# *Orthogonal Double Covers by Super-Extendable Cycles*

**Christian Bey, Sven Hartmann, Uwe Leck, Volker Leck**
*Universitőt Rostock, Fachbereich Mathematik, 18051 Rostock, Germany*

Received January 2, 2001; revised February 20, 2002

**Abstract: An Orthogonal Double Cover (ODC) of the complete graph $K_n$ by an almost-hamiltonian cycle is a decomposition of $2K_n$ into cycles of length $n-1$ such that the intersection of any two of them is exactly one edge. We introduce a new class of such decompositions. If $n$ is a prime, the special structure of such a decomposition allows to expand it to an ODC of $K_{n+1}$ by an almost-hamiltonian cycle. This yields the existence of an ODC of $K_{p+1}$ by an almost-hamiltonian cycle for primes $p$ of order $3 \bmod 4$ and its eventual existence for arbitrary primes $p$.** © 2002 Wiley Periodicals, Inc. J Combin Designs 10: 283–293, 2002; Published online in Wiley InterScience (www.interscience.wiley.com). DOI 10.1002/jcd.10011

**Keywords:** *edge decomposition; ODC; cycle; asymptotic existence*

## 1. INTRODUCTION

Let $\mathcal{O} = \{G_0, \ldots, G_{n-1}\}$ be a collection of $n$ simple spanning graphs on an $n$-element vertex set and let $K_n$ denote the complete graph on this vertex set. We call $\mathcal{O}$ an *orthogonal double cover* (ODC) of $K_n$, if it has the following properties:

(1) *Double Cover Property*:
Every edge of $K_n$ is covered by exactly two of the graphs $G_0, \ldots, G_{n-1}$;
(2) *Orthogonality Property*:
For every choice of integers $i, j$ with $0 \leq i < j \leq n-1$, the graphs $G_i$ and $G_j$ have exactly one common edge.

The graphs $G_0, \ldots, G_{n-1}$ are called *pages*. If all pages are isomorphic to a graph $G$, we speak of an *ODC by G.* As an immediate consequence of the definition of an ODC, we can compute the number of edges of each page.

*Correspondence to:* Uwe Leck, Universitőt Rostock, Fachbereich Mathematik, 18051 Rostock, Germany;
E-mail: uwe.leck@mathematik.uni-rostock.de

**Lemma 1.1.** *Every page of an ODC of $K_n$ has exactly $n-1$ edges.*

The question of the existence of an ODC originated in two articles by Alspach, Heinrich, and Rosenfeld [2] and Hering [10], who asked for the existence of an ODC by an almost-hamiltonian cycle. Since then, different classes of graphs have been investigated, among them paths, trees of small diameter, graphs consisting of small cliques, graphs of maximum degree two. For more information, see the survey studies [1, 7].

In the sequel, we consider the original problem of the existence of an ODC of $K_n$ by an almost-hamiltonian cycle, that is, a graph consisting of a cycle of length $n-1$ and an isolated vertex.

Let an additive group $\mathcal{G}$ on the set $\{0,\dots,n-1\}$ be given, and let the vertices of $K_n$ be denoted by the elements of $\mathcal{G}$. We call an ODC $\mathcal{O}$ of $K_n$ *group-generated* by $\mathcal{G}$, if the page $G_i$ of $\mathcal{O}$ is derived from a given page $G_0$ by adding (with respect to $\mathcal{G}$) the fixed element $i \in \mathcal{G}$ to every vertex of $G_0$. We use the notation $G_i = G_0 + i$ for this property. Thus, a group-generated ODC is determined completely already by one arbitrary page $G_0$ and the generating group $\mathcal{G}$. We call $G_0$ *ODC-generating* (or *ODC-generator*) with respect to $\mathcal{G}$.

Alspach, Heinrich, and Rosenfeld [2] introduced a construction of an ODC-generating almost-hamiltonian cycle with respect to the additive group of a finite field. They made the following observation.

**Theorem 1.1** ([2]). *Let $GF(q)$ be the finite field of order $q, q > 3$. Furthermore, let $\omega$ be a primitive element. Then, the cycle $(1,\omega,\omega^2,\dots,\omega^{q-2})$ is an ODC-generating almost-hamiltonian cycle with respect to the additive group of $GF(q)$.*

This construction was found, independently, also by Hering [10]. In addition, he verified the existence of an ODC of $K_n$ by an almost-hamiltonian cycle for $4 \le n \le 36$. Heinrich and Nonay [9] constructed an ODC of $K_{4n}$ by an almost-hamiltonian cycle from an ODC of $K_n$ by a path.

The nonexistence of an abelian-group-generated ODC by an almost-hamiltonian cycle has been shown for a certain class of vertex numbers by Ganter, Gronau, and Mullin [5].

**Theorem 1.2** ([5]). *There is no ODC-generating almost-hamiltonian cycle with respect to an abelian group of order $n$, whenever $n \equiv 2 \bmod 4$.*

## 2. NEARLY-CYCLIC ODCs

Hering [10] introduced a class of ODCs by almost-hamiltonian cycles in which all but one page are generated cyclically from a given cycle.

Let $g \in \mathbb{Z}_n$ be an element of order $n$. An ODC $\mathcal{O}$ of $K_{n+1}$ by an almost-hamiltonian cycle is called *nearly-cyclic*, if it consists of cycles $C_0,\dots,C_{n-1}$ and $C_\infty$ on the vertex set $\mathbb{Z}_n \cup \{\infty\}$ such that, for $i \in \mathbb{Z}_n$, $C_i = C_0 + i$ where the addition in $\mathbb{Z}_n$ is extended by $\infty + i = \infty$. Furthermore, $C_\infty$ is the almost-hamiltonian cycle $(0, g, 2g, 3g, \dots, (n-1)g)$ generated by the multiples of $g$ with the isolated vertex $\infty$. We say, the pair $(C_0, g)$ generates $\mathcal{O}$.

**Example 2.1.** If we choose $g = 1$ in $\mathbb{Z}_5$ and let $C_0 = (\infty, 0, 3, 4, 2)$, then the pair $(C_0, g)$ generates a nearly-cyclic ODC of $K_6$ consisting of the almost-hamiltonian cycles $C_0 = (\infty, 0, 3, 4, 2), C_1 = (\infty, 1, 4, 0, 3), C_2 = (\infty, 2, 0, 1, 4)$, $C_3 = (\infty, 3, 1, 2, 0)$, $C_4 = (\infty, 4, 2, 3, 1)$, and $C_\infty = (0, 1, 2, 3, 4)$.

In other than cyclic groups, there are no generating elements. Hence, for those groups the graph $C_\infty$ is not an almost-hamiltonian cycle. Therefore, we focus on cyclic groups.

Hering [11] verified the existence of a nearly-cyclic ODC of $K_n$ by an almost-hamiltonian cycle for $4 \leq n \leq 36$. He also observed that the number of such nearly-cyclic ODCs seems to grow much faster than the number of cyclic ODCs by almost-hamiltonian cycles. In addition, there is no restriction to vertex numbers of order $\not\equiv 2 \bmod 4$ for a nearly-cyclic ODC as in the case of a cyclic ODC by an almost-hamiltonian cycle (see Theorem 1.2).

Hering [10] used a finite field $GF(q)$ to generate a nearly-cyclic ODC. To describe this construction, we adopt multiplicative notation. Then, such an ODC $\mathcal{O}$ consists of almost-hamiltonian cycles $C_0$ and $C_1, C_\omega, C_{\omega^2}, \ldots, C_{\omega^{q-2}}$ on the elements of $GF(q)$, where the field has order $q$ and $\omega$ is a primitive element. Furthermore, $C_{\omega^i} = \omega^i C_1$ and $C_0 = (1, \omega, \omega^2, \ldots, \omega^{q-2})$. Again, we say that the pair $(C_1, \omega)$ generates $\mathcal{O}$.

**Theorem 2.1** ([10]). *Let $GF(q)$ be a finite field of order $q > 3$, and let $\omega$ be a primitive element. Furthermore, define the almost-hamiltonian cycle $C_1 = (0, \omega - 1,\ \omega^2 - 1, \ldots,\ \omega^{q-2} - 1)$ on the elements of $GF(q)$. Then, the pair $(C_1, \omega)$ generates a nearly cyclic ODC of $K_q$.*

**Example 2.2.** In $GF(5)$, we choose $\omega = 2$ and define $C_1 = (0, 1, 3, 2)$. Then, the pair $(C_1, \omega)$ generates a nearly-cyclic ODC of $K_5$ consisting of the almost-hamiltonian cycles $C_1 = (0, 1, 3, 2)$, $C_2 = (0, 2, 1, 4)$, $C_3 = (0, 4, 2, 3)$, $C_4 = (0, 3, 4, 1)$, and $C_0 = (1, 2, 4, 3)$.

Unfortunately, Theorem 2.1 does not settle the existence of an ODC by an almost-hamiltonian cycle for new classes of vertex numbers, since we know already by Theorem 1.1 that there is a cyclic ODC by an almost-hamiltonian cycle in every finite field.

Next, we describe necessary and sufficient conditions on a pair to generate a nearly-cyclic ODC. Since we investigate arbitrary cyclic groups, we use additive notation. Let the *length* $\ell$ of an edge $\{a, b\}$ be defined as $\{\pm(a - b)\}$. Now, let $\{a, b\}$ and $\{c, d\}$ be edges of the same length, such that $a - c = b - d$. The *distance* dist of $\{a, b\}$ and $\{c, d\}$ is defined as $\{\pm(a - c)\}$.

**Lemma 2.1** (cf [10]). *Let $C$ be an almost-hamiltonian cycle on the elements of $\mathbb{Z}_n \cup \{\infty\}$ containing the edges $\{\infty, a\}$ and $\{\infty, b\}$. Furthermore, let $P_C$ denote the path arising from $C$ by deleting the edges $\{\infty, a\}$ and $\{\infty, b\}$. The pair $(C, g)$, where $g \in \mathbb{Z}_n$ is of order $n$, generates a nearly-cyclic ODC of $K_{n+1}$ by an almost-hamiltonian cycle, if and only if the following conditions are satisfied:*

(a) *For all elements $z \in \mathbb{Z}_n \backslash \{0, g\}$ of order different from 2, there are exactly two edges of length $\{\pm z\}$ in $P_C$;*

(b) *If $n$ is even, then there is exactly one edge of length $\{\frac{n}{2}\}$ in $P_C$;*

(c) *There is exactly one edge of length $\{\pm g\}$ in $P_C$;*

(d) *The order of the element $a - b$ is not 2, i.e., $a - b \neq \frac{n}{2}$;*

(e) *The union of the distances of edges of the same length includes all elements from* $\mathbb{Z}_n \backslash \{0, a-b, -a+b\}$ *of order different from* 2.

In the original formulation of the lemma, Hering [10] restricted $g$ to be 1.

**Example 2.3.** In the cycle $C = (\infty, 0, 3, 4, 2)$ from Example 4, we have that $P_C = 0, 3, 4, 2$. In $\mathbb{Z}_5$, $\ell(\{0,3\}) = \{\pm 2\}$, $\ell(\{3,4\}) = \{\pm 1\}$, $\ell(\{4,2\}) = \{\pm 2\}$ and $\text{dist}(\{0,3\}, \{4,2\}) = \{\pm 1\}$. Clearly, there is no element of order 2 in $\mathbb{Z}_5$. Hence, the pair $(C, 1)$ fulfills the conditions of Lemma 2.1.

## 3. EXTENDABLE CYCLES

Let the cycle $A = (v_1, \ldots, v_{n-1})$ be an ODC-generator with respect to $\mathbb{Z}_n$. We obtain a cycle $C$ on the vertex set $Z_n \cup \{\infty\}$ after replacing an edge $\{v_i, v_{i+1}\}$ in $A$ by the path $v_i, \infty, v_{i+1}$. If there is an edge $\{v_i, v_{i+1}\}$ in $A$ and an element $g \in \mathbb{Z}_n$ such that the pair $(C, g)$ generates a nearly-cyclic ODC of $K_{n+1}$ by an almost-hamiltonian cycle, then we call $A$ *extendable*.

As pointed out by Gronau [6], there are necessary and sufficient conditions on a cyclic ODC-generating cycle to be extendable.

**Lemma 3.1** ([6]). *An ODC-generating almost-hamiltonian cycle A with respect to* $\mathbb{Z}_n$ *is extendable, if and only if there is an element* $g \in \mathbb{Z}_n$ *of order n such that the two edges of length* $\{\pm g\}$ *in A have also distance* $\{\pm g\}$.

*Proof.* In order to comply with the first three conditions in Lemma 2.1, we have to replace an edge $\{v_i, v_{i+1}\}$ of length $\{\pm g\}$, where $g \in \mathbb{Z}_n$ is of order $n$. Clearly, then also the fourth condition holds.

Let $P$ be the path arising from $A$ by deleting $\{v_i, v_{i+1}\}$. Since $A$ is an ODC-generator, the set of distances of edges with the same length in $P$ is $\mathbb{Z}_n \backslash \{0, \pm d\}$, where $\{\pm d\}$ is the distance that involves $\{v_i, v_{i+1}\}$. Thus, by the fifth condition in Lemma 2.1, $\{\pm d\} = \{\pm(v_i - v_{i+1})\} = \{\pm g\}$. □

The two edges of length $\{\pm g\}$ have a common vertex. Hence, they are neighboring edges on the cycle.

**Example 3.1.** The cycle $(1, 5, 2, 3, 4, 6)$ is an ODC-generator with respect to $\mathbb{Z}_7$. Furthermore, $\ell(\{2,3\}) = \ell(\{3,4\}) = \{\pm 1\}$. Thus, by Lemma 3.1, the cycle is extendable, and the pair $((\infty, 3, 4, 6, 1, 5, 2), 1)$ generates a nearly-cyclic ODC of $K_8$ by an almost-hamiltonian cycle.

We modified a hill-climbing algorithm of Dinitz and Stinson [4] to construct ODC-generating almost-hamiltonian cycles consisting of two starters such that the distance of the edges of length $\{\pm 1\}$ is $\{\pm 1\}$. We derived the following results for small cyclic groups of odd order.

**Lemma 3.2.** *Let* $7 \leq 2n+1 \leq 101$, $2n+1 \neq 9$. *There exists an extendable ODC-generating almost-hamiltonian cycle with respect to* $\mathbb{Z}_{2n+1}$.

**Corollary 3.1.** *Let* $8 \leq 2n \leq 102$, $2n \neq 10$. *There is a nearly-cyclic ODC of* $K_{2n}$ *by an almost-hamiltonian cycle.*

The unique ODC-generating cycle with respect to $\mathbb{Z}_5$ is not extendable. There is no ODC-generating cycle with respect to $\mathbb{Z}_9$ [11].

## 4. SUPER-EXTENDABLE CYCLES

Some of the extendable ODC-generating cycles possess an even stronger property. Namely, for any non zero element $g$ of the cyclic group, the edges of length $\{\pm g\}$ have distance $\{\pm g\}$. Thus, edges of the same length are neighboring. This means that the cycle is extendable at an edge of length $\{\pm g\}$ whenever $g$ is a generating element.

More general, we call an almost-hamiltonian cycle on the elements of some odd order abelian group $\mathcal{A}$ *super-extendable*, if, for every $a \in \mathcal{A}\backslash\{0\}$, there are exactly two edges of length $\{\pm a\}$, and these two edges are adjacent.

**Remark 4.1.** A super-extendable almost-hamiltonian cycle consists of two skew-orthogonal starters (see [4] for definition). Hence, super-extendability implies the property of being ODC-generating.

**Remark 4.2.** Since in a cyclic group $\mathbb{Z}_p$ of prime order every nonzero element generates the group, a super-extendable cycle with respect to $\mathbb{Z}_p$ is extendable at any of its edges.

**Example 4.1.** The cycle $(1, 5, 2, 3, 4, 6)$ from Example 10 is super-extendable.

**Example 4.2.** The cycle $(1, 4, 7, 5, 3, 12, 8, 2, 9, 10, 11, 6)$ generates an ODC with respect to $\mathbb{Z}_{13}$ and is super-extendable.

Let $GF(q)$ be the finite field of order $q$, where $q = 2^e t + 1$ and $t$ is odd. Furthermore, let $T$ be the cyclic subgroup of order $t$ of the multiplicative group of $GF(q)$, and let $\delta$ be a generator of $T$.

Following Examples 4.1 and 4.2, our objective is to construct a super-extendable almost-hamiltonian cycle on the elements of $GF(q)$ as the union of a path $P_1 = p_0, p_1, \ldots, p_{2^e}$, where $p_0 = 1$ and $p_{2^e} = \delta$, and paths $\delta^i P_1$ for $0 \leq i < t$. To ensure a cycle on the nonzero elements of $GF(q)$ by this construction, we have to choose the $p_j$'s, $1 \leq j \leq 2^e$, from distinct cosets modulo $T$. To make sure that edges of the same length share a vertex, we demand that

$$p_{2j} - p_{2j+1} = p_{2j+1} - p_{2j+2} \quad \text{for} \quad 0 \leq 2j \leq 2^e - 2. \tag{1}$$

An edge $\{p_{2j}, p_{2j+1}\}$ in $P_1$ generates the lengths $\{\pm\delta^i(p_{2j} - p_{2j+1})\}$, $0 \leq i < t$, in the cycle. Hence, to force every edge length to occur in the cycle, we further need to choose the $p_j$'s in such a way that the differences $p_{2j} - p_{2j+1}$ for $0 \leq 2j < 2^e - 2$ lie in distinct cosets modulo $T \cup (-T)$.

**Example 4.3.** Let us consider $GF(13)$. Since $13 = 2^2 \cdot 3 + 1$, the subgroup $T$ is of order 3. We find that $T$ has the element set $\{1, 3, 9\}$. Thus, we derive modulo $T$ the four cosets $C_0 = T = \{1, 3, 9\}$, $C_1 = \{2, 5, 6\}$, $C_2 = \{4, 10, 12\}$, and $C_3 = \{7, 8, 11\}$. We observe that $C_0 = -C_2$ and $C_1 = -C_3$.

Now, let us consider the path $P_1 = 1, 4, 7, 5, 3$. Clearly, $4, 7, 5, 3$ are from distinct cosets. The occurring differences in $P_1$ are $\{\pm 3\}$ and $\{\pm 2\}$ and comply with Equation (1). Furthermore, they are from distinct cosets modulo $T \cup (-T)$. Hence, $P_1$ fulfills the conditions we need, and the graph arising as the union of $P_1$, $3P_1 = 3, 12, 8, 2, 9$, and $9P_1 = 9, 10, 11, 6, 1$ is a super-extendable cycle with respect to $\mathbb{Z}_{13}$. This cycle is the one given in Example 4.2.

**Example 4.4.** We have that $41 = 2^3 \cdot 5 + 1$. In $GF(41)$, the subgroup $T$ consists of the elements $1, 16, 10, 37, 18$. Thus, we derive the cosets

$$\begin{array}{ll} C_0 = T = \{1,16,10,37,18\} & C_1 = \{2,32,20,33,36\} \\ C_2 = \{3,7,30,29,13\} & C_3 = \{4,23,40,25,31\} \\ C_4 = \{5,39,9,21,8\} & C_5 = \{6,14,19,17,26\} \\ C_6 = \{11,12,28,38,34\} & C_7 = \{15,35,27,22,24\}. \end{array}$$

We observe that $C_0 = -C_3$, $C_1 = -C_4$, $C_2 = -C_6$, and $C_5 = -C_7$.
In the path $P_1 = 1, 34, 26, 3, 21, 27, 33, 4, 16$, apart from 1 and 16, all elements are from distinct cosets. Furthermore, $P_1$ satisfies the Equation (1), the occurring lengths are $\{\pm 8\}, \{\pm 18\}, \{\pm 6\}$, and $\{\pm 12\}$. These are from distinct cosets modulo $T \cup (-T)$. Thus, the union of the paths $16^i \cdot P_1$, $0 \leq i < 5$,

$$\begin{array}{l} 1,34,26,3,21,27,33,4,16 \\ 16,11,6,7,8,22,36,23,10 \\ 10,12,14,30,5,24,2,40,37 \\ 37,28,19,29,39,15,32,25,18 \\ 18,38,17,13,9,35,20,31,1 \end{array}$$

is a super-extendable cycle with respect to $\mathbb{Z}_{41}$.

**Remark 4.3.** A super-extendable cycle arising from this construction consists of two so called $2^{e-1}$-quotient coset starters. These starters were introduced by Dinitz and Stinson [3].

The main result of this work is the proof of the existence of super-extendable cycles for almost all prime powers with a nontrivial multiplicative subgroup of odd order.

**Theorem 4.1.** *Let $GF(q)$ be the finite field of order $q = 2^e t + 1$ with $t$ odd and greater than some integer $t_0(e)$. Then, there is a path $P_1$ with the properties described above. Hence, there is a super-extendable cycle with respect to the additive group of $GF(q)$.*

This statement is a direct consequence of Theorem 5.1, which will be proved in Section 5.

From Theorem 4.1 and Lemma 3.1, we derive a new class of ODCs by almost-hamiltonian cycles.

**Corollary 4.1.** *Let $q$ be a prime with $q = 2^e t + 1$, where $t$ is odd and greater than some integer $t_0(e)$. Then, there exists an ODC of $K_{q+1}$ by an almost-hamiltonian cycle.*

We remark that, by Corollary 5.1, $t_0(1) = 1$, i.e., for every prime $q \equiv 3 \bmod 4$, $q > 3$, there is an ODC of $K_{q+1}$ by an almost-hamiltonian cycle.

## 5. PROOF OF THE MAIN RESULT

Throughout, let $b$ be an even positive integer, and $q \equiv b + 1 \bmod 2b$ be a prime power. We consider the finite field $GF(q)$ with elements $0, 1, \ldots, q - 1$. By $\Gamma$, we denote the cyclic multiplicative group of $GF(q)$, and by $T$ its unique subgroup of index $b$. Note, that $T \cup (-T)$ is the unique subgroup of index $b/2$ in $\Gamma$.

In this section, we are going to prove the following result.

**Theorem 5.1.** *For every even positive integer $b$ and almost every prime power $q \equiv b+1 \bmod 2b$, there exist elements $p_0 = 1, p_1, \ldots, p_b$ satisfying*

- $(a')$ *$p_b$ is a generator of $T$,*
- $(b')$ *the elements $p_i$ lie in pairwise distinct cosets modulo $T$,*
- $(c')$ $p_{2j} - p_{2j-1} = p_{2j-1} - p_{2j-2}$,
- $(d')$ *the differences $p_{2j} - p_{2j-1}$ lie in pairwise distinct cosets modulo $T \cup (-T)$,*

*where $i$ runs over $\{1, \ldots, b\}$, and $j$ over $\{1, \ldots, b/2\}$.*

Clearly, condition (c′) can be rewritten as

$$p_{2j-1} = \tfrac{1}{2}(p_{2j} + p_{2j-2}), \tag{2}$$

such that condition (d′) says that the elements $\frac{1}{2}(p_{2j} - p_{2j-2})$ lie in pairwise distinct cosets modulo $T \cup (-T)$, for $j$ running over $\{1, \ldots, b/2\}$.

In the first place, let $b$ equal to 2. In this case, we only have two cosets modulo $T$, namely $T$ and $-T$. Hence, it suffices to find an element $p_2$ generating $T$, such that $p_1 = \frac{1}{2}(p_2 + 1)$ belongs to $-T$. One observation may be noted almost immediately. Suppose, 3 is a generator of the multiplicative group $\Gamma$, for example for $q = 7$. We put $p_2 = -3$, which generates $T$, and put $p_1 = \frac{1}{2}(p_2 + 1) = \frac{1}{2}(-2) = -1$, which is in $-T$. This gives us a first partial result, which will be recorded for future reference.

**Lemma 5.1.** *For $b = 2$ and every prime power $q \equiv 3 \bmod 4$ having 3 as a generator of $\Gamma$, there exist elements $p_0 = 1, p_1, p_2$ satisfying the conditions $(a'$–$d')$ in Theorem 5.1.*

To verify the claimed result in general, we need some well-known definitions from group theory. A *character* on $\Gamma$ is a map $\chi$ from $\Gamma$ to the complex numbers such that $|\chi(x)| = 1$ and $\chi(xy) = \chi(x)\chi(y)$ hold for all elements $x$ and $y$ in $\Gamma$. The characters on $\Gamma$ form a cyclic group of order $q - 1$, the *dual group* $\Gamma^{\perp}$ of $\Gamma$. For every positive integer $d$, let $M_d$ be the set of all characters of order $d$ in $\Gamma^{\perp}$. By $\chi^0$, we denote the *trivial character* with $\chi^0(x) = 1$ for each element $x \in \Gamma$.

For $b = 2$, $T$ is the set of all squares in $\Gamma$, and the character $\eta$ given by

$$\eta(x) = \begin{cases} 1 & \text{if } x \in T, \\ -1 & \text{if } x \in (-T) \end{cases}$$

is said to be the *quadratic character* on $\Gamma$.

For every element $x \in \Gamma$, put

$$V(x) = \sum_{d|q-1} \frac{\mu(d)}{\phi(d)} \sum_{\chi \in M_d} \chi(x),$$

where $\mu$ is the *Möbius function*, and $\phi$ the *Euler totient function*. According to Vinogradov (see [13, p.258, Ex.5.14]), $V(x)$ equals $(q-1)/\phi(q-1)$ if $x$ is a generator of $\Gamma$, and vanishes otherwise. Next, we put

$$P(x) = V(-x)(1 - \eta(\tfrac{1}{2}(x+1))).$$

It is not difficult to check, that $P(x)$ is positive if and only if $x$ generates $T$ and $\frac{1}{2}(x+1)$ lies not in $T$.

**Example 5.1.** For q = 7, the element 3 is a generator of the multiplicative group $\Gamma$. It is easy to compute $V(3) = 3$ and $P(-3) = V(3)(1 - \eta(\frac{1}{2}(-2))) = V(3)\ (1- \eta(-1)) = 6$. Hence, the element $x = -3$ has the desired properties.
It is now convenient to extend the definition of a character $\chi$ on $\Gamma$ by setting

$$\chi(0) = \begin{cases} 1 & \text{if } \chi = \chi^0, \\ 0 & \text{otherwise.} \end{cases}$$

Clearly, this definition implies $V(0) = 1$ and

$$P(0) = \begin{cases} 0 & \text{if } \frac{1}{2} \in T, \\ 2 & \text{if } \frac{1}{2} \notin T. \end{cases}$$

To ensure the existence of an element $x$ generating $T$, such that $\frac{1}{2}(x+1) \in (-T)$ holds, it suffices to confirm the relation

$$\sum_{x \in GF(q)} P(x) > P(0). \tag{3}$$

When expanding the left hand side of this inequality, we obtain

$$\begin{aligned} \sum_{x \in GF(q)} P(x) &= \sum_{x \in GF(q)} V(x) - \eta(\tfrac{1}{2}) \sum_{x \in GF(q)} V(-x)\eta(x+1) \\ &= q - \eta(\tfrac{1}{2}) \sum_{d \mid q-1} \frac{\mu(d)}{\phi(d)} \sum_{\chi \in M_d} \sum_{x \in GF(q)} \chi(-x)\eta(x+1). \end{aligned}$$

The inner sum $J(\chi, \eta) = \sum_{x \in GF(q)} \chi(-x)\eta(x+1)$ is called the *Jacobi sum* of $\chi$ and $\eta$. By virtue of [13, p.209], we have

$$|J(\chi, \eta)| = \begin{cases} 0 & \text{if } \chi = \chi^0, \\ 1 & \text{if } \chi = \eta, \\ q^{1/2} & \text{otherwise,} \end{cases}$$

for the absolute value of the Jacobi sum. This enables us to infer

$$\left|\sum_{x\in GF(q)} P(x) - q\right| \leq \sum_{d|q-1} \frac{|\mu(d)|}{\phi(d)} \sum_{\chi\in M_d} |J(\chi,\eta)|$$
$$\leq q^{1/2} \sum_{d|q-1} |\mu(d)|.$$

With $\alpha(q) = \sum_{d|q-1} |\mu(d)|$, we obtain

$$\sum_{x\in GF(q)} P(x) \geq q - q^{1/2}\alpha(q).$$

In order to conclude (3), it remains to show $q - q^{1/2}\alpha(q) > 2$, i.e.,

$$\alpha(q) < q^{1/2} - 2q^{-1/2} \tag{4}$$

for almost all $q$. This turns out to be possible with the help of a result by Lenstra and Schoof [12]. Recall, that $\log_2 \alpha(q)$ equals the number of distinct prime factors of $q - 1$, as pointed out in [13, p.142, Ex.3.32].

**Lemma 5.2** ([12]). *Let $m$ and $k$ be positive integers, and let $P_k$ be the set of all primes not exceeding $k$. The number $s$ of distinct prime factors of $m$ satisfies*

$$s \leq \frac{1}{\log_2 k}\left(\log_2 m - \sum_{p\in P_k} \log_2 p\right) + |P_k|.$$

For $m = q - 1$, this implies

$$\alpha(q) \leq 2^{|P_k|}(q-1)^{1/\log_2 k} \prod_{p\in P_k} p^{-1/\log_2 k}.$$

It is advantageous to choose $k = 12$ with $P_{12} = \{2, 3, 5, 7, 11\}$, which leads to

$$\alpha(q) \leq 2^5 \cdot 2310^{-1/\log_2 12}(q-1)^{1/\log_2 12}. \tag{5}$$

A straightforward calculation shows the right-hand side of (5) to be smaller than the right-hand side of (4) whenever $q \geq 375$. This establishes (3) for almost all prime powers $q \equiv 3 \bmod 4$.

For the remaining values $q < 375$, we checked (4) directly by calculating $\alpha(q)$. It is a remarkable fact, that (4) holds for each $q \equiv 3 \bmod 4$ not in the set $\{3, 7, 11, 19, 31, 43, 67, 211\}$. For $q = 11$ we have $P(3) = 5$, and for $q = 67$ we have $P(16) = 33/5$. For all other values different from 3, however, Lemma 5.1 applies.

Thus we may even conclude the following result.

**Corollary 5.1.** *For $b = 2$ and every prime power $q > 3$ with $q \equiv 3 \bmod 4$, there exist elements $p_0 = 1, p_1, p_2$ satisfying the conditions $(a'–d')$ in Theorem 5.1.*

Henceforth, let $b$ be larger than 2. We choose some bijection $\beta$ from $\{1,\ldots,b\}$ onto $\Gamma/T$ such that $\beta(b)=T$ and $\beta(j+b/2)=-\beta(j)$ hold for every $j\in\{1,\ldots,b/2\}$.

To verify Theorem 5.1 for $q\geq 2$ it suffices to find elements $p_{2j}$ with $j$ running over $\{1,\ldots,b/2\}$ satisfying the conditions

$$\begin{aligned} &(a'') \quad p_{2j}\in\beta(2j)\\ &(b'') \quad p_{2j-1}=\tfrac{1}{2}(p_{2j}+p_{2j-2})\in\beta(2j-1),\\ &(c'') \quad p_{2j}-p_{2j-1}=\tfrac{1}{2}(p_{2j}-p_{2j-2})\in\beta(j),\end{aligned}$$

where, in addition, $p_b$ generates $T$. Let $\delta$ be an arbitrary generator of $T$, and put $p_b=\delta$. To detect the remaining elements $p_{2j}$, we use a result from [8].

**Lemma 5.3** ([8]). *Let $b,r,s$ be positive integers. For almost all prime powers $q\equiv 1 \bmod b$, for all r-element subsets $U$ of $GF(q)$, for all s-element subsets $Z$ of $GF(q)$ and for all maps $\theta: U\to\Gamma/T$, there exists an element $x\in GF(q)$ satisfying*

$$\begin{aligned} &(a''') \quad x\notin Z,\\ &(b''') \quad x-u\in\theta(u) \text{ for every } u\in U.\end{aligned}$$

To find the desired elements $p_{2j}$, we proceed by induction on $j$. Recall, that $p_0=1$ is already known. For $j\leq b/2-2$, let $U$ be the 3-element set $\{0,-p_{2j-2},p_{2j-2}\}$. Moreover, we define $\theta$ by $\theta(0)=\beta(2j)$, $\theta(-p_{2j-2})=2\beta(2j-1)$ and $\theta(p_{2j-2})=2\beta(j)$.

Finally, for $j=b/2-1$, let $U$ be the 5-element set $\{0,-p_{b-4},p_{b-4},-p_b,p_b\}$. Similarly, we define $\theta$ by $\theta(0)=\beta(b-2)$, $\theta(-p_{b-4})=2\beta(b-3)$, and $\theta(p_{b-4})=2\beta(b/2-1)$ as well as $\theta(-p_b)=2\beta(b-1)$ and $\theta(p_b)=-2\beta(b/2)$. It is easy to check, that Lemma 5.3 ensures the existence of the elements $p_2,p_4,\ldots,p_{b-2}$, satisfying ($a''$–$c''$), as claimed for almost all prime powers $q$. This, however, concludes the proof of Theorem 5.1. A straightforward recomputation of the results in [8] furnishes us with an upper bound of $16b^{10}$ for possible exceptions to Theorem 5.1.

## REFERENCES

[1] B. Alspach, K. Heinrich, and G. Liu, Orthogonal factorizations of graphs; contemporary design theory, chapter 2, J. H. Dinitz and D. R. Stinson (Editors), Wiley, NewYork, 1992, pp. 13–40.

[2] B. Alspach, K. Heinrich, and M. Rosenfeld, Edge partitions of the complete symmetric directed graph and related designs, Israel J Math 40(2) (1981), 118–128.

[3] J. H. Dinitz and D. R. Stinson, Some new perfect one-factorizations from starters in finite fields, J Graph Theory 13(4) (1989), 405–415.

[4] J. H. Dinitz and D. R. Stinson, Room squares and related designs; contemporary design theory, chapter 5, J. H. Dinitz and D. R. Stinson (Editors), Wiley, New York, 1992, pp. 137–204.

[5] B. Ganter, H.-D. O. F. Gronau, and R. C. Mullin, On orthogonal double covers of $K_n$, Ars Combin 37 (1994), 209–221.

[6] H.-D. O. F. Gronau, personal communication.

[7] H.-D. O. F. Gronau, M. Grüttmüller, S. Hartmann, U. Leck, and V. Leck, On orthogonal double covers of graphs, Designs Codes Cryptogr, (2002), in press.

[8] S. Hartmann, Orthogonal decompositions of complete digraphs, Graphs and Combin, (2002), in press.

[9] K. Heinrich and G. Nonay, Path and cycle decompositions of complete multigraphs, Ann Discrete Math 27 (1985), 275–286.

[10] F. Hering, Block designs with cyclic block structure, Ann Discrete Math 6 (1980), 201–214.

[11] F. Hering, Balanced pairs, Ann Discrete Math 20 (1984), 177–182.

[12] H. W. Lenstra and R. J. Schoof, Primitive normal bases for finite fields, Math Comp 48 (1987), 217–231.

[13] R. Lidl and H. Niederreiter, Finite fields, CUP, Cambridge, 1987.