the whole linear space; since the dimension of this space is $|A| = \binom{n}{k}$, this will mean that we must have $|U| \geqslant \binom{n}{k}$ columns.

The fact that the columns of M span the whole linear space follows directly from the following claim saying that every unit vector lies in the span.

Claim 14.9. *Let $a \in A$ and $U_a = \{u \in U : m_{a,u} = 1\}$. Then*

$$\sum_{u \in U_a} m_{b,u} = \begin{cases} 1 & \text{if } b = a; \\ 0 & \text{if } b \neq a. \end{cases}$$

Proof. By the definition of U_a, we have (all sums are over $\mathbb{F}_2$):

$$\sum_{u \in U_a} m_{b,u} = \sum_{\substack{u \in U \\ u \leqslant a \wedge b}} 1 = \sum_{x \leqslant a \wedge b} (T_k^n(x) + g(x)) = \sum_{x \leqslant a \wedge b} T_k^n(x) + \sum_{x \leqslant a \wedge b} g(x).$$

The second term of this last expression is 0, since $a \wedge b$ has at least $d+1$ 1's (Exercise 14.16). The first term is also 0 except if $a = b$.

This completes the proof of the claim, and thus, the proof of the lemma. □

14.2.3 Disjointness matrices

Let $k \leqslant n$ be natural numbers, and X be a set of n elements. A *k-disjointness matrix* over X is a 0-1 matrix $D = D(n,k)$ whose rows and columns are labeled by subsets of X of size at most k; the entry $D_{A,B}$ in the A-th row and B-th column is defined by:

$$D_{A,B} = \begin{cases} 0 & \text{if } A \cap B \neq \emptyset, \\ 1 & \text{if } A \cap B = \emptyset. \end{cases}$$

This matrix plays an important role in computational complexity (we will use it in Sects. 15.2.2 and 16.4). Its importance stems from the fact that it has full rank over $\mathbb{F}_2$, i.e., all its $\sum_{i=0}^{k} \binom{n}{i}$ rows are linearly independent.

Theorem 14.10. *The k-disjointness matrix $D = D(n,k)$ has full rank over $\mathbb{F}_2$, that is,*

$$\mathrm{rk}_{\mathbb{F}_2}(D) = \sum_{i=0}^{k} \binom{n}{i}.$$

There are several proofs of this result. Usually, it is derived from more general facts about Möbius inversion or general intersection matrices. Here we present one particularly simple and direct proof due to Razborov (1987).

Proof. Let $N = \sum_{i=0}^{k} \binom{n}{i}$. We must show that the rows of D are linearly independent over $\mathbb{F}_2$, i.e., that for any non-zero vector $\lambda = (\lambda_{I_1}, \lambda_{I_2}, \ldots, \lambda_{I_N})$ in $\mathbb{F}_2^N$ we have $\lambda \cdot D \neq 0$. For this, consider the following polynomial:

$$f(x_1, \dots, x_n) \rightleftharpoons \sum_{|I| \leqslant k} \lambda_I \prod_{i \in I} x_i.$$

Since $\lambda \neq 0$, at least one of the coefficients λ_I is nonzero, and we can find some I_0 such that $\lambda_{I_0} \neq 0$ and I_0 is *maximal* in that $\lambda_I = 0$ for all $I \supset I_0$. Assume w.l.o.g. that $I_0 = \{1, \dots, t\}$, and make in the polynomial f the substitution $x_i := 1$ for all $i \notin I_0$. After this substitution has been made, a *non-zero* polynomial over the first t variables $x_1, \dots, x_t$ remains such that the term $x_1 x_2 \cdots x_t$ is left untouched (here we use the maximality of I_0). Hence, after the substitution we obtain a polynomial which is 1 for some assignment $(a_1, \dots, a_t)$ to its variables. But this means that the polynomial f itself takes the value 1 on the assignment $b = (a_1, \dots, a_t, 1, \dots, 1)$. Hence,

$$1 = f(b) = \sum_{|I| \leqslant k} \lambda_I \prod_{i \in I} b_i.$$

Let $J_0 \rightleftharpoons \{i : a_i = 0\}$. Then $|J_0| \leqslant k$ and, moreover, $\prod_{i \in I} b_i = 1$ if and only if $I \cap J_0 = \emptyset$, which is equivalent to $D_{I,J_0} = 1$. Thus,

$$\sum_{|I| \leqslant k} \lambda_I D_{I,J_0} = 1,$$

meaning that the J_0-th coordinate of the vector $\lambda \cdot D$ is non-zero. □

14.3 Spaces of polynomials

In order to apply the linear algebra method, in many situations it is particularly useful to associate sets not to their incidence vectors but to some (multivariate) polynomials $f(x_1, \dots, x_n)$ and show that these polynomials are linearly independent as a members of the corresponding functions space. This idea, know as the *polynomial technique*, has found many applications. We will present only few of them. All these applications are based on the following simple and powerful lemma connecting algebra to linear algebra.

Lemma 14.11. *For $i = 1, \dots, m$ let $f_i : \Omega \to \mathbb{F}$ be functions and $v_i \in \Omega$ elements such that*

(a) $f_i(v_i) \neq 0$ *for all* $1 \leqslant i \leqslant m$;
(b) $f_i(v_j) = 0$ *for all* $1 \leqslant j < i \leqslant m$.

Then $f_1, \dots, f_m$ are linearly independent members of the space $\mathbb{F}^{\Omega}$.

Proof. By contradiction: Suppose there is a nontrivial linear relation

$$\lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_m f_m = 0$$

between the f_i's. Take the smallest i for which $\lambda_i \neq 0$. Substitute v_i for the variables. By the assumption, all but the ith term vanish. What remains is $\lambda_i f_i(v_i) = 0$, which implies $\lambda_i = 0$ because $f_i(v_i) \neq 0$, a contradiction. □