Corrected proof of Theorem 2.7 in Allouche and Shallit (1992)

Jeffrey Shallit

February 23, 2020

We present two different corrected proofs of Theorem 2.7, from Allouche and Shallit (1992) on the merge of k-regular sequences.

1 Proof number 1

This proof uses the interpretation of k-regular sequences in terms of the k-kernel, and is an "arithmetic" proof.

Theorem 1. *Suppose $k \geq 2, a \geq 1$ are integers, and suppose $(f(n))_{n\geq 0}$ is a sequence such that each subsequence $(f(an+i))_{n\geq 0}$ is k-regular for $0 \leq i < a$. Then $(f(n))_{n\geq 0}$ itself is k-regular.*

Proof. The idea behind the proof is as follows: we define $f_i(n) = f(an+i)$ for $0 \leq i < a$. By hypothesis each $(f_i(n))_{n\geq 0}$ is k-regular. We also define the sequences $(g_i(n))_{n\geq 0}$ by

$$g_i(am+j) = \begin{cases} f_i(m), & \text{if } i \equiv j \pmod{a}; \\ 0, & \text{otherwise}; \end{cases}$$

for $0 \leq i, j < a$. Thus each $(g_i(n))_{n\geq 0}$ is just $(f_i(n))_{n\geq 0}$ that has been modified by shifting and insertion of $a-1$ 0's between terms. Then $f(n) = \sum_{0\leq i<a} g_i(n)$, so it suffices to show that each $(g_i(n))_{n\geq 0}$ is k-regular.

To do this, we show that the k-kernel of $(g_i(n))_{n\geq 0}$ is a subset of a finitely-generated module. Let $(g_i(k^e n + c))_{n\geq 0}$ be an arbitrary element of the k-kernel of $(g_i(n))_{n\geq 0}$. To evaluate it, we need to know when $k^e n + c = am + i$. By a standard theorem about two-variable Diophantine equations, we know this equation has solutions iff $\gcd(k^e, a) \mid i - c$. If this condition holds, then all solutions are parameterized by

$$n = N_e \ell + n_0$$
$$m = M_e \ell + m_0$$

for $\ell \geq 0$, where

$$N_e := \frac{a}{\gcd(k^e, a)}, \quad M_e := \frac{k^e}{\gcd(k^e, a)}$$

and $0 \leq n_0 < N_e$, $0 \leq m_0 < M_e$.

It follows that $(g_i(k^e n + c))_{n\geq 0}$ is either the 0 sequence (if $\gcd(k^e, a) \not| i - c$) or a shift (by at most $N_e - 1 < a$) of the sequence $(f_i(M_e \ell + m_0))_{\ell \geq 0}$ interspersed with $N_e - 1$ 0's.

We now claim that the k-kernel of $(g_i(n))_{n\geq 0}$ is finitely generated. It suffices to show that the k-kernel of $(f_i(M_e \ell + m_0))_{\ell\geq 0}$ is finitely generated. The key remark is that there are only finitely many different values of $\gcd(k^e, a)$, so M_e can always be written in the form $k^{e-t}s$, where t and s are bounded. Write $sq + d = m_0$ for $0 \leq q < m_0/s$ and $0 \leq d < s$. Thus $(f_i(M_e \ell + m_0))_{\ell\geq 0}$ is an element of the k-kernel of $(f_i(sn + d))_{n\geq 0}$, namely, the one given by taking the subsequence corresponding to $n = k^{e-t}\ell + q$. Since, by Theorem 2.6, each subsequence $(f_i(sn + d))_{n\geq 0}$ is k-regular, their k-kernels are finitely generated. The result now follows. □

2 Proof number 2

This proof is based on the linear representation of k-regular sequences.

Lemma 2. *Let $(f(n))_{n\geq 0}$ be a k-regular sequence, and let $\Sigma_k = \{0, 1, \ldots, k - 1\}$. Let $T = (Q, \Sigma_k, \Sigma_k, \delta, q_0, \rho)$ be a deterministic finite-state transducer with transitions on single letters only, but allowing arbitrary words as outputs on each transition. More precisely,*

- *$Q = \{q_0, \ldots, q_{r-1}\}$;*
- *$\delta : Q \times \Sigma_k \to Q$ is the transition function; and*
- *$\rho : Q \times \Sigma_k \to \Sigma_k^*$ is the output function.*

Let the domain of δ and ρ be extended to Σ_k^* in the obvious way. Define $g(n) = f(T((n)_k)))$. Then $(g(n))_{n\geq 0}$ is also a k-regular sequence.

Proof. Let (v, μ, w) be a rank-s linear representation for f. We create a linear representation (v', μ', w') for g.

The idea is that $\mu'(a)$, $0 \leq a < k$, is an $n \times n$ matrix, where $n = rs$. It is easiest to think of $\mu'(a)$ as an $r \times r$ matrix, where each entry is itself an $s \times s$ matrix. In this interpretation, $(\mu'(a))_{i,j} = \mu(\rho(q_i, a))$ if $\delta(q_i, a) = q_j$.

An easy induction now shows that if $\delta(q_i, x) = q_j$ and $\rho(q_i, x) = y$, then $(\mu'(x))_{i,j} = \mu(y)$. If we now let v' be the vector $[v \quad v \quad \cdots \quad v]$ and w' be the vector $[w \quad w \quad \cdots \quad w]$, then it follows that $v'\mu'(x)w' = v\mu(T(x))w$. This gives a linear representation for $(g(n))_{n\geq 0}$. □

Now we can prove the desired result.

Proof. First, we build build a finite-state transducer T that outputs the base-k representation of $\lfloor n/a \rfloor$ on input $(n)_k$. The idea is just to use long division, keeping track of the carries (which can be at most a) in the state. A slight complication is to avoid outputting leading zeroes, but this is easily handled (see example for $a = 3$, $k = 2$).

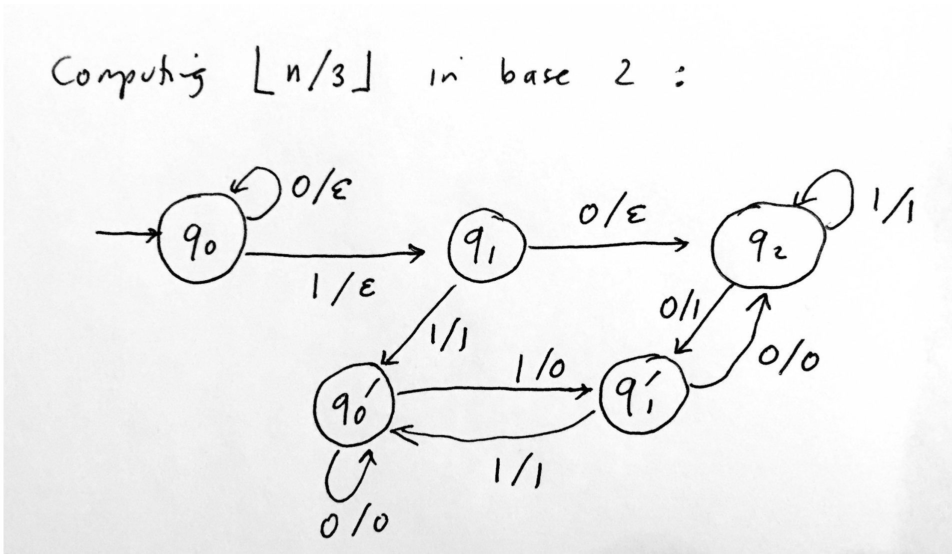

Figure 1: Transducer dividing by 3

Next, we use the lemma above to see that $(f(T((n)_k)))_{n\geq 0}$ is k-regular. Thus we have shown that $(f(\lfloor n/a \rfloor))_{n\geq 0}$ is k-regular.

Now consider the periodic sequences $(p_i(n))_{n\geq 0}$ defined by $p_i(n) = 1$ if $n \equiv i \pmod a$ and 0 otherwise. Each such sequence is k-automatic and hence k-regular. Let $f_i(n)$ be k-regular sequences for $0 \leq i < a$. By above each sequence $(f_i(\lfloor n/a \rfloor))_{n\geq 0}$ is k-regular. Hence $f(n)$, the a-way merge of the sequence $f_i(n)$, is given by

$$f(n) := \sum_{0\leq i<a} p_i(n) f_i(\lfloor n/a \rfloor),$$

and is k-regular by the closure properties of these sequences. □