Publications in Communication Complexity Theory
László Babai
(in the order of my preference, annotated)

[93] László Babai, Noam Nisan, and Mario Szegedy. Multiparty protocols and Logspace-hard pseudorandom sequences. In *Proc. 21st STOC*, pages 1–11. ACM Press, 1989. doi:10.1145/73007.73008. See 1992.126.

[126] László Babai, Noam Nisan, and Mario Szegedy. Multiparty protocols, pseudorandom generators for Logspace, and time-space tradeoffs. *J. Comput. System Sci.*, 45(2):204–232, 1992. doi:10.1016/0022-0000(92)90047-M. Special issue. Full version of item 1989.93.

This pair of papers contains lower bounds in the "number-on-forehead" (NOF) model of multi-party communication complexity that remain the strongest even to date[1], after 24 years, in spite of considerable effort. The paper includes applications to a variety of models of computation: time-space tradeoff for multi-head Turing machines, lower bounds for branching programs, pseudorandom generators for Logspace, and more. Many more applications were found later in a variety of contexts, including circuit complexity and the analysis of streaming data; the results and techniques continue to inspire work to this date. The paper introduced "cylinder intersections" and characterized NOF complexity in terms of these. It introduced an iterated Cauchy-Schwarz scheme to prove lower bounds on the discrepancy of certain functions over cyclinder-intersections. This method has found many subsequent applications and is similar to a method used by Bourgain two decades later to estimate certain exponential sums (C. R. Math. 2005).

---

[79] László Babai, Péter Frankl, and Janos Simon. Complexity classes in communication complexity theory. In *Proc. 27th FOCS*, pages 337–347. IEEE Comp. Soc. Press, 1986. doi:10.1109/SFCS.1986.15.

This paper introduced the communication complexity analogues of TM complexity classes like NP^{cc}, proved some separations, and left a large number of open problems that have given rise to research that continues to this date. The paper introduced "rectangular reductions" and completeness with respect to these reductions. It identified comple problems for many of the classes; most notably the DISJOINTNESS problem, complete for coNP. The paper gave the first lower bound on the probabilistic c.c. of DISJOINTNESS, $\Omega(\sqrt{n})$, subsequently improved to $\Omega(n)$ by Balasubramaian and Schnitger, and simplified by Razborov. DISJOINTNESS became one of the most studied problems in communication complexity theory.

---

[167] László Babai, Thomas Hayes, and Peter Kimmel. The cost of the missing bit: Communication complexity with help. In *Proc. 30th STOC*, pages 673–682. ACM Press, 1998. doi:10.1145/276698.276883. Conference version of item 2001:177.

[1] A widely cited but erroneous announcement by Chung and Tetali (SICOMP 1993) notwithstanding.

[177] László Babai, Thomas Hayes, and Peter Kimmel. The cost of the missing bit: Communication complexity with help. *Combinatorica*, 21(4): 455–488, 2001. doi:10.1007/s004930100009. URL `http://people.cs.uchicago.edu/~laci/papers/missingbit1.pdf`. Expanded version of item 1998.167.

This pair of paper extends the BNS lower bounds (above) to m-bit output and shows that the same strong lower bounds remain in effect even if an all-knowing and benevolent helper reveals $m-1$ bits of information. The paper introduces two notions of multi-color discrepancy, a combinatorial and an analytic one; the latter employs characters of finite abelian groups. The main new tool is an interplay between these two concepts of discrepancy. This method is similar to one introduced by Grolmusz around the same time. The paper also proves strong new lower bounds in the Boolean (one-bit output) model; in particular, it gives a BNS-type lower bound for the trace of the product of k matrices over $\mathbb{F}_2$.

---

[142] László Babai, Peter Kimmel, and Satyanarayana V. Lokam. Simultaneous messages vs. communication. In E. Mayr and C. Puech, editors, *Proc. 12th Symp. Theoretical Aspects of Comp. Sci. (STACS'95)*, volume 900 of *Lect. Notes in Comp. Sci.*, pages 361–372, Munich, 1995. Springer. doi:10.1007/3-540-59042-0_88.

[183] László Babai, Anna Gál, Peter Kimmel, and Satyanarayana V. Lokam. Communication complexity of simultaneous messages. *SIAM J. Comput.*, 33(1):137–166, 2004. doi:10.1137/S0097539700375944. URL `http://people.cs.uchicago.edu/~laci/papers/bgkl-SM.pdf`. Greatly expanded version of 1995.142.

This pair of papers lays the foundations of the study of the "simultaneous messages" (SM) model of multi-party communication: the players do not communicate with each other; each player sends a message to a referee who does not see any of the input. The referee then annouces the result. Lower bounds in this model suffice for applications to other models of computation such as ACC. The paper describes polynomial lower bounds and unexpected upper bounds in this model; notably, it is shown that with $k \geq 2+\log_2 n$ players, the Generalized Inner Product function can be computed with polylogarithmic communication in the SM model.

---

[156] László Babai and Peter Kimmel. Randomized simultaneous messages: Solution of a problem of Yao in communication complexity. In *Proc. 12th IEEE Conf. on Computational Complexity (CCC'97)*, pages 239–246. IEEE Comp. Soc. Press, 1997. doi:10.1109/CCC.1997.612319.

This paper solves a then 17-year old problem of Yao. The solution is entirely different from and considerably simpler than a prior solution (not known to us at the time) by Newman and Szegedy that solves a special case (STOC 1996). A proof similar to ours in spirit was simultaneously found by Bourgain and Wigderson.