On Sparse Languages L Such That $LL = \Sigma^*$

 $Per\ Enflo$ $Department\ of\ Mathematics\ and\ Computer\ Science$ $Kent\ State\ University$ $Kent,\ Ohio\ 44242$ USA

Andrew Granville†
Department of Mathematics
University of Georgia
Athens, GA 30602
USA
andrew@joe.math.uga.edu

Jeffrey Shallit*
Department of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
shallit@graceland.uwaterloo.ca

Sheng Yu
Department of Computer Science
University of Western Ontario
London, Ontario N6A 5B7
Canada
syu@csd.uwo.ca

Abstract.

A language $L \in \Sigma^*$ is said to be sparse if L contains a vanishingly small fraction of all possible strings of length n in Σ^* . C. Ponder asked if there exists a sparse language L such that $LL = \Sigma^*$. We answer this question in the affirmative. Several different constructions are provided, using ideas from probability theory, fractal geometry, and analytic number theory. We obtain languages that are optimally sparse, up to a constant factor. Finally, we consider the generalization $L^j = \Sigma^*$.

Keywords: sparse languages, sparse basis.

[†] An Alfred P. Sloan Research Fellow.

^{*} Supported in part by a grant from NSERC Canada.

I. Introduction.

We recall some familiar notation from formal language theory: if A is a set, then by |A| we mean the cardinality of A. If B and C are sets of strings, then by BC we mean the set $\{bc \mid b \in B, c \in C\}$. We define $A^0 = \{\epsilon\}$, where ϵ denotes the empty string, and $A^i = AA^{i-1}$ for $i \geq 1$. By $A^{\leq n}$ we mean $\bigcup_{0 \leq i \leq n} A^i$, and A^* denotes the set $\bigcup_{i \geq 0} A^i$. (The reader unfamiliar with these concepts may wish to consult a text on formal language theory such as [HU].)

Let Σ be a finite alphabet with $|\Sigma| \geq 2$. Consider the following definitions:

Definition 1.

A language $L \in \Sigma^*$ is said to be *sparse* if

$$\lim_{n \to \infty} \frac{|L \cap \Sigma^{\leq n}|}{|\Sigma^{\leq n}|} = 0.$$

Definition 2.

A language L is said to be dense if

$$\liminf_{n \to \infty} \frac{|L \cap \Sigma^{\leq n}|}{|\Sigma^{\leq n}|} = c,$$

for some c > 0.

(Note: these definitions were given by Yu [Y], except that he used the term "weakly sparse" in place of "sparse". We trust there will be no confusion with another meaning of "sparse" used in structural complexity theory, namely that the number of strings of length n is bounded by a polynomial in n.)

In response to a question of Ponder [P], Yu constructed two sparse languages, A and B, such that AB is dense; see [Y]. However, the following question was left unresolved [P]: is there a sparse language L such that $LL = \Sigma^*$?

In this note, we answer this question in the affirmative. Several different constructions are provided, using ideas from probability theory, fractal geometry, and analytic number theory. We discuss exactly how sparse such a language can be. Finally, we also discuss the equation $L^j = \Sigma^*$ for $j \geq 3$.

II. Bounds on the Sparseness of L.

Here, and in the rest of the paper, we assume that $|\Sigma| = 2$. Results similar to those given below can easily be obtained for larger alphabets.

For a language L, define

$$\lambda_n = \lambda_n(L) = \frac{|L \cap \Sigma^n|}{2^n}.$$
 (1)

Thus λ_n is the probability that a randomly chosen string of length n is in L.

Yu [Y] made the following observation:

Proposition 3.

L is sparse iff $\lim_{n\to\infty} \lambda_n = 0$.

A natural question is the following: if $LL = \Sigma^*$, how sparse can L be? We have

Theorem 4.

If $LL = \Sigma^*$, then

$$\sum_{1 \le i \le n} \lambda_i \ge \sqrt{n} - 1. \tag{2}$$

Proof.

$$2^{i} = |LL \cap \Sigma^{i}| \leq \sum_{k=1}^{i-1} |L \cap \Sigma^{k}| |L \cap \Sigma^{i-k}| + |L \cap \Sigma^{i}|$$
$$\leq 2^{i} \left(\sum_{k=1}^{i-1} \lambda_{k} \lambda_{i-k} + \lambda_{i}\right).$$

Therefore

$$\left(\sum_{1 \le i \le n} \lambda_i\right) \left(1 + \sum_{1 \le i \le n} \lambda_i\right) \ge \sum_{1 \le i \le n} \left(\sum_{k \ge 1}^{i-1} \lambda_k \lambda_{i-k} + \lambda_i\right) \ge n$$

and so

$$\sum_{1 < i < n} \lambda_i \ge \sqrt{n + 1/4} - 1/2 > \sqrt{n} - 1. \quad \blacksquare$$

We now introduce some notation: let us write $f(n) = \Omega(g(n))$ if there exists a constant c > 0 such that f(n) > cg(n) for infinitely many positive integers n.

Then we have

Corollary 5.

If
$$LL = \Sigma^*$$
, then $\lambda_n = \Omega(n^{-1/2})$.

Proof.

Follows easily from Theorem 4.

III. A Construction Based on Probability Theory.

Our first construction of a sparse L such that $LL = \Sigma^*$ uses some ideas from probability theory. The method is essentially contained in the paper of Yu [Y], but we modify the construction somewhat and give an improved analysis.

Let $\Sigma = \{a, b\}$. (The construction could easily be modified for alphabets with more than two letters.) Let f(x) be a function to be specified later, and define

$$A = \{x \in \Sigma^* \mid \text{ at least the first } \frac{1}{2}f(|x|) \text{ symbols of } x \text{ are } a's\}.$$

Similarly, let

$$B = \{x \in \Sigma^* \mid \text{ at least the last } \frac{1}{2}f(|x|) \text{ symbols of } x \text{ are } a's\}.$$

Finally, let

$$C = \{x \in \Sigma^* \mid x \text{ does not contain a run of at least } f(|x|) \text{ consecutive } a'\mathbf{s}\}.$$

By definition we suppose that the empty string belongs to C. We put $L_f = A \cup B \cup C$.

Theorem 6.

Let f(n) = 0 for $n \le 2$, and $f(n) = \log_2(n/\log n)$ for $n \ge 3$. Then

- (i) L_f is sparse;
- (ii) $L_f L_f = \Sigma^*$.

Proof.

To prove (i), it suffices to show that each of A, B, and C is sparse.

The sparseness of A and B is easy to see, as

$$\lambda_n(A) = \lambda_n(B) = O\left(\left(\frac{\log n}{n}\right)^{1/2}\right).$$

For C, we use the well-known fact that almost all strings of length n contain a run of about $(1 - \epsilon) \log_2 n$ a's. More precisely, we use the following result of Guibas and Odlyzko [GO]:

Lemma 7. (Guibas & Odlyzko)

The probability that a randomly chosen string of a's and b's of length n contains no run of k consecutive a's is

$$\exp(-n2^{-k-1} + O(nk^22^{-2k} + k2^{-k})),$$

where the constant implied by the O does not depend on k and n.

Now, by putting k = f(n) in this lemma, we find that

$$\lambda_n(C) = n^{-1/2} e^{O((\log n)^4/n)} = O(n^{-1/2}).$$

Hence C is sparse, and so L_f is sparse.

To prove (ii), we let

 $D = \{x \in \Sigma^* \mid x \text{ contains a run of at least } f(|x|) \text{ consecutive } a's\}.$

We claim that $D \subseteq BA \subseteq L_fL_f$. To see this, notice that any string x of length n containing a run of at least f(n) consecutive a's can be written as x = yz, where y ends in $\frac{1}{2}f(n)$ consecutive a's, and z begins with $\frac{1}{2}f(n)$ consecutive a's. Since $|y| \leq |x|$ and $|z| \leq |x|$, we see that y ends in $\geq \frac{1}{2}f(|y|)$ consecutive a's, and z begins with $\geq \frac{1}{2}f(|z|)$ consecutive a's. Hence $y \in B$, $z \in A$, and so $D \subseteq BA$.

To complete the proof, we note that $C \cup D = \Sigma^*$.

Note that for this choice of L_f , we have

$$\sum_{1 \le i \le n} \lambda_i(L_f) = \Theta\left(\sqrt{n \log n}\right),\,$$

where by $f = \Theta(g)$ we mean, as usual, that f = O(g) and g = O(f). Thus L_f is not as sparse as the lower bound given in Theorem 4. In the next section we will give an example of a language that actually achieves the lower bound (2) to within a constant factor.

IV. A Construction Inspired by Fractal Geometry.

In this section, and the next one, we give two more constructions for sparse sets L such that $LL = \Sigma^*$. Both constructions work as follows:

First, we find a sufficiently sparse set of non-negative integers S that is an "additive basis of order 2"; i.e. $S + S = \mathbb{Z}^{\geq 0}$, where by T + U for sets T and U we mean the set

$$T+U=\{t+u\mid t\in T,\ u\in U\}.$$

Next, we consider the language

$$L = L(S) = \{ x \in \Sigma^* \mid |x|_a \in S \},$$

where $\Sigma = \{a, b\}$, and by $|x|_a$ we mean the number of occurrences of the symbol a in the string x.

Since $S + S = \mathbb{Z}^{\geq 0}$, we see that $LL = \Sigma^*$, as desired. Also,

$$\lambda_n(L) = \frac{1}{2^n} \sum_{\substack{k \in S \\ 0 \le k \le n}} \binom{n}{k},\tag{3}$$

so if we can show this quantity is o(1), we can conclude that L is sparse.

We can also see how close L comes to the lower bound in (2), which can be viewed as another measure of sparseness. By the binomial theorem,

$$(1-x)^{-s-1} = \sum_{i\geq 0} {s+i \choose i} x^i = \sum_{i\geq 0} {s+i \choose s} x^i$$
$$= \sum_{k\geq s} {k \choose s} x^{k-s} = x^{-s} \sum_{k\geq s} {k \choose s} x^k.$$

Setting x = 1/2, we get

$$\sum_{k \ge s} \frac{1}{2^k} \binom{k}{s} = 2,\tag{4}$$

for all $s \geq 0$.

Hence

$$\sum_{1 \le k \le n} \lambda_k = \sum_{\substack{s \in S \\ 0 \le s \le n}} \sum_{k=s}^n \frac{1}{2^k} \binom{k}{s} \le \sum_{\substack{s \in S \\ 0 \le s \le n}} \sum_{k \ge s} \frac{1}{2^k} \binom{k}{s} \le 2 |S \cap [0, n]|. \tag{5}$$

In this section, an appropriate set S is constructed using inspiration from fractal geometry, while in the next section, we use an old idea from number theory. The reader may wish to compare the construction that follows with a theorem of Steinhaus [S]: every real number in the interval [0,2] can be written as the sum of two elements chosen from the Cantor set. The Cantor set is the set of real numbers in the interval [0,1] that can be expressed using only 0's and 2's in base 3. It is an uncountable set of measure 0, but its fractal dimension is $(\log 2)/(\log 3) \doteq .6309$.

Let T be the set

$$\{0, 1, 4, 5, 16, 17, 20, 21, 64, 65, 68, 69, \ldots\},\$$

the non-negative integers that can be written using only 0's and 1's in their base-4 expansion, and let $S_1 = T \cup 2T$.

We now prove that the set S_1 is indeed an additive basis, and hence that $L(S_1)L(S_1) = \Sigma^*$:

Lemma 8.

Every positive integer can be written as the sum of two elements of S_1 .

Proof.

Let the base-4 expansion of n be $\sum_{i\geq 0} n_i 4^i$, where $n_i \in \{0, 1, 2, 3\}$. Then let y and z be integers whose base-4 expansion is given by $y_i = 2\lfloor n_i/2\rfloor$, and $z_i = n_i \mod 2$. Clearly $n_i = y_i + z_i$, and hence n = y + z (and y and z can be added digit-by-digit without carries).

Our goal is to prove a lemma that allows us to estimate the sum (3) given a bound on $|S \cap [x, x+h]|$. First, however, we state the following useful result of Feller [F, p. 170]:

Lemma 9. (Feller)

There exist constants A and B, independent of k and n, such that

$$\binom{n}{n/2+k} \le \frac{2^n}{\sqrt{\pi n/2}} e^{-2k^2/n} \left(1 + \frac{A}{n} + \frac{B(|k|+1)^3}{n^2}\right).$$

We are now ready to estimate the sum (3). We do this in the following technical Lemma, which is slightly more general than necessary for our immediate purposes. It will, however, also be useful in Section VI.

We will use Vinogradov's notation, common in work on analytic number theory: we write $f(x) \ll g(x)$ for f(x) = O(g(x)).

Lemma 10.

For any set S of positive integers, and any positive integer n, define M to be the largest number of integers in S in any interval of length \sqrt{n} near n/2. More specifically, let

$$M = \max_{\substack{m = n/2 | < \sqrt{n \log n}}} |S \cap [m, m + \sqrt{n}]|.$$

Then

$$\sum_{\substack{k \in S \\ 0 \le k \le n}} \binom{n}{k} \ll \frac{2^n}{\sqrt{n}} (M+1).$$

Proof.

We first note that

$$\sum_{|m-n/2| > \sqrt{n \log n}} \binom{n}{m} \le n \binom{n}{n/2 + \sqrt{n \log n} + O(1)} \ll \frac{2^n}{\sqrt{n}},$$

by Lemma 9. Now set $J = \lfloor \sqrt{\log n} \rfloor$; then

$$\sum_{\substack{m \in S \\ |m-n/2| \le \sqrt{n \log n}}} \binom{n}{m} \le \sum_{j=-(J+1)}^{J} \sum_{\substack{m=n/2-(j+1)\sqrt{n} \\ m \in S}}^{n/2-j\sqrt{n}} \binom{n}{m}$$

$$\le 2 \sum_{j=0}^{J+1} M \binom{n}{n/2 - j\sqrt{n} + O(1)}$$

$$\ll \frac{2^n}{\sqrt{n}} M \sum_{j=0}^{J} e^{-2j^2} \ll \frac{2^n}{\sqrt{n}} M$$

by an application of Lemma 9, and the result follows.

To apply Lemma 10 to the set S_1 mentioned above, we next obtain a bound on $|S_1 \cap [x, x+h]|$:

Lemma 11.

If S_1 is as defined above, then

$$|S_1 \cap [x, x+h)| \le 4\sqrt{h}.$$

(Here [x, x+h) denotes, as usual, the half-open interval containing x but not containing x + h.)

Proof.

First we prove that for all $j \geq 0$,

$$|T \cap [x, x + 4^j)| \le 2^j.$$

To see this, note that the last j base-4 digits in $x, x+1, \ldots, x+4^j-1$ cycle through all 4^j possible combinations of j copies of the digits 0, 1, 2, 3, and exactly 2^j of these contain only 0's and 1's.

From this, it easily follows that

$$|S_1 \cap [x, x+4^j)| \le 2^{j+1}$$
.

Given arbitrary h, we let 4^j be the smallest power of 4 which is $\geq h$; then $4^j < 4h$. Hence

$$|S_1 \cap [x, x+h)| \le |S_1 \cap [x, x+4^j)| \le 2^{j+1} \le 4\sqrt{h}.$$

Hence, combining Lemmas 10 and 11, we find

Theorem 12.

For S_1 defined as above, we have

$$\lambda_n(L(S_1)) = O(n^{-1/4}).$$

Up to a constant factor, this set S_1 is optimal for the averaged lower bound in (2), as the following theorem shows:

Theorem 13.

For S_1 defined as above, we have

$$\sum_{1 \le k \le n} \lambda_k(L(S_1)) \le 8\sqrt{n}.$$

Proof.

Use Lemma 11 and equation (5).

Remark.

Note that, as each integer is represented at least twice in L^2 , we can prove

$$\sum_{1 \le n \le N} \lambda_n \ge \sqrt{2N} - 1.$$

Actually, the maximum of

$$\frac{|S \cap [0, N]|}{\sqrt{N}}$$

can be shown to occur when $N=4^k+4^{k-1}+\ldots+1$, allowing us to replace the 8 in Theorem 13 with $3\sqrt{3}$.

V. A Construction Based on Analytic Number Theory.

In this section, we give a third proof of our result, using methods from analytic number theory.

Let S_2 denote the set of non-negative integers that can be written as the sum of two integer squares. Then by Lagrange's theorem [HW, Thm. 369], which says that every non-negative integer is the sum of *four* integer squares, we easily see that $L_2 = L(S_2)$ satisfies $L_2L_2 = \Sigma^*$.

Theorem 14.

 L_2 is sparse; more precisely, $\lambda_n(L_2) = O((\log n)^{-1/2})$.

Proof.

To apply Lemma 10, it suffices to provide a sufficiently strong upper bound for

$$R(x,h) = |S_2 \cap [x,x+h)|.$$

Landau proved in 1908 [L] that if

$$R(0,h) = \sum_{\substack{0 \le k < h \\ k = u^2 + v^2}} 1,$$

then there is a constant c_3 such that

$$R(0,h) \sim c_3 \frac{h}{\sqrt{\log h}},$$

but this result is not sufficiently strong for our purposes.

Hooley [H] remarked that, "an easy argument involving Selberg's or Brun's method yields the upper bound

$$R(x,h) < \frac{A(\epsilon)h}{\sqrt{\log x}}$$

for $x^{\epsilon} < h < x$," but he did not provide a proof.

We provide a proof along the lines of Hooley's suggestion. We write $f(x) \ll_{\epsilon} g(x)$ to indicate that the constant in the O depends on ϵ .

The idea is to use the fact that a positive integer n is the sum of two squares iff all its prime divisors congruent to 3 (mod 4) appear to an even power. Let $x^{\varepsilon} < h \leq x$. Let $A = A(x,h) = \{n \mid x < n \leq x+h\}, \beta = \{\text{primes } p \equiv 3 \pmod{4} \}$, and $z = x^{\varepsilon\delta}$ for some small fixed $\delta > 0$. Then

$$S(A, \beta, z) = \sum_{\substack{x < n \le x + h \\ p \mid n \Rightarrow p > z \\ \text{or } p \equiv 1 \pmod{4}}} 1 \text{ which is } \ll_{\delta, \varepsilon} \frac{h}{\sqrt{\log z}}$$

by [HRi, Theorem 2.5 (Brun) or 7.2 (Selberg)]. Now, for $any z \ge 1$,

$$R(x,h) \le \sum_{\substack{d \ge 1 \\ p \mid d \Rightarrow p \equiv 3 \pmod{4}}} \sum_{\substack{x/d^2 \le m \le x/d^2 + h/d^2 \\ p \mid m \Rightarrow p > z \text{ or } p \equiv 1 \pmod{4}}} 1$$

(here $n = d^2m$)

$$\leq \sum_{1 \leq d \leq \sqrt{\log x}} S(A\left(\frac{x}{d^2}, \frac{h}{d^2}\right), \beta, z) + \sum_{d \geq \sqrt{\log x}} h/d^2$$

$$\ll \sum_{1 \leq d \leq \sqrt{\log x}} \frac{h/d^2}{\sqrt{\log z}} + \frac{h}{\sqrt{\log x}}$$

$$\ll h/\sqrt{\log x}.$$

Thus $R(x,h) = O(h/\sqrt{\log x})$; combining this with Landau's result, we get $R(x,h) = O(h/\sqrt{\log h})$.

So, taking $h = \sqrt{n}$ and x = n/2 above, we see that we can apply Lemma 10 with $M = O(\sqrt{n/(\log n)})$, which gives

$$\lambda_n = 2^{-n} \sum_{\substack{0 \le k \le n \\ k = u^2 + v^2}} \binom{n}{k} = O((\log n)^{-1/2}).$$

This completes the proof of Theorem 14.

VI. Even Sparser Solutions to $LL = \Sigma^*$.

In the example of Section IV, we constructed a sequence L_1 such that $\lambda_n(L_1) \to 0$, and $\sum_{1 \le k \le n} \lambda_k(L_1)$ was as small as possible (within a constant factor), but individual

 λ_n could get quite large, as large as $cn^{-1/4}$. (Incidentally, the λ_n of that example are sometimes very small, as small as e^{-cn} for some absolute constant c > 0.)

It would be desirable to find a language L with each $\lambda_n = O(n^{-1/2})$ which is, in general, as sparse as such a language can get. If we were to use our method of finding a suitable additive basis S, then we would need S to be quite sparse; i.e. that there exists a constant B such that

$$|S \cap (x, x + \sqrt{x})| \le B,\tag{7}$$

for all x. A slightly stronger requirement on S would be that if $S = \{s_1, s_2, \ldots\}$ and $s_1 < s_2 < \cdots$, then there exists a constant c > 0 such that $s_{n+1} - s_n > cn$.

Then, using Lemma 10, we immediately see

Theorem 15.

If the set S satisfies (7), then $\lambda_n(L(S)) = O(n^{-1/2})$.

It remains to establish that there exists a sequence satisfying (7). However this was done by Cassels [C] (or see the discussion in Halberstam and Roth [HR, pp. 37-43]). The construction is quite complicated.

VII. Generalizations to $L^j = \Sigma^*$.

We might reasonably ask for generalizations of these results to the equation $L^j = \Sigma^*$. A lower bound on the sparseness of such an L is given by $|L \cap \Sigma^n| = \Omega_j(2^n/n^{1-1/j})$ infinitely often and

$$\sum_{1 \le k \le n} \lambda_k \ge n^{1/j} - 1.$$

An "additive basis" construction, as discussed previously in Section IV, goes as follows: let T be the set of non-negative integers whose expansion in base- 2^j contains only 0's and 1's. Let $S = T \cup 2T \cup \cdots \cup 2^{j-1}T$. Then

$$\sum_{1 \leq k \leq n} \lambda_k \leq 2 \left| S \cap [0,n] \right| \leq 4j n^{1/j}.$$

Also, in this case,

$$\sum_{1 \le k \le n} \lambda_k \ge (j!)^{1/j} n^{1/j} - 1$$
$$\ge (e^{-1} + o(1)) j n^{1/j}.$$

Actually we can obtain the better upper bound:

$$\sum_{1 \le k \le n} \lambda_k \le 2|S \cap [1, n]| \le 2(j+2)(1-2^{-j})^{1/j} \ n^{1/j}$$
$$\le (2+o(1))jn^{1/j}$$

as the optimal case occurs where $n = 2^{jr} + 2^{j(r-1)} + \ldots + 1$ so that $|S \cap [1, n]| = 2^{r+1} + j \cdot 2^r$ and $n^{1/j} \ge 2^r / (1 - 2^{-j})^{1/j}$.

Cassels [C] also gave appropriate bases of arbitrary order j. Using his results, we can construct languages L, with $L^j = \Sigma^*$, and $|L \cap \Sigma^n| = O(2^n/n^{1-1/j})$.

VIII. Acknowledgments.

The authors would like to thank C. Ponder for bringing the problem to their attention, and for generously sharing his early insights on the problem.

The third author would like to thank A. Lubiw for useful discussions, and E. Bach, B. Reznick, and P. Flajolet for pointers to the literature.

References

- [C] J. W. S. Cassels, Über Basen der natürlichen Zahlenreihe, Abh. math. Semin. Univ. Hamburg 21 (1957), 247–257.
- [F] W. Feller, An Introduction to Probability Theory and Its Applications, John Wiley & Sons, New York, 1957.
- [GO] L. J. Guibas and A. M. Odlyzko, Long repetitive patterns in random sequences, Z. Wahrscheinlichkeitstheorie verw. Gebiete, 53 (1980), 241–262.
 - [H] C. Hooley, On the intervals between numbers that are sums of two squares. III, J. reine angew. Math. 267 (1974), 207–218.
- [HRi] H. Halberstam and H.-E. Richert, Sieve Methods, Academic Press, London, 1974.
- [HRo] H. Halberstam and K. F. Roth, Sequences, Springer-Verlag, New York, 1983.
- [HU] J. E. Hopcroft and J. D. Ullman, Introduction to Automata Theory, Languages, and Computation, Addison-Wesley, 1979.
- [HW] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, 1985.
 - [L] E. Landau, Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate, Archiv der Mathematik und Physik, **13** (1908), 305–312.

- [P] C. Ponder, A sparse, recursive root of Σ^* , manuscript, March 1989.
- [S] H. Steinhaus, Własność mnogości G. Cantora, Wektor 6 (1916/7), 105–107. In Polish; English translation in Selected Papers, Polish Scientific Publishers, Warsaw, 1985, pp. 205–207.
- [Y] S. Yu, Can the catenation of two weakly sparse languages be dense?, *Disc. Appl. Math.* **20** (1988), 265–267.