ASYMPTOTICALLY UNIFORM PERIOD DISTRIBUTION FOR BINARY EXPANSIONS OF RATIONAL NUMBERS

GAL PORAT

What is to be presented here is a joint work with Guy Kapon under the supervision of Ofir David and Uri Shapira. The work up to section 3 was carried out in a research project in the Technion Institute of Technology, while section 4 was done later by the author.

1 Introduction

Let n be an odd number. It is well known that the binary expansion of $\frac{1}{n}$ is periodic and that the length of this period is $ord_n(2)$, the order of 2 in $(\mathbb{Z}/n\mathbb{Z})^\times$.

For each k, we see that $\frac{1}{n}$ induces a probabily measure on the set of binary strings of length k. Denote this probabily measure by $\lambda_{n,k}$. For example, the period of $\frac{1}{7} = (0.001001001...)_2$ is 001. For $k = 2$, each of the strings $00, 01, 10$ occur with probability $1/3$ and the string 11 occures with probability 0.

We are interested in finding sets of natural numbers $S = \{n_i\}_{i=1}^{\infty} = \{n_1 < n_2 < ...\}$ of large density such that the digits of the periods in this set tend to be uniformly distirbuted. In other words, if λ_k denotes the uniform measure on binary strings of length k, we want to have $\lambda_{n_i,k} \to \lambda_k$ for each k as $i \to \infty$.

Definition 1. *Let $S = \{n_i\}_{i=1}^{\infty}$ an infinite sequence of natural numbers. We say that S has asymptotically uniform period distribution (or AUPD for short) if $\lambda_{n_i,k} \to \lambda_k$ for every $k \geq 1$.*

Equivalently, we may consider for each n the subset of $S^1 = \mathbb{R}/\mathbb{Z}$ defined by

$$A = \left\{ \frac{2^i}{n} (\text{mod } \mathbb{Z}) | 0 \leq i < ord_n(2) \right\}$$

The number of 0's appearing in the period of $\frac{1}{n}$ is just the number of points of A on the first half of S^1; the number of 00's appearing in the period of $\frac{1}{n}$ is the number of points of A on the first quarter of S^1; and so on. We wish to find interesting sets S of large density such that these points tend to be uniformly distributed on S^1 as $n \to \infty$ for $n \in S$.

In section 2 we prove a a criterion for asymptotically uniform period distribution. In section 3 we use this criterion in order to prove our main theorem which gives the three main examples of interesting sequences which have AUPD. In section 4 we prove a generalization of one example of the main theorem.

2 A criterion for asymptotically uniform period distribution

Definition 2. *For n an odd integer, we define a measure on S^1,*

$$\mu_{\frac{1}{n}} := \frac{1}{ord_n(2)} \sum_{i=0}^{ord_n(2)-1} \delta_{\frac{2^i}{n}}$$

where the δ's are dirac measures. In other words, $\mu_{\frac{1}{n}}$ is the orbit measure with respect to the action $x \mapsto 2x$ and $\frac{1}{n} \in S^1$.

If $\mu_{\frac{1}{n_i}} \to \lambda_{Haar}$ then for each k we have $\mu_{\frac{1}{n_i}}([0, \frac{1}{2^k}]) \to \frac{1}{2^k}$, so this just means that the proportion of 00...0 segements tends to $\frac{1}{2^k}$. The same will hold for any other segment. In the other direction one also sees that if $\mu_{\frac{1}{n_i}}([0, \frac{1}{2^k}]) \to \frac{1}{2^k}$ for each k then the distribution must tend to the uniform distribution. We conclude this with the following proposition:

Proposition 1. *An infinite sequence $S = \{n_i\}_{i=1}^{\infty}$ has AUPD if and only if $\mu_{\frac{1}{n_i}} \to \lambda_{Haar}$ as measures on S^1.*

Since $S^1$is compact, this is equivalent to having the convergence for every nontrival character, i.e. for each $k \neq 0$ we want:

$$\int e^{2\pi kti} d\mu_{\frac{1}{n_i}}(t) \to \int e^{2\pi kti} d\lambda(t) = 0$$

Let ζ be an n'th root of unity. Since $\int e^{2\pi kti} d\mu_{\frac{1}{n_i}}(t) = \frac{1}{ord_{n_i}(2)} \sum_{j=0}^{ord_{n_i}(2)-1} \zeta^{k2^j}$, we can therefore refine the proposition above to

Proposition 2. *S has AUPD if and only if $\frac{1}{ord_{n_i}(2)} \sum_{j=0}^{ord_{n_i}(2)-1} \zeta^{k2^j} \to 0$ for each $k \neq 0$.*

Although the property we are investigating is *multiplicative* in nature, the key to our understanding of these sums lies in our interpertation of them as certain *additive* discrete Fourier transforms.

Proposition 3. *Let $1_{<2>} : \mathbb{Z}/n\mathbb{Z} \to \{0, 1\}$ be the indicator function for the subgroup $< 2 >$, and let $\widehat{1_{<2>}} : \widehat{\mathbb{Z}/n\mathbb{Z}} :\to \mathbb{C}$ be its discrete Fourier transform with respect to the additive group $\mathbb{Z}/n\mathbb{Z}$. Recall there is an isomorphism $\mathbb{Z}/n\mathbb{Z} \simeq \widehat{\mathbb{Z}/n\mathbb{Z}}$ defined by*

$$k \mapsto (\chi_k : 1 \mapsto \zeta^k)$$

where ζ is a fixed n'th root of unity. We then have

(1) $\widehat{1_{<2>}}(\chi_{-k}) = \sum_{j=0}^{ord_n(2)-1} \zeta^{k2^j}$

(2) $\sum_k |\widehat{1_{<2>}}(\chi_k)|^2 = nord_n(2)$

Proof. (1) is immediate from the definition of the Fourier transform, and (2) is Parseval's equality. □

For the corollary to be proven next one first needs to obtain a technical lemma.

Lemma 1. *Let $t, n \in \mathbb{N}$ such that $t|n$. Then $ord_{\frac{n}{t}}(2) \geq \frac{ord_n(2)}{t}$.*

Proof. We can immediately reduce to the case where $t = p$ is a prime and n is odd. We split the proof into two cases.

Case 1: suppose $p^2|n$. We have $\frac{n}{p}|2^{ord_{\frac{n}{p}}(2)} - 1$, and in particular $p|2^{ord_{\frac{n}{p}}(2)} - 1$. It is well known that for p and odd prime and for coprime x, y with $x \equiv y (\text{mod } p)$, one has

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n)$$

Where v_p is the p-adic valuation. Applying this to $x = 2^{pord_{\frac{n}{p}}(2)}$ and $y = 1$ we get that $n|2^{pord_{\frac{n}{p}}(2)} - 1$. Hence $ord_n(2) \leq pord_{\frac{n}{p}}(2)$ which is equivalent to the statement.

Case 2: suppose $p^2 \nmid n$, so that p and $\frac{n}{p}$ are coprime. Again $\frac{n}{p}|2^{ord_{\frac{n}{p}}(2)} - 1$, so by Fermat's little theorem $n|2^{ord_{\frac{n}{p}}(2)(p-1)} - 1$. Thus, $ord_n(2) \leq (p-1)ord_{\frac{n}{p}}(2) \leq pord_{\frac{n}{p}}(2)$. □

We now obtain the following key estimate.

Corollary 1. *For $k \neq 0$, $\widehat{|1_{<2>}}(\chi_k)| \leq \sqrt{n}\sqrt{gcd(k,n)}$*

Proof. Clearly $| < 2 > k| = ord_{\frac{n}{gcd(k,n)}}(2)$. Now consider part (2) of Proposition 3. The summand $\widehat{|1_{<2>}}(\chi_k)|$ appears $| < 2 > k|$ times on the left hand side of the equation, so $ord_{\frac{n}{gcd(k,n)}}(2)\widehat{|1_{<2>}}(\chi_k)|^2 \leq ord_n(2)(n - ord_n(2))$. Using the previous Lemma we deduce that $\widehat{|1_{<2>}}(\chi_k)|^2 \leq ngcd(k,n)$, hence $\widehat{|1_{<2>}}(\chi_k)| \leq \sqrt{n}\sqrt{gcd(k,n)}$. □

This enables us to prove a very useful theorem for proving that sequences have AUPD.

Theorem 1. (Criterion for AUPD) *Let $\{n_i\} = S$ be an infinite set such that*

$$\frac{\sqrt{n_i}}{ord_{n_i}(2)} \to 0$$

Then S has AUPD.

Proof. Indeed, for any fixed $k \neq 0$ we have $\frac{1}{ord_{n_i}(2)}|\sum_{j=0}^{ord_{n_i}(2)-1}\zeta^{k2^j}| = \frac{\widehat{|1_{<2>}}(\chi_{-k})|}{ord_{n_i}(2)} \leq \frac{\sqrt{n_i}\sqrt{gcd(k,ord_{n_i}(2))}}{ord_{n_i}(2)} \to 0$, which guarantees that S has AUPD by Proposition 2. □

3 The main theorem

For the next theorem, we quote the following results. We denote by $\mathbb{P}$ the set of prime numbers.

[1], Theorem 4.1. *There exists a subset $\mathbb{P}' \subset \mathbb{P}$ of density 1 and some $\delta > 0$ such that $ord_p(2) > \sqrt{p}exp((logp)^\delta)$ for all $p \in \mathbb{P}'$.*

[2], Theorem 1. *If the Generalized Riemann Hypothesis holds, there is a subset $\mathbb{N}' \subset \mathbb{N}$ of density 1 and some $\varepsilon > 0$ such that $ord_n(2) > n^{1-\varepsilon}$ (where $ord_n(2)$ of an even number is defined in the natural way as the length of the period of 2 in $\mathbb{Z}/n\mathbb{Z}$).*

We now arrive at our main theorem.

Theorem 2. *(1) Let $p_1, ..., p_t$ be a finite set of primes, and let $S \subset \mathbb{N}$ be the set of numbers divisible only by $p_1, ..., p_t$. Then S has AUPD.*

(2) Let $\mathbb{P}$ be the set of primes. There is a density 1 subset $\mathbb{P}' \subset \mathbb{P}$ such that $\mathbb{P}'$ has AUPD.

(3) Assuming GRH, there is a subset $\mathbb{N}' \subset \mathbb{N}$ that has AUPD.

Proof. (1) It is easy to see that in such a case $\frac{n}{ord_n(2)}$ is bounded; now use the previous theorem.

(2) Use the result of [1] and the previous theorem.

(3) Use the result of [2] and the previous theorem.

4 A generalization of part (2) of the main theorem

From now on, we will focus on a generalization of part (2) of the main theorem. The result is the following.

Theorem 3. *For any fixed r, there is a set of density 1 in $T \subset \mathbb{P}^r$ such that the sequence (ordered by size)*

$$S = \{p_1...p_r : (p_1, ..., p_r) \in T\}$$

has AUPD.

Part (2) of the main theorem is the case $r = 1$. For reasons of simplicity, we will only present the case $r = 2$.

Remark. Note that the proof of part (2) of the main theorem does not immediately generalize to $r \geq 2$, the essential reason being that in order to invoke Theorem 1 one has to understand quantities of the form

$$\frac{\sqrt{p_1...p_r}}{ord_{p_1...p_r}(2)}$$

If it were true that $ord_{p_1...p_r}(2) = ord_{p_1}(2)...ord_{p_r}(2)$ up to a bounded constant the situation would have been very simple. However, in generally one only has the equality

$$ord_{p_1...p_r}(2) = lcm(ord_{p_1}(2), ..., ord_{p_r}(2)) = \frac{ord_{p_1}(2)...ord_{p_r}(2)}{gcd(\prod_{i\neq 1} ord_{p_i}(2), ..., \prod_{i\neq r} ord_{p_i}(2))}$$

In particular, for $r = 2$ we have

$$ord_{pq}(2) = \frac{ord_p(2)ord_q(2)}{gcd(ord_p(2), ord_q(2))} \geq \frac{ord_p(2)ord_q(2)}{gcd(p-1, q-1)}$$

So that $\frac{\sqrt{p_i q_i}}{ord_{p_i q_i}(2)} = \frac{\sqrt{p_i q_i} gcd(p_i-1, q_i-1)}{ord_{p_i}(2) ord_{q_i}(2)}$, and this is not guaranteed to tend to zero even if $\frac{\sqrt{p_i}}{ord_{p_i}(2)}, \frac{\sqrt{q_i}}{ord_{q_i}(2)}$ tend to zero individually.

If we still want to use the criterion, that is, to find a large subset of prime products with $\frac{\sqrt{pq}}{ord_{pq}(2)} \to 0$ when ordered by size, one way to this is to find a large subset of prime products while still keeping $gcd(p-1, q-1)$ from being too large. This is what we are going to do.

In order to initiate our control over $gcd(p-1, q-1)$, we prove the following.

Proposition 4. *The density of the set of prime pairs such that $gcd(p-1, q-1) = 2r$ is*

$$\sum_d \frac{\mu(d)}{\phi(2rd)^2}$$

Proof (a generalization of a proof conferred to the author by as an answer to a question in mathoverflow by user Lucia).

Recall the identity $\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n \neq 1 \end{cases}$. It follows that if $p \equiv q \equiv 1(2r)$, one has $1_{(p-1,q-1)=2r}(p, q) = \sum_{d|(\frac{p-1}{2r}, \frac{q-1}{2r})} \mu(d) = \sum_{d|\frac{p-1}{2r}, d|\frac{q-1}{2r}} \mu(d)$.

This enables us to write

$$\#\{p, q \leq N \mid (p-1, q-1) = 2r\} = \sum_{\substack{p,q\leq N \\ p\equiv q\equiv 1(2r)}} \sum_{d|\frac{p-1}{2r}, d|\frac{q-1}{2r}} \mu(d) = \sum_{d\leq N} \mu(d) \sum_{\substack{p,q\leq N \\ p\equiv q\equiv 1(2rd)}} 1$$

For $d > (logN)^3$ there is a trivial bound $\sum_{d\leq N} \mu(d) \sum_{\substack{p,q\leq N \\ p\equiv q\equiv 1(2rd)}} 1 \ll \sum_{(logN)^3 < d} \frac{N^2}{d^2} \ll \frac{N^2}{(logN)^3}$ which contributes nothing to the density.

For $d \leq (logN)^3$, we can use the Siegel-Walfisz theorem to get that

$$\#\{p,q \leq N \mid (p-1,q-1) = 2r\} \sim \sum_{d \leq (logN)^3} \mu(d) \sum_{\substack{p,q \leq N \\ p \equiv q \equiv 1 (2rd)}} 1 \sim \sum_{d \leq (logN)^3} \frac{\mu(d)}{\phi(2rd)^2} \frac{N^2}{(logN)^2}$$

Hence the density of such primes is precisely $\sum_d \frac{\mu(d)}{\phi(2rd)^2}$. $\square$

We rewrite the consequence of this calculation in a more convinient way.

Proposition 5. *Let A_r be the set of prime divisors of r. The density of prime pairs such that $gcd(p-1, q-1) = r$ is*

$$\frac{1}{r^2} \prod_{p \notin A_r} (1 - \frac{1}{(p-1)^2}) \prod_{p \in A_r} (1 + \frac{2}{p-1})$$

Proof. For odd r both the density and the expression are zero. Hence we can restrict to even r, and use the previous proposition. Let $T \subset A_r$ be a subset; for such T, let X_T be the set of squarefree integers that the primes of A_r that divide them are exactly T. Clearly one has

$$\sum_{d \in X_T} \frac{\mu(d)}{\phi(rd)^2} = \frac{(-1)^{|T|}}{\phi(\prod_{p \in T} p^{v_p(r)+1})^2 \phi(\prod_{p \in A_r \setminus T} p^{v_p(r)})^2} \sum_{d \in X_\emptyset} \frac{\mu(d)}{\phi(d)^2}$$

By multiplicity one has $\sum_{d \in X_\emptyset} \frac{\mu(d)}{\phi(d)} = \prod_{p \notin A_r} (1 - \frac{1}{(p-1)^2})$. Hence

$$\sum_d \frac{\mu(d)}{\phi(rd)^2} = \sum_{T \subset A_r} \sum_{d \in X_T} \frac{\mu(d)}{\phi(rd)^2} = \prod_{p \notin A_r} (1 - \frac{1}{(p-1)^2}) \sum_{T \subset A_r} \frac{(-1)^{|T|}}{\phi(\prod_{p \in T} p^{v_p(r)+1})^2 \phi(\prod_{p \in A_r \setminus T} p^{v_p(r)})^2}$$

$$= \prod_{p \notin A_r} (1 - \frac{1}{(p-1)^2}) \prod_{p \in A_r} \frac{p^2-1}{(p-1)^2 p^{2v_p(r)}} = \frac{1}{r^2} \prod_{p \notin A_r} (1 - \frac{1}{(p-1)^2}) \prod_{p \in A_r} (1 + \frac{2}{p-1})$$

So this finishes the proof. $\square$

Remark. One can also write this density as

$$\prod_{p \notin A_r} (1 - \frac{1}{(p-1)^2}) \prod_{p \in A_r} \frac{1}{(p-1)^2} \frac{1}{(p^{v_p(r)-1})^2} (1 - \frac{1}{p^2})$$

Which is what is to be expected if everything behaved independently and randomly. Indeed, one expects that the probablity for $p-1$ to be divisible by some prime l exactly $v_l(r)$ times is $\frac{1}{(l-1)^2} \frac{1}{(l^{v_l(r)-1})^2} (1 - \frac{1}{l^2})$.

Corollary 2. *For every $\varepsilon > 0$ there is some $C_\varepsilon \in \mathbb{N}$ such that the density of primes pairs p, q such that $gcd(p-1, q-1) \leq C_\varepsilon$ is at least $1-\varepsilon$. In other words, the density of prime pairs such that $gcd(p-1, q-1) \leq n$ tends to 1 as $n \to \infty$.*

Proof. Let d_r be the density of prime pairs such that $gcd(p-1, q-1) = r$ that was found in the previous proposition. It is enough to show that these d_r sum to 1. Now one calculates that if A is a set of primes, the density of prime pairs divisble precisley by the primes in A is $\prod_{p \notin A}(1 - \frac{1}{(p-1)^2}) \prod_{p \in A} \frac{1}{(p-1)^2}$. But the sum over all these A's is exactly $\prod_p (1 - \frac{1}{(p-1)^2} + \frac{1}{(p-1)^2}) = 1$ so this proves the theorem. □

Lemma 2. *Let $\mathbb{P}$ be the set of primes and let $f : \mathbb{P} \times \mathbb{P} \to \mathbb{R}$. Let $A_n = \{(p, q) \in \mathbb{P} \times \mathbb{P} : n \leq f(p, q)\}$, $A_f = \{(p, q) \in \mathbb{P} \times \mathbb{P} : gcd(p-1, q-1) \leq f(p, q)\}$. Suppose that for all n, $d(A_n) = 1$ where d denotes the density. Then $d(A_f)$=1. In particular, this holds if $f(p, q) \to \infty$ as $p + q \to \infty$.*

Proof. For all n, one has the trivial inclusion $\{(p, q) : gcd(p-1, q-1) \leq n\} \cap A_n \subset A_f$. Hence $d(A_f) \geq d(\{(p, q) : gcd(p-1, q-1) \leq n\} \cap A_n) = d(\{(p, q) : gcd(p-1, q-1) \leq n\})$, but this approaches 1 as $n \to \infty$ by the corollary. Hence we must have $d(A_f) = 1$. □

We are finally in a position to prove Theorem 3.

Proof of Theorem 3. We know there is a density 1 set of $\mathbb{P}$ such that $ord_p(2) \geq \sqrt{p}\psi(p)$ where ψ is some function that tends to infinity as p tends to infinity. Now take the density 1 set as in the previous lemma, for example one may take $f(p, q) = \sqrt{\psi(p)\psi(q)}$. Then for the elements of this set one has $\frac{\sqrt{pq}}{ord_{pq}(2)} \leq \frac{gcd(p-1,q-1)}{\psi(p)\psi(q)} \leq \frac{1}{\sqrt{\psi(p)\psi(q)}} \to \infty$. We can now conclude that the theorem holds by invoking Theorem 1.

References

[1] F. Pappalardi, *On the Order of Finitely Generated Subgroups of $\mathbb{Q}^\times (mod\ p)$ and Divisors of $p-1$,* Journal of Number Theory 57, 207-222 (1996).

[2] P. Kurlbeg, *On the order of unimodular matrices modulo integers*, arXiv:math/0202053 (2002).