International Journal of Pure and Applied Mathematics
Volume 54 No. 2 2009, 265-277

EXTENSION OF A RANDOM WALK ON FINITE ABELIAN GROUPS

Joseph McCollum
Department of Quantitative Business Analysis
Siena College
515, Loudon Road, Loudonville, NY 12211, USA
e-mail: jmccollum@siena.edu

Abstract: In the survey articles written by M. Hildebrand and L. Saloff-Coste, there is a good overview of some known results in the theory of random walks on finite groups. One result of interest focuses on an Abelian group G with n elements such that $n = n_1 \cdots n_t$ where $n_1 \geq \cdots \geq n_t$ are prime numbers. Plus, $t \leq L$ for some value L not depending on n, and $n_1 \leq An_t$ for some value A not depending on n. It was shown by C. Dou that a k element set chosen uniformly from all subsets of G will create a random walk that will converge to the uniform distribution. This paper will extend this result to a larger class of groups by changing the restrictions.

AMS Subject Classification: 60G50
Key Words: random walk, Abelian groups

1. Main Result

The following theorem was proven by Dou in his thesis [2]. The assumptions that Dou make are that G is an Abelian group with n elements such that $n = n_1 \cdots n_t$, where $n_1 \geq \cdots \geq n_t$ are prime numbers. Plus, $t \leq L$ for some value L not depending on n, and $n_1 \leq An_t$ for some value A not depending on n.

Theorem 1. *Suppose G is Abelian and satisfies the conditions in the above paragraph and $k > 2L + 1$ is constant. Suppose $(a_1, \cdots, a_k)$ is chosen uniformly from the k-tuples with distinct elements of G. Then for some function*

Received: June 3, 2009

$f(n) \to 0$ as $n \to \infty$ (with $f(n)$ not depending on the choice of G)

$$E(\|P^{*m}_{a_1,\cdots,a_k} - U\|) \leq f(n)\,,$$

where $m = c(n)n^{2/(k-1)}$, where $c(n) \to \infty$ as $n \to \infty$ and $p_1 = \cdots = p_k = 1/k$ so that $P_{a_1,\cdots,a_k}(s) = 1/k$ if $s = a_i$ for some i in $1, \cdots, k$.

Let us talk about the restrictions that Dou used and the corresponding restrictions that we will set.

Dou's Restriction 1: $k > 2L + 1 \geq 2t + 1$.

Dou's Restriction 2: $m = c(n)n^{2/(k-1)}$ with $c(n) \to \infty$.

Dou's Restriction 3: $m < n_t$.

Dou's Restriction 4: $n_1 \leq An_t$ for some value A not depending on n.

These will be the new restrictions that we will use.

Restriction 1: $k \geq t + 2$.

Restriction 2: $m \geq \sigma(n)n^{2/(k-1)}$ for any $\sigma(n) \to \infty$ as $n \to \infty$.

Restriction 3: m does not have to be less than n_t.

Restriction 4: $n_t > n^{\epsilon+1/(k-1)}$ for some $\epsilon \in (0, \frac{1}{t(t+1)})$.

Using the new restrictions we will establish the main result.

Theorem 2. *Suppose G is Abelian and satisfies the new restrictions. Suppose $(a_1, \cdots, a_k)$ is chosen uniformly from the k-tuples with distinct elements of G. Then for some function $f(n) \to 0$ as $n \to \infty$ (with $f(n)$ not depending on the choice of G)*

$$E(\|P^{*m}_{a_1,\cdots,a_k} - U\|) \leq f(n)\,,$$

where $m = c(n)n^{2/(k-1)}$, where $c(n) \to \infty$ as $n \to \infty$ and $p_1 = \cdots = p_k = 1/k$ so that $P_{a_1,\cdots,a_k}(s) = 1/k$ if $s = a_i$ for some i in $1, \cdots, k$.

Note. To see if we have generalized Dou's Theorem to a larger set of groups we will end with an example. So, assume $k = 4$ and $t = 2$ and $n = n_1 n_2$ for n_1 and n_2 are prime. This implies that $k \leq t + 2 = 4$ and $\epsilon < \frac{1}{t(t+1)} = (1/6)$. Hence, choose $\epsilon = 1/10$ and so

$$n_2 > n^{(1/10)+(1/3)} > n_1^{13/30} n_2^{13/30}\,.$$

So, we need $n_2^{17} > n_1^{13}$. Now, if we let $p = n_2$ this implies $p^{17} > n_1^{13}$ and so $n_1 < p^{17/13}$. Thus, all we need to do is let n_1 be between $p^{1.1}$ and $2p^{1.1}$ for sufficiently large primes p and we arrive at an example that Dou's restrictions would not allow but with the new restrictions is allowed. We should note Bertrand's postulate that for every $n \geq 1$, there is some prime number p with

$n < p \leq 2n$.

2. Introduction

We will first state some results that Carl Dou has achieved and then state and prove an extension to his work. We should note that for a more detailed account we could use [2] and [4]. This introduction section will follow closely the ideas from [2]. The lemmas in this section are from [2].

Lemma 3. *Let Q be a probability on a group G of order n. Then for any positive integer m,*

$$4\|Q^{*m} - U\|^2 \leq \sum_{\Omega} nQ(x_1)\cdots Q(x_{2m}) - \sum_{G^{2m}} Q(x_1)\cdots Q(x_{2m}),$$

where G^{2m} is the set of all $2m$-tuples $(x_1, \cdots, x_{2m})$ with $x_i \in G$ and Ω is the subset of G^{2m} consisting of all $2m$-tuples such that $x_1x_2\cdots x_m = x_{m+1}x_{m+2}\cdots x_{2m}$.

The following lemma corresponds to Lemma 8 of [4].

Lemma 4. *$N_\pi(\tau)$ is the number of i-tuples $(y_1, \cdots, y_i)$ with distinct coordinates in G that are solutions to the induced equation obtained from $x_1\cdots x_m = x_{m+1}\cdots x_{2m}$ by substituting y_j for x_l if $l \in \Delta_j$.*

Lemma 5. *Suppose $(a_1, \cdots, a_k)$ are chosen uniformly from all k-tuples with distinct elements of G. Also suppose that $Q(a_i) = 1/k$. Then,*

$$4E(\|Q^{*m} - U\|^2) \leq \sum_{i=1}^{\min(k,2m)} \sum_{\pi\in P(i)} \frac{1}{k^{2m}} \frac{[k]_i}{[n]_i} \sum_{\tau\in T(\pi)} (nN_\pi(\tau) - [n]_i),$$

where

$$[n]_i = n(n-1)\cdots(n-i+1),$$

and $P(i)$ is the set of all i-partitions of $2m$ and finally $T(\pi)$ is the set of all types which correspond to π.

Note. In proving the main Theorem 1 by Dou we would need the following lemma.

Lemma 6. *If G is an Abelian group satisfying the conditions for Theorem 1 and $m = c(n)n^{2/(k-1)}$, where $c(n) \to \infty$ as $n \to \infty$ such that*

$$c(n) < n^{(1/L)-(2/(k-1))} A^{-1+(1/L)},$$

then for each k-type τ, either $N_\pi(\tau) = [n]_k$ or $N_\pi(\tau) \leq [n]_{k-1}$. If $T_1 = \{k-$ types $\tau | N_\pi(\tau) = [n]_k\}$ and $T_2 = \{k-$types $\tau | N_\pi(\tau) \leq [n]_{k-1}\}$, then $|T_1|+|T_2| =$

$S_{2m,k}$ *and*

$$|T_1| \leq \kappa_{m,k} := \sum_{r_1+\cdots+r_k=m,\ r_1,\cdots,r_k\geq 0} \binom{m}{r_1,\cdots,r_k}^2 .$$

3. Proof of Main Result

Proof. We will use Lemma 5 and follow a similar argument to the one in Chapter 4.4 of [4] but we could also use [2]. Let

$$B_1 = \sum_{i=1}^{k-1} \sum_{\pi\in P(i)} \frac{1}{k^{2m}} \frac{[k]_i}{[n]_i} \sum_{\tau\in T(\pi)} (nN_\pi(\tau) - [n]_i).$$

It can be shown that $nN_\pi(\tau) - [n]_i \leq n[n]_i$. So,

$$\begin{aligned} B_1 &\leq \sum_{i=1}^{k-1} \sum_{\pi\in P(i)} \frac{1}{k^{2m}} \frac{[k]_i}{[n]_i} \sum_{\tau\in T(\pi)} n[n]_i \\ &= (1/k^{2m})n \sum_{i=1}^{k-1} [k]_i \sum_{\pi\in P(i)} \sum_{\tau\in T(\pi)} 1 \\ &= (1/k^{2m})n \sum_{i=1}^{k-1} [k]_i S_{2m,i}\,. \end{aligned}$$

We note that $S_{2m,i}$ is a Stirling number of the second kind, that is, this number is the number of ways to place $2m$ labeled balls in i unlabeled boxes such that there are no empty boxes. Hence we can state

$$\sum_{\pi\in P(i)} \sum_{\tau\in T(\pi)} 1 = S_{2m,i}\,.$$

Note.

$$(k-1)^{2m} = \sum_{i=1}^{k-1} [k-1]_i S_{2m,i}\,.$$

Note.

$$[k]_i = \frac{k[k-1]_i}{k-i} \leq k[k-1]_i\,,$$

and this is true if $k - i \geq 1$ but we know that $i \leq (k-1)$.

Thus, using the last two notes we find the following bound on B_1:

$$B_1 \leq k\frac{1}{k^{2m}}n(k-1)^{2m} = kn(\frac{k-1}{k})^{2m} \to 0$$

as $n \to \infty$ for the specified m.

Now, let $i = k$ and define

$$B_2 = \sum_{\tau} \frac{[k]_k}{[n]_k}(nN_\pi(\tau) - [n]_k)\,,$$

where the sum is over all k-partitions of the set $\{1, 2, \cdots, m\}$. To bound B_2 we will use the following lemma.

Recall that λ_i is the number of times y_i is substituted for x_j with $1 \leq j \leq m$ minus the number of times y_i is substituted for x_j with $(m+1) \leq j \leq 2m$. Or, another way to think of λ_i is that $\lambda_i = |\Delta_i \cap \{1, \cdots, m\}| - |\Delta_i \cap \{m+1, \cdots, 2m\}|$.

Lemma 7. *If G is an Abelian group satisfying the new restrictions then, for each k-type τ either*

$$N_\pi(\tau) = [n]_k,\ N_\pi(\tau) \leq [n]_{k-1},\ [n]_{k-1} < N_\pi(\tau) < [n]_k.$$

If

$$T_1 = \{k - \text{types } \tau | \lambda_i = 0 for\ all\ i\},$$

$$T_2 = \{k - \text{types } \tau | there\ exist\ \lambda_i\ such\ that\ (\lambda_i, n_j) = 1\ for\ all\ n_j\},$$

$$and\ T_3 = \{k - \text{types } \tau | other\}\,,$$

then $|T_1| + |T_2| + |T_3| = S_{2m,k}$ and

$$|T_1| \leq \sum_{r_1+\cdots+r_k=m,\ r_1,\cdots,r_k \geq 0} \binom{m}{r_1, \cdots, r_k}^2,$$

$$|T_3| \leq k^{2m} m^{(1-k)/2}\,.$$

We note that if we used Dou's restrictions then $|T_3| = 0$ since $m < n_t$ (look at [4] for a more detailed description of Dou's restrictions).

Before we prove the above lemma let us look an example to help acquaint us with the terminology.

Example. If $G = \mathbb{Z}_3 \times Z_4 \times Z_9$ and the induced equation is $4y_1 - 4y_2 + 0y_3 + 0y_4 = 0$ then we will pick y_2, y_3, y_4 distinctly in $[108]_3$ possible ways. Now that leaves the element $y_1 = (a_1, a_2, a_3)$, where the coordinates a_1 and a_3 are defined by the choices we have made for the other y_i. The thing to note is that the coordinate a_2 can be any of the 4 possible choices and all of these choices will still solve the induced equation. Thus, the k-type τ that corresponds to

the induced equation is an element of T_3 since $N_\pi(\tau) \leq 4[108]_3$.

In conclusion if all the $\lambda_i = 0$ under the group G then $N_\pi(\tau) = [n]_k$ and we are in set T_1. Also, if for some j we find that $\lambda_j \neq 0$ for all the modular classes then y_j is solvable in terms of the other y_i. Hence $N_\pi(\tau) \leq [n]_{k-1}$ which places us in set T_2. The rest of the cases will be in T_3.

Proof. $|T_1| + |T_2| + |T_3| = S_{2m,k}$ follows straight from the definitions.

We note if $\lambda_1 = \cdots = \lambda_k = 0$ then $\tau = \{\Delta'_1 \cup \Delta''_1, \cdots, \Delta'_k \cup \Delta''_k\}$, where $\tau' = \{\Delta'_1, \cdots, \Delta'_k\}$ and $\tau'' = \{\Delta''_1, \cdots, \Delta''_k\}$ are k-types of $\{1, \cdots, m\}$ and $\{m+1, \cdots, 2m\}$ respectively with $|\Delta'_i| = |\Delta''_i|$ for $i = 1, 2, \cdots, k$. So, the number of choices for τ' is $\binom{m}{r_1, \cdots, r_k}$ and the number of choices for τ'' is $\binom{m}{r_1, \cdots, r_k}$. Hence,

$$|T_1| \leq \sum_{r_1 + \cdots + r_k = m,\ r_1, \cdots, r_k \geq 0} \binom{m}{r_1, \cdots, r_k}^2$$

is easy to see once you define $r_i = |\Delta'_i| = |\Delta''_i|$ for $i = 1, \cdots, k$. We will prove that $|T_3| \leq k^{2m} m^{(1-k)/2}$ in Lemma 9.

Hence, Lemma 7 is proved. □

Thus, $B_2 \leq B_{2,1} + B_{2,2} + B_{2,3}$, where

$$B_{2,1} = \sum_{\tau \in T_1} \frac{1}{k^{2m}} \frac{[k]_k}{[n]_k} (n-1)[n]_k \,,$$

$$\begin{aligned} B_{2,2} &= \sum_{\tau \in T_2} \frac{1}{k^{2m}} \frac{[k]_k}{[n]_k} (nN_\pi(\tau) - [n]_k) \\ &\leq \sum_{\tau \in T_2} \frac{1}{k^{2m}} \frac{[k]_k}{[n]_k} (n[n]_{k-1} - [n]_k) \\ &= \sum_{\tau \in T_2} \frac{1}{k^{2m}} \frac{[k]_k}{[n]_k} (n[n]_{k-1} - [n]_{k-1}(n-k+1)) \\ &= \sum_{\tau \in T_2} \frac{1}{k^{2m}} \frac{[k]_k}{[n]_k} (k-1)[n]_{k-1} \,, \end{aligned}$$

$$B_{2,3} = \sum_{\tau \in T_3} \frac{1}{k^{2m}} \frac{[k]_k}{[n]_k} (n-1)[n]_k \,.$$

Now,

$$B_{2,2} \leq (k-1) \frac{1}{k^{2m}} [k]_k \cdot |T_2| \cdot \frac{1}{n-k+1}$$

$$\begin{aligned} &\leq (k-1)\frac{1}{k^{2m}}[k]_k \cdot S_{2m,k} \cdot \frac{1}{n-k+1} \\ &\leq (k-1)\frac{1}{k^{2m}}k^{2m}\frac{1}{n-k+1} \\ &= \frac{k-1}{n-k+1} \to 0\,, \end{aligned}$$

where the convergence to zero is as $n \to \infty$. We should note that the second inequality is due to Lemma 7 and the fact that $|T_2| \leq S_{2m,k}$. The final inequality is due to the fact that $S_{2m,k} \leq \frac{k^{2m}}{k!}$.

Next,

$$\begin{aligned} B_{2,1} &\leq \frac{1}{k^{2m}}[k]_k(n-1)|T_1| \\ &\leq \frac{1}{k^{2m}}[k]_k(n-1)\cdot \sum_{r_1+\cdots+r_k=m,\ r_1,\cdots,r_k\geq 0} \binom{m}{r_1,\cdots,r_k}^2 \\ &\leq \frac{1}{k^{2m}}[k]_k(n-1)\cdot c_0 k^{2m} m^{(1-k)/2} \\ &\leq c(n-1)\cdot c_0 m^{(1-k)/2} \to 0\,, \end{aligned}$$

where the convergence to zero is as $n \to \infty$ and the value for c may depend on k but not n. The second inequality is due to Lemma 7 and the third inequality is due to a lemma in the appendix of [2]. The lemma in the appendix of Dou's thesis and a quick but different proof will be shown next.

Lemma 8. *For a positive constant c_0 that may depend on k*

$$K_{m,k} := \sum_{r_1+\cdots+r_k=m,\ r_1,\cdots,r_k\geq 0} \binom{m}{r_1,\cdots,r_k}^2 \leq c_0 k^{2m} m^{(1-k)/2}\,.$$

Proof. Observe

$$K_{m,k} \leq \left[\max_{r_1+\cdots+r_k=m,\ r_1,\cdots,r_k\geq 0} \binom{m}{r_1,\cdots,r_k}\right]\cdot k^m\,,$$

since using the definition of the multinomial coefficient gives

$$\sum_{r_1+\cdots+r_k=m,\ r_1,\cdots,r_k\geq 0} \binom{m}{r_1,\cdots,r_k} = k^m.$$

Now,

$$\begin{aligned} &\max_{r_1+\cdots+r_k=m,\ r_1,\cdots,r_k\geq 0} \binom{m}{r_1,\cdots,r_k} \\ &\quad\leq \frac{m!}{(\lfloor m/k\rfloor!)^k}\cdot\frac{1}{(m/k)^{m-k\lfloor m/k\rfloor}} \end{aligned}$$

$$\leq \frac{e^{-m}m^m\sqrt{2\pi m}}{e^{-k\lfloor m/k\rfloor}\lfloor m/k\rfloor^{k\lfloor m/k\rfloor}(\sqrt{2\pi\lfloor m/k\rfloor})^k}\cdot\frac{1}{(m/k)^{m-k\lfloor m/k\rfloor}}$$

$$\leq \frac{e^{-m+k\lfloor m/k\rfloor}m^m\sqrt{2\pi}m^{1/2}}{((m/k)+g(m/k))^{k\lfloor m/k\rfloor}(2\pi[(m/k)+g(m/k)])^{k/2}}\cdot\frac{1}{(m/k)^{m-k\lfloor m/k\rfloor}}$$

$$\leq \frac{c_1e^{-m+k\lfloor m/k\rfloor}\sqrt{2\pi}m^{1/2}}{(1/k)^m(m/k)^{k/2}}$$

$$\leq c_0k^mm^{(1-k)/2}.$$

Note that $g(m,k)=\lfloor m/k\rfloor-(m/k)$ and so $|g(m/k)|\leq 1$. We also note that the negative exponential can be bounded by a positive constant and that $c_1>0$ is a constant. Hence we have a bound similar to the one that Carl Dou found. □

Last,

$$\begin{aligned} B_{2,3} &\leq \frac{1}{k^{2m}}\frac{[k]_k}{[n]_k}[n]_k(n-1)|T_3| \\ &\leq \frac{1}{k^{2m}}[k]_k(n-1)k^{2m}m^{(1-k)/2} \\ &= [k]_k(n-1)m^{(1-k)/2}\to 0\,, \end{aligned}$$

where the convergence to zero is due to n going to infinity. Thus, with the help of the next lemma the theorem is proven. □

Lemma 9. *For some i let $r_i\neq r_i'$ and note*

$$\sum_{i=1}^k r_i=\sum_{i=1}^k r_i'=m$$

then

$$\sum_{A_1}\frac{(m!)^2(1/k)^{2m}}{r_1!\cdots r_k!r_1'!\cdots r_k'!}\ll m^{(1-k)/2}$$

with $A_1=\{(r_1,\cdots,r_k,r_1',\cdots,r_k')|r_i-r_i'\equiv 0\pmod{n_j}$ for $i=1,\cdots,k$ for some j depending on i }.

We note that with A_1 as described above

$$|T_3|=\sum_{A_1}\frac{(m!)^2}{r_1!\cdots r_k!r_1'!\cdots r_k'!}\,.$$

This is true since $m=r_1+r_2+\cdots+r_k$ and the number of ways to pick r_1 in m trials is $\binom{m}{r_1}$. Plus, the number of ways to pick r_2 in the remaining $(m-r_1)$ trials is $\binom{m-r_1}{r_2}$ and so the total number of possible sequences for m is $\frac{m!}{r_1!r_2!\cdots r_k!}$. Hence the cardinality of T_3 is as stated above.

Proof.

Claim 10.

$$np_i - 1 < k_i \leq (n + r - 1)p_i$$

for $i = 1, 2, \cdots, r$ and where k_i is the maximal term of the multinomial distribution.

Note that Claim 10 is an exercise on p. 171 of [3] and so is left as an exercise.

Now, to prove the lemma we will follow similar arguments to the ones in [1].

By using Claim 10 we can observe

$$\max_{r_1,\cdots,r_k} \left[\frac{m!(1/k)^m}{r_1! \cdots r_k!} \right] \leq \frac{m!(1/k)^m}{m_1! \cdots m_k!}$$

for some nonnegative integers $m_1, \cdots, m_k$ with $m_1 + \cdots + m_k = m$ and $|m_l - (m/k)| < k$ for $l = 1, \cdots, k$. Hence, $(m/k) - k < m_l < (m/k) + k$ and without loss of generality we may assume m is large enough so that m_l is positive for $l = 1, \cdots, k$. Consider for some l that either $|r_l - m_l| \geq (n_j/2)$ or $|r'_l - m_l| \geq (n_j/2)$. Now, this is true since by definition of A_1 for some l we know $|r_l - r'_l| \neq 0$. But, for some j we know $r_i \equiv r'_i \pmod{n_j}$ and this implies that $|r_l - r'_l| \geq n_j$ for some l, for some j. So, $|r_l - m_l - r'_l + m_l| \leq |r_l - m_l| + |r'_l - m_l|$ implies $|r_l - m_l| \geq (n_j/2)$ or $|r'_l - m_l| \geq (n_j/2)$. We shall assume $r_1 - m_1 \geq (n_j/2)$ but the other cases can be treated similarly.

Note.

$$(m!)^2 \prod_{l=1}^{k} \frac{(1/k)^{2m_l}}{(m_l!)^2} < 1\,.$$

The reason the note is valid is because the left-hand side is the square of the probability of a particular multinomial distribution with m trials and $m_1, \cdots, m_k$ outcomes each with probability $(1/k)$. It is a probability and so must be less than or equal to one. Now, if $k \geq 2$ then we have strictly less than 1 since there is more than one possibility for $m_1, \ldots, m_k$ which has positive probability of occurring.

Consider

$$\frac{\left[(m!)^2 \prod_{l=1}^{k} \left(\frac{(1/k)^{r_l + r'_l}}{r_l! r'_l!} \right) \right] m^{2m}}{(m!)^2 \prod_{l=1}^{k} \left(\frac{(1/k)^{2m_l}}{(m_l!)^2} \right) m^{2m}} = \prod_{l=1}^{k} \frac{(m_l!)^2}{r_l! r'_l!} \cdot \frac{(m/k)^{r_l + r'_l}}{(m/k)^{2m_l}}$$

$$\leq \left(\prod_{l=1}^{k}\left(\max\left(1,\frac{m_l}{(m/k)}\right)^{2k}\right)\right)\frac{m/k}{m_1+1}\cdots\frac{m/k}{m_1+\lfloor n_j/2\rfloor}$$

$$\leq c_2\cdot\frac{m_1+k}{m_1+k+1}\frac{m_1+k}{m_1+k+2}\cdots\frac{m_1+k}{m_1+\lfloor n_j/2\rfloor}$$

$$\leq \frac{c_2}{(1+1/(m_1+k))(1+2/(m_1+k))\cdots(1+(\lfloor n_j/2\rfloor-k)/(m_1+k))},$$

where the term in the first bracket is the term that we are summing over A_1 with. Now, the first inequality will be proven by Claim 13 and the second inequality will be shown by Claim 12. The last inequality is a re-write of the line above it. Hence,

$$\prod_{l=1}^{k}\frac{(m_l!)^2}{r_l!r_l'!}\cdot\frac{(m/k)^{r_l+r_l'}}{(m/k)^{2m_l}}\leq\frac{c_2}{(1+\lfloor(1/2)\lfloor n_j/2\rfloor\rfloor/(m_1+k))^{\lfloor(1/2)\lfloor n_j/2\rfloor\rfloor-k}},$$

where the base of the denominator is the middle term of the last inequality and the exponent is the number of terms that we will be replacing. Thus, for some positive constants c_2, c_3, and c_4 and sufficiently large n

$$\prod_{l=1}^{k}\frac{(m_l!)^2}{r_l!r_l'!}\cdot\frac{(m/k)^{r_l+r_l'}}{(m/k)^{2m_l}}\leq c_2e^{\frac{-c_3(n^{\epsilon+1/(k-1)})^2}{m_1}}\leq c_2e^{\frac{-c_3(n^{\epsilon+1/(k-1)})^2}{m}}\leq c_2e^{-c_4n^{\epsilon}}.$$

We note that the first inequality will be proven by Claim 11. The last inequality is due to

$$\frac{(n^{\epsilon}n^{1/(k-1)})^2}{m}>\frac{(n^{\epsilon}n^{1/(k-1)})^2}{n^{\epsilon}n^{2/(k-1)}}=n^{\epsilon},$$

where without loss of generality we can assume $\sigma(n)\ll n^{\epsilon}$. Hence, each term in A_1 is less than or equal to $c_2e^{-c_4n^{\epsilon}}$. Now, there exists less than $(m+1)^{2k}$ terms in A_1 since for each r_i we have a choice of $0,1,\cdots,m$ and r_i,r_i' have to be filled. So, we conclude that

$$\sum_{A_1}\frac{(m!)^2(1/k)^{2m}}{r_1!\cdots r_k!r_1'!\cdots r_k'!}<(m+1)^{2k}\cdot c_2e^{-c_4n^{\epsilon}}\ll m^{(1-k)/2}$$

as $n\to\infty$. We note that $f(n)\ll g(n)$ if $\lim_{n\to\infty}\frac{f(n)}{g(n)}=0$.

So,

$$\begin{aligned}\lim_{n\to\infty}\left(\frac{m^{2k}e^{-c_4n^{\epsilon}}}{m^{(1-k)/2}}\right) &\leq m^{2k-(1-k)/2}e^{-c_4n^{\epsilon}}\\ &\leq n^{\epsilon(2k-(1-k)/2)}n^{(4k)/(k-1)-1}e^{-c_4n^{\epsilon}}\\ &\leq n^{3k\epsilon+8}e^{-c_4n^{\epsilon}}\to 0,\end{aligned}$$

where convergence to zero is as $n\to\infty$. Thus we have proved the lemma using

the following claims. □

Claim 11.

$$\frac{c_2}{(1+\lfloor(1/2)\lfloor n_j/2\rfloor\rfloor/(m_1+k))^{\lfloor(1/2)\lfloor n_j/2\rfloor\rfloor-k}} \leq c_2 e^{\frac{-c_3(n^{\epsilon+1/(k-1)})^2}{m_1}}$$

for some positive constants c_2 and c_3.

Proof. Note,

$$\frac{\lfloor(1/2)\lfloor n_j/2\rfloor\rfloor}{m_1+k} \approx \frac{n_j}{4m_1} \geq \frac{n^{\epsilon+1/(k-1)}}{(4\sigma(n)n^{2/(k-1)})/k} \to 0\,.$$

To get the approximation we note that k is fixed and that as $n_j \to \infty$ the floor will not matter. The limit goes to zero as $n \to \infty$ using the bounds we have on m.

Now, recall two usual limits.

First, if $\ln(x+1) = xf(x)$ then $f(x) = \frac{\ln(x+1)}{x} \to 1$ as $x \to 0$.

Second,

$$\lim_{x\to 0} \frac{e^{cx}-1}{x} = c$$

which implies that $x+1 = e^{f(x)x}$ with $f(x) \to 1$ as $x \to 0$.

Hence,

$$1 + \frac{n^{\epsilon+1/(k-1)}}{(4\sigma(n)n^{2/(k-1)})/k} = e^{f(\frac{n^{\epsilon+1/(k-1)}}{(4\sigma(n)n^{2/(k-1)})/k})\frac{n^{\epsilon+1/(k-1)}}{(4\sigma(n)n^{2/(k-1)})/k}}\,.$$

Thus,

$$\begin{aligned}
&\frac{c_2}{(1+\lfloor(1/2)\lfloor n_j/2\rfloor\rfloor/(m_1+k))^{\lfloor(1/2)\lfloor n_j/2\rfloor\rfloor-k}} \\
&\quad\leq \frac{c_2}{(1+\frac{n^{\epsilon+1/(k-1)}}{(4\sigma(n)n^{2/(k-1)})/k})^{\lfloor(1/2)\lfloor n_j/2\rfloor\rfloor-k}} \\
&\leq c_2 / \left(e^{f(\frac{n^{\epsilon+1/(k-1)}}{(4\sigma(n)n^{2/(k-1)})/k})\frac{n^{\epsilon+1/(k-1)}}{(4\sigma(n)n^{2/(k-1)})/k}} \right)^{(1/4)n_j(1+o(1))} \\
&\quad\leq c_2 e^{\frac{-c_3(n^{\epsilon+1/(k-1)})^2}{m_1}}
\end{aligned}$$

for some positive constant c_3 and so the claim is proved. □

Claim 12.

$$\left(\prod_{l=1}^{k}\left(\max\left(1,\frac{m_l}{(m/k)}\right)^{2k}\right)\right)\frac{m/k}{m_1+1}\cdots\frac{m/k}{m_1+\lfloor n_j/2\rfloor}$$

$$\leq c_2 \cdot \frac{m_1+k}{m_1+k+1}\frac{m_1+k}{m_1+k+2}\cdots\frac{m_1+k}{m_1+\lfloor n_j/2\rfloor}$$

for some positive constant c_2.

Proof. Since $|m_l-(m/k)| < k$ this implies $m_l < (m/k)+k$. So, $(m_l)/(m/k) < ((m/k)+k)/(m/k) = 1+(k^2/m) \to 1$ as m goes to infinity and k is fixed. So,

$$\prod_{l=1}^{k}\left(\max\left(1,\frac{m_l}{(m/k)}\right)^{2k}\right) \to 1$$

will be part of a constant c_2.

Now, $m_1-k < (m/k) < m_1+k$ so

$$[\frac{m/k}{m_1+1}\frac{m/k}{m_1+2}\cdots\frac{m/k}{m_1+k-1}][\frac{m/k}{m_1+k}][\frac{m/k}{m_1+k+1}\cdots\frac{m/k}{m_1+\lfloor n_j/2\rfloor}]\,.$$

We note that in the first bracket each term is bounded by 1 as $m\to\infty$ since $(m/k) < m_1+k$ so these terms will be grouped into the constant c_2. The middle bracket term is less than one so it will also be grouped under the constant c_2. Last but not least the third bracket terms all have numerators less than m_1+k so replace them in the bound. Hence this claim is proved. □

Claim 13.

$$\prod_{l=1}^{k}\frac{(m_l!)^2}{r_l!r_l'!}\cdot\frac{(m/k)^{r_l+r_l'}}{(m/k)^{2m_l}}$$

$$\leq\left(\prod_{l=1}^{k}\left(\max\left(1,\frac{m_l}{(m/k)}\right)^{2k}\right)\right)\frac{m/k}{m_1+1}\cdots\frac{m/k}{m_1+\lfloor n_j/2\rfloor}\,.$$

Proof. This proof is left as an excercise for the reader. □

4. Questions for Further Study

We have extended the work of Carl Dou's thesis but can it be extended further than what has been done? We could ask, for the τ in T_3 can we improve on the bound that $[n]_{k-1} < N_\pi(\tau) < [n]_k$?

Acknowledgements

The author would like to acknowledge that this paper is based on a part of the author's Ph.D. thesis [5]. The author would like to thank Martin Hildebrand for suggesting this problem. The author would also like to thank Scott Bianco, a graduate student at SUNY Albany, for finding some errors in the bounds. Finally, the author would like to thank Marcus Jaiclin of Westfield State College for technical assistance.

References

[1] J. Dai, M. Hildebrand, Random random walks on integers mod$n$, *Statistics and Probability Letters*, **35** (1997), 371-379.

[2] Carl Dou, *Studies of Random Walks on Groups and Random Graphs*, Ph.D. Dissertation, Mass. Institute of Technology (1992).

[3] William Feller, *Introduction to Probability Theory and its Applications*, Volume 1, Third Edition, John Wiley (1968).

[4] Martin Hildebrand, A survey of results on random random walks on finite groups, *Probability Surveys*, **2** (2005).

[5] Joseph McCollum, *Random Walks on the Dihedral Group and Abelian Group*, Ph.D. Dissertation, SUNY Albany, Department of Mathematics (2006).

[6] L. Saloff-Coste, *Probability on Discrete Structures*, Volume 110, Springer-Verlag (2004).