Abstract for an Invited Paper
for the MAR05 Meeting of
The American Physical Society

How more is different: a quantum information perspective

JOHN PRESKILL, California Institute of Technology

Studies in quantum information science are deepening our understanding of the properties of quantum many-body systems. I will review and assess recent progress in the development of fast quantum algorithms, the analysis of the security of quantum cryptographic protocols, and the characterization of quantum entanglement. I will emphasize especially the quest for fault-tolerant implementations of quantum information processing. A large scale quantum computer (if we ever succeed in building one that really works) will be a very unusual quantum many-body system. To operate reliably despite the debilitating effects of environmental decoherence and imperfect control, the computer must process quantum information that resides in a large protected subsystem of a still larger system, where operations that act nontrivially on the protected subsystem are highly nonlocal. The theory of quantum error-correcting codes and fault-tolerant quantum computation prescribes how such subsystems can be constructed and manipulated. Protected subsystems could be realized naturally in two-dimensional systems with nonabelian topological order.