SUBSPACE LATTICES OF FINITE VECTOR SPACES ARE 5-GENERATED

LÁSZLÓ ZÁDORI

To the memory of András Huhn

Abstract. Let $n \geq 3$. From the description of subdirectly irreducible complemented Arguesian lattices with four generators given by Herrmann, Ringel and Wille it follows that the subspace lattice of an n-dimensional vector space over a finite field is generated by four elements if and only if the field is a prime field. By exhibiting a 5-element generating set we prove that the subspace lattice of an n-dimensional vector space over an arbitrary finite field is generated by five elements.

1. Introduction

The subdirectly irreducible complemented Arguesian lattices with four generators were completely described by C. Herrmann, C. M. Ringel and R. Wille in [5]. From their result it follows that for $n \geq 3$ the subspace lattices of n-dimensional vector spaces over finite prime fields are generated by four elements. C. Herrmann's [3] has a description of the 4-generated subdirectly irreducible lattices in the variety generated by all complemented Arguesian lattices. These results stemmed from the work of Gelfand and Ponomarev [2] in which certain quadruples of subspaces of finite dimensional vector spaces are characterized. In [4] C. Herrmann, M. Kindermann and R. Wille give a complete list of subdirectly irreducible lattices generated by an ordered set of the form $1+2+2$ in the variety generated by all complemented Arguesian lattices. In fact, it turns out that these lattices are generated by four elements as well. In contrast with the 4-generated case, the 5-generated subdirectly irreducible complemented Arguesian lattices do not have a complete description.

1991 *Mathematics Subject Classification.* 06C05, 50D30, 14N20, 51D25.

Key words and phrases. Arguesian lattice, subspace lattice of a vector space, generating set of a subspace lattice.

The author's research is supported by OTKA grants T48809 and K60148.

In this paper we show that for $n \geq 3$ the subspace lattices of n-dimensional vector spaces over finite fields distinct from prime fields have generating sets with minimal cardinality five.

To prove that we need at least five elements to generate such lattices we quote a result from [5]: a subdirectly irreducible sublattice of a finite dimensional complemented modular lattice is generated by four elements if and only if it is isomorphic to M_4 or to $S(n,4)$ (first defined in [1]), or to the subspace lattice of an n-dimensional vector space over a prime field where $n \geq 3$, or to a non-Arguesian plane with four generators.

For each $n \geq 3$ the subspace lattice of an n-dimensional vector space over a finite field distinct from a prime field is simple (hence subdirectly irreducible), complemented, and modular. The height of the subspace lattice of a finite vector space of dimension at least two equals the dimension of the vectorspace, and the number of elements covered by an element of height two in the lattice coincides with the cardinality of the field plus 1. Moreover, the lattices $S(1,4)$ and $S(2,4)$ are isomorphic to D_2 and M_3, respectively, and for each $n \geq 3$, $S(n,4)$ is a lattice of height n which has an element of height two with a unique lower cover. Therefore by the above theorem any generating set of the subspace lattice of an n-dimensional finite vectorspace over a field distinct from a prime field consists of at least five subspaces, provided $n \geq 3$. Our aim is to show that five subspaces are sufficent to generate it.

2. Results

First we introduce some notation related to finite fields and subspace lattices. Let K be a finite field of order $|K| = q = p^m$ where p is a prime and m is a positive integer. We will denote by K^+ and K^* the additive and multiplicative groups of K, respectively. The subspace lattice of the n-dimensional vector space K^n will be denoted by $L(K^n)$. The subspace of K^n spanned by the vectors $c_i = (c_{i,1}, \dots, c_{i,n})$, $i = 1, \dots, l$, will be denoted by $[\sum_{i=1}^{l} c_{i,1}x_i, \dots, \sum_{i=1}^{l} c_{i,n}x_i]$. We require the following simple lemma.

Lemma 2.1. *For every finite field K and for every integer $n \geq 3$ the following subspaces generate the subspace lattice of K^n :*

$$s_{i,j}(a) = [0, \dots, 0, x, 0, \dots, 0, ax, 0, \dots, 0]$$

where x and ax appear in the i-th and j-th positions, respectively, $a \in K^*,\ 1 \leq i < j \leq n$, *and*

$$s_i = [0, \ldots, 0, x, 0, \ldots, 0]$$

where x appears in the i-th position, $1 \leq i \leq n$.

Proof. Let S denote the sublattice of $L(K^n)$ generated by the above subspaces. It suffices to show that every one dimensional subspace of K^n belongs to S. We proceed by induction. It is clear from the definition of S that S contains every one dimensional subspace of K^n with a spanning vector which has at most two nonzero components. Let $2 \leq k < n$ and let us suppose that every one dimensional subspace of K^n with a spanning vector which has at most k nonzero components belongs to S. Let us consider a one dimensional subspace s spanned by a vector with $k+1$ non-zero components. By symmetry we may assume that this vector has the form $(b_1, \ldots, b_{k+1}, 0, \ldots, 0)$ where $b_1, \ldots, b_{k+1}$ are distinct from 0. Let s' denote the subspace of K^n spanned by $(b_1, \ldots, b_k, 0, \ldots, 0)$. By the induction hypothesis $s' \in S$, hence

$$s = (s' \vee s_{k+1}) \wedge (s_1 \vee \cdots \vee s_{k-1} \vee s_{k,k+1}(b_{k+1}b_k^{-1})) \in S.$$

$\square$

For a simple, connected graph $G = (V, E)$, with $V = \{1, \ldots, n\}$ let

$H_G = \{s_i :\ 1 \leq i \leq n\} \cup \{s_{i,j}(a) :\ a \in K^*,\ 1 \leq i < j \leq n,\ (i,j) \in E\}$.

Lemma 2.1 can be strenghtened as follows.

Lemma 2.2. *For every simple, connected graph $G = (V, E)$ with $V = \{1, \ldots, n\}$ the elements of H_G generate $L(K^n)$.*

Proof. Let S be the sublattice of $L(K^n)$ generated by the elements of H_G. In view of Lemma 2.1 it suffices to show that every $s_{i,j}(a)$, $1 \leq i < j \leq n,\ a \in K^*$ belongs to S. The *distance* between two vertices i and j of G, denoted by $d(i,j)$, is the minimum length of the paths between i and j. We use induction on the distance between the vertices in G. Let $i, j \in V$. If $d(i,j) = 1$ then $s_{i,j}(a) \in H_G \subseteq S$. Suppose now that $d(i,j) = k+1$, $1 \leq k < n-1$, and S contains every subspace $s_{i',j'}(a)$ such that the distance $d(i',j')$ is at most k, $1 \leq i' < j' \leq n,\ a \in K^*$. Then there exists $l \in V$ such that $d(i,l) = k$ and $d(l,j) = 1$. The subspace $s_{i,l}(1)$ belongs to S by the induction hypothesis and $s_{l,j}(a), s_i, s_j, s_l \in H_G \subseteq S$. Hence

$$s_{i,j}(a) = (((s_i \vee s_{l,j}(a)) \wedge (s_{i,l}(1) \vee s_j)) \vee s_l) \wedge (s_i \vee s_j) \in S.$$

$\square$

Let $N[z]$ denote the set of polynomials in one variable z with non-negative integer coefficients. In the proof of our main result we shall use the following lemma on finite fields.

Lemma 2.3. *Let K be a finite field, and c a generating element of the cyclic group K^*. Then*

$$K = \{g(c^2) : \ g \in N[z]\}.$$

Proof. Let A denote the right hand side of the equality in the claim. Clearly, $(A, +)$ is a subgroup of K^+, hence $|K^+| = q = p^m$ is divisible by $|A|$. So $|A|$ is a power of p. Since $0, c^2, c^4, \ldots, c^{2[q/2]}$ are distinct elements of A, we have that $|A| \geq [q/2] + 1 > p^{m-1}$. Therefore $|A| = p^m = |K|$ which implies A=K. $\square$

Now we have all the necessary tools at our disposal to prove the main result of the paper.

Theorem 2.4. *For every finite field K and for every integer $n \geq 3$ the subspace lattice $L(K^n)$ of the n-dimensional vector space K^n is generated by five elements. According to whether n is odd or even the following five subspaces form a generating set of $L(K^n)$:*

for $n = 2k + 1, \ k \geq 1$,

$$\begin{aligned}
t_1 &= [0, \ldots, 0, x_{k+1}, \ldots, x_{2k+1}], \\
t_2 &= [x_1, \ldots, x_k, 0, \ldots, 0], \\
t_3 &= [x_1, \ldots, x_k, 0, x_1, \ldots, x_k], \\
t_4 &= [x_1, \ldots, x_k, cx_1, \ldots, cx_k, 0], \\
t_5 &= [cx_1, \ldots, cx_k, x_1, \ldots, x_k, 0];
\end{aligned}$$

for $n = 2k, \ k \geq 2$,

$$\begin{aligned}
t_1 &= [0, \ldots, 0, x_{k+1}, \ldots, x_{2k}], \\
t_2 &= [x_1, \ldots, x_k, 0, \ldots, 0], \\
t_3 &= [x_1, \ldots, x_k, x_1, \ldots, x_k], \\
t_4 &= [0, x_2, \ldots, x_k, cx_2, \ldots, cx_k, 0], \\
t_5 &= [0, cx_2, \ldots, cx_k, x_2, \ldots, x_k, 0];
\end{aligned}$$

where c is a generating element of the multiplicative group of K.

Proof. First we prove the claim for $n = 3$. Then by using induction, we step from $2k - 1$ to $2k$ and from $2k - 1, \ 2k$ to $2k + 1$ where $k \geq 2$. Through out the proof, we shall denote by S the sublattice of $L(K^n)$ generated by $\{t_i : \ 1 \leq i \leq 5\}$ where n will always be clear from the context.

First let $n = 3$ and let us consider the following elements of S:

$$
\begin{aligned}
t_6 &= (t_2 \vee t_4) \wedge t_1 &&= [0, x, 0],\\
t_7 &= (t_2 \vee t_3) \wedge t_1 &&= [0, 0, x],\\
t_8 &= (t_5 \vee t_7) \wedge (t_3 \vee t_6) &&= [cx, x, cx],\\
t_9 &= (t_2 \vee t_8) \wedge t_1 &&= [0, x, cx],\\
t_{10} &= (t_4 \vee t_7) \wedge (t_3 \vee t_6) &&= [x, cx, x],\\
t_{11} &= (t_{10} \vee t_2) \wedge t_1 &&= [0, cx, x].
\end{aligned}
$$

We show that $r_l = [x, 0, c^{2l}x]$ and $r'_l = [x, c^{2l+1}x, 0]$ belong to S for all non-negative integer l. We use induction on l. Obviously, $r_0 = t_3$ and $r'_0 = t_4$ belong to S. Let us assume that $r_l, r'_l \in S$. Then

$$w_l = (r'_l \vee t_7) \wedge (t_2 \vee t_9) = [x, c^{2l+1}x, c^{2l+2}x] \in S$$

and so

$$r_{l+1} = [x, 0, c^{2l+2}x] = (w_l \vee t_6) \wedge (t_2 \vee t_7) \in S.$$

Similarly,

$$w'_l = (r_{l+1} \vee t_6) \wedge (t_2 \vee t_{11}) = [x, c^{2l+3}x, c^{2l+2}x] \in S$$

and so

$$r'_{l+1} = [x, c^{2l+3}x, 0] = (w'_l \vee t_7) \wedge (t_2 \vee t_6) \in S.$$

Then

$$s_l = (r'_l \vee t_7) \wedge (t_3 \vee t_6) = [x, c^{2l+1}x, x] \in S$$

and so

$$\hat{r}_l = (s_l \vee t_2) \wedge t_1 = [0, c^{2l+1}x, x] \in S$$

for all non-negative integers l.

We now show that for every polynomial $g \in N[z]$

$$u(g) = [x, cg(c^2)x, 0] \text{ and } \hat{u}(g) = [0, cg(c^2)x, x]$$

belong to S. We proceed by induction on the sum of the coefficients of g. Clearly, for $g = 0$, $u(g) = t_2 \in S$ and $\hat{u}(g) = t_7 \in S$. Let us assume that $g \neq 0$ and $g(z) = g'(z) + z^l$ where $g' \in N[z]$ and l is a non-negative integer. Then we have that

$$t(g) = (\hat{r}_l \vee u(g')) \wedge (t_3 \vee t_6) = [x, cg(c^2)x, x] \in S,$$

hence

$$u(g) = (t(g) \vee t_7) \wedge (t_2 \vee t_6) \in S \text{ and } \hat{u}(g) = (t(g) \vee t_2) \wedge t_1 \in S.$$

Lemma 2.3 implies now that all subspaces of the form $[x, ax, 0]$ and $[0, x, ax]$, $a \in K$, are in S. Since t_2, t_6 and t_7 belong to S, an application of Lemma 2.2 yields the statement of the theorem for $n = 3$.

Let us suppose now that $n = 2k$, $k \geq 2$ and consider the following elements in S:

$$\begin{aligned} t_6 = & \quad (t_1 \vee t_4) \wedge t_2 = & [0, x_2, \ldots, x_k, 0, \ldots, 0], \\ t_7 = & \quad (t_1 \vee t_4) \wedge t_3 = & [0, x_2, \ldots, x_k, 0, x_2, \ldots, x_k]. \end{aligned}$$

Observe that $t_1,\ t_6,\ t_7,\ t_4,\ t_5$ are exatly the five subspaces claimed to generate the subspace lattice of the $(2k-1)$-dimensional space $[0, x_1, \ldots, x_{2k-1}]$. So applying the induction hypothesis we get that every one dimensional subspace of K^n spanned by a vector whose first component is 0 belongs to S.

The vector space automorphism

$$\varphi : K^n \to K^n,\ (a_1, \ldots, a_{2k}) \mapsto (a_{2k}, \ldots, a_1)$$

maps each of the subspaces $t_i,\ i = 1, \ldots, 5$, into some $t_j,\ j = 1, \ldots, 5$, and the subpace $[0, x_1, \ldots, x_{2k-1}]$ into the subspace $[x_1, \ldots, x_{2k-1}, 0]$. Let $\varphi^* : L(K^n) \to L(K^n)$ be the lattice automorphism induced by φ in the natural way. Since φ^* permutes the $t_i,\ i = 1, \ldots, 5$, and $t_1,\ t_6,\ t_7,\ t_4,\ t_5$ are in S, the subspaces

$$\varphi^*(t_1),\ \varphi^*(t_6),\ \varphi^*(t_7),\ \varphi^*(t_4),\ \varphi^*(t_5)$$

are in S, as well. By applying the observation in the preceding paragraph and using the fact that a suitable restriction of φ^* is a lattice isomorphism between the subpace lattices of $[0, x_1, \ldots, x_{2k-1}]$ and $[x_1, \ldots, x_{2k-1}, 0]$ we get that

$$\varphi^*(t_1),\ \varphi^*(t_6),\ \varphi^*(t_7),\ \varphi^*(t_4),\ \varphi^*(t_5)$$

generate the subspace lattice of $[x_1, \ldots, x_{2k-1}, 0]$. Therefore it follows that every one dimensional subspace of K^n spanned by a vector whose last component is 0 belongs to S. Thus, by Lemma 2.2 the statement of the theorem holds for $n = 2k$.

Finally, let us suppose that $n = 2k+1$, $k \geq 2$ and consider the following elements of S:

$$\begin{aligned}
t_6 = &\quad (t_2 \vee t_3) \wedge t_1 = &\quad [0,\dots,0,x_{k+2},\dots,x_{2k+1}],\\
t_7 = &\quad (t_2 \vee t_3) \wedge t_4 = &\quad [0,x_2,\dots,x_k,0,cx_2,\dots,cx_k,0],\\
t_8 = &\quad (t_2 \vee t_3) \wedge t_5 = &\quad [0,cx_2,\dots,cx_k,0,x_2,\dots,x_k,0],\\
t_9 = &\quad (t_2 \vee t_4) \wedge t_1 = &\quad [0,\dots,0,x_{k+1},\dots,x_{2k},0],\\
t_{10} = &\quad (t_2 \vee t_4) \wedge t_3 = &\quad [x_1,\dots,x_{k-1},0,0,x_1,\dots,x_{k-1},0],\\
t_{11} = &\quad (t_9 \vee t_{10}) \wedge t_4 = &\quad [x_1,\dots,x_{k-1},0,cx_1,\dots,cx_{k-1},0,0],\\
t_{12} = &\quad (t_9 \vee t_{10}) \wedge t_5 = &\quad [cx_1,\dots,cx_{k-1},0,x_1,\dots,x_{k-1},0,0],\\
t_{13} = &\quad (t_9 \vee t_{10}) \wedge t_2 = &\quad [x_1,\dots,x_{k-1},0,\dots,0].
\end{aligned}$$

Clearly, $t_6,\ t_2,\ t_3,\ t_7,\ t_8$ are exactly the five subspaces claimed to generate the subspace lattice of the $2k$-dimensional space

$$[x_1,\dots,x_k,0,x_{k+2},\dots,x_{2k+1}].$$

Furthermore, $t_9,\ t_{13},\ t_{10},\ t_{11},\ t_{12}$ are exactly the five subspaces claimed to generate the subspace lattice of the $(2k-1)$-dimensional space

$$[x_1,\dots,x_{k-1},0,x_{k+1},\dots,x_{2k},0].$$

Therefore, by the induction hypothesis we get that S contains every one dimensional subspace of K^n spanned by a vector in which either the $(k+1)$-st component is 0 or both of the k-th and $(2k+1)$-st components are 0. Thus, an application of Lemma 2.2 concludes the proof. $\square$

References

[1] A. Day, C. Herrman and R. Wille, On modular lattices with four generators, Algebra Universalis 2 (1972), 317-323

[2] I.M. Gelfand and V.A. Ponomarev, Problems of linear algebra and classification of quadruples of subspaces in a finite dimensional vector space, Coll. Math. Soc. J. Bolyai, vol. 5, Hilbert Space Operators, Tihany, 1970.

[3] C. Herrmann, On the equational theory of submodule lattices, Proc. Univ. Of Houston Lattice Theory Conference, (1973) , 105-118.

[4] C. Herrmann, M. Kindermann, and R. Wille, On modular lattices generated by 1+2+2, Algebra Universalis 5 (1975), 243-251.

[5] C. Herrmann, C.M. Ringel, and R. Wille, On modular lattices with four generators, Notices Amer. Math Soc. 20 (1973), A-418.

Bolyai Intézet, Aradi vértanúk tere 1, H-6720, Szeged, Hungary

E-mail address: zadori@math.u-szeged.hu