Substitutions and Cycles

ALEX RUTAR

ABSTRACT. We investigate an entertaining recreational math problem which involves iterated doubling of digits. It turns out that this problem reduces to counting finite prefixes of a substitution on a finite alphabet.

1. INTRODUCTION: A NUMBER MULTIPLICATION GAME

I was talking to a friend recently and he made an amusing observation: he noticed an interesting relationship between his phone passcode and a friend's phone passcode[1]. His code was the 6-digit number 485394 and his friend's code was the 6-digit number 816106. He noticed that you could obtain the second code from the first by the following procedure: take each digit in the initial code, multiply it by 2, join the resulting digits together, and then remove all characters except the first 6. In this situation,

$$4\ 8\ 5\ 3\ 9\ 4 \to 8\ 16\ 10\ 6\ 18\ 8 \to 8\ 1\ 6\ 1\ 0\ 6$$

gives the second code from the first.

So then he wondered: what happens if you repeat this process? Let's do this for a number of steps.

0	485394
1	816106
2	162122
3	212424
4	424848
5	848168
6	168162
7	**212162**
8	424212
9	848424
10	168168
11	**212162**

After 11 iterations, we see the same number 212162 twice! After this stage, we will see a repeating pattern consisting of $\{212162, 424212, 848424, 168168\}$.

Try this process yourself with another 6-digit number which does not start with 0. Surprisingly, you will eventually again see exactly the 4 numbers which we saw above!

[1]Of course, the original numbers are modified!

Available online. https://rutar.org/notes/substitutions_and_cycles.pdf

Why does this happen? Can we come up with a good explanation for this phenomenon? What are the special features of this process which enable such a thing to happen?

Since there are only finitely many code words, any well-defined process taking codes to other codes will always be eventually periodic. But the above process has a special feature: it is defined by some fixed action on individual digits in the code. It turns out that this property will yield a substantial amount of structure about the process, which we can use to understand why this phenomenon occurs in general.

2. MAKING THINGS PRECISE

2.1. Substitutions. A good setting for the above system comes from the language of *substitutions*. Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ denote the natural numbers starting at zero. Fix a finite alphabet $\mathcal{A}$; for instance, $\mathcal{A}$ might be the set of digits used in a code.

Let's introduce some language in order to make it easier to discuss some concepts. For $n \in \mathbb{N}$, we let $\mathcal{A}^n$ denote the set of strings of length n on the alphabet $\mathcal{A}$. We also write $\mathcal{A}^* = \bigcup_{n=0}^{\infty} \mathcal{A}^n$ to denote the set of all finite strings. We let ε denote the unique string of length zero. Given two strings $\sigma = (a_1, \ldots, a_n)$ and $\tau = (b_1, \ldots, b_k)$, we denote the *concatenation* $\sigma\tau = (a_1, \ldots, a_n, b_1, \ldots, b_k)$. We denote the *length* of $\sigma = (a_1, \ldots, a_n)$ by $|\sigma| = n$.

Now fix a function $f \colon \mathcal{A} \to \mathcal{A}^*$. The function f extends to a unique function on $\mathcal{A}^*$ by the rule $f(\varepsilon) = \varepsilon$ and $f(a_1 \ldots a_n) = f(a_1) \cdots f(a_n)$.

Example 2.1. In our original example, our finite alphabet is $\mathcal{A} = \{0, 1, \ldots, 9\}$. Then the function $f \colon \mathcal{A} \to \mathcal{A}^*$ is as follows:

a	0	1	2	3	4	5	6	7	8	9
$f(a)$	0	2	4	6	8	10	12	14	16	18

Now suppose we are given a finite word, say 175231. We then extend the definition of f on the finite word by applying f to each individual character, and then joining the results:

$$f(175231) = f(1)f(7)f(5)f(2)f(3)f(1) = 21410462.$$

Note that, at this stage, we *do not* truncate the process: we let the length of the word increase when we apply the map f.

Observe that if σ and τ are any finite words, then $f(\sigma\tau) = f(\sigma)f(\tau)$. In fancier terminology, f is a *semigroup homomorphism*: the set $\mathcal{A}^*$ is a semigroup equipped with the operation of concatenation, and the function $f \colon \mathcal{A}^* \to \mathcal{A}^*$ respects concatenation. In this specific situation, one often calls the function f a *substitution*.[2]

It could happen that $f(a) = \varepsilon$ for some a. However, in this situation, we can effectively ignore all the characters a where $f(a) = \varepsilon$ without any loss. Therefore

[2]Alternatively, we could have started with a substitution $g \colon \mathcal{A}^* \to \mathcal{A}^*$. Then the function g must satisfy $g(\varepsilon) = \varepsilon$ (since for any $\sigma \in \mathcal{A}^*$, $g(\sigma) = g(\varepsilon)g(\sigma)$ which is only satisfied if $g(\varepsilon) = \varepsilon$), and if $\sigma = (a_1, \ldots, a_n)$ is arbitrary, $g(\sigma) = g(a_1) \cdots g(a_n)$ is uniquely determined by its values on $\mathcal{A}$.

the substitution f is equivalent to the substitution restricted to the subfamily

$$\{a \in \mathcal{A} : f(a) \neq \varepsilon\}.$$

For the rest of this document, we will assume that $|f(a)| \geq 1$ for all $a \in \mathcal{A}$.

2.2. Truncated substitutions. We recall that we began with a procedure which is defined on some finite set of characters $\mathcal{A}$, and then extended it to a procedure which takes finite words. In the terminology of the previous section, this is the same as fixing a substitution $f\colon \mathcal{A}^* \to \mathcal{A}^*$. However, we recall that we do not just want the full action of the process f: in the passcode example, we only cared about the first 6 digits (and discarded the rest). Let's formalize this process.

First, we need some more notation again. Given a finite word $\sigma \in \mathcal{A}^*$, a *prefix* is a word formed by taking some initial segment of characters. For instance, 1532 is a prefix of 153204. Given $n \in \mathbb{N}$ and a word $\sigma \in \mathcal{A}^*$ with $|\sigma| \geq n$, we write $[\sigma]_n \in \mathcal{A}^n$ to denote the (unique) prefix of σ of length n. Since we assumed that $|f(a)| \geq 1$ for all $a \in \mathcal{A}$, we must have $|f(\sigma)| \geq |\sigma|$, so f induces a function $f_m\colon \mathcal{A}^m \to \mathcal{A}^m$ by the rule

$$f_m(\sigma) = [f(\sigma)]_m.$$

We also let f_m^n denote the n-fold composition of f_m with itself.

Example 2.2. Continuing the original example, with the function f defined in Example 2.1, the actual process we are interested in is the function $f_6\colon \mathcal{A}^6 \to \mathcal{A}^6$.

Our goal in this document is to (in some form) answer the following question.

Question 2.3. *What can one say about the asymptotic behaviour of the orbits $(f_m^n(\sigma))_{n=1}^\infty$ for some word $\sigma \in \mathcal{A}^m$?*

First, since $\mathcal{A}^m$ is a finite set and $(f_m^n(\sigma))_{n=1}^\infty$ is an infinite sequence, there must be some n_1 and n_2 so that $f_m^{n_1}(\sigma) = f_m^{n_2}(\sigma)$. But then for any $n \in \mathbb{N}$, this again implies that $f_m^{n_1+n}(\sigma) = f_m^{n_2+n}(\sigma)$. In other words, $(f_m^n(\sigma))_{n=1}^\infty$ must be *eventually periodic*: there is some $k, \theta \in \mathbb{N}$ and a finite set of words $\tau_1, \ldots, \tau_\theta$ so that

$$f_m^{k+\ell\theta+i}(\sigma) = \tau_i$$

for all $\ell \in \mathbb{N}$ and $0 \leq i \leq \theta - 1$. If θ is chosen to have minimal length, we call θ the *period* and the corresponding words $(\tau_1, \ldots, \tau_\theta)$ the *cycle*. We say that two cycles are *equivalent* if the cycles are cyclic permutations of the other.

So we now know that for each word $\sigma \in \mathcal{A}^*$, there is a unique period θ and unique (up to equivalence) cycle $(\tau_1, \ldots, \tau_\theta)$. Moreover, suppose some $f_m^n(\sigma) = \tau_i$ for some n: then the cycle of σ must be determined by $(\tau_1, \ldots, \tau_\theta)$. In other words, for each $m \in \mathbb{N}$ and $\sigma \in \mathcal{A}^m$, the cycle of σ is uniquely determined by any member of the set $\mathcal{C}_m(\sigma) \coloneqq \{\tau_1, \ldots, \tau_\theta\}$. For distinct words σ_1 and σ_2, either $\mathcal{C}_m(\sigma_1) = \mathcal{C}_m(\sigma_2)$ or $\mathcal{C}_m(\sigma_1) \cap \mathcal{C}_m(\sigma_2) = \emptyset$.

2.3. Characterizing cycles. We now return to our original substitution f. It will turn out that there are essentially two meaningful cases to understand the long-term behaviour of $f_m^n(\sigma)$: either the initial letter of σ eventually grows to be arbitrarily long (and it completely determines the first m letters of $f^n(\sigma)$), or it does not, and it must have some other nice properties. Moreover, we will see that we can reduce the analysis to the case when the first character of σ is fixed by some power of f. Let's do this analysis now.

We say that a symbol $a \in \mathcal{A}$ is *prefix invariant* if there is some $k \in \mathbb{N}$ so that a is a prefix of $f^k(a)$. Note that, by induction, for any $j \in \mathbb{N}$, $f^{jk}(a)$ is a prefix of $f^{(j+1)k}(a)$. We also say that $a \in \mathcal{A}$ is *bounded* if $(|f^n(a)|)_{n=1}^{\infty}$ is a bounded sequence, and *unbounded* otherwise.

Suppose $a_0 \in \mathcal{A}$ is prefix invariant and bounded, and get k so that a_0 is a prefix of $f^k(a_0)$. But if $|f^k(a_0)| \geq 2$, then for any $j \in \mathbb{N}$, we would have $|f^{jk}(a_0)| \geq j+1$, which contradicts boundedness: so in fact $f^k(a_0) = a_0$.

Otherwise, suppose $a_0 \in \mathcal{A}$ is prefix invariant and unbounded. Equivalently, there is a $k \in \mathbb{N}$ so that a_0 is a prefix of $f^k(a_0)$ and moreover $|f^k(a_0)| \geq 2$. Then for any $m \in \mathbb{N}$ and $\sigma \in \mathcal{A}^m$, if a_0 is a prefix of σ, since $|f^{mk}(a_0)| \geq m$, for any $j \in \mathbb{N}$

$$f_m^{mk}(\sigma) = [f^{mk}(a_0)]_m = [f^{(m+j)k}(a_0)]_m$$

In other words, the cycle of $(f_m^n(\sigma))$ is uniquely determined by the first m characters of $f^{mk}(a_0)$.

Finally, what happens if $a_0 \in \mathcal{A}$ is *not* prefix invariant? Since the sequence $(f_1^n(a_0))_{n=1}^{\infty}$ is again eventually periodic, there is some $k \in \mathbb{N}$ so that the first character b of $f^k(a_0)$ is prefix invariant. But then if a_0 is not the first character of $f^j(b)$ for some $j \in \mathbb{N}$, a_0 will never appear again as the first character.

Example 2.4. Again, let's continue with the substitution f defined in Example 2.1. What are the possible cases? Firstly, since $f(0) = 0$, 0 is prefix invariant and bounded since under iteration, the length does not increase. There are also words which are prefix invariant and unbounded: $f(1) = 2$, $f(2) = 4$, $f(4) = 8$, and $f(8) = 16$. Since $|f^4(1)| = 16$ has length 2, the characters $\{1, 2, 4, 8\}$ are all prefix invariant and unbounded.

What about the remaining characters? Well, $f^2(3) = 12$, $f(5) = 10$, $f(6) = 12$, $f(7) = 14$, and $f(9) = 18$, all of which begin with the digit 1 which is prefix invariant, and none of the characters are images of 1 under iteration. Thus the characters $\{3, 5, 6, 7, 9\}$ are not prefix invariant.

2.4. Putting everything together. Now, fix an $m \in \mathbb{N}$ and an arbitrary word $\sigma \in \mathcal{A}^m$. Let a_0 be the first character of σ. If a_0 is not prefix invariant, we observed that there is some k so that the first character of $f^k(a_0)$ is prefix invariant. Thus by considering the word $f_m^k(\sigma)$, we may assume that a_0 is prefix invariant.

If a_0 is bounded, then there is some $k \in \mathbb{N}$ so that $f^k(a_0) = a_0$. Otherwise, a_0 is prefix invariant and unbounded, and $f_m^n(\sigma)$ is fully determined by $f^n(a_0)$ In other words, we can write $\sigma = \omega\eta$ where all the characters in ω are prefix invariant and bounded, and the first character of η is prefix invariant and unbounded. Moreover, any cycle is uniquely determined by some choice of ω and the first character of

η. This gives a complete description of all possible cycles which can appear in $(f_m^n(\sigma))_{n=1}^{\infty}$.

Example 2.5. Let's complete the analysis started in Example 2.1 in the case $m = 6$. Suppose we begin with a 6-digit code. If the code begins with some collection of 0s, then the 0s will remain there forever: this is precisely the contribution from the bounded prefix invariant characters. Then let's take the first non-zero digit a_0 But there is only one group of unbounded prefix invariant characters: $\{1, 2, 4, 8\}$. If the first non-zero digit does not lie in this group, after at most 5 steps, the first digit will be a 1. But the digit 1 is fixed under f^4, so by repeatedly iterating this power of f, the image of 1 will eventually offset all other characters in σ.

Visually, here is a depiction. Let's suppose we have a word $\sigma = 3*****$, where the $*$ are placeholders for any characters which do not matter in the long run.

0	$3*****$
1	$6*****$
2	$1*****$
6	$16****$
10	$16816*$
11	212162

Since 3 is not prefix invariant, after 2 steps, we arrive at 1 which is prefix invariant. Then we iterate enough times until the image of 1 is sufficiently long that none of the other characters matter. At this point, we have arrived at 212162, which is precisely the same word which we saw appear in the first section, and is one of the four words in the repeating cycle (of length four).

2.5. Another example: iterated squares. Let's illustrate the concepts in the previous sections using the following example. Let $\mathcal{A} = \{0, 1, \ldots, 9\}$, and define $f : \mathcal{A} \to \mathcal{A}^*$ so that $f(a)$ is the base-10 encoding of a^2. This map is summarized as follows:

a	0	1	2	3	4	5	6	7	8	9
$f(a)$	0	1	4	9	16	25	36	49	64	81

Let's separate the characters in $\mathcal{A}$ into the three cases discussed in §§2.3.

- *Prefix invariant and bounded:* The characters 0 and 1 are prefix invariant and bounded, since they are fixed points under f.
- *Prefix invariant and unbounded:* The characters 3, 6, 8, and 9 are all prefix invariant and unbounded in the same cycle since $(f_1^n(3))_{n=1}^{\infty}$ is periodic with cycle $(3, 9, 8, 6)$.
- *Not prefix invariant:* The characters 2, 4, 5, and 7 are not prefix invariant since $f^2(2) = 16$, $f(4) = 16$, $f^3(5) = 16425$, and $f^2(7) = 1681$ and 1 is prefix invariant.

Therefore, for any $m \in \mathbb{N}$, all the possible cycles of length m are characterized by words of the form $\omega\eta$ where $\omega \in \{0, 1\}^k$ and η is the length $m - k$ prefix of $f^{4(m-k)}(3)$, for $k = 0, \ldots, m$. Here, the 4 occurs since the prefix invariant and unbounded characters form a cycle of length 4.

For fun, here are some of the initial values of $f^k(3)$ for some $k \in \mathbb{N}$:

0	3
1	9
2	81
3	641
4	**3616**1
5	**9361**361
6	**8193**619361
7	**6418**19361819361
8	3616164181936164181936
12	361616418193616418193616418193618193618193 6...

For instance, if $\sigma = 10\mathit{6345}$, our word will be eventually periodic with period 4 given by the cycle $\{10\mathbf{3616}, 10\mathbf{9361}, 10\mathbf{8193}, 10\mathbf{6418}\}$.

2.6. A final example illustrating varied behaviour. To conclude, we show that some more complex behaviour is possible. Consider the substitution defined by

a	0	1	2	3	4	5	6	7	8	9
$f(a)$	1	2	0	45	5	3	7	69	7	13

Again, let's separate the characters in $\mathcal{A}$ into the three cases.

- *Prefix invariant and bounded:* The characters 0, 1, and 2 are prefix invariant and bounded. They form a cycle of length 3.
- *Prefix invariant and unbounded:* The characters $\{3, 4, 5\}$ form a prefix invariant and unbounded cycle of length 3, and the characters $\{6, 7\}$ form a prefix invariant and unbounded cycle of length 2.
- *Not prefix invariant:* The characters 8 and 9 are not prefix invariant since the first characters of $f(8)$ and $f(9)$ are prefix invariant.

Now, there are multiple cases for the cycle: this happens since the bounded characters form periods of length 3, and there are unbounded characters form either a period of length 3 or a period of length 2. Again, for $m \in \mathbb{N}$, the possible cycles of length m are characterized by words of the form $\omega\eta$ where $\omega \in \{0, 1, 2\}^k$ and η is the length $m - k$ prefix of either $f^{3(m-k)}(3)$ or $f^{2(m-k)}(6)$.

For example, if $\sigma = 1\mathit{820}$, then our word will be eventually periodic with period $6 = \operatorname{lcm}(3, 2)$ given by

$$(1713, 2692, 0713, 1692, 2713, 0692).$$

Alex Rutar
University of St Andrews, Mathematical Institute, St Andrews KY16 9SS
Email: alex@rutar.org