1 Coefficients of $AH_p(x)$ are $\mathbb{Z}_{(p)}$-integral

In the following section, let G be a topological group, and let S_n denote the symmetric group on n letters equipped with the discrete topology. Let t_n be the number of continuous homomorphisms $\varphi : G \to S_n$, and let s_n be the number of such continuous homomorphisms where $\varphi(G)$ is a transitive subgroup of S_n.

Lemma 1.1. *Let G, S_n, t_n, and s_n be as above. Then*

$$t_n = s_1 t_{n-1} + \binom{n-1}{1} s_2 t_{n-2} + \ldots + \binom{n-1}{n-2} s_{n-1} t_1 + s_n t_0.$$

Proof. Suppose $\varphi : G \to S_n$ is a continuous homomorphism so $\mathcal{O}(1) = \{1, i_2, \ldots, i_k\}$ is an orbit of the action of $\varphi(G)$ on $\{1, 2, \ldots, n\}$ where $1 \leq k \leq n$. Then $\varphi(G)$ acts transitively on $\mathcal{O}(1)$ and acts as a subgroup of S_{n-k} on the other $n-k$ letters in $\{1, 2, \ldots, n\} \setminus \mathcal{O}(1)$. We can pick the $(k-1)$ letters $\{i_2, i_3, \ldots, i_k\}$ from $\{2, 3, \ldots, n\}$ in $\binom{n-1}{k-1}$ ways, so for each k, there are $\binom{n-1}{k-1} s_k t_{n-k}$ such homomorphisms φ where $|\mathcal{O}(1)| = k$. The result follows by taking a sum of the number of continuous homomorphisms for $k = 1, 2, \ldots, n$. $\square$

Lemma 1.2. *Let M_n be the number of open subgroups of G with index n. Then $s_n = M_n \cdot (n-1)!$.*

Proof. Let $\varphi : G \to S_n$ be a continuous homomorphism so $\varphi(G)$ acts transitively on $\{1, 2, \ldots, n\}$. Let H be the stabilizer of 1. Note that H is open in G since $\varphi(H)$ is open in S_n and φ is continuous. By the Orbit-Stabilizer theorem, $|\mathcal{O}(1)| = n = [G : H]$, so there are M_n choices for H. The action of $\varphi(G)$ is then determined by the images of the other $n-1$ right cosets of H under φ which each send 1 to a unique element of $\{2, 3, \ldots, n\}$. This can be done in $(n-1)!$ ways, so we conclude that there are $M_n \cdot (n-1)!$ choices for φ. $\square$

Lemma 1.3. *Let G be a topological group such that for every integer n, there are finitely many open subgroups of index n. Then*

$$\frac{t_n}{(n-1)!} = t_0 M_n + t_1 \frac{M_{n-1}}{1!} + t_2 \frac{M_{n-2}}{2!} + \ldots + t_{n-1} \frac{M_1}{(n-1)!}.$$

Proof. We may simply compute using the results of Lemma 1.1 and Lemma 1.2:

$$\begin{aligned} t_n &= \sum_{k=1}^{n} \binom{n-1}{k-1} s_k t_{n-k} \\ &= \sum_{k=1}^{n} \binom{n-1}{k-1} M_k (k-1)! t_{n-k} \\ &= \sum_{k=1}^{n} \frac{(n-1)!}{(n-k)!} M_k t_{n-k} \\ \frac{t_n}{(n-1)!} &= \sum_{k=1}^{n} \frac{M_k}{(n-k)!} t_{n-k} \end{aligned}$$

$\square$

Theorem 1.4. *Let G be a topological group so that for every integer n, there are finitely many open subgroups of index n. Then*

$$\exp\left(\sum_{H\leq G}\frac{x^{[G:H]}}{[G:H]}\right)=\sum_{n\geq 0}\frac{t_n}{n!}x^n$$

where H runs over the open subgroups of G with finite index.

Proof. Since M_k is finite for all $k\geq 1$, we may rewrite the left hand side as follows:

$$\begin{aligned}\exp\left(\sum_{H\leq G}\frac{x^{[G:H]}}{[G:H]}\right)&=\exp\left(\sum_{k\geq 1}\frac{M_k}{k}x^k\right)\\&=\exp\left(\sum_{k\geq 1}M_k(k-1)!\frac{x^k}{k!}\right)\\&=\sum_{n\geq 0}B_n\big(M_1(0!),M_2(1!),\ldots,M_n(n-1)!\big)\frac{x^k}{k!}.\end{aligned}$$

where B_n is the nth complete exponential Bell polynomial. It therefore suffices to show $t_n=B_n\big(M_1(0!),M_2(1!),\ldots,M_n(n-1)!\big)$ for all $n\geq 0$. We proceed by induction.

The base case is trivial since $t_0=B_0=1$. Suppose the equation holds for all $n=1,2,\ldots,k$. By the recurrence definition of complete Bell polynomials, we have

$$B_{k+1}\big(M_1,M_2,\ldots,M_{k+1}(k!)\big)=\sum_{\ell=0}^{k}\binom{k}{\ell}\big(M_{\ell+1}\ell!\big)B_{k-\ell}\big(M_1,M_2,\ldots,M_{k-\ell}(k-\ell-1)!\big)$$

and so, by our inductive hypothesis,

$$\begin{aligned}&=\sum_{\ell=0}^{k}\binom{k}{\ell}(M_{\ell+1}\ell!)t_{k-\ell}\\&=k!\sum_{\ell=0}^{k}t_{k-\ell}\frac{M_{\ell+1}}{(k-\ell)!}\end{aligned}$$

but this is exactly the form of the recurrence for t_{k+1} of Lemma 1.3. The claim is therefore true by induction, and the proof follows. $\square$

CONSIDER TALKING ABOUT COMBINATORIC IMPLICATIONS OF USING BELL POLYNOMIALS?

Theorem 1.5. *Let $t_{\mathbb{Z}_p,n}$ denote the number of continuous homomorphisms from $\mathbb{Z}_p$ to S_n. Then the coefficients of AH_p are $t_{\mathbb{Z}_p,n}/n!$, so*

$$AH_p(x)=1+\sum_{n\geq 1}\frac{t_{\mathbb{Z}_p,n}}{n!}x^n.$$

Proof. Note that for all $k \geq 1$, there exists a unique (open) subgroup of $\mathbb{Z}_p$ of index p^k, and that there are no subgroups not of p-power index. From here, apply the result of Theorem 1.4 to see

$$\sum_{n\geq 0} \frac{t_{\mathbb{Z}_p,n}}{n!} x^n = \exp\left(\sum_{H\leq \mathbb{Z}_p} \frac{x^{[\mathbb{Z}_p:H]}}{[\mathbb{Z}_p:H]}\right) = \exp\left(\sum_{k\geq 0} \frac{x^{p^k}}{p^k}\right) = AH_p(x). \qquad \square$$

For the following proof, let v_p denote the p-adic valuation on $\mathbb{Q}$. Let $\mathbb{Z}_{(p)}$ be the subring of the p-adic integers $\mathbb{Z}_p$ given by $\{r \in \mathbb{Q} : |r|_p \leq 1\} = \{r/s \in \mathbb{Q} : (r,s) = 1,\ p \nmid s\}$.

Theorem 1.6. *$AH_p(x) \in \mathbb{Z}_{(p)}[[x]]$.*

Proof. Let $m \in \mathbb{Z}$ be such that $n! = p^{v_p(n!)}m$ and $(p,m) = 1$. We will show that for each $n \geq 0$, there exists an integer ℓ so $p^{v_p(n!)}\ell = t_{\mathbb{Z}_p,n}$, and therefore

$$\frac{t_{\mathbb{Z}_p,n}}{n!} = \frac{\ell}{m} \in \mathbb{Z}_{(p)}.$$

Let $T = \{\sigma \in S_n : \sigma^{p^k} = 1,\ k \in \mathbb{N}\}$ be the elements of S_n with p-power order. Note that $t_{\mathbb{Z}_p,n} = |T|$. By a theorem of Frobenius, $p^{v_p(n!)}$ divides the size of $A := \{\sigma \in S_n : \sigma^{p^{v_p(n!)}} = 1\}$. Clearly $A \subseteq T$. To see that $T \subseteq A$, consider an element $\tau \in T$. There exists $k \geq 0$ so $\tau^{p^k} = 1$ and $p^k \leq n$. Thus, $p^k \mid n!$, and moreover, since $(p,m) = 1$ and $m \mid n!$, we have $mp^k \mid n!$, so $p^k \mid p^{v_p(n!)}$. Hence $\tau^{p^{v_p(n!)}} = 1$, so $\tau \in A$. We conclude that $p^{v_p(n!)} \mid |T| = t_{\mathbb{Z}_p,n}$, so such an ℓ exists.

The coefficients of $AH_p(x)$ are therefore in $\mathbb{Z}_{(p)}$, so $AH_p(x) \in \mathbb{Z}_{(p)}[[x]]$. $\square$

2 Image of AH_p contains all p^k roots of unity in $\mathbb{C}_p$

Lemma 2.1. *If $x \in m_p := \{\alpha \in \mathbb{C}_p : |\alpha|_p < 1\}$, then $AH_p(x)$ converges.*

Proof. Let $AH_p(x)$ be written as the power series

$$AH_p(x) = \sum_{k\geq 0} c_k x^k.$$

We have shown above that the coefficients $\{c_k\}$ are in $\mathbb{Z}_p$, so for all k, $|c_k|_p \leq 1$. Since $|x|_p < 1$, it is clear that $|c_k x^k|_p = |c_k|_p |x|_p^k \to 0$ as $k \to \infty$. Thus $AH_p(x)$ converges at x with respect to the p-adic norm. $\square$

Lemma 2.2. *In particular, $AH_p(x)$ diverges everywhere on the boundary $\{\alpha \in \mathbb{C}_p : |\alpha|_p = 1\}$; thus the disc of convergence for $AH_p(x)$ is exactly m_p.*

Proof. (A completion of the proof of Theorem 2.10 in Kieth Conrad's notes) It suffices to show $AH_p(x)$ diverges at 1, i.e. the coefficients of $AH_p(x)$ do not tend to 0. We do this by showing $AH_p(x)$ has infinitely many coefficients in $\mathbb{Z}_p^\times$ (note $u \in \mathbb{Z}_p^\times$ implies $|u|_p = 1$).

Equivalently, we show $AH_p(x) \mod p \in \mathbb{F}_p[[x]]$ is not in $\mathbb{F}_p[x]$ (where $\mathbb{F}_p$ is the field of p elements). From the definition of $AH_p(x)$, we have

$$x\frac{AH_p(x)}{AH_p'(x)} = \sum_{k=0}^{\infty} x^{p^k} := f(x)$$

This is an equation in $\mathbb{Z}_p[[x]]$, so we can reduce $\mod p$, and it will also be true in $\mathbb{F}_p[[x]]$. Since $\mathrm{char}(\mathbb{F}_p) = p$, we have $(f(x)^p) = f(x) - x$, so $f(x)$ mod p must be a root of $t^p - t + x$ in $\mathbb{F}_p(x)$. We derive a contradiction by showing $t^p - t + x$ has no roots in $\mathbb{F}_p(x)$:

Consider $t^p = t - x$; we have $p\deg(t) = \deg(t - x) \in \{\deg(t), 1, 0\}$. All three possibilities for $\deg(t-x)$ lead to contradiction: If $p\deg(t) = \deg(g)$, $p = 1$. If $p\deg(t) = 1$, $p \mid 1$. Finally, $p\deg(t) = 0$ implies $\deg(t) = 0$, so we can write $t = f/g$ for $f, g \in \mathbb{F}_p[x]$ with $\deg(f) = \deg(g)$. This forces $\deg(f^p/g^p - f/g) = 1$, which is impossible. Thus $t^p - t + x$ has no roots in $\mathbb{F}_p(x)$, and in particular $AH_p(x)$ mod $p \notin \mathbb{F}_p[x]$. $\square$

Lemma 2.3. *The power series* $\exp(x)$ *does not converge on the boundary of its disc of convergence* E*,* $\{\alpha \in \mathbb{C}_p : |\alpha|_p = p^{1/(1-p)}\}$.

Proof. Let $\alpha \in \mathbb{C}_p$ so $|\alpha|_p = p^{1/(1-p)}$. Then $\exp(\alpha)$ converges only if $\lim_{n\to\infty} |\alpha^n/n!|_p$ exists and equals 0. See that

$$\lim_{n\to\infty} |\alpha^n/n!|_p = \lim_{n\to\infty} \frac{(p^{1/(1-p)})^n}{p^{(s_n-n)/(p-1)}} = \lim_{n\to\infty} p^{-s_n/(p-1)} = \lim_{n\to\infty} |\alpha|_p^{s_n}.$$

For any $n = p^k$, we have $s_n = 1$, so $\limsup_{n\to\infty} |\alpha|_p^{s_n} \geq |\alpha|_p \neq 0$. We conclude that $\exp(x)$ does not converge at α. $\square$

Lemma 2.4. $AH_p : m_p \to m_p + 1$ *is a surjective isometry.*

Proof. $\square$

Theorem 2.5. *For every* p^k *root of unity* $\zeta \in \mathbb{C}_p$*, there exists* $\alpha \in m_p$ *for which* $AH_p(\alpha) = \zeta$.

Proof. Let ζ be a primitive p^k root of unity for $k \geq 1$. Let $f(x)$ be given by

$$f(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = 1 + x^{p^{k-1}} + \ldots + x^{(p-1)p^{k-1}}$$

so $f(1) = p$. The roots of $f(x)$ are then all ζ^r so $1 \leq r < p^k$ and $(r, p) = 1$. Therefore,

$$f(1) = p = \prod_{\substack{1\leq r<p^k \\ (r,p)=1}} (1 - \zeta^r). \tag{$*$}$$

Note that for all such r, by the strong triangle inequality $u := (\zeta^r - 1)/(\zeta - 1)$ is a unit in $\mathbb{C}_p$:

$$|u| = \left|\frac{\zeta^r - 1}{\zeta - 1}\right| = |1 + \zeta + \zeta^2 + \ldots + \zeta^{r-1}| \leq \max_{0\leq k<r}\{|\zeta^k|\} = 1.$$

Since $(r, p^k) = 1$, there exist $s, t \in \mathbb{Z}$ so that $1 = sr + tp^k$. Using this, we obtain the following formula for u^{-1}:

$$u^{-1} = \frac{\zeta - 1}{\zeta^r - 1} = \frac{\zeta^{sr+tp^k} - 1}{\zeta^r - 1} = \frac{(\zeta^r)^s - 1}{\zeta^r - 1} = 1 + \zeta^r + \zeta^{2r} + \ldots + \zeta^{(s-1)r}$$

so likewise by the strong triangle inequality, $|u^{-1}| \leq 1$. But since $uu^{-1} = 1$, this forces $|u| = |u^{-1}| = 1$. In particular, we get $|\zeta^r - 1| = |\zeta - 1|$.

Taking norms of $(*)$ above, we can use this to see

$$|p| = \prod_{\substack{1 \leq r < p^k \\ (r,p)=1}} |1 - \zeta^r| = |1 - \zeta|^{\varphi(p^k)} = |1 - \zeta|^{(p-1)p^{k-1}}$$

so, by evaluating the norms,

$$|1 - \zeta| = \left(p^{\frac{1}{1-p}}\right)^{p^{1-k}} < 1$$

and thus $\zeta - 1 \in m_p$, so $\zeta \in m_p + 1$. Since $AH_p(x)$ takes m_p onto $m_p + 1$, there exists $\alpha \in m_p$ for which $AH_p(\alpha) = \zeta$. □

References

[1] Conrad, K. (n.d.). *Artin-Hasse-type Series and Roots of Unity*. University of Connecticut. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/AHrootofunity.pdf`.

[2]

[3]