Finite Fields and Their Applications 57 (2019) 128–138

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Designs over finite fields by difference methods

Marco Buratti [a], Anamari Nakić [b,*]

[a] *Dipartimento di Matematica e Informatica, Università di Perugia, via Vanvitelli 1, 06123 Italy*

[b] *University of Zagreb, Faculty of Electrical Engineering and Computing, Unska 3, 10000 Zagreb, Croatia*

ARTICLE INFO

Article history:
Received 20 August 2018
Received in revised form 15 February 2019
Accepted 15 February 2019
Available online xxxx
Communicated by Dieter Jungnickel

MSC:
05B05
05B10

Keywords:
Difference family
Design over a finite field
Group divisible design over a finite field

ABSTRACT

One of the very first results about designs over finite fields, by S. Thomas, is the existence of a cyclic 2-$(n, 3, 7)$ design over $\mathbb{F}_2$ for every integer n coprime with 6. Here, by means of difference methods, we reprove and improve a little bit this result showing that it is true, more generally, for every odd n. In this way, we also find the first infinite family of non-trivial cyclic group divisible designs over $\mathbb{F}_2$.

1. Introduction

In this paper we adapt very well known difference methods to the construction of *designs over finite fields*. Our main result will be the existence of a cyclic 2-$(n, 3, 7)$ design over $\mathbb{F}_2$ for every odd positive n. It should be noted that in the case $n \equiv \pm 1$

* Corresponding author.
E-mail addresses: buratti@dmi.unipg.it (M. Buratti), anamari.nakic@fer.hr (A. Nakić).

https://doi.org/10.1016/j.ffa.2019.02.006
1071-5797/

(mod 6) our designs are the same found by S. Thomas [8] a long time ago by means of a geometric approach. Anyway our proof is algebraic and completely different; we hope it may open the door to new ideas on this topic. In the new case $n \equiv 3 \pmod 6$ we get designs which, maybe, are not very nice since they are far from being simple; indeed they have $\frac{2^n-1}{7}$ blocks repeated 7 times. On the other hand, though "ugly", these designs allow us to get the first infinite class of cyclic and simple *group divisible designs over finite fields*.

Here we give all prerequisites that are necessary for understanding our proof of the main result.

Classic 2-designs and group divisible designs

A 2-(n, k, λ) design is a pair $(\mathcal{P}, \mathcal{B})$ with $\mathcal{P}$ a set of n *points* and $\mathcal{B}$ a multiset of k-subsets (*blocks*) of $\mathcal{P}$ with the property that any 2-subset of $\mathcal{P}$ is contained in precisely λ blocks.

A (mg, g, k, λ) *group divisible design*, briefly a (mg, g, k, λ)-GDD, is a triple $(\mathcal{P}, \mathcal{G}, \mathcal{B})$ with $\mathcal{P}$ a set of mg *points*, $\mathcal{G}$ a partition of $\mathcal{P}$ into m subsets (*groops*)[1] of size g, and $\mathcal{B}$ a multiset of k-subsets (*blocks*) of $\mathcal{P}$ with the two properties that a block and a groop have at most one common point, and any two points belonging to distinct groops are contained, together, in exactly λ blocks.

It is clear that a $(n, 1, k, \lambda)$-GDD is completely equivalent to a 2-(n, k, λ) design.

An automorphism of a 2-design or group divisible design is a permutation of its point-set leaving invariant its block-multiset.

A 2-design or group divisible design is said to be *simple* if it does not have repeated blocks.

Cyclic 2-designs and difference families

A 2-design is said to be *cyclic* if it admits an automorphism cyclically permuting all its points or, equivalently, if it has a cyclic automorphism group acting sharply transitively on the points. It is known that every cyclic 2-design can be described in terms of differences [1]. We recall here the difference methods using the notion of an *ordinary difference family*.

If B is a subset of an additive (resp. multiplicative) group H, the list of differences of B is the multiset ΔB of all possible differences $x-y$ (resp. quotients xy^{-1}) with (x, y) an ordered pair of distinct elements of B. The *development* of B under H is the collection $\mathrm{dev}B = \{B * h \mid h \in H\}$ where $*$ is the (additive or multiplicative) operation of H.

Note that if $\mathrm{stab}(B)$ is the stabilizer of B under the regular right action of H on itself, then $\mathrm{dev}B$ coincides with the orbit of B replicated $|H : \mathrm{stab}(B)|$ times. So $\mathrm{dev}B$ coincides with the orbit of B when $\mathrm{stab}(B)$ is trivial.

[1] Here, following [2], we misspell the word "group" on purpose in order to avoid confusion with the groups understood as algebraic structures.

If $\mathcal{F}$ is a collection of subsets of H, then the list of differences and the development of $\mathcal{F}$ are, respectively, the multiset sums

$$\Delta\mathcal{F} := \biguplus_{B\in\mathcal{F}} \Delta B \qquad \text{and} \qquad \mathrm{dev}\mathcal{F} := \biguplus_{B\in\mathcal{F}} \mathrm{dev}B.$$

Definition 1.1. Let H be a group of order n. A collection $\mathcal{F}$ of k-subsets of H is an ordinary (n,k,λ) difference family if the list of differences of $\mathcal{F}$ covers every non-identity element of H exactly λ times.

In the following, the adjective "ordinary" will be omitted. The members of a difference family are usually called *base blocks*. Sometimes, as in [2], it is also required that the base blocks have trivial stabilizers. We prefer to remove this constraint since it is not necessary for the validity of the following well known result.

Theorem 1.2. *If $\mathcal{F}$ is a (n,k,λ) difference family in a group H, then the pair $(H, dev\mathcal{F})$ is a 2-(n,k,λ) design admitting an automorphism group isomorphic to H acting sharply transitively on the points.*

So, in particular, the existence of a (n,k,λ) difference family in a cyclic group is a sufficient condition for the existence of a cyclic 2-(n,k,λ) design.

Remark 1.1. The design generated by a difference family $\mathcal{F}$ is simple if and only if all the base blocks of $\mathcal{F}$ have trivial stabilizer and they belong to pairwise distinct orbits.

Designs and difference families over $\mathbb{F}_2$

As it is standard, we denote by $\mathbb{F}_q^n$ the n-dimensional vector space over the field $\mathbb{F}_q$ of order q. The multiplicative group of a field $\mathbb{F}$ will be denoted by $\mathbb{F}^*$ and the set of non-zero vectors of $\mathbb{F}_q^n$ will be often identified with $\mathbb{F}_{q^n}^*$.

The q-analog of a t-(n,k,λ) design – also said a t-(n,k,λ) design over $\mathbb{F}_q$ or t-$(n,k,\lambda)_q$ design – is a collection $\mathcal{S}$ of k-dimensional subspaces of $\mathbb{F}_q^n$ with the property that any t-dimensional subspace of $\mathbb{F}_q^n$ is contained in exactly λ members of $\mathcal{S}$. For the survey on recent results, we refer the reader to [6]. The most spectacular design over a finite field, obtained by Braun et al. [5], has parameters 2-$(13,3,1)_2$. Its discovering allowed to disprove the longstanding conjecture according to which the only Steiner t-designs over finite fields are the trivial ones (spreads).

Here we are interested only in 2-(n,k,λ) designs over $\mathbb{F}_2$.

Remark 1.2. Every 2-(n,k,λ) design over $\mathbb{F}_2$ is completely equivalent to a 2-$(2^n-1, 2^k-1, \lambda)$ design $(\mathbb{F}_{2^n}^*, \mathcal{B})$ in the classic sense with the crucial property that $B \cup \{0\}$ is a subspace of the vector space $\mathbb{F}_2^n$ for every $B \in \mathcal{B}$.

Indeed, deleting the zero-vector from each block of a 2-$(n,k,\lambda)_2$ design one gets the block-multiset of a classic 2-$(2^n-1, 2^k-1, \lambda)$ design with point-set $\mathbb{F}_{2^n}^*$.

For instance, the mentioned 2-$(13, 3, 1)_2$ design is a classic 2-$(8191, 7, 1)$ design where the points are the non-zero vectors of $\mathbb{F}_2^{13}$ and where every block is the set of non-zero vectors of a 3-dimensional subspace of $\mathbb{F}_2^{13}$. It is cyclic since it admits $\mathbb{F}_{2^{13}}^*$ as an automorphism group acting sharply transitively on the points. The authors found it by using the famous Kramer-Mesner method and then they proved that it could be also obtained from a $(8191, 7, 1)$ difference family.[2] Of course this difference family has the special property that all its members are subspaces of $\mathbb{F}_2^{13}$ with the zero-vector removed. This naturally leads to the following definition.

Definition 1.3. A (n, k, λ) difference family over $\mathbb{F}_2$ or, briefly, a $(n, k, \lambda)_2$ difference family, is a $(2^n - 1, 2^k - 1, \lambda)$ difference family in $\mathbb{F}_{2^n}^*$ with the property that $B \cup \{0\}$ is a subspace of $\mathbb{F}_2^n$ for every $B \in \mathcal{F}$.

The above terminology is justified by the following.

Proposition 1.4. *A $(n, k, \lambda)_2$ difference family generates a cyclic 2-$(n, k, \lambda)_2$ design.*

Proof. Let $\mathcal{F}$ be a $(n, k, \lambda)_2$ difference family. By Definition 1.3, $\mathcal{F}$ is a $(2^n - 1, 2^k - 1, \lambda)$ difference family in $\mathbb{F}_{2^n}^*$ and then, by Theorem 1.2, the pair $\mathcal{D} = (\mathbb{F}_{2^n}^*, dev\mathcal{F})$ is a cyclic 2-$(2^n - 1, 2^k - 1, \lambda)$ design. By definition of dev$\mathcal{F}$, each block of $\mathcal{D}$ is of the form xB with $x \in \mathbb{F}_{2^n}^*$ and $B \in \mathcal{F}$. Also, by Definition 1.3, we have that $B \cup \{0\}$ is a subspace of the vector space $\mathbb{F}_2^n$ so that $xB \cup \{0\}$ is a subspace of $\mathbb{F}_2^n$ as well. Thus every block of $\mathcal{D}$ is a subspace of $\mathbb{F}_2^n$ deprived of the zero vector. This means, by Remark 1.2, that $\mathcal{D}$ can be seen as a 2-$(n, k, \lambda)_2$ design. □

We will use the above proposition to reprove and improve an old result by S. Thomas [8] about cyclic 2-$(n, 3, 7)$ designs over $\mathbb{F}_2$.

Cyclic group divisible designs and relative difference families

Cyclic group divisible designs – namely group divisible designs with an automorphism group acting sharply transitively on the point-set – can be also described in terms of differences. In particular, some of them are generated by *relative difference families.*

Definition 1.5. Let G be a subgroup of order g of a group H of order mg. A collection $\mathcal{F}$ of k-subsets of H is a (mg, g, k, λ) difference family if the list of differences of $\mathcal{F}$ does not contain any element of G and covers every element of $H \setminus G$ exactly λ times.

One usually says that a difference family $\mathcal{F}$ as above is *relative to G*. It is clear that an ordinary difference family in H can be seen as a difference family relative to the

[2] As a matter of fact, there was no need to prove this since it is possible to see that every cyclic 2-(n, k, λ) design with $\gcd(n, k) = 1$ is necessarily generated by a (n, k, λ) difference family.

trivial subgroup of H. More specifically, a (v, k, λ) difference family in H is nothing but a $(v, 1, k, \lambda)$ difference family.

Here is the "group-divisible-analog" of Theorem 1.2 [3].

Theorem 1.6. *Let $\mathcal{F}$ be a (mg, g, k, λ) difference family in H relative to G. Then, if $\mathcal{G}$ is the set of right cosets of G in H, the triple $(H, \mathcal{G}, dev\mathcal{F})$ is a (mg, g, k, λ)-GDD with an automorphism group isomorphic to H acting sharply transitively on the points.*

So, in particular, the existence of a (mg, g, k, λ) difference family in a cyclic group is a sufficient condition for the existence of a cyclic (mg, g, k, λ) group divisible design.

The GDD generated by a relative difference family $\mathcal{F}$ is simple if and only if all the base blocks of $\mathcal{F}$ have trivial stabilizer and they belong to pairwise distinct orbits.

We will need the following very elementary fact.

Proposition 1.7. *Let $\mathcal{F}$ be a (mk, k, k) difference family in H with a base block G that is a subgroup of H. Then $\mathcal{F} \setminus \{G\}$ is a (mk, k, k, k) difference family in H relative to G.*

Proof. It is enough to note that ΔG is k times the set of non-identity elements of G. $\square$

Group divisible designs and relative difference families over $\mathbb{F}_2$

The q-analog of a group divisible design is a concept very recently introduced in [4]. First recall that a *g-spread* of the vector space $\mathbb{F}_q^n$ is a set of g-dimensional subspaces covering $\mathbb{F}_q^n$ and intersecting each other trivially.

Definition 1.8. Let $\mathcal{S}$ be a g-spread of $\mathbb{F}_q^n$ and let $\mathcal{T}$ be a collection of k-dimensional subspaces of $\mathbb{F}_q^n$. The triple $(\mathbb{F}_q^n, \mathcal{S}, \mathcal{T})$ is a (n, g, k, λ) group divisible design over $\mathbb{F}_q$, briefly a $(n, g, k, \lambda)_q$-GDD, if any 2-dimensional subspace of $\mathbb{F}_q^n$ is either contained in exactly one member of $\mathcal{S}$ or contained in exactly λ members of $\mathcal{T}$ but not both.

Note that when $g = 1$, then $\mathcal{S}$ is necessarily the set of all 1-dimensional subspaces of $\mathbb{F}_q^n$ and $\mathcal{T}$ is a 2-$(n, k, \lambda)_2$ design.

Remark 1.3. Every (mg, g, k, λ) design over $\mathbb{F}_2$ is completely equivalent to a $(2^{mg} - 1, 2^g - 1, 2^k - 1, \lambda)$-GDD with point-set $\mathbb{F}_{2^{mg}}^*$ and the properties that the groops are the elements – with the zero-vector removed – of a g-spread, and that each block is the set of non-zero vectors of a k-dimensional subspace.

Indeed, deleting the zero-vector from each groop and from each block of a $(mg, g, k, \lambda)_2$-GDD one get a classic $(2^{mg} - 1, 2^g - 1, 2^k - 1, \lambda)$-GDD.

Definition 1.9. A $(mg, g, k, \lambda)_2$ difference family over $\mathbb{F}_2$, briefly a $(mg, g, k, \lambda)_2$ difference family, is a $(2^{mg} - 1, 2^g - 1, 2^k - 1, \lambda)$ difference family in $\mathbb{F}_{2^{mg}}^*$ with the property that $B \cup \{0\}$ is a subspace of $\mathbb{F}_2^{mg}$ for every $B \in \mathcal{F}$.

The above terminology is justified by the following result.

Proposition 1.10. *Every* $(mg, g, k, \lambda)_2$ *difference family generates a cyclic* $(mg, g, k, \lambda)_2$*-GDD.*

Proof. Let $\mathcal{F}$ be a $(mg, g, k, \lambda)_2$ difference family. So, by definition, $\mathcal{F}$ is a $(2^{mg}-1, 2^g-1, 2^k-1, \lambda)$ difference family in $\mathbb{F}^*_{2^{mg}}$. Let G be the subgroup of $\mathbb{F}^*_{2^{mg}}$ not covered by the list of differences of $\mathcal{F}$ and let $\mathcal{G}$ be the set of cosets of G in $\mathbb{F}^*_{2^{mg}}$. Then, by Theorem 1.6, the triple $\mathcal{D} = (\mathbb{F}_q^n, \mathcal{G}, dev\mathcal{F})$ is a cyclic $(2^{mg}-1, 2^g-1, 2^k-1, \lambda)$-GDD. Now note that G is the multiplicative group of the subfield of order 2^g of $\mathbb{F}_q^{mg}$. Hence, adding 0 to each member of $\mathcal{G}$ we get the so-called *regular* or *Desarguesian* g-spread. Also, each block of $dev\mathcal{F}$ is of the form xB with $x \in \mathbb{F}^*_{2^n}$ and $B \in \mathcal{F}$. On the other hand, by Definition 1.9, we have that $B \cup \{0\}$ is a subspace of $\mathbb{F}_{2^n}$ so that $xB \cup \{0\}$ is a subspace of $\mathbb{F}_{2^n}$ as well. Thus every block of $\mathcal{D}$ is a subspace of $\mathbb{F}_2^n$ deprived of the zero vector. We conclude that $\mathcal{D}$ can be seen as a $(mg, g, k, \lambda)_2$ design by Remark 1.3. □

The above proposition will allow us to get a cyclic $(n, 3, 3, 7)_2$-GDD for every $n \equiv 3 \pmod 6$.

2. Revisiting and improving Thomas' result on 2-$(n, 3, 7)$ designs over $\mathbb{F}_2$

Here we obtain a $(n, 3, 7)_2$ difference family for any positive odd integer n. Thus, in view of Proposition 1.4, we prove the following.

Theorem 2.1. *There exists a cyclic* 2-$(n, 3, 7)$ *design over* $\mathbb{F}_2$ *for every odd positive integer* n.

The above result was already obtained by Thomas [8] in the hypothesis that $\gcd(n, 6) = 1$. We first need to recall how the solvability of a quadratic equation over $\mathbb{F}_{2^n}$ can be established using the *absolute trace* of $\mathbb{F}_{2^n}$. This is the function $Tr : x \in \mathbb{F}_{2^n} \longrightarrow \sum_{i=0}^{n-1} x^{2^i} \in \mathbb{F}_2$. Some elementary properties of this function which could be useful later are the following:

$Tr(x) + Tr(y) = Tr(x + y)$ for all $x, y \in \mathbb{F}_{2^n}$;
$Tr(x^2) = Tr(x)$ for all $x \in \mathbb{F}_{2^n}$;
$Tr(1) = 0$ or 1 according to whether n is even or odd, respectively.

Here is the well known result concerning quadratic equations in a finite field of characteristic two (see, e.g., [7]).

Lemma 2.2. *Let* $ax^2 + bx + c = 0$ *be a quadratic equation in* $\mathbb{F}_{2^n}$ *and let* m *be the number of its distinct solutions in the same field. We have:*

$m = 1$ *if and only if* $b = 0$;
$m = 2$ *if and only if* $b \neq 0$ *and* $Tr(\frac{ac}{b^2}) = 0$;
$m = 0$ *if and only if* $b \neq 0$ *and* $Tr(\frac{ac}{b^2}) = 1$.

The following fact is an immediate consequence of the above lemma.

Lemma 2.3. *Let* $ax^2 + bx + c = 0$ *and* $\alpha x^2 + \beta x + \gamma = 0$ *be two quadratic equations in* $\mathbb{F}_{2^n}$ *with* $b\beta \neq 0$. *Exactly one of these equations is solvable in* $\mathbb{F}_{2^n}$ *if and only if* $Tr(\frac{ac}{b^2}) + Tr(\frac{\alpha\gamma}{\beta^2}) = 1$.

We are now ready to prove our main result.

Theorem 2.4. *There exists a* $(n, 3, 7)_2$ *difference family for every positive odd integer* n.

Proof. We first associate with every $x \in \mathbb{F}_{2^n}^* \setminus \{1\}$ the subspace S_x of $\mathbb{F}_2^n$ generated by 1, x and x^2. Note that these three elements are independent since, in the opposite case, we would have $x^2 + x + 1 = 0$ which implies $x^3 = 1$. This would mean that x has order 3 in $\mathbb{F}_{2^n}^*$ so that $2^n - 1$ would be divisible by 3 contradicting the hypothesis that n is odd. Thus S_x has dimension three. Now set $B_x := S_x \setminus \{0\}$, hence

$$B_x = \{1, x, x^2, x + 1, x^2 + 1, x^2 + x, x^2 + x + 1\}. \tag{2.1}$$

Note that $B_x = B_{x+1}$ for every x. It is convenient, anyway, to consider B_x and B_{x+1} as distinct blocks. Now consider the collection

$$\mathcal{F} := \{B_x \mid x \in \mathbb{F}_{2^n}^* \setminus \{1\}\}$$

and, for any $t \in \mathbb{F}_{2^n}^* \setminus \{1\}$, let $m(t)$ be the multiplicity of t in $\Delta\mathcal{F}$.

Let $\delta_{ij}(x)$ be the (i, j) entry in the following table

$-$	$\frac{1}{x}$	$\frac{1}{x^2}$	$\frac{1}{x+1}$	$\frac{1}{x^2+1}$	$\frac{1}{x^2+x}$	$\frac{1}{x^2+x+1}$
x	$-$	$\frac{1}{x}$	$\frac{x}{x+1}$	$\frac{x}{x^2+1}$	$\frac{1}{x+1}$	$\frac{x}{x^2+x+1}$
x^2	x	$-$	$\frac{x^2}{x+1}$	$\frac{x^2}{x^2+1}$	$\frac{x}{x+1}$	$\frac{x^2}{x^2+x+1}$
$x+1$	$\frac{x+1}{x}$	$\frac{x+1}{x^2}$	$-$	$\frac{1}{x+1}$	$\frac{1}{x}$	$\frac{x+1}{x^2+x+1}$
x^2+1	$\frac{x^2+1}{x}$	$\frac{x^2+1}{x^2}$	$x+1$	$-$	$\frac{x+1}{x}$	$\frac{x^2+1}{x^2+x+1}$
x^2+x	$x+1$	$\frac{x+1}{x}$	x	$\frac{x}{x+1}$	$-$	$\frac{x^2+x}{x^2+x+1}$
x^2+x+1	$\frac{x^2+x+1}{x}$	$\frac{x^2+x+1}{x^2}$	$\frac{x^2+x+1}{x+1}$	$\frac{x^2+x+1}{x^2+1}$	$\frac{x^2+x+1}{x^2+x}$	$-$

representing the list ΔB_x of quotients of B_x. More precisely, $\delta_{ij}(x)$ is the quotient between the i-th and the j-th element of B_x in the ordering of (2.1). For every $t \in \mathbb{F}_{2^n}^* \setminus \{1\}$, let $m_{ij}(t)$ be the number of distinct solutions in $\mathbb{F}_{2^n}$ of the equation

$$E_{ij}(t): \ \delta_{ij}(x) = t$$

in the unknown x. It is clear that we have

$$m(t) = \sum_{i \neq j} m_{ij}(t).$$

Note that $E_{ij}(t)$ can be rewritten as a quadratic equation $ax^2 + bx + c = 0$ with $b \neq 0$ for any pair (i, j) belonging to the 18-set

$$I = \{(1,6),(1,7),(2,5),(2,7),(3,4),(3,7),(4,3),(4,7),(5,2),\\ (5,7),(6,1),(6,7),(7,1),(7,2),(7,3),(7,4),(7,5),(7,6)\}.$$

Thus $m_{ij}(t) = 0$ or 2 for every $(i, j) \in I$. On the other hand, it is easily seen that for all twenty-four pairs $(i, j) \notin I$ we have $m_{ij}(t) = 1$ since in this case $E_{ij}(t)$ becomes either an equation of the first degree or an equation of the form $ax^2 + c = 0$. It follows that $m(t) = 24 + 2 \cdot r(t)$ where $r(t)$ is the number of equations $E_{ij}(t)$ with $(i, j) \in I$ which are solvable in $\mathbb{F}_{2^n}$. We want to prove that $r(t) = 9$ for every t. For this, we have to show that it is possible to match the eighteen equations $E_{ij}(t)$ with $(i, j) \in I$ in such a way that, in each match, only one equation is solvable in $\mathbb{F}_{2^n}$. Using Lemma 2.3 and taking into account the mentioned properties of the trace function, the reader can easily check that such a good matching is the following.

$E_{61}(t): \ x^2 + x + t = 0$	$E_{71}(t): \ x^2 + x + t + 1 = 0$
$E_{16}(t): \ tx^2 + tx + 1 = 0$	$E_{17}(t): \ tx^2 + tx + t + 1 = 0$
$E_{52}(t): \ x^2 + tx + 1 = 0$	$E_{37}(t): \ (t+1)x^2 + tx + t = 0$
$E_{72}(t): \ x^2 + (t+1)x + 1 = 0$	$E_{27}(t): \ tx^2 + (t+1)x + t = 0$
$E_{43}(t): \ tx^2 + x + 1 = 0$	$E_{73}(t): \ (t+1)x^2 + x + 1 = 0$
$E_{74}(t): \ x^2 + (t+1)x + t + 1 = 0$	$E_{47}(t): \ tx^2 + (t+1)x + t + 1 = 0$
$E_{75}(t): \ (t+1)x^2 + x + t + 1 = 0$	$E_{25}(t): \ tx^2 + x + t = 0$
$E_{76}(t): \ (t+1)x^2 + (t+1)x + 1 = 0$	$E_{67}(t): \ (t+1)x^2 + (t+1)x + t = 0$
$E_{34}(t): \ x^2 + tx + t = 0$	$E_{57}(t): \ (t+1)x^2 + tx + t + 1 = 0$

Consider, as an example, the third of the above pairs $(E_{52}(t), E_{37}(t))$. By Lemma 2.2, $E_{52}(t)$ is solvable if and only if $Tr(\frac{1}{t^2}) = 0$, while $E_{37}(t)$ is solvable if and only if $Tr(\frac{t+1}{t}) = 0$. Now, by the properties of the trace function, we have:

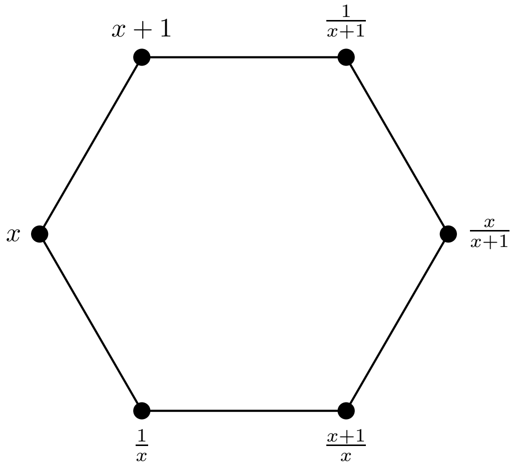
$$Tr\left(\frac{1}{t^2}\right) + Tr\left(\frac{t+1}{t}\right) = Tr\left(\frac{1}{t}\right) + Tr\left(\frac{t+1}{t}\right) = Tr(1) = 1.$$

Hence, by Lemma 2.3, only one of the two equations $E_{52}(t)$ and $E_{37}(t)$ is solvable in $\mathbb{F}_{2^n}$.

We conclude that $m(t) = 24 + 2 \cdot 9 = 42$ for any $t \in \mathbb{F}_{2^n}^* \setminus \{1\}$. This means that $\mathcal{F}$ is a $(n, 3, 42)_2$ difference family.

Now consider the 2-regular graph Γ with vertex-set $\mathbb{F}_{2^n}^* \setminus \{1\}$ where the two neighbors of any vertex x are $x + 1$ and $\frac{1}{x}$. It is clear that the connected components of Γ are all the hexagons of the form

$H_x :=$



We note that all blocks B_y with y lying in the hexagon H_x are in the same $\mathbb{F}_{2^n}^*$-orbit. Indeed we already commented that B_x and B_{x+1} coincide. Also, the reader can easily check that $B_{1/x} = \frac{1}{x^2} \cdot B_x$. It follows that all six blocks associated with the vertices of any hexagon of Γ produce the same list of quotients. Then, considering that $\mathcal{F}$ is a $(n, 3, 42)_2$ difference family, it is evident that if X is a complete system of representatives for the hexagons of Γ, then $\mathcal{F}' := \{B_x \mid x \in X\}$ is a $(n, 3, 7)_2$ difference family. The assertion follows. □

In the following we will keep the same notation that we used in the above proof. It is clear that the design constructed in the above theorem does not depend on the system X of representatives for the hexagons of Γ. Recall in fact that $B_x = B_{x+1}$ and that $B_x = x^2 \cdot B_{1/x}$ so that the blocks associated with the vertices of H_x have all the same development.

When $n \equiv \pm 1 \pmod 6$, that is the case also considered by Thomas, our design coincides with his design. Indeed our blocks are exactly what he calls *special triangles*. The two descriptions are different since while Thomas' approach is essentially geometric, our approach is purely algebraic.

Now, given $x \in \mathbb{F}_{2^n}^* \setminus \{1\}$, we want to show that a block B_y of the $(n, 3, 7)_2$ difference family $\mathcal{F}$ is in the same $\mathbb{F}_{2^n}^*$-orbit of B_x if and only if y is in $V(H_x)$, the set of vertices of the hexagon H_x. The "if-part" has been already shown in the proof of Theorem 2.4. Let us prove the "only-if-part". Assume that B_y is in the same $\mathbb{F}_{2^n}^*$-orbit of B_x so that there exists a non-zero field element t such that $B_y = tB_x$. Such equality implies that $\begin{cases} 1 = tf_0 \\ y = tf_1 \\ y^2 = tf_2 \end{cases}$ with (f_0, f_1, f_2) a triple of distinct elements of B_x. In its turn the above system implies that $f_0f_2 + f_1^2 = 0$. Considering the form of the elements of B_x, we see that

$$f_0f_2 + f_1^2 = c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4$$

for a suitable quintuple $(c_0, \dots, c_4)$ of elements of $\mathbb{F}_2$, namely x is a zero of the polynomial $p(z) = \sum_{i=0}^{4} c_iz^i \in \mathbb{F}_2[z]$. First note that $p(z)$ is the null polynomial – namely we have $c_i = 0$ for each i – exactly when (f_0, f_1, f_2) and y are as follows:

f_0	1	x^2	1	x^2+1	x^2	x^2+1
f_1	x	x	$x+1$	$x+1$	x^2+x	x^2+x
f_2	x^2	1	x^2+1	1	x^2+1	x^2
y	x	$\frac{1}{x}$	$x+1$	$\frac{1}{x+1}$	$\frac{x+1}{x}$	$\frac{x}{x+1}$

So we see that in this case y is a vertex of H_x.

Now assume that $p(z)$ has degree d with $1 \le d \le 4$. In this case the zeros of $p(z)$ lying in $\mathbb{F}_{2^n}$ are in the subfield of order $2^{\gcd(n,d)}$. Considering that n is odd we have either $\gcd(n, d) = 1$ or $\gcd(n, d) = 3$. In the first case x should lie in the subfield of order 2, i.e., $x \in \{0, 1\}$ which is absurd. In the second case x would be in the subfield $\mathbb{K}$ of order 8 and consequently both B_x and $V(H_x)$ coincide with $\mathbb{K}^* \setminus \{1\}$. It immediately follows that y is also in $\mathbb{K}$ and then $y \in V(H_x)$.

It is clear that the stabilizer of any B_x is a common divisor of $2^n - 1$ and $|B_x| = 7$. Thus it is always trivial when $n \equiv \pm 1 \pmod 6$. Instead, for $n \equiv 3 \pmod 6$, B_x has non-trivial stabilizer if and only if B_x is the multiplicative group of the subfield $\mathbb{K}$ of order 8.

The above considerations, together with Remark 1.1, allow us to state the following.

Remark 2.1. The cyclic $(n, 3, 7)_2$ design constructed in Theorem 2.4 is simple if and only if $n \equiv \pm 1 \pmod 6$.

When $n \equiv 3 \pmod 6$, that is the case not considered by Thomas, $\mathbb{F}_{2^n}$ has a subfield $\mathbb{K}$ of order 8 and we already commented that for every $x \in \mathbb{K}^*$ the block B_x coincides with $\mathbb{K}^*$ (which is also the vertex-set of H_x). Thus, if y is the representative of X in $\mathbb{K}^*$, then $\mathcal{F}'$ is a $(2^n - 1, 7, 7)$ difference family in $\mathbb{F}_{2^n}^*$ with a base block B_y that is a subgroup of $\mathbb{F}_{2^n}^*$. It follows, by Proposition 1.7, that $\mathcal{F}'' := \mathcal{F}' \setminus \{B_y\}$ is a $(n, 3, 3, 7)_2$ difference family and then, by Proposition 1.10, we can state the following.

Theorem 2.5. *There exists a cyclic and simple* $(n, 3, 3, 7)_2$ *group divisible design for every integer* $n \equiv 3$ $(mod\ 6)$.

As far as we know this the first infinite family of cyclic GDDs over a finite field.

Acknowledgments

This work has been performed under the auspices of the G.N.S.A.G.A. of the C.N.R. (National Research Council) of Italy. The first author carried out this research within the project "Disegni combinatori con un alto grado di simmetria", supported by Fondo Ricerca di Base, 2015, of Università degli Studi di Perugia. The second author is supported in part by the Croatian Science Foundation under the project 6732.

References

[1] R.J.R. Abel, M. Buratti, Difference families, in: C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs, second edition, Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. 392–409.
[2] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, Cambridge, 1999.
[3] M. Buratti, Recursive constructions for difference matrices and relative difference families, J. Comb. Des. 6 (1998) 165–182.
[4] M. Buratti, M. Kiermaier, S. Kurz, A. Nakić, A. Wassermann, q-analogs of group divisible designs, in: K.-U. Schmidt, A. Winterhof (Eds.), Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications, in: Radon Series on Computational and Applied Mathematics, vol. 23, de Gruyter, Berlin, 2019.
[5] M. Braun, T. Etzion, P.R.J. Östergård, A. Vardy, A. Wassermann, On the existence of q-analogs of Steiner systems, Forum Math. PI 4 (2016).
[6] M. Braun, M. Kiermaier, A. Wassermann, q-analogs of designs: subspace designs, in: M. Greferath, M.O. Pavčević, N. Silberstein, M.A. Vázquez-Castro (Eds.), Network Coding and Subspace Designs, Springer International Publishing, 2018, pp. 171–211.
[7] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Oxford Mathematical Monographs, Clarendon Press, 1998.
[8] S. Thomas, Designs over finite fields, Geom. Dedic. 93 (1987) 237–242.