Example 10.13 (Maximum weight traveling salesman problem). We are given a complete directed graph with non-negative weights on edges, and we must find a maximum weight Hamiltonian cycle, that is, a cycle that visits every vertex exactly once. This problem is very hard: it is a so-called "NP-hard" problem. On the other hand, using Theorem 10.8 and Lemma 10.10 we can show that the greedy algorithm can find a Hamiltonian cycle whose weight is at least one third of the maximum possible weight of a Hamiltonian cycle.

The ground-set X of our family $\mathcal{F}$ in this case consists of the directed edges of the complete graph. A set is independent if its edges form a collection of vertex-disjoint paths or a Hamiltonian cycle. It is enough to show that $\mathcal{F}$ is 3-extendible.

To show this, let $A+x$ and B be any two members of $\mathcal{F}$, where $A \subset B$ and $x = (u, v)$ is an edge not in B. First remove from B the edges (if any) out of u and into v. There can be at most two such edges, and neither of them can belong to A since otherwise $A+(u, v)$ would not belong to $\mathcal{F}$. If we add (u, v) to B then every vertex has in-degree and out-degree at most one. Hence, the only reason why the resulting set may not belong to $\mathcal{F}$ is that there may be a non-Hamiltonian cycle which uses (u, v). But then there must be an edge in the cycle, not in A, that we can remove to break it: if all edges, except for (u, v), of the cycle belong to A, then $A + (u, v)$ contains a non-Hamiltonian cycle and could not belong to $\mathcal{F}$. Therefore we need to remove at most three edges in total.

10.4 The Kruskal–Katona theorem

A *neighbor* of a binary vector v is a vector which can be obtained from v by flipping one of its 1-entries to 0. A *shadow* of a set $A \subseteq \{0, 1\}^n$ of vectors is the set $\partial(A)$ of all its neighbors. A set A is *k-regular* if every vector in A contains exactly k 1-entries. Note that in this case $\partial(A)$ is $(k-1)$-regular.

A basic question concerning shadows is the following one: What can one say about $|\partial(A)|$ in terms of the total number $|A|$ of vectors in a k-regular set A?

In general one cannot improve on the trivial upper bound $|\partial(A)| \leq k|A|$. But what about *lower* bounds? The question is non-trivial because one and the same vector with $k-1$ ones may be a neighbor of up to $n-k+1$ vectors in A. Easy counting shows that

$$|\partial(A)| \geq \frac{k}{n-k+1}|A| = \frac{|A|}{\binom{n}{k}}\binom{n}{k-1} .$$

This can be shown by estimating the number N of pairs (u, v) of vectors such that $v \in A$ and u is a neighbor of v. Since every $v \in A$ has exactly k neighbors, we have that $N = k|A|$. On the other hand, every vector u

with $k-1$ ones can be a neighbor of at most $n-k+1$ vectors of A. Hence, $k|A| = N \leq (n-k+1)|\partial(A)|$, and the desired lower bound on $|\partial(A)|$ follows.

Best possible lower bounds on $|\partial(A)|$ were obtained by Kruskal (1963) and Katona (1966). The idea, again, is to show that the minimum of $|\partial(A)|$ over all sets A with $|A| = m$ is achieved by sets of a very special structure, and use the Pascal identity for binomial coefficients $\binom{x}{k} = x(x-1)\cdots(x-k+1)/k!$: for every real number $x \geq k$

$$\binom{x}{k-1} + \binom{x}{k} = \binom{x+1}{k}. \tag{10.1}$$

In Proposition 1.3 we gave a combinatorial proof of this identity in the case when x is a natural number. The case when x is not necessarily an integer can be shown by a simple algebraic manipulation:

$$\begin{aligned}\binom{x}{k-1} + \binom{x}{k} &= \frac{x!}{(x-(k-1))!(k-1)!} + \frac{x!}{(x-k)!k!} \\ &= \frac{kx! + (x+1-k)x!}{(x+1-k)!k!} = \binom{x+1}{k}.\end{aligned}$$

The following lemma allows us to restrict our attention to sets with a very special structure. For a set of vectors $A \subseteq \{0,1\}^n$, let A_0 and A_1 denote the sets of vectors in A starting, respectively, with 0 and 1. Hence, $A = A_0 \cup A_1$. Let also e_i denote the vector in $\{0,1\}^n$ with exactly one 1-entry in the i-th position.

Proposition 10.14. *For every set $B \subseteq \{0,1\}^n$ there is a set $A \subseteq \{0,1\}^n$ of the same size such that $|\partial(B)| \geq |\partial(A)|$ and*

$$\partial(A_0) + e_1 \subseteq A_1. \tag{10.2}$$

That is, if we take a vector v in A with $v_1 = 0$, flip any of its 1s to 0 and at the same time flip its first bit to 1, then the obtained vector will again belong to A.

Proof. For $1 < j \leq n$, the *j-th shift* of B is the set $s_j(B)$ of vectors defined as follows. First, we include in $s_j(B)$ all vectors $v \in B_1$. For the vectors $v \in B_0$ we look whether $v_j = 1$. If yes, we include in $s_j(B)$ the vector $v \oplus e_1 \oplus e_j$ (obtained from vector v by flipping its 1-st and j-th bits), but only if this vector does not already belong to B; if $v \oplus e_1 \oplus e_j$ belongs to B, we include in $s_j(B)$ the vector v itself. This last requirement ensures that $|s_j(B)| = |B|$ for every $1 < j \leq n$. For example, if

$$B = \begin{matrix} 1\,0\,1\,0 \\ 1\,1\,0\,1 \\ 0\,1\,1\,0 \\ 0\,1\,0\,1 \end{matrix} \qquad \text{then} \qquad s_2(B) = \begin{matrix} 1\,0\,1\,0 \\ 1\,1\,0\,1 \\ 0\,1\,1\,0 \\ 1\,0\,0\,1 \end{matrix}$$

We claim that the shifting operation preserves the neighborhood. Namely, for every $1 < j \leq n$,

$$\partial(s_j(B)) \subseteq s_j(\partial(B)) \,.$$

The following diagram sketches the proof idea:

$$\begin{tikzcd}
(0\ldots1\ldots1\ldots) \arrow[r, "\text{shift}"] \arrow[d, "\text{neighbor}"] & (1\ldots0\ldots1\ldots) \arrow[d, "\text{neighbor}"] \\
(0\ldots1\ldots0\ldots) \arrow[r, "\text{shift}"] & (1\ldots0\ldots0\ldots)
\end{tikzcd}$$

If we repeatedly apply the shift operators s_j, $j = 2, \ldots, n$ to B, the number of vectors containing 1 in the first position increases, so that after a finite number of applications the shifts must therefore cease to make any change. We have then obtained a new set A of the same size as B, with $s_j(A) = A$ for each $j \geq 2$, and with $|\partial(B)| \geq |\partial(A)|$. We claim that A satisfies (10.2).

To show this, take a vector $u \in \partial(A_0)$. Then $u + e_j$ belongs to A_0 for some $j \geq 2$, and hence, $u + e_1$ belongs to $s_j(A) = A$. □

We first state and prove a slightly weaker but much more handy version of the Kruskal–Katona theorem.

Theorem 10.15. *If $A \subseteq \{0,1\}^n$ is k-regular, and if*

$$|A| \geq \binom{x}{k} = x(x-1)\cdots(x-k+1)/k!$$

for some real number $x \geq k$, then

$$|\partial(A)| \geq \binom{x}{k-1} \,. \tag{10.3}$$

Note that this is the best possible: If $A \subseteq \{0,1\}^n$ is the set of all $\binom{n}{k}$ vectors with exactly k ones, then $|\partial(A)| = \binom{n}{k-1}$.

Proof (due to Lovász 1979). By Proposition 10.14, we can assume that A satisfies (10.2). Consider the set

$$A^0 := \{(0, w) \;:\; (1, w) \in A\}$$

obtained from A_1 by flipping the first bit from 1 to 0. Note that $|A^0| = |A_1|$. Observe also that

$$|\partial(A)| \geq |A^0| + |\partial(A^0)| \,. \tag{10.4}$$

Indeed, vectors in the set A^0 are neighbors of A by the definition of this set. Moreover, each neighbor of A^0 plus the unit vector e_1 is also a neighbor of A.

We now argue by double induction on k and $m = |A|$. For $k = 1$ and m arbitrary, (10.3) holds trivially.

For the induction step, we first use the fact that A has a special structure—namely, satisfies (10.2)—to show that $|A^0|$ cannot be smaller than $\binom{x-1}{k-1}$. To show this, assume the opposite. Then

$$|A_0| = |A| - |A_1| = |A| - |A^0| > \binom{x}{k} - \binom{x-1}{k-1} = \binom{x-1}{k},$$

and so, by induction, $|\partial(A_0)| \geq \binom{x-1}{k-1}$. But then (10.2) implies that

$$|A^0| = |A_1| \geq \binom{x-1}{k-1},$$

a contradiction. Hence, $|A^0| \geq \binom{x-1}{k-1}$.

Since A^0 is $(k-1)$-regular, the induction hypothesis yields $|\partial(A^0)| \geq \binom{x-1}{k-2}$. Together with (10.4) this implies

$$|\partial(A)| \geq |A^0| + |\partial(A^0)| \geq \binom{x-1}{k-1} + \binom{x-1}{k-2} = \binom{x}{k-1},$$

as desired. □

To state the Kruskal–Katona theorem in its original form, we write $m = |A|$ in *k-cascade* form:

$$m = \binom{a_k}{k} + \binom{a_{k-1}}{k-1} + \cdots + \binom{a_s}{s} \tag{10.5}$$

where $a_k > a_{k-1} > \ldots > a_s \geq s \geq 1$ are integers. Such a representation of m can be obtained as follows. Let a_k be the maximal integer for which $\binom{a_k}{k} \leq m$. Then choose a_{k-1} as the largest integer for which $\binom{a_{k-1}}{k-1} \leq m - \binom{a_k}{k}$. If $a_{k-1} \geq a_k$, then we would have $m \geq \binom{a_k}{k} + \binom{a_k}{k-1} = \binom{1+a_k}{k}$, contradicting the maximality of a_k. Therefore $a_{k-1} < a_k$. Continuing this process we eventually reach a stage where the choice of a_s for some $s \geq 2$ actually gives an equality,

$$\binom{a_s}{s} = m - \binom{a_k}{k} - \binom{a_{k-1}}{k-1} - \cdots - \binom{a_{s+1}}{s+1},$$

or we get right down to choosing a_1 as the integer such that

$$\binom{a_1}{1} \leq m - \binom{a_k}{k} - \cdots - \binom{a_2}{2} < \binom{a_1+1}{1}$$

in which case we have

$$0 \leq m - \binom{a_k}{k} - \cdots - \binom{a_1}{1} < 1,$$

so that

$$m = \binom{a_k}{k} + \cdots + \binom{a_1}{1}.$$

It can be shown by induction (do this!) that the representation (10.5) is unique.

Theorem 10.16 (Kruskal–Katona Theorem)**.** *If $A \subseteq \{0,1\}^n$ is k-regular, and if*

$$|A| = \binom{a_k}{k} + \binom{a_{k-1}}{k-1} + \cdots + \binom{a_s}{s}$$

then

$$|\partial(A)| \geq \binom{a_k}{k-1} + \binom{a_{k-1}}{k-2} + \cdots + \binom{a_s}{s-1}.$$

We leave the proof as an exercise. It is the same as that of Theorem 10.15 with $\binom{x}{k}$ and $\binom{x}{k-1}$ replaced by the corresponding sums of binomial coefficents.

The representation (10.5) of $m = |A|$ in the k-cascade form seems somewhat magical. To interpret this representation, let us consider the so-called *colexicographic order* (or *colex order*) of vectors in $\{0,1\}^n$. This order is defined by letting $u \prec v$ iff there is an i such that $u_i = 0$, $v_i = 1$ and $u_j = v_j$ for all $j > i$. Note that the only difference from the more standard *lexicographic* order is that we now scan the strings from right to left. For example, the colex order of all $\binom{5}{3} = 10$ vectors in $\{0,1\}^5$ with exactly 3 ones is (with the "smallest" vector on the top):

$$\begin{array}{c}
1\,1\,1\,0\,0 \\
1\,1\,0\,1\,0 \\
1\,0\,1\,1\,0 \\
0\,1\,1\,1\,0 \\
1\,1\,0\,0\,1 \\
1\,0\,1\,0\,1 \\
0\,1\,1\,0\,1 \\
1\,0\,0\,1\,1 \\
0\,1\,0\,1\,1 \\
0\,0\,1\,1\,1
\end{array}$$

Let E^n_k denote the k-th slice of the binary n-cube, that is, the set of all vectors in $\{0,1\}^n$ with exactly k ones.

Proposition 10.17. *If the m-th vector in the colex order of E^n_k contains 1s in positions $a_1 + 1 < a_2 + 1 < \ldots < a_k + 1$ then*

$$m = \binom{a_k}{k} + \binom{a_{k-1}}{k-1} + \cdots + \binom{a_1}{1}.$$

Proof. Let v be the m-th vector in the colex order of E^n_k. To reach v we must skip all vectors whose k-th 1 appears before position $a_k + 1$, and there are

$\binom{a_k}{k}$ of these. Some vectors with last (rightmost) 1 in position a_k may also precede v. These are the vectors whose first $k-1$ 1s precede position $a_{k-1}+1$, and there are $\binom{a_{k-1}}{k-1}$ of these. Arguing further in this way gives the result. □

By the same argument one can show that the shadow of the first $m = \sum_{i=1}^{k}\binom{a_i}{i}$ vectors in the colex order of E_k^n consists of the first $\partial_k(m) := \sum_{i=1}^{k}\binom{a_i}{i-1}$ vectors in the colex order of E_{k-1}^n. Thus, the Kruskal–Katona theorem says that the shadow of a family of m vectors in E_k^n is minimized by the set consisting of the first m vectors in the colex ordering on E_{k-1}^n. Furthermore, the size of the shadow is $\partial_k(m)$.

10.5 Universal sets

The (n,k)-density of a set of vectors means that its projection on *at least one* set of k coordinates gives the whole binary k-cube. We now consider a stronger property – (n,k)-universality – where we require that the same holds for *all* subsets of k coordinates.

Of course, the whole cube $\{0,1\}^n$ is (n,k)-universal for every $k \leq n$. This is the trivial case. Do there exist smaller universal sets? Note that 2^k is a trivial lower bound.

Using the probabilistic argument it can be shown that there *exist* (n,k)-universal sets of size only $k2^k \log n$ (see Theorem 3.2).

This result tells us only that small universal sets exist, but gives us no idea of how to construct them. In this section we will show how to construct explicit sets in $\{0,1\}^n$ which only have size n and are (n,k)-universal as long as $k2^k < \sqrt{n}$. The construction employs some nice combinatorial properties of so-called Paley graphs.

In this section we introduce one property of (bipartite) graphs which is equivalent to the universality property of 0-1 vectors. In the next section we will describe an explicit construction of such graphs based on the famous theorem of Weil (1948) regarding character sums.

By a bipartite graph with parts of size n we will mean a bipartite graph $G = (V_1, V_2, E)$ with $|V_1| = |V_2| = n$. We say that a node $y \in V_2$ is a *common neighbor* for a set of nodes $A \subseteq V_1$ if y is joined to *each* node of A. Dually, a node $y \in V_2$ is a *common non-neighbor* for a set of nodes $B \subseteq V_1$ if y is joined to *no* node of B. Given two disjoint subsets A and B of V_1, we denote by $v(A,B)$ the number of nodes in V_2 which are common neighbors for A, and at the same time are common non-neighbors for B. That is, $v(A,B)$ is the number of nodes in V_2 joined to each node of A and to no node of B.

Definition 10.18. A bipartite graph $G = (V_1, V_2, E)$ satisfies the *isolated neighbor condition for k* if $v(A,B) > 0$ for any two disjoint subsets $A, B \subseteq V_1$ such that $|A| + |B| = k$.