Space Complexity of Abelian Groups

Douglas Cenzer, Rodney G. Downey,
Jeffrey B. Remmel, Zia Uddin

December 11, 2008

The Model of Computation

- Multi-tape Turing machine; independent heads.
- Read-only input tape.
- Write-only output tape.
- Space used on other tapes is counted.
- $F : \mathbb{N} \to \mathbb{N}$ is a *proper complexity function* if nondecreasing and there is Turing machine M which computes $1^{F(x)}$ in $\leq \mathcal{O}(|x| + F(|x|)$ steps and uses space $\leq \mathcal{O}(F(|x|)$.
- $LOG = \bigcup_n SPACE(c\ log\ n)$.
- $PLOG = \bigcup_n SPACE((log\ n)^c)$.
- $P = PTIME = \bigcup_n TIME(n^c)$.
- **FACTS**:
  (a) $TIME(G) \subseteq SPACE(G)$;
  (b) $SPACE(G) \subseteq TIME(k^{G(n)+log\ n})$;
  (c) For $f \in LOG$, $|f(x)| \leq |x|^k$.

Standard Universes

- $Tal(0) = Bin(0) = 0$; $Tal(n+1) = 1^{n+1}$.

- $B_k(n) = b_0 b_1 \dots b_r \in \{0, 1, \dots, k-1\}^{r+1}$ when $n = b_0 + b_1 k + \cdots + b_r k^r$.

- $Tal(\mathbb{N}) = \{Tal(n) : n \in \mathbb{N}\}$; $B_k(\mathbb{N}) = \{B_k(n) : n \in \mathbb{N}\}$; $Bin(n) = B_2(n)$.

- The sets $Tal(\mathbb{N})$ and $B_k(\mathbb{N})$ are said to be *standard universes*

- For computable algebra and model theory, every computable set is computably isomorphic to $\mathbb{N}$, so a computable structure is assumed to have universe $\mathbb{N}$ without loss of generality.

- For complexity theoretic model theory and algebra, this is not the case. $Bin(\mathbb{N})$ and $Tal(\mathbb{N})$ are NOT $PTIME$ isomorphic.

- Any computable relational structure is computably isomorphic to a $LOGSPACE$ structure.

- However, there may not be a $PTIME$ structure with a standard universe.

Examples

- In $Tal(\mathbb{N})$, addition, multiplication are $ZEROSPACE$.
- In $Bin(\mathbb{N})$, addition is $ZEROSPACE$ and multiplication is $LOGSPACE$
  – NOT by the usual algorithm!
- In $Bin(\mathbb{N})$, 2^x is $LINSPACE$ (essentially the same as converting to tally.)
- In $Bin(\mathbb{N})$, division (with remainder) is $LOGSPACE$
  – Chiu, Davida and Litow (Theor. Inform. Appl. 2001).
- In $Bin(\mathbb{N})$, primality is $PTIME$
  – Agrawal, Kayhal and Saxena, Ann. Math. 2004.
- Intuition is that $PTIME$ algorithms can be converted into $LOGSPACE$.

Composition Lemma

- **Lemma 1**. Let F, G be proper nonconstant complexity functions, g a unary function in $SPACE(G)$ and f an n-ary function in $SPACE(F)$. Then the composition $g \circ f$ can be computed in $SPACE \leq G(2^{kF})$ for some constant k.

  Proof is a generalization of the standard proof that $LOGSPACE$ is closed under composition.

- **Corollary 1**

  (a) $LOGSPACE \circ LINSPACE = LINSPACE$;

  (b) $PLOGSPACE \circ PLOGSPACE = PLOGSPACE$;

  (c) $PLOGSPACE \circ LINSPACE \subseteq PSPACE$;

  (d) $EXPSPACE \circ LOGSPACE = EXPSPACE$;

Logspace Set Isomorphisms

- **Theorem 1**. Let $A \subseteq Tal(\mathbb{N})$ be $LOGSPACE$, and let $A = \{a_0 < a_1 < a_2 < \ldots\}$. The following are equivalent:

  (a) A is $LOGSPACE$ set-isomorphic to $Tal(\mathbb{N})$.

  (b) For some k and all $n \geqslant 2$, we have $|a_n| \leq n^k$.

  (c) The canonical bijection between $Tal(\mathbb{N})$ and A mapping 1^n to a_n, $n \geq 0$, is $LOGSPACE$.

  Sketch: To compute 1^n from $a \in A$, count the number of members of A which are less than a. Keep track of the numbers in binary and do the testing in tally. To compute a_n from 1^n, test $1^i \in A$ until n members are found. The test is a composition of (1) converting $Bin(i)$ to $Tal(i)$ and (2) testing $Tal(i) \in A$, which is $LINSPACE$ in $Bin(i)$ and hence $LOGSPACE$ in $Tal(n)$.

More Logspace Set Isomorphisms

- **Lemma 2**. (Radix Representation.) For $k \geq 2$, the following sets are $LOGSPACE$ isomorphic:

  (a) $Bin(\mathbb{N})$;

  (b) $B_k(\mathbb{N})$;

  (c) $\{0, 1, \ldots, k-1\}^*$.

  Furthermore, for each isomorphism f above, $|f(x)| \leq c|x|$ for some c.

- **Definition**. $A \oplus B = \{2n : n \in A\} \cup \{2n+1 : n \in B\}$. $A \otimes B = \{\langle a, b\rangle : a \in A \;\&\; b \in B\}$, where $\langle a, b\rangle$ is a (new) logspace pairing function.

- **Lemma 3**. Let $A \subseteq Tal(\mathbb{N})$ be nonempty $LOGSPACE$.

  (a) $A \oplus Tal(\mathbb{N})$ is $LOGSPACE$ isomorphic to $Tal(\mathbb{N})$ and $A \oplus Bin(\mathbb{N})$ is $LOGSPACE$ isomorphic to $Bin(\mathbb{N})$.

  (b) $A \otimes Tal(\mathbb{N})$ is $LOGSPACE$ isomorphic to $Tal(\mathbb{N})$ and $A \otimes Bin(\mathbb{N})$ is $LOGSPACE$ isomorphic to $Bin(\mathbb{N})$.

  (c) $Bin(\mathbb{N}) \oplus Bin(\mathbb{N})$ and $Bin(\mathbb{N}) \otimes Bin(\mathbb{N})$ are $LOGSPACE$ isomorphic to $Bin(\mathbb{N})$.

Logspace Structures

- Complexity Theoretic Model Theory and Algebra was developed by Nerode and others, focusing on $PTIME$ structures. [Cenzer & Remmel, Handbook of Recursive Mathematics, 1998.]

- **Lemma 4**. If $\mathcal{A}$ is a $LOGSPACE$ structure and φ a $LOGSPACE$ bijection from A to $\mathcal{B}$, then $\mathcal{B}$ is $LOGSPACE$.

  If $\mathcal{M}$ is a structure with universe $M \subseteq \mathbb{N}$, then $Tal(\mathcal{M})$ denotes the representation of $\mathcal{M}$ with universe $Tal(M)$ and $Bin(\mathcal{M})$ the representation with universe $Bin(M)$.

- **Lemma 5**.

  (a) If $Bin(\mathcal{M})$ is LOG, then $Tal(\mathcal{M})$ is $PLOG$.

  (b) If $Bin(\mathcal{M})$ is $LINSPACE$ and for all functions f, $|f^{\mathcal{B}}(m_1, \ldots, m_n)| \leqslant c(|m_1| + \cdots + |m_n|)$ for some constant c, then $Tal(\mathcal{M})$ is $LOGSPACE$.

Abelian Groups

- $\mathbb{Z}$ is the group of integers, and $\mathbb{Z}_k = \mathbb{Z}\ mod\ k\mathbb{Z}$.
- $\mathbb{Q}$ is the group of rationals and $\mathbb{Q} \mod \mathbb{Z}$, the quotient group.
- $\mathbb{Q}_p$ is the p-adic rationals and $\mathbb{Z}(p^\infty) = \mathbb{Q}_p \mod \mathbb{Z}$.
- $\oplus_i \mathcal{A}_i$ is the direct sum of $\langle A_i \rangle_{i<\omega}$, that is, the set of $(a_0, a_1, \dots)$ where all but finitely many $a_i = 0$. $\oplus_\omega \mathcal{A}$ denotes $\oplus_i \mathcal{A}_i$ where each $\mathcal{A}_i = \mathcal{A}$.
- The sequence $\mathcal{A}_i$ is *fully uniformly* $LOGSPACE$ over $B = Bin(\mathbb{N})$ (and similarly for $B = Tal(\mathbb{N})$) if
  (i) The set $\{\langle Bin(n), a\rangle : a \in A_n\}$ is $LOGSPACE$.
  (ii) The functions $F(Bin(n), a, b) = a +_n b$ and $G(Bin(n), a, b) = a -_n b$, are $LOGSPACE$.
  (iii) The function $e(Tal(i)) = e_i$, is $LOGSPACE$.

Direct Sums

- **Lemma 6**. Let B be either $Tal(\mathbb{N})$ or $Bin(\mathbb{N})$. Suppose that the sequence $\mathcal{A}_i = (A_i, +_i, -_i, e_i)$ of groups is fully uniformly $LOGSPACE$ over B. Then

  (a) $\oplus_i \mathcal{A}_i$ is computably isomorphic to a $LOGSPACE$ group with universe contained in $Bin(\mathbb{N})$.

  (b) If $A_i \subset A_{i+1}$ for all i,and if there is a $LOGSPACE$ function $f : \{0,1\}^* \to B$ such that $a \in A_{f(a)}$, then $\bigcup_i \mathcal{A}_i$ is a $LOGSPACE$ group with universe contained in B.

  (c) If each $\mathcal{A}_i$ has universe $Bin(\mathbb{N})$, then $\oplus_i \mathcal{A}_i$ is computably isomorphic to a $LOGSPACE$ group with universe $Bin(\mathbb{N})$.

  (d) If each $\mathcal{A}_i$ has universe $Tal(\mathbb{N})$ and there is a constant c such that for each i and any $a, b \in A_i$, $|a +_i b| \leqslant c(|a| +_i |b|)$ and $|a -_i b| \leqslant c(|a| +_i |b|)$, then $\oplus_i \mathcal{A}_i$ is computably isomorphic to a $LOGSPACE$ group with universe $Tal(\mathbb{N})$.

LOGSPACE Representation of $\mathbb{Q}$

- **Theorem 2**. Let $k > 1$ be in $\mathbb{N}$ and let p be a prime. Each of the groups $\mathbb{Z}$, $\bigoplus_\omega \mathbb{Z}_k$, $\mathbb{Z}(p^\infty)$, and $\mathbb{Q}_p$ are computably isomorphic to $LOGSPACE$ groups $\mathcal{A}$ with universe $Bin(\mathbb{N})$, and $\mathcal{B}$ with universe $Tal(\mathbb{N})$.

  Sketch: For $\mathbb{Z}$ this follows from $LOGSPACE$ addition.

  For $\oplus_\omega Z_k$, there is a natural $LOGSPACE$ model with universe $B_k(\mathbb{N})$. Lemma 2 gives universe $Bin(\mathbb{N})$ and Lemma 5 gives universe $Tal(\mathbb{N})$.

  For $Z(p^\infty)$, let $e_1 e_2 \ldots e_n \in B_p(\mathbb{N})$ represent $\frac{e_1}{p} + \frac{e_2}{p^2} + \cdots \frac{e_n}{p^n}$.

  For $\mathbb{Q}_p$, let $\langle z, q \rangle$ represent $z + q$ where $z \in \mathbb{Z}$ and $q \in Z(p^\infty)$. For addition of $z_1 + q_1$ and $z_2 + q_2$, check whether $q_1 + q_2 \geq 1$.

- **Theorem 3**. $\mathbb{Q}$ and $\mathbb{Q}$ mod $\mathbb{Z}$ are computably isomorphic to $LOGSPACE$ groups with universe $Bin(\mathbb{N})$, and to $LOGSPACE$ groups with universe $Tal(\mathbb{N})$.

  Sketch: $\mathbb{Q}$ mod $\mathbb{Z} = \oplus_p \mathbb{Z}(p^\infty)$. Use Lemma 6 and the fact that the primes are $PTIME$ in binary and hence $LOGTIME$ in tally.

  For $\mathbb{Q}$, proceed as in Theorem 2 for $\mathbb{Q}_p$.

Typical Failure of Categoricity

- **Lemma 7** For any p-time set $A = \{Bin(a_0) < Bin(a_1) < \cdots\}$, there is a set $M = M(A) = \{Bin(m_0) < Bin(m_1) < \cdots\}$ such that M is in $LOGSPACE$ and the map which takes $Bin(m_i)$ to $Bin(a_i)$ is $LOGSPACE$, but there is no primitive recursive injection of A into M.

- **Theorem 4** There is a countably infinite family of $LOGSPACE$ groups each isomorphic to $\mathbb{Z}(p^\infty)$ such that no two of these are primitive recursively isomorphic. These may be taken to have standard universe $Bin(\mathbb{N})$ or $Tal(\mathbb{N})$, as desired.

- Similar results obtain for the groups $\mathbb{Q}$ and $\mathbb{Q}\ mod\ \mathbb{Z}$.

Some Qualified Categoricity

- Let $o(a)$ denote the order of a in a fixed group G.

  G is said to have *linear size order* if there exists $c \geq 1$ such that for all $a \in G$:

  $|Bin(o(a))| \leq c|a|$ and $|a| \leq c|Bin(o(a))|$.

- **Theorem 5** Let G and H be two $LINSPACE$ groups isomorphic to $Z(p^{\infty})$ and each having linear size order. Then there is a $LINSPACE$ isomorphism between G and H.

- A similar result obtains for the group $\mathbb{Q} mod \mathbb{Z}$.

The End