Arktische Muster im Visier

Mit einer Computersimulation lässt sich die Vielfalt faszinierender Bodenstrukturen in polaren Gegenden erklären.

In den vegetationslosen arktischen Zonen, die meist von Eis bedeckt sind, zeigen sich im Hochsommer, wenn der Boden freigelegt ist, oftmals herrliche Muster auf der Skala von Metern, in denen Steinchen, wie von Kinderhand aufgetürmt, schlierenförmige, hexagonale oder einfach runde Häufchen bilden [1]. Diese Formen waren mit Sicherheit schon den ersten Eskimos oder auch den Wikingern bekannt.

Obwohl über die Jahrhunderte hinweg Polarforscher und Geologen diese Strukturen beschrieben und über ihren Ursprung nachgedacht haben, ist ihre Entstehung bis heute ein Rätsel. Mindestens fünf sehr verschiedene Erklärungen wurden bereits veröffentlicht, doch keine deckt sich zufriedenstellend mit den Beobachtungen. Anfang dieses Jahres veröffentlichten Mark A. Kessler und Brad T. Werner von der Universität von Kalifornien in San Diego ein Modell zur Entstehung der Steinhäufchen [2], das durch seine Originalität und beeindruckende Übereinstimmung mit den beobachteten Mustern hervorsticht.

Während unserem Auge die einsame Landschaft der Arktis völlig regungslos erscheint, ist auf der Zeitskala von Monaten durch das periodische Frieren und Auftauen („Gefrierzyklen“) des Bodens der arktische Untergrund stets in Bewegung. In der Stille kann der aufmerksame Zuhörer sogar bisweilen das Knistern der rutschenden Steine hören.

Ausgehend von der periodischen Deformation des (teils freien und teils mit Steinen bedeckten) Bodens identifizierten die Autoren aus Kalifornien zwei Mechanismen, um die Strukturen zu erklären:

▶ Steigt die Frostgrenze im Boden nach oben, werden (die relativ trockenen) Steine aus den gefrorenen (wassergesättigten) Sandschichten in die weicheren, aufgetauten Bereiche gedrückt. Eine Neigung des Bodens führt zusätzlich dazu, dass sich die Steine auch seitlich bewegen. Über mehrere Gefrierzyklen hinweg entmischen sich so die gröberen Steine vom feinkörnigen Sand und sammeln sich in den Senken an.

▶ Die entstandenen Steinansammlungen werden dann in die Länge gezogen, weil breitere Bereiche durch das laterale Ausfrieren nahe der Stein-Sand-Grenze stärker zusammengedrückt werden. Außerdem fallen Steine von erhöhten Bereichen hinunter, so dass sich Höhenunterschiede ausgleichen.

Diese beiden Bewegungsformen beschreiben die Autoren mit Hilfe von Feldgleichungen für die Bodenform und die lokale Steinkonzentration. Der erste Mechanismus wird implementiert durch einen Entmischungstransport proportional zur Steigung des Bodens. Die Streckung der Steinhaufen durch das laterale Zusammendrücken wird mittels einer anisotropen Diffusion modelliert, wobei die Anisotropie aus der vorliegenden Form des Steinhaufens bestimmt wird. Dieses Gleichungssystem wird numerisch für verschiedene Parameter, d. h. Diffusionskonstanten und Transportkoeffizienten, gelöst. Eine geeignete physikalische Interpretation dieser Konstanten erlaubt es, die aus der Rechnung entspringenden Muster mit den beobachteten zu vergleichen.

Die Autoren konnten so nicht nur die Reichhaltigkeit der natürlichen Formen reproduzieren, sondern stellten sogar ein morphologisches Phasendiagramm auf als Funktion der Steinmenge und der Bodenform. Dominiert eher der Mechanismus des Entmischens von Sand und Stein, so entstehen Kreise, Labyrinthe oder Inseln, während sich bei vorherrschender Streckung der Steinansammlungen eher polygonale Netzwerke bilden, die bei anwachsender Bodensteigung in Streifen übergehen.

Höhepunkt ist ein quantitativer Vergleich zwischen Beobachtung und Simulation bei den hexagonalen Strukturen. In Bezug auf die Verteilung der Winkel und der Flächen der Polygone stimmen Modell und Wirklichkeit überraschend gut überein. Dieses Modell scheint somit zur Zeit die beste Erklärung für die Entstehung der arktischen Muster zu bieten. Es ist auch von seinem Grundkonzept ziemlich anders als die bisherigen Erklärungsversuche, da es absieht von den einzelnen Kornbewegungen und den klassischen binären Entmischungseffekten und einen kontinuumsmechanischen Ansatz vorschlägt, in dem die Lage der Steine nicht diskretisiert wird.

Die Arbeit von Kessler und Werner zeigt wieder einmal eindrucksvoll, wie moderne Ideen der Strukturbildung und seriöse Computersimulation in zunehmendem Maße die Geomorphologie bestimmen. Während vor wenigen Jahren viele wohlbekannte Muster der Geologie in der Fachliteratur nur qualitativ beschrieben und mit wohlklingenden Namen klassifiziert wurden, waren sie erstaunlicherweise faktisch unerklärt. Beispiele sind die Dünen in der Wüste [3], Gesteinsschichungen (Strata), die durch

Geordnete Kreismuster in Kvadehuksletta auf Spitzbergen sind nur ein Beispiel für die faszinierenden Bodenstrukturen, welche selbstorganisiert entstehen. Die Kreise haben etwa einen Durchmesser von einem Meter. (aus [2])

Erdrutsche entstehen [4], Steinformationen auf dem Meeresgrund oder die Fragmentierung des trocknenden Bodens eines Schlammsees. Wie für den vorliegenden Fall der arktischen Bodenmuster haben die letzten 10 bis 15 Jahre im wesentlichen durch den Eingriff statistischer Physiker eine Revolution in der Erkenntnisgewinnung erlebt und die klassischen Geologen und Geographen immer mehr zu einer mathematischen Modellierung geführt. Doch im Alleingang kann die Physik die beobachteten Phänomene nicht erklären, denn oftmals, und die arktischen Muster sind ein gutes Beispiel dafür, lassen sich die Phänomene im Labor experimentell nicht reproduzieren, da entweder die Zeitskalen oder die räumlichen Ausdehnungen oder beides Laborexperimente unmöglich machen. Da jedoch traditionellerweise Geowissenschaftler in ihren Expeditionen meist jene quantitativen Größen, die dem physikalischen Modell zugute kommen, nicht bestimmen, kommt es auch immer häufiger vor, dass Physiker selbst in die Wüste oder in die Arktis fahren, um jene Messungen durchzuführen, die sie

brauchen, um die Theorien quantitativ verifizieren zu können.

HANS J. HERRMANN

Prof. Dr. Hans Herrmann, Institut für Computeranwendungen der Universität Stuttgart, Pfaffenwaldring 27, 70569 Stuttgart

[1] *A.L. Washburn*, Geol. Soc. Am. Bull. **67**, 823 (1956)
[2] *M.A. Kessler* und *B.T. Werner*, Science **299**, 380 (2003)
[3] *K. Kroy, G. Sauermann, H.J. Herrmann,* Phys. Rev. Lett. **88**, 054301 (2002)
[4] *H.A. Makse, S. Havlin, P.R. King* and *H.E. Stanley*, Nature **386**, 379 (1997)

Mehr Sicherheit durch Quantenschlüssel

Das Bestreben der Menschen, Botschaften möglichst geheim verschicken zu können, ist so alt wie die Menschheit selbst [1]. Die kryptografischen Methoden wurden mit der Zeit immer ausgefeilter und haben nicht nur in sicherheitstechnischen Bereichen, sondern auch im Geschäftsleben eine besonders hohe, nicht zu unterschätzende Bedeutung. Bereits seit einigen Jahren sind kryptografische Verfahren in der Diskussion, die auf den speziellen Eigenschaften von Quantensystemen beruhen, etwa von nicht-orthogonalen Polarisationszuständen schwacher Lichtpulse oder von Paaren einzelner Photonen, die miteinander korreliert (verschränkt) sind.[1)] Nun ist es Frédérik Grosshans et al. gelungen zu zeigen, dass auch intensive Lichtfelder eine Quantenkryptografie ermöglichen, die zudem schneller und effizienter ist [2].

1) vgl. *H. Briegel,* Phys. Blätter, Juni 2000, S. 12 *W. Tittel, J. Brendel, N. Gisin, G. Ribordy* und *H. Zbinden*, Phys. Blätter, Juni 1999, S. 25

Bei der einzigen gemeinhin als absolut sicher geltenden Methode muss der Datensatz mit einem Zufallsdatensatz gleicher Länge verschlüsselt werden. Dieser Schlüssel darf aber nur einmal verwendet werden (*one time pad*). Das Problem bei diesem Verfahren ist der Austausch des geheimen Schlüssels zwischen Empfänger und Sender. Wenn die Sicherheitsstufe es erlaubt, wird heute oft das vergleichsweise einfache, aber um so wirksamere Verfahren des öffentlichen Schlüssels (*public key*) verwendet. Es beruht darauf, dass es Rechenaufgaben gibt, die in der einen Richtung vergleichsweise einfach und damit schnell durchzuführen sind, in der anderen aber unvergleichlich viel schwieriger. Diese Komplexität der Berechnung wird danach bewertet, ob die benötigte Rechenzeit polynomial oder exponentiell von der Größe der Zahl im Eingangsregister abhängt. Ein Beispiel ist die Multiplikation zweier ganzer Zahlen und deren Umkehrung, die Faktorisierung. Für die schwierige Richtung sind zwar keine Algorithmen bekannt, die auf herkömmlichen Rechnern effizient, d. h. in polynomialer Zeit ablaufen, aber es gibt bislang auch keinen mathematischen Beweis dafür, dass solche Algorithmen nicht existieren. Ein gewisses Unbehagen bleibt. Hinzu kommt, dass ein Quanten-Computer, der die besonderen Eigenschaften quantenmechanischer Systeme ausnutzt, die bekannten „schwierigen" Probleme effizient lösen kann. Ein solches Quanten-Rechenwerk für Spezialaufgaben gibt es zwar noch nicht und wird es wohl auch in absehbarer Zeit nicht geben, aber aus all den genannten Gründen steht hinter der heute kommerziell erwerbbaren Sicherheit ein kleines Fragezeichen.

Die Quantentheorie stellt der Kryptografie mit dem Quanten-Rechenwerk ein Bein; sie bietet aber auch einen Ausweg. Ein einzelnes unbekanntes Quantensystem, dessen mögliche Zustände nicht orthogonal sind, lässt sich durch eine Messung nicht vollständig charakterisieren. Damit Hand in Hand geht die Unmöglichkeit, ein unbekanntes Quantensystem exakt zu klonen bzw. davon eine Kopie anzufertigen. Das kanonische Beispiel hierfür ist ein einzelnes Photon, das in einer Überlagerung zweier unterschiedlicher Zustände vorliegt. Dies können z. B. zwei orthogonale lineare Polarisationszustände sein. S. Wiesner hatte die Idee, die besonderen Eigenschaften derartiger einfachster Quantenobjekte für die absolut geheime Verteilung kryptografischer Schüssel auszunutzen. Ein unerwünschter Mithörer kann zwar versuchen, die Botschaft abzufangen, aber er wird das Quantenobjekt, also z. B. das Photon, durch seine Messung so verändern, dass er nicht unentdeckt bleiben kann. Außerdem gibt es Verfahren in der (klassischen) Kryptografie, die einen geheimen Schlüssel aus den Korrelationen zwischen Sender und Empfänger „herausdestillieren" können. Dabei werden zunächst Fehler korrigiert, und dann mögliche Korrelationen mit einem Mithörer mittels sog. *privacy amplification* abgebaut [3]. Eine notwendige Voraussetzung dafür ist, dass die Korrelationen zwischen Empfänger und Sender noch quantenmechanische Züge tragen. Letztes Jahr erst ist es dem Team um Harald Weinfurter gelungen, von der Zugspitze aus einen geheimen Schlüssel zu einem 21 km entfernten Empfänger zu übertragen [4]. Und gerade erschien die Beschreibung eines neuen Experiments, das wesentlich für die Weiterentwicklung der Quanten-Schlüsselverteilung ist: die Teleportation eines Photons über 2 km [5]. Dabei handelt es sich um die Übertragung der Quantenstruktur von einem Photon der Wellenlänge 1,3 μm auf ein anderes der Wellenlänge 1,55 μm. Die Teleportation könnte es ermöglichen, künftig kryptografische Schlüssel über noch größere Distanzen zu verteilen.

All diese Experimente benutzen (näherungsweise) einzelne Lichtquanten. Das stellt besondere Anforderungen an die Lichtquellen und begrenzt auch die Übertragungsrate. Vor kurzem wurde jedoch theoretisch gezeigt, dass Quanten-Schlüsselverteilung auch mit intensiven Lichtfeldern möglich ist, die viele Photonen pro Messzeitintervall enthalten. Solche Felder werden am besten durch kontinuierliche Quantenvariablen beschrieben, z. B. Amplitude und Phase. Es stellte sich heraus, dass sogar kohärente Laserfelder geeignet sind, die keine nichtklassischen Eigenschaften besitzen. Aber noch vor Jahresfrist wurde vermutet, dass die Schlüsselverteilung mit kohärenten Zustände nur möglich sei, wenn die Verluste auf der Übertragungsstrecke kleiner als 50 % sind. Seitdem sind zwei unterschiedliche Methoden zur Überwindung auch dieser Grenze gefunden worden, die beide das klassische Protokoll der *privacy amplification* benutzen, um einen geheimen Schlüssel aus geteilten Korrelationen herauszudestillieren. Dabei darf der Mithörer nach einer geeigneten Fehlerkorrektur keine vollständige Information über die korrigierten Korrelationen besitzen. Die Methoden unterscheiden sich darin, wie dieser Informationsvorsprung gegenüber dem Mithörer entsteht. Dieser Unterschied bezieht sich auf verschiedenen Fehlerkorrekturverfahren. In manchen Verfahren werden die Positionen von Fehlern durch interaktive Protokolle bekannt (bidirektional). Dies ist nicht der Fall bei der starren unidirektionalen Methode, die dafür den Nachteil hat, nicht effizient zu sein.

Die wesentliche Größe ist die gemeinsame Information, die zwei