Preprint 96 – 032

Shadows in Linear Lattices

by

Peter Weidl

Mitgeteilt von W. Deuber
29.4.1996

Sonderforschungsbereich “Diskrete Strukturen in der Mathematik”
Universität Bielefeld
POB 10 01 31
33501 Bielefeld
Germany
Telefon: (0521) 106–4970
Telex: 932 362 unibi
Telefax: 106–4743
Electronic mail: sfbmath@mathematik.uni-bielefeld.de

ISSN: 0936–7926

Typeset in TEX

1. Introduction

One of the famous results in the combinatorics of finite sets is the Kruskal-Katona Theorem ([10], [11]). Kruskal and Katona investigated the following problem:

Let $\binom{S}{k}$ denote the set of k-element subsets of a finite set S. For a given $m \in \mathbb{N}$ one asks which m-element families $\mathcal{A} \subseteq \binom{S}{k}$ have the property that the *shadow of* $\mathcal{A}$ has minimal cardinality, where the shadow $\Delta\mathcal{A}$ is defined as

$$\triangle\mathcal{A} = \{B \in \binom{S}{k-1} \ : \ B \subset A \text{ for some } A \in \mathcal{A}\}.$$

Kruskal and Katona defined a total order on $\binom{S}{k}$ such that the m smallest elements with respect to this order minimize the cardinality of the shadow. It is quite common to call this order the *squashed order* (see [1], other notions can be found in [2]) and for completeness sake its definition is given as follows:

$$A <_s B \Leftrightarrow \max((A \cap (S \setminus B)) \cup ((S \setminus A) \cap B)) \in B \ \text{ for } A, B \in \binom{S}{k}.$$

Before stating the theorem, we would like to mention that there exists a well-known relationship between the squashed order and the so-called "k-binomial representation" of m (see, e.g. [1]).

Theorem A ([10], [11]) *Let* $\mathcal{A} = \{A_1, \ldots, A_m\} \subseteq \binom{S}{k}$*, and suppose that the* k*-binomial representation of* m *is*

$$m = \binom{a_k}{k} + \binom{a_{k-1}}{k-1} + \ldots + \binom{a_t}{t}$$

where $a_k > a_{k-1} > \ldots > a_t \geq t \geq 1$*. Then*

$$| \triangle \mathcal{A}| \geq \binom{a_k}{k-1} + \binom{a_{k-1}}{k-2} + \ldots + \binom{a_t}{t-1}.$$

Several proofs for Theorem A are known. The original proofs of Kruskal and Katona are quite complicated but a number of authors have since given

shorter proofs (see e.g. [5], [7], [9]).
The basic problem in all proofs seems to be the analysis of the relation of $\mathcal{A} \subseteq \binom{S}{k}$ to its *compression* $C\mathcal{A}$ (these are the $|\mathcal{A}|$ smallest elements of the squashed order) with respect to their shadows. One important method for this analysis is a shifting process which operates on the set $\mathcal{A}$.
As an example we take a brief look at Daykin's proof [5] of the Kruskal-Katona Theorem. If $\mathcal{A}$ and $C\mathcal{A}$ do not coincide then we can replace some specific set N in each $X \in \mathcal{A}$ in which it occurs as a subset by another set M satisfying $M \cap X = \emptyset$, $M <_s N$, $M \cap N = \emptyset$, $|M| = |N|$ and moreover $(X \backslash N) \cup M \notin \mathcal{A}$ and $(X \backslash N) \cup M <_s X$. Daykin requires some additional properties for N and M. For the idea of the proof it is enough to observe that the new set $\mathcal{A}^*$ with $|\mathcal{A}| = |\mathcal{A}^*|$ obtained by the replacements has at most the cardinality of the shadow of $\mathcal{A}$ and is "closer" to the compression of $\mathcal{A}$. That means that repetitions of this process finally transform $\mathcal{A}$ into $C\mathcal{A}$.

A careful analysis of the squashed order leads to an explicit formula for the minimal cardinality of the shadow. Frankl [7] used this formula together with another shifting process in order to give a short proof of Theorem A.

A natural generalization of the Kruskal-Katona Theorem refers to the shadow of *multisets*, where a multiset, denoted by $S(k_1, \ldots, k_n)$, consists of all n-tuples or vectors $x = (x_1, \ldots, x_n)$ such that each x_i is an integer satisfying $0 \leq x_i \leq k_i$. Since each k-element subset of S can be represented by a $0,1$-vector of length $|S|$ (using the characteristic function), we see that $\binom{S}{k}$ is representable by a multiset with $n = |S|$ and $k_1 = \ldots = k_n = 1$ and the additional property that for each $x \in S(1, \ldots, 1)$ the *rank* $|x|$ of x, defined by $|x| = x_1 + \ldots + x_n$, is k. If $\mathcal{A} \subseteq S(k_1, \ldots, k_n)$ with $|\mathcal{A}| = m$ and each $x \in \mathcal{A}$ has rank k, then the *shadow of* $\mathcal{A}$ in the multiset sense is given by
$\Delta\mathcal{A} = \{x = (x_1, \ldots, x_n) : |x| = k-1; (x_1, \ldots, x_{i-1}, x_i + 1, x_{i+1}, \ldots, x_n) \in \mathcal{A}$ for some $i \leq n\}$.
Again a total order on the vectors of a multiset of rank k (a natural generalization of the squashed order) may be defined with the property that the first m elements according to this order minimize the cardinality of the shadow. The theorem establishing this fact is usually called the generalized Macauley Theorem (see e.g. [1] , pp. 145-151) and was proved by Clements and Lindström [4] under the condition that $k_1 \leq k_2 \leq \ldots \leq k_n$.

The q-analog of Theorem A is a well-known problem for *linear lattices*. One refers to a linear lattice $L_n(q)$ as the poset of all subspaces of a n-dimensional vector space over a finite field $F = GF(q)$ of q elements, ordered by inclusion. Instead of using a set of k-element subsets of S, one uses a family of k-dimensional subspaces in a fixed n-dimensional vector space F^n. The *shadow-elements* in linear lattices are $(k-1)$-dimensional spaces and each of them is a subspace of at least one of the k-dimensional spaces in the family.

In this paper we investigate the Kruskal-Katona type problem for linear lattices. First (section 2) we show that there is a dual problem to the minimization problem, namely the maximization of the cardinality of the "reverse shadow" which will be defined later. We prove that the minimization problem and the maximization problem are equisolvable.
In section 3 we relax the problem by asking for which subset S of $(GF(q))^n$ of vectors of given cardinality do we get the maximal number of m-dimensional subspaces that are subsets of S. An upper bound for this maximal number will be given. This turns out to be exact for $|S| = q^k$ with $k \leq n, k \in \mathbb{N}$.

In section 4 we restrict our attention to $L_n(2)$. Our main result states that for all $s \in \mathbb{N}$ with $s \leq 2^n$ and for all $S \subseteq (GF(2))^n$ satisfying $|S| = s$, the maximal number of 2-dimensional spaces in S is achieved by using a set S^s_{lex} consisting of the s smallest elements in the lexicographic order on the vectors of $(GF(2))^n$ with its canonical basis. With the help of the dual problem we finally obtain a partial Kruskal-Katona type result for 2-dimensional vector spaces over $GF(2)$ with their 1-dimensional shadow-elements.

Remark: S.L. Bezrukov [12] informed me that since 1991 (unpublished) he knew how to prove the minimization problem for a family of k-dimensional vector spaces and their 1-dimensional subspaces - each 1-dimensional subspace is included in at least one member of the family - in $L_n(2)$, where $2 \leq k \leq n$.

2. Duality of the problems "Minimizing the shadow" and "Maximizing the reverse shadow"

Let $F^n (n \in \mathbb{N})$ denote the n-dimensional vector space over the finite field F. The set of all m-dimensional subspaces of F^n where the field F has q elements is denoted by $[n,m]_q$. We define the meaning of shadow in the context of linear lattices.

Definition 1 *Let $M \subseteq [n,k]_q$ ($k \in \mathbb{N}$, $k \leq n$).*
The shadow of M is defined by

$$\Delta M = \{U \in [n,k-1]_q \ : \ \textit{there exists a } V \in M \textit{ such that } U \subseteq V\}.$$

Our first aim is to give a notion that leads us to a problem that is dual to the problem of minimizing the cardinality of the shadow.

Definition 2 *Let $N \subseteq [n, k-1]_q$ ($k-1 \in \mathbb{N}$, $k-1 \leq n-1$).*
The reverse shadow of N is defined by

$$\nabla N = \{W \in [n,k]_q \ : \ \Delta\{W\} \subseteq N\}.$$

The crucial point for approaching the Kruskal-Katona type problem in linear lattices is to find an appropriate definition of a total order on $[n,k]_q$. In Theorem A the squashed order on $\binom{S}{k}$ is used where in the generalized Macauley Theorem a generalization of this order is helpful for multisets of rank k.
Let $\binom{n}{m}_q$ denote the Gaussian coefficient that stands for the number of elements in $[n,m]_q$. For abbriviation, we say that a total order on $[n,k]_q$ minimizes the shadow if for all $s \leq \binom{n}{k}_q$ the s smallest elements with respect to this order have the minimal cardinality of the shadow for all s-element sets in $[n,k]_q$. If we replace "shadow" by "reverse shadow" and "minimal" by "maximal" then we talk about a total order that maximizes the reverse shadow.
Let s be given. If $<$ denotes such a minimizing or maximizing total order then $M^s_<$ or $N^s_<$ respectively denotes the set of the s smallest elements according to $<$.

The following Lemma says that the problems of finding an order that maximizes the reverse shadow or an order that minimizes the shadow are equivalent.

Lemma 1 *The following statements are equivalent:*

1. *There exists a total order, denoted by $<_\Delta$, on $[n,k]_q$ such that for all $s \in \mathbb{N}$ where $s \leq \binom{n}{k}_q$ and for all $M \subseteq [n,k]_q$ with $|M| = s$ it holds*

$$|\Delta M| \geq |\Delta M^s_{<_\Delta}|.$$

2. *There exists a total order, denoted by $<^\nabla$, on $[n,k-1]_q$ such that for all $s \in \mathbb{N}$ where $s \leq \binom{n}{k-1}_q$ and for all $N \subseteq [n,k-1]_q$ with $|N| = s$ it holds*

$$|\nabla N| \leq |\nabla N^s_{<^\nabla}|.$$

Proof:
We assume that 1. holds. The total order $<_\Delta$ on $[n,k]_q$ can be used to induce a total order on $[n,k-1]_q$. The meaning of "induced" will be explained now. We start with the smallest element $A_1 \in [n,k]_q$, where $[n,k]_q$ is ordered by $<_\Delta$. Then we choose a total order for the elements in $\Delta\{A_1\}$. Next we say what to do if the shadow of the set $\mathcal{A}_t = \{A_1,\dots,A_t\} \subseteq [n,k]_q$ of the t smallest elements for $<_\Delta$ where $t \geq 1$ is totally ordered and we add $A_{t+1} \in [n,k]_q \setminus \mathcal{A}_t$ which comes next with respect to $<_\Delta$. In this case we only have to take care of the elements in $\Delta\{A_{t+1}\} \setminus \Delta\{A_1,\dots,A_t\} = A$. If $A = \emptyset$ we do nothing. Else we choose a total order for the elements in A and extend the total order which is already constructed by defining that all elements in A are greater than the elements in $\Delta\{A_1,\dots,A_t\}$. After finitely many steps we have a total order, denoted by $<^*$, on $[n,k-1]_q$.
We have to show that $<^*$ has the maximizing property of statement 2.
We assume, for a contradiction, that there exists a set $N \in [n,k]_q$ and $s \leq \binom{n}{k-1}_q$ such that $|\bigtriangledown N| > |\bigtriangledown N^s_{<^*}|$ with $|N| = s$. Because of the construction of $<^*$ there exists a set $M^x_{<_\Delta}$ with $M^x_{<_\Delta} = \bigtriangledown N^s_{<^*}$. Observe that $M^x_{<_\Delta}$ is maximal in such a way that if you add an element to $M^x_{<_\Delta}$ then $|\Delta M^x_{<_\Delta}| < |\Delta M^{x+1}_{<_\Delta}|$. Now $|\bigtriangledown N| > |M^x_{<_\Delta}|$ and since $\Delta(\bigtriangledown N) \subseteq N$ (by the definition of the reverse shadow) we know that $|\Delta(\bigtriangledown N)| \leq |N| = s$.
But if we take $M^y_{<_\Delta}$ with $y > x$ and $y = |\bigtriangledown N|$ we get $|\Delta M^y_{<_\Delta}| > s$ ($M^x_{<_\Delta}$ is maximal). That is a contradiction to the minimizing property of $<_\Delta$ because $|\Delta(\bigtriangledown N)| < |\Delta M^y_{<_\Delta}|$.

We assume that 2. holds. Analogously we can induce a total order, denoted this time by $<_*$, on $[n,k]_q$ in the following way. We take the smallest $\binom{k}{k-1}_q$ elements with respect to $<^\bigtriangledown$ in order to produce the smallest element in the induced order $<_*$. Let $\mathcal{B}_r = \{B_1,\dots,B_r\} \subseteq [n,k-1]_q$ be the set of the r smallest elements according to $<^\bigtriangledown$ with $r \geq \binom{k}{k-1}_q$. Assume that $\mathcal{B}_r$ has been used in order to build up a total order in $\bigtriangledown\mathcal{B}_r$. We have to describe what happens for $B_{r+1} \in [n,k-1]_q \setminus \mathcal{B}_r$ which comes next in the order $<^\bigtriangledown$. Let $B = \bigtriangledown\{B_1,\dots,B_{r+1}\} \setminus \bigtriangledown\mathcal{B}_r$. If $B = \emptyset$ then we do nothing. Else we simply extend the order that we have constructed so far by the elements of B which can be totally ordered in an arbitrary way. Clearly each element of B is defined to be greater than the elements in $\bigtriangledown\{B_1,\dots,B_r\}$. We go on like this until all elements in $[n,k]_q$ are totally ordered.

Next we show that $<_*$ satisfies 1.
We assume, for a contradiction, that there exists a set $M \in [n,k]_q$ and $s \leq \binom{n}{k}_q$ with $|M| = s$ and $|\Delta M| < |\Delta M^s_{<_*}|$. Because of the construction of

$<_*$ there exists a set $N^a_{<\triangledown}$ with $N^a_{<\triangledown} = \Delta M^s_{<_*}$ and $N^a_{<\triangledown}$ is minimal in the sense that if you take away an element from $N^a_{<\triangledown}$ then $| \triangledown N^{a-1}_{<\triangledown}| < | \triangledown N^a_{<\triangledown}|$. It follows that $|N^a_{<\triangledown}| > |\Delta M|$. And since $M \subseteq \triangledown(\Delta M)$ we have $s = |M| \leq | \triangledown (\Delta M)|$. Take a look at $N^b_{<\triangledown}$ with $b < a$ and $b = |\Delta M|$. Finally we get $| \triangledown N^b_{<\triangledown}| < s$ ($N^a_{<\triangledown}$ is minimal) and the contradiction to the maximazing property of $<^\triangledown$ is caused by: $| \triangledown (\Delta M)| \geq s > | \triangledown N^b_{<\triangledown}|$. •

With the help of this result we are able to formulate a problem which is still closely related to our original problem of "minimizing the cardinality of the shadow".

3. Relaxation of the problem

The main question for section 3 and 4 is how to choose a set of vectors $S \subseteq F^n$ with $|S| = s$, where $s \in \mathbb{N}$ is given, such that the number of m-dimensional subspaces of F^n, where each subspace is included in S as a subset, is maximal. Again we are interested in finding a total order, this time on the vectors of F^n, such that the first s elements with respect to this order maximize the number of the "included" subspaces. We use the following definition.

Definition 3 *Let $S \subseteq F^n$ and $m \in \mathbb{N}$ with $m \leq n$.*
The m-th product of S is defined by

$$P_m(S) = \{U \subseteq S \ : \ U \in [n,m]_q\}.$$

In the following we will also say that a subset $B \subseteq S$ *produces* a subspace $U \in [n,m]_q$ if the set of vectors in U is equal to B.
It is possible to give an upper bound for $|P_m(S)|$ that only depends on $|S| = s$. Also we can see that this bound is reached in the case where the set S is a k-dimensional subspace of F^n with $n \geq k \geq m$ (if $k < m$ then $|P_m(S)| = 0$).

Lemma 2 *Let $S \subseteq F^n$ with $|S| = s$.*
Then

$$|P_m(S)| \leq \left\lfloor \frac{(s-1)(s-q)(s-q^2)\cdots(s-q^{m-1})}{(q^m-1)(q^m-q)(q^m-q^2)\cdots(q^m-q^{m-1})} \right\rfloor .$$

Proof:
Remark: It should be mentioned that if $s = q^k$ for a $k \geq m$ the bound becomes the Gaussian coefficient $\binom{k}{m}_q$.
At first we count how many ordered bases of a m-dimensional space there

are at most in S. Therefore we have to make sure that if we have a basis that the space spanned by this basis belongs to S. Otherwise this basis would not increase the value of $|P_m(S)|$. We can assume that the vector 0 belongs to S (if not then $|P_m(S)| = 0$ and there is nothing to show). Hence there are $s-1$ vectors that we can choose for a basis. If we want to have a 2-dimensional space in S then the whole line spanned by the first chosen vector has to be in S. So there are at most $s-q$ possible choices for the second vector. For the third vector in a basis of a m-dimensional space we have to guarantee that the plane spanned by the first two vectors of the basis is a subset of S. Therefore there are $s-q^2$ possible choices for this vector. If we go on arguing like this we obtain all possible ordered bases in S that may span a m-dimensional space in S, i.e. at most $(s-1)(s-q)(s-q^2)\cdots(s-q^{m-1})$ many. Now each basis occurs $(q^m-1)(q^m-q)(q^m-q^2)\cdots(q^m-q^{m-1})$ times. This can be seen with the help of the same argumentation for $s = q^m$. Now we get the claim (the bound should be a natural number, so we use Gaussian brackets; that means that $\lfloor a \rfloor$ stands for the largest integer smaller or equal to $a \in \mathbb{R}$). •

If we look at the more complicated question about the cardinality of the reverse shadow of a set of $(k-1)$-dimensional subspaces of F^n, we obtain the following relation between the reverse shadow and the m-th product of S.

Proposition 1. *Let $N = \{A_1, A_2, \ldots, A_r\}$ be a set of $(k-1)$-dimensional subspaces in F^n.*
Then

$$|\bigtriangledown N| \leq |P_k(\bigcup_{i=1}^{r} A_i)|.$$

Proof:
Let $B \in \bigtriangledown N$, and B consists of a set of vectors that belong to the elements of N. Of course these vectors also belong to $\bigcup_{i=1}^{r} A_i$ and therefore $B \in P_k(\bigcup_{i=1}^{r} A_i)$ by the definition of P_k. Since B is an arbitrary element of $\bigtriangledown N$ we get $\bigtriangledown N \subseteq P_k(\bigcup_{i=1}^{r} A_i)$. Now the claim follows.

Obviously this bound for $|\bigtriangledown N|$ isn't helpful if e.g. the union of the elements of N is F^n but the cardinality of the reverse-shadow of N is quite small (it could be 0).

As a consequence of Lemma 2 we know that a possible candidate for a "maximizing" total order on F^n can have the property that for $s = q^k$ $(1 \leq k \leq n)$ the s smallest elements with respect to this order produce a k-dimensional subspace of F^n.

4. A partial Kruskal-Katona type result

From now on we will restrict our attention to the field $GF(2)$ and we prove for the lexicographic order on the vectors of $(GF(2))^n$ that the s smallest elements according to this order maximize the value $|P_2(S)|$ for all $S \subseteq GF(2)^n$ where $|S| = s$ is given. Instead of $(GF(2))^n$ we will also write $GF(2)^n$. Since the 1-dimensional spaces of $GF(2)^n$ consist of 2 vectors where one is the 0-vector, we immediately receive a result for the reverse shadow case from dimension 1 to dimension 2. With the help of Lemma 1 we finally obtain a partial Kruskal-Katona type result for this special case.
For completeness, we define the lexicographic order on $GF(2)^n$ with respect to the canonical basis of $GF(2)^n$, indicated by $<_{lex}$, which is of course a total order.

Definition 4 *Let $u = (u_1, u_2, \ldots, u_n)$, $v = (v_1, v_2, \ldots, v_n) \in GF(2)^n$.*
Then $u <_{lex} v$ if and only if either there exists an $i \in \{1, \ldots, n\}$ such that $u_j = v_j$ for all $j < i$ and $u_i = 0, v_i = 1$ or $u = v$.

Before we state the theorem we would like to mention one of the main problems to answer the Kruskal-Katona question for linear lattices or the related question for $|P_m(S)|$ at the beginning of section 3. Following the main idea of Daykin's proof mentioned in the introduction we can try to use "replacements" also for k-dimensional spaces. Obviously the problem here is to preserve the structure of a vector space when exchanging one subset in one subspace of F^n by another subset. Similar problems arise for other shifting techniques which operate on $\mathcal{A} \subseteq \binom{S}{k}$ if one wants to use them in order to prove analogous results in linear lattices.
We will tell the main ideas of the proof of the following theorem within its proof.

Theorem 1 *Suppose that $s \in \mathbb{N}$ is given by $s = 2^{i-1} + a$ where $0 \leq a < 2^{i-1}$ and $i \leq n+1$. Let S^s_{lex} denote the set of the s smallest elements in $GF(2)^n$ with respect to $<_{lex}$.*
Then for all $S \subseteq GF(2)^n$ with $|S| = s$ it holds:

$$|P_2(S)| \leq |P_2(S^s_{lex})| = \binom{i-1}{2}_2 + \binom{a}{2}.$$

Proof: Let $s \in \mathbb{N}$ be given as supposed in Theorem 1. And let S be an arbitrary but fixed subset of $GF(2)^n$ with $|S| = s$. We will list all vectors of $GF(2)^n \setminus \{0\}$ with respect to $<_{lex}$ and partition $GF(2)^n \setminus \{0\}$ into blocks B_j of length 2^{j-1}, starting from the left with $j = 1$. We will also use block B_0 which consists of the vector 0. The following figure illustrates the situation for $n = 4$.

$$\begin{array}{c|c|cc|cccc|cccccccc}
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
\underbrace{\quad}_{B_0}&\underbrace{\quad}_{B_1}&\multicolumn{2}{c|}{\underbrace{\qquad}_{B_2}}&\multicolumn{4}{c|}{\underbrace{\qquad\qquad}_{B_3}}&\multicolumn{8}{c}{\underbrace{\qquad\qquad\qquad\qquad}_{B_4}}
\end{array}$$

The following observations will be helpful:

1. If $v_i, v_j \in B_l$ with $v_i + v_j \in B_m$ then $m < l$. Another fact is that each 2-dimensional space in $GF(2)^n$ has to include exactly 2 vectors of one block. As a consequence we have:

$$\binom{n}{2}_2 = \sum_{k=1}^{n-1} \binom{2^k}{2}.$$

2. Since $s = 2^{i-1} + a$ with $0 \leq a < 2^{i-1}$ and $\sum_{j=0}^{i-1} |B_j| = 2^{i-1}$ it follows that exactly a elements of S^s_{lex} are in block B_i.

Observation 1. and 2. also imply that

$$|P_2(S^s_{lex})| = \binom{i-1}{2}_2 + \binom{a}{2}.$$

We will prove Theorem 1 by an induction on s and in this induction by another induction on the number of blocks h. In order to be able to refer the set S to the blocks we write the elements of S lexicographically ordered. Then we get a set $B \subseteq S$ with $|B| = b \geq 1$ and an index $h \geq i$ such that $S^* = S \setminus B$ satisfies $S^* \subseteq \bigcup_{j=0}^{h-1} B_j$ and $B \subseteq B_h$.
Remark: If $a = 0$ then $h = i - 1$ is possible but in this case $S = S^s_{lex}$ and there is nothing to show.

1. Induction on s:
The statement of Theorem 1 is clearly true for $s = 1$ since $|P_2(S)| = 0 = |P_2(S^1_{lex})|$.

Now assume that the statement $|P_2(S)| \leq |P_2(S^s_{lex})|$ holds for all $s < 2^{i-1}+a$ and for all $S \subseteq GF(2)^n$ with $|S| = s$. In the following we will indicate the use of the assumption of the induction by the sign $(\star)$.
Let $W = S^s_{lex} \cap B_i$ with $|W| = a$.

Case 1: Suppose that $b \leq a$.
Remove one vector x from B and one vector y from W. Because of $(\star)$ we get:

$$|P_2(S \setminus \{x\})| \leq |P_2(S^s_{lex} \setminus \{y\})|.$$

Since x can only be combined with vectors from B in order to produce new 2-dimensional spaces we can add at most $b-1$ to $|P_2(S\setminus\{x\})|$ (see observation 1) by adding x to $S\setminus\{x\}$. If we add y to $S^s_{lex}\setminus\{y\}$ we will increase $|P_2(S^s_{lex}\setminus\{y\})|$ by exactly $a-1$. So if $b \leq a$ we get

$$|P_2(S)| \leq |P_2(S^s_{lex})|.$$

From now on we assume that $b > a$.

Case 2: Suppose that $b \leq 2^{i-2}$.
Let $M = U \cup W$ denote the set of the b largest elements in S^s_{lex}. With the help of $(\star)$ we have:

$$|P_2(S \setminus B)| \leq |P_2(S^s_{lex} \setminus M)|.$$

Since $b \leq 2^{i-2}$ and $|B_{i-1}| = 2^{i-2}$ it follows that $U \subseteq B_{i-1}$. Now we count the 2-dimensional spaces which are produced by adding M to $S^s_{lex} \setminus M$. We receive

$$\binom{2^{i-2}}{2} - \binom{2^{i-2}-(b-a)}{2} + \binom{a}{2}$$

spaces by using observation 1 for the counting. If we add B to $S \setminus B$ we can get at most $\binom{b}{2}$ spaces. It remains to be shown that

$$\binom{2^{i-2}}{2} - \binom{2^{i-2}-(b-a)}{2} + \binom{a}{2} \geq \binom{b}{2}.$$

A little calculation transfers this inequality into

$$(2^{i-1}-2b)(b-a) \geq 0$$

which is correct because $b > a$ and $b \leq 2^{i-2}$.

After having handled the cases 1 and 2 we have to show the induction step for S with $b > \max\{a, 2^{i-2}\}$. In this situation we start the second induction on the number of blocks h, where h is the minimal index such that $S \subseteq \bigcup_{j=0}^{h} B_j$.

Induction on h:
It is clear that we have to start the induction with $h = i$, i.e. the sets W and B are both included in block B_i. Now let $b = 2^{i-2} + c$ with $c > 0$ and $b > a$ and let $X = \bigcup_{j=0}^{i-1} B_j \setminus S$ with $|X| = b - a$. We need the following proposition:

Proposition 2 *$|P_2(B \cup X \cup \{0\})| \geq c(b-a)$ where $c = b - 2^{i-2}$ and $c > 0$.*

Proof: Each 2-dimensional space in $P_2(B_i \cup X \cup \{0\}) \setminus P_2(X \cup \{0\})$ includes vector 0, exactly one element from X and exactly two elements from B_i (see observation 1). Let $x \in X$.($X \neq \emptyset$ because $b > a$.)
Then $|P_2(\{x\} \cup B_i \cup \{0\})| = 2^{i-2}$. Since $b = 2^{i-2} + c$ with $c > 0$ it follows with the pigeon hole principle that there exist at least c 2-dimensional spaces that include vector x. Because all elements in X are pairwise distinct and each element in X is part of at least c 2-dimensional spaces we obtain at least $c(b-a)$ 2-dimensional spaces in $P_2(B \cup X \cup \{0\})$. •

Like at the beginning of case 2 with the help of ($\star$) and the same notation we receive

$$|P_2(S \setminus B)| \leq |P_2(S^s_{lex} \setminus M)|.$$

But now Proposition 2 guarantees us that if we add B to $S \setminus B$ then we get at most $\binom{b}{2} - c(b-a)$ new spaces. So this time we prove the correctness of the inequality

$$\binom{2^{i-2}}{2} - \binom{2^{i-2} - (b-a)}{2} + \binom{a}{2} \geq \binom{b}{2} - c\,(b-a).$$

If we replace b by $2^{i-2} + c$ we get:

$$\binom{2^{i-2}}{2} - \binom{(a-c)}{2} + \binom{a}{2} \geq \binom{2^{i-2} + c}{2} - c\,(2^{i-2} + c - a).$$

Take a look at the right side of the inequality:

$$\binom{2^{i-2} + c}{2} = \binom{2^{i-2}}{2} + \sum_{j=0}^{c-1}(2^{i-2} + j) = \binom{2^{i-2}}{2} + c \cdot 2^{i-2} + \binom{c}{2} \text{ and}$$

$$-c(2^{i-2} + c - a) + c \cdot 2^{i-2} + \binom{c}{2} = c \cdot a - \binom{c+1}{2}.$$

Finally we have to show that

$$\binom{a}{2} - \binom{(a-c)}{2} + \binom{c+1}{2} - c \cdot a \geq 0.$$

A short calculation shows in the case where $a \leq c$ that the left side of this inequality is equal to 0. If $a - c < 0$ then define $\binom{(a-c)}{2} = 0$. Another calculation proves this case too. Hence the start of the second induction on h is proved.

In the following the induction hypothesis for the induction on h looks like this:

$$|P_2(S)| \leq |P_2(S^s_{lex})| \quad \text{holds for all } S \subseteq GF(2)^n$$
$$\text{with } |S| = 2^{i-1} + a \text{ and } S \subseteq \bigcup_{j=0}^{h} B_j \text{ where } h \geq i.$$

Now let $S \subseteq \bigcup_{j=0}^{h+1} B_j$. Still we only have to take care of the case $b > \max\{a, 2^{i-2}\}$ for the induction step ($b \leq \max\{a, 2^{i-2}\}$ is covered by case 1 and case 2 of the induction on s). We already mentioned the problem to preserve the structure of the vector spaces if we want to apply one of the known shifting techniques. Our basic idea now is to use a linear function f operating on V where $V = \bigcup_{j=0}^{h+1} B_j$ with a special kernel that is denoted by $\ker f$. This idea will be explained on the next pages.
Since the following lemma might be helpful for a generalization of our result we will state it not only for $m = 2$ but for all $m \in \mathbb{N}$.

Lemma 3 *Given a linear function $f : GF(2)^n \longrightarrow GF(2)^n$ with ker $f = \{0, v\}$ where $v \in GF(2)^n \setminus \{0\}$. Let $S \subseteq GF(2)^n$ and let $D = \{w \in f(S) : |f^{-1}(w) \cap S| = 2\}$ with $|D| = d$. Then*

$$|P_m(S)| \leq |P_m(f(S))| + \binom{d}{2^{m-1}} \quad \textit{where } m \in \mathbb{N}.$$

Proof: We take a fixed but arbitrary $m \in \mathbb{N}$. For $d < 2^{m-1}$ we define $\binom{d}{2^{m-1}} = 0$. Observe that if $m = 1$ the statement of Lemma 3 is obviously correct. Our aim is to construct a function $g : P_m(S) \longrightarrow P_m(f(S)) \cup \binom{D}{2^{m-1}}$ that is injective. Here $\binom{D}{2^{m-1}}$ denotes the set of all subsets of D with 2^{m-1} elements. If we have such a function then the inequality in the lemma is obvious.
We define an equivalence relation on $P_m(S)$ by

$$A \sim B \Longleftrightarrow f(A) = f(B)$$

where $A, B \in P_m(S)$ and $f(A) = \{f(x) \in f(GF(2)^n) : x \in A\}$. We restrict our attention to one equivalence class in order to show how we can define a function g. There are two cases:

Case 1:
Claim: If $A \in P_m(S)$ with $v \in A$ then $f(A) \in \binom{D}{2^{m-1}}$ and there is no $B \in P_m(S)$ with $A \neq B$ such that $f(A) = f(B)$.
That means we have an equivalence class with only one member and we define g on this class by $g(A) = f(A)$.
Proof:
Since $v \in A$ where $v \in \ker f$ it follows that $\frac{|A|}{2} \leq |f(A)| < |A|$. We know that $A \in P_m(S)$ and that the image of a vector space under a linear function is again a vector space. Hence $f(A)$ can only have dimension $m-1$ because of the above inequality. We conclude that $f(A) \in \binom{D}{2^{m-1}}$. For the last part of the claim we just have to observe that under the contrary assumption, there would be an element $x \in f(A)$ with at least 3 elements from $A \cup B$ mapped on x. That contradicts $\ker f = \{0, v\}$.

Case 2:
In order to see how we define a function g in general we assume that there exists an equivalence class with at least two elements $A, B \in P_m(S)$ where $v \notin A \cup B$. It is easy to see that $f(A) \in P_m(f(S))$ (otherwise there would be two elements $x, y \in A$ with $f(x) = f(y)$ and so $x + y = v \in A$, a contradiction). We choose one element of this equivalence class, e.g. A, and map it onto $f(A) \in P_m(f(S))$. Now we have to say what to do for B (or any other element in the class). Before that we prove the following:

Proposition 3 *If $A, B \in P_m(S), A \neq B$ with $v \notin A \cup B$ and $f(A) = f(B)$, then* $\dim\,(A \cap B) = m - 1$.

Proof: As $A \cap B$ is a vector space ($A, B \in P_m(S), A \neq B$) we know that $\dim\,(A \cap B) \leq m - 1$. We assume that $\dim\,(A \cap B) < m - 1$ and lead this statement to a contradiction. For our purpose we denote A and B in a certain way where numbers in A stand for vectors in $GF(2)^n$:
$A = \{0, 1, \ldots, 2^m - 1\}$ and there exists $A^* \subseteq A \setminus \{0\}$ such that $B = \{v + A^*\} \cup A \setminus A^*$ where $'0'$ represents the vector 0 and $\{v + A^*\} = \{v + x \ : \ x \in A^*\}$. Recall that $v \in \ker f$.
Since $A \setminus A^* = A \cap B$ and because of the assumption we obtain $|A \setminus A^*| \leq 2^{m-2}$. Therefore $|\{v + A^*\}| \geq 2^m - 2^{m-2} = 3 \cdot 2^{m-2}$. Now we can choose a basis of B that only consists of elements from $\{v + A^*\}$. If there were at most $m - 1$ linearly independent vectors in $\{v + A^*\}$ then we would have $|\{v + A^*\}| \leq 2^{m-1}$ which is a contradiction to $|\{v + A^*\}| \geq 3 \cdot 2^{m-2}$.

So let $B = < 1' + v, \ldots, m' + v >$ with $i + v \in \{v + A^*\}$ for all $i \in \{1', \ldots, m'\} = I \subset A^*$ ($< v_1, \ldots, v_n >$ denotes the span of the vectors $v_1, \ldots, v_n$). We will count the number of different sums $\sum_{j \in J}(j + v)$ where $J \subseteq I$ and $|J|$ is even and compare this number with $|A \setminus A^*|$.
In the first step we show that all these special sums are pairwise distinct. Assume that there are $H, J \subseteq I, H \neq J$ with $|H|, |J|$ is even and

$$\sum_{j \in J}(j + v) = \sum_{h \in H}(h + v).$$

Then it follows:

$$\sum_{i \in J \cup H}(i + v) = 0.$$

We have a contradiction to the fact that the vectors $(i+v)$ for $i \in J \cup H \subseteq I$ belong to a basis of B. We conclude that the number of sums with $J \subseteq I$, $|J|$ is even is

$$\sum_{k=1}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{2k} = 2^{m-1} - 1.$$

Finally we receive $2^{m-1} - 1 > 2^{m-2} \geq |A \setminus A^*|$ for $m \geq 3$. As a consequence there exists a $J \subseteq I$ with $|J|$ is even and

$$\sum_{j \in J}(j + v) = x + v \in \{v + A^*\}.$$

Then it follows that $\sum_{j \in J} j + x = v \in A$, that is a contradiction to $v \notin A$. In the case $m = 2$ we assume that $A \cap B = \{0\}$. Then we have $B = \{0, 1 + v, 2 + v, 3 + v\}$ and hence $1 + 2 + 3 = v \in A$, again a contradiction and the proof of Proposition 3 is complete. •

This result enables us to see that $f(B \setminus A) \in \binom{D}{2^{m-1}}$ and g can be defined on B by:

$$g(B) = f(B \setminus A).$$

In general, if one equivalence class consists of $A_1, \ldots, A_t$ with $t \geq 1$ where $v \notin A_i$ for all $i \in \{1, \ldots, t\}$ (else we would have case 1 with $t = 1$), we choose one A_i, e.g. A_1, and define:

$$g(A_i) = \begin{cases} f(A_1) & if \quad i = 1 \\ f(A_i \setminus A_1) & if \quad i \in \{2, \ldots, t\} \end{cases}$$

If we do this for every equivalence class then we get a well defined function g.

Next we prove the assertion that g is injective.
We have already proved in case 1 that if an equivalence class consists of one element A with $v \in A$ then its image occurs only once under g. There are two cases to look at:
Case I:
Let $A, B \in P_m(S)$ with $A \neq B$, $v \notin A \cup B$ and $f(A) = f(B)$.
If $g(A) = f(A)$ then $g(B) = f(B - A)$. Of course $g(A) \neq g(B)$ (Recall that we choose only one element C in each equivalence class which is mapped on $f(C)$).
So assume that $g(A), g(B) \in \binom{D}{2^{m-1}}$ and $g(A) = g(B)$. Under this assumption we want to show that there exists an element $x \in D$ with $|f^{-1}(x)| > 2$. That contradicts ker $f = \{0, v\}$. Let $C \in P_m(S)$ with $f(C) = f(A) = f(B)$ but $g(C) = f(C)$.
Next we prove the inequality

$$|(A \setminus C) \cap (B \setminus C)| < 2^{m-1}.$$

Proof: Because of dim $(A \cap C) =$ dim $(B \cap C) = m - 1$ (see Proposition 3 before) we have $|A \setminus C| = 2^{m-1} = |B \setminus C|$. Now we just have to exclude the case where $|(A \setminus C) \cap (B \setminus C)| = 2^{m-1}$. Since $A \setminus C$ includes 2^{m-1} vectors distinct from vector 0 we get a basis for A by using m vectors from $A \setminus C$. But if we assume that $A \setminus C = B \setminus C$ then $A = B$ since A and B have a common basis. Hence we have a contradiction to $A \neq B$.

With $|(A \setminus C) \cap (B \setminus C)| < 2^{m-1}$ and $|(B \cap C)| = 2^{m-1}$ it follows that there exists an element $b \in B \setminus C$ with $b \notin A \setminus C$. Since $b \notin C$ we get $b \notin A \cup C$. Then there exist two vectors $x \in C$, $y \in A - C$ such that $f(x) = f(y) = f(b)$ (recall that we assumed $g(A) = g(B)$). So we have found an element $x = f(b) \in D$ with $|f^{-1}(x)| > 2$.

Case II:
Again let $A, B \in P_m(S)$ with $A \neq B$, $v \notin A \cup B$ and $g(A) = g(B) \in \binom{D}{2^{m-1}}$ but $f(A) \neq f(B)$. We know that $|g(A)| = |g(B)| = 2^{m-1}$ and neither $g(A)$ nor $g(B)$ includes the vector 0. Once more we find one basis for the m-dimensional vector spaces $f(A)$ and $f(B)$ because $g(A) \subseteq f(A)$ and $g(B) \subseteq f(B)$. Therefore $f(A) = f(B)$, a contradiction.
The proof of Lemma 3 is finished. •

Our next aim is to formulate and prove a lemma that refers to Lemma 3. It shows the existence of a vector $v \in V = \bigcup_{j=0}^{h+1} B_j$, for which we later define

a linear function satisfying ker $f = \{0, v\}$, such that the value d in Lemma 3 has an upper bound. This bound enables us then to use the induction hypothesis for $|S|$ or the number of blocks h.
Since the beginning of the second induction is done we can assume that $h+1 \geq i+1$. It will suffice for the proof to take care of $h+1 = i+1$. Let $v \in V$. We define as before that $v + S = \{v + w \,:\, w \in S\}$.

Lemma 4

1. *If $a \leq 2^{i-2}$ then for all $S \subseteq GF(2)^n$ with $|S| = 2^{i-1} + a$ there exists a vector $v \in V \setminus \{0\}$ such that*

$$|(v + S) \cap S| \leq 2^{i-1}.$$

2. *If $2^{i-2} < a < 2^{i-1}$ then for all $S \subseteq GF(2)^n$ with $|S| = 2^{i-1} + a$ there exists a vector $v \in V \setminus \{0\}$ such that*

$$|(v + S) \cap S| \leq 2a.$$

Proof: Since there are $|S|$ vectors we have $\binom{|S|}{2}$ sums $x + y \neq 0$ with $x, y \in S$ and $x \neq y$. Each sum corresponds to a possible, we call it, shift vector v for which we are looking in Lemma 4. Because of $h+1 \geq i+1$ we have at least $2^{i+1} - 1$ shift vectors.
In order to see statement 1. we assume the contrary, i.e. there exists a set $S \subseteq GF(2)^n$ with $|S| = 2^{i-1} + a$ such that for all $v \in V \setminus \{0\}$ we have $|(v + S) \cap S| > 2^{i-1}$ and $a \leq 2^{i-2}$.
So each shift vector has to occur as a sum of elements of S at least $2^{i-2} + 1$ times. It follows that the following inequality is a necessary condition for our opposite assumption:

$$\binom{|S|}{2} \geq (2^{i+1} - 1)(2^{i-2} + 1).$$

We make $|S|$ as big as possible by setting $a = 2^{i-2}$. That means that $|S| = 2^{i-1} + 2^{i-2} = 3 \cdot 2^{i-2}$. Now we have:

$$3 \cdot 2^{i-2}\,(3 \cdot 2^{i-2} - 1) \geq 2\,(2^{i+1} - 1)(2^{i-2} + 1) \text{ and}$$
$$0 \geq 7 \cdot 2^{2i-4} + 17 \cdot 2^{i-2} - 2.$$

Obviously this inequality is wrong for $i \in \mathbb{N}$. We conclude that statement 1. is correct.

With the help of an analogous argument for statement 2. we finally have to show that the following inequality is false:

$$\binom{|S|}{2} \geq (2^{i+1} - 1)(a + 1).$$

We obtain for $|S| = 2^{i-1} + a$ the calculation:

$$(2^{i-1} + a)(2^{i-1} + a - 1) \geq 2(2^{i+1} - 1)(a + 1)$$
$$2^{2i-2} + a^2 \geq 6a \cdot 2^{i-1} + 9 \cdot 2^{i-1} - a - 2.$$

Since $i \in \mathbb{N}$ and $a < 2^{i-1}$ we have $9 \cdot 2^{i-1} - a - 2 \geq 0$. It will be enough to check that $2^{2i-2} \geq a(6 \cdot 2^{i-1} - a)$. Observe that the polynomial given by $p(a) = a(6 \cdot 2^{i-1} - a)$ is monotonicly increasing for $2^{i-2} < a < 2^{i-1}$. Therefore we only need to look at the inequality

$$2^{2i-2} \geq 2^{i-2}(6 \cdot 2^{i-1} - 2^{i-2}) = \frac{11}{4} \cdot 2^{2i-2}$$

in order to see a contradiction. Therefore statement 2. also holds. •

Now we are able to show a link between Lemma 3 and Lemma 4. We define a linear function, denoted by f_v, with ker $f_v = \{0, v\}$ where $v \in V \setminus \{0\}$ satisfies condition 1. or 2. of Lemma 4. Since $v \neq 0$ there exists a component v_i with $v_i = 1$.
We use $f_v : V \longrightarrow V$ with

$$f_v(x) = \begin{cases} x & \text{if } x_i = 0 \\ v + x & \text{if } x_i = 1 \end{cases}$$

where x_i denotes the i-th component of vector $x \in V$. It is clear that ker $f_v = \{0, v\}$. Also it is easy to verify the linearity of f_v. Later we need the fact that f_v maps V on a hyperplane of V.
If we use f_v in Lemma 3 then we can guarantee that the value of d in the inequality

$$|P_m(S)| \leq |P_m(f(S))| + \binom{d}{2^{m-1}}$$

has an upper bound corresponding to the cases of Lemma 4. In order to give the bounds we again refer to the parameter b that stands for the number of vectors of S in block B_{h+1}. If $a \leq 2^{i-2} < b$ then $d \leq 2^{i-2}$ and if $2^{i-2} < a < b$ then $d \leq a$. There are mainly two cases for the final induction steps which depend on d.

Case 1: Suppose that $d \geq 2$.
We have to prove that

$$|P_2(f_v(S))| + \binom{d}{2} \leq |P_2(S^s_{lex})|.$$

Since $d \geq 2$ we can use the induction hypothesis on s because $|S| > |f_v(S)|$. For $d \leq 2^{i-2}$ and for $d \leq a$ it remains to show the correctness of the following inequality where N denotes the set of the d largest elements in S^s_{lex},

$$|P_2(S^s_{lex} \setminus N)| + \binom{d}{2} \leq |P_2(S^s_{lex})|.$$

But now we see that we are in a similar situation as at the beginning of this proof, that means d plays the role of b before.
We obtain for $d \leq 2^{i-2}$:

$$\binom{2^{i-2}}{2} - \binom{2^{i-2} - (d-a)}{2} + \binom{a}{2} \geq \binom{d}{2}$$

and for $d \leq a$:

$$\binom{a}{2} - \binom{a-d}{2} \geq \binom{d}{2}.$$

Both inequalities can be verified by easy calculations.

Case 2: Suppose that $d = 0$.
Let $H_1 = f_v(V)$ denote the hyperplane of V with $f_v(S) \subseteq H_1$. If $f_v(S) \subseteq \bigcup_{j=0}^h B_j$ then we apply the assumption of the second induction on the number of blocks. So we receive

$$|P_2(S)| \leq |P_2(f_v(S))| \leq |P_2(S^s_{lex})|.$$

For the last case let H_2 denote the hyperplane consisting of the first h blocks, that means $H_2 = \bigcup_{j=0}^h B_j$. If $f_v(S) \not\subseteq \bigcup_{j=0}^h B_j$ then $H_1 \neq H_2$. But now it is well-known that there exists a linear bijection, denoted by g, that maps H_1 on H_2 (for instance use a projection along a one dimensional subspace $Z = \{0, z\}$ of V with $z \notin H_1 \cup H_2$). With the help of the induction hypothesis of the induction on the blocks we finally obtain

$$|P_2(S)| \leq |P_2(f_v(S))| = |P_2(g(f_v(S)))| \leq |P_2(S^s_{lex})|.$$

The proof of Theorem 1 is finished. ∎

Remark: This theorem was also conjectured by B. Bolze [3]. She proved Theorem 1 to be true for the cases where $s = 2^k$ with $0 \leq k \leq n$. This result can also be derived from Lemma 2.

Theorem 1 also shows that there exists a total order on $[n, 1]_2$ which maximizes the reverse shadow. We simply order the 1-dimensional spaces according to the lexicographic order of the vectors distinct from vector 0 in each of the spaces.
With the help of Lemma 1 we now define a total order on $[n, 2]_2$ which minimizes the shadow.
Let $V, W \in [n, 2]_2$ with $V = \{0, v_1, v_2, v_3\}$ and $W = \{0, w_1, w_2, w_3\}$ where $v_1 <_{lex} v_2 <_{lex} v_3$ and $w_1 <_{lex} w_2 <_{lex} w_3$. Then

$$V <_{lex2} W \iff \text{ either } V = W \text{ or } v_3 <_{lex} w_3 \text{ or } (v_3 = w_3 \text{ and } v_2 <_{lex} w_2).$$

We finally obtain a partial Kruskal-Katona type result from dimension 2 to dimension 1 in $L_n(2)$.

Corollary 1 *For all $m \in \mathbb{N}$ with $m \leq \binom{n}{2}_2$ and for all $M \subseteq [n, 2]_2$ where $|M| = m$, the m smallest elements with respect to $<_{lex2}$, denoted by M^m_{lex2}, satisfy:*

$$|\Delta M| \geq |\Delta M^m_{lex2}|.$$

The next question is: Can we prove analogous statements to Theorem 1 for $m \geq 3$ in $|P_m(S)|$ with the help of the same method? We already proved Lemma 3 for the general situation. In the proof we made use of the knowledge how many 2-dimensional spaces at most can be obtained with the help of the vectors in the last block. In order to understand why we didn't see how to prove other cases for m, we will give an explicit formula for $|P_3(S^s_{lex})|$.

Lemma 5 *Let $s \in \mathbb{N}$ be given as follows:*

$$s = 2^{k_1} + 2^{k_2} + \ldots + 2^{k_m} + z$$

where $k_i \in \mathbb{N}$ for $i \in \{1, \ldots, m\}$, $k_1 > k_2 > \ldots > k_m \geq 2$ and $0 \leq z < 4$. Then

$$|P_3(S^s_{lex})| = \binom{k_1}{3}_2 + \frac{1}{4}\sum_{j=2}^{m} \binom{2^{k_j}}{3} + \sum_{j=2}^{m} \binom{(\sum_{i=j+1}^{m} 2^{k_i}) + z}{2} 2^{k_j - 1}.$$

Proof: We will prove this lemma by listing all necessary observations in order to be able to see the formula for $|P_3(S^s_{lex})|$. It might be helpful to recall the figure at the beginning of the proof of Theorem 1.
1) For all $i \in \{1, \ldots, m\}$ we have: $2^{k_i} > (\sum_{j=i+1}^{n} 2^{k_j}) + z$ (Obviously the representation of s is unique and therefore this must be correct too).

2) It is clear that the first 2^{k_1} elements of S^s_{lex} form a k_1- dimensional subspace. So we obtain $\binom{k_1}{3}_2$ 3-dimensional spaces.

3) Because of 1) we have $(\sum_{i=2}^{m} 2^{k_i}) + z$ elements in block B_{k_1+1}. We claim that if we want to have a 3-dimensional space in S^s_{lex} with the help of vectors of block B_{k_1+1} then we have to take exactly 4 vectors from B_{k_1+1} and the other 4 from $\bigcup_{j=0}^{k_1} B_j$.
Proof: If we used more than 4 vectors from B_{k_1+1} then we would have at least 4 linearly independent vectors and we would not get a 3-dimensional space. (If there were only three linearly independent vectors there would be only one way - the sum of all of them - to produce another vector included in the same block B_{k_1+1} by a linear combination.)
If there were less than 4 vectors in B_{k_1+1} then the sum of one of those together with at least 4 nonzero vectors in $\bigcup_{j=0}^{k_1} B_j$ would produce another 4 vectors in block B_{k_1+1}. So there must be more than 3 vectors in B_{k_1+1} if we want to produce a 3-dimensional space.

4) Since 3) holds and if we choose a basis $a, b, c \in B_{k_1+1}$ of a 3-dimensional space then the fourth vector $d \in B_{k_1+1}$ of this space must satisfy: $a+b+c = d$.

5) Our next aim is to show that the representation of s induces a special structure on block B_{k_1+1}. For each $i \in \{2, \ldots, m\}$ we receive a, we call it, subblock of length 2^{k_i} that has the following properties if we write the vectors as columns and if we refer to the subblock as a matrix (in this situation we will count the rows from bottom to top):
Claim a): Each row above row k_i is constant (either 0 or 1, of course row number $k_1 + 1$ consists only of 1's if it exists).
Claim b): If we look at the 2^{k_i} columns restricted on the first k_i rows then this submatrix describes a k_i-dimensional space (the columns are the vectors of the space).

Example for $s = 56 = 2^5 + 2^4 + 2^3$ and $GF(2)^6$ and the subblock for $k_3 = 3$:

$$\begin{array}{r|cccccccc}
 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
k_3{=}3 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1
\end{array}$$

Proof: It will be enough to show a) and b) for k_2. Inductively one can easily prove the other cases too by using analogous arguments.
Let SB_{k_2} denote the subblock for k_2. We know that the entries of the vector right before this subblock in the lexicographic order in the first k_1 rows is 1 and above 0. So our first vector with respect to $<_{lex}$ in SB_{k_2} has only ceros from row 1 up to row k_1 (included). In row k_1+1 there is a 1 and in the rows above ceros. If we pick the next $2^{k_2}-1$ vectors in the lexicographic order we obtain our subblock SB_{k_2}. Since $k_1 > k_2$ we didn't change the entries of the rows with a number higher than k_2. Hence they are constant. The last vector in SB_{k_2} has 1's in the first k_2 rows.

6) If we choose a basis of a 3-dimensional space in one subblock SB_{k_i} for $i \in \{2, \dots, m\}$ then the fourth vector belongs also to this subblock. This can be seen with the help of the observations 3) to 5). Since we get $\binom{4}{3}$ times the same 3-dimensional space with the help of 4 vectors satisfying 4), there are $\frac{1}{4}\sum_{j=2}^{m}\binom{2^{k_j}}{3}$ 3-dimensional spaces constructable like this in S^s_{lex}. This is the second part of the formula that we want to show.

7) Assume that $a, b, c, d \in B_{k_1+1}$ belong to one 3-dimensional space in S^s_{lex}, where $a <_{lex} b <_{lex} c <_{lex} d$. We will show that a and b are in the same subblock.
Because of 6) it remains to take care of the cases where there are at least 2 subblocks which include a, b, c, d. Let $a^*, b^*, c^* \in \{a, b, c, d\}$ with $a^* \in SB_{k_i}, b^* \in SB_{k_j}$ and $c^* \in SB_{k_h}$ where $i < j \leq h$. We will restrict our attention to the last vector, denoted by x, in subblock SB_{k_i} and the first vector, denoted by y, in subblock $SB_{k_{i+1}}$. Horizontally written these vectors look like this:

$$x = (\overbrace{1, 1, \dots, 1}^{k_i}, a_1, \dots, a_{n-k_i}),$$
$$y = (\underbrace{0, 0, \dots, 0}_{k_i}, b_1, \dots, b_{n-k_i}).$$

Let $\bar{x} = (a_1, a_2, \dots, a_{n-k_i})$ and $\bar{y} = (b_1, b_2, \dots, b_{n-k_i})$; we call $\bar{x}$ and $\bar{y}$ the upper part of x and y respectively. With the help of 1) we know that $2^{k_i} >$

$(\sum_{j=i+1}^{m} 2^{k_j})+z$, i.e. $\bar{y}$ is also the upper part of b^* and c^*. Now we receivce for $a^*+b^*+c^*=d^*$ that the upper part of d^* must be $\bar{x}$. If we restrict the sum of a^*, b^*, c^* on the first k_i rows then we stay in a k_i-dimensional space that is formed by the lower part of subblock SB_{k_i} (see observation 5)). Finally we have $d^* \in SB_{k_i}$.

8) Now we are able to calculate the last part of the formula. We will do this inductively by starting with $i=2$. The question is how many 3-dimensional spaces can be produced in S^s_{lex} with the property that exactly 2 vectors of each space belong to subblock SB_{k_2}. Because of 3) there are $\binom{(\sum_{j=3}^{m} 2^{k_j})+z}{2}$ ways to choose two vectors not laying in SB_{k_2}. For each such pair there are 2^{k_2-1} possible pairs in SB_{k_2} such that we satisfy 4) (if we pick one vector, the second is determined by the sum). In this context we need observation 7). So we get $\binom{(\sum_{j=3}^{m} 2^{k_j})+z}{2} 2^{k_2-1}$ spaces of dimension 3.
In the general step for subblock SB_{k_s} where $s>2$ we only have to look for all pairs of vectors that belong to subblocks SB_{k_j} with $k_j > k_s$. All other combinations are counted in the steps before. So we get $\binom{(\sum_{j=s+1}^{m} 2^{k_j})+z}{2} 2^{k_s-1}$ spaces. The sum of all values for each subblock gives the last part of the formula.

If we look at all these observations then it is clear that there is no other way to construct 3-dimensional spaces in S^s_{lex}. Therefore the proof of Lemma 5 is complete. •

Under the assumption that $<_{lex}$ has the maximizing property for all $m \leq n$, Lemma 5 indicates a possible correspondence between Theorem A and the outstanding generalization of Theorem 1. The unique representation of s in Lemma 5 plays a similar role for the explicit formula of $|P_3(S^s_{lex})|$ as the k-binomial representation of m for the cardinality of the shadow in Theorem A.

5. Remarks and open problems

The crucial point why we are able to prove Theorem 1 is the block structure of the vectors of $GF(2)^n$ listed lexicographically and hence the knowledge about how 2-dimensional spaces can be constructed in $GF(2)^n$. This structure gets lost if we look at vector spaces over other finite fields.
For $GF(3)$ for instance, we tried to find a definition for a total order on $[n,k]_3$ that could be a candidate for fulfilling the properties we are looking for. Recall how we used the lexicographic order on $GF(2)^n$ in order to define $<_{lex2}$ on $[n,2]_2$. It is easy to find examples where an order, that is similarly

defined with the help of the lexicographic order on the vectors of $GF(3)^n$ with its canonical basis, does not have the property to minimize or maximize the cardinality of the shadow or reverse shadow respectively.

There is a canonical way to order the elements of $[n,k]_q$ with respect to the shadow minimization problem. The reverse shadow maximization problem can be handled analogously.
We take an arbitrary $X_1 \in [n,k]_q$ and set $\mathcal{A}_1 = \{X_1\}$. For the general step let us assume that we have taken n elements $\{X_1, X_2, \cdots, X_n\} = \mathcal{A}_n \subseteq [n,k]_q$. Then we take an element $X_{n+1} \in [n,k]_q - \mathcal{A}_n$ such that

$$|\Delta(\mathcal{A}_n \cup \{X_{n+1}\})| \leq |\Delta(\mathcal{A}_n \cup \{X\})| \quad \text{for all } X \in [n,k]_q - \mathcal{A}_n.$$

Set $\mathcal{A}_{n+1} = \mathcal{A}_n \cup \{X_{n+1}\}$ and go on like this taking one element in each step until all elements of $[n,k]_q$ are used. So for $A, B \in [n,k]_q$ we can define: $A < B \Leftrightarrow A = B$ or A is taken before B in the above sense.
Because of the possibility that there exists more than one element for extending the set $\mathcal{A}_n$ to $\mathcal{A}_{n+1}$, there are several orders on $[n,k]_q$ possible that result from this method.
Finally we want to formulate two questions arising from this method of obtaining orders on $[n,k]_q$. Given $m \leq \binom{n}{k}_q$. Does every order restricted on the m smallest elements lead to the same cardinality of the shadow? And if this is true, can these orders be of help for answering the Kruskal-Katona type question in linear lattices?

Acknowledgement

The author would like to thank for the support of the SFB 343, Diskrete Strukturen in der Mathematik, Universität Bielefeld.

References

[1] I. Anderson, *Combinatorics of Finite Sets*, Clarendon Press, Oxford, 1987.

[2] B. Bollobás, *Combinatorics*, Cambridge University Press, 1986.

[3] B. Bolze, "Ein Kruskal-Katona-Typ Problem: Schattenminimierung in Vektorräumen", Diplomarbeit an der Universität Bielefeld, 1994.

[4] G.G. Clements and B. Lindström, "A generalization of a combinatorial theorem of Macaulay", *Journal of Comb. Theory* **7**, pp. 230-238, 1969.

[5] D.E. Daykin, "A simple proof of the Kruskal-Katona Theorem", *Journal of Comb. Theory (A)* **17**, pp. 252-253, 1974.

[6] K. Engel and H.-D.O.F. Gronau, *Sperner theory in partially ordered sets*, B.G. Teubner Verlagsgesellschaft, Leibniz, 1985.

[7] P. Frankl, "A new short proof for the Kruskal-Katona theorem", *Discrete Math.* **48**, pp. 327-329, 1984.

[8] C. Greene and D.J. Kleitman, "Proof techniques in the theory of finite sets", in: G.-C. Rota (ed.), *Studies in combinatorics*, vol. 17 of MAA Studies in Mathematics, 1978.

[9] A.J.W. Hilton, "A simple proof of the Kruskal-Katona Theorem and of some associated binomial inequalities", *Periodica Mathematica Hungarica*, vol. 10, pp. 25-30, 1979.

[10] G. Katona, "A theorem on finite sets", *Theory of Graphs Proc. Colloq. Tihany* 1966, Akademiai Kiado, pp. 187-207, 1968.

[11] J.B. Kruskal, "The number of simplices in a complex", *Mathematical optimization Techniques*, Berkeley and Los Angeles, pp. 251-278, 1963.

[12] Private conversation at the Colloquium of Combinatorics in Braunschweig, Germany, 1995.