Electronic Colloquium on Computational Complexity - Reports Series 1996 - available via:

Comment 01 on ECCC TR96-041

FTP: ftp.eccc.uni-trier.de:/pub/eccc/
WWW: http://www.eccc.uni-trier.de/eccc/
Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

In TR-96-041, Goldreich and Wigderson show

Theorem 1 (Goldreich and Wigderson) *For every n, k, and $k \leq m \leq 2k$, and for every $S \subseteq \{0,1\}^n$ of size 2^k, there is a circuit of size $2^{2k-m}n^{O(1)}$ mapping S 1-1 to $\{0,1\}^m$.*

They also show their bound to be tight, but only up to a polynomial in n. Examining the dependence of their bounds on n, we find that for $m = 2k$, their construction gives at best a circuit of size $O(n \log n \log\log n)$. This is because their construction is based on universal hashing, and the best known circuits for universal hashing (with the weakest possible definition of universal) are based on Schonhage and Strassen's multiplication circuit which has the stated size. For $m < 2k$, the situation becomes worse: If the proofs of TR-96-041 are left unmodified, the dependence on n becomes cubic. This can be optimized somewhat, but since the circuits of TR-96-041 are based on circuits for n-wise independent hashfunctions, it is not obvious how to get an $o(n^2)$ bound.

In a recent paper [1], I obtain the following improved bounds:

Theorem 2 *For every $S \subseteq \{0,1\}^n$ of size 2^k, the following circuits exist:*

- *For any $\epsilon > 0$, a circuit of size $O(n)$ mapping S 1-1 to $(2+\epsilon)k$ bits.*
- *A circuit of size $O(n + k \log k)$ mapping S 1-1 to $2k$ bits.*
- *A circuit of size $O(n + k2^{2k-m} + k \log k)$, mapping S 1-1 to m bits for $k \leq m \leq 2k$.*
- *A circuit of size $O(n + k2^k)$, mapping S 1-1 to k bits.*

Since this paper is mainly about data structures, I am not making it into an ECCC-report, but as I indicate below, it can be accessed from my homepage.

References

[1] P.B. Miltersen Error correcting codes, perfect hashing circuits, and deterministic dynamic dictionaries. Manuscript, 1997. Available from *http://www.brics.dk/~bromille/*