Balanced $0,1$-words and the Galois group of $(x+1)^n - \lambda x^p$

L.Glebsky

November 15, 2011

Abstract

We study the number of $0,1$-words where the fraction of 0 is "almost" fixed for any initial subword. It turns out that this study use and reveal the structure of the Galois group (the monodromy group) of the polynomials $(x+1)^n - \lambda x^p$. (p is not necessary a prime here.)

1 Introduction and formulation of the main results

We need some notations. Let $w \in \{0,1\}^*$. By $|w|$ we denote the length of w ($|w_1 w_2 \dots w_n| = n$). By $|w|_0$ we denote the number of zeros in w ($|w_1 w_2 \dots w_n|_0 = |\{i \,:\, w_i = 0\}|$). Similarly, $|w|_1$ is the number of 1 in w. For $k \in \mathbb{N}$, $k \le |w|$ let $w[: k] = w_1 w_2 \dots w_k$ be the prefix of length k. Generally, $w[l : k] = w_l, w_{l+1}, \dots, w_k$. For $n, r \in \mathbb{N}$, $0 \le \alpha \le 1$ let

$$B_{n,\alpha,r} = \{w \in \{0,1\}^n \;:\; \forall k \le n \;\; \alpha k - r < |\, w[: k] \,|_0 \le \alpha k + r\}.$$

The condition $\alpha k - r < |\, w[: k] \,|_0 \le \alpha k + r$ is equivalent to the condition $|\, w[: k] \,|_0 - \lfloor \alpha k \rfloor \in \{-r+1, -r+2, \dots, r\}$. We often use the last conditions as more manageable. The elements of $B_{n,\alpha,r}$ is said to be (α, r)-balanced words of length n. We are interesting in $|B_{n,\alpha,r}|$, or, precisely, in growth exponent

$$e_{\alpha,r} = \lim_{n\to\infty} \sqrt[n]{|B_{n,\alpha,r}|}. \tag{1}$$

In Section 2 we calculate $B_{n,\alpha,r}$ for rational α. It implies the existence of the limit (1) for rational α. In Section 3 we prove that the limit exists for all $\alpha \in (0,1)$ and that $e_{\alpha,r}$ is continuous in α, uniformly with respect to r.

Let us define

$$\tilde{B}_{n,\alpha,r} = \{w \in \{0,1\}^n \;:\; \alpha n - r < |w|_0 \le \alpha n + r\}.$$

It follows from study of generating function (as in [3, 4, 5]) that the growth exponent

$$\tilde{e}_\alpha = \lim_{n\to\infty} \sqrt[n]{|\tilde{B}_{n,\alpha,r}|}.$$

is independent of r and $\tilde{e}_\alpha = \left(\frac{1}{\alpha}\right)^\alpha \left(\frac{1}{1-\alpha}\right)^{1-\alpha}$. It is obvious that $B_{n,\alpha,r} \subset \tilde{B}_{n,\alpha,r}$ and

$$e_{\alpha,r} \le \tilde{e}_\alpha. \tag{2}$$

In the paper we show by calculation that

$$\lim_{r\to\infty} e_{\alpha,r} = \tilde{e}_\alpha = \left(\frac{1}{\alpha}\right)^\alpha \left(\frac{1}{1-\alpha}\right)^{1-\alpha}. \tag{3}$$

I was not able to find direct combinatorial argument for this limit.

It is interesting that there is a relation of our results with Galois group $\mathrm{Gal}(P, \mathbb{C}(\lambda))$ of polynomial $P = (x+1)^n - \lambda x^p$. In order to establish Limit (3) we use the fact that $\mathrm{Gal}(P, \mathbb{C}(\lambda))$ contains a cyclic permutation of length n. Then, using the combinatorial inequality (2), we show that $\mathrm{Gal}(P, \mathbb{C}(\lambda)) = S_n$ for relatively prime n and p. Let us finish the introduction by repeating the main results of the paper:

- The convergence of r.h.s of Eq.1 is proved.
- The limit of Eq.3 is proved.
- The equality $\mathrm{Gal}(P, \mathbb{C}(\lambda)) = S_n$ is proved for relatively prime n and p. If $gcd(n,p) = k$ then $(S_{n/t})^t$ is a normal subgroup of $\mathrm{Gal}(P, \mathbb{C}(\lambda))$ and $\mathrm{Gal}(P, \mathbb{C}(\lambda))/(S_{n/t})^t$ is a cyclic group of order t.

The questions discussed in the paper appear during the investigation of directional complexity and entropy for lift mappings initiated by V. Afraimovich and M. Courbage. The author is thankful to them for the problem and useful discussions. As a reader may see we don't touch the lift mappings in the present paper for it will be discussed in [1]. I believe also that the combinatorial problem is interesting for its own sake.

2 Estimation of $|B_{n,\alpha,r}|$ for rational α

In order to calculate $|B_{n,\alpha,r}|$ we define a vector $b(n) = (b_1, b_2, \dots, b_{2r})^t \in \mathbb{R}^{2r}$, $b_j(n) = |\{w \in B_{n,\alpha,r} \ : |w|_0 - \lfloor \alpha n \rfloor = j - r\}|$. Clearly, $|B_{n,\alpha,r}| = \sum\limits_j b_j(n)$ and $b_r(0) = 1$, $b_j(0) = 0$ for $j \neq r$. Let

$$N_+ = \begin{pmatrix} 0 & 0 & \dots & \dots & 0 \\ 1 & 0 & \dots & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & 1 & 0 \end{pmatrix}, \quad N_- = N_+^t$$

be a low and upper 0-Jordan cells and E be the unit matrix. One may check that $b(n+1) = (E+N_+)b(n)$, if $\lfloor \alpha(n+1) \rfloor = \lfloor \alpha n \rfloor$, and $b(n+1) = (E+N_-)b(n)$, if $\lfloor \alpha(n+1) \rfloor = \lfloor \alpha n \rfloor + 1$. So, at list for a rational $\alpha = p/q$ the problem of finding $e_{p/q,r}$ may be reduced to finding the maximal eigenvalue $e_{\max}$ of M_{p+q}, where $M_0 = E$ and $M_{n+1} = (E+N_+)M_n$, if $\lfloor \alpha(n+1) \rfloor = \lfloor \alpha n \rfloor$, and $M_{n+1} = (E+N_-)M_n$, if $\lfloor \alpha(n+1) \rfloor = \lfloor \alpha n \rfloor + 1$. Notice, that the matrix M_{p+q} is nonnegative irreducible primitive matrix[1] (if $p, q \neq 0$). So, the Perron-Frobenius theorem implies that

$$e_{\max} = e_{\alpha,r}^{p+q}. \tag{4}$$

Let $e_1 = (1, 0, \dots, 0)^t$, $e_2 = (0, 1, \dots, 0)^t$,...,$e_j = (0, \dots, 0, 1, 0, \dots)^t$ (the one on j-th place). One can check that $N_- e_j = e_{j-1}$, for $j > 1$ and $N_+ e_j = e_{j+1}$, for $j < 2r$. Now notice, that for $p < j \leq 2r - q$ one has $N_-^{p_1} N_+^{q_1} \dots N_-^{p_k} N_+^{q_k} e_j = e_{j-p+q}$, where $p = p_1 + p_2 + \dots + p_k$ and $q = q_1 + \dots + q_k$. So, the result is independent of the exact order N_- and N_+ (the matrices N_- and N_+ almost commute in some sense.) We know that

$$M_{p+q} = (E + N_-)^{p_1} (E + N_+)^{q_1} \dots (E + N_-)^{p_k} (E + N_+)^{q_k}. \tag{5}$$

It follows that for $p < j \leq 2r - q$ the coefficients $M_{k,j}$ depend only on $p = p_1 + \dots + p_k$ and $q = q_1 + \dots + q_k$. Notice that $M_{k,j} = 0$ if $j \notin \{k - q, \dots, k + p\}$. Put $n = p + q$. So, there exist two submatrices $S_u \in Mat_{q \times n}$ and $S_d \in Mat_{p \times n}$ whose coefficients does depend on the exact order of the multipliers in Eq.5. A simple calculation shows $M_{k,j} = C_{k-j+p}^{p+q}$ if $(k, j) \notin \{1, \dots, q\} \times \{1, \dots, n\} \cup \{2r - p, \dots, 2r\} \times \{2r - n, \dots, 2r\}$. So the matrix M looks like

$$\begin{pmatrix} & & & & & & 0 & \dots & 0 \\ & S_u & & \dots & 0 & \dots & \dots & \dots & \dots \\ & & & & & & 0 & \dots & 0 \\ 0 & \dots & 0 & & & & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & C_{k-j+p}^{p+q} & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & & & & 0 & \dots & 0 \\ 0 & \dots & 0 & & & & & & \\ \dots & \dots & \dots & \dots & 0 & \dots & & S_d & \\ 0 & \dots & 0 & & & & & & \end{pmatrix}$$

[1] It is an oscillation matrix [2] and all its eigen-values are simple and positive

Recall that the matrix M depends on p, q and r and $M \in Mat_{2r\times 2r}$. Some times we write this dependence explicitly (for example, $M(r)$). Recall that $n = p + q$.

Theorem 1. *Let $0 \le \lambda_1 < \lambda_2 \le \frac{n^n}{p^p q^q}$. Then the number of spectral points of $M(r)$ on (λ_1, λ_2) goes to infinity as $r \to \infty$.*

The theorem immediately imply

Corollary 1. *Let $\alpha(r)$ be the maximal eigenvalue of $M(r)$. Then $\inf \lim \alpha(r) \ge \tilde{e}^n_\alpha$. With Inequality (2) and Eq.4 it proves Limit (3) for rational α.*

In the next section we show how to manage irrational α. We postpone the proof of Theorem 1 up to Section 6 as we need some technical results.

3 Estimates for irrational α

Let us start listing some simple facts about $B_{n,\alpha,r}$.

- If $w \in B_{n,\alpha,r}$ then $\{w0, w1\} \cap B_{n+1,\alpha,r} \ne \emptyset$. (The prolongation property)
- If $n_1 \le n_2$ and $r_1 \le r_2$ then $|B_{n_1,\alpha,r_1}| \le |B_{n_2,\alpha,r_2}|$.
- $|B_{n,\alpha,r}| = |B_{n,1-\alpha,r}|$. Since there exists bijection between $|B_{n,\alpha,r}|$ and $|B_{n,1-\alpha,r}|$ induced by $0 \leftrightarrow 1$.

Proposition 1. *There exist $K_n(\alpha, \alpha') : \mathbb{N} \times (0,1) \times (0,1) \to (1, \infty)$*

$$\lim_{\alpha' \to \alpha} (\lim_{n\to\infty} \sqrt[n]{K_n(\alpha, \alpha')}) = 1$$

and $K_n(\alpha, \alpha')^{-1} |B_{n,\alpha',r}| \le |B_{n,\alpha,r}| \le K_n(\alpha, \alpha')|B_{n,\alpha',r}|$.

From the proposition follows that if limit (1) exists for all rational $\alpha \in (0, 1)$ then it exists for all $\alpha \in (0, 1)$. Moreover, the resulting family of functions $e_{\alpha,r}$ is uniformly continuous. So, $e_\alpha = \lim_{r\to\infty} e_{\alpha,r}$ is continuous function. (Also, it is enough to check the convergence only for rational α.)

Proof. Let $\alpha < \alpha'$. We start by constructing a map $\psi : B_{n,\alpha,r} \to B_{n',\alpha',r}$ where n' will be specified later. To define $\psi(w)$ we add some 0 between letters of w by the following procedure.

start w, $w' = \emptyset$ (w' =empty word)
step=0
while($w \ne \emptyset$):
  step=step+1
  w_1 is the first letter of w
  $w = w[2 :]$ # remove the first letter from w
  $w' = w'0^k w_1$, where k is minimum k, such that $w'0^k w_1 \in B_{|w'|+k+1,\alpha',r}$
end while

We have to check that the algorithm works. The only possible problem is in the last operation inside *while*. We prove that such k exists by induction on *step*. Let w be an initial word and $w'(s)$ be the word w' after s steps of algorithm.

Statement Let $w'(s)$ exist $s < |w|$ and $|\, w[: s]\,|_0 - \lfloor \alpha s \rfloor \ge |\, w'(s)\,|_0 - \lfloor \alpha' |w'(s)| \rfloor$. Then $w'(s+1)$ exists and $|\, w[: s+1]\,|_0 - \lfloor \alpha(s+1) \rfloor \ge |\, w'(s+1)\,|_0 - \lfloor \alpha' |w'(s+1)| \rfloor$.

Indeed, $|\, w[: s+1]\,|_0 - \lfloor \alpha(s+1) \rfloor \ge |\, w'(s) w_{s+1}\,|_0 - \lfloor \alpha'(|w'(s)| + 1) \rfloor$. (Recall that $\alpha < \alpha'$.) So, if $w'(s)w_{s+1} \in B_{|w'(s)|+1,\alpha',r}$ we are done. If $w'(s)w_{s+1} \notin B_{|w'(s)|+1,\alpha',r}$ then $-r+1 > |\, w'(s)w_{s+1}\,|_0 - \lfloor \alpha'(|w'(s)| + 1) \rfloor$. Particularly, it implies that $w_{s+1} = 1$. By the prolongation property $w'(s)0 \in B_{|w'(s)|+1,\alpha',r}$ and there exists minimal k such that $-r+1 = |\, w'(s)w_{s+1}\,|_0 + k - \lfloor \alpha'(|w'(s)| + k + 1) \rfloor$. It is easy to check that this k is the

k from the last command of *wile* for the *step*$= s+1$. The inequality of the Statement holds because $-r+1$ is the minimum possible value for $|\,w[:s]\,|_0 - \lfloor \alpha s \rfloor$.

Now, after $n = |w|$ steps we have $w' \in B_{|w'|,\alpha',r}$. This w' is made from w by adding somewhere j zeroes. The statement allows us to estimate j: $|\,w\,|_0 - \lfloor \alpha n \rfloor \geq |\,w\,|_0 + j - \lfloor \alpha'(n+j) \rfloor$, and $j \leq (1-\alpha')^{-1}(\alpha' n - \lfloor \alpha n \rfloor)$. Let $j_{\max} = \lfloor (1-\alpha')^{-1}(\alpha' n - \lfloor \alpha n \rfloor) \rfloor$ and $n' = n + j_{\max}$. Now we define $\psi : B_{n,\alpha,r} \to B_{n',\alpha',r}$ as follows $\psi(w) = w'u$ where $w'u \in B_{n',\alpha',r}$, and u, say, lexicographically minimal satisfying this condition.

Let $w \in B_{n',\alpha',r}$. One has

$$|\psi^{-1}(w)| \leq \sum_{j=0}^{j_{\max}} C_j^{\alpha' n' + r}.$$

Indeed, any word from $\psi^{-1}(w)$ is made by removing a suffix of length $\leq j_{\max} - j$ and then by removing j zeros from the rest. Now, we estimate

$$|B_{n,\alpha,r}| \leq \left(\sum_{j=0}^{j_{\max}} C_j^{\alpha' n' + r} \right) |B_{n',\alpha',r}| \leq K_n \cdot |B_{n,\alpha',r}|,$$

where $K_n = 2^{j_{\max}} \sum_{j=0}^{j_{\max}} C_j^{\alpha' n' + r}$. Now,

$$\sqrt[n]{K_n} \leq 2^{\frac{j_{\max}}{n}} \sqrt[n]{n} \sqrt[n]{C_{j_{\max}}^{\alpha' n' + r}},$$

but $\frac{j_{\max}}{n} \to \frac{\alpha' - \alpha}{1-\alpha'}$, $\sqrt[n]{n} \to 1$ and $\sqrt[n]{C_{j_{\max}}^{\alpha' n' + r}} \to \left(\frac{1}{\beta}\right)^{\beta} \left(\frac{1}{1-\beta}\right)^{1-\beta}$ when $n \to \infty$. Where $\beta = \lim\limits_{n\to\infty} \frac{j_{\max}}{\alpha' n' + r} = \frac{\alpha' - \alpha}{1-\alpha}$. In order to find $\lim\limits_{n\to\infty} \sqrt[n]{C_{j_{\max}}^{\alpha' n' + r}}$ one can use the methods of [3] as it is explained in Section 7. For inequality from over direction we change $\alpha \to 1-\alpha$ and $\alpha' \to 1-\alpha'$. Generally, we get another K_n, but then we take maximum of them. ☐

4 About intersections of linear subspaces.

For the proof of Theorem 1 I need several lemmas about linear spaces. In all these lemmas we use an extension of linear space to a larger field. Let V be an n-dimension vector space over a field K. Let F be a finite extension of K. Then $F \otimes_K V$ is an n-dimension vector space over F. Clearly, if $\tilde{S}$ is a p-dimension subspace of V then $F \otimes_K \tilde{S}$ is a p-dimension subspace (as a vector space over F) of $F \otimes_K V$. Let $\alpha \in \mathrm{Gal}(F:K)$. α may be extended to $\alpha \otimes id : F \otimes_K V \to F \otimes_K V$. One can see that $\alpha \otimes id$ is not linear over F, but as we will see it conserve linear dependence. In what follows I write α instead of $\alpha \otimes id$ in order to simplify notations. So, for example, $\alpha(f \otimes v) = \alpha(f) \otimes v$. Let $\bar{x}_1 \in F \otimes_K V$, $\bar{x}_2 = \alpha(\bar{x}_1)$, $\bar{x}_3 = \alpha(\bar{x}_2), \ldots, \bar{x}_{j+1} = \alpha(\bar{x}_j), \ldots$.

Lemma 2. *Suppose that $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n$ form a basis of $F \otimes_K V$ over F. Then*

$$span(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{n-p}) \cap F \otimes_K \tilde{S} = \{0\}$$

Proof. Notice the following simple fact:

- $\alpha(F \otimes_K \tilde{S}) = F \otimes_K \tilde{S}$.
- Let $y \in F \otimes_K V$ and $\alpha^k(y) \in span\left(y, \alpha(y), \alpha^2(y), \ldots, \alpha^{k-1}(y)\right)$.
  Then $\alpha^m(y) \in span\left(y, \alpha(y), \alpha^2(y), \ldots, \alpha^{k-1}(y)\right)$ for any $m \in \mathbb{N}$.

We prove the following inductive

Statement Let $k \leq n-p$ and $span(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_k) \cap F \otimes_K \tilde{S} \neq \{0\}$. Then $span(\bar{x}_1, \ldots, \bar{x}_{2k+p-n-1}) \cap F \otimes_K \tilde{S} \neq \{0\}$. (We suppose here that $span(\bar{x}_1, \ldots, \bar{x}_m) = span(\emptyset) = \{0\}$ for $m < 1$. In this case the statement leads to a contradiction that proves our lemma.)

Indeed, let $0 \neq z \in span(\bar{x}_1, \dots, \bar{x}_k) \cap F \otimes_K \tilde{S}$. Then $0 \neq \alpha(z) \in span(\bar{x}_2, \dots, \bar{x}_{k+1}) \cap F \otimes_K \tilde{S}$,..., $0 \neq \alpha^{p-1}(z) \in span(\bar{x}_p, \dots, \bar{x}_{k+p-1}) \cap F \otimes_K \tilde{S}$,...., $0 \neq \alpha^{n-k}(z) \in span(\bar{x}_{n-k+1}, \dots, \bar{x}_n) \cap F \otimes_K \tilde{S}$. As the dimension of $F \otimes_K \tilde{S}$ is p one has that $\alpha^p(z) \in span\left(z, \alpha(z), \dots, \alpha^{p-1}(z)\right)$ and, consequently, $\alpha^{n-k}(z) \in span\left(z, \alpha(z), \dots, \alpha^{p-1}(z)\right)$. It follows that $\alpha^{n-k}(z) \in span(\bar{x}_1, \dots, \bar{x}_{k+p-1}) \cap span(\bar{x}_{n-k+1}, \dots, \bar{x}_n)$ and $\alpha^{n-k}(z) \in span(\bar{x}_{n-k+1}, \dots, \bar{x}_{k+p-1})$, as $\bar{x}_i$ form a basis. Applying α^{-n+k} to the last inclusion one gets $z \in span(\bar{x}_1, \dots, \bar{x}_{2k+p-n-1})$. Obviously, $2k+p-n-1 < k$ for $k < n-p+1$ and the lemma is proved. $\square$

The next lemma is an easy corollary of Lemma 2.

Lemma 3. *Let $P \in \mathbb{C}(\lambda)[x]$ of order n, x_i be the roots of P and the cyclic permutation $(x_1, x_2, \dots, x_n) \in \mathrm{Gal}(P, \mathbb{C}(\lambda))$. Let $S \in Mat_{p,n}(\mathbb{C}(\lambda))$ with $rank(S) = p$. Let*

$$X = \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_p \\ x_1^2 & x_2^2 & \dots & x_p^2 \\ . & . & \dots & . \\ . & . & \dots & . \\ . & . & \dots & . \\ x_1^{n-1} & x_2^{n-1} & \dots & x_p^{n-1} \end{pmatrix}$$

Then equation $\det(SX) = 0$ (as the function of λ) has finite solutions in each compact subset of the corresponding Riemann surface.

Proof. Suppose the contrary, that $\det(SX) = 0$ has a countable set of solutions in a compact subset of $\mathbb{C}$. It follows that $\det(SX) \equiv 0$ for all λ. Now, the lemma follows by application of Lemma 2 with $K = C(\lambda)$, F being the splitting field of P, $\tilde{S} = \mathrm{Ker}(S)$ and $\bar{x}_1 = x_1^{[0:n-1]} = (1, x_1, \dots, x_1^{n-1})$. $\square$

Let $V = \mathbb{R}^n$ be a real linear space. We need the complexification $\mathbb{C} \otimes_{\mathbb{R}} V$ of V. On $\mathbb{C} \otimes_{\mathbb{R}} V$ the following antilinear involution is defined $\cdot^* : \mathbb{C} \otimes_{\mathbb{R}} V \to \mathbb{C} \otimes_{\mathbb{R}} V$ as $(c \otimes v)^* = c^* \otimes v$. A subspace Y of $\mathbb{C} \otimes_{\mathbb{R}} V$ is of the form $Y = \mathbb{C} \otimes_{\mathbb{R}} X$ if and only if Y is closed with respect to involution $(\cdot)^*$. In this case we denote $X = Re(Y)$.

Let V_u be a subspace of V, $\dim(V_u) = q$. Let $L : V \to V$ be a real linear operator, diagonalizable in $\mathbb{C} \otimes_{\mathbb{R}} V$. Let $e_1, \dots e_n$ be eigen-vectors of L with corresponding eigen-values $\alpha_1, \dots, \alpha_n$, ordering such that $|\alpha_1| \geq |\alpha_2| \geq \dots \geq |\alpha_n|$.

Lemma 4. *Suppose that*

- $\alpha_q = \rho e^{i\phi} \notin \mathbb{R}$, $\alpha_{q+1} = \alpha_q^*$ *and* $|\alpha_{q+1}| > |\alpha_{q+2}|$.
- $span(e_{q+1}, \dots e_n)$ *and* $\mathbb{C} \otimes_{\mathbb{R}} V_u$ *are in general position.*

Then $L^d(V_u) \to span(Re\left(span(e_1, e_2, ..., e_{q-1})\right), ae^{id\phi}e_q + a^*e^{-id\phi}e_{q+1})$ as $d \to \infty$. Precisely, $L^d(V_u)$ has a basis $b_1 + v_1, \dots, b_{q-1} + v_{q-1}, ae^{in\phi}e_q + a^*e^{-in\phi}e_{q+1} + v_q$ with $\|v_i\| \leq c\left(\frac{|\alpha_{q+2}|}{|\alpha_i|}\right)^d$. Where c is independent of d and $b_1, \dots b_{q-1}$ is a (real) basis of $Re\left(span(e_1, e_2, ..., e_{q-1})\right)$.

Proof. One can choose e_j such that $e_j^* = e_{\tilde{j}}$, where $\tilde{\cdot} : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$. Moreover, $\tilde{j} \in \{1, \dots, q\}$ for $j \in \{1, \dots, q\}$ and $e_q^* = e_{q+1}$.

Let $V^\perp$ ($(\mathbb{C} \otimes_{\mathbb{R}} V)^\perp$) denote the dual space of V over $\mathbb{R}$ ($\mathbb{C} \otimes_{\mathbb{R}} V$ over $\mathbb{C}$). Clearly, $V^\perp \subset (\mathbb{C} \otimes_{\mathbb{R}} V)^\perp$ and $f \in V^\perp$ if and only if $f(v^*) = (f(v))^*$ for any $v \in \mathbb{C} \otimes_{\mathbb{R}} V$. Let $f_1, f_2, \dots, f_{n-q} \in V^\perp$ be such that $v \in V_u \iff \forall j \in \{1, 2, \dots, n-q\}\ f_j(v) = 0$. Let $(j,k) \in \{1, 2, \dots, n-q\}^2$. One has that $\det(f_j(e_{q+k})) \neq 0$ (the condition of the general position). It follows that $\mathbb{C} \otimes_{\mathbb{R}} V_u$ has a basis $e_j + w_j$ where $j \in \{1, \dots, q\}$ and $w_j \in span(e_{q+1}, \dots, e_n)$, $w_j^* = w_{\tilde{j}}$. Now, for $j = 1, 2, \dots, q-1$ one has that $w_j \in span(e_{q+2}, \dots, e_n)$ and $w_q = e_{q+1} + \dots$. In order to finish the proof one should apply L^d to the basis and change a pair e_j, $e_{\tilde{j}}$ by $b_j = (e_j + e_{\tilde{j}})/2$ and $b_{\tilde{j}} = (e_j - e_{\tilde{j}})/2i$. $\square$

I need a parametric variant of the presiding lemma. Now our space V_u and linear operator L are C_1-smoothly depend on a real parameter λ, $\dim(V_u) = q$. All eigen-values α_i of L are different for $\lambda = \lambda_0$ and ordered as before. Also we have another space V_d, $\dim(V_d) = n - q$. V_d as well C_1-smoothly depends on λ.

Lemma 5. *Let for λ_0 one have*

- $\alpha_q = \rho e^{i\phi} \notin \mathbb{R}$, $\alpha_{q+1} = \alpha_q^*$ *and* $|\alpha_{q+1}| > |\alpha_{q+2}|$*;*
- $\frac{d\phi}{d\lambda} \neq 0$
- $span(e_{q+1}, \dots e_n)$ *and* $\mathbb{C} \otimes_{\mathbb{R}} V_u$ *are in general position*
- $span(e_1, \dots e_q)$ *and* $\mathbb{C} \otimes_{\mathbb{R}} V_d$ *are in general position.*

Then for any interval $(\lambda_1, \lambda_2) \ni \lambda_0$ there exists d_0 such that for any $d_0 < d \in \mathbb{N}$ one has $L^d(V_u) \cap V_d \neq \{0\}$ for some $\lambda \in (\lambda_1, \lambda_2)$.

Proof. Fix a basis $w_1, w_2, \dots, w_{n-q}$ of V_d. Let $\det(w_1 \dots, w_{n-q}, b_1, \dots, b_{q-1}, e_q) = A(\lambda)$ (I suppose that $V = R^n \subset \mathbb{C}^n$. So, each vector is a vector column. b_i is from Lemma 4.) One has that $A(\lambda_0) \neq 0$ (general position). Let $L^d(V_u) = span(B_d)$, where B_d is a basis of Lemma 4. It follows that

$$\det(w_1, \dots, w_{n-q}, B_d) = A(\lambda)e^{id\phi(\lambda)} + A^*(\lambda)e^{-id\phi(\lambda)} + C(\lambda, d) = 2|A(\lambda)|\cos(d\phi(\lambda) + \phi_0) + C(\lambda, d) \quad (6)$$

where $C(\lambda, d) \to 0$ when $d \to \infty$. The r.h.s. of Eq.6 is a fast oscillating function. So, for any $\epsilon > 0$, one can find $d_0 \in \mathbb{N}$ such that for any $d > d_0$ r.h.s of Eq.(*) change the sign on $(\lambda_0 - \epsilon, \lambda_0 + \epsilon)$. It follows that the l.h.s. determinant is 0 for some $\lambda \in (\lambda_0 - \epsilon, \lambda_0 + \epsilon)$. The zeros of the determinant correspond to nontrivial intersections of $L^d(V_u)$ and V_d. □

5 Some property of $P = (x+1)^n - \lambda x^p$

Critical values of P.

Proposition 6. *The only critical values are $\lambda = 0$ (with all roots $x = -1$) and $\lambda = \frac{n^n}{p^p(n-p)^{(n-p)}}$ with the only double root $x = \frac{p}{n-p}$*

Proof. The proof is a direct computation. □

Proposition 7. *There exists a converging around 0 series f, such that the roots of P are $x_i = \gamma_i + \gamma_i^2 f(\gamma) - 1$ where $\gamma_i = \sqrt[n]{(-1)^p \lambda}$ (the i-th root) and $|\lambda|$ small enough (γ are inside the convergence ball of f).*

Proof. We apply the Newton method to calculate roots of P for small $|\lambda|$. □

We are interesting in small positive λ. Let $\lambda = \epsilon^n$, $\epsilon > 0$. Then $x_j = \epsilon \exp(2i\pi j/n) - 1 + O(\epsilon^2)$ for even p and $x_j = \epsilon \exp(2i\pi(j + 1/2)/n) - 1 + O(\epsilon^2)$ for odd p. It follows from Proposition 7 that $x_j \to x_{j+1}$ if λ rotates around 0. It means that Galois group $\mathrm{Gal}(P, \mathbb{C}(\lambda))$ (that is the monodromy group in this case) contains cycle $(x_1, x_2, \dots, x_n)$.

Proposition 8. *Let $\lambda \in \mathbb{R}$, $P(x) = 0$, $P(y) = 0$ with $|x| = |y|$. Then $x = y$ or $x = y^*$.*

Proof. Indeed, $|x+1|^n = |\lambda| \cdot |x|^p = |y+1|^n$. It follows that $|x+1|^2 = |y+1|^2$. Denoting $x = \rho e^{i\phi}$ and $y = \rho e^{i\psi}$ one gets $\cos(\phi) = \cos(\psi)$. □

Notice that $|x_j|^2 = 1 - 2\epsilon \cos(2\pi(j + (1 - (-1)^k)/4)/n) + O(\epsilon^2)$. So, for small enough $\lambda = \epsilon^n$, one has the following ordering of $|x_j|$:

Proposition 9.

- $|x_{\frac{n-1}{2}}| = |x_{-\frac{n-1}{2}}| > |x_{\frac{n-1}{2}-1}| = |x_{-\frac{n-1}{2}+1}| > \dots > |x_j| = |x_{-j}| > \dots > |x_0|$ *if p is even and n is odd;*
- $|x_{\frac{n-1}{2}}| > |x_{\frac{n-1}{2}-1}| = |x_{-\frac{n-1}{2}}| > \dots > |x_j| = |x_{-j-1}| > \dots > |x_0| = |x_{-1}|$ *if p is odd and n is odd;*
- $|x_{\frac{n}{2}-1} = |x_{\frac{n}{2}}| > |x_{\frac{n}{2}-2} = |x_{-\frac{n}{2}+1}| > \dots > |x_j| = |x_{-j-1}| > \dots > |x_0| = |x_{-1}|$ *if p is odd and n is even.*

From Proposition 6 and Proposition 8 it follows that this order is conserved for $\lambda \in (0, \frac{n^n}{p^p(n-p)^{(n-p)}})$.

Proposition 10. *Let $x = \rho e^{i\phi} \notin \mathbb{R}$ be a root of P, and $\lambda \in \mathbb{R}$. Then $\frac{d\phi}{d\lambda} \neq 0$.*

Proof. $\frac{d\phi}{d\lambda} = 0$ if and only if $\frac{1}{x}\frac{dx}{d\lambda} \in \mathbb{R}$. Direct calculations show

$$\frac{dx}{d\lambda} = \frac{x(x+1)}{\lambda((n-p)x-p)},$$

but $\frac{x+1}{\lambda((n-p)x-p)} \in \mathbb{R}$ if and only if $x \in \mathbb{R}$ (at least for $p \leq n$). $\square$

Now we formulate our result on the Galois group of P. It will be proved in the next section.

Theorem 2. *Let $P = (x+1)^n - \lambda x^p$, $n > p$, $gcd(n, p) = 1$. Then* $\mathrm{Gal}(P, \mathbb{C}(\lambda)) = S_n$. *Where S_n is a group of all permutations of n elements.*

6 Proofs of Theorem 1 and Theorem 2

We start with a proof of Theorem 1. We show that for any $0 < \lambda_0 < \frac{n^n}{p^p q^q}$ and any $\epsilon > 0$ and large enough r there exists a nontrivial solution to

$$Mv = \lambda v \tag{7}$$

for $\lambda \in (\lambda_0 - \epsilon, \lambda_0 + \epsilon)$. We reduce this problem to the application of Lemma 5. Define $x^{[0:2r-1]} = (1, x, ..., x^{2r-1})^t$. Let x_i be the roots of $(x+1)^n - \lambda x^p$. All of them are different if $0 < \lambda < \frac{n^n}{p^p q^q}$. Notice that $(Mv - \lambda v)[q+1, 2r-p] = 0$ if and only if v is a linear combinations of $x_i^{[0:2r-1]}$. So, we only need to find λ and linear combinations of $x_i^{[0:2r-1]}$ to satisfy the boundary conditions, that is, to find $\alpha_1, \alpha_2, \ldots, \alpha_n$ and λ such that $(S_u - \lambda)(\alpha_1 x_1^{[0:n-1]} + \cdots + \alpha_n x_n^{[0:n-1]}) = 0$ and $(S_d - \lambda)(\sum x_i^{2r-n} \alpha_i x_i^{[0:n-1]}) = 0$. Where I use the inclusions $\mathbb{R} \to Mat_{p,n}$ ($\mathbb{R} \to Mat_{q,n}$) defined as

$$\lambda \to \begin{pmatrix} \lambda & 0 & \ldots & 0 \\ 0 & \lambda & \ldots & 0 \\ \vdots & \vdots & \vdots & 0 \end{pmatrix}$$

One can consider $S_u - \lambda$ as a linear operator $\mathbb{R}^n \to \mathbb{R}^p$ and $S_d - \lambda$ as a linear operator $\mathbb{R}^n \to \mathbb{R}^q$. Let the linear operator $L : \mathbb{R}^n \to \mathbb{R}^n$ be defined as $x_i^{[0:n-1]} \to x_i \cdot x_i^{[0,n-1]}$. Let $V_u = \mathrm{Ker}(S_u - \lambda)$ and $V_d = \mathrm{Ker}(S_d - \lambda)$. Notice that $rank(S_u - \lambda) = p$ ($rank(S_d - \lambda) = q$) over $\mathbb{C}(\lambda)$. So, $\dim(V_u) = q$ ($\dim(V_d) = p$) for all but finite exceptions λ. The following proposition is standard:

Proposition 11. *Eq.7 has a nontrivial solution if and only if $L^d(V_u) \cap V_d \neq \{0\}$ with $d = 2r - n$.*

So, in order to finish the proof we show that L, V_u, V_d satisfy Lemma 5 for all, but some finite exceptions, $0 < \lambda_0 < \frac{n^n}{p^p q^q}$.

- The first item is fulfilled by Proposition 9.
- The second item is fulfilled by Proposition 10.
- The third and fourth items are fulfilled thanks to Lemma 3.

Now, let us consider Theorem 2. By Inequality (2), M has no spectral values $> \frac{n^n}{p^p q^q}$. It means, that $\lambda \geq \frac{n^n}{p^p q^q}$ the conditions of Lemma 5 are no more fulfilled. Using this one can easily figure out that pair of roots collides for $\lambda = \frac{n^n}{p^p q^q}$. These are $(x_{\frac{p}{2}}, x_{-\frac{p}{2}})$ for even p and $(x_{\frac{p-1}{2}}, x_{-\frac{p-1}{2}-1})$ for odd p. It means that the transposition $(x_{\frac{p}{2}}, x_{-\frac{p}{2}}) \in \mathrm{Gal}(P, C(\lambda))$ ($(x_{\frac{p-1}{2}}, x_{-\frac{p-1}{2}-1}) \in \mathrm{Gal}(P, C(\lambda))$). So, $\mathrm{Gal}(P, C(\lambda))$ (which is the same as the monodromy group) is generated by a pair of permutations $(0, 1, 2, \ldots, n-1)$ and $(a, a+p)$. One can check that this is S_n if $gcd(p, n) = 1$. If $gcd(p, n) = t$ then $\mathrm{Gal}(P, C(\lambda)) = \langle (1, 2, \ldots, n)(1, 1+t) \rangle$ is an extension of C_t (the cyclic group of order t) by $S_{\frac{n}{t}}^t$.

7 Asymptotic for 2-variable generating functions.

I rewrite Theorem 1.3 of [5], see also [3, 4]

Let

$$G(x,y) = \frac{P(x,y)}{D(x,y)} = \sum_{r=0,s=0}^{\infty} a_{rs}x^r y^s, \ \ a_{rs} \geq 0$$

Theorem 3. *1. For each positive (r,s) (in the positive octant), there is a unique positive solution (x,y) of the system*

$$D = 0 \tag{8}$$

$$sx\frac{\partial D}{\partial x} = ry\frac{\partial D}{\partial y} \tag{9}$$

(clearly, the solution depends on the direction s/r, but not the absolute value of (s,r).)

2. With (x,y) being the solution defined above, if $P(x,y) \neq 0$,

$$a_{rs} \sim f_{rs} = \frac{P(x,y)}{\sqrt{2\pi}} x^{-r} y^{-s} \sqrt{\frac{-yD_y}{sQ(x,y)}}$$

uniformly over compact cones of (r,s) for which (x,y) is a smooth point of the manifold $D=0$. (This means that if (r,s) is in the cone then $|1 - a_{rs}/f_{rs}| \leq \epsilon(\sqrt{s^2+r^2})$ for some $\epsilon(n)$, $\epsilon(n) \to 0$ when $n \to \infty$.) Where

$Q(x,y) = -xD_x(yD_y)^2 - yD_y(xD_x)^2 - [(yD_y)^2 x^2 D_x x + (xD_x)^2 y^2 D_y y - 2xD_x yD_y xyD_{xy}]$

Particularly, it implies that $\lim_{n\to\infty} \sqrt[n]{a_{\lfloor \alpha n \rfloor, \lfloor (1-\alpha)n \rfloor}} = x^{-\alpha} y^{-(1-\alpha)}$. In our case

$$G(x,y) = \sum_{r=0,s=0}^{\infty} C_r^{r+s} x^r y^s = \frac{1}{1-x-y},$$

and $x(\alpha) = \alpha$ and $y(\alpha) = 1 - \alpha$.

8 Concluding remarks

We may consider the similar problem in more general situation. Let Γ be a graph. Let $\Gamma = \Gamma_0 \cup \Gamma_1$. We are interesting in paths p of the graph. Let $|p|$ be the length of p and $|p|_i$ be the number of transitions (edges) of p from the graph Γ_i. Let P be the set of paths of Γ and

$$P_{n,\alpha,r} = \{p \in P \ \mid \ |p| = n, \ \forall k \ \alpha k - r < |\, p[: k] \,| \leq \alpha k + r\}.$$

One may ask the same questions about $|P_{n,\alpha,r}|$. Some part of our consideration may be easily generalized for this new situation. For example, the matrix M become a product of $N_+ \otimes A_1 + E \otimes A_2$ and $E \otimes A_1 + N_- \otimes A_2$, where A_i is the incidence matrix of Γ_i.

In general, one can redefine $e_{\alpha,r}$ and $\tilde{e}_r$ for this situation.

Open Question 1. *Is it true that for any $\Gamma = \Gamma_1 \cup \Gamma_2$ one has that $\lim_{r\to\infty} e_{\alpha,r} = \tilde{e}_r$.*

If the answer is "yes" it may happens that it is more easy to find a combinatorial proof. But I was not able to find a combinatorial proof even for the case considered in the present article.

Notice, that establishing our limits we use a fast oscillating function. It is interesting, that in the proof of Theorem 3 the authors use a fast oscillating integrals. So, it may happens that there exists more deep relation between our calculations and results of [3, 4, 5]

References

[1] V. Afraimovich, M. Courbage, L. Glebsky, Directional complexity and entropy for lift mappings, in preparation.

[2] F. R. Gantmacher, Theory of Matrices. *Trans. from the Russian by K. A. Hirsch*, vols. I and II. New York, Chelsea, 1959. 10+374 pp.; 9+276 pp

[3] R. Pemantle, M. Wilson, Asymptotics of multivariate sequences, I. Smooth points of the singular variety. *J. Combin. Theory Ser. A*, **97** (1), 129-161, 2002

[4] R. Pemantle, M. Wilson, Asymptotics of multivariate sequences, II. Multiple points of the singular variety. *Combin. Probab. Comput*, **13**, 735-761, 2004

[5] R. Pemantle, M. Wilson, Twenty combinatorial examples of asymptotics derived from multivariate generating functions, *SIAM Review*, **50** (2), 199-272, 2008