Cyclic Steiner Quadruple Systems and Köhler’s Orbit Graphs

HELMUT SIEMON
PH Ludwigsburg, FB III, Abt. Mathematik, Reuteallee 46, Postfach 2 20, D-7140 Ludwigsburg, West Germany

Dedicated to Hanfried Lenz on the occasion of his 75th birthday.

Communicated by D. Jungnickel
Received July 5, 1990. Revised November 6, 1990.

Abstract. In this article we are concerned with the problem of the existence of strictly cyclic Steiner Quadruple Systems \(sSQS(v)\), where \(v = 2, 10 \mod (24)\). E. Köhler (cf. Köhler 1978) used an orbit graph approach to handle such systems and obtained the result that in case \(p\) is a prime number with \(p = 53, 77 \mod (120)\) then \(sSQS(v)\) exists provided that the associated orbit graph \(OKG(p)\) is bridgeless. We continue these investigations by classifying the orbit graphs \(OKG(p)\) with \(p = 5 \mod (12)\), where the ones with \(p = 53, 77 \mod (120)\) constitute one out of four classes and thus show that \(sSQS(2p)\), \(p = 5 \mod (12)\) exists if \(OKG(p)\) or a reduced graph of it is bridgeless by discussing the four classes separately. Subsequent to this discussion we use the proof of Theorem 2 (Siemon 1991) to state that the bridgelessness of the graphs in all classes is equivalent to the number theoretic claim (3.1).

1. Introduction

A Steiner Quadruple System \(SQS(v)\) with order \(v\) is called cyclic (cf. Lindner and Rosa 1978) if the automorphism group \(Aut(SQS(v))\) of \(SQS(v)\) contains a cycle \((0, 1, \ldots, v - 1)\) of length \(v\) and strictly cyclic if additionally all orbits have length \(v\). We denote strictly cyclic \(SQS(v)\) by \(sSQS(v)\). In (Köhler 1978) E. Köhler has established a connection between his construction of \(sSQS(2p)\), \(p = 5 \mod (12)\) being a prime number, and certain orbit graphs. These orbit graphs can easily be described by the following isomorphic images \(G(p)\) (cf. Köhler 1978; Lenz and Ringel 1991; Lindner and Rosa 1978; Siemon 1987; Siemon 1989; Siemon 1991).

Let \(E(p) := GF(p)^*\) be the multiplicative group of the Galois field \(GF(p)\)—that is, the group of units modulo \(p\). The elements of \(E(p)\) shall be represented by the set of smallest residues modulo \(p\), that is, by \([1, p - 1] := \{1, 2, \ldots, p - 1\}\). We call \([a, b] := \{x \mid x \in [1, p - 1] \text{ and } a \leq x \leq b\}\) an interval of \([1, p - 1]\). Let \(I_2\) be the interval \([2, (p - 3)/2]\) and by \((x^{-1}) \in I_2\) we denote the representative of the (multiplicative) inverse element modulo \(p\) of \(x \in [1, p - 1]\). Additionally we define

\[
x^* := \min \{x, p - 1 - x\}, \quad x \in [1, p - 1]. \quad (1.1)
\]

Now \(I_2\) can be decomposed by the sets \(K(x) := \{x, (x^{-1})^*, (-(1 + x)^{-1})^*\}, x \in I_2\). It can be readily seen that the sets \(K(x)\) are equivalent classes of \(I_2\), so that

\[
K(x) = K((x^{-1})^*) = K((-(1 + x)^{-1})^*).
\]
By these classes we define the graph $G(p)$:

\[
G(p) : \text{vertices of } G(p) : \text{The classes } K(x) \text{ of } \mathbb{I}_2 \\
\text{edges of } G(p) : \{K(x), K(y)\} \text{ is an edge iff there exists } u \in K(x), v \in K(y) \text{ with } |u - v| = 1.
\]

Köhler stated in (Köhler 1978) that $sSQS(2p)$ exists if $G(p)$ has a 1-factor. That follows from his Satz 1 and Lemma 6, which he thought immediate, but still requiring proof (cf. (Siemon 1991), prop.). Then Köhler investigated $G(p)$ and could prove the following fact (cf. (Köhler 1978)):

\[\text{If } p = 53, 77 (120) \text{ and if } G(p) \text{ is bridgeless then it has a 1-factor (and } sSQS(2p) \text{ exists).} \] (1.2)

In (Siemon 1991) the condition of bridgelessness was reduced to the following number theoretic claim, which can be described roughly by:

\[\text{No proper subinterval of } \mathbb{I}_2 \text{ can be covered by the classes } K(x).\] (1.3)

By means of (1.3) and by using a PC it could be verified that $sSQS(2p)$ exists for all $p < 500\,000$ and $p = 53, 77 (120)$ (cf. (Siemon 1991)).

In Köhler’s paper (Köhler 1978) Lemma 10 is not stated correctly. It says:

\[G(p) \text{ with } p = 5 + 12k \text{ has exactly two vertices of degree 2 iff } k = 4, 6 (10). \] (1.4)

However, the graph $G(p)$ with $p = 149 = 5 + 12 \cdot 12, k = 12 = 2 (10)$ has exactly two vertices of degree 2 (and one vertex of degree 1) but $k$ does not satisfy $k = 4, 6 (10)$ as Lemma 10 would require. So $G(149)$ is a counterexample of this Lemma.

Starting from this observation we will divide the graphs $G(p)$ with $p = 5 (12)$ in four classes, so correcting Lemma 10 (Section 2). Extending our Theorem 2 in (Siemon 1991) we arrive in Section 3 at the following theorem.

**Theorem.** If $p = 5 + 12k, k > 1$ and if (3.1) holds true then $sSQS(2p)$ exists.

2. **The Graph $G(p)$**

In this section we review part of the results of (Köhler 1978) and provide them with simpler proofs for the convenience of the reader.

Since in the following we have to consider both values of (1.1) it is suitable to define (besides the classes $K(x)$ of $I_2$) the augmented classes $\omega(x) = \{x, -1 - x, x^{-1}, -1 - x^{-1}, -1 + (1 + x)^{-1}\}$ of $\Pi_2 = \{2, (p - 3)/2, [2^{-1}, p - 1 - 2] = \{2, 3, \ldots, p - 3\} \setminus \{(p - 1)/2\}$, which can be interpreted as follows: Let $P = \langle x \mapsto x^{-1}, x \mapsto -1 - x \rangle$ be the group of order 6 which is generated by $x \mapsto x^{-1}, x \mapsto -1 - x$ and let $P$ operate on the projective line $GF(p) \cup \{\infty\}$. The orbits $\omega(x)$ of $P$ are