PHYSICAL REVIEW A **92**, 062303 (2015)

Quantum metrology: Heisenberg limit with bound entanglement

Ł. Czekaj,[1] A. Przysiężna,[1,*] M. Horodecki,[1] and P. Horodecki[2]

[1]*Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-952 Gdańsk, Poland and Institute of Theoretical Physics and Astrophysics, and National Quantum Information Centre in Gdańsk, 81-824 Sopot, Poland*

[2]*Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, 80-233 Gdańsk, Poland and National Quantum Information Centre in Gdańsk, 81-824 Sopot, Poland*

(Received 1 September 2014; revised manuscript received 14 August 2015; published 1 December 2015)

Quantum entanglement may provide a huge boost in the precision of parameter estimation. However, quantum metrology seems to be extremely sensitive to noise in the probe state. There is an important still open question: What type of entanglement is useful as a resource in quantum metrology? Here we raise this question in relation to entanglement distillation. We provide a counterintuitive example of a family of *bound entangled* states which can be used in quantum enhanced metrology with the precision advantage approaching the Heisenberg limit. This shows that so-called *distillability* is not necessary for quantum advantage in metrology. Surprisingly, entanglement of the applied states is very weak, which is reflected by the lack of the so-called unlockability property. Moreover we find instances where quantum Fisher information reports the presence of entanglement where a well-known class of nonlinear entanglement witnesses (stronger than multisetting correlation Bell inequalities) does not. We have thus provided strong evidence that quantum metrology can be treated as additional operational face of multipartite entanglement, independent of two other basic operational features used in quantum information theory: nonlocality and distillability.

DOI: 10.1103/PhysRevA.92.062303 PACS number(s): 03.67.Bg

I. INTRODUCTION

Estimation of a physical parameter is an important goal in many areas of science [1]. One of intriguing aspects of quantum mechanics in this context is quantum metrology. In its most popular form quantum metrology has its origins in atomic spectroscopy [2,3]; however, the idea was present even earlier in fermionic systems [4] and, from a different perspective, quantum optical interferometry [5] (for recent developments along this line, see [6] and references therein). The general search for possible improvement of estimation precision is also of great importance in the domain of atomic clocks [7] and interferometric measurement of a phase shift in gravitational wave detection [8]. Since there are many quantities we cannot measure directly, a protocol for a measurement is typically indirect: we use an additional probe system to interact with the one under investigation. Due to the interaction the probe gains information about the parameter we want to measure. Then, we inspect the probe coming out from the measurement, and on the basis of the obtained data, we estimate the desired parameter. Obviously, we want to obtain the highest possible accuracy for that estimation. We can improve the accuracy by repeating the experiment multiple times or, equivalently, making a multipartite probe to interact with the system.

In the quantum world there is another possibility to increase the accuracy: prepare the probe in a particular quantum state, i.e., in the entangled state. To be more concrete, for a classical probe that contains n particles (we can also consider it a measurement performed n times) accuracy scales as $1/\sqrt{n}$. That is the so-called shot-noise limit (SNL). However, if the system is in a particular entangled state, then accuracy can be improved up to $1/n$. This limit, called the Heisenberg limit (HL) gives us the best accuracy we can get that is allowed by quantum mechanics. Both of these bounds can be derived from the quantum Cramér-Rao bound and quantum Fisher information (QFI) [9–13]. For a more general description of the parameter estimation procedure see [14,15].

Recently, it has been shown [16,17] that local (memoryless) noise puts limits on the accuracy, offering only a linear improvement of the precision when compared to the shot-noise limit. Since this no-go theorem was established, the efforts in the quantum metrology domain have split into optimization of the performance for a finite number of entangled particles [18], extending the paradigm of metrology and combining it with error correction schemes (see [19–21]), and witnessing genuine quantum correlations with QFI. We would like to take a different perspective: analyzing the relation of metrology as an operational approach to studying quantum resources to other operational paradigms [e.g., distributed laboratories and local operations and classical communication (LOCC) paradigm, nonlocality theory] known in the quantum information domain. The main motivation here is the following broad perspective: entanglement is a peculiar kind of correlation of a composite quantum system. The weirdness of these correlations can manifest itself in many different way. But there is only one definition of entanglement. We thus face fundamental questions: To what extent are those various manifestations mutually interconnected, and to what extent can they appear independently of one another?

These questions were deeply explored in quantum information theory, for example, the relation between algebraic entanglement and distillability [22] and the relation between nonlocality and entanglement distillation or the Peres conjecture [23–25]. However, the relation between usefulness for quantum enhanced metrology and other operational manifestations of entanglement such as nonlocality and entanglement has not been yet explored.

In this paper, we want to fill this gap by constructing nondistillable states which are useful for metrology. We also

*a.przysiezna@gmail.com

provide states which do not violate a wide class of Bell inequalities (hence, it is plausible that they admit a local hidden-variable model) but offer a quantum advantage for metrology.

Apart from the above fundamental questions, there are some more technical issues related to our results. Namely, it is known that genuine multipartite quantum entanglement is necessary to surpass the SNL (see [26]); however, not every entangled state gives the same improvement, and among entangled states there are also states that are not suitable for quantum metrology; that is, they do not surpass the SNL. In particular, quantum scaling is hard to obtain in the case of entangled states with a high noise factor (see [17]), which we have to deal with in realistic experiments where decoherence and preparation errors are present and perfect NOON states seem to be far beyond our reach. Right now, searching for optimal states fulfilling certain constraints is a highly complicated optimization problem (see using matrix product state (MPS) [18]). Therefore, an important question is, What features of entanglement are needed for the state to be useful in quantum metrology, or taking another point of view, what type of entanglement can be detected by QFI? We believe that to be able to break the present impasse, we need to build a theory of "use of entanglement in metrology" analogous to the theory of entanglement itself, and our results are the first steps in this direction.

The states on which we focus in this paper belong to a group of states with such a high noise factor that they are unusable for most quantum information tasks. These highly mixed states are bound entangled (BE) states and were predicted in 1998 [27,28] as a new kind of entanglement. Bound entangled states are those from which no pure entanglement can be distilled when only LOCC are available (see the Appendix for a short introduction to the paradigm involving LOCC). The sufficient condition for an entangled state to be bound entangled is its positive partial transposition [27,29]. The bound entangled states, called "black holes" of quantum information [30], have been created in laboratories in a series of experiments with ions, photons, and nuclear spins. Among multipartite bound entangled states we distinguish unlockable and nonunlockable ones. Unlockable BE states are those in which it is possible to group parties in such way that performing collective quantum operations in one group makes distillation of pure entanglement between two parties from the other group possible. The prominent example here is a four-qubit Smolin state [31]. For this state no entanglement can be distilled by local quantum operations and classical communication among the parties, but a joint measurement performed on any two of the parties enables the other two parties to create a pure maximally entangled state between them without coming together. Nonunlockable BE states are those in which we cannot obtain a pure entangled state by these means. One may say that entanglement is "more bound" there.

The impossibility of pure entanglement distillation makes BE states (in particular nonunlockable ones) not useful for many quantum information and communication tasks such as quantum teleportation or dense coding. When it comes to quantum cryptography, on the one hand, it has been shown that BE states may be useful [32]; on the other hand, very recent results show that the resulting cryptographic key in some cases may be not suitable for quantum repeater schemes [33]. In the case of metrology, no instance of usefulness of BE states is known so far. In [34] the authors relate QFI and BE states and show that for certain BE states, averaged Fisher information is higher than for separable states. However, there are no results linking QFI and the average QFI. Even though the relation of BE states with averaged QFI was given, the usability of BE in the case of standard formulation of quantum metrology (i.e., with known interaction between a system and a probe) remained an open question.

Intuition suggests that the high degree of noise of BE should be the reason for the negative answer for the question regarding its usability in quantum metrology. It is, in particular, especially tempting to expect such an answer in classes of multiqubit states, the entanglement of which cannot be *unlocked*: even if some parties get together, they cannot help the other parties to distill entanglement.

We will show that this intuition is misleading. We will investigate a class of mixed states that are Greenberger-Horne-Zeilinger (GHZ) diagonal and present an example of bound entangled states which have an advantage over product states in the metrology of the phase shift around the z axis. Moreover, the entanglement of those states cannot be unlocked. Our family of states exhibits an an^2 scaling (with $a \geqslant \frac{1}{4}$) of the QFI in the asymptotic limit.

The first immediate implication of our result is that metrology is not related to the fundamental concept of entanglement theory, which is distillation of entanglement, as we can get a quantum advantage from states that cannot be distilled. Furthermore, we know that bound entangled states usually do not display nonlocality (although there are exceptions [23,24], they are quite hard to find). This poses a question of whether nonlocality is necessary for metrology and suggests that the two operational tasks, metrology and nonlocality, may be independent of each other. We show that some of our states do not violate Bell inequalities for all multisetting correlation Bell inequalities, which strongly suggests that metrology is not fundamentally related to another central operational feature of entanglement, which is nonlocality. Last but not least, we did the above nonlocality check by showing that some of our states are not detected by a strong nonlinear entanglement witness [35], which illustrates the power of QFI as a tool for entanglement detection: the sub-shot noise can report entanglement even when the other well-known tool does not.

One may ask how our states, although highly noisy, can surpass the no-go result [17] according to which quantum scaling cannot be obtained in the presence of generic local noise. The reason is the different structure of the noise in our case. In particular, our states do not have full rank, unlike in the case of generic local noise.

II. QUANTUM FISHER INFORMATION FOR GHZ-DIAGONAL STATES

We consider a class of n-qubit states that are diagonal in the generalized GHZ basis:

$$\rho = \sum_{i=0}^{2^{n-1}-1} (\lambda_i^+ |\phi_i^+\rangle\langle\phi_i^+| + \lambda_i^- |\phi_i^-\rangle\langle\phi_i^-|), \tag{1}$$

where for simplicity we assume that $\lambda_i^+ \geqslant \lambda_i^-$. States ρ constitute a superset of states studied in [36–38] in the context of separability and distillability conditions. By generalized GHZ basis we mean

$$|\phi_i^\pm\rangle = \frac{1}{\sqrt{2}}(|i\rangle \pm |\bar{i}\rangle), \tag{2}$$

where for an n-qubit system $i \in \{0,1,\ldots,2^{n-1}-1\}$. Here we put an n-digit binary representation of i in $|i\rangle$ and its negation in $|\bar{i}\rangle$. Note that in the range of indices (i.e., $\{0,1,\ldots,2^{n-1}-1\}$) the n-digit binary representation of i always starts with zero. For example, for a four-qubit system we have $|\phi_2^\pm\rangle = \frac{1}{\sqrt{2}}(|0010\rangle \pm |1101\rangle)$.

We study the usefulness of states ρ for quantum metrology in terms of Fisher information (FI). FI quantifies the amount of information on an unknown parameter θ that may be extracted by measurements. For a probe state $\rho(\theta)$ which depends on the parameter θ and the positive operator-valued measurement (POVM) with elements $\{E_\mu\}$ and values μ, FI reads

$$F = \sum_\mu \frac{1}{P(\mu|\theta)}[\partial_\theta P(\mu|\theta)]^2, \tag{3}$$

where $P(\mu|\theta) = \mathrm{Tr}[\rho(\theta)E_\mu]$ are conditional probabilities and POVM values μ estimate the parameter θ. FI gives a lower bound, referred to as the Cramér-Rao bound, for a standard deviation of the estimator for a fixed value of the parameter θ [39,40]:

$$\Delta\theta_{\mathrm{est}} = \sqrt{\langle(\mu-\theta)^2\rangle} \geqslant \frac{1}{\sqrt{F}}. \tag{4}$$

The maximum value of FI which may be achieved by measurement optimization [10–13] is given by the quantity called quantum Fisher information. It depends only on the initial state of the probe system and a form of evolution which links the estimated parameter θ and the final state of the probe system $\theta \mapsto \rho(\theta)$. In the case of multipartite separable states, the maximal value of QFI scales linearly with the system size (SNL). This is reflected by the separability condition for quantum Fisher information F_Q (see [34]); that is, for any separable state ρ_{sep}, the following holds:

$$F_Q(\rho_{\mathrm{sep}}) \leqslant n. \tag{5}$$

On the contrary, the highest scaling, i.e., the quadratic one (HL), $F_Q(\rho) \approx n^2$ may be achieved only by entangled states ρ. For more information, see [9].

In this paper we discuss a setup where a phase shift around the z axis is estimated. Probe state ρ undergoes evolution according to $U_\theta = \exp[-i\theta Z]$, where Z is a Hermitian generator of the form $Z = (\sigma_Z^{(1)} + \cdots + \sigma_Z^{(n)})/2$. The index (i) denotes a qubit on which σ_Z acts. In such a case, QFI for the probe state $\omega = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ is given by [12]

$$F_Q = 2\sum_{i,j} \frac{(\lambda_i - \lambda_j)^2}{\lambda_i + \lambda_j} |\langle\phi_i|Z|\phi_j\rangle|^2. \tag{6}$$

For states of the form (1), this formula simplifies to

$$F_Q = \sum_i w_i^2 \frac{(\lambda_i^+ - \lambda_i^-)^2}{\lambda_i^+ + \lambda_i^-}, \tag{7}$$

where $w_i = [\#0(i) - \#1(i)]$ is the difference between number of zeros and ones in a binary representation of i (e.g., in a four-qubit system $w_0 = 4$, $w_1 = 2$, $w_2 = 2$, etc.). This is easy to check when we observe that operator Z is diagonal in the standard basis with $z_{i,i} = w_i, z_{2^n-1-i,2^n-1-i} = -w_i$ and that the only nonzero terms are those with $\langle\phi_i^+|Z|\phi_i^-\rangle = w_i/2$.

III. BOUND ENTANGLED GHZ-DIAGONAL STATES

Since here we are interested in bound entangled states, we derive the criterion for a state to be BE.

Proposition 1. A GHZ-diagonal state is nonunlockable bound entangled for every $1:(n-1)$ cut if its eigenvalues $\lambda_i^\pm$ (we assumed that $\lambda_j^+ \geqslant \lambda_j^-$) satisfy

$$\min_{i\in\Omega_j}(\lambda_i^+ + \lambda_i^-) \geqslant \lambda_j^+ - \lambda_j^- \tag{8}$$

for every $j \in 0,1,\ldots,2^{n-1}-1$, where

$$\Omega_j = \{\mathrm{NOT}_{2,3,\ldots,n}(j)\} \cup \{\mathrm{NOT}_k(j) | k \in \{1,2,\ldots,n\}\}. \tag{9}$$

$\mathrm{NOT}_k(j)$ is a negation on the kth bit of the binary representation of j.

For the proof see the Appendix.

IV. THE FAMILLY OF $\rho_{n,k}$ STATES

Let us now introduce a subset of GHZ-diagonal states. It contains states $\rho_{n,k}$ that are BE and, as we show next, are useful for quantum metrology. The considered states $\rho_{n,k}$ are parameterized by two numbers: n, which is the number of qubits in the system, and k, which characterizes the structure of the states as follows:

$$\rho_{n,k} = \lambda P_{n,k}^+ + \frac{\lambda}{2}(Q_{n,k}^+ + Q_{n,k}^-), \tag{10}$$

where the projector $P_{n,k}^+ = \sum_{i:\ \#1(i)<k \text{ or } \#1(i)>n-k} |\phi_i^+\rangle\langle\phi_i^+|$ and $Q_{n,k}^\pm = \sum_{i:\ \#1(i)=k \text{ or } \#1(i)=n-k} |\phi_i^\pm\rangle\langle\phi_i^\pm|$, with the linear factor $\lambda = 1/\sum_{i=0}^k \binom{n}{i}$ following directly from the normalization condition $\mathrm{Tr}(\rho_{n,k}) = 1$. Here the notation $\#1(i)$ means the number of ones in the binary representation of the number i. For instance, $\#1(i=7) = 3$ since the binary representation "1101" of the number 7 contains three ones. The exemplary state $\rho_{n,k}$ with $n = 4, k = 2$ is

$$\rho_{4,2} = \frac{1}{11}\sum_{i\in I_1} |\phi_i^+\rangle\langle\phi_i^+| + \frac{1}{22}\sum_{i\in I_2} |\phi_i^+\rangle\langle\phi_i^+| + |\phi_i^-\rangle\langle\phi_i^-|, \tag{11}$$

where $I_1 = \{0,1,2,7\}$ and $I_2 = \{3,4,5,6\}$.

Proposition 2. For any n,k the state $\rho_{n,k}$ passes the positive partial transpose test (PPT) with respect to local transposition on any single-qubit system, and as such, it is bound entangled.

For the proof see the Appendix. States $\rho_{n,k}$ are, however, non positive partial trace (NPPT) in the $m:(n-m)$ cuts for $m \geqslant 2$.

In the case of the states under consideration, with the assumption $k < \lfloor\frac{n}{2}\rfloor$, the equation for quantum Fisher infor-

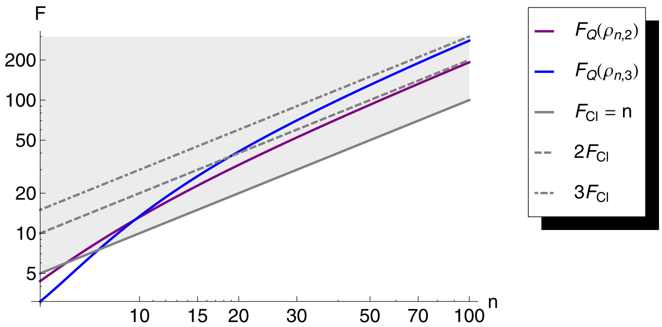

FIG. 1. (Color online) Precisely calculated QFI and the limit it achieves at infinity for two different values of k. Blue and purple lines show how $F_Q^{n,k}$ change for $k = 3$ and $k = 2$, respectively, and dashed lines are limits that these functions achieve at infinity. The gray region denotes better than classical metrology.

mation (7) takes the form

$$F_Q^{n,k} = \lambda \sum_{j=0}^{k-1} (n-2j)^2 \binom{n}{j}. \tag{12}$$

It simply comes from counting the number of states with given w. In Fig. 1 we show how QFI approaches the limit of nk for $k = 2$ and $k = 3$. We see that if k does not grow with n, the usual shot-noise classical limit is kept. However, things dramatically change when we put the dependence of k on n. In what follows, we shall utilize this fact, proving the central result of the paper.

Proposition 3. Quantum Fisher information $F_Q^{n,k}$ given by Eq. (12) satisfies

$$F_Q^{n,k} \geqslant (n-2k)^2 \frac{k}{n+1} \tag{13}$$

for any n and $k < \frac{n}{2}$. In particular, putting $k(n) = an$ $(a < \frac{1}{2})$ we obtain following asymptotic behavior

$$\lim_{n\to\infty} \frac{F_Q^{n,k(n)}}{a(1-2a)^2 n^2} \geqslant 1. \tag{14}$$

For the proof see the Appendix.

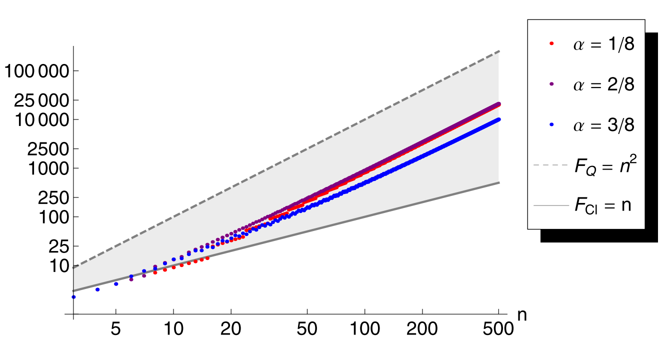

FIG. 2. (Color online) Asymptotic behavior of the quantum Fisher information for $\rho_{n,k}$ states for the case when $k = an$. The dependence on n is calculated for three different values of a: 1/8 (blue dots), 1/4 (green dots), and 3/8 (red dots). The gray region denotes better than classical metrology.

Optimizing the denominator in formula (14) gives $a = \frac{1}{4}$. Hence, the Fisher information scales in this case not worse than $\sim\frac{n^2}{16}$. In the end, this results in an upper bound for the scaling of the measurement precision (4) by $\frac{2\sqrt{2}}{n}$ as opposed to its shot-noise lower bound $\frac{1}{\sqrt{n}}$. Asymptotic behavior of $F_Q^{n,k(n)}$ is illustrated in Fig. 2 for three different values of a.

V. CORRESPONDENCE WITH BELL INEQUALITIES

One of the fundamental features of quantum states caused by quantum entanglement is the *lack of local realism*. It is known that some entangled states satisfy all Bell inequalities since the explicit hidden-variable model can be constructed for them (see [41] for some states with A nonpositive partial transpose and [42] for PPT states). It, however, does not follow automatically that the states are fully locally realistic. As was shown recently [43], there exist entangled states whose nonlocality can be revealed only by using a *sequence of measurements* (i.e., when each party performs sequentially more than one measurement on the system; for formal definitions see [44,45]; it was formerly discussed in Refs. [46,47]). One of the fundamental open questions of quantum physics is whether all entangled quantum states are nonlocal at least in the latter weaker sense.

Here we find that the Fisher information treated as a separability test may outperform the efficiency of some strong Bell inequality tests (see [48,49]). Even more, we prove it by showing that it outperforms a much stronger nonlinear entanglement witness based on the correlation tensor of the state [35]. This entanglement witness has the form of the following inequality:

$$\|T\|_{HS}^2 = \sum_{k_1,\ldots,k_n=1}^{3} T_{k_1\cdots k_n}^2 \leqslant 1, \tag{15}$$

satisfied by any separable state where T is a correlation tensor of the state (see the Appendix). Now we want to compare this test with our present separability test which is shot-noise-limit bound for Fisher information. We have calculated the factor (15) for some states from the class $\rho_{n,k}$ or some states from the class $\rho_{n,k}$. We obtained that for $k = 2$ and $k = 3$ and n respectively from the sets {7,8} and {8,9,10}, the Fisher information criterion outperforms separability condition (15); that is, it detects entanglement while the latter does not (implying also fulfilment of the specific Bell inequalities), which can be seen in Fig. 3.

This is surprising since quantum metrology involves only two settings of binary Pauli observables per site. We believe that the possible power of QFI lies in *its differential character*. Indeed, the above observation suggests the need for deep study of nonlocality in the context of metrology, which has, to our knowledge, not been pursued so far. In particular, one of the questions that may be raised is the possible role of metrology as a necessary condition for standard or even weaker, i.e., sequential, nonlocality. In fact, it may be that some of the presented states even allow for the general (not only a finite number of settings, like here, but with continuum settings) single-measurement hidden-variable model, even though they

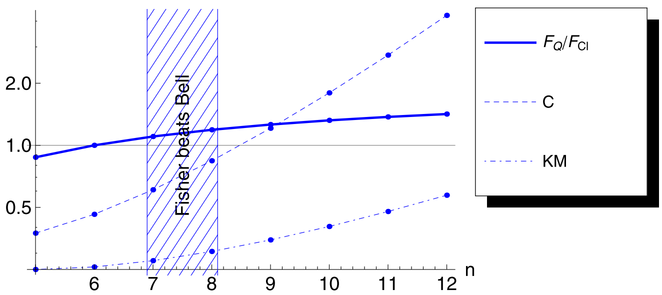

FIG. 3. (Color online) Comparison of the Fisher information criterion and correlation condition in the power of entanglement detection. Here we plot F_Q/F_{Cl} and $\mathcal{C}^{(n)}$ for states in the form $\rho_{n,2}$. Tests detect entanglement when their values exceed 1. The most interesting region is where the Fisher information criterion detects entanglement for states which do not violate any correlation Bell inequality with dichotomic observables and $2^{n-1} \times 2^{n-1} \times 2^{n-2} \times \cdots \times 2$ settings [48,49] (i.e., $F_Q/F_{Cl} > 1$ and $\mathcal{C}^{(n)} < 1$). For comparison we also plot value of the Klyachko-Mermin (KM) inequality. For the analyzed states it performs much worse than $\mathcal{C}^{(n)}$.

exhibit sequential nonlocality. Metrology may be just a first signature of that.

VI. DISCUSSION AND CONCLUSIONS

We have shown by explicit construction that there exist bound entangled states that can be useful for quantum metrology and can reach the accuracy scaling exactly according to the Heisenberg limit. The result has been shown for a very noisy entanglement which is not only unlockable but even essentially weaker since, as long as some qubit is kept as an elementary subsystem, no collection of the remaining qubits into groups can result in free entanglement.

The most natural question here is about the maximal value of the linear factor in the sub-shot-noise limit for bound entanglement cn^2. We have found here that c is not less than $\frac{1}{8}$. The question is whether it can reach the optimal pure GHZ-state value and only the speed of the convergence is an issue or if there is a threshold imposed on c from the bound-entanglement property.

The character of the results opens new directions of possible research. The fact that Fisher information outperforms strong Bell inequalities as a multiparty entanglement witness naturally suggests the need for further analysis of the interplay of the role of nonlocality in the sub-shot-noise limit. The natural question (especially in the context of recent results on nonlocality [43]) to answer would be, Is there any family of quantum states that allows for a general Local Hidden Variables (LHV) model but can be used to obtain sub-shot-noise (i.e., better than classical) quantum metrology? This question is related to another question (especially in the context of both general requirements in quantum metrology [26] and recent results on nonlocality [43]) regarding whether there is any chance for sub-shot-noise metrology for states obeying the PPT condition with respect to *any* cut. While the present result may be generalized to get the sub-shot-noise metrology with bound entanglement with the PPT property under an arbitrary sublinear fraction of qubits, further improvement to PPT under any cut does not seem to be possible for GHZ-diagonal states. We believe, however, that our result can be generalized to Dicke-type states, where a possible chance for a positive answer to the above question may be more likely.

The next important question that naturally arises, especially because of the unlockability property, is, What is the general role of error correction in the case of metrology? In fact, the noise can never be filtered out from bound entanglement, and this is the reason why the corresponding binding entanglement channels are resistant to *any* error correction and have a quantum capacity of zero [50,51]. This is what makes the present results quite nonintuitive.

As a by-product, it seems that the phenomenon presented here may reopen the fundamental question of quantum computational tasks at a high noise rate even on the level of quantum correlations beyond entanglement [52]. Indeed, as opposed to the quantum games theory based on "kinematical" aspects of quantum physics, quantum metrology exploits dynamics explicitly and, as such, may be closer to the perspective of quantum algorithmic tasks.

ACKNOWLEDGMENTS

We thank P. Mazurek for numerous discussions at the early stage of this project. This work is supported by ERC AdG QOLAPS and EC grant QUASAR. A.P. is supported by the International Ph.D. Project "Physics of future quantum-based information technologies" Grant No. MPD/2009-3/4 from the Foundation for Polish Science, by University of Gdańsk Grant No. 538-5400-B169-13, and by National Center of Science Grant No. UMO-2014/14/M/ST2/00818.

APPENDIX

1. Bound entanglement

We start this short introduction to bound entanglement with a description of the local operation and classical communication (LOCC) paradigm. In this paradigm we consider several separated laboratories which share an entangled state. Any local quantum operation may be performed in the laboratory. Moreover classical bits may be exchanged between laboratories; however, any transfer of the quantum system is prohibited. For example, laboratories may perform a sequence of measurements on their local parts of the shared state, where the choice of measurement depends on the classical message obtained from other laboratories. Restriction to classical communication is interesting for two reasons: from a practical point of view, classical communication is much easier than quantum communication, but more important, classical communication cannot convey any quantum information. Therefore, in the LOCC paradigm no "new" entanglement can be established between laboratories.

Many results of quantum information theory (e.g., state teleportation, the advantage in distributed computation, etc.) are based on the assumption that separated laboratories share pure maximally entangled states. Since it is hard to meet this condition because of imperfection during state transmission, it is important to know how to obtain pure entanglement from a noisy state. Entanglement distillation protocols [53] address this problem, providing a way to obtain pure entanglement

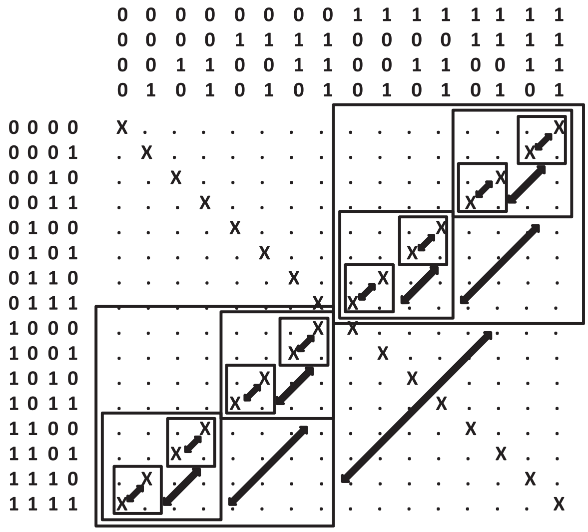

FIG. 4. The pictorial structure of an exemplary (four-qubit) GHZ diagonal state written in the standard basis (the numeration of the basis is explicitly provided). Only the elements depicted by an X are nonzero. Partial transposition with respect to a given qubit is represented by the group of elementary transpositions represented by arrows of the same length starting from the longest arrow that corresponds to the transposition with the first qubit. Note that partial transpositions with respect to different qubits commute. Hence, a transposition with respect to a given subset of qubits corresponds just to a composition of several operations, each consisting of all arrows of one kind. For example, the state transposed partially with respect to the first and the last qubits results from the application of the operation corresponding to the longest arrow followed by the operations corresponding to all the smallest arrows.

from a much large amount of noisy entanglement. Formally, state ρ is distillable if there exist an n such that $\rho^{\otimes n}$ may be transformed by the use of LOCC to pure bipartite entanglement.

However, not every entangled state is a resource in entanglement distillation. This leads to the notion of bound entanglement: algebraic entanglement which is not distillable. Bound entangled states may be thought of as quantum information black holes. They require entanglement for their preparation, but no pure entanglement can be extracted from them. It was shown that nonpositive partial transposition is a necessary condition for distillability [27]. The first examples of entangled PPT states were provided in [54].

The phenomenon of bound entanglement shows that not all entangled states are equivalent according to the LOCC paradigm. Bound entanglement cannot be a resource in many information theoretical tasks. The area of its application is still not fully recognized. One of the important long-standing questions was if bound entanglement may exhibit nonlocality [25], and it was recently answered in [24].

2. Proof of proposition 1

First, let us recall that the GHZ-diagonal family has a diagonal-antidiagonal form, and the partial transpose with respect to each qubit looks eminently simple here (see Fig. 4 for illustration). To prove the statement of proposition 1, first, we show that the state is PPT for every $1:(n-1)$ cut. A GHZ-diagonal state written in the standard basis contains nonzero elements only on the diagonal and antidiagonal: $\rho_{i,i}=\rho_{2^n-1-i,2^n-1-i}=\frac{\lambda_i^+ +\lambda_i^-}{2}$ and $\rho_{i,2^n-1-i}=\rho_{2^n-1-i,i}=\frac{\lambda_i^+ -\lambda_i^-}{2}$. Partial transposition with respect to the kth-qubit influences only antidiagonal elements (in the standard basis) of the density matrix such that

$$\lambda_i^+ - \lambda_i^- \rightarrow \lambda_j^+ - \lambda_j^-, \tag{A1}$$

where

$$i=\begin{cases}\mathrm{NOT}_{2,3,\ldots,n}(j) & \text{if} \quad k=1,\\ \mathrm{NOT}_k(j) & \text{elsewhere.}\end{cases} \tag{A2}$$

The state after the transposition remains diagonal-antidiagonal, and its eigenvalues are

$$\Lambda_i^{k\pm}=\tfrac{1}{2}[(\lambda_i^+ +\lambda_i^-)\pm(\lambda_j^+ -\lambda_j^-)]. \tag{A3}$$

They are positive when

$$\lambda_i^+ +\lambda_i^- \geqslant |\lambda_j^+ -\lambda_j^-|. \tag{A4}$$

Finally, the state is PPT with respect to every one-qubit partial transpositions when

$$\min_{i\in\Omega_j}(\lambda_i^+ +\lambda_i^-)\geqslant|\lambda_j^+ -\lambda_j^-| \tag{A5}$$

for $\Omega_j=\{\mathrm{NOT}_{2,3,\ldots,n}(j)\}\cup\{\mathrm{NOT}_k(j)|k\in\{1,2,\ldots,n\}\}$, which comes from condition (A2). If the state is PPT for a given $1:(n-1)$ cut, no entanglement can be distilled between these two parties. Since we put $n-1$ parties together in this cut, every collective quantum operation is allowed for this group. It is easy to see that this setup is less restrictive than the unlocking protocol. That means that two-particle entanglement cannot be unlocked for any two particles of the discussed states.

3. Proof of proposition 2

To prove that $\rho_{n,k}$ is BE we have to show that it satisfies (8) for every n (number of qubits) and k (maximal number of ones in a binary representation of indices i associated with nonzero eigenvalues). From condition (A2) we can see that, for a given i, Ω_j contains numbers for which a binary representation has only three possible numbers of ones: $j+1$, $j-1$, $n-j-1$. Let us discuss separately three different possibilities: (a) For $\#1(j)<k$ or $\#1(j)>n-k$, in Ω_j we can have only those i with $\#1(i)\leqslant k$ or $\#1(i)\geqslant n-k$. Therefore, $\min_{i\in\Omega_j}(\lambda_i^+ +\lambda_i^-)=\lambda$ and $|\lambda_j^+ -\lambda_j^-|=\lambda$ and (8) is satisfied. (b) If $\#1(j)=k$ or $\#1(j)=n-k$, then in Ω_k we have i with $\#1(i)\in\{k-1,k+1,n-k-1\}$. In Ω_{n-k} there are i satisfying $\#1(i)\in\{k-1,n-k-1,n-k+1\}$. In both cases $\min_{i\in\Omega_j}(\lambda_i^+ +\lambda_i^-)=\lambda$ and $|\lambda_j^+ -\lambda_j^-|=0$ and (8) is satisfied. (c) If $\#1(j)>k$ or $\#1(j)<n-k$, in Ω_j we can have only those i with $\#1(i)\geqslant k$ or $\#1(i)\leqslant n-k$, with at least one i for which these inequalities are sharp. So $\min_{i\in\Omega_j}(\lambda_i^+ +\lambda_i^-)=0$ and $|\lambda_j^+ -\lambda_j^-|=0$, which also satisfy (8). With the above we have checked all the transpositions for any given n,k and have seen that, indeed, (8) is always satisfied, which proves that $\rho_{n,k}$ states are nonunlockable BE.

4. Proof of proposition 3

Here we derive (13) for the quantum Fisher information in the form (12): First, we bound the QFI from below:

$$F_Q^{n,k} = \frac{\sum_{j=0}^{k-1}(n-2j)^2\binom{n}{j}}{\sum_{j=0}^{k}\binom{n}{j}} \geqslant (n-2k)^2\frac{\sum_{j=0}^{k-1}\binom{n}{j}}{\sum_{j=0}^{k}\binom{n}{j}}. \tag{A6}$$

Consider the last factor $S_{n,k} := \frac{\sum_{j=0}^{k-1}\binom{n}{j}}{\sum_{j=0}^{k}\binom{n}{j}}$. One can estimate its inverse $S_{n,k}^{-1}$ as follows:

$$S_{n,k}^{-1} = \frac{\sum_{j=0}^{k}\binom{n}{j}}{\sum_{j=0}^{k-1}\binom{n}{j}} = \frac{\sum_{j=0}^{k-1}\binom{n}{j}+\binom{n}{k}}{\sum_{j=0}^{k-1}\binom{n}{j}} = 1+\frac{\binom{n}{k}}{\sum_{j=0}^{k-1}\binom{n}{j}} \leqslant 1+\frac{\binom{n}{k}}{\binom{n}{k-1}} = \frac{n+1}{k}, \tag{A7}$$

and hence, the original factor satisfies $S_{n,k} \geqslant \frac{k}{n+1}$, from which the lower bound (13) immediately follows. The limit (14) immediately results from (13).

5. Nonlinear correlation entanglement witness and Bell inequalities

It has been shown [35] that given any n-qubit state, one can use its correlation tensor $T_{k_1\cdots k_n} = \mathrm{Tr}[(\sigma_{k_1}\otimes\cdots\otimes\sigma_{k_n})\rho]$, where $\sigma_0 = \mathbb{I}$ and indices 1,2,3 refer to Pauli operators $\{\sigma_X,\sigma_Y,\sigma_Z\}$, to build a nonlinear entanglement test of the form

$$\|T\|_{HS}^2 = \sum_{k_1,\ldots,k_n=1}^{3} T_{k_1,\ldots,k_n}^2 \leqslant 1. \tag{A8}$$

Remarkably, the above can be used as a sufficient condition for checking a wide class of Bell inequalities. Indeed, the *necessary and sufficient condition* for the $2^{n-1}\times 2^{n-1}\times 2^{n-2}\times 2^{n-3}\times\cdots\times 2$ setting correlation Bell inequalities [48,49] (which are a generalization of the class [55–57] including the Mermin-Klyshko inequality [58,59]) can be written as

$$\mathcal{C}^{(n)}(\rho) = \max \sum_{k_1,\ldots,k_n=1}^{2} T_{k_1,\ldots,k_n}^2 \leqslant 1, \tag{A9}$$

where the maximum is taken over all possible sequences of pairs of orthogonal vectors $\{\hat{e}_{k_i},k_i = 1,2\}_{i=1}^n$. Formula (A9) guarantees that there is no Bell inequality with dichotomic measurements and $2^{n-1}\times 2^{n-1}\times 2^{n-2}\times 2^{n-3}\times\cdots\times 2$ settings which is violated by the state. Clearly, one has $\mathcal{C}^{(n)}(\rho) \leqslant ||T||_{HS}^2$, which reflects the dependence mentioned above. We have found the analytical formulas for the correlation tensor elements $\{T_{k_1\ldots k_n}\}$ (they are complicated and will be analyzed elsewhere) and calculated the upper bound $||T||_{HS}^2$ from (A8). It happens that for some specific states $\rho_{n,k}$ it is smaller than 1, although quantum Fisher information still detects entanglement (see the main text).

6. Sub-shot-noise limit with much weaker bound entanglement

The states

$$\rho_{n,k,m} = \lambda' P_{n,k}^{+} + \frac{\lambda'}{2}\sum_{j=k}^{m}(Q_{n,j}^{+}+Q_{n,j}^{-}), \tag{A10}$$

where $\lambda' = [\sum_{j=0}^{k+m}\binom{n}{j}]^{-1}$, satisfy the PPT test for any cut $j : n-j$ with $j \leqslant m+1$. The corresponding Fisher information is bounded by

$$F_Q^{n,k,m} \geqslant (n-2k)^2\frac{k(k+1)\cdots(k+m)}{m(n-k)(n-k-1)\cdots[n-(k+m)]}. \tag{A11}$$

Putting linear scaling of $k(n) = cn$ and sublinear scaling of $m(n) = n^{1-\varepsilon}$ (which makes the corresponding entanglement much weaker than that of previous states where only one-qubit cuts obey the PPT test) in the above leads to the sub-shot-noise behavior of the Fisher information $F_Q^{n,k(n),m(n)} \sim n^{1+\varepsilon}$.

[1] V. Giovannetti, S. Lloyd, and L. Maccone, Advances in quantum metrology, Nat. Photonics **5**, 222 (2011).
[2] J. J. Bollinger, W. M. Itano, D. J. Wineland, and D. J. Heinzen, Optimal frequency measurements with maximally correlated states, Phys. Rev. A **54**, R4649 (1996).
[3] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac, Improvement of Frequency Standards with Quantum Entanglement, Phys. Rev. Lett. **79**, 3865 (1997).
[4] B. Yurke, Input States for Enhancement of Fermion Interferometer Sensitivity, Phys. Rev. Lett. **56**, 1515 (1986).
[5] C. Caves, Quantum-mechanical noise in an interferometer, Phys. Rev. D **23**, 1693 (1981).
[6] F. Benatti, S. Alipour, and A. T. Rzekhani, Dissipative quantum metrology in manybody systems of identical particles, New J. Phys. **16**, 015023 (2014).
[7] V. Bužek, R. Derka, and S. Massar, Optimal Quantum Clocks, Phys. Rev. Lett. **82**, 2207 (1999).
[8] The LIGO Scientific Collaboration, A gravitational wave observatory operating beyond the quantum shot-noise limit, Nat. Phys. **7**, 962 (2011).
[9] M. G. A. Paris, Quantum estimation for quantum technology, Int. J. Quantum Inf. **07**, 125 (2009).
[10] H. P. Yuen and M. Lax, Multiple-parameter quantum estimation and measurement of nonselfadjoint observables, IEEE Trans. Inf. Theory **19**, 740 (1973).
[11] C. W. Helstrom and R. S. Kennedy, Noncommuting observables in quantum detection and estimation theory, IEEE Trans. Inf. Theory **20**, 16 (1974).
[12] S. Braunstein and C. Caves, Statistical distance and the geometry of quantum states, Phys. Rev. Lett. **72**, 3439 (1994).
[13] S. Braunstein, C. Caves, and G. Milburn, Generalized Uncertainty Relations: Theory, Examples, and Lorentz Invariance, Ann. Phys. (N.Y.) **247**, 135 (1996).

[14] M. Zwierz, C. A. Pérez-Delgado, and P. Kok, General Optimality of the Heisenberg Limit for Quantum Metrology, Phys. Rev. Lett. **105**, 180402 (2010).
[15] M. J. W. Hall, D. W. Berry, M. Zwierz, and H. M. Wiseman, Universality of the Heisenberg limit for estimates of random phase shifts, Phys. Rev. A **85**, 041802(R) (2012).
[16] B. M. Escher, R. L. de Matos Filho, and L. Davidovich, General framework for estimating the ultimate precision limit in noisy quantum-enhanced metrology, Nat. Phys. **7**, 406 (2011).
[17] R. Demkowicz-Dobrzanski, J. Kolodynski, and M. Guta, The elusive Heisenberg limit in quantum-enhanced metrology, Nat. Commun. **3**, 1063 (2012).
[18] M. Jarzyna and R. Demkowicz-Dobrzanski, Matrix Product States for Quantum Metrology, Phys. Rev. Lett. **110**, 240405 (2013).
[19] G. Arrad, Y. Vinkler, D. Aharonov, and A. Retzker, Increasing sensing resolution with error correction, Phys. Rev. Lett. **112**, 150801 (2014).
[20] E. J. Kessler, I. Lovchinsky, A. O. Sushkov, and M. D. Lukin, Quantum Error Correction for Metrology, Phys. Rev. Lett. **112**, 150802 (2014).
[21] W. Dür, M. Skotiniotis, F. Fröwis, and B. Kraus, Improved Quantum Metrology Using Error Correction, Phys. Rev. Lett. **112**, 080801 (2014).
[22] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).
[23] R. Augusiak and P. Horodecki, Bound entanglement maximally violating Bell inequalities: Quantum entanglement is not equivalent to quantum security, Phys. Rev. A **74**, 010305 (2006).
[24] T. Vértesi and N. Brunner, Disproving the Peres conjecture: Bell nonlocality from bipartite bound entanglement, Nat. Commun. **5**, 5297 (2014).
[25] A. Peres, All the Bell inequalities, Found. Phys. **29**, 589 (1999).
[26] G. Tóth, Multipartite entanglement and high-precision metrology, Phys. Rev. A **85**, 022322 (2012).
[27] M. Horodecki, P. Horodecki, and R. Horodecki, Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature? Phys. Rev. Lett. **80**, 5239 (1998).
[28] P. Horodecki and R. Horodecki, Distillation and bound entanglement, Quantum Inf. Comput. **1**, 45 (2001).
[29] A. Peres, Separability Criterion for Density Matrices, Phys. Rev. Lett. **77**, 1413 (1996).
[30] B. M. Terhal, Is entanglement monogamous? IBM J. Res. Dev. **48**, 71 (2004).
[31] J. A. Smolin, Four-party unlockable bound entangled state, Phys. Rev. A **63**, 032306 (2001).
[32] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Locking Entanglement with a Single Qubit, Phys. Rev. Lett. **94**, 200501 (2005).
[33] S. Bauml, M. Christ, K. Horodecki, and A. Winter, Limitations on quantum key repeaters, Nat. Commun. **6**, 6908 (2015).
[34] P. Hyllus, W. Laskowski, R. Krischek, C. Schwemmer, W. Wieczorek, H. Weinfurter, L. Pezze, and A. Smerzi, Fisher information and multiparticle entanglement, Phys. Rev. A **85**, 022321 (2012).
[35] P. Badziag, C. Brukner, W. Laskowski, T. Paterek, and M. Zukowski, Experimentally Friendly Geometrical Criteria for Entanglement, Phys. Rev. Lett. **100**, 140403 (2008).
[36] W. Dür, J. I. Cirac, and R. Tarrach, Separability and Distillability of Multiparticle Quantum Systems, Phys. Rev. Lett. **83**, 3562 (1999).
[37] W. Dür and J. I. Cirac, Activating bound entanglement in multiparticle systems, Phys. Rev. A **62**, 022302 (2000).
[38] W. Dür and J. I. Cirac, Classification of multiqubit mixed states: Separability and distillability properties, Phys. Rev. A **61**, 042314 (2000).
[39] H. Cramér, *Mathematical Methods of Statistics* (Princeton University Press, Princeton, NJ, 1946).
[40] S. Kay, *Fundamentals of Statistical Signals Processing: Estimation Theory* (Prentice Hall, New Jersey, 1993).
[41] R. F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, Phys. Rev. A **40**, 4277 (1989).
[42] J. Gruca, W. Laskowski, M. Żukowski, N. Kiesel, W. Wieczorek, C. Schmid, and H. Weinfurter, Nonclassicality thresholds for multiqubit states: Numerical analysis, Phys. Rev. A **82**, 012118 (2010).
[43] F. Hirsch, M. T. Quintino, J. Bowles, and N. Brunner, Genuine Hidden Quantum Nonlocality, Phys. Rev. Lett. **111**, 160402 (2013).
[44] M. Zukowski, R. Horodecki, M. Horodecki, and P. Horodecki, Generalized quantum measurements and local realism, Phys. Rev. A **58**, 1694 (1998).
[45] S. Teufel, K. Brendl, W. Dürr, S. Goldstein, and N. Zanghi, Locality and causality in hidden-variables models of quantum theory, Phys. Rev. A **56**, 1217 (1997).
[46] S. Popescu, Bell's Inequalities and Density Matrices: Revealing "Hidden" Nonlocality, Phys. Rev. Lett. **74**, 2619 (1995).
[47] N. Gisin, Phys. Lett. A **210**, 151 (1996).
[48] W. Laskowski, T. Paterek, M. Zukowski, and C. Brukner, Tight Multipartite Bell's Inequalities Involving Many Measurement Settings, Phys. Rev. Lett. **93**, 200401 (2004).
[49] T. Paterek, W. Laskowski, and M. Zukowski, On series of multiqubit Bell's inequalities, Mod. Phys. Lett. **21**, 111 (2006).
[50] P. Horodecki, M. Horodecki, and R. Horodecki, Binding entanglement channels, J. Mod. Opt. **47**, 347 (2000).
[51] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Unextendible Product Bases, Uncompletable Product Bases and Bound Entanglement, Commun. Math. Phys. **238**, 379 (2003).
[52] R. Jozsa and N. Linden, On the role of entanglement in quantum-computational speed-up, Proc. R. Soc. A **459**, 1364 (2011).
[53] C. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters, Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, Phys. Rev. Lett. **76**, 722 (1996).
[54] M. Horodecki, P. Horodecki, and R. Horodecki, Inseparable Two Spin 1/2 Density Matrices Can Be Distilled to a Singlet Form, Phys. Rev. Lett. **78**, 574 (1997).
[55] G. Toth, C. Knapp, O. Guehne, and H. J. Briegel, Optimal Spin Squeezing Inequalities Detect Bound Entanglement in Spin Models, Phys. Rev. Lett. **99**, 250405 (2007).

[56] C. Brukner and M. Zukowski, Bell's Theorem for General N-Qubit States, Phys. Rev. Lett. **88**, 210401 (2002).

[57] R. Werner and M. W. Wolf, All-multipartite Bell-correlation inequalities for two dichotomic observables per site, Phys. Rev. A **64**, 032112 (2001).

[58] N. D. Mermin, Extreme quantum entanglement in a superposition of macroscopically distinct states, Phys. Rev. Lett. **65**, 1838 (1990).

[59] A. V. Belinskii and D. N. Klyshko, Interference of light and Bell's theorem, Phys. Usp. **36**, 653 (1993).