Monotone complexity of a pair

Pavel Karpovich

25 june 2009

Abstract

We define monotone complexity $KM(x, y)$ of a pair of binary strings x, y in a natural way and show that $KM(x, y)$ may exceed the sum of the lengths of x and y (and therefore its a priori complexity) by $\alpha \log(|x| + |y|)$ for every $\alpha < 1$ (but not for $\alpha > 1$).

We also show that decision complexity of a pair or triple of strings does not exceed the sum of its lengths.

1 Introduction

There are different versions of Kolmogorov complexity: plain complexity (C), prefix complexity (K), decision complexity (KR), monotone complexity(KM), etc. Let us recall the definitions of plain, monotone and decision complexities in a form suitable for generalizations.

1.1 Plain complexity

Kolmogorov complexity $C_F(x)$ of a binary string x with respect to a computable function F (a decompressor) is defined by

$$C_F(x) = min\{|p|, F(p) = x\}$$

There exists an optimal decompressor U such that C_U is minimal up to $O(1)$; C_U is then called (plain) Kolmogorov complexity of x.

Let us reformulate this definition in a way that is parallel to the definition of monotone complexity. Instead of a function F let us consider its graph. A *description mode* is an enumerable set W of pairs of binary strings that is a graph of a function, i.e.,

$$\langle p, x\rangle \in W,\ \langle p', x'\rangle \in W,\ p = p' \ \Rightarrow\ x = x',$$

If $\langle p, x\rangle \in W$, then p is called a *description for x with respect to W*. The complexity $C_W(x)$ of a binary string x is the length of the shortest description for x with respect to W. There is an optimal description mode S such that for every description mode W there exists c_W such that

$$C_S(x) \leqslant C_W(x) + c_W$$

for every binary string x. The corresponding function C_S is the plain Kolmogorov complexity.

1.2 Monotone complexity

Monotone complexity $KM(x)$ was defined by L. A. Levin [3] who gave a criterion of Martin-Löf randomness in its terms: a binary sequence ω is Martin-Löf random if and only if

$$|x| - KM(x) < c$$

for some constant c and all prefixes x of sequence ω. We will use the definition of monotone complexity in terms of binary relations. A *monotone description mode* is an enumerable set W of pairs of binary strings such that:

1. if $\langle p, x\rangle \in W$ and $p \preceq p'$, then $\langle p', x\rangle \in W$.
2. if $\langle p, x\rangle \in W$ and $x' \preceq x$, then $\langle p, x'\rangle \in W$.
3. if $\langle p, x\rangle \in W$ and $\langle p, x'\rangle \in W$, then $x \preceq x'$ or $x' \preceq x$.

Here $x \preceq x'$ means that x is a prefix of x' (or $x = x'$).

If $\langle p, x\rangle \in W$, then p is called a *description for x with respect to W*. The monotone complexity $KM_W(x)$ of x with respect to a monotone description mode W is (again) the length of the shortest description for x. There is an optimal monotone description mode S such that:

$$KM_S(x) \leqslant KM_W(x) + c_W$$

for every monotone description mode W and binary string x. The function KM_S is called *monotone Kolmogorov complexity.* It is indeed monotone: If x is a prefix of x', then $KM(x) \leqslant KM(x')$.

1.3 Decision complexity

Decision complexity was defines by Loveland D.W. [?]. As before we reformulate the definition in terms of binary relations.

A *decision description mode* is an enumerable set W of pairs of binary strings such that:

1. if $\langle p, x\rangle \in W$ and $x' \preceq x$, then $\langle p, x'\rangle \in W$.
2. if $\langle p, x\rangle \in W$ and $\langle p, x'\rangle \in W$, then $x \preceq x'$ or $x' \preceq x$.

If $\langle p, x\rangle \in W$, then p is called a *description for the string x with respect to W*. The decision complexity $KR_W(x)$ of x is the length of the shortest description for x with respect to W. There is an optimal desicion description mode S such that:

$$KR_S(x) \leqslant KR_W(x) + c_W$$

for every decision description mode W and binary string x. $KR_S(x)$ is called *decision Kolmogorov complexity.*

The notions of monotone complextity and decision complexity are naturaly generalized to definitions of monotone complexity of a pair and decision complexity of a pair.

2 Monotone complexity of a pair.

A *monotone description mode for pairs* is a pair of enumerable sets W_1 and W_2; each of them is the monotone description mode (as defined earlier).

The monotone complexity $KM_{W_1,W_2}(x,y)$ of a pair of binary strings x and y is the length of the shortest string p, such that $\langle p,x\rangle \in W_1$ and $\langle p,y\rangle \in W_2$ (i.e., p describes x with respect to W_1 and p describes y with respect to W_2).

There is an optimal monotone description mode for pairs and we can define monotone complexity of a pair, denoted by $KM(x,y)$.

Monotone complexity of pairs has property of monotonicity: if a binary string x is a prefix of another string x' and y is a prefix of y', then monotone complexity of a pair $\langle x,y\rangle$ is less then monotone complexity of a pair $\langle x',y'\rangle$.

Monotone complexity of a pairs $\langle x,x\rangle$, $\langle x,\Lambda\rangle$ and $\langle \Lambda,x\rangle$ is equal (with up to constant) ordinary monotone complexity $KM(x)$ of the string x.

Ordinary monotone complexity of the string x is less then the length of the string x with up to a constant:

$$KM(x) < |x| + c$$

It' easy to prove that monotone complexity of a pair $\langle x,y\rangle$ is less then sum of lengths of strings x and y and additional weight $\alpha\log(|x|+|y|)$ with up to a constant and $\alpha < 1$:

$$KM(x,y) \leqslant |x| + |y| + \alpha\log(|x|+|y|) + O(1).$$

Indeed, we can use string a like description for the pair $\langle x,y\rangle$, wich is a concatenation of prefix code for the x and string y. The result of this paper shows that this bound cann't be significantly improved.

Theorem. *For every $\alpha < 1$ and a constant $c \in \mathbb{N}$ it's possible to find a pair of binary strings $\langle x,y\rangle$ such that*

$$KM(x,y) > |x| + |y| + \alpha\log(|x|+|y|) + c.$$

Proof. Suppose the inequality

$$KM(x,y) \leqslant |x| + |y| + \alpha\log(|x|+|y|) + c$$

holds for some $\alpha < 1$ and $c \in \mathbb{N}$ and all pairs of binary strings $\langle x,y\rangle$. We will find a contradiction in this assumtion. Let

$$f(n) = n + \lfloor \alpha \log n \rfloor + c$$

($f(0)$ will be equal c). We should lead to a contradiction the assumption that every pair of binary strings $\langle x,y\rangle$ has description of length $f(|x|+|y|)$. (note: if p is a description for a string x, then every p' such that $p \preceq p'$ is also description for x). We fix some universal monotone description mode W of pairs.

Let S is a some set of binary strings. We will say that S gets 2^{-k} points for a pair of binary strings $\langle x,y\rangle$ with $|x|+|y| = k$ if there is a string p in S such that p is a description of the pair $\langle x,y\rangle$ with respect to monotone description mode W and the length of p is equal $f(k)$. We will sum such points for different pairs, but the set S can get points for a pair $\langle x,y\rangle$ only once(if a pair $\langle x,y\rangle$ has two good descriptions p and p' in the set S we will only add 2^{-k} points to the sum). We will call such sum a gain of the set S, denoted by $F(S)$.

Some set S can get $k+1$ points for good descriptions of pairs with sum of string's lengths k(each of 2^k binary strings of length k can be devided in a pair of strings in $k+1$ ways). It's the maximal value.

Let S is a set of all strings with length less or equal then $f(n)$ for some n. By the assumption, in the S there are descriptions for all pairs $\langle x, y\rangle$ with sum of string's lengths less or equal then n, $|x|+|y| \leqslant n$. And the gain of S should be equal

$$\sum_{k \leqslant n}(k+1) \simeq n^2/2$$

We will prove that it cann't be greater then $O(n^{1+\alpha})$. This fact will lead us to a contradiction.

Lemma. *The gain of the set of all strings with the length less or equal then $f(n)$ cann't be greater then $O(n^{1+\alpha})$.*

Proof. We will get upper bounds on gains of sets $S_{k,n}$ for $0 \leqslant k \leqslant n$, where $S_{k,n}$ is a tree of binary strings, it consists of all strings with lengths less or equal then $f(n)$, wich have prefix x - some binary string with the length $f(k)$. The set $S_{k,n}$ can get points only for pairs with sum of string's lengths greater or equal then k and less or equal then n. There are $2^{f(k)}$ different subsets $S_{k,n}$ with different string-roots, wich have length $f(k)$, but subtrees have similar structure and we will get common bound on gain.

We will get a bound on gain of subtree $S_{0,n}$. It will prove the lemma. At first, we will prove a bound on the gain of $S_{n,n}$, then on the gain of $S_{n-1,n}$, and so on. The set $S_{n,n}$ consists of only one string with the length $f(n)$, wich can be description for $n+1$ pairs of binary strings or less. Obviosly, the gain of $S_{n,n}$ is less or equal then $(n+1)2^{-n}$ points.

We will get a bound on $F(S_{k,n})$, the gain for $S_{k,n}$, by induction. Suppose that $f(k+1) = f(k)+1$, the set $S_{k,n}$ contains the root of subtree $S_{k,n}$(a binary string x with length $f(k)$) and two subtrees $S_{k+1,n}$. The most simple bound on $F(S_{k,n})$ is the sum of gains of this subtrees and the root's gain, but we should use the fact that if the root of set $S_{k,n}$ is a description for many pairs then there should be of lot of pairs wich will have descriptions in both subtrees $S_{k+1,n}$, and we should take into acount points for each of this pairs only once.

Let string u is a root of subtree $S_{k,n}$. There is some maximal pair of binary strings $\langle x, y\rangle$ such that u is a description of $\langle x, y\rangle$ and if u is a description of some another pair $\langle x', y'\rangle$ then $x' \preceq x$ and $y' \preceq y$, u is a description for all such pairs. Suppose there are r pairs with sum of string's lengths k such that the root u is a description for each of them(obviosly, $0 \leqslant r \leqslant k+1$). The gain of the root for this pairs will be $r2^{-k}$ points. Also there are at least $r-1$ pairs with sum of string's lengths $k+1$ such that the root u is a description for them too, this pairs have descriptions with length $f(k+1)$ in both subtress $S_{k+1,n}$. And we should substruct from result bound on gain a penalty $\max(r-1, 0)2^{-(k+1)}$ for this pairs. Also the root u will be a description for at least $r-2$ pairs with sum of string's lengths $k+2$, at least $r-3$ pairs with sum of string's lengths $k+3$ and so on. We should take into account penalties for this pairs too. Gains and penalties shoud be taken only for pairs with sum of string's lenghts less or equal the n. We have the following bound on the gain of $S_{k,n}$:

$$F(S_{k,n}) < 2F(S_{k+1,n}) + r2^{-k} - (r-1)2^{-(k+1)} - \\ - (r-2)2^{-(k+2)} - \ldots - \max(1, r+k-n)2^{-\min(k+r-1,n)}$$

We can simlify the expression on rights side of the inequality:

$$F(S_{k,n}) < 2F(S_{k+1,n}) + 2^{-k} + (r-1)2^{-k} - (r-1)2^{-(k+1)} - \\ - (r-2)2^{-(k+2)} - \ldots - \max(1, r+k-n)2^{-\min(k+r-1,n)}$$

$$F(S_{k,n}) < 2F(S_{k+1,n}) + 2^{-k} + 2^{-(k+1)} + \\ + (r-2)2^{-(k+1)} - (r-2)2^{-(k+2)} - \ldots - \max(1, r+k-n)2^{-\min(k+r-1,n)}$$

$$F(S_{k,n}) < 2F(S_{k+1,n}) + 2^{-k} + 2^{-(k+1)} + \\ + (r-2)2^{-(k+2)} - \ldots - \max(1, r+k-n)2^{-\min(k+r-1,n)}$$

$$F(S_{k,n}) < 2F(S_{k+1,n}) + 2^{-k} + 2^{-(k+1)} + \\ + 2^{-(k+2)} + \ldots + 2^{-\min(k+r-1,n)+1} + \max(1, r+k-n)2^{-\min(k+r-1,n)}$$

$$F(S_{k,n}) < 2F(S_{k+1,n}) + 2^{-k} + 2^{-(k+1)} + 2^{-(k+2)} + \ldots + 2^{-\min(k+r-1,n)+1} \\ + 2^{-\min(k+r-1,n)+1} - 2 \cdot 2^{-\min(k+r-1,n)} + \max(1, r+k-n)2^{-\min(k+r-1,n)}$$

At the end we will have the expression:

$$F(S_{k,n}) < 2F(S_{k+1,n}) + 2^{-k+1} + \max(-1, r+k-n-2)2^{-\min(k+r-1,n)} \tag{1}$$

We have to notice that right side of the inequality has it's maximum with $r = k+1$, and our final bound will not depend on the value of r. We have made the assumption that $f(k+1) = f(k)+1$, in the case $f(k+1) = f(k)+2$ we will use a coefficient 4 with $F(S_{k+1,n})$. The final bound will be:

$$F(S_{k,n}) < 2^{f(k+1)-f(k)}F(S_{k+1,n}) + 2^{-k+1} + max(-1, 2k-n-1)2^{max(-2k,-n)} \tag{2}$$

We multiply left and right sides of inequality on $2^{f(k)}$, start with bound on the gain of $F(S_{n,n})$ we will get bound on $F(S_{0,n})$ by induction:

$$2^{f(0)}F(S_{0,n}) < \sum_{k=1}^{n} 2^{f(k)-k+1} + \sum_{k=1}^{n} max(-1, 2k-n-1)2^{f(k)-min(2k,n)} \tag{3}$$

Increase $f(k) = k + \lfloor \alpha \log k \rfloor + c$ to the value $k + \alpha \log k + c$ and delete a half of summands from the second sum with coefficient -1:

$$2^{f(0)}F(S_{0,n}) < 2^{c+1}\sum_{k=1}^{n} k^{\alpha} + \sum_{k=\lfloor \frac{n+1}{2} \rfloor}^{n} (2k-n-1)k^{\alpha}2^{k-n+c} \tag{4}$$

Both sums from the inequality (4) have $O(n^{1+\alpha})$ values. It proves the lemma.

3 Decision complexity of a pair.

A *decision description mode for pairs* is a pair of enumerable sets W_1 and W_2; each of them is a decision description mode.

The complexity $KR_{W_1,W_2}(x,y)$ of a pair of binary strings x and y is the length of the shortest string p, such that $\langle p,x\rangle \in W_1$ and $\langle p,y\rangle \in W_2$ (i.e., p describes x with respect to W_1 and p describes y with respect to W_2).

There is an optimal decision description mode for pairs and we can define decision complexity of a pair, denoted by $KR(x,y)$.

We can also define decision complexity of a triple in the same way, denoted by $KR(x,y,z)$. It's easy to see that ordinary decision complexity of a binary string x is less then length of x with up to a constnt.

It's also easy to prove that decision complexity of a pair is less then the sum of string's lengths in this pair with up to a constant. The set W_1 from our definition will be the set of all pairs $\langle p,p'\rangle$ such that p' is some prefix of string p. The set W_2 will be the set of all pairs $\langle p,p'_R\rangle$ such that p'_R is a prefix of the reversed string p. For this mode a description of a pair $\langle x,y\rangle$ will be a string, wich is a concatenation of the string x and the reversed string y. It's length is equal to the sum of string's lengths in the pair and:

$$KR(x,y) < |x| + |y| + c$$

In this paper we will prove the same inequality for decision complexity of a triple:

$$KR(x,y,z) < |x| + |y| + |z| + c$$

We will prove that there is a set $Z_n(n \in N)$ from 2^n different triples of binary strings such that lengths of strings in each triple is equal to n and for every triple $\langle x,y,z\rangle$ with sum of string's length $n(\ |x|+|y|+|z| = n)$ there is a triple $\langle x',y',z'\rangle$ in the set Z_n such that $x \preceq x'$, $y \preceq y'$ and $z \preceq z'$. The construction will be made for all n.

Actually we will find a set $A_n = \{a^n_{i,j}\}$ from $3n$ different binary vectors in n-dimensional linear space F_2^n indexed by two indexes: i and $j(i \in \{1,..,n\}, j \in \{1,2,3\})$. For every subset B of A_n from n vectors wich has the following property: if it contains some vector $a^n_{i,j}$ then it contains all vectors $a^n_{i',j}$ with $i' \leqslant i$, the subset B will be a linear independent set of vectors.

Suppose we have such subsets of vectors A_n. There are 2^n different linear binary functions on space F_2^n. For each linear function f we constract a triple of binary strings $\langle x,y,z\rangle$ from the set A_n: the string x will be a concatenation of n bits $\{f(a^n_{1,1}),..,f(a^n_{n,1})\}$, the string y will be a concatenation of n bits $\{f(a^n_{1,2}),..,f(a^n_{n,2})\}$, the string z will be a concatenation of $\{f(a^n_{1,3}),..,f(a^n_{n,3})\}$. We will construct 2^n different triples of binary strings. It's easy to see that the set of this triples will have all properties of the set Z_n described above. If we construct set of vectors A_n we will construct the set of triples Z_n too.

Lemma. There is a set $A_n = \{a^n_{i,j}\}$ from $3n$ different binary vectors in n-dimensional linear space F_2^n indexed by two indexes i and $j(i \in \{1,..,n\}, j \in \{1,2,3\})$ such that for every subset B of A_n from n vectors wich has the following property: if B contains some vector $a^n_{i,j}$ then it contains all vectors $a^n_{i',j}$ with $i' \leqslant i$, the subset B is the linear independent set of vectors.

Proof. We will construct sets A_n in different dimensions by induction. It's easy to construct sets A_1, A_2 and A_3. We will prove that if we can construct the set A_k for dimension k then it's possible to construct the set A_{k+3} too.

At first notice that we can described desired sets B by maximal values of index i of their vectors with another index $j = 1$, $j = 2$, $j = 3$, it can be described by three numbers. We will say that a set B has maximal indexes $\{p, q, r\}$ if it's the union of the sets $\{a^{k+3}_{1,1}, .., a^{k+3}_{p,1}\}$, $\{a^{k+3}_{1,2}, .., a^{k+3}_{q,2}\}$, $\{a^{k+3}_{1,3}, .., a^{k+3}_{r,3}\}$, some of numbers in the triple $\{p, q, r\}$ could be equal 0, and we are interested only in sets B with $p + q + r = k + 3$.

Let a set $\{x_1, ..., x_k\}$ be a basis for linear space F^k_2. Vectors from the set $A_k = \{a^k_{i,j}\}$ are linear combinations of vectors $\{x_1, ..., x_k\}$. Let a set $\{x_1, ..., x_k, a, b, c\}$ be a basis for linear space F^{k+3}_2. We will think that F^k_2 is a subbspace of F^{k+3}_2 and vectors from A_k belong to the space F^{k+3}_2 too. We are ready to construct the set $A_{k+3} = \{a^{k+3}_{i,j}\}$:

$$
\begin{array}{lll}
a^{k+3}_{1,1} = a & a^{k+3}_{1,2} = b & a^{k+3}_{1,3} = c \\[1em]
a^{k+3}_{i+1,1} = a^k_{i,1} + \delta_{i,1}c & a^{k+3}_{i+1,2} = a^k_{i,2} + \delta_{i,2}a & a^{k+3}_{i+1,1} = a^k_{i,1} + \delta_{i,3}b \\[1em]
a^{k+3}_{k+2,1} = b + c & a^{k+3}_{k+2,2} = a + c & a^{k+3}_{k+2,3} = a + b \\[1em]
a^{k+3}_{k+3,1} = c & a^{k+3}_{k+3,2} = a & a^{k+3}_{k+3,3} = b
\end{array}
$$

where index i belongs to the set $\{1, .., k\}$ and coefficients $\delta_{i,j}$ are binary. We will explain how to choose coefficients $\delta_{i,j}$ later. At first we will check that the property of linear independency holds for a part of desired sets B. It's easy to see that the following sets of vectors will be linear independent, and it doesn't depend on the choise of coefficients $\delta_{i,j}$:

1. 3 sets with maximal indexes: $\{k + 3, 0, 0\}$, $\{0, k + 3, 0\}$, $\{0, 0, k + 3\}$.

2. 6 sets with maximal indexes: $\{k + 2, 1, 0\}$, $\{1, k + 2, 0\}$, $\{1, 0, k + 2\}$, $\{k + 2, 0, 1\}$, $\{0, k + 2, 1\}$, $\{0, 1, k + 2\}$.

3. All sets B are lenear independent wich contain all three vectors $a^{k+3}_{1,1}, a^{k+3}_{1,2}, a^{k+3}_{1,3}$(all maximal indexes greater then 0).

We should also check other sets B: sets B wich don't contain vectors with $j = 1$, sets B wich don't contain vectors with $j = 2$, sets B wich don't contain vectors with $j = 3$.

We will choose coefficients $\{\delta_{i,1}\}$ such that all sets B with maximal indexes $\{p, q, 0\}(p > 0, q > 0)$ will be linear independent sets. We should not take into account coefficients $\delta_{i,2}$, because there is a vector $a^{k+3}_{1,1} = a$ in this sets B. We will think that coefs $\delta_{i,2}$ are equal 0 on this step. Suppose the set B is a set with maximal indexes $\{2, k + 1, 0\}$. It has $k + 1$ vectors with index i greater then 1. If coef $\delta_{1,1}$ is equal 0, then this vectors aren't linear independent set by induction, vector $a^k_{1,1}$ is some linear combination of vectors $\{a^k_{i,2}\}$. We will set $\delta_{1,1}$ to 1 and the set B will be linear independent set. We take into account this choise then we will choose another coefs $\{\delta_{i,1}\}$. Look at the next set B with maximal indexes $\{3, k, 0\}$. There are two cases : the subset of vectors wich have index i greater then 1 can be linear independent or not. If it's linear independent then we will set coef $\{\delta_{2,1}\}$ to 0, in the other case it will be equal 1. Step by step we will determine all coefs $\{\delta_{i,1}\}$. In the same way we will also choose sets of coefs $\{\delta_{i,2}\}$ and $\{\delta_{i,3}\}$. And all desired sets B will be linear independent.

References

[1] Li M., Vitányi P., *An Introduction to Kolmogorov Complexity and Its Applications*, Second Edition, Springer, 1997. (638 pp.)

[2] A. Shen, *Algorithmic Information Theory and Kolmogorov Complexity.* Lecture notes of an introductory course. Uppsala University Technical Report 2000-034.

[3] . ., , , 1973, . 212, . 3, . 548-550. Levin L.A., On the notion of a random sequence, Soviet Math. Dokl., 14:1413-1416, 1973.

[4] P. Gács, On the relation between descriptional complexity and algorithmic probability, FOCS 1981. Journal version: Theoretical Computer Science, 1983, v. 22, p. 71-93.

[5] . ., . ., . , . 25, . 6 (156), . 85-127. : A.K. Zvonkin, L.A. Levin, The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms. Russian Math. Surveys, 25:6 (1970), p. 83-124.