Proof. Take any $x, y \in C_n$, $x \neq y$. If these two vectors have been obtained from the i-th rows of H and $-H$ respectively, then they disagree in all n coordinates. Otherwise, there are two different rows u and v in H such that x is obtained (by changing -1s to 0s) from u or $-u$, and y from v or $-v$. In all cases, x and y differ in $n/2$ coordinates, because $\pm u$ and $\pm v$ are orthogonal. □

Hadamard matrices can also be used to construct combinatorial designs with good parameters. Recall that a (v, k, λ) *design* is a k-uniform family of subsets (also called *blocks*) of a v-element set such that every pair of distinct points is contained in exactly λ of these subsets; if the number of blocks is the same as the number v of points, then the design is *symmetric* (see Chap. 12).

By Theorem 14.9, we have that, if there is a Hadamard matrix of order n, then $n = 2$ or n is divisible by 4. It is conjectured that Hadamard matrices exist for *all* orders that are divisible by 4.

Theorem 14.11. *Every Hadamard matrix of order* $4n$ *gives a symmetric* $(4n-1, 2n-1, n-1)$ *design.*

Proof. Let H be a Hadamard matrix of order $4n$, and assume that it is normalized, i.e., the first row and the first column consist entirely of 1s. Form a $(4n-1) \times (4n-1)$ 0-1 matrix M by deleting the first column and the first row in H, and changing -1s to 0s. This is the incidence matrix of a symmetric $(4n-1, 2n-1, n-1)$ design, because by Theorem 14.9, each row of M has $2n-1$ ones and any two columns of M have exactly $n-1$ ones in common. □

14.4 Matrix rank and Ramsey graphs

A matrix $A = (a_{ij})$ is *lower co-triangular* if $a_{ii} = 0$ and $a_{ij} \neq 0$ for all $1 \leq j < i \leq n$. That is, such a matrix has zeroes on the diagonal and nonzero entries below the diagonal; the entries above the diagonal may be arbitrary.

Lemma 14.12. *Let* p *be a prime number, and* A *an* $n \times n$ *lower co-triangular matrix over* $\mathbb{F}_p$ *of rank* r*. Then*

$$n \leq \binom{r+p-2}{p-1} + 1 \leq (r+p)^{p-1} .$$

Proof. Let $r = \mathrm{rk}_{\mathbb{F}_p}(A)$ and $A = B \cdot C$ be the corresponding decomposition of A. For $i = 1, \ldots, n$ consider the polynomials $f_i(x) = 1 - g_i(x)^{p-1}$ in r variables $x = (x_1, \ldots, x_r)$ over $\mathbb{F}_p$, where $g_i(x)$ is the scalar product of x with the i-th row of B. Let $c_1, \ldots, c_n$ be the columns of C. Then $g_i(c_i) = 0$ and $g_i(c_j) \neq 0$ for every $i > j$. Since p is a prime, Fermat's Little Theorem (see Exercise 1.15) implies that $a^{p-1} = 1$ for every $a \neq 0$ in $\mathbb{F}_p$. Hence, $f_i(c_i) \neq 0$

and $g_i(c_j) = 0$ for every $i > j$. By Lemma 13.11, the polynomials $f_1, \ldots, f_n$ are linear independent elements of a vector space V of all polynomials over $\mathbb{F}_p$ of degree $p-1$, all of whose monomials $\prod_{i=1}^r x_i^{t_i}$ satisfy $\sum_{i=1}^r t_i = p-1$ and $t_i \geq 0$. By Proposition 1.5, the number of such monomials is $\binom{r+(p-1)-1}{p-1}$. Since the polynomials can also have a constant term (which accounts for the "+1" in the final equation), we have that

$$n \leq \dim V \leq \binom{r+p-2}{p-1} + 1 \leq (r+p)^{p-1} . \qquad \square$$

Let R be a ring and $A = (a_{ij})$ an $n \times n$ matrix with entries from R. The rank $\mathrm{rk}_R(A)$ of A over R is defined as the minimum number r for which there exists an $n \times r$ matrix B and an $r \times n$ matrix C over R such that $A = B \cdot C$; if all entries of A are zeroes then $\mathrm{rk}_R(A) = 0$. If $R = \mathbb{F}$ is a field, then $\mathrm{rk}_R(A)$ is the usual rank over $\mathbb{F}$, that is, the largest number of linear independent rows.

By Lemma 14.12, lower co-triangular matrices over $R = \mathbb{Z}_m$ have large rank, if m is a prime number. But what about $R = \mathbb{Z}_m$ for non-prime m, say, for $m = 6$? In this case R is no longer a field—it is just a ring (division is not defined). Still one can extend the notion of rank also to rings.

Let R be a ring and $A = (a_{ij})$ an $n \times n$ matrix with entries from R. The rank $\mathrm{rk}_R(A)$ of A over R is defined as the minimum number r for which there exists an $n \times r$ matrix B and an $r \times n$ matrix C over R such that $A = B \cdot C$; if all entries of A are zeroes then $\mathrm{rk}_R(A) = 0$. If $R = \mathbb{F}$ is a field, then $\mathrm{rk}_R(A)$ is the usual rank over $\mathbb{F}$, that is, the largest number of linear independent rows.

It turns out that explicit low rank matrices over the ring $R = \mathbb{Z}_6$ of integers modulo 6 would give us explicit graphs with good Ramsey properties, that is, graphs without any large clique or large independent set.

Let $A = (a_{ij})$ be an $n \times n$ lower co-triangular matrix over $\mathbb{Z}_6$. Associate with A the graph $G_A = (V, E)$ with $V = \{1, \ldots, n\}$, where two vertices $i > j$ are adjacent iff a_{ij} is odd.

Lemma 14.13 (Grolmusz 2000)**.** *If $r = \mathrm{rk}_{\mathbb{Z}_6}(A)$ then the graph G_A contains neither a clique on $r+2$ vertices nor an independent set of size $\binom{r+1}{2} + 2$.*

Proof. It is clear that $\mathrm{rk}_{\mathbb{F}_p}(A) \leq r$ for $p \in \{2, 3\}$. Let $S \subseteq V$ be a clique in G_A of size $|S| = s$, and $B = (b_{ij})$ be the corresponding $s \times s$ submatrix of A; hence, $b_{ii} = 0$ and $b_{ij} \in \{1, 3, 5\}$ for all $i > j$. Then $B \bmod 2$ is a lower co-triangular matrix over $\mathbb{F}_2$, and Lemma 14.12 (with $p = 2$) implies that $|S| \leq r + 1$.

Now let $T \subseteq V$ be an independent set in G_A of size $|T| = t$, and $C = (c_{ij})$ be the corresponding $t \times t$ submatrix of A; hence, $c_{ii} = 0$ and $c_{ij} \in \{2, 4\}$ for all $i > j$. Then $C \bmod 3$ is a lower co-triangular matrix over $\mathbb{F}_3$, and Lemma 14.12 (with $p = 3$) implies that $|T| \leq \binom{r+1}{2} + 1$. $\square$

In Sect. 13.7 (Theorem 13.15) we have shown how to construct explicit n-vertex graphs with no clique or independent set larger than

$$t := 2^{c\sqrt{\ln n \ln\ln n}}$$

for an absolute constant c. Grolmusz (2000) constructed a co-triangular $n \times n$ matrix A over $R = \mathbb{Z}_6$ with $\mathrm{rk}_{\mathbb{Z}_6}(A) \le t$. Together with Lemma 14.13, this gives an alternative construction of a graph G_A with no clique or independent set larger than t.

14.5 Lower bounds for boolean formulas

Boolean *formulas* (or De Morgan formulas) are defined inductively as follows:

- Every boolean variable x_i and its negation $\overline{x}_i$ is a formula of size 1 (these formulas are called *leaves*).
- If F_1 and F_2 are formulas of size l_1 and l_2, then both $F_1 \wedge F_2$ and $F_1 \vee F_2$ are formulas of size $l_1 + l_2$.

Note that the size of F is exactly the number of leaves in F.

Often one uses an equivalent definition of a formula as a circuit with And, Or, and Not gates, whose underlying graph is a tree. That is, now negation is allowed not only at the leaves. But using De Morgan rules $\neg(x \vee y) = \neg x \wedge \neg y$ and $\neg(x \wedge y) = \neg x \vee \neg y$ one can move all negations to leaves without increasing the formula size.

Given a boolean function f, how it can be shown that it is hard, i.e., that it cannot be computed by a formula of small size? Easy counting shows that almost all boolean functions in n variables require formulas of size exponential in n. Still, for a *concrete* boolean function f, the largest remains the lower bound $n^{3-o(1)}$ proved by Håstad (1993).

The main difficulty here is that we allow negated variables $\overline{x}_i$ as leaves. It is therefore natural to look at what happens if we forbid this and require that our formulas are *monotone* in that they do not have negated leaves. Of course, not every boolean function $f(x_1, \ldots, x_n)$ can be computed by such a formula – the function itself must be also *monotone*: if $f(x_1, \ldots, x_n) = 1$ and $x_i \le y_i$ for all i, then $f(y_1, \ldots, y_n) = 1$. Under this restriction progress is substantial: we are able to prove that some explicit monotone functions require monotone formulas of super-polynomial size.

14.5.1 Reduction to set-covering

Let A and B be two disjoint subsets of $\{0,1\}^n$. A boolean formula F *separates* A and B if $F(a) = 1$ for all $a \in A$ and $F(b) = 0$ for all $b \in B$. A *rectangle* is a subset $R \subseteq A \times B$ of the form $R = S \times T$ for some $S \subseteq A$ and $T \subseteq B$. A