Non-expander Cayley graphs of simple groups

Gábor Somlai
Alfréd Rényi Institute of Mathematics
email: zsomlei@gmail.com*

Abstract

For every infinite sequence of simple groups of Lie type of growing rank we exhibit connected Cayley graphs of degree at most 10 such that the isoperimetric number of these graphs converges to 0. This proves that these graphs do not form a family of expanders.

1 Introduction

Let G be a finite group and T a subset of G. The Cayley graph $Cay(G,T)$ is defined by having vertex set G and g is adjacent to h if and only if $g^{-1}h \in T$. A Cayley graph $Cay(G,T)$ is undirected if and only if $T = T^{-1}$, where $T^{-1} = \{t^{-1} \mid t \in T\}$.

Let Γ be an arbitrary graph with vertex set $V(\Gamma)$. Let $S \subseteq V(\Gamma)$. We define the boundary of S, which we denote by $\partial(S)$, to be the set of vertices in $V(\Gamma) \setminus S$ with at least one neighbour in S. For a graph Γ the isoperimetric number $h(\Gamma)$ is defined by

$$h(\Gamma) = min \left\{ \frac{|\partial(S)|}{|S|} \;\middle|\; S \subset V(\Gamma),\, 0 < |S| \leq \frac{|V(\Gamma)|}{2} \right\}.$$

A graph Γ is called an ϵ-expander if $h(\Gamma) \geq \epsilon$, and a series of k-regular graphs Γ_n is called an expander family if there is a constant $\epsilon > 0$ such that for every n the graph Γ_n is an ϵ-expander. Finally, we say that a family of groups G_n is a family of uniformly expanding groups if there exist $0 < \epsilon \in \mathbb{R}$ and $k \in \mathbb{N}$ such that for every i and every generating set $S_i \subset G_i$ of size at most k the Cayley graphs $Cay(G_i, S_i)$ are ϵ-expanders.

The study of series of Cayley graphs of finite simple groups has received great attention.

It was announced by Kassabov, Lubotzky and Nikolov in [7] that there exist $k \in \mathbb{N}$ and $0 < \epsilon \in \mathbb{R}$ such that every non-abelian finite simple group which is not a Suzuki group has a set of generators S of size at most k for which

*Research is partially supported by MTA Renyi "Lendulet" Groups and Graphs Research Group

$Cay(G,S)$ is an ϵ-expander. The details of the proof of this result are given in a series of papers (see [5],[8],[6],[12],[14]), and the theorem has been extended by Breuillard, Green and Tao in [1] to the Suzuki groups. These results motivate a question which was asked by Lubotzky in [13] - is every family of Chevalley groups of bounded rank a family of uniformly expanding groups?

In [11], Lubotzky also suggested that one should investigate families of simple groups of unbounded rank, and wrote that it seems likely that if G_n is a sequence of non-abelian simple groups of Lie type such that the rank of G_n is unbounded, then for every n there exists a generating set $T_n \subset G_n$ such that the graphs $Cay(G_n, T_n)$ do not form a family of expanders. An explicit example (see [10, p.31]) of a non-expander family of Cayley graphs of special linear groups was given by Luz. The diameter of the graphs given by Luz was investigated by Kassabov and Riley, and it was proved in [9] that there exists $c \in \mathbb{R}$ such that the diameter of the graphs is smaller than $c\ log(|SL(n,p)|)$.

Similarly, the symmetric group S_n is generated by $\gamma = (1,2)$ and $\sigma_n = (1,2,\ldots,n)$ for every $n \in \mathbb{N}$ and the corresponding sequence of isoperimetric numbers $h\left(Cay\left(S_n, \{\gamma, \sigma_n\}\right)\right)$ tends to 0. Moreover, one can find a set of generators of S_n such that the diameter of the corresponding Cayley graphs is $\Omega(n^2)$ which shows that these Cayley graphs do not form a family of expanders, see [10, Proposition 6.1.8].

One of the breakthroughs in solving questions on growth in groups is due to Helfgott (see [4]), who proved that for a generating set $A \subset SL(2,p)$ we have either $|A^3| \geq |A|^{1+\delta}$ or $(A \cup A^{-1} \cup e)^k = SL(2,p)$, where $\delta > 0$ and $k \geq 1$ are absolute constants. Complete generalizations of this result to all finite simple groups of Lie type of bounded rank were given by Pyber and Szabó (see [16]) and by Breuillard, Green and Tao (see [2]). For every $n \geq 3$, an explicit example of generating set A of $SL(n,3)$ was also given by Pyber and Szabó (see [16]) such that $|A^3| \leq 100|A|$ and it is mentioned that large families of generating sets of constant growth, which are union of a few cosets of some subgroup, can also be given for $SL(n,q)$, where $q > 2$. Similar counterexamples for growth in symmetric groups were given in [15] and in [17].

For every prime power q we will investigate 7 series $A_l(q), B_l(q), C_l(q), D_l(q)$, ${}^2A_{2n-1}(q^2), {}^2A_{2n}(q^2), {}^2D_n(q^2)$ of finite simple groups of Lie type. These are the series of groups of Lie type of fixed type for which the rank of the groups tends to infinity. In order to define generators and subgroups of these groups we will use the generators given by Steinberg in [18] and we will use the notation and several results in the book of Carter [3].

For these 7 series of finite simple groups of Lie type we construct Cayley graphs and subsets such that the number of neighbours of these subsets depends on the rank of the group. Moreover, the isoperimetric number of these graphs tends to 0. This proves the conjecture of Lubotzky concerning the series of Cayley graphs of simple groups of unbounded rank. More precisely, we prove the following:

Theorem 1. *(a) Let G be a Chevalley group of rank l of type A_l, B_l, C_l or D_l. For every $l \geq 5$ and for every finite field $GF(q)$ there exists a* *generating set T of cardinality at most* 10 *and a subset of the vertices* $S \subset V(Cay(G,T))$ *with* $|S| \leq \frac{|G|}{2}$ *such that* $\frac{|\partial(S)|}{|S|} \leq \frac{6}{l-3}$.

(b) *Let G be a twisted group of type* ${}^2A_{2n-1}$, ${}^2A_{2n}$ *or* ${}^2D_n$. *For every* $n \geq 5$ *and for every finite field* $GF(q)$ *there exists a generating set* T' *of cardinality at most* 8 *and* $S' \subset V(Cay(G,T'))$ *with* $|S'| \leq \frac{|G|}{2}$ *such that* $\frac{|\partial(S')|}{|S'|} \leq \frac{6}{n-2}$.

The paper is organized into the following 4 sections. In Section 2 we give all necessary definitions and we collect some important facts concerning the construction of simple groups of Lie type. The proof of Theorem 1 (a) is contained in Section 3, and Theorem 1 (b), which is the case of twisted groups, will be handled in Section 4. Finally, in Section 5 we present the original construction in terms of matrices.

2 Preliminaries

In this section we collect important facts about finite simple groups of Lie-type and we build up the notation we will use throughout this paper.

Let $K = GF(q)$ be a finite field. We denote by Φ the system of roots and $\Phi = \Phi^+ \cup \Phi^-$ is the union of the positive and negative roots. We also choose $\Pi = \{r_1, r_2, \ldots, r_l\} \subset \Phi^+$ which is the set of fundamental roots.

The Weyl group W is generated by the reflections w_r, where $r \in \Phi$. It is well known that W is generated by the fundamental reflections w_r, where $r \in \Pi$. In order to simplify notation we denote by w_i the fundamental reflection w_{r_i}, where $r_i \in \Pi$. We denote by $x_r(t)$ the standard generators of the Chevalley group G, where $r \in \Phi$ and $t \in K$. If $r = r_i$ for some $r_i \in \Pi$, then we denote by $x_i(t)$ the standard generator $x_{r_i}(t)$. The subgroups $X_r = \{x_r(t) \mid t \in K\}$ for $r \in \Phi$ are called root subgroups of G.

Let $n_r(t) = x_r(t)x_{-r}(-t^{-1})x_r(t)$ and set $n_r = n_r(1)$. Clearly, $n_r(t)$ is an element of the subgroup generated by the root subgroups X_r and X_{-r} for every $t \in K$ and $r \in \Phi$. It is well known that $n_r x_s(t) n_r^{-1} = x_{w_r(s)}(\eta_{r,s} t)$ for some $\eta_{r,s} \in K$ depending only on r and s, see [3, p.101]. Let $h_r(t) = n_r(t)n_r(-1)$. It is easy to see that $h_r(t) \in \langle X_r, X_{-r} \rangle$.

We denote by H the subgroup generated by the elements $h_r(t)$ for all $r \in \Phi$ and $t \in K$ and let N be the subgroup of G generated by H and the elements n_r for all $r \in \Phi$. The elements of H can be written in the form $h(\chi)$, where χ is a K-character of $\mathbb{Z}\Phi$, see [3, p.97]. The K-character corresponding to $h_r(t)$ is denoted by $\chi_{r,t}$ and $\chi_{r,t}(a) = t^{\frac{2(a,r)}{(r,r)}}$. H is a normal subgroup of N and $n_w h(\chi) n_w^{-1} = h(\chi')$, where $\chi'(r) = \chi(w^{-1}(r))$, see [3, p.102].

The Weyl group W is isomorphic to N/H and every element of the Weyl group W acts on the root system Φ. Using this isomorphism, the cosets of H in N can be written as $n_w H$ with $n_{w_r} = n_r$ for all $r \in \Phi$.

3 Chevalley groups

In this section we construct series of Cayley graphs for 4 different series of Chevalley groups. For these Chevalley groups we need 6 series of Cayley graphs. The six different constructions are similar but we will treat them separately.

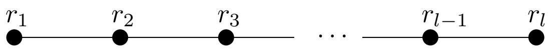
We first prove the following technical lemma.

Lemma 1. *Let $w = w_1 w_2 \dots w_l$ be a Coxeter element of the Weyl group W and let us assume that the fundamental root r_i is orthogonal to r_j if $i+1 < j \leq l$ and r_{i+1} is orthogonal to r_k if $1 \leq k \leq i-1$. We also assume that r_i and r_{i+1} have the same length and $w_i(r_{i+1}) = r_i + r_{i+1}$. Then $w(r_i) = r_{i+1}$.*

Proof. Since r_i is orthogonal to r_j for every $j > i+1$ we have that $w(r_i) = w_1 w_2 \dots w_i w_{i+1}(r_i)$. The elements w_k are reflections through the hyperplane perpendicular to r_k. Thus $w_k(r_k) = -r_k$ for every $1 \leq k \leq l$ and $w_{i+1}(r_i) = r_i + r_{i+1} = w_i(r_{i+1})$ since r_i and r_{i+1} have the same length. It follows that $w_i w_{i+1}(r_i) = w_i(r_i + r_{i+1}) = w_i(r_i) + w_{r_{i+1}} = -r_i + (r_i + r_{i+1}) = r_{i+1}$. Hence $w(r_i) = w_1 w_2 \dots w_{i-1}(r_{i+1}) = r_{i+1}$ since r_{i+1} is orthogonal to r_k for $1 \leq k \leq i-1$. ■

3.1 A_l

Let G be a Chevalley group of type A_l. The Dynkin diagram of the corresponding root system is the following:



One can see from the Dynkin diagram that $w_i(r_{i+1}) = r_i + r_{i+1} = w_{i+1}(r_i)$ for $i = 1, \dots, l-1$.

Let $w = w_1 w_2 \dots w_l$ be a Coxeter element of the Weyl group. We choose λ to be a generator of the multiplicative group of $GF(q)$.

Lemma 2. *$x_1(1)$, n_w and $h_{r_1}(\lambda)$ generate the Chevalley group G.*

Proof. It was proved in [18, Theorem 3.11] that $x_1(1)n_w$ and $h_{r_1}(\lambda)$ generate G if $q > 3$, and $x_1(1)$ and n_w generate G if $q \leq 3$. ■

For every $l \geq 5$ we define the following undirected Cayley graph:

$$\Gamma_a = Cay(G, \{x_1(1), n_w, h_{r_1}(\lambda), x_1(1)^{-1}, n_w^{-1}, h_{r_1}(\lambda)^{-1}\}).$$

Let K_a be the subgroup of the Chevalley group G generated by the root subgroups $X_{r_1}, X_{-r_1}, X_{r_2}, X_{-r_2}, \dots, X_{r_{l-1}}, X_{-r_{l-1}}$. Clearly, $K_a \cong A_{l-1}$. Let

$$S_a = \bigcup_{i=0}^{l-1} K_a n_w^i.$$

Lemma 3. *The orbit of w which contains r_1 is the following:*

$$\to r_1 \xrightarrow{w} r_2 \xrightarrow{w} r_3 \xrightarrow{w} \cdots \xrightarrow{w} r_{l-1} \xrightarrow{w} r_l \xrightarrow{w} -r_1 - \ldots - r_l \xrightarrow{w}$$

This can be formulated as follows:

$$\begin{aligned} w(r_i) &= r_{i+1} \; for \; 1 \leq i \leq l-1 \\ w(r_l) &= -r_1 - \ldots - r_l \\ w(-r_1 - r_2 - \ldots - r_l) &= r_1 \end{aligned}$$

Proof. Lemma 1 gives that $w(r_i) = r_{i+1}$ for $1 \leq i \leq l-1$ and

$$w(r_l) = w_1 w_2 \ldots w_l(r_l) = w_1 w_2 \ldots w_{l-1}(-r_l) = -w_1 w_2 \ldots w_{l-1}(r_l)$$

since w is a linear transformation of the vector space spanned by the roots. We also have $w_j(r_{j+1} + \cdots + r_l) = r_j + r_{j+1} + \cdots + r_l$ for $1 \leq j \leq l-1$. Therefore

$$\begin{aligned} w_1 w_2 \ldots w_{l-1}(r_l) &= w_1 w_2 \ldots w_{l-2}(r_{l-1} + r_l) \\ &= w_1 w_2 \ldots w_{l-3}(r_{l-2} + r_{l-1} + r_l) = \cdots = r_1 + r_2 + \ldots + r_l. \end{aligned}$$

This shows that

$$w(r_l) = -(r_1 + r_2 + \ldots + r_l). \tag{1}$$

Using again the linearity of w and equation (1) we get

$$w(r_1 + r_2 + \ldots + r_l) = r_2 + r_3 + \ldots + r_l - (r_1 + r_2 + \ldots + r_l) = -r_1.$$

This gives $w(-(r_1 + r_2 + \ldots + r_l)) = r_1$, finishing the proof Lemma 3. ■

It follows from the proof of Lemma 3 that if $1 \leq i \leq l-1$, then $n_w^i K_a n_w^{-i}$ contains $n_w^i X_{r_{l-i}} n_w^{-i} = X_{r_l}$. Therefore $n_w^i K_a n_w^{-i} \neq K_a$ which shows that $n_w^i \notin K_a$ for every $1 \leq i \leq l-1$. This implies that $K_a, K_a n_w, \ldots, K_a n_w^{l-1}$ are different right cosets of K_a so S_a is the union of l pairwise disjoint subsets of the vertices of Γ_a and these subsets have the same cardinality.

Lemma 4. $\frac{|\partial(S_a)|}{|S_a|} \leq \frac{6}{l}$

Proof. S_a is the union of l right cosets of K_a so $|S_a| = l\,|K_a|$. It is clear from the definition of S_a that $(K_a n_w^i) n_w \subset S_a$ for every $0 \leq i \leq l-2$ and similarly $\left(K_a n_w^i\right) n_w^{-1} \subset S_a$ if $1 \leq i \leq l-1$. Therefore those neighbors of S_a which are not in S_a can only be obtained as an element of the following subset of the vertices of Γ_a:

$$K_a n_w^l \bigcup K_a n_w^{-1} \bigcup_{i=1}^{l-1} \left(K_a n_w^i\right) x_1(1) \bigcup_{i=1}^{l-1} \left(K_a n_w^i\right) x_1(1)^{-1} \bigcup_{i=1}^{l-1} \left(K_a n_w^i\right) h_r(\lambda)$$
$$\bigcup_{i=1}^{l-1} \left(K_a w^i\right) h_r(\lambda)^{-1}.$$

K_a is a subgroup of G so $\left(K_a n_w^i\right) x = K_a n_w^i$ if and only if $n_w^i x n_w^{-i} \in K_a$. We first apply this observation to $x_1(1)$ and $x_1(1)^{-1} = x_1(-1)$. It is easy to see from Lemma 3 that $n_w^i x_1(\pm 1) n_w^{-i}$ is of the form $x_{w^i(r_1)}(\alpha) = x_{i+1}(\alpha)$ for some $\alpha \in GF(q)^*$ if $0 \leq i \leq l-1$. It follows that $n_w^i x_1(\pm 1) n_w^{-i} \in X_{r_{i+1}} \subset K_a$ if $i \neq l-1$.

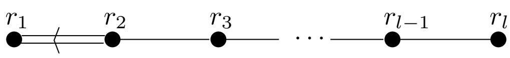
Using the fact that $h_r(\lambda)$ and $h_r(\lambda)^{-1}$ are in the subgroup $\langle X_r, X_{-r}\rangle$ we get that $n_w^i h_{r_1}(\lambda)^{\pm 1} n_w^{-i} \in \langle X_{w^i(r_1)}, X_{-w^i(r_1)}\rangle = \langle X_{r_{i+1}}, X_{-r_{i+1}}\rangle \subset K_a$ if $i \neq l-1$.

Now, $\partial(S_a) \subseteq K_a n_w^l \cup K_a n_w^{-1} \cup K_a n_w^{l-1} x_1(1) \cup K_a n_w^{l-1} x_1(-1) \cup K_a n_w^{l-1} h_{r_1}(\lambda)$ $\cup\, K_a n_w^{l-1} h_{r_1}\left(\lambda^{-1}\right)$. All of these subsets are right cosets of K_a so they have the same cardinality which proves that $|\partial(S_a)| \leq 6\,|K_a|$, while $|S_a| = l\,|K_a|$. ■

Remark 1. *In order to prove Theorem 1 (a) we repeat the previous construction several times. In every single case the chosen generating set of the Cayley graph will consist of a few standard generators of the Chevalley group, an element of the form n_w, where $w = w_1 w_2 \ldots w_l$ is a Coxeter element of the corresponding Weyl group, and an element of the group H. If G is of rank l we will choose a subgroup of G which is isomorphic to a Chevalley group of rank $l-1$ and which is of the same type. The subset of the vertices for which the isoperimetric number is sufficiently small will be a union of cosets of the subgroup of rank $l-1$.*

3.2 B_l

Let G be a Chevalley group of type B_l. The Dynkin diagram of a Chevalley group of type B_l is the following:



It is easy to see from the Dynkin diagram that $w_1(r_2) = r_2 + 2r_1$ and $w_2(r_1) = r_1 + r_2$. Set $w = w_1 \ldots w_l$.

One can see using Lemma 1 that

$$w(r_i) = w_1 w_2 \ldots w_l(r_i) = r_{i+1} \quad \text{for } 2 \leq i \leq l-1. \tag{2}$$

The fundamental roots $r_3, \ldots, r_l$ are orthogonal to r_1. Therefore $w(r_1) = w_1 w_2(r_1) = w_1(r_1 + r_2) = -r_1 + (r_2 + 2r_1) = r_1 + r_2$. We also have that w is linear so using equation (2) we have that if $2 \leq j \leq l-1$, then

$$w(r_1 + r_2 + \ldots + r_j) = w(r_1) + w(r_2) + \ldots + w(r_j) = r_1 + r_2 + r_3 + \ldots + r_{j+1}. \tag{3}$$

Using these observations we conclude that the following picture represents a part of the $\langle w\rangle$-orbit of r_1:

$$r_1 \xrightarrow{w} r_1 + r_2 \xrightarrow{w} r_1 + r_2 + r_3 \xrightarrow{w} \cdots \longrightarrow r_1 + r_2 + \ldots + r_l \xrightarrow{w}$$

This can be formulated as follows:

$$w^i(r_1) = r_1 + r_2 + \ldots + r_{i+1} \text{ for } i = 1, \ldots, l-1. \tag{4}$$

The orbit of $\langle w \rangle$ containing these elements contains $w(r_1 + r_2 + \ldots + r_l)$ as well. It is easy to see that $w_i(r_{i+1} + r_{i+2} + \ldots + r_l) = r_i + r_{i+1} + \ldots + r_l$ if $2 \leq i \leq l-1$. We also have $w_1(r_2) = 2r_1 + r_2$ hence

$$\begin{aligned} w(r_l) &= w_1 \ldots w_{l-1} w_l(r_l) = -w_1 \ldots w_{l-1}(r_l) \\ &= -w_1 \ldots w_{l-2}(r_{l-1} + r_l) = \cdots = -w_1(r_2 + \ldots + r_l) \\ &= -(r_l + \ldots + r_2 + 2r_1). \end{aligned}$$

This implies using equation (3) that

$$w(r_1 + \ldots + r_l) = w(r_1 + \ldots + r_{l-1}) + w(r_l) = -r_1. \tag{5}$$

One can easily describe the remaining elements of the orbit since w is linear.

We also investigate the action of $\langle w \rangle$ on $2r_1 + r_2 + \ldots + r_l$ and $r_2 + \ldots + r_l$. Using equation (5) and the linearity of w we get that $w(2r_1 + r_2 + \ldots + r_l) = w(r_1) + w(r_1 + r_2 + \ldots + r_l) = r_1 + r_2 - r_1 = r_2$. It follows using equation (2) that

$$w^i(2r_1 + r_2 + \ldots + r_l) = r_{i+1} \text{ for } 1 \leq i \leq l-1. \tag{6}$$

One can also prove using equation (4) and equation (6) that

$$w^i(r_2 + \ldots + r_l) = -2(r_1 + r_2 + \ldots + r_{i+1}) + r_{i+1} \text{ for } 1 \leq i \leq l-1. \tag{7}$$

3.2.1 $Char(K) > 2$

Let us assume that $char(K) > 2$.

Lemma 5. *$x_1(1)$, n_w and $h_t(\lambda)$, where $t = 2r_1 + r_2 + \cdots + r_l$, generate the Chevalley group G of type B_l if the characteristic of the underlying field is not 2.*

Proof. It was proved in [18, Theorem 3.11] that $x_1(1)n_w$ and $h_t(\lambda)$ generate the Chevalley group G if $char(K) \neq 2$ and $|K| \neq 3$, and $x_1(1)$ and n_w generate G is $|K| = 3$. ■

We define again a sequence of connected Cayley graphs. Let

$$\Gamma_b = Cay\left(G, \left\{x_1(1), x_1(-1), n_w, n_w^{-1}, h_t(\lambda), h_t(\lambda)^{-1}\right\}\right),$$

where $G = B_l$ and $w = w_1 w_2 \ldots w_l$. Similarly to the previous case let

$$K_b = \langle X_{r_1}, X_{-r_1}, X_{r_2}, X_{-r_2}, \ldots, X_{r_{l-1}}, X_{-r_{l-1}} \rangle$$

and let

$$S_b = \bigcup_{i=0}^{l-2} K_b n_w^i. \tag{8}$$

Lemma 6. $\frac{|\partial(S_b)|}{|S_b|} \leq \frac{4}{l-1}$

Proof. We claim that S_b is the union of pairwise disjoint right cosets of K_b. We only have to show that $n_w^i \notin K_b$ if $1 \leq i \leq l-2$. Straightforward calculation shows using equation (2) that $n_w^i X_{r_{l-i}} n_w^{-i} = X_{r_l}$ if $1 \leq i \leq l-2$. Therefore $X_{r_l} \subset n_w^i K_b n_w^{-i} \neq K_b$ if $1 \leq i \leq l-2$ which gives that $n_w^i \notin K_b$. Thus S_b is the union of $l-1$ pairwise disjoint right cosets of K_b.

Using the definition of the Cayley graph Γ_b we have that $\partial(S_b)$ is a subset of the following set:

$$\bigcup_{i=0}^{l-2}(K_b n_w^i)n_w \bigcup_{i=0}^{l-2}(K_b n_w^i)n_w^{-1} \bigcup_{i=0}^{l-2}(K_b n_w^i)x_1(1) \bigcup_{i=0}^{l-2}(K_b n_w^i)x_1(-1)$$
$$\bigcup_{i=0}^{l-2}(K_b n_w^i)h_t(\lambda) \bigcup_{i=0}^{l-2}(K_b n_w^i)h_t(\lambda)^{-1}.$$

By the definition of S_b the subsets $K_b n_w^i n_w$ are contained in S_b if $0 \leq i \leq l-3$ and $K_b n_w^i n_w^{-1} \subset S_b$ if $1 \leq i \leq l-2$.

Using equation (4) we have $n_w^i x_1(\pm 1) n_w^{-i} = x_{r_1+r_2+\ldots+r_{i+1}}(u)$ for some $u \in K^*$. If $0 \leq i \leq l-2$, then $x_{r_1+r_2+\ldots+r_{i+1}}(u) \in K_b$ since $r_1 + r_2 + \ldots + r_{i+1}$ is in the root system generated by the fundamental roots $r_1, r_2, \ldots, r_{l-1}$ and K_b is the Chevalley group of type B_{l-1} generated by the corresponding root subgroups. Therefore $K_b n_w^i x_1(\pm 1) = K_b n_w^i \subset S_b$ if $0 \leq i \leq l-2$.

The elements $h_t(\lambda)$ and $h_t(\lambda)^{-1} = h_t(\lambda^{-1})$ are in the subgroup generated by X_t and X_{-t}. Equation (6) shows that $n_w^i X_t n_w^{-i} = X_{w^i(t)} = X_{r_{i+1}}$ and by the linearity of w we have $n_w^i X_{-r} n_w^{-i} = X_{-r_{i+1}}$ for $i = 1, 2, \ldots, l-2$. Thus $n_w^i h_t(\lambda) n_w^{-i}$ and $n_w^i h_t(\lambda^{-1}) n_w^{-i}$ are in $\langle X_{r_{i+1}}, X_{-r_{i+1}} \rangle \leq K_b$ if $1 \leq i \leq l-2$.

It follows that $\partial(S_b) \subset K_b n_w^{l-1} \cup K_b n_w^{-1} \cup K_b h_t(\lambda) \cup K_b h_t(\lambda^{-1})$ which gives $\frac{|\partial(S_b)|}{|S_b|} \leq \frac{4|K_b|}{(l-1)|K_b|} = \frac{4}{l-1}$. ■

3.2.2 $Char(K) = 2$

Lemma 7. *$x_s(1)$, $x_{-r_1}(1)$, n_w and $h_t(\lambda)$, where $s = r_2 + \cdots + r_l$ and $t = 2r_1 + r_2 + \cdots + r_l$, generate the Chevalley group G of type B_l if $char(K) = 2$.*

Proof. It was proved in [18, Theorem 3.14] that $x_s(1)x_{-r_1}(1)n_w$ and $h_t(\lambda)$ generate G if $|K| > 2$ and $x_s(1)x_{-r_1}(1)$ and n_w generate G if $|K| = 2$. ■

Let
$$\Gamma_b' = Cay\left(G, \left\{x_s(1), x_{-r_1}(1), n_w^{\pm 1}, h_t(\lambda)^{\pm 1}\right\}\right).$$

The set S_b, which is defined as in equation (8), can be considered as a subset of $V(\Gamma_b')$ so we claim the following.

Lemma 8. $\frac{|\partial(S_b)|}{|S_b|} \leq \frac{5}{l-1}$

Proof. It was proved in Lemma 6 that $|S_b| = (l-1)|K_b|$.

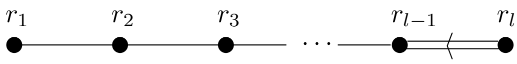
Similarly, the proof of Lemma 6 shows that $K_b n_w^i h_t(\lambda)^{\pm 1} \subset S_b$ if $1 \le i \le l-2$. By the definition of S_b we have $K_b n_w^i n_w \subset S_b$ if $0 \le i \le l-3$ and $K_b n_w^i n_w^{-1} \subset S_b$ if $1 \le i \le l-2$.

Using $w(-r_1) = -w(r_1)$ and equation (4) we get that $n_w^i x_{-r_1}(1) n_w^{-i} \in K_b$ if $0 \le i \le l-2$ since $w^i(r_1) = r_1 + r_2 + \ldots + r_{i+1}$ by equation (4). Hence $K_b n_w^i x_{-r_1}(1) = K_b n_w^i \subset S_b$.

Equation (7) shows that $n_w^i x_s(1) n_w^{-i}$ is in K_b if $1 \le i \le l-2$. Therefore $\left(\cup_{i=1}^{l-2} K_b n_w^i\right) x_s(1) \subset S_b$. Finally, we conclude that $\partial(S_b) \subset K_b n_w^{-1} \cup K_b n_w^{l-1} \cup K_b h_t(\lambda) \cup K_b h_t(\lambda)^{-1} \cup K_b x_s(1)$. ∎

3.3 C_l

The Dynkin diagram is the following in this case:



It can easily be verified using the Dynkin diagram that $w_{l-1}(r_l) = r_l + 2r_{l-1}$ and $w_l(r_{l-1}) = r_{l-1} + r_l$.

Using Lemma 1 one can see that $w(r_i) = r_{i+1}$ for $i = 1, 2, \ldots, l-2$. We also have

$$\begin{aligned} w(r_{l-1}) &= w_1 w_2 \ldots w_l(r_{l-1}) = w_1 w_2 \ldots w_{l-1}(r_l + r_{l-1}) \\ &= w_1 w_2 \ldots w_{l-2}(r_l + r_{l-1}). \end{aligned}$$

Since r_l is orthogonal to the remaining roots $r_1, r_2, \ldots, r_{l-2}$ we have

$$w(r_{l-1}) = r_l + w_1 w_2 \ldots w_{l-2}(r_{l-1}).$$

Since $w_i(r_{i+1} + \ldots + r_{l-1}) = r_i + r_{i+1} + \ldots + r_{l-1}$ for $i = 1 \ldots l-2$ we also have

$$w_1 w_2 \ldots w_{l-2}(r_{l-1}) = w_1 w_2 \ldots w_{l-3}(r_{l-2} + r_{l-1}) = r_1 + \ldots + r_{l-2} + r_{l-1}.$$

This gives $w(r_{l-1}) = r_1 + r_2 + \ldots + r_l$.

Using all these observations we can determine a part of the orbit of $\langle w \rangle$ containing r_1, which is the following:

$$\longrightarrow r_1 \xrightarrow{w} r_2 \xrightarrow{w} \cdots \xrightarrow{w} r_{l-1} \xrightarrow{w} r_l + r_{l-1} + r_{l-2} + \ldots + r_1 \longrightarrow$$

Lemma 9. *$x_1(1)$, n_w and $h_{r_1}(\lambda)$ generate the Chevalley group G.*

Proof. The proof can be found in [18, Theorem 3.11]. ∎

The construction is almost the same as in the case A_l. Let

$$\Gamma_c = Cay\left(G, \left\{x_1(1), x_1(-1), n_w, n_w^{-1}, h_{r_1}(\lambda), h_{r_1}(\lambda)^{-1}\right\}\right).$$

Let

$$K_c = \langle X_{r_2}, X_{-r_2}, X_{r_3}, X_{-r_3}, \ldots, X_{r_l}, X_{-r_l} \rangle$$

and let

$$S_c = \bigcup_{i=0}^{l-2} K_c n_w^i.$$

Lemma 10. $\frac{|\partial(S_c)|}{|S_c|} \leq \frac{6}{l-1}$

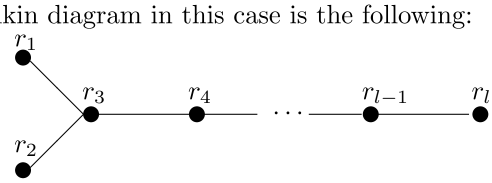
Proof. As in the previous cases, $n_w^{-i} K_c n_w^i$ contains $n_w^{-i} X_{r_{i+1}} n_w^i = X_{r_1}$ for $1 \leq i \leq l-2$ which gives that n_w^i is not in K_c if $1 \leq i \leq l-2$. This proves that $|S_c| = (l-1)\,|K_c|$.

Again, $K_c n_w^i n_w \subset S_c$ if $1 \leq i \leq l-3$ and $K_c n_w^i n_w^{-1} \subset S_c$ if $i \neq 0$.

It is also easy to verify that $n_w^i x_1(1)^{\pm 1} n_w^{-i} = (x_{i+1}(u))^{\pm 1}$ for some $u \in GF(q)^*$. Therefore $n_w^i x_1(1)^{\pm 1} n_w^{-i} \in X_{r_{i+1}}$ and $n_w^i h_{r_1}(\lambda)^{\pm 1} n_w^{-i}$ are in the subgroup generated by $X_{r_{i+1}}$ and $X_{-r_{i+1}}$ for $i = 1, \ldots, l-2$. Thus the elements of the right cosets $K_c n_w^i x_1(1)^{\pm 1}$ and $K_c n_w^i h_{r_1}(\lambda)^{\pm 1}$ are in S_c if $1 \leq i \leq l-2$. This proves that $\partial(S_c) \subseteq K_c n_w^{l-1} \cup K_c n_w^{-1} \cup K_c x_1(1) \cup K_c x_1(1)^{-1} \cup K_c h_{r_1}(\lambda) \cup K_c h_{r_1}(\lambda)^{-1}$, which is the union of 6 right cosets of K_c. Thus $|\partial(S_c)| \leq 6|K_c|$. ■

3.4 D_l

The Dynkin diagram in this case is the following:



Lemma 11. *(a) $x_{r_1}(1)$, n_w and $h_{r_1}(\lambda)$ generate the Chevalley group G if the rank of G is odd.*

(b) $x_{-r_1}(1)$, $x_{r_1}(1)$, $x_3(1)$, n_w and $h_{r_1}(\lambda)$ generate the Chevalley group G if the rank of G is even.

Proof. The proof can be found in [18, Theorem 3.11 and Theorem 3.13]. ■

First, we describe a part of the orbit of $\langle w \rangle$ which contains r_1. The root r_1 is orthogonal to $r_4, \ldots, r_l$ hence $w(r_1) = w_1 w_2 w_3(r_1)$ so we have

$$w_1 w_2 w_3(r_1) = w_1 w_2(r_1 + r_3) = w_1(r_1 + r_2 + r_3) = -r_1 + r_2 + r_3 + r_1 = r_2 + r_3$$

and similarly

$$w(r_2) = w_1 w_2 w_3(r_2) = w_1 w_2(r_2 + r_3) = w_1(-r_2 + r_3 + r_2) = r_3 + r_1.$$

Using Lemma 1 we get $w(r_i) = r_{i+1}$ for $i = 3, \ldots, l-1$. This gives that both $w^i(r_1)$ and $w^i(r_2)$ are of the form

$$r_{i+2} + r_{i+1} + \ldots + r_3 + y, \tag{9}$$

where $y = r_1$ or $y = r_2$.

3.4.1 Odd case

Let us assume that l is odd.

Let

$$\Gamma_d = Cay\left(G, \left\{x_{r_1}(1), x_{r_1}(1)^{-1}, n_w, n_w^{-1}, h_{r_1}(\lambda), h_{r_1}(\lambda)^{-1}\right\}\right).$$

Let

$$K_d = \langle X_{r_1}, X_{-r_1}, X_{r_2}, X_{-r_2}, \ldots, X_{r_{l-1}}, X_{-r_{l-1}}\rangle$$

and let

$$S_d = \bigcup_{i=0}^{l-3} K_d n_w^i.$$

Lemma 12. $\frac{|\partial(S_d)|}{|S_d|} \leq \frac{2}{l-2}$

Proof. It is easy to see that if $0 \leq i \leq l-3$, then $n_w^i x_{r_1}(1)^{\pm 1} n_w^{-i} = x_{w^i(r_1)}(u)^{\pm 1} \in K_d$ for some $u \in GF(q)^*$ since by (9) the root $w^i(r_1)$ is a linear combination with integer coefficients of the fundamental roots $r_1, r_2, \ldots, r_{l-1}$ and similarly $n_w^i h_{r_1}(\lambda)^{\pm 1} n_w^{-i} \in K_d$. It follows that $\partial(S_d) \subseteq K_d n_w^{l-2} \cup K_d n_w^{-1}$.

It remains to show that S_d is the union of $l-3$ pairwise disjoint cosets of K_d. Again, $n_w^i K_d n_w^{-i}$ contains the subgroup $n_w^i X_{r_{l-i}} n_w^{-i} = X_{r_l}$ if $1 \leq i \leq l-3$ which shows that $n_w^i \notin K_d$. ■

3.4.2 Even case

Let us assume that l is even.

Let

$$\Gamma'_d = Cay\left(G, \left\{x_{-r_1}(\pm 1), x_{-r_1}(\pm 1), x_{r_3}(\pm 1), n_w, n_w^{-1}, h_{r_1}(\lambda), h_{r_1}(\lambda)^{-1}\right\}\right).$$

Let

$$K'_d = \langle X_{r_1}, X_{-r_1}, X_{r_2}, X_{-r_2}, \ldots, X_{r_{l-1}}, X_{-r_{l-1}}\rangle$$

and let

$$S'_d = \bigcup_{i=0}^{l-4} K'_d n_w^i.$$

Lemma 13. $\frac{|\partial(S'_d)|}{|S'_d|} \leq \frac{2}{l-3}$

Proof. It is clear that $w^i(-r_1) = -w^i(r_1)$ and hence $w^i(-r_1)$ is in the root system generated by the roots $r_1, r_2, \ldots, r_{l-1}$ if $1 \leq i \leq l-4$. This shows that $n_w^i x_{\pm r_1}(\pm 1) n_w^{-i} = x_{w^i(\pm r_1)}(u) \in K'_d$ for some $u \in GF(q)^*$.

It was proved in Lemma 12 that $n_w^i h_{r_1}(\lambda)^{\pm 1} n_w^{-i} \in K'_d$ if $0 \leq i \leq l-4$. Finally, by Lemma 1 $n_w^i x_{r_3}(\pm 1) n_w^{-i} = x_{r_{3+i}}(t)$ for some $t \in K^*$ which is in K'_d if $0 \leq i \leq l-4$. It follows that $\partial(S'_d) \subseteq K'_d n_w^{l-3} \cup K'_d n_w^{-1}$.

It remains to show that S'_d is the union of $l-3$ pairwise disjoint cosets of K'_d. This is clear since if $1 \leq i \leq l-4$, then $n_w^i K'_d n_w^{-i}$ contains the subgroup X_{r_l} which shows that $n_w^i \notin K'_d$. ■

4 Twisted groups

The twisted groups can be obtained as subgroups of Chevalley groups. In order to define twisted groups we need to find a non-trivial symmetry ρ of the Dynkin diagram. We restrict our attention to those twisted groups which are defined using a symmetry of order 2 and we also assume that the roots in Φ have the same length. It is well known that such a symmetry ρ can be extended to a unique isometry τ of the vector space spanned by Φ. We assume that $Aut(K)$ contains an element f of order 2, where $K = GF(q)$. Then the Chevalley group G has an automorphism of order 2, which we denote by α such that $x_r(k)^\alpha = x_{\overline{r}}(\overline{k})$ for every $r \in \pm\Pi$ and $k \in K$, where $\overline{k} = f(k)$ and $\overline{r} = \tau(r)$. Furthermore, $x_r(k)^\alpha = x_{\overline{r}}(\gamma_r\overline{k})$ for every $r \in \Phi$ and $k \in K$ with $\gamma_r = \pm 1$.

Let U be the subgroup of G generated by the elements $x_r(t)$ for all $r \in \Phi^+$ and $t \in K$ and let V be generated by the elements $x_r(t)$ for all $r \in \Phi^-$ and $t \in K$. The subgroup U^1 is the set of elements $u \in U$ such that $u^\alpha = u$ and similarly $V^1 = \{v \in V \mid v^\alpha = v\}$. The twisted group G^1 is generated by U^1 and V^1. The subgroups H^1 and N^1 are defined as the intersection of G^1 with H and N, respectively, where H and N are defined in Section 2. We denote by W^1 the elements w of the Weyl group W such that $\tau w \tau^{-1} = w$. There is a natural isomorphism of the group W^1 to N^1/H^1 and we denote by n_w^1 an element of $N^1 \leq N$ which corresponds to $w^1 \in W^1$.

The set of positive roots Φ^+ has a partition where the elements of the partition are of the following form:

$$\begin{aligned} Z &= \left\{r \mid r \in \Phi^+ \text{ and } \overline{r} = r\right\} \\ Z &= \left\{r, \overline{r} \mid r \in \Phi^+ \text{and } r + \overline{r} \notin \Phi\right\} \\ Z &= \left\{r, \overline{r}, r + \overline{r} \mid r \in \Phi^+ \text{and } r + \overline{r} \in \Phi\right\}. \end{aligned}$$

We denote by Π^1 the collection of sets which are elements of the partition. For each set Z in the partition there is a unique element $w_Z \in W^1$, which is an element of the subgroup generated by w_r for $r \in Z$, such that $w_Z(Z) = -Z$. These elements are the following:

$$\begin{aligned} &w_Z = w_r \ \text{ if } \ Z = \left\{r \mid r \in \Phi^+ \text{ and } \overline{r} = r\right\} \\ &w_Z = w_r w_{\overline{r}} \ \text{ if } \ Z = \left\{r, \overline{r} \mid r \in \Phi^+ \text{and } r + \overline{r} \notin \Phi\right\} \\ &w_Z = w_{r+\overline{r}} = w_r w_{\overline{r}} w_r \ \text{ if } \ Z = \left\{r, \overline{r}, r + \overline{r} \mid r \in \Phi^+ \text{and } r + \overline{r} \in \Phi\right\}. \end{aligned}$$

Every element of Π^1 can be obtained as $w(Z)$, where $w \in W^1$ and Z contains a fundamental root. Those sets which contain a fundamental root are called fundamental sets. Moreover, W^1 is generated by $\left\{w_Z \mid Z \in \Pi^1\right\}$.

For every $Z \in \Pi^1$ we denote by X_Z the subgroup generated by the root subgroups X_r for $r \in Z$, and we set $X_Z^1 = X_Z \cap G^1$.

4.1 $^2A_{2n-1}$

The fundamental sets in this case are the following:

$$Z_n = \{r_n\}\,,\ Z_i = \{r_i, r_{2n-i}\} \text{ for } 1 \le i \le n-1,$$

and the corresponding elements of the Weyl group W^1 are:

$$w_{Z_n} = w_n, \text{ and } w_{Z_i} = w_i w_{2n-i} \text{ for } 1 \le i \le n-1.$$

We may assume (see [3, p.233]) that the subgroups defined above are of the following form:

$$X_Z^1 = \left\{x_r(t) \mid t = \bar{t}\right\} \text{ if } Z = \{r\}$$
$$X_Z^1 = \left\{x_r(t)x_{\bar{r}}(\bar{t}) \mid t \in K\right\} \text{ if } Z = \{r, \bar{r}\}.$$

Let $n_w^1 = n_{w_1^1} n_{w_2^1} \dots$ and $h_e = h_{r_1}(\lambda)h_{\overline{r_1}}(\overline{\lambda})$, where λ generates the multiplicative group of the finite field $K = GF(q)$. In the following in order to simplify notation we write n_w instead of n_w^1.
We also define $x_e = x_{r_1}(1)x_{r_{2n-1}}(1)$ which is an element of $X_{Z_1}^1$ and which can also be written as $x_{r_1}(1)x_{r_1}(1)^\alpha = x_{r_1}(1)x_{\overline{r_1}}(1)$.

Lemma 14. *x_e, n_w and h_e generate the group G^1.*

Proof. The proof can be found in [18, Theorem 4.1]. ∎

Let
$$\Gamma_e = Cay\left(G, \left\{x_e, x_e^{-1}, n_w, n_w^{-1}, h_e, h_e^{-1}\right\}\right).$$
Let
$$K_e = \langle X_{Z_2}^1, X_{-Z_2}^1, X_{Z_3}^1, X_{-Z_3}^1, \dots, X_{Z_n}^1, X_{-Z_n}^1\rangle$$
and let
$$S_e = \bigcup_{i=0}^{n-2} K_e n_w^i.$$

K_e can be considered as a twisted group which is a subgroup of the Chevalley group generated by the root subgroups $X_{r_2}, X_{-r_2}, \dots, X_{r_{2n-2}}, X_{-r_{2n-2}}$. The corresponding set of fundamental roots is ρ-invariant and we denote by Φ_{2n-3} the root system generated by these roots. The restriction of ρ to the set $\{r_2, r_3, \dots, r_{2n-2}\}$ gives a symmetry of the Dynkin diagram of these roots which extends to an isometry. This isometry is the restriction of τ. This gives that for $Z \in \Pi^1$ the subgroup X_Z^1 is a subgroup of K_e if and only if $Z \subset \Phi_{2n-3}$. Clearly, $h_r(t)$ is in $\langle X_Z^1, X_{-Z}^1\rangle \subset G^1$ if $Z = \{r\}$ with $r = \bar{r}$. If $Z = \{r, \bar{r}\}$, then there is a homomorphism of $SL_2(K)$ onto $\langle X_Z^1, X_{-Z}^1\rangle \subset G^1$ which shows that $x_r(t)x_{\bar{r}}(\bar{t}) \in G^1$ and $h_r(t)h_{\bar{r}}(\bar{t}) \in G^1$.

Conjugating by $n_w^i \in N^1$ we get the following:

$$\begin{aligned} n_w^{-i} X_Z^1 n_w^i &= n_w^{-i}(X_Z \cap G^1)n_w^i = n_w^{-i} X_Z n_w^i \cap n_w^{-i} G^1 n_w^i = X_{w^{-i}(Z)} \cap G^1 \\ &= X_{w^{-i}(Z)}^1. \end{aligned} \tag{10}$$

Lemma 15. $\frac{|\partial(S_e)|}{|S_e|} \leq \frac{6}{n-1}$

Proof. We claim that S_e is the union of $n-1$ disjoint subsets. $K_e n_w^j = K_e n_w^{j'}$ if and only if $n_w^{j-j'} \in K_e$ so we have to show that $n_w^i \notin K_e$ if $1 \leq i \leq n-2$. We claim that $w^i(r_1) = r_{i+1}$ if $1 \leq i \leq n-2$. If $k \leq n-3$, then

$$w(r_k) = w_1 w_{2n-1} \dots w_k w_{2n-k} w_{k+1}(r_k)$$

since r_k is orthogonal to r_j if $j \geq k+2$. Therefore

$$\begin{aligned} w(r_k) &= w_1 w_{2n-1} \dots w_k(r_k + r_{k+1}) \\ &= w_1 w_{2n-1} \dots w_{k-1}(r_{k+1}) = r_{k+1} \end{aligned}$$

since r_{k+1} is orthogonal to the roots $r_{2n-k}, \dots, r_{2n-1}$ and r_{k+1} is orthogonal to $r_1, \dots, r_{k-1}$. It follows that $w^{-i}(Z_{i+1}) = Z_1$ and hence by equation (10) $X^1_{Z_1} \subset n_w^{-i} K_e n_w^i$ if $1 \leq i \leq n-2$. This proves that $n_w^i \notin K_e$ if $1 \leq i \leq n-2$ hence $|S_e| = (n-1)\,|K_e|$.

It is easy to see that S_e contains $K_e n_w^i n_w$ if $i = 0, 1, \dots, n-3$ and S_e contains $K_e n_w^i n_w^{-1}$ if $i = 1, 2, \dots, n-2$.

We use again the fact that $K_e n_w^i g = K_e n_w^i$ if and only if $n_w^i g n_w^{-i} \in K_e$. Since $n_w^i x_{r_1}(1) n_w^{-i} = x_{w^i(r_1)}(\xi)$ for some $\xi \in K$ and $x_e = x_{r_1}(1) x_{r_1}(1)^\alpha$ we have

$$\begin{aligned} &n_w^i x_{r_1}(1) x_{r_1}(1)^\alpha n_w^{-i} = n_w^i x_{r_1}(1) n_w^{-i} n_w^i x_{r_1}(1)^\alpha n_w^{-i} \\ =&n_w^i x_{r_1}(1) n_w^{-i} (n_w^i x_{r_1}(1) n_w^{-i})^\alpha = x_{w^i(r_1)}(\xi) x_{w^i(r_1)}(\xi)^\alpha = x_{r_{i+1}}(\xi) x_{r_{i+1}}(\xi)^\alpha. \end{aligned}$$

This shows that $n_w^i x_e n_w^{-i} \in X^1_{Z_{i+1}}$ which proves that if $i = 1, 2, \dots, n-2$, then $n_w^i x_e^{\pm 1} n_w^{-i} \in K_e$ and hence $K_e n_w^i x_e^{\pm 1} = K_e n_w^i$ since $Z_{i+1} \subset \Phi_{2n-3}$.

We also have $n_w^i h_{r_1}(\lambda) h_{\overline{r_1}}(\overline{\lambda}) n_w^{-i} = h_{r_{i+1}}(\theta) h_{w^i(\overline{r_1})}(\theta')$ for some θ,$\theta' \in K$. Using the fact that $w \in W^1$ we have $w^i(\overline{r_1}) = \overline{w^i(r_1)}$ so $h_{r_{i+1}}(\theta) h_{w^i(\overline{r_1})}(\theta') = h_{r_{i+1}}(\theta) h_{\overline{r_{i+1}}}(\theta')$. Clearly, $n_w^i h_e n_w^{-i} \in H^1$. Thus $\theta' = \overline{\theta}$ and $n_w^i h_e^{\pm 1} n_w^{-i} = \left(h_{r_{i+1}}(\theta) h_{\overline{(r_{i+1})}}(\overline{\theta}) \right)^{\pm 1} \in K_e$ since $r_{i+1} \in \Phi_{2n-3}$ if $i = 1, \dots, n-2$. This proves that $K_e n_w^i h_e^{\pm 1} = K_e n_w^i$ if $i = 1, \dots, n-2$ and hence $\partial(S_e) \subset K_e n_w^{n-1} \cup K_e n_w^{-1} \cup K_e x_e \cup K_e x_e^{-1} \cup K_e h_e \cup K_e h_e^{-1}$, finishing the proof of Lemma 15. ∎

4.2 ^2D_n

The fundamental sets in this case are the following:

$$Z_1 = \{r_1, r_2\}\,,\ Z_i = \{r_{i+1}\} \text{ for } 2 \leq i \leq n-1,$$

and the corresponding elements of the Weyl group W^1 are:

$$w_{Z_1} = w_1 w_2, \text{ and } w_{Z_i} = w_{i+1} \text{ for } 2 \leq i \leq n-1.$$

Let $n_w = n_{w_1^1} n_{w_2^1} \dots n_{w_{n-1}^1}$ and $h_f = h_{r_1}(\lambda) h_{\overline{r_1}}(\overline{\lambda})$, where λ generates K^*. We also define $x_f = x_{r_1}(1) x_{r_2}(1)$ which can also written as $x_{r_1}(1) x_{r_1}(1)^\alpha = x_{r_1}(1) x_{\overline{r_1}}(1)$.

Lemma 16. *x_f, n_w and h_f generate the group G^1.*

Proof. The proof can be found in [18, Theorem 4.1]. ■

Let

$$\Gamma_f = Cay\left(G, \left\{x_f, x_f^{-1}, n_w, n_w^{-1}, h_f, h_f^{-1}\right\}\right).$$

Let

$$K_f = \langle X^1_{Z_1}, X^1_{-Z_1}, X^1_{Z_2}, X^1_{-Z_2}, \ldots, X^1_{Z_{n-2}}, X^1_{-Z_{n-2}}\rangle$$

and let

$$S_f = \bigcup_{i=0}^{n-3} K_f n_w^i.$$

We denote by Φ_{n-1} the root system generated by the fundamental roots $r_1, r_2, \ldots, r_{n-1}$.

Lemma 17. $\frac{|\partial(S_f)|}{|S_f|} \leq \frac{2}{n-2}$

Proof. The Coxeter element in this case is exactly the same as in Section 3.4. This gives that $n_w^i(r_{n-i}) = r_n$ for $0 \leq i \leq n-3$. The fundamental sets $Z_2, Z_3, \ldots, Z_{n-1}$ consist of only one element thus $n_w^i S_f n_w^{-i}$ contains $X^1_{w^i(Z_{n-1-i})} = X_{w^i(r_{n-i})} = X_{r_n} = X^1_{Z_{n-1}}$ if $1 \leq i \leq n-3$ since S_f contains X^1_{n-i}. This proves that if $1 \leq i \leq n-3$, then $n_w^i \notin K_f$. Thus S_f is the union of $n-2$ disjoint subsets of the same cardinality. Therefore $|S_f| = (n-2)\,|K_f|$.

Using the definiton of S_f one can see that $K_f n_w^i n_w \subset S_f$ if $i = 0, 1, \ldots, n-4$ and $K_f n_w^i n_w^{-1} \subset S_f$ if $i = 1, \ldots, n-3$.

The elements $n_w^i x_f n_w^{-i}$ are of the form $x_r(t)x_{\overline{r}}(\pm\overline{t})$ for some $r \in \Phi$ and $t \in K^*$. In order to prove that these elements are in K_f for $i = 0, 1, \ldots, n-3$ we only have to show that $r \in \Phi_{n-1}$. Using the fact that the Coxeter element in this case is the same as in Section 3.4 we have that both $w^i(r_1)$ and $w^i(r_2)$ are of the form $r_1 + r_3 + r_4 + \ldots + r_{i+1}$ or $r_2 + r_3 + r_4 + \ldots + r_{i+1}$. These roots are clearly in the root system generated by the fundamental roots $r_1, r_2, \ldots, r_{l-1}$ if $i \leq n-2$. This proves that $n_w^i x_f^{\pm} n_w^{-i}$ is in K_f if $0 \leq i \leq n-3$ and hence $S_f x_f^{\pm} \subset S_f$.

Similarly, the elements $n_w^i h_f n_w^{-i}$ are of the form $h_r(t)h_{\overline{r}}(\overline{t})$ for some $r \in \Phi$ and $t \in K^*$ and it is easy to see that $r \in \Phi_{n-1}$ if $0 \leq i \leq n-3$. This proves that $n_w^i h_f^{\pm} n_w^{-i}$ is in K_f if $0 \leq i \leq n-3$ and hence $S_f h_f^{\pm} \subset S_f$.

Therefore $\partial(S_f) \subseteq K_f n_w^{n-2} \cup K_f n_w^{-1}$, which shows that $\frac{|\partial(S_f)|}{|S_f|} \leq \frac{2|K_f|}{(n-2)|K_f|}$, finishing the proof of Lemma 17. ■

4.3 $^2A_{2n}$

The fundamental sets are the following:

$$Z_1 = \{r_n, r_{n+1}, r_n + r_{n+1}\}, \;\; Z_i = \{r_{n+1-i}, r_{n+i}\} \text{ for } 2 \leq i \leq n.$$

Let $n_w^1 = n_{w_1^1} n_{w_2^1} \ldots n_{w_n^1}$ and $h_g = h_{r_n}(\lambda) h_{\overline{r_n}}(\overline{\lambda})$, where λ generates K^*. We also define $x_g = x_{r_n}(1) x_{r_{n+1}}(1) x_{r_n + r_{n+1}}(k)$ with $k + \overline{k} = 1$.

Lemma 18. *x_g, n_w and h_g generate the group G^1.*

Proof. The proof can be found in [18, Theorem 4.1]. ■

Let
$$\Gamma_g = Cay\left(G, \left\{x_g, x_g^{-1}, n_w, n_w^{-1}, h_g, h_g^{-1}\right\}\right).$$
Let
$$K_g = \langle X^1_{Z_1}, X^1_{-Z_1}, X^1_{Z_2}, X^1_{-Z_2}, \ldots, X^1_{Z_{n-1}}, X^1_{-Z_{n-1}} \rangle$$
and let
$$S_g = \bigcup_{i=0}^{n-2} K_g n_w^i.$$

Lemma 19. $\frac{|\partial(S_g)|}{|S_g|} \le \frac{2}{n-1}$

Proof. First, we show that S_g is the union of $n-1$ disjoint subsets of the same cardinality. It is enough to show that $n_w^i \notin K_g$ for $i = 1, \ldots, n-2$. This will be done by proving that $X^1_{Z_n}$ is contained in $n_w^i K_g n_w^{-i}$. Using equation (10) we only have to show that $w^i(Z_{n-i}) = Z_n$ for $i = 1, \ldots n-2$.

The fundamental root r_{k+1} is contained in Z_{n-k}. Let us assume that $1 \le k \le n-2$.

$$\begin{aligned} w(r_{k+1}) &= w_n w_{n+1} w_n w_{n-1} w_{n+2} \ldots w_1 w_{2n}(r_{k+1}) \\ &= w_n w_{n+1} w_n w_{n-1} w_{n+2} \ldots w_{k+1} w_{2n-k} w_k(r_{k+1}) \end{aligned}$$

since r_{k+1} is orthogonal to the roots r_j if $j > n$ or $j < k-1$. Clearly, $w_{k+1} w_{2n-k} w_k(r_{k+1}) = r_k$ so

$$w(r_{k+1}) = w_n w_{n+1} w_n \ldots w_{k+2} w_{2n-k-1}(r_k) = r_k$$

since the remaining reflections fix r_k.

One can see by induction that $w^i(r_{i+1}) = r_1$ for $i = 1, \ldots n-2$ and since $w \in W^1$ we have $w^i(\overline{r_{i+1}}) = \overline{w^i(r_{i+1})} = r_{2n}$ and hence $w^i(Z_{n-i}) = Z_n$. This proves that for $i = 1, \ldots, n-2$ the subgroup $n_w^i(K_g)n_w^{-i}$ contains $X^1_{Z_n}$. Therefore $|S_g| = (n-1)\,|K_g|$.

The definition of S_g shows that $K_g n_w^i n_w \subset S_g$ if $i \neq n-2$ and $K_g n_w^i n_w^{-1} \subset S_g$ if $i \neq 0$. It remains to investigate the elements of the form $n_w^i x_g^{\pm} n_w^{-i}$ and $n_w^i h_g^{\pm} n_w^{-i}$.

We claim that $w^i(r_n) = r_n + r_{n-1} + \ldots + r_{n-i}$ if $i \le n-2$. Using the orthogonality of the fundamental roots r_j, r_k, where $|j-k| \ge 2$ we get the following:

$$\begin{aligned} w(r_n) &= w_n w_{n+1} w_n w_{n-1} w_{n+2} \ldots w_1 w_{2n}(r_n) \\ &= w_n w_{n+1} w_n w_{n-1}(r_n) = w_n w_{n+1}(r_{n-1}) = r_{n-1} + r_n. \end{aligned} \tag{11}$$

Similarly, if $1 \le k \le n-2$, then

$$\begin{aligned} w(r_{n-k}) &= w_n w_{n+1} w_n w_{n-1} w_{n+2} \ldots w_1 w_{2n}(r_{n-k}) \\ &= w_n w_{n+1} w_n \ldots w_{n-k} w_{n+k+1} w_{n-k-1}(r_{n-k}) \\ &= w_n w_{n+1} w_n \ldots w_{n-k+1}(r_{n-k-1}) = r_{n-k-1}. \end{aligned} \tag{12}$$

Since w is linear we get using (11) and (12) that

$$w^i(r_n) = r_n + r_{n-1} + \ldots + r_{n-i}. \tag{13}$$

From equation (13) one can see that if $i = 0, \ldots, n-2$, then both r_1 and r_{2n} are orthogonal to $w^i(r_n)$, and similarly r_1 and r_{2n} are orthogonal to $w^i(r_{n+1}) = w^i(\overline{r_n}) = \overline{w^i(r_n)} = r_{n+i+1}$. This shows that for

$$w' = w_n w_{n+1} w_n w_{n-1} w_{n+2} \ldots w_2 w_{2n-1}$$

we have $w^i(r_n) = (w')^i(r_n)$ and $w^i(r_{n+1}) = (w')^i(r_{n+1})$. Therefore $w^i(r_n + r_{n+1}) = (w')^i(r_n + r_{n+1})$. Moreover, $n_w^i x_g n_w^{-i} = n_{w'}^i x_g n_{w'}^{-i}$ and $n_w^i h_g n_w^{-i} = n_{w'}^i h_g n_{w'}^{-i}$.

Clearly, $n_{w'} \in K_g$ and hence the elements $n_{w'}^i x_g^{\pm} n_{w'}^{-i}$ and $n_{w'}^i h_g^{\pm} n_{w'}^{-i}$ are in K_g if $i = 0, 1, \ldots, n-2$. ■

In order to finish the proof of Theorem 1 we have to verify that for those sets S for which the boundary $\partial(S)$ is relatively small we have $|S| \leq \frac{|G|}{2}$. The order of the investigated simple groups is the following:

$$\begin{array}{rc}
A_l(q): & \frac{1}{(l+1,q-1)} q^{\frac{l(l-1)}{2}} \prod_{i=1}^{l} \left(q^{i+1} - 1\right) \\
B_l(q): & \frac{1}{(2,q-1)} q^{l^2} \prod_{i=1}^{l} \left(q^{2i} - 1\right) \\
C_l(q): & \frac{1}{(2,q-1)} q^{l^2} \prod_{i=1}^{l} \left(q^{2i} - 1\right) \\
D_l(q): & \frac{1}{(4,q^l-1)} q^{\frac{l(l-1)}{2}} \prod_{i=1}^{l} \left(q^{2i} - 1\right) \\
{}^2A_l(q^2): & \frac{1}{(l+1,q+1)} q^{\frac{l(l-1)}{2}} \prod_{i=1}^{l} \left(q^{i+1} - (-1)^{i+1}\right) \\
{}^2D_l(q^2): & \frac{1}{(4,q^l+1)} q^{l(l-1)} \left(q^l + 1\right) \prod_{i=1}^{l} \left(q^{2i} - 1\right)
\end{array}$$

It is easy to see that such a simple group can not have a subgroup of index at most $2l$, finishing the proof of Theorem 1.

5 Identification

In this section we give explicit generators of the groups that we investigated in Sections 3 and 4. We also show how to find the subsets of the vertices S for which $\partial(S)$ is relatively small. We only handle the case of special linear groups which can easily be transformed to the case of the projective special linear groups which is clearly the easiest one. This example includes the original idea which was extended to several different series of simple groups. In order to show the simplicity of the original construction we forget about the machinery which was built up before.

Let

$$A_l = \begin{pmatrix} 1 & 1 & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix},$$

where $A_l \in GF(q)^{(l+1)\times(l+1)}$. Let

$$B_l = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 & (-1)^l \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & 0 \end{pmatrix}.$$

We denote by C_l the diagonal matrix $diag(\frac{1}{\lambda}, \lambda, 1, 1, \dots, 1) \in GF(q)^{(l+1)\times(l+1)}$, where λ generates $GF(q)^*$.

We denote by $e_{i,j}$ the matrix with 1 in the (i,j)-th position and zeros everywhere else and let $T_{i,j}(\delta) = I + \delta e_{i,j}$, where I denotes the identity matrix and $\delta \in K$. Using this notation we can write $A_l = T_{1,2}(1)$.

The standard generator $x_{r_1}(1)$ of the Chevalley group given in Section 3.1 corresponds to the matrix A_l and the Coxeter element n_w can be identified with B_l. Finally, C_l plays the role of $h_{r_1}(\lambda)$.

Clearly, $T_{i,j}(\alpha)T_{i,j}(\beta) = T_{i,j}(\alpha+\beta)$ and $[T_{i,j}(\alpha), T_{j,k}(\beta)] = T_{i,k}(\alpha\beta)$ if $i \neq k$, where $[g,h] = g^{-1}h^{-1}gh$ denotes the commutator of g and h.

Lemma 20. *For every $l \in \mathbb{N}$ the set $\{A_l, B_l, C_l\}$ forms a generating set of $SL(l+1,q)$.*

Proof. We fix the size of the matrices and hence we can write $A = A_l$, $B = B_l$ and $C = C_l$. Let $H = \langle A, B, C\rangle$. It is enough to verify that $T_{i,j}(\delta) \in H$ for every $i \neq j$ and $\delta \in GF(q)$.

It is easy to see that $A^{C^k} = T_{1,2}(1)^{C^k} = T_{1,2}(\lambda^{2k})$. Using $T_{1,2}(\alpha)T_{1,2}(\beta) = T_{1,2}(\alpha+\beta)$ we get that $T_{1,2}(\delta) \in \langle A, C\rangle \leq H$ for every $\delta \in GF(q)$. For $i \neq j$ we have $B^k T_{i,j}(\delta)B^{-k} = T_{i+k,j+k}(\pm\delta)$, where the indices are taken modulo $l+1$ and hence $T_{i,i+1}(\delta) \in H$ for every $1 \leq i \leq l$ and for every $\delta \in GF(q)$. This implies that for every $1 < l \leq l+1$ and for every $\delta \in GF(q)$

$$[\dots[[T_{1,2}(\delta), T_{2,3}(1)], T_{3,4}(1)]\dots, T_{k-1,k}(1)] = T_{1,k}(\delta) \in H.$$

Using again the fact that $B^k T_{1,l}(\delta)B^{-k} = T_{1+k,l+k}(\pm\delta)$ we get that $T_{i,j}(\delta) \in H$ for every $i \neq j$ and for every $\delta \in GF(q)$. ■

Let

$$S_0 = \left\{ \begin{pmatrix} D & 0 \\ 0 & 1 \end{pmatrix} \in SL(l+1,q) \middle| D \in SL(l,q) \right\}.$$

For every $1 \leq i \leq l$ we define

$$S_i = S_0 B^i.$$

Finally, let

$$S = \bigcup_{i=0}^{l-1} S_i.$$

It is easy to see that $|S| < \frac{|SL(l+1,q)|}{2}$ if $l \geq 1$.

Lemma 21. $\frac{|\partial(S)|}{|S|} \leq \frac{6}{l}$

Proof. Every element of S has exactly l columns with 0 in the last row, and exactly 1 column with 0 in the first l rows and 1 in the last row. The sets S_i are pairwise disjoint since an invertible matrix can not have a column with only zero entries. Furthermore, they all have the same cardinality since S_0 is a subgroup of $SL(l+1,q)$ and S_i are right cosets of S_0 in $SL(l+1,q)$.

It is easy to see that $SB \setminus S \subseteq S_0B^l = S_l$ and $SB^{-1} \setminus S \subseteq S_0B^{-1}$. The remaining elements of $\partial(S)$ are of the form MA, MC and MA^{-1}, MC^{-1} where $M \in S$.

Let us assume that $M \in S_i$. Then

$$M = \begin{pmatrix} D & 0 & D' \\ 0 & 1 & 0 \end{pmatrix}$$

for some $D \in GF(q)^{l,l-i}$ and $D' \in GF(q)^{l,i}$. Multiplying a matrix M by A or A^{-1} from the right only modifies the second column of M. Therefore if $M \in S_i$ with $i \neq l, l-1$, then it is easy to see that $MA, MA^{-1} \in S_i$.

Multiplying a matrix M by C or C^{-1} from the right only modifies the first and the second columns of M thus if $M \in S_i$ with $i \neq l, l-1$, then $MC^{\pm 1} \in S_i$.

This gives that $\partial(S) \subseteq S_l \cup S_0B^{-1} \cup S_{l-1}A \cup S_{l-1}A^{-1} \cup S_{l-1}C \cup S_{l-1}C^{-1}$ since $S = \cup_{i=0}^{l-1} S_i$.

■

Acknowledgement

The author is grateful to László Pyber for many valuable suggestions during the research.

References

[1] E. Breuillard, B. Green, T. Tao, Suzuki groups as expanders, Groups Geom. Dyn. 5, (2011) 281-299.

[2] E. Breuillard, B. Green, and T. Tao, Approximate subgroups of linear groups, Geom. Funct. Anal. 21 (4), (2011) 774-819.

[3] R. W. Carter, Simple groups of Lie type, John Wiley & Sons, New York, Reprint of the 1972 original; A Wiley-Interscience Publication (1989).

[4] H. A. Helfgott. Growth and generation in $SL_2(Z/pZ)$, Ann. of Math. (2), 167 (2), (2008) 601-623.

[5] M. Kassabov, Universal lattices and unbounded rank expanders, Invent. Math. 170, (2007) no. 2, 297-326.

[6] M. Kassabov, Symmetric groups and expander graphs, Invent. Math. 170, (2007) no. 2. 327-354.

[7] M. Kassabov, A. Lubotzky, N. Nikolov, Finite Simple Groups as Expanders, Proc. Natl. Acad. Sci. USA 103, (2006) no. 16, 6116-6119.

[8] M. Kassabov, N. Nikolov, Universal lattices and property tau, Invent. Math. 165, (2006) no. 1, 209-224.

[9] M. Kassabov, R. Riley, Diameters of Cayley graphs of Chevalley groups, Eur. J. Comb. 28 (3), (2007) 791-800.

[10] A. Lubotzky, Discrete groups, expanding graphs and invariant measures, with an appendix by J. D. Rogawski, Reprint of the 1994 edition. Modern Birkhauser Classic. Bikrhauser Verlag, Basel, (2010).

[11] A. Lubotzky, Expander Graphs in Pure and Applied Mathematics, Bull. Amer. Math. Soc. 49, (2012) 113-162.

[12] A. Lubotzky, Finite simple groups of Lie type as expanders, J. Eur. Math. Soc. 13, (2011) 1331-1341.

[13] A. Lubotzky, A. Zuk, On Property (τ), monograph in preparation.

[14] N. Nikolov, A product decomposition for the classical quasisimple groups, J. Group Theory 10, (2007) 43-53.

[15] Ch. E. Praeger, L. Pyber, P. Spiga, E. Szabó, Graphs with automorphism groups admitting composition factors of bounded rank, Proc. Amer. Math. Soc. 140 (7), (2012) 2307- 2318.

[16] L. Pyber, E. Szabó, Growth in finite simple groups of Lie type of bounded rank, Submitted, Available at arxiv.org: 1005.1881.

[17] P. Spiga. Two local conditions on the vertex stabiliser of arc-transitive graphs and their effect on the Sylow suubgroups, J. Group Theory 15 (1), (2012) 23-35.

[18] R. Steinberg, Generators for simple groups, Canad. J. Math. 14, (1962) 277-283.