1067-68-1246 **Yevgeniy Dodis**, **Mihai Patrascu** and **Mikkel Thorup*** (mthorup@research.att.com), 180 Park Avenue, Florham Park, NJ 07932. *Changing Base without Losing Space.*

We describe a simple, but powerful local encoding technique, implying two surprising results:

1. We show how to represent a vector of n values from a set Σ using $\lceil n \log_2 |\Sigma| \rceil$ bits, such that reading or writing any entry takes $O(1)$ time. This demonstrates, for instance, an "equivalence" between decimal and binary computers, and has been a central toy problem in the field of succinct data structures. Previous solutions required space of $n \log_2 |\Sigma| + n / \lg^{O(1)} n$ bits for constant access.

2. Given a stream of n bits arriving online (for any n, not known in advance), we can output a *prefix-free* encoding that uses $n + \log_2 n + O(\lg \lg n)$ bits. The encoding and decoding algorithms only require $O(\lg n)$ bits of memory, and run in constant time per word. This result is interesting in cryptographic applications, as prefix-free codes are the simplest counter-measure to extensions attacks on hash functions, message authentication codes and pseudorandom functions. Our result refutes a conjecture of [Maurer, Sjödin 2005] on the hardness of online prefix-free encodings. (Received September 20, 2010)