Some New Perfect One-Factorizations from Starters in Finite Fields

J. H. Dinitz
UNIVERSITY OF VERMONT

D. R. Stinson
UNIVERSITY OF MANITOBA

ABSTRACT

We construct seven new examples of perfect one-factorizations, in the complete graphs K_{126}, K_{170}, K_{730}, K_{1370}, K_{1850}, K_{2198}, and K_{3126}. These are generated by two- and four-quotient starters in finite fields. We also find several examples of perfect one-factorizations that are not isomorphic to previously known examples.

1. INTRODUCTION

A *one-factorization* of a complete graph K_{2n} is a partition of the edge-set of K_{2n} into $2n - 1$ *one-factors*, each of which contains n edges that partition the vertex set of K_{2n}. One-factorizations have been the subject of much interest over the years; a good survey is given in [17]. In this paper, we study one-factorizations with the additional property that every pair of distinct one-factors forms a Hamiltonian cycle. Such a one-factorization is termed *perfect;* we denote a perfect one-factorization by P1F.

Two infinite classes of P1Fs of K_{2n} are known to exist. When n is prime, the one-factorization known as GA_{2n} is perfect [1]; and when $2n - 1$ is prime, the one-factorization known as GK_{2n} is perfect [16,1]. P1Fs of several other orders have been constructed by ad hoc methods. P1Fs of K_{16}, K_{28}, K_{244}, and K_{344} were found by Anderson [2,3] and Anderson and Morse [6] in the mid-1970s. Quite recently, a P1F of K_{36} was found by Seah and Stinson [20]; a nonisomorphic example was found by Kobayashi, Awoki, Nakazaki, and Nakamura [14]. A P1F of K_{50} was found by Ihrig, Seah, and Stinson in [13], and a P1F of K_{40} was found by Seah and Stinson in [22]. P1Fs of K_{1332} and K_{6860} were found by Kobayashi and Kiyasu-Zen'iti in [15]. Most of these P1Fs have been constructed by the method of starters, which are defined in Section 2.

Journal of Graph Theory, Vol. 13, No. 4, 405–415 (1989)
 CCC 0364-9024/89/040405-11$04.00

In this paper, we construct P1Fs of seven new orders from starters in finite fields. We find P1Fs in K_{126}, K_{170}, K_{730}, K_{1370}, K_{1850}, K_{2198}, and K_{3126}. Note that these graphs all have $p^m + 1$ vertices, where p is prime.

Although the authors believe it is undoubtedly true that a P1F of K_{2n} exists for all $2n = 4, 6, \dots$, we are still far from being able to prove it. Recent work of Ihrig [9–12] gives some indications as to why P1Fs are so difficult to construct. Roughly speaking, Ihrig proves that most P1Fs that have reasonably large automorphism groups are already known.

Finally, we mention that, up to isomorphism, there is a unique P1F of K_{2n} when $n = 4$, 6, 8, or 10. There are precisely 5 nonisomorphic P1Fs of K_{12} [18] and precisely 21 nonisomorphic P1Fs of K_{14} having nontrivial automorphism groups [19,21]. Starter-generated and even-starter-generated P1Fs of K_{2n} are enumerated for $2n \leq 22$ in [4]. In [8], 5 nonisomorphic P1Fs of K_{24} are presented.

2. STARTERS AND ONE-FACTORIZATIONS

Most of the known constructions for (perfect) one-factorizations use starters. A *starter* in an additive abelian group G of order $2n - 1$ is a set $S = \{\{x_1, y_1\}, \{x_2, y_2\}, \dots, \{x_{n-1}, y_{n-1}\}\}$ such that every nonzero element of G occurs as

(1) an element in exactly one pair of S, and
(2) a difference of exactly one pair of S.

For example, $\{\{1,6\},\{2,5\},\{3,4\}\}$ is a starter in $\mathbf{Z}_7$.

Define $S^* = S \cup \{0, \infty\}$. For any $g \in G$, define $S^* + g = \{\{x_1 + g, y_1 + g\}, \{x_2 + g, y_2 + g\}, \dots, \{x_{n-1} + g, y_{n-1} + g\}, \{g, \infty\}\}$, where $\infty + g = g + \infty = \infty$ for all $g \in G$. Then, it is easy to see that $F = \{S^* + g : g \in G\}$ is a one-factorization of K_{2n}. Further, F contains G in its automorphism group.

This fact makes it easier than it would otherwise be to determine if F is perfect. Instead of checking all $(n-1)(2n-1)$ pairs of one-factors to see if they form Hamiltonian cycles, it suffices to check only $n - 1$ pairs of one-factors, as follows. Choose any $n - 1$ nonzero group elements $g_1, g_2, \dots, g_{n-1}$ such that no two of them sum to zero. Then, it is easy to see that F is perfect if and only if $S^* \cup (S^* + g_i)$ is a Hamiltonian cycle, for $1 \leq i \leq n - 1$.

We will employ starters with more algebraic structure, which will enable us to determine the perfection of the resulting one-factorizations with even less work. We use a special type of starter defined by Dinitz in [7], which we now describe.

Suppose $q = 2^\alpha t + 1$ is an odd prime power, where t is odd. Let ω be a primitive element in $GF(q)$, and let C_0 be the (unique) subgroup of G^* of order t and index 2^α, where G^* denotes the multiplicative group $G \backslash \{0\}$. Denote the cosets of C_0 by C_i $(0 \leq i \leq 2^\alpha - 1)$, where $C_i = \omega^i C_0$.

A starter S in $GF(q)$ is said to be a *$2^{\alpha-1}$-quotient coset starter* (or $2^{\alpha-1}$-QCS) if the following property is satisfied:

for all pairs $\{x, y\}, \{x', y'\} \in S$, if $x, x' \in C_i$ for some i, then $y/x = y'/x'$.

For any $z \in GF(q)$, $z \neq 1$, define $C_i^z = (1/(z-1))C_i$. Given a list of $2^{\alpha-1}$ field elements from $GF(q)$, say $A = (a_0, \ldots, a_{2^{\alpha-1}-1})$, define $S(A) = \{\{x, a_i x\}: x \in C_i^{a_i}, 0 \leq i \leq 2^{\alpha-1} - 1\}$. If $S(A)$ is a starter, then it is a $2^{\alpha-1}$-QCS. The conditions for $S(A)$ to be a starter were given explicitly in the case $2^{\alpha-1} = 2$ in [7, Lemma 3.1]. In a similar fashion, we have the following, which we state without proof:

Lemma 2.1. Suppose $q = 2^\alpha t + 1$ is an odd prime power, where t is odd. Then, $S(A)$ is a $2^{\alpha-1}$-QCS in $GF(q)$ if and only if the following conditions are satisfied:

(a) $a_i \notin C_0$, $0 \leq i \leq 2^{\alpha-1} - 1$.
(b) $(a_j - 1)/(a_i - 1) \notin C_{(j-i \bmod 2^\alpha)}, 0 \leq i,j \leq 2^{\alpha-1} - 1, i \neq j$.
(c) $(a_j - 1)/(a_j(a_i - 1)) \notin C_{(j-i \bmod 2^\alpha)}, 0 \leq i,j \leq 2^{\alpha-1} - 1, i \neq j$.
(d) $a_i(a_j - 1)/(a_i - 1) \notin C_{(j-i \bmod 2^\alpha)}, 0 \leq i,j \leq 2^{\alpha-1} - 1, i \neq j$.
(e) $a_i(a_j - 1)/(a_j(a_i - 1)) \notin C_{(j-i \bmod 2^\alpha)}, 0 \leq i,j \leq 2^{\alpha-1} - 1, i \neq j$.

Remark. It is not difficult to see that any $2^{\alpha-1}$-QCS can be written as $S(A)$ for a suitable set A.

Example. $25 = 5^2 = 2^3 3 + 1$. $GF(25)$ can be constructed from the irreducible polynomial $x^2 + x + 2$ over $GF(5)$. Then, x is a primitive element. It is easy to verify using Lemma 2.1 that $S(x^1, x^{13}, x^{10}, x^{14})$ is a 4-QCS.

The $2^{\alpha-1}$-QCS are plentiful, but usually do not generate P1Fs. Of course, we are interested in the situation where $2^{\alpha-1}$-QCS generate P1Fs. In the case where $2^{\alpha-1} = 1$, it has been shown in [3] and [8] that the starter $S(A)$ generates a *uniform* one-factorization: for any two pairs of one-factors, $\{F_1, F_2\}$ and $\{F_3, F_4\}$, the two-factor $F_1 \cup F_2 \cong F_3 \cup F_4$. We generalize this result to $\alpha > 1$ in the following theorem:

Theorem 2.2. Suppose $S(A)$ is a $2^{\alpha-1}$-QCS in $GF(q)$, where $q = 2^\alpha t + 1$ is an odd prime power and t is odd. Let $g_1, g_2 \neq 0$. Then, $S(A)^* \cup (S(A)^* + g_1) \cong S(A)^* \cup (S(A)^* + g_2)$ if $g_2/g_1 \in C_0 \cup C_{2^{\alpha-1}}$.

Proof. First we prove that $S(A)^* \cup (S(A)^* + g_1) \cong S(A)^* \cup (S(A)^* + g_2)$ if $g_2/g_1 \in C_0$. Denote $g_2/g_1 = g \in C_0$. Then $gS(A)^* = S(A)^*$ and $g(S(A)^* + g_1) = (S(A)^* + g_2)$. Hence, $g(S(A)^* \cup (S(A)^* + g_1)) = S(A)^* \cup (S(A)^* + g_2)$. Next, we prove that $S(A)^* \cup (S(A)^* + g_1) \cong S(A)^* \cup (S(A)^* + g_2)$ if $g_2/g_1 \in C_{2^{\alpha-1}}$. Suppose $g_2/g_1 \in C_{2^{\alpha-1}}$; then $-g_2/g_1 = g \in C_0$. Then $(-g)S(A)^* = -S(A)^*$ and $(-g)(S(A)^* + g_1) = (-S(A)^* + g_2)$. But, $-S(A)^* \cup (-S(A)^* + g_2) \cong S(A)^* \cup (S(A)^* - g_2) \cong (S(A)^* + g_2) \cup S(A)$, as desired.

Consequently, it is not difficult to determine if a $2^{\alpha-1}$-QCS, $S(A)$, generates a P1F. We have the following:

Corollary 2.3. Suppose $S(A)$ is a $2^{\alpha-1}$-QCS in $GF(q)$, where $q = 2^\alpha t + 1$ is an odd prime power and t is odd. For $0 \leq i \leq 2^{\alpha-1} - 1$, let $g_i \in C_i$. Then $S(A)$ generates a P1F if and only if $S(A)^* \cup (S(A) + g_i)$ is a Hamiltonian cycle, for $0 \leq i \leq 2^{\alpha-1} - 1$.

Proof. Consider the union of two one-factors, $(S(A)^* + g') \cup (S(A)^* + g'')(g' \neq g'')$. It is clear that $(S(A)^* + g') \cup (S(A)^* + g'') \cong S(A)^* \cup (S(A)^* + g'' - g')$, so it suffices to consider pairs of one-factors of the form $S(A)^* \cup (S(A)^* + g)$ where $g \neq 0$. If $g/g_i \in C_0$, for some i, $0 \leq i \leq 2^{\alpha-1} - 1$, then $S(A)^* \cup (S(A)^* + g)$ is a Hamiltonian cycle, from the hypotheses and Theorem 2.2. Otherwise, $g/g_i \in C_{2^{\alpha-1}}$, for some i, $0 \leq i \leq 2^{\alpha-1} - 1$. In this case as well, $S(A)^* \cup (S(A)^* + g)$ is a Hamiltonian cycle.

Example (continued). The starter $S(A) = S(x^1, x^{13}, x^{10}, x^{14})$ in $GF(25)$ generates a P1F. In view of Corollary 2.3, it suffices to check that $S(A)^* \cup (S(A)^* + x^i)$ is a Hamiltonian cycle, for $0 \leq i \leq 3$.

We can determine the automorphism groups of the resulting one-factorizations. Suppose F is a P1F arising from $S(A)$, a $2^{\alpha-1}$-QCS in $GF(q)$, and denote by $\mathrm{Aut}(F)$ its automorphism group. It is clear that F contains the additive group of $GF(q)$, namely $(\mathbf{Z}_p)^n$, as a subgroup. It is also easy to verify that multiplication by any element in C_0 is also an automorphism. Hence, $\mathrm{Aut}(F)$ contains as a subgroup the semidirect product $[(\mathbf{Z}_p)^n]Z_t$, which is a group of order qt. In fact, the following theorem of Ihrig tells us that this must be the entire automorphism group:

Theorem 2.4. ([12, Theorem 4.1(b)]). Suppose F is a P1F of K_{2n}, and $\mathrm{Aut}(F)$ contains G as a subgroup, where G has order $2n - 1$ and G acts transitively on the one-factors. If F is not isomorphic to GK_{2n}, then $\mathrm{Aut}(F)$ is a semidirect product $[G]H$, where H is a subgroup of $\mathrm{Aut}(G)$, $|H|$ is odd, and $|H|$ divides $n - 1$.

Remark. In [5], Anderson proves that $\mathrm{Aut}(GK_{2n}) = [\mathbf{Z}_{2n-1}]\mathbf{Z}_{2n-2}$.

Hence, we have the following:

Theorem 2.5. Suppose $q = 2^\alpha t + 1 = p^n$ is an odd prime power, where t is odd. Suppose that a $2^{\alpha-1}$-QCS in $GF(q)$ generates a perfect one-factorization F not isomorphic to GK_{q+1}. Then, $\mathrm{Aut}(F)$ is the semidirect product $[(\mathbf{Z}_p)^n]\mathbf{Z}_t$, and hence has order qt.

Proof. By Theorem 2.4, $\mathrm{Aut}(F)$ has the form $[(\mathbf{Z}_p)^n]H$, where $|H|$ is odd and $|H|$ divides $2^{\alpha-1}t$. Hence, $|H|$ divides t. But H contains C_0 ($\cong \mathbf{Z}_t$) as a subgroup, and $|C_0| = t$. Hence, $H = \mathbf{Z}_t$.

Example (continued). The one-factorization of K_{26} generated from the 4-QCS $S(x^1, x^{13}, x^{10}, x^{14})$ in $GF(25)$ has automorphism group $[(\mathbf{Z}_5)^2]\mathbf{Z}_3$.

Starters that generate isomorphic one-factorizations will be termed *isomorphic*. We can determine certain conditions under which distinct $2^{\alpha-1}$-QCS in $GF(q)$ will be isomorphic. For any starter $S = \{\{x_i, y_i\}: 1 \le i \le (q-1)/2\}$ in $GF(q)$, and for any $c \ne 0$, define $cS = \{\{cx_i, cy_i\}: 1 \le i \le (q-1)/2\}$. It is clear that cS is a starter if S is, and that they are isomorphic. If S is a $2^{\alpha-1}$-QCS, then cS will also be one, with parameters as given by the following theorem (in the special case of 2-QCS, this result was proved in [7]):

Theorem 2.6. Suppose $q = 2^\alpha t + 1$ is an odd prime power, where t is odd. Suppose that $S(a_0, \ldots, a_{2^{\alpha-1}-1})$ is a $2^{\alpha-1}$-QCS in $GF(q)$, and $c \in C_1$. Then $cS(a_0, \ldots, a_{2^{\alpha-1}-1}) = S(1/a_{2^{\alpha-1}-1}, a_0, \ldots, a_{2^{\alpha-1}-2})$.

Proof. We have that

$$\begin{aligned} cS(a_0, \ldots, a_{2^{\alpha-1}-1}) &= \{\{cx, a_i cx\}: x \in C_i^{a_i}, 0 \le i \le 2^{\alpha-1} - 1\} \\ &= \{\{cx, a_i cx\}: x \in (1/(a_i - 1))C_i, 0 \le i \le 2^{\alpha-1} - 1\} \\ &= \{\{y, a_i y\}: y \in (1/a_i - 1))C_{i+1}, 0 \le i \le 2^{\alpha-1} - 1\} \\ &\quad (\text{where } y = cx)\,. \end{aligned}$$

Hence, $cS(a_0, \ldots, a_{2^{\alpha-1}-1}) = S(b, a_0, \ldots, a_{2^{\alpha-1}-2})$, where b is determined as follows: When $i = 2^{\alpha-1} - 1$, we obtain

$$\begin{aligned} &\{\{y, a_{2^{\alpha-1}-1} y\}: y \in (1/(a_{2^{\alpha-1}-1} - 1))C_{2^{\alpha-1}}\} \\ &\qquad = \{\{z, (1/a_{2^{\alpha-1}-1})z\}: z \in (a_{2^{\alpha-1}-1}/(a_{2^{\alpha-1}-1} - 1))C_{2^{\alpha-1}}\} \end{aligned}$$

(where $z = a_{2^{\alpha-1}-1} y$)

$$= \{\{z, (1/a_{2^{\alpha-1}-1})z\}: z \in (1/((1/a_{2^{\alpha-1}-1}) - 1))C_0\}\,.$$

Hence, $b = 1/a_{2^{\alpha-1}-1}$, and thus

$$cS(a_0, \ldots, a_{2^{\alpha-1}-1}) = S(1/a_{2^{\alpha-1}-1}, a_0, \ldots, a_{2^{\alpha-1}-2})\,.$$

Using Theorem 2.6, it is easy to determine $cS(A)$ for any $c \ne 0$. If $c \in C_i$, then we would apply Theorem 2.6 i times. It is interesting to note that $-S(a_0, \ldots, a_{2^{\alpha-1}-1}) = S(1/a_0, \ldots, 1/a_{2^{\alpha-1}-1})$, since $-1 \in C_{2^{\alpha-1}}$.

Example (continued). By Theorem 2.6, we see that $S(x^1, x^{13}, x^{10}, x^{14}) \cong S(x^{10}, x^1, x^{13}, x^{10}) \cong S(x^{14}, x^{10}, x^1, x^{13}) \cong S(x^{11}, x^{14}, x^{10}, x^1) \cong S(x^{23}, x^{11}, x^{14}, x^{10}) \cong S(x^{14}, x^{23}, x^{11}, x^{14}) \cong S(x^{10}, x^{14}, x^{23}, x^{11}) \cong S(x^{13}, x^{10}, x^{14}, x^{23})$.

Finally, we consider the effect of a Frobenius automorphism on a starter. Suppose $q = p^m = 2^\alpha t + 1$ is an odd prime power, where t is odd and p is prime, and $S = \{\{x_i, y_i\}: 1 \le i \le (q-1)/2\}$ is any starter in $GF(q)$. Then we define the starter $S^p = \{\{x_i^p, y_i^p\}: 1 \le i \le (q-1)/2\}$. S^p will be a starter provided S is, and the two starters will be isomorphic.

Define π: $\mathbf{Z}_{2^\alpha} \to \mathbf{Z}_{2^\alpha}$ by $\pi(i) = pi$ modulo 2^α. It is clear that π is a permutation. Then, we have the following:

Theorem 2.7. Suppose $q = p^m = 2^\alpha t + 1$ is an odd prime power, where t is odd and p is prime. Suppose that $S(a_0, \ldots, a_{2^{\alpha-1}-1})$ is a $2^{\alpha-1}$-QCS in $GF(q)$. Then $S(a_0, \ldots, a_{2^{\alpha-1}-1})p = S(b_0, \ldots, b_{2^{\alpha-1}-1})$, where

$$b_j = (a_{\pi^{-1}(j)})^p, \quad \text{if } \pi^{-1}(j) < 2^{\alpha-1}$$
$$b_j = 1/(a_{\pi^{-1}(j)-2^{\alpha-1}})^p, \quad \text{if } \pi^{-1}(j) \ge 2^{\alpha-1}.$$

Proof. Let $0 \le i \le 2^{\alpha-1} - 1$. Then

$$\begin{aligned}
\{\{x^p, (a_i x)^p\}: x \in C_i^{a_i}\} &= \{\{x^p, a_i^p x^p\}: x \in (1/(a_i - 1))C_i\} \\
&= \{\{y, a_i^p y\}: y \in (1/(a_i - 1))^p (C_i)^p\} \\
&\qquad \text{(where } (C_i)^p = \{z^p: z \in C_i\} \text{ and } y = x^p) \\
&= \{\{y, a_i^p y\}: y \in (1/(a_i^p - 1))(C_i)^p\} \\
&\qquad \text{(since } (a_i - 1)^p = a_i^p - 1, \\
&= \{\{y, a_i^p y\}: y \in (1/(a_i^p - 1))C_{\pi(i)}\}.
\end{aligned}$$

If $\pi(i) < 2^{\alpha-1}$, then let $j = \pi(i)$ and let $b_j = a_i^p$. Then,

$$\begin{aligned}
\{\{y, a_i^p y\}: y \in (1/(a_i^p - 1))C_{\pi(i)}\} &= \{\{y, b_j y\}: y \in (1/(b_j - 1))C_j\} \\
&= \{\{y, b_j y\}: y \in C_j^{b_j}\}.
\end{aligned}$$

If $\pi(i) \ge 2^{\alpha-1}$, then let $j = \pi(i) - 2^{\alpha-1}$ and let $b_j = 1/a_i^p$. Note that $C_j = -C_{\pi(i)}$ and that $\pi(i + 2^{\alpha-1}) \equiv \pi(i) + 2^{\alpha-1} \pmod{2^\alpha}$. Then,

$$\begin{aligned}
\{\{y, a_i^p y\}: y \in (1/(a_i^p - 1))C_{\pi(i)}\} &= \{\{y, (1/b_j)y\}: y \in (1/((1/b_j) - 1))C_{j+2^{\alpha-1}}\} \\
&= \{\{y, (1/b_j)y\}: y \in (b_j/(b_j - 1))C_j\} \\
&= \{\{z, b_j z\}: z \in (1/(b_j - 1))C_j\} \\
&\qquad \text{(where } z = (1/b_j)y) \\
&= \{\{z, b_j z\}: z \in C_j^{b_j}\}.
\end{aligned}$$

It remains to show that the j's, as defined above, take on every value from 0 to $2^{\alpha-1} - 1$ exactly once. This is a simple verification, which we leave to the interested reader.

Example (continued). In $GF(25)$, the permutation π: $\mathbf{Z}_8 \rightarrow \mathbf{Z}_8$ can be computed to be (0)(1 5)(2)(3 7)(4)(6). Then, $S(x^1, x^{13}, x^{10}, x^{14})^5 = S(x^5, x^{17}, x^2, x^{22})$. We obtain a total of 16 distinct starters isomorphic to $S(x^1, x^{13}, x^{10}, x^{14})$ by combining the isomorphisms of Theorems 2.6 and 2.7.

3. NEW PERFECT ONE-FACTORIZATIONS

Using 2-QCS and 4-QCS, we found P1Fs of seven new orders, as follows:

Theorem 3.1. There exist P1Fs of the complete graphs K_{126}, K_{170}, K_{730}, K_{1370}, K_{1850}, K_{2198}, and K_{3126}.

Proof. The starters are displayed below.

K_{126} $125 = 5^3 = 2^2 31 + 1$. Construct $GF(5^3)$ from the polynomial $x^3 + x^2 + 2$, which is irreducible over $\mathbf{Z}_5$. Then, x is a generator. $S(x^9, x^{41}) = S(2x^2 + 4x + 4, x^2 + 2x + 3)$ generates a P1F of K_{126}, as does $S(x^{18}, x^{38}) = S(4x + 2, 4x^2 + 3x)$.

K_{170} $169 = 13^2 = 2^3 21 + 1$. Construct $GF(13^2)$ from the polynomial $x^2 + 12x + 2$, which is irreducible over $\mathbf{Z}_{13}$. Then, x is a generator. $S(x, x^5, x^{46}, x^{14}) = S(x, 12x + 6, 2x + 3, 2)$ generates a P1F of K_{170}.

K_{730} $729 = 3^6 = 2^3 91 + 1$. Construct $GF(3^6)$ from the polynomial $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, which is irreducible over $\mathbf{Z}_3$. Then, $g = x^2 + x + 2$ is a generator. $S(g, g^{36}, g^{217}, g^{580}) = S(x^2 + x + 2, 2x^3 + x^2 + 2x + 1, x^5 + 2x^3 + 1, x^5 + x^3 + 1)$ generates a P1F of K_{730}.

K_{1370} $1369 = 37^2 = 2^3 161 + 1$. Construct $GF(37^2)$ from the polynomial $x^2 + 36x + 22$, which is irreducible over $\mathbf{Z}_{37}$. Then, x is a generator. $S(x^{421}, x^5, x^{773}, x^{1317}) = S(29x + 11, 12x + 21, 36x + 33, 3x + 22)$ generates a P1F of K_{1370}.

K_{1850} $1849 = 43^2 = 2^3 231 + 1$. Construct $GF(43^2)$ from the polynomial $x^2 + 42x + 34$, which is irreducible over $\mathbf{Z}_{43}$. Then, x is a generator. $S(x^{531}, x^{878}, x^{1358}, x^{957}) = S(31x + 15, 22x + 38, 34x + 37, 3x + 9)$ generates a P1F of K_{1850}.

K_{2198} $2197 = 13^3 = 2^2 549 + 1$. Construct $GF(13^3)$ from the polynomial $x^3 + 12x + 12$, which is irreducible over $\mathbf{Z}_{13}$. Then, $g = x + 2$ is a generator. $S(g^7, g^{557}) = S(12x^2 + 11x + 7, 6x^2 + 10x)$ generates a P1F of K_{2198}.

K_{3126} $3125 = 5^5 = 2^2 781 + 1$. Construct $GF(5^5)$ from the polynomial $x^5 + 4x + 4$, which is irreducible over $\mathbf{Z}_5$. Then, $g = 2x$ is a generator. $S(g^{11}, g^{2097}) = S(3x^3 + x^2 + 3x, 2x^4 + x^3 + 3x^2 + 3x + 3)$ generates a P1F of K_{3126}.

We also found P1Fs of several other orders that are not isomorphic to previously known P1Fs. These are presented in Table 1. The elements in the sets of A in Table 1 are all written as powers of the given primitive element.

TABLE 1. Perfect One-Factorizations of K_{p^m+1} Arising from $2^{\alpha-1}$-Quotient Coset Starters

p^m	Irreducible Polynomial	Primitive Element	Quotients in A (Powers of Primitive Element)
$25 = 5^2$	$x^2 + x + 2$	x	1, 13, 10, 14
$49 = 7^2$	$x^2 + x + 3$	x	1, 5, 1, 30, 33, 42, 38, 36
$81 = 3^4$	$x^4 + x^3 + 2x + 1$	$x + 1$	1, 2, 37, 71, 66, 73, 52, 72
$121 = 11^2$	$x^2 + x + 7$	x	1, 7, 51, 65
$361 = 19^2$	$x^2 + x + 3$	x	1, 9, 129, 79
$841 = 29^2$	$x^2 + x + 3$	x	1, 18, 343, 170

We did a complete enumeration of the 4-QCS in $GF(25)$, which generate P1Fs, and found 16 of them. These are all isomorphic, by Theorems 2.6 and 2.7, as noted in the examples.

We also did an exhaustive enumeration of 2-QCS in $GF(125)$, which generate P1Fs; there are 24 of them. The isomorphisms from Theorems 2.6 and 2.7 tell us that we have at most 2 nonisomorphic starters among the set of 24, forming 2 orbits of 12 starters each. One starter from each orbit was presented above. We can prove that starters from different orbits are indeed nonisomorphic by use of a type of invariant called the *train* of the one-factorization. The train of a one-factorization is a particular digraph having outdegree one (a complete description is given in [8]). We computed the indegree sequence of the trains of the 2 P1Fs; since these indegree sequences are different, the P1Fs are nonisomorphic. We present the vectors obtained by dividing each element in the indegree sequences by 125.

$$S(9,41): \quad (2635, 3256, 1457, 434, 62, 31)$$

$$S(18,38): \quad (3100, 2636, 1333, 682, 93, 31)\,.$$

In Table 2, we summarize the known results on P1Fs of K_{p^m+1}, as follows. We list all prime powers p^m of moderate size, where $m > 1$. For each value, we indicate the known P1Fs of K_{p^m+1}. It is easy to see that the new P1Fs are not isomorphic to the previously known P1Fs, by considering their automorphism groups. Anderson proved in [5] that $\mathrm{Aut}(GA_{2n}) = [\mathbf{Z}_{2n}]\mathbf{Z}_{n-1}$. Also, the known P1Fs of K_{50} all have automorphism groups $[\mathbf{Z}_{49}]\mathbf{Z}_3$. These are different from the automorphism groups of the P1Fs generated from $2^{\alpha-1}$-QCS (Theorem 2.5).

4. SUMMARY

There remain three cases for which $2n - 1$ is a prime power less than 1000 and a P1F of K_{2n} is not known to exist. These are $2n = 290$, 530, and 962. It would be nice to use the methods of this paper to find P1Fs of these orders, but we have been unable to do so.

TABLE 2. Known Perfect One-Factorizations of K_{p^m+1}

$p^m = 2^\alpha t + 1$	$2^{\alpha-1}$-QCS P1F?	Other P1Fs?
$9 = 3^2 = 2^3 + 1$	No	GA_{10}
$27 = 3^3 = 2^1 13 + 1$	Yes [3]	
$81 = 3^4 = 2^4 5 + 1$	Yes (Table 1)	GA_{82}
$243 = 3^5 = 2^1 121 + 1$	Yes [6]	
$729 = 3^6 = 2^3 91 + 1$	Yes (Theorem 3.1)	
$2187 = 3^7 = 2^1 1093 + 1$	No	
$25 = 5^2 = 2^3 3 + 1$	Yes (Table 1)	GA_{26}
$125 = 5^3 = 2^2 31 + 1$	Yes (Theorem 3.1)	
$625 = 5^4 = 2^4 39 + 1$	???	GA_{626}
$3125 = 5^5 = 2^2 781 + 1$	Yes (Theorem 3.1)	
$49 = 7^2 = 2^4 3 + 1$	Yes (Table 1)	[13]
$343 = 7^3 = 2^1 171 + 1$	Yes [6]	
$2401 = 7^4 = 2^5 75 + 1$	???	GA_{2402}
$121 = 11^2 = 2^3 15 + 1$	Yes (Table 1)	GA_{122}
$1331 = 11^3 = 2^1 665 + 1$	Yes [15]	
$169 = 13^2 = 2^3 21 + 1$	Yes (Theorem 3.1)	
$2197 = 13^3 = 2^2 549 + 1$	Yes (Theorem 3.1)	
$289 = 17^2 = 2^5 9 + 1$	???	
$4913 = 17^3 = 2^4 307 + 1$	???	
$361 = 19^2 = 2^3 45 + 1$	Yes (Table 1)	GA_{362}
$6859 = 19^3 = 2^1 3429 + 1$	Yes [15]	
$529 = 23^2 = 2^4 33 + 1$	???	
$841 = 29^2 = 2^3 105 + 1$	Yes (Table 1)	GA_{842}
$961 = 31^2 = 2^6 15 + 1$	???	
$1369 = 37^2 = 2^3 161 + 1$	Yes (Theorem 3.1)	
$1681 = 41^2 = 2^4 105 + 1$	???	
$1849 = 43^2 = 2^3 231 + 1$	Yes (Theorem 3.1)	

We had hoped that it might be possible to prove theoretically that there is always a $2^{\alpha-1}$-quotient starter-generated P1F in K_{q+1} whenever $q = 2^\alpha t + 1$ is a prime power and t is odd. At least in the case $\alpha = 1$, this is not true. For $q = 9$, there is *no* P1F of K_{10} having $(\mathbf{Z}_3)^2$ contained in its automorphism group. This is easily seen, since GA_{10} is the only P1F of K_{10}, and $\mathrm{Aut}(GA_{10}) = [\mathbf{Z}_{10}]\mathbf{Z}_4$. More distressing, there is no P1F of K_{2188} generated from a one-quotient starter in $GF(2187)$. This suggests that a general existence theorem for $2^{\alpha-1}$-quotient starter-generated P1Fs might be difficult.

ACKNOWLEDGMENT

This research was supported in part by the Institute for Mathematics and its Applications with funds provided by the National Science Foundation. The research of D. R. S. was supported by NSERC operating grant A9287.

References

[1] B. A. Anderson, Finite topologies and Hamiltonian paths. *J. Combinat. Theory B* **14** (1973) 87–93.

[2] B. A. Anderson, A perfectly arranged room square. *Proceedings of the 4th Southeastern Conference on Combinatorics, Graph Theory and Computing*. Utilitas Mathematica Publishing Inc., Winnipeg, Canada. (1973) 141–150.

[3] B. A. Anderson, A class of starter induced 1-factorizations. *Lecture Notes Math.* **406** (1974) 180–185.

[4] B. A. Anderson, Some perfect 1-factorizations. *Proceedings of the 7th Southeastern Conference on Combinatorics, Graph Theory and Computing*. Utilitas Mathematica Publishing Inc., Winnipeg, Canada. (1976) 79–91.

[5] B. A. Anderson, Symmetry groups of some perfect 1-factorizations of complete graphs. *Discrete Math.* **18** (1977) 227–234.

[6] B. A. Anderson and D. Morse, Some observations on starters. *Proceedings of the 5th Southeastern Conference on Combinatorics, Graph Theory and Computing*. Utilitas Mathematica Publishing Inc., Winnipeg, Canada. (1974) 229–235.

[7] J. H. Dinitz, Room n-cubes of low order. *J. Austral. Math. Soc. A* **36** (1984) 237–252.

[8] J. H. Dinitz, Some perfect room squares. *J. Combinat. Math. Combinat. Comput.* **2** (1987) 29–36.

[9] Edwin C. Ihrig, Symmetry groups related to the construction of perfect one-factorizations of K_{2n}. *J. Combinat. Theory B* **40** (1986) 121–51.

[10] Edwin C. Ihrig, Symmetry groups of perfect one-factorizations of K_{2n}. *Congressus Numerantium* **60** (1987) 105–130.

[11] Edwin C. Ihrig, Cyclic perfect one-factorizations of K_{2n}. *Ann. Discrete Math.* **34** (1987) 259–272.

[12] Edwin C. Ihrig, The structure of symmetry groups of perfect one-factorizations of K_{2n}. Preprint.

[13] Edwin C. Ihrig, E. Seah, and D. R. Stinson, A perfect one-factorization of K_{50}. *J. Combinat. Math. Combinat. Comput.* **1** (1987) 217–219.

[14] Midori Kobayashi, Hitoshi Awoki, Yoshimi Nakazaki, and Gisaku Nakamura, A perfect one-factorization of K_{36}. Preprint.

[15] Midori Kobayashi and Kiyasu-Zen'iti, Perfect one-factorizations of K_{1332} and K_{6860}. *J. Combinat. Theory A*, to appear.

[16] A. Kotzig, *Theory of Graphs and Its Applications*. Academic Press, New York (1964).

[17] E. Mendelsohn and A. Rosa, One-factorizations of the complete graph — A survey. *J. Graph Theory* **9** (1985) 43–65.

[18] L. Petrenyuk and A. Petrenyuk, Intersection of perfect one-factorizations of complete graphs. *Cybernetics* **16** (1980) 6–9.

[19] E. Seah and D. R. Stinson, Some perfect one-factorizations of K_{14}. *Ann. Discrete Math.* **34** (1987) 419–436.

[20] E. Seah and D. R. Stinson, A perfect one-factorization for K_{36}. *Discrete Math.* **70** (1988) 199–202.
[21] E. Seah and D. R. Stinson, On the enumeration of one-factorizations of the complete graph containing prescribed automorphism groups. *Math. Comp.* **50** (1988) 607–618.
[22] E. Seah and D. R. Stinson, A perfect one-factorization for K_{40}. *Congressus Numerantium,* to appear.