CDMTCS Research Report Series

Kraft-Chaitin Inequality Revisited

C. Calude and C. Grozea
University of Auckland, New Zealand
Bucharest University, Romania

CDMTCS-013
April 1996

Centre for Discrete Mathematics and
Theoretical Computer Science

KRAFT-CHAITIN INEQUALITY REVISITED*

Cristian Calude†‡ **Cristian Grozea**§

Abstract

Kraft's inequality [9] is essential for the classical theory of noiseless coding [1, 8]. In algorithmic information theory [5, 7, 2] one needs an extension of Kraft's condition from finite sets to (infinite) recursively enumerable sets. This extension, known as Kraft-Chaitin Theorem, was obtained by Chaitin in his seminal paper [4] (see also, [3, 2], [10]). The aim of this note is to offer a simpler proof of Kraft-Chaitin Theorem based on a new construction of the prefix-free code.

Keywords: Kraft inequality, Kraft-Chaitin inequality, prefix-free codes.

1 Prerequisites

Denote by $\mathbf{N} = \{0, 1, 2, \ldots\}$ the set of non-negative integers. If X is a finite set, then $\#X$ denotes the cardinality of X.

Fix $A = \{a_1, \ldots, a_Q\}, Q \geq 2$, a finite alphabet. By A^* we denote the set of all strings $x_1 x_2 \ldots x_n$ with elements $x_i \in A$ $(1 \leq i \leq n)$; the empty string is denoted by λ. For x in A^*, $|x|$ is the length of x $(|\lambda| = 0)$. For $p \in \mathbf{N}$, $A^p = \{x \in A^* \mid |x| = p\}$ is the set of all strings of length p. Fix a total ordering on A, say $a_1 < a_2 < \cdots < a_Q$, and consider the induced lexicographical order on each set A^p, $p \in \mathbf{N}$. A string x is a prefix of a string y (we write $x \subset y$) in case $y = xz$, for some string z. A set $S \subset A^*$ is *prefix-free* if there are no distinct strings x, y in S such that $x \subset y$. We shall use [2] for the basics on partial recursive (p.r.) functions.

2 Main Proof

This section is devoted to a new and simpler proof of the Kraft-Chaitin Theorem.

Theorem. (Kraft-Chaitin) *Let* $\varphi : \mathbf{N} \stackrel{o}{\to} \mathbf{N}$ *a p.r. function having the domain,* $dom(\varphi)$*, to be* $\mathbf{N}$ *or a finite set* $\{0, 1, \ldots, N\}$*, with* $N \geq 0$*. Assume that*

$$\sum_{i \in dom(\varphi)} Q^{-\varphi(i)} \leq 1. \tag{1}$$

There exists (and can be effectively constructed) an injective p.r. function

$$\Phi : dom(\varphi) \to A^*$$

---

*C. Calude (ed.). *The Finite, the Unbounded and the Infinite, Proceedings of the Summer School "Chaitin Complexity and Applications"*, Mangalia, Romania, 27 June – 6 July, 1995.

†Computer Science Department, The University of Auckland, Private Bag 92019, Auckland, New Zealand; email: cristian@cs.auckland.ac.nz.

‡The work of the first author has been partially supported by Auckland University Research Grant A18/XXXXX/62090/3414050.

§Faculty of Mathematics, Bucharest University, Str. Academiei 14, R-70109 Bucharest, Romania; chrisg@math.math.unibuc.ro.

such that for every $i \in dom(\varphi)$,

$$| \Phi(i) |= \varphi(i),$$

and

$$\{\Phi(i) \mid i \in dom(\varphi)\}$$

is a prefix-free set.

Proof. We will construct three sequences $(M_n)_{n\in dom(\varphi)}$ (of finite subsets of A^*), $(m_n)_{n\in dom(\varphi)}$ (of non-negative integers), $(\mu_n)_{n\in dom(\varphi)}$ (of strings over A) as follows:

$$m_n = \max\{| x | \mid x \in M_n, | x |\leq \varphi(n)\},$$

$$\mu_n = \min(M_n \cap A^{m_n}),$$

where min is taken according to the lexicographical order.

The sets M_n are constructed as follows: $M_0 = \{\lambda\}$, and if $M_1, \ldots, M_n$ have been constructed and $\varphi(n+1) \neq \infty$, then:

$$M_{n+1} = (M_n \setminus \{\mu_n\}) \cup T_{n+1},$$

where

$$T_{n+1} = \{\mu_n a_1^j a_p \mid 0 \leq j \leq \varphi(n) - m_n - 1, 2 \leq p \leq Q\}.$$

Finally put

$$\Phi(n) = \mu_n a_1^{\varphi(n)-m_n}.$$

The proof consists in checking, by induction on $n \geq 0$, the following five conditions:

A) $\sum_{x\in M_n} Q^{-|x|} = 1 - \sum_{i=0}^{n-1} Q^{-\varphi(i)}$.

B) For all $p \geq 0, \#(A^p \cap M_n) \leq Q - 1$.

C) The string μ_n does exist.

D) The sets M_n and $\{\Phi(0), \Phi(1), \ldots, \Phi(n-1)\}$ are disjoint.

E) The set $M_n \cup \{\Phi(0), \Phi(1), \ldots, \Phi(n-1)\}$ is prefix-free.

The induction basis is very simple: $M_0 = \{\lambda\}$, so $m_0 = 0, \Phi(0) = a_1^{\varphi(0)}$. Consequently, $\sum_{x\in M_0} Q^{-|x|} = 1 - \sum_{i=0}^{-1} Q^{-\varphi(i)}$. For all $p \geq 1, \#(A^p \cap M_n) = 0 \leq Q - 1$. Finally, $\mu_0 = \lambda$ and the last two conditions are vacuously true.

Assume now that conditions A)-E) are true for some fixed $n \geq 0$ and prove that they remain true for $n + 1$.

We start by proving the formula

$$(M_n \setminus \{\mu_n\}) \cap T_{n+1} = \emptyset. \tag{2}$$

In fact, $M_n \cap T_{n+1} = \emptyset$. Otherwise, $\emptyset \neq M_n \cap T_{n+1} \subset M_n$ and M_n is prefix-free. So, for some $0 \leq j \leq \varphi(n) - m_n - 1$ and $2 \leq p \leq Q$, $\mu_n a_1^j a_p \in M_n \cap T_{n+1} \subset M_n$. As $\mu_n \in M_n$, it follows that M_n is no longer prefix-free, a contradiction.

We continue by checking the validity of conditions A)-E). For A), using (2), the induction hypothesis and the construction of M_{n+1}, we have:

$$\begin{aligned}
\sum_{x\in M_{n+1}} Q^{-|x|} &= \sum_{x\in(M_n\setminus\{\mu_n\}) \cup T_{n+1}} Q^{-|x|} \\
&= \sum_{x\in M_n\setminus\{\mu_n\}} Q^{-|x|} + \sum_{x\in T_{n+1}} Q^{-|x|} \\
&= \sum_{x\in M_n} Q^{-|x|} - Q^{-m_n} + (Q-1) \sum_{0\leq j\leq\varphi(n)-m_n-1} Q^{-(m_n+j+1)} \\
&= 1 - \sum_{i=0}^{n-1} Q^{-\varphi(i)} - Q^{-m_n} + (Q-1)Q^{-m_n-1} \sum_{j=0}^{\varphi(n)-m_n-1} Q^{-j} \\
&= 1 - \sum_{i=0}^{n} Q^{-\varphi(i)},
\end{aligned}$$

provided $m_n \leq \varphi(n) - 1$, and

$$\begin{aligned}
\sum_{x \in M_{n+1}} Q^{-|x|} &= \sum_{x \in M_n \cup T_{n+1}} Q^{-|x|} \\
&= \sum_{x \in M_n \setminus \{\mu_n\}} Q^{-|x|} + \sum_{x \in T_{n+1}} Q^{-|x|} \\
&= 1 - \sum_{i=0}^{n-1} Q^{-\varphi(i)} - Q^{-m_n} \\
&= 1 - \sum_{i=0}^{n} Q^{-\varphi(i)},
\end{aligned}$$

in case $m_n = \varphi(n)$ (and, consequently, $T_{n+1} = \emptyset$).

For B) we note that in case $k < m_n$ or $k > \varphi(n)$ we have

$$M_{n+1} \cap A^k = M_n \cap A^k.$$

For $k = m_n$,

$$\#(M_{n+1} \cap A^k) = \#(M_n \cap A^k) - 1,$$

so in all these situations B) is true by virtue of the inductive hypothesis.

In case

$$m_n + 1 \leq k \leq \varphi(n), \tag{3}$$

we have

$$M_{n+1} \cap A^k = T_{n+1} \cap A^k. \tag{4}$$

Indeed, if $x \in A^k$ and k satisfies (3), then $x \notin M_n$. For such a k,

$$\begin{aligned}
M_{n+1} \cap A^k &= ((M_n \setminus \{\mu_n\}) \cup T_{n+1}) \cap A^k \\
&= ((M_n \setminus \{\mu_n\}) \cap A^k) \cup (T_{n+1} \cap A^k) \\
&= (M_n \cap A^k) \cup (T_{n+1} \cap A^k) \\
&= T_{n+1} \cap A^k.
\end{aligned}$$

In view of (4),

$$\#(M_{n+1} \cap A^k) = \#(T_{n+1} \cap A^k) = Q - 1.$$

For C), μ_{n+1} does exist if in M_{n+1} we can find at least one string of length less or equal than $\varphi(n+1)$. To prove this we assume, for the sake of a contradiction, that every string in M_n has length greater than $\varphi(n+1)$. We have:

$$\begin{aligned}
\sum_{x \in M_{n+1}} Q^{-|x|} &= \sum_{p=0}^{\infty} \sum_{x \in M_{n+1} \cap A^p} Q^{-|x|} \\
&= \sum_{p=\varphi(n+1)+1}^{\infty} \sum_{x \in M_{n+1} \cap A^p} Q^{-|x|} \\
&< \sum_{p=\varphi(n+1)+1}^{\infty} Q^{-p}(Q-1) \\
&= Q^{-\varphi(n+1)},
\end{aligned}$$

as $M_{n+1} \cap A^p = \emptyset$, for almost all $p \in \mathbf{N}$, and by B), $\#(M_{n+1} \cap A^p) \leq Q - 1$. From A) we get

$$1 - \sum_{i=0}^{n} Q^{-\varphi(i)} = \sum_{x \in M_{n+1}} Q^{-|x|} < Q^{-\varphi(n+1)},$$

which contradicts the hypothesis (1), thus concluding the existence of μ_{n+1}.

In proving D) we write $M_{n+1} \cap \{\Phi(0), \Phi(1), \ldots, \Phi(n)\}$ as a union of four sets:

$$(M_n \setminus \{\mu_n\}) \cap \{\Phi(0), \Phi(1), \ldots, \Phi(n-1)\}$$
$$T_{n+1} \cap \{\Phi(0), \Phi(1), \ldots, \Phi(n-1)\}$$
$$(M_n \setminus \{\mu_n\}) \cap \{\Phi(n)\}$$
$$T_{n+1} \cap \{\Phi(n)\}$$

each of which will be shown to be empty. Indeed, the first set is empty by virtue of the induction hypothesis. For the second set we notice that in case $\Phi(i) \in T_{n+1}$ (for some $0 \leq i \leq n-1$), then $\Phi(i) = \mu_n a_1^j a_p$, for some $0 \leq j \leq \varphi(n) - m_n - 1$ and $2 \leq p \leq Q$. So, $\mu_n \subset \Phi(i)$, and, as $\mu_n \in M_n \subset M_n \cup \{\Phi(0), \Phi(1) \ldots \Phi(n-1)\}$ – which is prefix-free by induction hypothesis – we arrive to a contradiction. Further on we have $\Phi(n) \notin M_n \setminus \{\mu_n\}$ as $\mu_n \subset \Phi(n)$, $\mu_n \in M_n$ and M_n is prefix-free. Finally, $\Phi(n) \notin T_{n+1}$ by virtue of the construction of $\Phi(n)$ and T_{n+1}.

For E) we write

$$M_{n+1} \cup \{\Phi(0), \Phi(1), \ldots, \Phi(n)\} = (M_n \setminus \{\mu_n\}) \cup \{\Phi(0), \Phi(1), \ldots, \Phi(n-1)\} \cup T_{n+1} \cup \{\Phi(n)\}.$$

The set $M_n \cup \{\Phi(0), \Phi(1), \ldots, \Phi(n-1)\}$ is prefix-free by induction hypothesis; $T_{n+1} \cup \{\Phi(n)\}$ is prefix-free by construction. To finish, four cases should be analyzed:

- The set $(M_n \setminus \{\mu_n\}) \cup \{\Phi(n)\}$ is prefix-free as $\mu_n \subset \Phi(n)$ and M_n is prefix-free.
- The set $(M_n \setminus \{\mu_n\}) \cup T(n+1)$ is prefix-free as $\mu_n \subset x$, for each string $x \in T(n+1)$ and M_n is prefix-free.
- To prove that the set $T_{n+1} \cup \{\Phi(0), \Phi(1), \ldots, \Phi(n-1)\}$ is prefix-free we have to consider two cases:
  - ∘ if $x \subset \Phi(i)$, for some $x \in T(n+1)$ and $0 \leq i \leq n-1$, then $\mu_n \subset x, \mu_n \in M_n \subset M_n \cup \{\Phi(0), \Phi(1), \ldots, \Phi(n-1)\}$, a prefix-free set (by induction hypothesis), which is impossible;
  - ∘ if $\Phi(i) \subset x$, for some $x \in T(n+1)$ and $0 \leq i \leq n-1$, then $\Phi(i) = \mu_n a_1^t$, for some $t > 0$ (the case $t = 0$ implies $\Phi(i) \subset \mu_n$ which is impossible). This implies that $\mu_n \subset \Phi(i)$, which is also impossible.
- To show that the set $\{\Phi(0), \Phi(1), \ldots, \Phi(n-1), \Phi(n)\}$ is prefix-free we have to consider again two cases:
  - ∘ if $\Phi(n) \subset \Phi(i)$, for some $0 \leq i \leq n-1$, then $\mu_n \subset \Phi(i)$ (as $\mu_n \subset \Phi(n)$), which is a contradiction;
  - ∘ if $\Phi(i) \subset \Phi(n)$, for some $0 \leq i \leq n-1$, then $\Phi(i) = \mu_n a_1^t$, for some $t > 0$ (the case $t = 0$ is impossible), so $\mu_n \subset \Phi(i)$, a contradiction.

The injectivity of Φ follows directly from E). Hence, the theorem has been proved.

3 Comments

A careful examination of the procedure used in the above proof shows that it produces the *same* code strings as Chaitin's original algorithm [4]:

> Start with $\Phi(0) = a_1^{\varphi(0)}$, and if $\Phi(1), \ldots, \Phi(n)$ have been constructed and $\varphi(n+1) \neq \infty$, then:
>
> $$\Phi(n+1) = \min\{x \in A^{\varphi(n+1)} \mid x \not\subset \Phi(i), \Phi(i) \not\subset x, \text{ for all } 0 \leq i \leq n\},$$
>
> where the minimum is taken according to the lexicographical order.

For an extension of Kraft-Chaitin inequality to free-extensible codes see [11].

References

[1] J. Berstel, D. Perrin. *Theory of Codes*, Academic Press, Orlando, 1985.

[2] C. Calude. *Information and Randomness — An Algorithmic Perspective*, EATCS Monographs in Theoretical Computer Science, Springer-Verlag, Berlin, 1994.

[3] C. Calude, E. Kurta. On Kraft-Chaitin inequality, *Rev. Roumaine Math. Pures Appl.* 35 (1990), 597-604.

[4] G. J. Chaitin. A theory of program size formally identical to information theory, *J. Assoc. Comput. Mach.* 22(1975), 329-340. (Reprinted in: [6], 197-223.)

[5] G. J. Chaitin. *Algorithmic Information Theory*, Cambridge University Press, Cambridge, 1987. (third printing 1990)

[6] G. J. Chaitin. *Information, Randomness and Incompleteness, Papers on Algorithmic Information Theory*, World Scientific, Singapore, 1987. (2nd ed., 1990)

[7] G. J. Chaitin. *The Limits of Mathematics*, IBM Watson Center, Yorktown Heights, July 17, 1994, 326 pp.

[8] D. S. Jones. *Elementary Information Theory*, Clarendon Press, Oxford, 1979.

[9] L. G. Kraft. *A Device for Quantizing Grouping and Coding Amplitude Modulated Pulses*, MS Thesis, Electrical Eng. Dept., MIT, Cambridge, MA, 1949.

[10] A. M. Sălăgean-Mandache. A geometrical proof of Kraft-Chaitin theorem, *An. Univ. Bucureşti Mat.-Inf.* 39/40 (1990/91), 90-97.

[11] I. Măndoiu. Kraft-Chaitin's theorem for free-extensible codes, *Stud. Cerc. Mat.* 44 (1992), 497-501.