Discrete Mathematics 331 (2014) 109–116

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

The q-analog of the middle levels problem

Tuvi Etzion

Department of Computer Science, Technion, Haifa 32000, Israel

ARTICLE INFO

Article history:
Received 27 September 2013
Received in revised form 12 March 2014
Accepted 25 April 2014
Available online 2 June 2014

Keywords:
Grassmannian
Hamiltonian cycles
Middle levels
Necklaces

ABSTRACT

The well-known middle levels problem is to find a Hamiltonian cycle in the graph induced from the binary Hamming graph $\mathcal{H}_2(2k+1)$ by the words of weight k or $k+1$. In this paper we define the q-analog of the middle levels problem. Let $n = 2k+1$ and let q be a power of a prime number. Consider the set of $(k+1)$-dimensional subspaces and the set of k-dimensional subspaces of $\mathbb{F}_q^n$. Can these subspaces be ordered in a way that for any two adjacent subspaces X and Y, either $X \subset Y$ or $Y \subset X$? A construction method which yields many Hamiltonian cycles for any given q and $k = 2$ is presented.

1. Introduction

Let $\mathcal{H}_2(n)$ denote the n-dimensional binary Hamming graph, known also as the n-dimensional hypercube. The graph has a set of 2^n vertices which are represented by the set of all the binary n-tuples. Two vertices are adjacent if the two n-tuples $(a_1, a_2, \dots, a_n)$ and $(b_1, b_2, \dots, b_n)$ which represent them differ in exactly one position. The *weight* of a binary n-tuple is defined as the number of position in which it has *ones*. The *middle levels graph* M_{2k+1} is a subgraph of $\mathcal{H}_2(2k+1)$ induced by the vertices represented by n-tuples of weight k or weight $k+1$ in $\mathcal{H}_2(2k+1)$. The *middle levels conjecture* asserts that the graph M_{2k+1} has a Hamiltonian cycle for every positive integer k. This conjecture was formulated first by [2]. Using computer search it was verified independently by various sources that M_{2k+1} has a Hamiltonian cycle for $1 \le k \le 15$. This was also verified for $k = 16$ and $k = 17$ in [6] and for $k = 18$ in [7]. In [5] it was shown how to produce long cycles in M_{2k+1} based on a Hamiltonian cycle in a graph $M_{2k'+1}$ for which $k' < k$. Finally, in [4] it is shown that asymptotically a Hamiltonian cycle exists in M_{2k+1}, i.e., that there exists a cycle of length $(1-o(1))2\binom{2k+1}{k}$ in M_{2k+1}.

In this paper we are interested in the q-analog of the middle levels problem. Let $\mathbb{F}_q^n$ be the vector space of dimension n over the finite field with q elements $\mathbb{F}_q$. Let $\mathcal{P}_q(n)$ be the graph whose set of vertices represents the set of all subspaces of $\mathbb{F}_q^n$. $\mathcal{P}_q(n)$ is called the *projective space graph*. Two subspaces X and Y are connected by an edge if $\dim X + \dim Y - 2\dim(X \cap Y) = 1$, i.e., the dimensions of X and Y differ by one and either $X \subset Y$ or $Y \subset X$. The *middle levels* of $\mathcal{P}_q(2k+1)$ is the graph which is induced by the vertices (subspaces) of dimension k and the vertices (subspaces) of dimension $k+1$ from $\mathcal{P}_q(2k+1)$. The *middle levels problem* for $\mathcal{P}_q(2k+1)$ is to find a Hamiltonian cycle in the middle levels of $\mathcal{P}_q(2k+1)$.

One of the most important methods to construct long cycles in M_{2k+1} was introduced in [1]. A *necklace* is a set which consists of an n-tuple and all its distinct cyclic shifts. Let $n = 2k+1$ and assume that there exists a sequence of n-tuples $P = x_1, y_1, x_2, y_2, \dots, x_t, y_t$ satisfying the following requirements.

- x_i, $1 \le i \le t$, is an n-tuple with weight k.
- y_i, $1 \le i \le t$, is an n-tuple with weight $k+1$.

E-mail address: etzion@cs.technion.ac.il.

http://dx.doi.org/10.1016/j.disc.2014.04.028
0012-365X/

- All the $2t$ n-tuples in the sequence are contained in $2t$ different necklaces.
- x_i and y_i, $1 \le i \le t$, are connected by an edge in M_{2k+1}.
- y_i and x_{i+1}, $1 \le i \le t-1$, are connected by an edge in M_{2k+1}.
- There exists a cyclic shift of x_1 by ℓ positions which yields an n-tuple x'_1, such that y_t and x'_1 are connected by an edge in M_{2k+1} and $\gcd(\ell, n) = 1$.

We form the sequence $\Pi \overset{\text{def}}{=} P^0 = P, P^{\ell}, P^{2\ell}, P^{3\ell}, \ldots$, where superscripts are taken modulo n. P^i is the sequence formed from P by taking the cyclic shifts by i positions of all the n-tuples in P, where the order of the n-tuples in P and P^i is the same. Hence, the sequence Π ends with the subsequence $P^{n-\ell} = P^{(n-1)\ell}$ since $\gcd(\ell, n) = 1$.

We suggest a method, akin to the one based on necklaces to solve the middle levels problem of $\mathcal{P}_q(2k+1)$. The method is applied successfully and very simply with $k = 1$. For $k = 2$, we note that even though the value of k is small, the graph can be very large. The number of two-dimensional subspaces of $\mathbb{F}_q^5$ is $\frac{(q^5-1)(q^4-1)}{(q^2-1)(q-1)} = (q^4+q^3+q^2+q+1)(q^2+1)$ which is getting larger as q increases. The method is also applied successfully in this case as will be proved in this paper. It is worth to mention that a similar q-analog problem to find universal cycles of two-dimensional subspaces of $\mathcal{P}_q(n)$ is solved in [3]. For this problem, the one-dimensional subspaces of $\mathcal{P}_q(n)$ are ordered cyclically in such a way that each two-dimensional subspace of $\mathcal{P}_q(n)$ is spanned by exactly one pair of adjacent one-dimensional subspaces and each one-dimensional subspace of $\mathcal{P}_q(n)$ appears at least once in the ordering.

The rest of this paper is organized as follows. In Section 2, we discuss the representation of subspaces. We define the cyclic shifts of subspaces and describe our method to form long cycles in the middle levels of $\mathcal{P}_q(2k+1)$. In Section 3, we prove some properties of two-dimensional subspaces and three-dimensional subspaces of $\mathbb{F}_q^5$ which will be very useful when our method is applied on $\mathcal{P}_q(5)$. In Section 4, we will show how to construct Hamiltonian cycles in the middle levels of $\mathcal{P}_q(5)$. Conclusion is given in Section 5.

2. Hamiltonian cycles based on cyclic shifts

Given a nonnegative integer $r \le n$, the set of all subspaces of $\mathbb{F}_q^n$ that have dimension r is known as a *Grassmannian*, and usually denoted by $\mathcal{G}_q(n, r)$. The number of subspaces in $\mathcal{G}_q(n, r)$ is

$$|\mathcal{G}_q(n,r)| = \begin{bmatrix} n \\ r \end{bmatrix}_q \overset{\text{def}}{=} \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-r+1}-1)}{(q^r-1)(q^{r-1}-1)\cdots(q-1)},$$

where $\begin{bmatrix} n \\ r \end{bmatrix}_q$ is the *q-ary Gaussian coefficient*. We note that the number of one-dimensional subspaces of $\mathbb{F}_q^n$ is $\frac{q^n-1}{q-1}$, where two vectors of $\mathbb{F}_q^n$ which are multiples of each other by an element of $\mathbb{F}_q$ belong to the same one-dimensional subspace.

Let $\mathbb{F}_{q^n}$ be a finite field with q^n elements, where q is a power of a prime number, and let α be a primitive element in $\mathbb{F}_{q^n}$. It is well-known that there is an isomorphism between $\mathbb{F}_{q^n}$ and $\mathbb{F}_q^n$, where the *zero* elements are mapped into each other, and $\alpha^i \in \mathbb{F}_{q^n}$, $0 \le i \le q^n-2$, is mapped into its q-ary n-tuple representation in $\mathbb{F}_q^n$, and vice versa. Assume that $\alpha^i, \alpha^j \in \mathbb{F}_{q^n}$ and their n-tuple representations are $X^i = (x_1^i, x_2^i, \ldots, x_n^i)$ and $X^j = (x_1^j, x_2^j, \ldots, x_n^j)$, respectively, where $x_\ell^i, x_\ell^j \in \mathbb{F}_q$, $1 \le \ell \le n$. The isomorphism implies that the n-tuple $(x_1^i + x_1^j, x_2^i + x_2^j, \ldots, x_n^i + x_n^j)$, where the addition is done in $\mathbb{F}_q$, is the n-tuple representation of $\alpha^i + \alpha^j$. Using this mapping, a subspace of $\mathbb{F}_q^n$ is represented by the corresponding elements of $\mathbb{F}_{q^n}$. Throughout this paper we will not distinguish between the two representations and the vector representation will coincide with the finite field representation. Moreover, we will also abuse notation by not distinguishing between one-dimensional subspaces and elements in the field. This will imply that α^i and $\beta\alpha^i$, $\beta \in \mathbb{F}_q \setminus \{0\}$, which are contained in the same one-dimensional subspace, will be considered as the same element. Using this notation and omitting the zero vector from the representation of a subspace, an r-dimensional subspace will be defined by its $\frac{q^r-1}{q-1}$ nonzero elements. Finally, if $X = \{\alpha^{i_1}, \ldots, \alpha^{i_{(q^r-1)/(q-1)}}\}$ is an r-dimensional subspace of $\mathbb{F}_q^n$ then we define the r-dimensional subspace βX by $\beta X \overset{\text{def}}{=} \{\beta\alpha^{i_1}, \ldots, \beta\alpha^{i_{(q^r-1)/(q-1)}}\}$, for any $\beta \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$.

We define the following relation E_r on the elements of $\mathcal{G}_q(n, r)$.

$$\text{For } X,\ Y \in \mathcal{G}_q(n,r), \quad (X,Y) \in E_r, \quad \text{if } Y = \alpha^j X \text{ for some } j\,. \tag{1}$$

The relation E_r will be applied for $r = k$ and $r = k+1$, where $n = 2k+1$.

The following three lemmas are essential in the discussion which follows. The first lemma can be readily verified.

Lemma 1. *E_r is an equivalence relation.*

Lemma 2. *If* $\gcd(\frac{q^r-1}{q-1}, \frac{q^n-1}{q-1}) = 1$ *then the number of elements in an equivalence class of* E_r *is* $\frac{q^n-1}{q-1}$.

Proof. Let X be an r-dimensional subspace of $\mathcal{P}_q(n)$ represented as $X = \{x_1, x_2, \ldots, x_{\frac{q^r-1}{q-1}}\}$. If $X = \alpha^j X$ for some j, $1 \le j < \frac{q^n-1}{q-1}$ then clearly $X = \alpha^{j\ell} X$ for any positive integer ℓ. Moreover, if such j exists then $x_i = \alpha^{j\frac{q^r-1}{q-1}} x_i$ for each i, $1 \le i \le \frac{q^r-1}{q-1}$.

Assume that there exists an equivalence class of E_r whose size is j, $j < \frac{q^n-1}{q-1}$. This implies that $X = \alpha^j X$ and hence for each i, $1 \leq i \leq \frac{q^r-1}{q-1}$, we have $x_i = \alpha^{j\frac{q^r-1}{q-1}} x_i$. Therefore, $\frac{q^n-1}{q-1}$ divides $j\frac{q^r-1}{q-1}$, but since $j < \frac{q^n-1}{q-1}$ it follows that $\gcd(\frac{q^r-1}{q-1}, \frac{q^n-1}{q-1}) > 1$. Hence, if $\gcd(\frac{q^r-1}{q-1}, \frac{q^n-1}{q-1}) = 1$ then there is no equivalence class of E_r whose size is less than $\frac{q^n-1}{q-1}$. $\square$

Finally, the following lemma is also trivial.

Lemma 3. $\gcd(\frac{q^k-1}{q-1}, \frac{q^n-1}{q-1}) = 1$ *if and only if* $\gcd(k, n) = 1$.

Corollary 1. *If* $n = 2k + 1$ *then* $\gcd(\frac{q^k-1}{q-1}, \frac{q^n-1}{q-1}) = 1$ *and* $\gcd(\frac{q^{k+1}-1}{q-1}, \frac{q^n-1}{q-1}) = 1$.

We will modify the construction, based on necklaces, for a cycle in the middle levels of the Hamming graph to form a cycle in the middle levels of the projective space graph $\mathcal{P}_q(2k + 1)$. Instead of necklaces we will use the equivalence classes of the relation E_r. The construction is implied by the following theorem.

Theorem 1. *Assume that there exists a sequence of subspace of* $\mathbb{F}_q^{2k+1}$, $P = X_1, Y_1, X_2, Y_2, \ldots, Y_t, Y_t$, *satisfying the following requirements.*

P.1 X_i, $1 \leq i \leq t$, *is a* k*-dimensional subspace of* $\mathbb{F}_q^{2k+1}$.
P.2 Y_i, $1 \leq i \leq t$, *is a* $(k + 1)$*-dimensional subspace of* $\mathbb{F}_q^{2k+1}$.
P.3 *All the* $2t$ *subspaces of* $\mathbb{F}_q^{2k+1}$ *in the sequence* P *are contained in* $2t$ *different equivalence classes of* E_k *and* E_{k+1}.
P.4 X_i *and* Y_i, $1 \leq i \leq t$, *are connected by an edge in* $\mathcal{P}_q(2k + 1)$.
P.5 Y_i *and* X_{i+1}, $1 \leq i \leq t - 1$, *are connected by an edge in* $\mathcal{P}_q(2k + 1)$.
P.6 $\alpha^\ell X_1$ *and* Y_t *are connected by an edge in* $\mathcal{P}_q(2k + 1)$ *and* $\gcd(\ell, \frac{q^{2k+1}-1}{q-1}) = 1$.

Then there exists a cycle of length $2t\frac{q^{2k+1}-1}{q-1}$ *in the middle levels of* $\mathcal{P}_q(2k + 1)$.

Proof. By P.1, P.2, P.3, P.4, and P.5, we have that P is a path in the middle levels of $\mathcal{P}_q(2k+1)$. By Lemma 2 and Corollary 1, we have that the number of subspaces in each equivalence class of E_k and each equivalence class of E_{k+1} is $\frac{q^{2k+1}-1}{q-1}$. By Corollary 1, we also have that the paths $P^{i\ell}$ and $P^{j\ell}$, $0 \leq i < j \leq \frac{q^{2k+1}-1}{q-1} - 1$, where superscripts are taken modulo $\frac{q^{2k+1}-1}{q-1}$, are disjoint. Taking P.6 into account too implies that $P^{i\ell}, P^{(i+1)\ell}$, $0 \leq i \leq \frac{q^{2k+1}-1}{q-1} - 1$, is also a path in the middle levels of $\mathcal{P}_q(2k + 1)$. Thus, $P^0, P^\ell, P^{2\ell}, \ldots, P^{\frac{q^{2k+1}-1}{q-1}-\ell}$ is a cycle in the middle levels of $\mathcal{P}_q(2k + 1)$. $\square$

Corollary 2. *If the requirements of Theorem 1 are satisfied with* $t = \begin{bmatrix} 2k+1 \\ k \end{bmatrix}_q \frac{q-1}{q^{2k+1}-1}$ *then there exists a Hamiltonian cycle in the middle levels of* $\mathcal{P}_q(2k + 1)$.

The requirements of Theorem 1 can be easily satisfied with $t = \begin{bmatrix} 2k+1 \\ k \end{bmatrix}_q \frac{q-1}{q^{2k+1}-1}$, for any q and $k = 1$. For this purpose we need the discussion in [8] in which the following theorem is proved.

Theorem 2. *Let* α *be a primitive element in* $\mathbb{F}_q^3$. *Let* $\alpha^{i_0}, \alpha^{i_1}, \ldots, \alpha^{i_q}$, $0 \leq i_0 < i_1 < \cdots < i_q \leq q^2 + q$, *be* $q + 1$ *elements in* $\mathbb{F}_q^3$, *for which any two are linearly independent and any three are linearly dependent. Then for any* ℓ *there exists exactly one pair* α^{i_r}, α^{i_s}, $r \neq s$, *such that* $i_r - i_s \equiv \ell \pmod{q^2 + q + 1}$.

Let Y be any two-dimensional subspace of $\mathbb{F}_q^3$. Clearly, Y contains $q + 1$ elements and can be regarded as a line in the projective plane of order q. Therefore, by Theorem 2 there exists a j, $0 \leq j < \frac{q^3-1}{q-1}$ such that $\alpha^j, \alpha^{j+1} \in Y$. If X is the one-dimensional subspace which contains α^j then we choose $P = X, Y$, and the requirements of Theorem 1 are satisfied with $t = \begin{bmatrix} 2k+1 \\ k \end{bmatrix}_q \frac{q-1}{q^{2k+1}-1} = 1$ and $\ell = 1$. Therefore, by Corollary 2, we have constructed a Hamiltonian cycle in the middle levels of $\mathcal{P}_q(3)$. In fact by Theorem 2, for each ℓ, $1 \leq \ell \leq q^2 + q$ there exists a j, $0 \leq j < \frac{q^3-1}{q-1}$ such that $\alpha^j, \alpha^{j+\ell} \in Y$, which implies the existence of a few Hamiltonian cycles in the middle levels of $\mathcal{P}_q(3)$.

3. Two- and three-dimensional subspaces of $\mathbb{F}_q^5$

In this section we will explore some interesting properties of two-dimensional subspaces and three-dimensional subspaces of $\mathbb{F}_q^5$. These properties will be used in the next section to construct many different Hamiltonian cycles in the middle levels of $\mathcal{P}_q(5)$. We start by considering the two equivalence relations E_2 on $\mathcal{G}_q(5, 2)$ and E_3 on $\mathcal{G}_q(5, 3)$ as was defined earlier in (1). Our construction of Hamiltonian cycles in the middle levels of $\mathcal{P}_q(5)$ is based on properties which connect E_2 and E_3. These properties are formulated in the following theorem whose proof requires a sequence of lemmas which follow.

Theorem 3. *Each three-dimensional subspace of $\mathbb{F}_q^5$ contains exactly $q+1$ elements from one equivalence class of the relation E_2 and exactly one element from each other equivalence class of E_2.*

The consequences of Theorem 3 in terms of the bipartite middle levels subgraph of $\mathcal{P}_q(5)$ will be used in our construction. Let v be a vertex, representing a three-dimensional subspace, in the middle levels of $\mathcal{P}_q(5)$. A three-dimensional subspace contains $\begin{bmatrix}3\\2\end{bmatrix}_q = q^2+q+1$ two-dimensional subspaces. Therefore, the degree of v is q^2+q+1, $q+1$ edges to $q+1$ distinct vertices representing one equivalence class of E_2, and q^2 edges to q^2 vertices representing the other q^2 equivalence classes of E_2. These are the basic properties used in our construction of a Hamiltonian cycle in the middle levels of $\mathcal{P}_q(5)$.

We start with an immediate consequence of Lemma 2 related to E_2 and E_3.

Corollary 3. *Each equivalence class of E_2 and each equivalence class of E_3 contains $s \overset{\text{def}}{=} \frac{q^5-1}{q-1} = q^4+q^3+q^2+q+1$ elements.*

Corollary 4. *The number of equivalence classes of E_2 is q^2+1 and this is also the number of equivalence classes of E_3.*

Proof. The number of two-dimensional subspaces of $\mathbb{F}_q^5$ is $\frac{(q^5-1)(q^4-1)}{(q^2-1)(q-1)} = s(q^2+1)$. Thus, by Corollary 3, the number of equivalence classes of E_2 is q^2+1. The same computation holds for E_3. $\square$

Lemma 4. *α^0, α^i, and α^{2i}, $1 \le i \le s-1$, are linearly independent elements in $\mathbb{F}_{q^5}$.*

Proof. Assume the contrary, that α^0, α^i, and α^{2i}, are linearly dependent. This implies that $\alpha^0, \alpha^i, \alpha^{2i}, \dots, \alpha^{qi}$, is a two-dimensional subspace and $\alpha^{(q+1)i} = \beta\alpha^0$ for some $\beta \in \mathbb{F}_q$ and hence $\alpha^{(q+1)i} \in \mathbb{F}_q$. Since $\alpha^0, \alpha^s, \dots, \alpha^{(q-2)s}$ are the elements of $\mathbb{F}_q$ in $\mathbb{F}_{q^5}$ it follows that $\alpha^{(q+1)i} = \alpha^{\ell s}$, for some $1 \le \ell \le q-1$. This implies that $q+1$ divides ℓs. Since $s = \frac{q^5-1}{q-1} = q^4+q^3+q^2+q+1$ it follows that $\frac{\ell s}{q+1} = \ell(q^3+q+\frac{1}{q+1})$ and hence $q+1$ divides ℓ. But, since $1 \le \ell \le q-1$ this is impossible, a contradiction. Thus, α^0, α^i, and α^{2i}, are linearly independent elements in $\mathbb{F}_{q^5}$. $\square$

Lemma 5. *Each two-dimensional subspace L has exactly q^2+q distinct pairs of the form (x, y) such that $L = \langle x, y \rangle$.*

Proof. Let L be a two-dimensional subspace. L is spanned by any two of its one-dimensional subspaces. L contains exactly $q+1$ distinct one-dimensional subspaces. Hence, the number of distinct ordered pairs of elements from L is $(q+1)q$. Thus, L has exactly q^2+q distinct pairs of the form (x, y) such that $L = \langle x, y \rangle$. $\square$

Lemma 6. *If (α^t, α^{t+i}), $(\alpha^\ell, \alpha^{\ell+j})$, $0 \le t < \ell < s$, are two distinct pairs of one-dimensional subspaces in a two-dimensional subspace L then $i \not\equiv j \pmod{s}$.*

Proof. Assume the contrary, that (α^t, α^{t+i}), $(\alpha^\ell, \alpha^{\ell+j})$ are two distinct pairs of one-dimensional subspaces in a two-dimensional subspace L and $i \equiv j \pmod{s}$. Since $L = \langle \alpha^t, \alpha^{t+i} \rangle = \langle \alpha^\ell, \alpha^{\ell+i} \rangle$ it follows that $L = \alpha^{\ell-t}L$. Since the number of one-dimensional subspaces in a two-dimensional subspace is $q+1$, it follows by Lemma 2 that $\gcd(q+1, s) > 1$, a contradiction. $\square$

The set $\mathcal{D} \overset{\text{def}}{=} \{i \;:\; \langle \alpha^0, \alpha^i \rangle \in \mathcal{G}_q(5, 2)\}$ contains $s-1 = q^4+q^3+q^2+q$ elements. By Lemmas 5 and 6 it follows that each equivalence class of E_2 can be represented by q^2+q distinct elements from $\mathcal{D}$ and the possible representatives of each equivalent class are disjoint. Therefore, an equivalence class of E_2 will be denoted by $[\langle \alpha^0, \alpha^i \rangle]$, where each subspace of the equivalence class has a distinct pair of elements of the form (α^t, α^{t+i}).

Lemma 7. *If $\langle \alpha^t, \alpha^{t+i} \rangle$ and $\langle \alpha^\ell, \alpha^{\ell+i} \rangle$, $1 \le i \le s-1$, are two distinct two-dimensional subspaces in a three-dimensional subspace Z of $\mathbb{F}_q^5$ then $Z = \langle \alpha^r, \alpha^{r+i}, \alpha^{r+2i} \rangle$ for some r, $0 \le r \le s-1$.*

Proof. For any given $\beta \in \mathbb{F}_q \setminus \{0\}$, we have $\alpha^t + \beta\alpha^\ell = \alpha^m$ and $\alpha^{t+i} + \beta\alpha^{\ell+i} = \alpha^{m+i}$, for some m, $0 \le m \le s-1$, $m \notin \{t, \ell\}$. This implies that in Z there are two two-dimensional subspaces of the form

$$\alpha^{b_0}, \alpha^{b_1}, \dots, \alpha^{b_q}$$
$$\alpha^{b_0+i}, \alpha^{b_1+i}, \dots, \alpha^{b_q+i}.$$

Any two distinct two-dimensional subspaces in a three-dimensional subspace intersect in exactly one one-dimensional subspace. Therefore, w.l.o.g. we can assume that $b_1 = b_0 + i$. Hence, Z contains the points α^{b_0}, $\alpha^{b_1} = \alpha^{b_0+i}$, $\alpha^{b_1+i} = \alpha^{b_0+2i}$. By Lemma 4, these three points are linearly independent and thus $Z = \langle \alpha_0^b, \alpha^{b_0+i}, \alpha^{b_0+2i} \rangle$. $\square$

Lemma 8. *Each three-dimensional subspace of $\mathbb{F}_q^5$ can be represented as $\langle \alpha^r, \alpha^{r+i}, \alpha^{r+2i} \rangle$ for some r and i such that $0 \le r \le s-1$, $1 \le i \le s-1$.*

Proof. A three-dimensional subspace Z contains q^2+q+1 distinct one-dimensional subspaces. Therefore, there are $(q^2+q+1)(q^2+q) = q^4+2q^3+2q^2+q$ ordered pairs of one-dimensional subspaces of the form (x, y), $x, y \in Z$, $x \neq y$. $s = \frac{q^5-1}{q-1} =$

$q^4+q^3+q^2+q+1$ and hence the set $\{i\ :\ (\alpha^t, \alpha^{t+i}) \in Z \times Z,\ 0 < i < s\}$ contains at most $q^4+q^3+q^2+q$ distinct integers. Hence, there exist at least two distinct pairs of the form (α^t, α^{t+i}), $(\alpha^\ell, \alpha^{\ell+i})$, $\alpha^t, \alpha^{t+i}, \alpha^\ell, \alpha^{\ell+i} \in Z$. Hence, Z contains two distinct two-dimensional subspaces of the form $\langle \alpha^t, \alpha^{t+i}\rangle$ and $\langle \alpha^\ell, \alpha^{\ell+i}\rangle$. Thus, by Lemma 7 the claim follows. □

Lemma 9. *If Z is a three-dimensional subspace of $\mathbb{F}_q^5$ represented as $\langle \alpha^r, \alpha^{r+i}, \alpha^{r+2i}\rangle$ for some r and i such that $0 \le r \le s-1$, $1 \le i \le s-1$, then it contains at least $q+1$ two-dimensional subspaces from the equivalence class $[\langle \alpha^0, \alpha^i\rangle]$ of E_2.*

Proof. For any given $\beta \in \mathbb{F}_q \setminus \{0\}$, we have $\alpha^r + \beta\alpha^{r+i} = \alpha^{m_\beta}$ and $\alpha^{r+i} + \beta\alpha^{r+2i} = \alpha^{m_\beta+i}$, for some m_β, $0 \le m_\beta \le s-1$. Therefore, $\langle \alpha^r, \alpha^{r+i}, \alpha^{r+2i}\rangle$ contains the $q-1$ two-dimensional subspaces $\langle \alpha^{m_\beta}, \alpha^{m_\beta+i}\rangle$, $\beta \in \mathbb{F}_q \setminus \{0\}$, and the two two-dimensional subspaces $\langle \alpha^r, \alpha^{r+i}\rangle$ and $\langle \alpha^{r+i}, \alpha^{r+2i}\rangle$. These $q+1$ two-dimensional subspaces are from the equivalence class $[\langle \alpha^0, \alpha^i\rangle]$ of E_2. □

Lemma 10. *For a three-dimensional subspace Z of $\mathbb{F}_q^5$ there exists exactly one i, $1 \le i \le s-1$, such that Z contains exactly $q+1$ two-dimensional subspaces from the equivalence class $[\langle \alpha^0, \alpha^i\rangle]$ of E_2.*

Proof. By Lemma 8, each three-dimensional subspace of $\mathbb{F}_q^5$ can be represented as $\langle \alpha^r, \alpha^{r+i}, \alpha^{r+2i}\rangle$ for some r and i such that $0 \le r \le s-1$, $1 \le i \le s-1$. Hence, by Lemma 9, it contains at least $q+1$ two-dimensional subspaces from the equivalence class $[\langle \alpha^0, \alpha^i\rangle]$ of E_2. This equivalence class of E_2 is the same for all the three-dimensional subspaces which are contained in the same equivalence class of E_3.

Let Z_1 and Z_2 be two three-dimensional subspaces which contain $q+1$ two-dimensional subspaces from the equivalence class $[\langle \alpha^0, \alpha^i\rangle]$ of E_2. Then by Lemma 7, $Z_j = \langle \alpha^{r_j}, \alpha^{r_j+i}, \alpha^{r_j+2i}\rangle$ for some r_j, $0 \le r_j \le s-1$, $j = 1, 2$. Hence, Z_1 and Z_2 are contained in the same equivalence class of E_3. By Corollary 4, the number of equivalence classes of E_3 is q^2+1 and the number of equivalence classes of E_2 is q^2+1. Therefore, by the above arguments and the pigeonhole principle, if there exists a three-dimensional subspace of $\mathbb{F}_q^5$ which contains $q+1$ two-dimensional subspaces from two different equivalences classes of E_2 then there exists a three-dimensional subspace of $\mathbb{F}_q^5$ which does not contain any $q+1$ two-dimensional subspaces which are contained in one equivalence class of E_2. This is a contradiction to Lemmas 8 and 9. □

In the sequel, an equivalence class of E_3 will be represented by $[\langle \alpha^0, \alpha^i, \alpha^{2i}\rangle]$, if each of its three-dimensional subspaces have a subspaces of the form $\langle \alpha^r, \alpha^{r+i}, \alpha^{r+2i}\rangle$. By Lemma 10 there is no ambiguity in using this representation and this representation is unique.

Lemma 11. *A three-dimensional subspace in the equivalence class $[\langle \alpha^0, \alpha^i, \alpha^{2i}\rangle]$ contains at most one two-dimensional subspace from each equivalence class of E_2 different from $[\langle \alpha^0, \alpha^i\rangle]$.*

Proof. Assume Z is a three-dimensional subspace in the equivalence class $[\langle \alpha^0, \alpha^i, \alpha^{2i}\rangle]$. If Z has two two-dimensional subspaces of the form $\langle \alpha^t, \alpha^{t+j}\rangle$ and $\langle \alpha^\ell, \alpha^{\ell+j}\rangle$, $j \ne i$, then by Lemma 7, $Z = \langle \alpha^u, \alpha^{u+j}, \alpha^{u+2j}\rangle$ for some u, $0 \le u \le s-1$. This implies that $Z \in [\langle \alpha^0, \alpha^i, \alpha^{2j}\rangle]$ and hence by Lemma 9, it contains $q+1$ distinct two-dimensional subspaces from $[\langle \alpha^0, \alpha^j\rangle]$. By Lemma 10, this implies that $[\langle \alpha^0, \alpha^i\rangle] = [\langle \alpha^0, \alpha^j\rangle]$ and the lemma follows. □

Proof of Theorem 3. By Lemma 10, each three-dimensional subspace Z of $\mathbb{F}_q^5$ contains $q+1$ distinct two-dimensional subspaces from exactly one equivalence class of E_2. By Lemma 11, from each other equivalence class of E_2 at most one two-dimensional subspace is contained in Z. Since a three-dimensional subspace contains q^2+q+1 distinct two-dimensional subspaces it follows that Z contains $q+1$ two-dimensional subspaces from one equivalence class of E_2 and one two-dimensional subspace from exactly q^2 different equivalence classes of E_2. Since by Corollary 4, E_2 has exactly q^2+1 equivalence classes the claim of the lemma follows immediately. □

Finally, we will use the following two lemmas in our construction.

Lemma 12. $[\langle \alpha^0, \alpha^1\rangle] \ne [\langle \alpha^0, \alpha^2\rangle]$.

Proof. Assume the contrary, that $[\langle \alpha^0, \alpha^1\rangle] = [\langle \alpha^0, \alpha^2\rangle]$. This implies that there exists a j, $5 \le j \le s-4$, such that $\alpha^0, \alpha^1, \alpha^j, \alpha^{j+2} \in \langle \alpha^0, \alpha^1\rangle$. This implies that $\alpha^{j+2} = a + b\alpha$ and $\alpha^j = c + d\alpha$, $a, b, c, d \in \mathbb{F}_q$. Therefore, $\alpha^2 = \frac{a+b\alpha}{c+d\alpha}$ and hence $c\alpha^2 + d\alpha^3 = a + b\alpha$. A nontrivial solution for this equation implies that α is a root of a cubic polynomial, contradicting the fact that lowest degree polynomial for which α is a root has degree five. Thus, $[\langle \alpha^0, \alpha^1\rangle] \ne [\langle \alpha^0, \alpha^2\rangle]$. □

Lemma 13. $[\langle \alpha^0, \alpha^1, \alpha^2\rangle] \ne [\langle \alpha^0, \alpha^1, \alpha^3\rangle]$.

Proof. Assume the contrary, that $[\langle \alpha^0, \alpha^1, \alpha^2\rangle] = [\langle \alpha^0, \alpha^1, \alpha^3\rangle]$. $\langle \alpha^0, \alpha^1\rangle = \{\alpha^0, \alpha^1, \alpha^{i_1}, \alpha^{i_2}, \ldots, \alpha^{i_{q-1}}\}$ and hence $\langle \alpha^1, \alpha^2\rangle = \{\alpha^1, \alpha^2, \alpha^{i_1+1}, \alpha^{i_2+1}, \ldots, \alpha^{i_{q-1}+1}\}$. Since $\langle \alpha^0, \alpha^1, \alpha^2\rangle \in [\langle \alpha^0, \alpha^1, \alpha^3\rangle]$ it follows that there exists a j, such that $\alpha^j, \alpha^{j+1}, \alpha^{j+3} \in \langle \alpha^0, \alpha^1, \alpha^2\rangle$. Clearly $j \in \{0, 1, i_1, i_2, \ldots, i_{q-1}\}$. If $j = 0$ or $j = 1$ then α is a root of a polynomial of degree less than five. Therefore, $j = i_r$ for some $1 \le r \le q-1$. This implies that $\langle \alpha^0, \alpha^2\rangle$ and $\langle \alpha^{i_r+1}, \alpha^{i_r+3}\rangle$ are subspaces of $\langle \alpha^0, \alpha^1, \alpha^2\rangle$.

Therefore, there are at least two distinct subspaces from $[\langle \alpha^0, \alpha^2\rangle]$ which are contained in $\langle \alpha^0, \alpha^1, \alpha^2\rangle$. Hence, by Theorem 3 we have that $[\langle \alpha^0, \alpha^1\rangle] = [\langle \alpha^0, \alpha^2\rangle]$ which contradicts Lemma 12. □

4. Hamiltonian cycles

In this section we will describe a construction for Hamiltonian cycles in the middle levels of $\mathcal{P}_q(5)$ for any given power of a prime q. The construction will be based on Theorem 1 and Corollary 2. To satisfy the requirements of Theorem 1 we will use the properties, of two-dimensional and three-dimensional subspaces, which were proved in the previous section. We will also show that the number of such Hamiltonian cycles is very large. The construction will be performed in a few steps. First, we will present a construction which can satisfy the requirements of Theorem 1. Unfortunately, we would not be able to prove this for all parameters. Therefore, we will make a small modification in the construction and present a construction which yields a Hamiltonian path. Finally, we will make more modifications in the construction which will enable us to construct many Hamiltonian cycles in the middle levels of $\mathcal{P}_q(5)$. In the sequel, given a path (cycle) $P = X_1, X_2, \dots, X_t$ which consists of subspaces from $\mathcal{P}_q(5)$ we define the path (cycle) βP, $\beta \in \mathbb{F}_{q^5}$, by $\beta P \overset{\text{def}}{=} \beta X_1, \beta X_2, \dots, \beta X_t$.

Let $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_e$ be any order of the $e = q^2 + 1$ equivalence classes of E_3, in which $\mathcal{A}_1 = [\langle \alpha^0, \alpha^1, \alpha^2 \rangle]$. Let $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_e$ be any order of the $q^2 + 1$ equivalence classes of E_2, in which $\mathcal{B}_e = [\langle \alpha^0, \alpha^1 \rangle]$. The following lemma is an immediate consequence of Theorem 3.

Lemma 14. *There exists a path $P = U_1, V_1, U_2, V_2, \dots, U_e, V_e$ in the middle levels of $\mathcal{P}_q(5)$, such that $U_i \in \mathcal{A}_i$, $V_i \in \mathcal{B}_i$, $U_i \supset V_i$, for each $1 \le i \le e$; $V_i \subset U_{i+1}$, for each $1 \le i \le e - 1$.*

The path obtained via Lemma 14 can be chosen in many different ways. We will restrict these choices in the following way. Let $U_1 = \langle \alpha^0, \alpha^1, \alpha^2 \rangle$, $V_1 = \langle \alpha^0, \alpha^2 \rangle$, U_e the two-dimensional subspace $\langle \alpha^{\ell+1}, \alpha^{\ell+2}, \alpha^{\ell+4} \rangle$ (clearly, by definition $V_{e-1} \subset U_e$), and V_e the unique two-dimensional subspace $\langle \alpha^{\ell+1}, \alpha^{\ell+2} \rangle$ for which $V_e \subset U_e$. These choices also determine the values of $\mathcal{A}_1$, $\mathcal{B}_1$, $\mathcal{A}_e$, and $\mathcal{B}_e$. By Lemmas 12 and 13, U_1, V_1, U_e, and V_e are contained in different equivalence classes of E_2 and E_3. Therefore, this order is possible and it is well defined. The parameter ℓ is defined by this order, even so we should understand that there are many possible choices to make this order and ℓ can differ between these different possible choices. If $g = \gcd(\ell, s)$, and assuming $\ell \ne 0$ (we consider the simpler case $\ell = 0$ at the end of this section), then let $\Pi = P, \alpha^\ell P, \alpha^{2\ell} P, \dots, \alpha^{(\frac{s}{g}-1)\ell} P$ be a sequence of subspaces (vertices) from the middle levels of $\mathcal{P}_q(5)$.

Lemma 15. *If $\ell \ne 0$ then the sequence of vertices (subspaces) $P, \alpha^\ell P$ is a path in the middle levels of $\mathcal{P}_q(5)$.*

Proof. By definition, P is a path in the middle levels of $\mathcal{P}_q(5)$ and hence also $\alpha^\ell P$ is a path in the middle levels of $\mathcal{P}_q(5)$. The last vertex in P is $V_e = \langle \alpha^{\ell+1}, \alpha^{\ell+2} \rangle$, while the first vertex in $\alpha^\ell P$ is $\alpha^\ell U_1 = \langle \alpha^\ell, \alpha^{\ell+1}, \alpha^{\ell+2} \rangle$. Clearly $V_e \subset \alpha^\ell U_1$ and hence $P, \alpha^\ell P$ is a path in the middle levels of $\mathcal{P}_q(5)$. □

Lemma 16. *If $\ell \ne 0$ then the sequence of vertices (subspaces) Π is a cycle in the middle levels of $\mathcal{P}_q(5)$ with $\frac{s}{g}2e$ distinct vertices.*

Proof. By Lemma 15, we have that Π is a cycle in the middle levels of $\mathcal{P}_q(5)$. Since $g = \gcd(\ell, s)$ it follows that the set $\{\alpha^{i\ell} U_j \,:\, 0 \le i < \frac{s}{g}\}$ contains $\frac{s}{g}$ distinct three-dimensional subspaces for each j, $1 \le j \le e$. Similarly, $\{\alpha^{i\ell} V_j \,:\, 0 \le i < \frac{s}{g}\}$ contains $\frac{s}{g}$ distinct two-dimensional subspaces for each j, $1 \le j \le e$. Therefore, Π is a cycle in the middle levels of $\mathcal{P}_q(5)$ with $\frac{s}{g}2e$ distinct vertices. □

Corollary 5. *If $\ell \ne 0$ and $g = 1$ then Π is a Hamiltonian cycle in the middle levels of $\mathcal{P}_q(5)$.*

Corollary 6. *If $\ell \ne 0$ then the g cycles Π, $\alpha\Pi$, $\alpha^2\Pi, \dots, \alpha^{g-1}\Pi$, contain exactly all the vertices of the middle levels of $\mathcal{P}_q(5)$. Each vertex from the middle levels of $\mathcal{P}_q(5)$ is contained exactly once in one of these cycles.*

The condition $g = 1$ in Corollary 5 is satisfied in many cases. For example, if s is a prime integer then $g = 1$. Moreover, due to many choices in which the equivalence classes can be ordered, and many choices for the relative shifts of the U_i's and V_j's, such that the requirements of Theorem 1 are satisfied, it is reasonable to believe that in many of them we will have $g = 1$. But, we were not able to prove this and hence we will slightly modify the construction to be able and obtain a desired Hamiltonian cycle.

If $g > 1$ then we consider Π as a path in the middle levels of $\mathcal{P}_q(5)$ and define the sequence of vertices (subspaces) $\Pi, \alpha\Pi, \alpha^2\Pi, \dots, \alpha^{g-1}\Pi$.

Lemma 17. *If $\ell \ne 0$ and $g \ne 1$ then the sequence of vertices (subspaces) $\Pi, \alpha\Pi$ is a path with $\frac{s}{g}4e$ distinct vertices in the middle levels of $\mathcal{P}_q(5)$.*

Proof. By Lemma 16, we have that Π is a path in the middle levels of $\mathcal{P}_q(5)$ and therefore $\alpha\Pi$ is also a path in the middle levels of $\mathcal{P}_q(5)$. The last vertex (subspace) of Π is $\alpha^{(\frac{s}{g}-1)\ell} V_e = \alpha^{(\frac{s}{g}-1)\ell} \langle \alpha^{\ell+1}, \alpha^{\ell+2} \rangle = \alpha^{\frac{s}{g}\ell} \langle \alpha^1, \alpha^2 \rangle = \langle \alpha^1, \alpha^2 \rangle$ and the first vertex (subspace) of $\alpha\Pi$ is $\alpha U_1 = \langle \alpha^1, \alpha^2, \alpha^3 \rangle$. Therefore, $\alpha^{(\frac{s}{g}-1)\ell} V_e \subset \alpha U_1$ and hence $\Pi, \alpha\Pi$ is a path with $\frac{s}{g}4e$ distinct vertices in the middle levels of $\mathcal{P}_q(5)$. □

Corollary 7. *If $\ell \neq 0$ and $g \neq 1$ then $T \stackrel{\text{def}}{=} \Pi, \alpha\Pi, \alpha^2\Pi, \ldots, \alpha^{g-1}\Pi$ is a Hamiltonian path in the middle levels of $\mathcal{P}_q(5)$.*

Corollary 7 implies the existence of many Hamiltonian paths in the middle levels of $\mathcal{P}_q(5)$ since by Theorem 3, we can order the equivalence classes of E_2 and E_3 in almost any way that we want. Anyway, our goal is still to show the existence and to construct Hamiltonian cycles in the middle levels of $\mathcal{P}_q(5)$. To achieve our goal we will modify the Hamiltonian path which was obtained to form a Hamiltonian cycle. This will be done by flipping the tail of the path several times, preserving that the sequence of subspaces is still a path $\mathcal{P}_q(5)$, until a cycle is obtained.

Lemma 18. *If $\ell \neq 0$ and $g \neq 1$ then there exists a Hamiltonian cycle in the middle levels of $\mathcal{P}_q(5)$.*

Proof. Recall that $\Pi = \langle \alpha^0, \alpha^1, \alpha^2 \rangle, \langle \alpha^0, \alpha^2 \rangle, \ldots, \langle \alpha^{\ell+1}, \alpha^{\ell+2}, \alpha^{\ell+4} \rangle, \langle \alpha^{\ell+1}, \alpha^{\ell+2} \rangle, \langle \alpha^{\ell}, \alpha^{\ell+1}, \alpha^{\ell+2} \rangle, \langle \alpha^{\ell}, \alpha^{\ell+2} \rangle, \ldots, \langle \alpha^1, \alpha^2, \alpha^4 \rangle, \langle \alpha^1, \alpha^2 \rangle$. For a path Q, let $r(Q)$ denote the *reverse* of Q, i.e., $r(Q)$ is generated by taking the vertices of the path Q in reverse order. Let Υ_1 be the prefix of the path T which starts with the vertex $\langle \alpha^0, \alpha^1, \alpha^2 \rangle$ and ends with the vertex $\langle \alpha^1, \alpha^2, \alpha^4 \rangle$. If we denote $T_1 \stackrel{\text{def}}{=} \Upsilon_1, \langle \alpha^1, \alpha^2 \rangle, \alpha\Pi, \alpha^2\Pi, \ldots, \alpha^{g-1}\Pi$ then $T_2 \stackrel{\text{def}}{=} r(\Upsilon_1), \langle \alpha^1, \alpha^2 \rangle, \alpha\Pi, \alpha^2\Pi, \ldots, \alpha^{g-1}\Pi$ is also a Hamiltonian path in the middle levels of $\mathcal{P}_q(5)$. Note, that the first vertex (subspace) of $r(\Upsilon_1)$ is $\langle \alpha^1, \alpha^2, \alpha^4 \rangle$. Let Υ_2 be the prefix of T_2 which starts with the vertex $\langle \alpha^1, \alpha^2, \alpha^4 \rangle$ and ends with the vertex $\langle \alpha^2, \alpha^3, \alpha^4 \rangle$. If we denote $T_2 = \Upsilon_2, \langle \alpha^2, \alpha^4 \rangle, \tilde{P}_2$ then $T_3 = r(\Upsilon_2), \langle \alpha^2, \alpha^4 \rangle, \tilde{P}_2$. This is the first step in modifying the Hamiltonian path T_1. Before the ith step we have the Hamiltonian path $T_{2i-1} \stackrel{\text{def}}{=} \Upsilon_{2i-1}, \langle \alpha^{2i-1}, \alpha^{2i} \rangle, \alpha^{2i-1}\Pi, \alpha^{2i}\Pi, \ldots, \alpha^{g-1}\Pi$, where Υ_{2i-1} starts with the vertex (subspace) $\langle \alpha^{2i-2}, \alpha^{2i-1}, \alpha^{2i} \rangle$ and ends with $\langle \alpha^{2i-1}, \alpha^{2i}, \alpha^{2i+2} \rangle$. We form a new Hamiltonian path in the middle levels of $\mathcal{P}_q(5)$, $T_{2i} \stackrel{\text{def}}{=} r(\Upsilon_{2i-1}), \langle \alpha^{2i-1}, \alpha^{2i} \rangle, \alpha^{2i-1}\Pi, \alpha^{2i}\Pi, \ldots, \alpha^{g-1}\Pi$. Note, that the first vertex (subspace) of $r(\Upsilon_{2i-1})$ is $\langle \alpha^{2i-1}, \alpha^{2i}, \alpha^{2i+2} \rangle$. Let Υ_{2i} be the prefix of T_{2i} which starts with $\langle \alpha^{2i-1}, \alpha^{2i}, \alpha^{2i+2} \rangle$ and ends with $\langle \alpha^{2i}, \alpha^{2i+1}, \alpha^{2i+2} \rangle$ (which is the first vertex in $\alpha^{2i}\Pi$). If we denote $T_{2i} = \Upsilon_{2i}, \langle \alpha^{2i}, \alpha^{2i+2} \rangle, \tilde{P}_{2i}$ then $T_{2i+1} \stackrel{\text{def}}{=} r(\Upsilon_{2i}), \langle \alpha^{2i}, \alpha^{2i+2} \rangle, \tilde{P}_{2i}$. The path $r(\Upsilon_{2i})$ starts with the vertex (subspace) $\langle \alpha^{2i}, \alpha^{2i+1}, \alpha^{2i+2} \rangle$ and ends with the vertex (subspace) $\langle \alpha^{2i-1}, \alpha^{2i}, \alpha^{2i+2} \rangle$. The next vertex (subspace) in T_{2i+1} is $\langle \alpha^{2i}, \alpha^{2i+2} \rangle$ (which is the second vertex in $\alpha^{2i}\Pi$). The last vertex (subspace) in $\alpha^{2i}\Pi$ is $\langle \alpha^{2i+1}, \alpha^{2i+2} \rangle$. Therefore, we can write $T_{2i+1} = \Upsilon_{2i+1}, \langle \alpha^{2i+1}, \alpha^{2i+2} \rangle, \alpha^{2i+1}\Pi, \alpha^{2i+2}\Pi, \ldots, \alpha^{g-1}\Pi$ and we can continue with the recursive construction. The $\frac{g-1}{2}$-th step is the last one. The outcome of this step is the Hamiltonian path $T_g = \Upsilon_g, \langle \alpha^g, \alpha^{g+1} \rangle$. The first vertex in T_g is $\langle \alpha^g, \alpha^{g+1}, \alpha^{g+2} \rangle$ and the last vertex in T_g is $\langle \alpha^g, \alpha^{g+1} \rangle$. Therefore T_g is a Hamiltonian cycle. □

We assumed in the process that $\ell \neq 0$. For $\ell = 0$ we have a similar result.

Lemma 19. *If $\ell = 0$ then there exists a Hamiltonian cycle in the middle levels of $\mathcal{P}_q(5)$.*

Proof. We modify the path P defined in Lemma 14 and the paragraph succeeding it as follows. $U_1, V_1, U_2, V_2, \ldots, U_e, V_e$ are taken as in P; note that $V_e = \langle \alpha^1, \alpha^2 \rangle$. Let $\Pi = P, \alpha P, \alpha^2 P, \ldots, \alpha^{s-1}P$. Π is a Hamiltonian cycle in the middle levels of $\mathcal{P}_q(5)$ as proved in Lemma 15. □

The fact that the order of the q^2+1 equivalence classes of E_2 and the q^2+1 equivalence classes of E_3 is arbitrary (with some minor restrictions) implies immediately more than $(q^2!)^2$ Hamiltonian cycles obtained by our construction. This number can be increased as the choices are even more flexible, but we will omit the details as they are of less importance. From our main construction and its modifications as implied by Corollary 5, Lemmas 18 and 19 we infer the following theorem.

Theorem 4. *For each power of a prime q there exists a Hamiltonian cycle in the middle levels of $\mathcal{P}_q(5)$.*

Note that by Theorem 4 there exists a Hamiltonian cycle in the middle levels of $\mathcal{P}_q(5)$, but our discussion makes it possible to produce many such cycles. Unfortunately, we do not know how to count their number.

5. Conclusion and problems for future research

The well-known middle levels problem was considered for the k-dimensional subspaces and the $(k+1)$-dimensional subspaces of $\mathbb{F}_q^{2k+1}$. We have presented a technique based on cyclic shifts of k-dimensional subspaces and $(k+1)$-dimensional subspaces. The technique was applied successfully for all q's with $1 \leq k \leq 2$. Applying the technique for larger values of k to find Hamiltonian cycles or long cycles in the middle levels of $\mathcal{P}_q(2k+1)$ is the main goal for future research. We note that if $k > 2$ then the degree of a vertex v, representing a $(k+1)$-dimensional subspace of $\mathcal{P}_q(2k+1)$, is $\frac{q^{k+1}-1}{q-1}$. The number of equivalence classes of E_k will be $\begin{bmatrix} 2k+1 \\ k \end{bmatrix}_q \frac{q-1}{q^{2k+1}-1}$ which is much larger than $\frac{q^{k+1}-1}{q-1}$ and hence v will not be connected with an edge to a vertex from each equivalence class of E_k. Thus, we will not have a result similar to Theorem 3 and hence constructing the Hamiltonian path will be more difficult, even though it looks that there is enough freedom and we have the following conjecture.

Conjecture 1. *For any integer $k \geq 1$, and for any power of a prime q, there exists a Hamiltonian cycle in the middle levels of $\mathcal{P}_q(2k+1)$.*

Acknowledgments

The author would like to thank Ronny Roth for many valuable discussions which have contributed to the content of the paper. He also thanks two anonymous reviewers whose careful reading and well spotted comments contribute to amend this paper. This research was supported in part by the Israeli Science Foundation (ISF), Jerusalem, Israel, under Grant 10/12.

References

[1] I.J. Dejter, Hamilton cycles and quotients of bipartite graphs, in: Graphs and Other Combinatorial Topics, (Kalamazoo, Michigan 1984), Wiley, New York, 1985, pp. 189–199.
[2] I. Havel, Semipaths in directed cubes, Teubner-Texte Math. 59 (1983) 101–108. Graphs and other combinatorial topics (Prague, 1982).
[3] B.W. Jackson, J. Buhler, R. Mayer, A recursive construction for universal cycles of 2-subspaces, Discrete Math. 309 (2009) 5328–5331.
[4] J.R. Johnson, Long cycles in the middle two layers of the discrete cube, J. Combin. Theory, Ser. A 105 (2004) 255–271.
[5] C.D. Savage, P. Winkler, Monotone gray codes and the middle levels problem, J. Combin. Theory, Ser. A 70 (1995) 230–248.
[6] I. Shields, B.J. Shields, C.D. Savage, An update on the middle levels problem, Discrete Math. 309 (2009) 5271–5277.
[7] M. Shimada, K. Amano, A note on the middle levels conjecture, arxiv.org/abs/0912.4564, September 2011.
[8] J. Singer, A theorem in finite projective geometry and some applications to number theory, Trans. Amer. Math. Soc. 43 (1938) 377–385.