A recursive construction for universal cycles of 2-subspaces

Bradley W. Jackson a,*, Joe Buhler b, Ray Mayer c

a Department of Mathematics, San Jose State University, United States
b Center for Communications Research, La Jolla, United States
c Department of Mathematics, Reed College, United States

A R T I C L E   I N F O
Article history:
Received 30 August 2007
Received in revised form 24 November 2008
Accepted 25 November 2008
Available online 20 February 2009

Keywords:
Universal cycle
2-subspaces

A B S T R A C T
We prove that universal cycles of 2-dimensional subspaces of vector spaces over any finite field $F$ exist, i.e., if $V$ is a finite-dimensional vector space over $F$, there is a cycle of vectors $v_1, v_2, \ldots, v_n$ such that each 2-dimensional subspace of $V$ occurs exactly once as the span of consecutive vectors.

© 2009 Elsevier B.V. All rights reserved.

1. Introduction

Many constructions of de Bruijn cycles (or universal cycles, or u-cycles) for $k$-sequences are known. In [2] the authors conjectured the existence of analogous universal cycles of many other combinatorial structures, including subsets, subspaces, and partitions. Universal cycles of $k$-permutations over an arbitrary alphabet have been constructed in [6], and [3]. Universal cycles of $k$-subsets of an $n$-set have been constructed, for $n = 3$, [6], for $n = 4$, [6,2], for $n = 5$, [7], and for $n = 6$, [4]. Universal cycles of multisets have also been constructed in [6,5]. In [1] it was shown that universal cycles of 2-subspaces of $n$-dimensional vector spaces over the field with two elements always exist for any $n \geq 3$. In this paper we show that universal cycles of 2-subspaces exist for finite-dimensional vector spaces of dimension $n \geq 3$ over any finite field, and briefly discuss the situation for $k$-subspaces, $k > 2$.

Fix a finite field $F$ with $q$ elements. Let $V$ be an $n$-dimensional vector space over $F$. For $0 \leq k \leq n$ let $G(k, n)$ denote the Grassmannian of all $k$-dimensional subspaces (or $k$-subspaces) of $V$. Let

$$g(k, n) := |G(k, n)| = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}$$

be the number of such subspaces.

If we choose an isomorphism $V \cong F^n$ then subspaces can be represented as full-rank $k$ by $n$ matrices over $F$, where the rows are basis vectors and two such matrices give the same subspace if and only if they are row-equivalent. Thus $G(k, n)$ can be viewed as the set of rank $k$ row-echelon reduced $k \times n$ matrices over $F$.

We will prove that u-cycles of 2-subspaces exist for all $F$ and all $n$ by induction on $n$. In order to do this we need a relationship between subspaces of $F^n$ and $F^{n+1}$. For the sake of pointing towards larger values of $k$ it is convenient to prove a lemma for arbitrary $k$; it amounts to saying that a $k$ by $n + 1$ rank $k$ row-echelon matrix either has the last standard basis
vector in its last row or it does not; in the former case the first \(k - 1\) elements of the last column are 0, and in the latter case the last column is arbitrary.

Let \(\langle v_1, \ldots, v_k \rangle\) denote the span of the vectors \(v_i\).

Regard \(F^n\) as embedded in \(F^{n+1}\) as the subspace of all vectors whose last coordinate is zero. Let \(\delta = e_{n+1} = (0, 0, \ldots, 1)\) denote the last standard basis vector in \(F^{n+1}\). A \(k\)-subspace is said to be special if it contains \(\delta\), and regular otherwise.

**Lemma 1.** Regular subspaces \(U\) in \(G(k, n + 1)\) correspond bijectively to a choice of an element \(W = \langle v_1, \ldots, v_k \rangle\) in \(G(k, n)\), and a \(k\)-tuple \(a_1, \ldots, a_k\) of elements of \(F\) via

\[
U := \langle v_1 + a_1 \delta, v_2 + a_2 \delta, \ldots, v_k + a_k \delta \rangle.
\]

Special subspaces \(U\) in \(G(k, n + 1)\) correspond bijectively to elements \(W = \langle v_1, \ldots, v_{k-1} \rangle\) of \(G(k - 1, n)\) via

\[
U = \langle v_1, \ldots, v_{k-1}, \delta \rangle.
\]

**Proof.** If \(U\) is in \(G(k, n + 1)\) then let \(W\) be its projection onto \(F^n\). If \(W\) has dimension \(k - 1\), then \(\delta\) is in \(U, U\) is special, and it is easy to check that \(U\) has the form described in the statement.

If \(W\) has dimension \(k\), then the projection is an isomorphism, and \(U\) has the form described above, where \(v_i + a_i \delta\) is the unique pre-image of \(v_i\) under the projection. \(\blacksquare\)

Note that the Lemma implies the (readily verified) identity

\[
g(k, n + 1) = q^k \cdot g(k, n) + g(k, n - 1).
\]

2. Universal Cycles of 2-subspaces

From now on, interpret finite sequences of vectors \(v_1, v_2, \ldots, v_N\) as cycles, i.e., interpret indices modulo \(N\).

**Definition 2.** A cycle of vectors \(v_1, v_2, \ldots, v_N\) is said to cover \(G(k, n)\) if every element of \(G(k, n)\) occurs as the span of \(k\) consecutive vectors in the cycle. The cycle of vectors exactly covers \(G(k, n)\) if every subspace occurs exactly once, i.e., \(N = g(k, n)\), in which case we say that the sequence is a \(u\)-cycle for \(G(k, n)\).

Thus a cycle is a \(u\)-cycle if every \(k\)-dimensional subspace \(W\) occurs exactly once in the form

\[
W = \langle v_i, v_{i+1}, \ldots, v_{i+k-1} \rangle, \quad 0 \leq i < N.
\]

As a simple example we construct a \(u\)-cycle for \(G(1, n)\). Choose an isomorphism between \(F^n\) and the (additive group of) the field \(K\) with \(q^n\) elements. Let \(x\) be a generator of the cyclic multiplicative group \(K^* = K - \{0\}\). If \(N = g(1, n) = (q^n - 1)/(q - 1)\) then

\[
1, x, x^2, \ldots, x^{N-1}
\]

is a \(u\)-cycle for \(G(1, n)\). Indeed, the nonzero elements of the ground field \(F\) are generated by \(x^n\), and if \(\langle x^i \rangle = \langle x^j \rangle\) then \(x^i = yx^j\) for \(y\) in the ground field \(F\), which is impossible for \(0 \leq i, j < N\), and \(y\) an \(N\)-th power not equal to 1.

The existence of \(u\)-cycles for 2-subspaces of \(F^n\) will be proved by induction on \(n\). As often happens, it is crucial for the induction proof that the assertion be strengthened.

**Theorem 3.** For \(n \geq 3\) there is a cycle that covers \(G(1, n)\) and exactly covers \(G(2, n)\).

In other words, for each \(n\) there is a sequence of vectors \(v_1, v_2, \ldots, v_N\), where \(N = g(2, n)\), such that every 2-subspace is of the form \(\langle v_i, v_{i+1} \rangle\), and every 1-subspace is of the form \(\langle v_i \rangle\) for at least one \(i\). In particular, \(u\)-cycles exist for \(G(2, n)\).

**Proof.** For \(n = 3\), the \(u\)-cycle constructed above \(1, x, x^2, \ldots, x^{N-1}\) for \(G(1, 3)\) is also a \(u\)-cycle for \(G(2, 3)\). Indeed, suppose that

\[
\langle x^i, x^{i+1} \rangle = \langle x^j, x^{j+1} \rangle.
\]

Dividing by \(x^i\) we can assume, without loss of generality, that \(i = 0\). If \(\langle 1, x \rangle = \langle x^i, x^{i+1} \rangle\) there are \(a, b, c, d\) in \(F\) such that

\[
a + bx = x^i \quad c + dx = x^{i+1}
\]

and \(ad - bc \neq 0\). Multiplying the first equation by \(x\) and subtracting the second equation gives \(bx^2 + (a - d)x - c = 0\). This quadratic equation satisfied by \(x\) contradicts the fact that the minimal polynomial for \(x\) over \(F\) has degree \(n > 2\) unless \(b = c = 0\) and \(a = d\), in which case the constraint \(0 \leq j < N\) implies (as in the argument above for \(k = 1\)) that \(j = 0\).

Now suppose that for some \(n \geq 3\) there is a \(u\)-cycle \(v_1, \ldots, v_N\) for \(G(2, n)\) that covers \(G(1, n)\). We think of this as a graph with vertices \(v_i\) and edges corresponding to elements \(\langle v_i, v_{i+1} \rangle\) of \(G(2, n)\). Our first step is to “blow up the graph” by a factor
of \( q \) as follows: let \( T \) be the (undirected) graph with vertices \( \{ v_i + a\delta : a \in F, 1 \leq i \leq N \} \) with edges from \( v_i + a\delta \) to \( v_{i+1} + b\delta \) for all \( i \), and all \( a, b \in F \). The graph \( T \) has \( qN \) vertices, \( q^2 N \) edges, and each vertex has degree \( 2q \). Note that the edges of \( T \) correspond to regular subspaces of \( F^{n+1} \), letting the edge from \( v_i + a\delta \) to \( v_{i+1} + b\delta \) correspond to \( \langle v_i + a\delta, v_{i+1} + b\delta \rangle \). \( T \) is obviously connected and is hence Eulerian. This means that there is an Eulerian circuit, i.e., a cycle of vectors \( w_i \) in \( F^{n+1} \) such that \( \langle w_i, w_{i+1} \rangle \) exactly covers all regular 2-subspaces. Moreover, each 1-dimensional subspace, other than \( \langle \delta \rangle \), is represented by exactly one vertex.

The idea of the proof is to modify \( T \) to get a larger graph \( T^* \) that is also Eulerian, and whose edges correspond to all 2-subspaces in \( F^{n+1} \), and vertices correspond to all 1-dimensional subspaces. In order to do this we have to add a vertex \( \delta \), corresponding to the one missing 1-dimensional subspace, and add an edge corresponding to each special subspace.

By hypothesis, the 1-dimensional subspaces are of the form \( \langle v_i \rangle \) for a suitable set of \( i \); we refer to these as chosen vectors. Without loss of generality, we can assume that \( v_1 \) and \( v_2 \) are chosen.

If \( u \) is any vector in \( F^{n+1} \) (other than \( \delta \)) let \( [u] \) denote the vertex of \( T \) that generates the same 1-dimensional subspace (i.e., has \( au = [u] \) for a nonzero scalar \( a \)). If \( u \) and \( v \) are vertices let \( e(u, v) \) denote an edge between them.

Our first modification to \( T \) is to add a vertex \( \delta \), delete \( e(v_1, v_2 + \delta) \) and \( e(v_1 + \delta, v_2) \), and add edges \( e(v_1 + \delta, \delta) \), \( e(v_2 + \delta, \delta) \), \( e(v_1, [v_1 + v_2 + \delta]) \), and \( e(v_2, [v_1 + v_2 + \delta]) \). Fig. 1 depicts this graphically.

![Fig. 1. Adding \( \delta \).](image)

After some algebraic juggling, one easily checks that the deleted edges correspond to the same subspaces as the edges to \( [v_1 + v_2 + \delta] \), and that the two edges to \( \delta \) correspond to the special subspaces \( \langle v_1, \delta \rangle \) and \( \langle v_2, \delta \rangle \).

For each chosen vector \( v_i \) with \( i > 2 \) we make the following modification. Delete \( e(v_{i-1}, v_i + \delta) \) and \( e(v_{i-1} - \delta, v_i) \), and add three edges: \( e(v_i, v_i + \delta) \), \( e([v_i - v_{i-1} + \delta], v_i) \), and \( e([v_i - v_{i-1} + \delta], v_{i-1}) \). See Fig. 2.

![Fig. 2. Adding special subspaces.](image)

It is easy to check that the deleted edges correspond to the same subspaces as the edges to \( [v_i - v_{i-1} + \delta] \), and the other new edge corresponds to the special subspace \( \langle v_i, \delta \rangle \).

Let \( T^* \) denote the graph obtained by making these modifications to \( T \). It is obviously connected and all its vertices have even degree. Therefore \( T^* \) is Eulerian, and an Eulerian cycle gives a \( u \)-cycle for \( G(2, n+1) \) as desired. Moreover, by earlier remarks the cycle covers \( G(1, n+1) \). 

It is natural to conjecture that \( u \)-cycles exist for \( G(k, n) \) for \( k > n \), and to hope that an induction proof as above could be constructed, beginning at \( k = 2n + 1 \), asserting that \( u \)-cycles exist for \( G(k, n) \) that cover \( G(m, n) \) for all \( m < k \). For \( k = 3 \) the base of the induction would be a cycle for \( G(3, 5) \) that is also a cycle for \( G(2, 5) \) and also covers \( G(1, 5) \). We believe that such a cycle exists, but note that in that case the map from \( \{ v_i, v_{i+1} \} \) to \( \{ v_{i+1}, v_{i+2} \} \) gives a bijection from \( G(2, 5) \) to \( G(3, 5) \) that “preserves inclusion”. It is easy to prove that such a map exists, using Hall’s theorem, but hard to find an explicit one. With some work, we were able to construct a somewhat reasonable bijection of this form, but have, so far, not been able to use this to follow the pattern for \( k = 2 \) and construct \( u \)-cycles for \( k = 3 \). However, the number of degrees of freedom seems to be large, so that we are convinced that \( u \)-cycles exist for all \( k \).

References