Project

Jingyang Chen

1 Ducci Sequences

(Ehrlich) Let $A = (a_1, a_2, ...a_n)$ be an n-tuple of non-negative integers, and define

$$D(A) = (|a_1 - a_2|, |a_2 - a_3|, ..., |a_n - a_1|)$$

Then sequences of the form $A, D(A), D^2(A), ...$ are called Ducci sequences. Some basic properties of Ducci sequences include

a) Ducci sequences eventually become periodic.

b) Ducci sequences vanish if $n = 2^k$ for some $k \in \mathbb{N}$.

Does vanish = (0, 0, .. , 0) ?

c) The period of any Ducci sequence divides the period of the basic Ducci sequence, denoted $P(n)$, which starts with the n-tuple $(0, 0, ..., 1)$.

Is a period the number of tuples between the same? Examples?

2 Ducci sequences in $\mathbb{F}_2$

Within the periodic part of a Ducci sequence, each component is equal to either 0 or a constant C and since for every positive $\lambda, D(\lambda A) = \lambda D(A)$. Without loss of generality, we can assume $C = 1$ and then work in $\mathbb{Z}_2^n$.
Let $H((a_1, a_2, ..., a_n) = (a_2, ..., a_n, a_1)$, then H is a linear transformation over $\mathbb{Z}_2^n$ (note that $D^n = I$).Since $|x - y| \equiv x + y \pmod 2$, then $D = I + H$ where I is the identity and D is also a linear transform over $\mathbb{Z}_n^2$. This is then used to prove many of the ideas in Ehrlich's paper.

2.1 List of theorems, lemmas and corollaries in Ehrlich's paper

1. If $2^m \equiv t \pmod n$ then $D^{(2^m)} = I + H^t$
2. If n is a power of 2, then the cycle of the Ducci sequence consists of a zero n-tuple $(0, 0, ..., 0)$. If not, then the cycle contains an n-tuple with exactly two 1's.
3. If $2^m \equiv 1 \pmod n$ then $P(n)|2^m - 1$
4. If $2^M \equiv -1 \pmod n$ then $P(n)|n(2^M - 1)$
5. If n is not a power of 2 then $n|P(n)$
6. If $n = 2^r l$ for some odd l then $P(n) = 2^r P(l)$
7. If $n|k$ then $P(n)|P(k)$

2.2 Calculating $P(n)$

Ehrlich uses the following abbreviation: for an odd n, let $m(n)$ be the smallest $m > 0$ such that $2^m \equiv 1 \pmod{n}$. By Euler's theorem ($a^{\phi(n)} \equiv 1 \pmod{n}$), such an m does exist and divides $\phi(n)$. Also, if there is a $2^M \equiv -1 \pmod{n}$, the smallest such M is $\frac{m(n)}{2}$ and n is 'without a -1'.
Then for every odd n such that $2^M \equiv -1 \pmod{n}$ from 3 to 163 except for 37 and 101,

$$P(n) = n(2^{\frac{m(n)}{2}} - 1)$$

For every odd n without a -1, from 7 to 165 except for 95 and 111

$$P(n) = 2^{m(n)} - 1$$

For all four of the exceptions $P(n)$ is a third of the 'expected value'.

3 Important ideas to remember

1. Euler's totient function:
$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

2. Primtive roots modulo n: If for every integer a coprime to n, there is an integer k such that $g^k \equiv a \pmod{n}$ then g is a primitive root modulo n. Note that g is a primitive root modulo n if and only if g is a generator of the multiplicative group of integers modulo n.

3. Artin's conjecture on primitive roots - for an integer a that is neither a perfect square nor -1 is a primitive root modulo infinitely many primes p.

4 Research Ideas

1. Asymptotic bounds for $P(n)$ - currently this bound
$$P(n) >> exp(\log 4 + o(1)\frac{m}{\sqrt{2n}})$$

2. The duality between n and $P(n)$ - Consider a Ducci sequence with period p in $\mathbb{F}_2^n$ then we can construct a Ducci sequence with period n in $\mathbb{F}_2^p$.

3. Applications? in coding theory/cryptogrophy/data compression. Primary challenge

4. Length of iterations until Ducci sequences become periodic, say for n-tuples where $n = 3, ..., 20$ or whatever you think is feasible. Just consider the n-tuple to have elements in $\mathbb{F}_2$ (just 0 or 1s). My idea of this implementation is that you could run it for each possible variation and record number of iterations until it is implemented with mean and variance. It has been proven that the cyclic part of the Ducci sequence contains an n-tuple that has two 1's so you can exclude that so that you only need to consider $2^n - 3$ iterations for each n (removing the 0 and all starting with two 1's).

5. Ducci sequences by the isomorphism of $\mathbb{F}_2$-vector spaces

$$\mathbb{F}_2^n \xrightarrow{\sim} \frac{\mathbb{F}_2[x]}{\langle x^n + 1 \rangle}$$
$$\vec{u} = (a_1, ..., a_n) \mapsto f_u(x) \pmod{x^n + 1}$$

where $f_u(x) = a_1 x^{n-1} + a_2 x^{n-2} + ... + a^n$. This sum is the discrete fourier transform of $j \mapsto u_{n-j}$ which leads to the potential areas listed below.

6. Discrete Fourier Transforms relation - Number theoritic transform in case of finite fields - values of $P(\zeta)$
   Link between Ducci sequences and discrete Fourier Transform?
   Uncertainty principle (if we have a function supported on narrow interval, then its transform is spread e.g. position and momentum)

7. Exceptions to $P(n)$