lambda;q)] := t\text{-}(n,n-k,\lambda\tfrac{\begin{bmatrix} n-t \\ k \end{bmatrix}_q}{\begin{bmatrix} n-t \\ k-t \end{bmatrix}_q};q).$$
- By taking an $(n-1)$-dimensional subspace $H \in \begin{bmatrix} V \\ n-1 \end{bmatrix}$ and by defining $i = t-1$ and $j = 1$ the pair $(H, \{K \in \mathcal{B} \mid K \subseteq H\})$ is a design for the *residual* parameters
$$\mathrm{res}[t\text{-}(n,k,\lambda;q)] := (t-1)\text{-}(n-1,k,\lambda\tfrac{q^{n-k}-1}{q^{k-t+1}-1};q).$$

Furthermore, by taking a 1-dimensional subspace $P \in \begin{bmatrix} V \\ 1 \end{bmatrix}$ and considering factor spaces the pair $(V/P, \{K/S \mid K \in \mathcal{B}, P \subseteq K\})$ yields a design for the *derived* parameters

$$\mathrm{der}[t\text{-}(n,k,\lambda;q)] := (t-1)\text{-}(n-1,k-1,\lambda;q).$$

The following theorem [11, Theorem 1] serves as the major construction tool for the aforementioned results of this work.

Theorem 2.2. *Let t-$(n,k,\lambda;q)$ be parameters of designs. The existence of designs for the derived and residual parameters implies the existence of a design for the reduced parameters.*

3. Extension of Suzuki's design

In 1992 Suzuki [17] found an infinite series of 2-$(n, 3, \frac{q^3-1}{q-1}; q)$ designs constructed for all integers $n \geq 7$ with $n \equiv \pm 1 \bmod 6$. By applying Theorem 2.2 and due to the existence of dual designs Suzuki's design can be extended to a new infinite family (also see [11, Corollary 2]).

Theorem 3.1. *For all prime powers q there exist* 2-$(8, 4, \frac{(q^3-1)(q^6-1)}{(q-1)(q^2-1)}; q)$ *designs.*

Proof. In the following let $n = 7$. Then we get:

$$\begin{aligned}
\operatorname{der}[3\text{-}(8, 4, \tfrac{q^3-1}{q-1}; q)] &= 2\text{-}(7, 3, \tfrac{q^3-1}{q-1}; q) \\
\operatorname{res}[3\text{-}(8, 4, \tfrac{q^3-1}{q-1}; q)] &= \operatorname{dual}[2\text{-}(7, 3, \tfrac{q^3-1}{q-1}; q)] = 2\text{-}(7, 4, \begin{bmatrix}4\\2\end{bmatrix}_q; q) \\
\operatorname{red}[3\text{-}(8, 4, \tfrac{q^3-1}{q-1}; q)] &= 2\text{-}(8, 4, \tfrac{(q^3-1)(q^6-1)}{(q-1)(q^2-1)}; q)
\end{aligned}$$

For $n = 7$ Suzuki's 2-$(7, 3, \frac{q^3-1}{q-1}; q)$ design and its dual 2-$(7, 4, \begin{bmatrix}4\\2\end{bmatrix}_q; q)$ design exist. Their parameters are the derived and residual parameters of 3-$(8, 4, \frac{q^3-1}{q-1}; 2)$. Theorem 2.2 implies the existence of designs over $\mathbb{F}_q$ for the reduced parameters 2-$(8, 4, \frac{(q^3-1)(q^6-1)}{(q-1)(q^2-1)}; q)$. □

4. Kramer–Mesner approach

In this section we recall the approach for a computer aided construction of designs proposed by Kramer and Mesner [13]. We use this approach to construct certain designs over the binary field which serve as initial values for the construction theorem in the next section. The designs in Table 1 can also be found [8]. For sake of completeness we recall the construction of these designs using the Kramer–Mesner approach.

Subgroups G of the general linear group $\mathrm{GL}(n, q)$ act on subspaces of V from the left considering subspaces as column spaces. The corresponding orbit of G on the subspace K is given by $G(K) := \{\alpha(K) := \{\alpha(v) \mid v \in K\} \mid \alpha \in G\}$.

A t-$(n, k, \lambda; q)$ design $(V, \mathcal{B})$ admits a subgroup G of $\mathrm{GL}(V)$ as a *group of automorphisms* if and only if it consists of orbits of G on the set of k-dimensional subspaces of V.

In order to obtain a selection of orbits of G on $\begin{bmatrix}V\\k\end{bmatrix}$ we consider the incidence matrix $A^G_{t,k}$ whose rows are indexed by the G-orbits on the set of t-dimensional subspaces of V and whose columns are indexed by the orbits on the set of k-dimensional subspaces. The entry of $A^G_{t,k}$ corresponding to the orbits $G(T)$ and $G(K)$, respectively, is defined by the number $a^G_{T,K} := \{K' \in G(K) \mid T \subseteq K'\}$.

Any t-$(n, k, \lambda; q)$ design admitting a subgroup G of $\mathrm{GL}(V)$ as a group of automorphisms bijectively corresponds to a binary vector x satisfying $A^G_{t,k}x = [\lambda, \ldots, \lambda]^t$.

The binary vector x stands for the selection of G-orbits on $\begin{bmatrix}V\\k\end{bmatrix}$ whose union forms the corresponding design.

Using this construction approach we list some 2-$(9, k, \lambda; 2)$ designs for $k \in \{3, 4\}$ in Table 1 which we utilize to get new designs by Theorem 2.2 in the next section. Solving the corresponding Diophantine system of equations with an LLL based algorithm [19] only takes a few seconds for the given parameters. An overview on published parameters can be found in [8].

We use the following constructions for subgroups of $\mathrm{GL}(n, q)$:

TABLE 1. 2-$(9,k,\lambda;2)$ designs for $k \in \{3,4\}$

t-$(n,k,\lambda;q)$	G	$\lvert A^G_{t,k}\rvert$	λ
2-$(9,3,\lambda;2)$	$N(3,2^3)$	31×529	21, 22, 42, 43, 63
	$N(8,2)\times 1$	28×408	7, 12, 19, 24, 31, 36, 43, 48, 55, 60
	$M(3,2^3)$	40×460	49
2-$(9,4,\lambda;2)$	$N(9,2)$	11×725	21, 63, 84, 126, 147, 189, 210, 252, 273, 315, 336, 378, 399, 441, 462, 504, 525, 567, 588, 630, 651, 693, 714, 756, 777, 819, 840, 882, 903, 945, 966, 1008, 1029, 1071, 1092, 1134, 1155, 1197, 1218, 1260, 1281, 1323

- A *Singer cycle* of the general linear group $\mathrm{GL}(n,q)$ is a cyclic group of order q^n-1 whereas its generator can be obtained from the matrix representation of any primitive element of the field $\mathbb{F}^*_{q^n}$. The normalizer $N(n,q)$ of the Singer cycle is given by as the semi-direct product of the Galois group $\langle\phi\rangle$ and a Singer cycle of $\mathrm{GL}(n,q)$ having the order $n(q^n-1)$.
- If G is a subgroup of $\mathrm{GL}(n,q)$ by $G\times 1$ we mean the *direct product* of G with the trivial group of matrix dimension 1 such that $G\times 1$ is a subgroup of $\mathrm{GL}(n+1,q)$.
- The set $M(n,q)$ denotes the subgroup of $\mathrm{GL}(n,q)$ consisting of all *monomial* matrices of $\mathrm{GL}(n,q)$ which is the set of all invertible matrices having exactly one non-zero entry in each row and in each column.
- By lifting any matrix group G of $\mathrm{GL}(m,q^\ell)$ can be interpreted as a subgroup of $\mathrm{GL}(m\ell,q)$.

5. NEW PARAMETERS

In this section we obtain new parameters for which designs exist by iterated application of Theorem 2.2.

Theorem 5.1. *The existence of designs with parameters* $(t-1)$-$(2t+3,t,\lambda;q)$ *and* $(t-1)$-$(2t+3,t+1,\lambda\frac{q^{t+3}-1}{q^2-1};q)$ *imply the existence of designs with the following parameters:*

- $(t-1)$-$(2t+4,t+1,\lambda\frac{q^{t+5}-1}{q^2-1};q)$,
- $(t-1)$-$(2t+4,t+2,\lambda\frac{(q^{t+3}-1)(q^{t+5}-1)}{(q^2-1)(q^3-1)};q)$,
- $(t-1)$-$(2t+5,t+2,\lambda\frac{(q^{t+5}-1)(q^{t+6}-1)}{(q^2-1)(q^3-1)};q)$,
- $(t-1)$-$(2t+5,t+2,\lambda\frac{(q^{t+3}-1)(q^{t+3}-1)(q^{t+5}-1)(q^{t+6}-1)}{(q^2-1)(q^3-1)(q^4-1)(q^4-1)};q)$,
- $(t-1)$-$(2t+6,t+3,\lambda\frac{(q^{t+5}-1)(q^{t+6}-1)(q^{t+7}-1)}{(q^2-1)(q^3-1)(q^4-1)};q)$.

Proof. The result can be checked along Figure 1. Starting with the two underlined parameters we successively can deduce the four parameters in the boxes due to the

fact that residual and derived designs imply reduced designs and that designs with dual parameters do exist. □

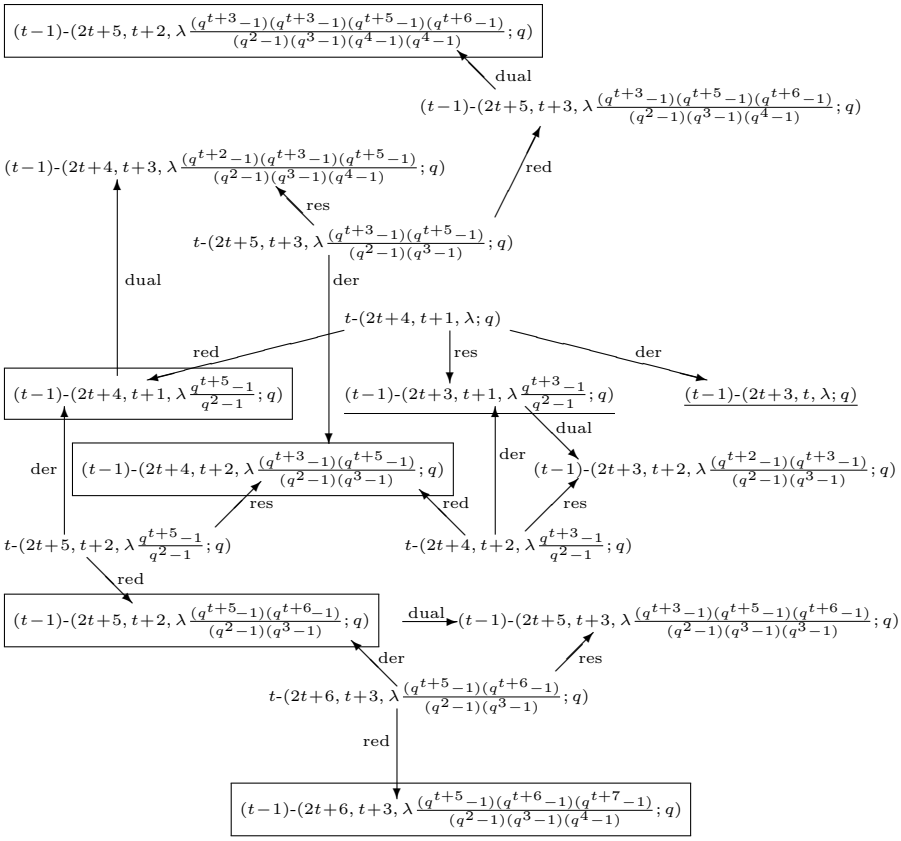

FIGURE 1. Connections of parameters

As an immediate consequence of this theorem for $t = 3$ and $q = 2$ applied to Table 1 containing 2-$(9, k, \lambda; 2)$ designs for $k \in \{3, 4\}$ we obtain the following corollary:

Corollary 1. *For* $\lambda = 7, 12, 19, 21, 22, 24, 31, 36, 42, 43, 48, 49, 55, 60, 63$ *designs with parameters* 2-$(9, 3, \lambda; 2)$ *and* 2-$(9, 4, 21\lambda; 2)$ *do exist which imply the existence of further designs with the following parameters:*

- 2-$(10, 4, 85\lambda; 2)$,
- 2-$(10, 5, 765\lambda; 2)$,
- 2-$(11, 5, 6205\lambda; 2)$,
- 2-$(11, 5, 502605\lambda; 2)$,
- 2-$(12, 6, 423181\lambda; 2)$.

References

[1] M. Braun, Designs over the binary field from the complete monomial group, *Australas. J. Combin.*, **67** (2017), 470–475.

[2] M. Braun, Some new designs over finite fields, *Bayreuth. Math. Schr.,* **74** (2005), 58–68.
[3] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy and A. Wassermann, Existence of q-analogs of steiner systems, *Forum Math. Pi,* **4** (2016), e7, 14pp.
[4] M. Braun, A. Kerber and R. Laue, Systematic construction of q-analogs of designs, *Des. Codes Cryptogr.*, **34** (2005), 55–70.
[5] M. Braun, M. Kiermaier, A. Kohnert and R. Laue, Large sets of subspace designs, *J. Combin. Theory Ser. A*, **147** (2017), 155–185.
[6] M. Braun, A. Kohnert, P. R. J. Östergård and A. Wassermann, Large sets of t-designs over finite fields, *J. Combin. Theory Ser. A*, **124** (2014), 195–202.
[7] S. Braun, Construction of q-analogs of combinatorial designs, ALCOMA 2010, Thurnau, 2010.
[8] M. Braun, M. Kiermaier and A. Wassermann, q-analogs of designs: subspace designs, In *M. Greferath, M.O. Pavčević, N. Silberstein, and M.A. Vázquez-Castro, editors, Network Coding and Subspace Designs,* Springer International Publishing, (2018), 171–211.
[9] M. Braun, M. Kiermaier and A. Wassermann, Computational methods in subspace designs, In *M. Greferath, M.O. Pavčević, N. Silberstein, and M.A. Vázquez-Castro, editors, Network Coding and Subspace Designs*, Springer International Publishing, (2018), 213–244.
[10] T. Itoh, A new family of 2-designs over $GF(q)$ admitting $SL_m(q^l)$, *Geom. Dedicata,* **69** (1998), 261–286.
[11] M. Kiermaier and R. Laue, Derived and residual subspace designs, *Adv. Math. Commun.*, **9** (2015), 105–115.
[12] M. Kiermaier, R. Laue and A. Wassermann, A new series of large sets of subspace designs over the binary field, *Des. Codes Cryptogr.*, **86** (2018), 251–268.
[13] E. Kramer and D. Mesner, t-designs on hypergraphs, Discrete Math., **15** (1976), 263–296.
[14] M. Miyakawa, A. Munemasa and S. Yoshiara, On a class of small 2-designs over $GF(q)$, *J. Combin. Des.*, **3** (1995), 61–77.
[15] H. Suzuki, 2-designs over $GF(2^m)$, *Graph. Combinator.*, **6** (1990), 293–296.
[16] H. Suzuki, On the inequalities of t-designs over a finite field, *Eur. J. Comb.*, **11** (1990), 601–607.
[17] H. Suzuki, 2-designs over $GF(q)$, *Graph. Combinator.*, **8** (1992), 381–389.
[18] S. Thomas, Designs over finite fields, *Geom. Dedicata*, **24** (1987), 237–242.
[19] A. Wassermann, Finding simple t-designs with enumeration techniques, *J. Combin. Des.*, **6** (1998), 79–90.

Received for publication June 2018.

E-mail address: michael.braun@h-da.de
E-mail address: michael.kiermaier@uni-bayreuth.de
E-mail address: reinhard.laue@uni-bayreuth.de