The affine part. In order to check the existence of these polarities we pass to the so-called affine part of these geometries. The normalizer B acts on $\mathcal{P}$ and $\mathcal{L}$ by left multiplication, and the orbits of B have length $1, q, \ldots, q^{r-1}$, respectively. The restriction of I to the *largest* orbits $\mathcal{P}_*$ and $\mathcal{L}_*$ (of size q^{r-1} each) defines the *affine subgeometry* $(\mathcal{P}_*, \mathcal{L}_*, I_*)$ of $(\mathcal{P}, \mathcal{L}, I)$. By Γ_* we denote its incidence graph.

It is known that if there is a polarity of the geometry, then there is one that maps $\mathcal{P}_* \cup \mathcal{L}_*$ into itself. Thus for the above cases, there exists a polarity π_* of the affine part $(\mathcal{P}_*, \mathcal{L}_*, I_*)$.

The nice thing about the incidence graphs and polarities of the affine part is that they admit a simple coordinatized description. In order to check their properties one does not need to have any idea where they came from. Of course one won't be able to come up with one without intuition. In Exercise 3.9 we looked at a coordinatization of a polarity of the affine part of the generalized quadrangle (of type $B_2(q)$), which eventually improved the leading constant of $ex(n, C_6)$ from $1/2\sqrt[3]{2}$ to $1/2$. Similar simple coordinatized description exists for the affine part of the generalized hexagon, but that would not lead us to a better construction, since for $ex(n, C_{10})$ the leading constant was already proved to be larger than $1/2$ in the last subsection.

3.6 Dense regular graphs with large girth

The starting point of our discussion in this chapter was the Moore-bound (see Proposition 3.1 and Exercise 3.1), providing a lower bound on the minimum number of vertices in d-regular graphs with girth g. A *Moore-graph* is a d-regular graph with girth g, having exactly as many vertices as the corresponding (odd or even) Moore-bound. The existence of Moore-graphs is decided for many values of the two parameters. For $g = 3$ and arbitrary $d \geq 3$ the complete graph K_{d+1} provides the unique example, while for $g = 4$ and arbitrary $d \geq 2$ the complete bipartite graph $K_{d,d}$ is the unique Moore-graph. For $g = 5$, it was proven by Hoffmann and Singleton using spectral methods, that Moore-graphs can only exist when $d = 2, 3, 7$, or 57. In the first three cases, there are unique examples: C_5, the Petersen graph, and the Hoffmann-Singleton graph. The existence of a 57-regular graph of girth 5 on $1 + 57 + 57 \cdot 56 = 3250$ vertices is still one of the tantalizing mysteries of algebraic graph theory. Then of course there is always the cycle C_g of length g, providing the unique example for $d = 2$ and arbitrary $g > 3$, but otherwise the existence of Moore-graph for $g > 5$ is very limited. Bannai and Ito [?] and Damerell [?] have shown that no Moore graph with odd girth $g \geq 7$ and $d > 2$ can exist. The even girth case was settled by a theorem of Feit and Higman [?], which implies that Moore-graphs with even girth g and $d > 2$ cannot exist unless $g = 4, 6, 8$, or 12. In the latter three cases the Benson-graphs provide Moore-graphs whenever d is of the form $q + 1$ with q being a prime power. The question of existence for $g = 6, 8$, and 12 is open for other values of d.

The limited range of parameters when the Moore-bound can be tight motivates the definition of the *cage number* $c(d, g)$, representing the smallest number n of vertices on

which there is a d-regular graph with girth g. We will see later that this quantity is well-defined.

Above we have overviewed the cases when the cage number can be equal to the Moore-bound and found that it can never happen if the girth g is larger than 12. For our investigation of the Turán number $ex(n, C_{2k})$ these construction were relevant, because we were interested in C_{2k}-free constructions for some *fixed value of* k and tried to create as dense graph as possible, which is equivalent to achieving a given degree d of regularity with as few vertices as possible.

Now we will concentrate the other end of the spectrum: keep the degree d of regularity a fixed constant and let g be large/tend to infinity.

In that case the order of magnitude of both the even and the odd Moore bound is $(d-1)^{\lfloor (g-1)/2 \rfloor} = \Omega\left((d-1)^{\frac{1}{2}g}\right)$, that is exponential in g with the base $\sqrt{d-1}$.

In the next exercise we describe an upper bound due to Erdős and Sachs.

Exercise 3.11 *Let $f(d,g)$ be the smallest n such that there exists a d-regular graph with girth at least g on n vertices.*

- *Let G be a graph on $2m \geq 4\sum_{i=0}^{g-2}(d-1)^i$ vertices such that (i) G has girth at least g and (ii) every vertex $v \in V(G)$ has degree $d-1$ or d, and G has the largest possible number of edges among graphs with these properties. Prove that G is d-regular*
- *Conclude that $f(d,g) \leq 4\sum_{i=0}^{g-2}(d-1)^i$*

Remark: The above bound is due to Erdős and Sachs and it is roughly the square of the Moore bound. They also derive that every d-regular graph with girth at least g *does have* a cycle of length g, so the cage number $c(d,g)$ exists and is equal to $f(d,g)$. That is, we obtain

$$c(d,g) \leq (d-1)^{(1+o(1))g},$$

that is roughly the square of the lower bound.

In the exercise we proved the upper bound using an implicit inductive argument. This bound turned out be very difficult to topple. Actually the explicit construction of a fixed d-regular graph with girth at least g on just exponentially many $c(d)^g$ vertices turned out to be not an easy task for any constant $c(d)$.

In the 1980's Margulis, and independently Lubotzky, Phillips and Sarnak, obtained construction using groups and sophisticated algebraic number theory to construct graphs for every fixed $d = q+1$ and arbitrary large g and number of vertices $c(d,g) \leq (d-1)^{\left(\frac{3}{4}+o(1)\right)g}$. The main goal of these constructions were to give explicit constant degree expander graphs, with second eigenvalue as small as possible, the lack of short cycles was only side product. Later Lazebnik, Ustimenko, and Woldar gave alternative constructions that give similar, but slightly better bound.

The description and proof of correctness of these constructions are beyond the scope of our lecture notes. Our goal in this section is to introduce a much simpler construction

of Margulis, with a somewhat larger, but still exponential, number of vertices. This construction will provide at least partial glimpse into how the more complicated ones came around. We largely follow the treatment of [?].

The simple canonical way to construct graphs that are regular is by Cayley graphs. They are also natural candidates to examine for girth problems as cycles in Cayley graphs have a simple description based on the generators.

For a group $\langle G, \cdot \rangle$ and a subset $S \subseteq G$ of generators with the property $S = S^{-1}$, and $1 \notin S$, we define the Cayley graph $C = C(G, S)$ as follows. The vertex set is the group G and two group elements g and $h \in G$ are adjacent if $gh^{-1} \in S$. Note that $gh^{-1} \in S$ if and only if $hg^{-1} = (gh^{-1})^{-1} \in S$, because $S = S^{-1}$. Moreover there are no loops since $1 \notin S$.

If $S = \{s_1, \dots s_d\}$, then the neighbors of any group element g are $gs_1, \dots gs_d$. In particular C is $|S|$-regular. Furthermore, there exists a cycle of length ℓ in C if and only if there is a relation $s_{i_1} \cdot \dots \cdot s_{i_\ell} = 1$ of minimal size that expresses the unit element as a product of ℓ elements $s_{i_1}, \dots, s_{i_\ell}$ of S. (That is, there is no proper subsequence $s_{i_j}, \dots, s_{i_k}$, $1 \leq j \leq k \leq \ell$ whose product is the identity element.)

To demonstrate the idea of Cayley graphs and establish explicitely that for *any* degree d, there exists a d-regular graph with arbitrary large girth, we describe first a simple construction with much worse parameters. Let r be arbitrary and let $T = T_{d,r}$ be the full d-ary tree of depth r, with root vertex w. Our Cayley graph will be over the symmetric group S_V of permutations of the vertex set $V = V(T)$. To define the generators, we fix an arbitrary proper d-coloring $\chi : E(T) \to [d]$. This is easy to find by first coloring the d edges incident to the root with distinct colors and then proceeding down the tree level by level, always coloring properly the $d - 1$ uncolored edges at each new vertex with the remaining colors. For each color $i = 1, \dots, d$ we define a permutation $\pi_i \in S_V$ as follows. For a vertex $u \in V(C)$ which has a neighbor z such that $\chi(uz) = i$, we set $\pi_i(u) = z$ (since χ is proper, there is no more than one such neighbor z). Otherwise, $\pi_i(u) = u$. Observe that this happens only for a leaf vertex u, if the color i is not exactly the one that appears on the sole edge incident to u.

We claim that the girth of this graph is at least $2r + 1$, which shows our promised statement as r was chosen arbitrarily. If there is a cycle of length g in C, then there exists a product $\pi_{i_1}\pi_{i_2} \cdots \pi_{i_g} = id_V$. Let us follow the position of the root vertex in this product. $\pi_{i_1}(w)$ is definitely on the first level as w has all colors, hence also i_1. Then $\pi_{i_2}\pi_{i_1}(w)$ is definitely on the second level of the tree T, since $i_2 \neq i_1$ and the vertex $\pi_{i_1}(w)$ has all colors but i_1 on its incident edges towards the second level. Similarly, $\pi_{i_1}\pi_{i_2} \cdots \pi_{i_\ell}(w)$ is on the ℓth level of T for every $\ell \in [r]$. Finally, $\pi_{i_1}\pi_{i_2} \cdots \pi_{i_r}(w)$ is a leaf vertex. The next permutation, $\pi_{i_{r+1}}$ should leave this leaf fixed, since $1_r \neq i_{r+1}$, and then we need r more step back to the root. So the cycle has length at least $2r + 1$.

Exercise 3.12 *Show that the girth of the above graph is in fact at least* $4r + 2$.

The number of vertices in the above example is at least doubly exponential in r and

hence also in the girth $\geq 2r+1$:

$$\left(\sum_{i=1}^{r}(d-1)^i\right)! \geq \left(\frac{(d-1)^r}{e}\right)^{(d-1)^r} \geq (d-1)^{(d-1)^r}.$$

In the main construction of this section we will define a 4-regular graph whose order is single exponential in its girth g. It will not be as good as the above existence proof which gives $O(3^g)$ vertices, but the constant in the base will also not be outrageous. This graph, due to Margulis, could be considered the prequel to the other, more complicated constructions which have only $O(3^{\frac{3}{4}g})$ vertices.

The idea is to start with the ultimate 4-regular graph of large girth: the infinite 4-regular tree, and construct it as a Cayley graph. Then we factor this group appropriately to make it finite. Factoring of the group creates a canonical Cayley graph, which is the homomorphic image of the original Cayley graph. What happens to the properties of the original Cayley graph, in particular what are the degrees and how can cycles occur? It turns out that the new Cayley graph is also 4-regular and cycles can occur only under very controled conditions and we will be able to track their size. The proof we include here is due to Gábor Tardos.

The group will be $SL_2(\mathbb{Z})$, i.e. the multiplicative group of (2×2) integer matrices with determinant 1. Our generator set S will contain four members, the following matrices:

$$A=\begin{pmatrix}1&2\\0&1\end{pmatrix}\quad A^{-1}=\begin{pmatrix}1&-2\\0&1\end{pmatrix}\quad B=\begin{pmatrix}1&0\\2&1\end{pmatrix}\quad B^{-1}=\begin{pmatrix}1&0\\-2&1\end{pmatrix}$$

First we show that $C(SL_2(\mathbb{Z}),S)$ is the infinite 4-regular tree.

Claim 4 *For any vector $x\in\mathbb{R}^2$ with $x_1,x_2\neq 0$ and $x_1\neq x_2$, exactly three of $||Ax||$, $||A^{-1}x||$, $||Bx||$, $||B^{-1}x||$ are larger than $||x||$, where the norm $||y||$ of vector $y\in\mathbb{R}^2$ denotes the infinity norm $\max\{|y_1|,|y_2|\}$.*

Proof. Suppose wlog that $x_1>x_2$. Then $|2x_1+x_2|$ and $|-2x_1+x_2|$ are both at least $2|x_1|-|x_2|>|x_1|$, so $||Bx||$ and $||B^{-1}x||$ are larger than $||x||=x_1$. Now among $|x_1+2x_2|$ and $|x_1-2x_2|$ exactly one is larger and one is smaller than $x_1=||x||$ (that which one is which depends on whether x_1 and x_2 have the same sign or not). That means that exactly one of $||Ax||$ and $||A^{-1}x||$ is larger than $||x||$ and the other is smaller. □

Now let us assume that there is a product $M_g\cdots M_1=I$, with factors from S, that give the identity matrix. We will show that g is large. Let us follow the movement of the particular vector $y=(1,\sqrt{2})$ when we start applying the sequentially the M_is. (But any vector with algebraically independent coordinates would do.) Let j be the index for which the infinity norm of the image $M_jM_{j-1}\cdots M_1y=:x$ is the largest. That means that two of the neighbors of x, that is $M_{j+1}x=M_{j+1}M_j\cdots M_1y$ and $M_j^{-1}x=M_{j-1}\cdots M_1y$ have norm that is not larger than $||x||$. This is a contradiction to the previous Claim, since the vector x satisfies its conditions. Indeed, $M_jM_{j-1}\cdots M_1=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ is an integer matrix

with determinant one. So applying it to y the resulting vector $x = (a + b\sqrt{2}, c + \sqrt{2})$ (i) cannot have a 0-coordinate, because that would mean that the matrix must have a 0 row, and (ii) cannot have equal coordinates because then the matrix had two equal rows. (All this because 1 and $\sqrt{2}$ are algebraically independent.) So there are no cycles and hence the Cayley graph $C(SL_2(\mathbb{Z}), S)$ is indeed the infinite 4-regular tree.

Now let us take the same four matrices as generators, but in the group $SL_2(\mathbb{Z}_p)$. This is a finite group of size $\frac{(p^2-1)(p^2-p)}{p-1} = p^2(p-1) \sim p^3$.

Let us take a shortest cycle and let $M_1, \ldots, M_g$ be the corresponding generators. We know that modulo p the product $M_g \cdots M_1 = I$ is the idenity matrix. But we also know that over $\mathbb{Z}$ the matrix is NOT the identity matrix I. So at least one of the entries must be at least p in absolute value, that is $||M_1, \ldots, M_g|| \geq p$. But multiplying an arbitrary matrix B with any one of the four generator matrices $M \in S$, the infinity norm of the new matrix MB is at most 3 times the infinity norm of M. The infinity norm of any of the generators is 2, so $2 3^{g-1} \geq p$. This means that the number of vertices is at most

$$|V(C(SL_2(\mathbb{Z}_p)))| \sim p^3 = O(27^g).$$

The bound is admittedly weaker than the bound $O\left((2.28)^g\right)$ of [?, ?], but the proof is sweet and self-contained. It is also weaker than the implicit bound $O\left(3^g\right)$ of Erdős and Sachs, but the construction is explicit. So let's just not worry (and be happy).