The Dual BKR Inequality and Rudich's Conjecture

JEFF KAHN[*]
Mathematics Dept.
Rutgers University
Piscataway, NJ, USA
jkahn@math.rutgers.edu

MICHAEL SAKS[†]
Mathematics Dept.
Rutgers University
Piscataway, NJ, USA
saks@math.rutgers.edu

CLIFFORD SMYTH
Mathematics Dept.
University of North Carolina Greensboro
Greensboro, NC USA
cdsmyth@uncg.edu

October 30, 2010

Abstract

Let $\mathcal{T}$ be a set of terms over an arbitrary (but finite) number of Boolean variables. Let $U(\mathcal{T})$ be the set of truth assignments that satisfy exactly one term in $\mathcal{T}$. Motivated by questions in computational complexity, Rudich conjectured that there exist $\epsilon, \delta > 0$ such that if $\mathcal{T}$ is any set of terms for which $U(\mathcal{T})$ contains at least a $(1-\epsilon)$-fraction of all truth assignments, then there exists a term $t \in \mathcal{T}$ such that at least a δ-fraction of assignments satisfy some term of $\mathcal{T}$ sharing a variable with t [7].

We prove a stronger version: for any independent assignment of the variables (not necessarily the uniform one), if the measure of $U(\mathcal{T})$

[*] Supported in part by NSF grants DMS0200856 and DMS0701175.
[†] Supported in part by NSF Grant CCR-9700239 and CCR-0832787.

is at least $1 - \epsilon$, there exists a $t \in \mathcal{T}$ so that the measure of the set of assignments satisfying either t or some term incompatible with t (i.e. having no satisfying assignments in common with t) is at least $\delta = 1 - \epsilon - \frac{4\epsilon}{1-\epsilon}$. (A key part of the proof is a correlation-like inequality on events in a finite product probability space that is in some sense dual to Reimer's inequality [10] a.k.a. the BKR inequality [4] or the van den Berg–Kesten conjecture [2]).

1 Introduction

Let $\Omega_1, \ldots, \Omega_n$ be fixed finite sets, each of size at least 2, and let $\Omega = \Omega_1 \times \cdots \times \Omega_n$. A *partial selection function* for $\Omega_1, \ldots, \Omega_n$ is a function f such that (i) its domain, $\mathrm{dom}(f)$, is a subset of $[n] := \{1, \ldots, n\}$, and (ii) for each $i \in \mathrm{dom}(f)$, $f(i) \in \Omega_i$. The *cylinder* of f is the set

$$C(f) := \{x \in \Omega : x_i = f(i), \forall i \in \mathrm{dom}(f)\}.$$

We tend to think of f and $C(f)$ as interchangeable, as different partial selection functions give different cylinders.

Let f and g be partial selection functions. We say that an index i is *fixed* in f if $i \in \mathrm{dom}(f)$ and *free* (in f) otherwise. We say f and g are *dependent* if they share a fixed variable, i.e. if $\mathrm{dom}(f) \cap \mathrm{dom}(g) \neq \emptyset$, and denote this by $f \sim g$ (or $C(f) \sim C(g)$). We say that f and g are *incompatible*, denoted $f \sim' g$ (or $C(f) \sim' C(g)$) if there exists $i \in \mathrm{dom}(f) \cap \mathrm{dom}(g)$ such that $f(i) \neq g(i)$. Note that $f \sim' g$ implies $f \sim g$.

Throughout this paper, $\mathcal{F}$ denotes a set of cylinders of Ω. For $F \in \mathcal{F}$, we define

$$N(F) = N_{\mathcal{F}}(F) := \{G \in \mathcal{F} : G \neq F, G \sim F\},$$

and

$$N[F] = N_{\mathcal{F}}[F] := N(F) \cup \{F\}.$$

These are respectively, the *open neighborhood* and *closed neighborhood* of F in the graph $(\mathcal{F}, \sim)$. Similarly, we define $N'(F) = N'_{\mathcal{F}}(F) := \{G \in \mathcal{F} : G \sim' F\}$, and $N'[F] = N'_{\mathcal{F}}[F] := N'(F) \cup \{F\}$, the *open neighborhood* and *closed neighborhood* of F in the graph $(\mathcal{F}, \sim')$.

We define $U(\mathcal{F})$ to be the set of elements of Ω *uniquely covered* by $\mathcal{F}$, i.e., those that belong to precisely one member of $\mathcal{F}$. Motivated by some questions in computational complexity, Rudich [6] investigated families of cylinders $\mathcal{F}$ of $\{0,1\}^n$ for which a large fraction of elements of Ω are uniquely covered. He conjectured that in any such family, there must be a cylinder whose closed neighborhood in $(\mathcal{F}, \sim)$ covers a non-trivial fraction of $\{0,1\}^n$.

Conjecture 1.1 (Rudich's Conjecture)
There exist $\epsilon, \delta > 0$ such that for all $n \geq 1$ and for any set of cylinders $\mathcal{F}$ of $\{0,1\}^n$, if $|U(\mathcal{F})| \geq (1-\epsilon)2^n$, there is a cylinder $F \in \mathcal{F}$ for which

$$|\bigcup_{G \in N[F]} G| \geq \delta 2^n.$$

Remark 1.1: If $\epsilon = 0$, $|U(\mathcal{F})| = 2^n$ and $\mathcal{F}$ is a partition. Thus $(\mathcal{F}, \sim)$ is the complete graph. We may then take $\delta = 1$: for every $F \in \mathcal{F}$, $N[F] = \mathcal{F}$ and $|\bigcup\{G : G \in N[F]\}| = 2^n$.

Remark 1.2: Rudich's conjecture fails for $\epsilon \geq 1 - 1/e$ (that is, for such ϵ, there is no $\delta > 0$ for which the conclusion of the conjecture holds). To see this, given $\delta > 0$, let $k > \log_2(1/\delta)$ be a positive integer and $n = k2^k$. Partition $[n]$ into 2^k blocks of size k and let $\mathcal{F}$ consist of 2^k cylinders of $\{0,1\}^n$, where the i^{th} cylinder has all indices in block i fixed to 1 and all other indices free. Then $|U(\mathcal{F})| = ((1-2^{-k})^{2^k-1})2^n > e^{-1}2^n$ (since $(1-1/t)^{t-1} > 1/e$ for all t). But $(\mathcal{F}, \sim)$ has no edges, so for any $F \in \mathcal{F}$, $|\bigcup\{G : G \in N[F]\}| = |F| = 2^{n-k} < \delta 2^n$.

Remark 1.3: The original statement of Rudich's conjecture. Rudich formulated Conjecture 1.1 as a statement about sets of boolean terms rather than cylinders. Let $V = \{x_1, \ldots, x_n\}$ be a set of *boolean variables*, i.e. each x_i takes on values from the set $\{True, False\}$. There is an obvious correspondence between $\{0,1\}^n$ and the set of all truth assignments to the variables in V. A *literal* is a boolean variable or the logical negation of a boolean variable and a *boolean term* is a conjunction of literals, i.e. an expression of the form $l_1 \wedge l_2 \wedge \cdots \wedge l_t$ where each l_i is a literal and no l_i is the negation of another l_j. The set of truth assignments that satisfy t is a cylinder in $\{0,1\}^n$. Conjecture 1.1 is thus a rephrasing of Rudich's original conjecture: there exist $\epsilon, \delta > 0$ such that for any set of terms, $\mathcal{T}$, in any number of variables, if the fraction of truth assignments that satisfy exactly one term in $\mathcal{T}$ is at least $1-\epsilon$, then there is a term $t \in \mathcal{T}$ such that at least a δ fraction of assignments satisfy a term that shares a variable with t.

Our main result, Theorem 1.2 below, is a strengthening of Rudich's Conjecture. For each $i \in [n]$, let μ_i be a probability measure on the finite set Ω_i and let $\mu = \mu_1 \times \cdots \times \mu_n$ be the corresponding product measure on Ω. We say (Ω, μ) is a *finite product probability space.*

Recalling that $U(\mathcal{F})$ is the set of elements covered by exactly one member of $\mathcal{F}$, we have the natural partition $U(\mathcal{F}) = \bigcup_{F \in \mathcal{F}} F'$, where (for $F \in \mathcal{F}$)

$$F' = F'_{\mathcal{F}} := F \setminus \bigcup \{G \in \mathcal{F} : G \neq F\}. \tag{1}$$

For $\mathcal{G} \subseteq \mathcal{F}$, we set

$$U_{\mathcal{F}}(\mathcal{G}) := \bigcup_{F \in \mathcal{G}} F'_{\mathcal{F}};$$

so in particular $U_{\mathcal{F}}(\mathcal{F}) = U(\mathcal{F})$.

Theorem 1.2 *Let $\mathcal{F}$ be a family of cylinders in a finite product probability space (Ω, μ). Let $\delta(\epsilon) = 1 - \epsilon - \frac{4\epsilon}{1-\epsilon}$. If $\mu(U(\mathcal{F})) \geq 1 - \epsilon$ then there is an $F \in \mathcal{F}$ such that*

$$\mu\left(\ U_{\mathcal{F}}\left(N'_{\mathcal{F}}[F]\right)\ \right) \geq \delta(\epsilon).$$

Note that $\delta(\epsilon) > 0$ for all $0 < \epsilon < 3 - 2\sqrt{2}$.

Note that the case of Theorem 1.2 in which μ is uniform measure on $\Omega = \{0,1\}^n$ contains Conjecture 1.1, since $\bigcup\{G : G \in N[F]\} \supseteq U_{\mathcal{F}}(N[F]) \supseteq U_{\mathcal{F}}(N'[F])$.

To prove Theorem 1.2, we first prove Theorem 1.4 below, an inequality that is in some sense dual to a celebrated inequality of Reimer. Note that for partial selection functions f and g, $f \not\sim g$ means they have disjoint domains while $f \not\sim' g$ means they agree on any common point of their domains.

Let $A, B \subseteq \Omega$ and $x, y \in \Omega$. We say

$x \in A$ and $y \in B$ *hold disjointly* if $\exists f \not\sim g$, $x \in C(f) \subseteq A$, $y \in C(g) \subseteq B$

and

$x \in A$ and $y \in B$ *hold compatibly* if $\exists f \not\sim' g$, $x \in C(f) \subseteq A$, $y \in C(g) \subseteq B$.

We define

$$\begin{aligned}
A \cap^d B &= \{x \in \Omega : x \in A \text{ and } x \in B \text{ hold disjointly}\}, \\
A \cap^c B &= \{x \in \Omega : x \in A \text{ and } x \in B \text{ hold compatibly}\}, \\
A \times^d B &= \{(x,y) \in \Omega \times \Omega : x \in A \text{ and } y \in B \text{ hold disjointly}\}, \\
A \times^c B &= \{(x,y) \in \Omega \times \Omega : x \in A \text{ and } y \in B \text{ hold compatibly}\}.
\end{aligned}$$

The notation above is chosen to emphasize the common framework; however: the by now well-studied operation $\cap^d$ is often denoted $\Box$ (e.g. in [2]) and we will do so below; and of course $\cap^c$ is simply $\cap$. We also remark that Goldstein and Rinott [4] use $A\Diamond B$ for $A\times^c B$ and that, trivially, $A\times^d B\subseteq A\times^c B$.

Theorem 1.3 (Reimer's Inequality [10])
If (Ω,μ) is a finite product probability space then

$$\forall A,B\subseteq\Omega,\ \ \mu(A\Box B)\le\mu(A)\mu(B). \tag{2}$$

∎

This was conjectured by van den Berg and Kesten [2], who proved it in case the Ω_i's are totally ordered and A,B are increasing with respect to the product order on Ω; this is the *BK inequality.* Theorem 1.3 is also called the *BKR inequality.*

We will prove the following, similar results.

Theorem 1.4 (The Strong Dual Inequality)
If (Ω,μ) is a finite product probability space then

$$\forall A,B\subseteq\Omega,\ \ (\mu\times\mu)(A\times^c B)\le\mu(A\cap B). \tag{3}$$

Corollary 1.5 (The Dual Inequality)
If (Ω,μ) is a finite product probability space then

$$\forall A,B\subseteq\Omega,\ \ (\mu\times\mu)(A\times^d B)\le\mu(A\cap B). \tag{4}$$

Since (2) can also be written as

$$\forall A,B\subseteq\Omega,\ \ \mu(A\cap^d B)\le(\mu\times\mu)(A\times B)$$

we view (4) as dual to (2).

It is easy to see (and well-known; see e.g. [16], Remark 4.4a) that Theorem 1.3 implies the historically first correlation inequality, *viz.*

Theorem 1.6 (Harris-Kleitman Inequality [5, 9]) *For any finite product probability space (Ω,μ) with $\Omega=\{0,1\}^n$, and $A,B\subseteq\Omega$ increasing,*

$$\mu(A\cap B)\ge\mu(A)\mu(B).$$

When A and B are increasing sets, it is easily verified that $A\times^c B=A\times B$ and thus Theorem 1.4 implies Theorem 1.6.

We prove Theorem 1.4 in Section 2 and Theorem 1.2 in Section 3. In the last section, we suggest some extensions of these results.

2 Proof of Theorem 1.4

The great step in Reimer's proof of Theorem 1.3 was his "Butterfly Lemma," Lemma 2.2 below. We first demonstrate how Theorems 1.3 and 1.4 are proved; they are reduced to a set of "local" inequalities which are then given by the lemma. A *subcube* Q of $\Omega = \Omega_1 \times \cdots \times \Omega_n$ is a set of the form $Q_1 \times \cdots \times Q_n$ where $Q_i \subseteq \Omega_i$ and $1 \leq |Q_i| \leq 2$ for each $i \in [n]$. For $x, y \in \Omega$, the subcube *generated* by x and y is

$$[x, y] := \{z \in \Omega : z_i \in \{x_i, y_i\}\}.$$

For a subcube Q, let $\mathrm{Pairs}(Q) := \{(x, y) | Q = [x, y]\}$. For each $x \in Q$, there is a unique $y \in \Omega$ such that $Q = [x, y]$; this is the *complement* of x *relative* to Q, denoted $\overline{x}^Q$. For $(x, y) \in \mathrm{Pairs}(Q)$, we have

$$(\mu \times \mu)(x, y) = \mu(x)\mu(y) = \prod_i \mu_i(x_i)\mu_i(y_i).$$

This product is the same for all $(x, y) \in \mathrm{Pairs}(Q)$ and is denoted μ_Q. Thus if $X \subseteq \Omega \times \Omega$, we have

$$(\mu \times \mu)(X) = \sum_Q |X_Q| \mu_Q,$$

where $X_Q = X \cap \mathrm{Pairs}(Q)$ and Q ranges over subcubes of Ω. It follows that for $X, Y \subseteq \Omega \times \Omega$,

$$\text{if } |X_Q| \leq |Y_Q| \text{ for all subcubes } Q \text{ then } (\mu \times \mu)(X) \leq (\mu \times \mu)(Y). \tag{5}$$

Since $\mu(S) = (\mu \times \mu)(S \times \Omega)$ (for any $S \subseteq \{0, 1\}^n$), we may rewrite the inequalities (2) and (3) of Theorems 1.3 and 1.4 in the form $(\mu \times \mu)(X) \leq (\mu \times \mu)(Y)$ for appropriate $X, Y \subseteq \Omega \times \Omega$, and hope to derive them from (5). Thus Reimer proves (2) by showing

$$|((A \Box B) \times \Omega)_Q| \leq |(A \times B)_Q|, \tag{6}$$

while Theorem 1.4 will follow from

Proposition 2.1 *For any $A, B \subseteq \Omega$ and subcube Q of Ω,*

$$|(A \times^c B)_Q| \leq |((A \cap B) \times \Omega)_Q|. \tag{7}$$

The statement of the Butterfly Lemma requires some definitions. A *butterfly* in Ω is an ordered pair of subcubes, $\beta = (R, Y)$, with $|R \cap Y| = 1$. We write b or $b(\beta)$ for the unique element of $R \cap Y$, called the *body* of β. The subcubes $R(\beta) := R$ and $Y(\beta) := Y$ are the *red* and *yellow wings* of β. The points $r = r(\beta) := \overline{b}^R$ and $y = y(\beta) := \overline{b}^Y$ are, respectively, the *red tip* and *yellow tip* of β. The *span* of β is then $[r, y]$, the unique minimal subcube containing $R \cup Y$. A butterfly with span Q is called a *Q-butterfly.*

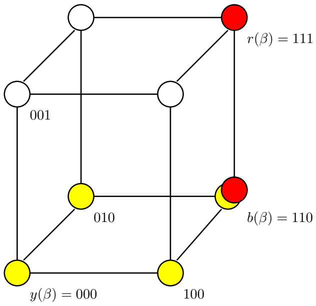

Figure 1: A butterfly β in $\{0,1\}^3$. Points in $R(\beta)$ are red, those in $Y(\beta)$, yellow. Note, $b(\beta) \in R(\beta) \cap Y(\beta)$.

If $\mathcal{B}$ is a family of Q-butterflies, we define:

$$\mathrm{R}(\mathcal{B}) := \bigcup_{\beta \in \mathcal{B}} \mathrm{R}(\beta), \qquad \mathrm{Y}(\mathcal{B}) := \bigcup_{\beta \in \mathcal{B}} \mathrm{Y}(\beta).$$

If no two butterflies of $\mathcal{B}$ have the same red tip, we say $\mathcal{B}$ *has distinct red tips.*

Lemma 2.2 (Butterfly Lemma [10])
If $\mathcal{B}$ is a family of Q-butterflies with distinct red tips, then

$$|\mathcal{B}| \leq |\mathrm{R}(\mathcal{B}) \cap \mathrm{Y}(\mathcal{B})|.$$

∎

Proof of Proposition 2.1. Let $Z = \{x \in Q : (x, \overline{x}^Q) \in A \times^c B\}$. Note $|Z| = |(A \times^c B)_Q|$. We will define a family $\mathcal{B} = \{\beta(x) : x \in Z\}$ of Q-butterflies that satisfies: (i) $\mathrm{R}(\mathcal{B}) \subseteq A$, (ii) $\mathrm{Y}(\mathcal{B}) \subseteq B$, and (iii) the red tip of $\beta(x)$ is x.

Condition (iii) implies that $\mathcal{B}$ satisfies the hypothesis of Lemma 2.2, while (i), (ii) and the fact that $\mathcal{B}$ is a Q-butterfly imply that $\mathrm{R}(\mathcal{B}) \cap \mathrm{Y}(\mathcal{B}) \subseteq A \cap B \cap Q$. Thus, by the lemma,

$$\begin{array}{rcl} |(A \times^c B)_Q| = |\mathcal{B}| & \leq & |\mathrm{R}(\mathcal{B}) \cap \mathrm{Y}(\mathcal{B})| \\ & \leq & |A \cap B \cap Q| \\ & = & |((A \cap B) \times \Omega)_Q|, \end{array}$$

where the final equality uses the easy identity $|T \cap Q| = |(T \times \Omega)_Q|$ for any $T \subseteq \Omega$.

It now suffices to define $\mathcal{B}$. Fix $x \in Z$. By definition, there are partial selection functions $f \not\sim' g$ such that $x \in C(f) \subseteq A$ and $\overline{x}^Q \in C(g) \subseteq B$. Since f and g are compatible, we may define the partial selection function h with $\mathrm{dom}(h) = \mathrm{dom}(f) \cup \mathrm{dom}(g)$ and

$$h(i) := \left\{ \begin{array}{ll} f(i) & i \in \mathrm{dom}(f) \\ g(i) & i \in \mathrm{dom}(g). \end{array} \right.$$

Let $b(x)$ be some element of $C(h) = C(f) \cap C(g) \subseteq A \cap B$. Since $x \in C(f)$ and $\overline{x}^Q \in C(g)$, we have $R(x) := [x, b(x)] \subseteq C(f) \subseteq A$ and $Y(x) := [\overline{x}^Q, b(x)] \subseteq C(g) \subseteq B$. If we set $\beta(x) := (R(x), Y(x))$, then $\mathcal{B} := \{\beta(x) : x \in Z\}$ is a family of Q-butterflies satisfying (i), (ii) and (iii), and the proof is complete.

■

3 Proof of Theorem 1.2

We are given a set $\mathcal{F}$ of cylinders of (Ω, μ) satisfying $\mu(U(\mathcal{F})) \geq 1 - \epsilon$. We want a lower bound for

$$\max_{F \in \mathcal{F}} \mu \left(\bigcup \{G' : G \in N'[F]\} \right) = \mu(U(\mathcal{F})) - \min_{F \in \mathcal{F}} \sum_{G \notin N'[F]} \mu(G'). \qquad (8)$$

Since the sets F' ($F \in \mathcal{F}$) defined in (1) form a partition of $U(\mathcal{F})$, we have

$$\begin{aligned}
\min_{F \in \mathcal{F}} \sum_{G \notin N'[F]} \mu(G') &\leq \frac{1}{\mu(U(\mathcal{F}))} \sum_{F \in \mathcal{F}} \mu(F') \sum_{G \notin N'[F]} \mu(G') \\
&= \frac{1}{\mu(U(\mathcal{F}))} (\mu \times \mu)(\bigcup \{F' \times G' : F \neq G, F \cap G \neq \emptyset\}) \\
&\leq \frac{1}{\mu(U(\mathcal{F}))} (\mu \times \mu)(\bigcup \{F \times G : F \neq G, F \cap G \neq \emptyset\}) \\
&= \frac{1}{\mu(U(\mathcal{F}))} (\mu \times \mu)(S(\mathcal{F}, \mathcal{F})), \qquad (9)
\end{aligned}$$

where for sets $\mathcal{F}, \mathcal{G}$ of cylinders, we define

$$S(\mathcal{F}, \mathcal{G}) = \bigcup \{F \times G : F \in \mathcal{F}, G \in \mathcal{G}, F \neq G, F \cap G \neq \emptyset\}.$$

Claim 3.1 $(\mu \times \mu)(S(\mathcal{F}, \mathcal{F})) \leq 4(1 - \mu(U(\mathcal{F})))$.

Proof: Let $\mathcal{F}_1, \mathcal{F}_2$ be a partition of $\mathcal{F}$ that maximizes $(\mu \times \mu)(S(\mathcal{F}_1, \mathcal{F}_2))$. Then $(\mu \times \mu)(S(\mathcal{F}_1, \mathcal{F}_2))$ is at least the expected value of $(\mu \times \mu)(S(\mathcal{G}, \mathcal{F} - \mathcal{G}))$ where $\mathcal{G}$ is a subset of $\mathcal{F}$ chosen uniformly at random. For each $(x, y) \in S(\mathcal{F}, \mathcal{F})$, there is a pair of distinct cylinders F, G in $\mathcal{F}$ with $x \in F$, $y \in G$, and $F \cap G \neq \emptyset$, whence

$$\Pr_{\mathcal{G}}[(x, y) \in S(\mathcal{G}, \mathcal{F} - \mathcal{G})] \geq \Pr_{\mathcal{G}}[(F \in \mathcal{G}) \wedge (G \notin \mathcal{G})] = 1/4$$

and, summing over $(x, y) \in \mathcal{F} \times \mathcal{F}$,

$$\mathbb{E}_{\mathcal{G}}[(\mu \times \mu)(S(\mathcal{G}, \mathcal{F} - \mathcal{G}))] \geq (1/4)(\mu \times \mu)(S(\mathcal{F}, \mathcal{F})).$$

Thus $(\mu \times \mu)(S(\mathcal{F}_1, \mathcal{F}_2)) \geq (1/4)(\mu \times \mu)(S(\mathcal{F}, \mathcal{F}))$.

Now let $A = \bigcup_{F \in \mathcal{F}_1} F$ and $B = \bigcup_{F \in \mathcal{F}_2} F$. Since $S(\mathcal{F}_1, \mathcal{F}_2) \subseteq A \times^c B$, Theorem 1.4 gives

$$\begin{aligned}
(\mu \times \mu)(S(\mathcal{F}, \mathcal{F})) &\leq 4(\mu \times \mu)(A \times^c B) \\
&\leq 4\mu(A \cap B) \\
&= 4\mu(\bigcup \{F \cap G : F \in \mathcal{F}_1, G \in \mathcal{F}_2\}) \\
&\leq 4(1 - \mu(U(\mathcal{F}))). \qquad (10)
\end{aligned}$$

∎

Finally, combining (8), (9) and Claim 3.1 with the assumption that $\mu(U(\mathcal{F})) \geq 1-\epsilon$ gives

$$\max_{F\in\mathcal{F}} \mu\left(\bigcup\{G' : G \in N'[F]\}\right) \geq \mu(U(\mathcal{F})) - 4\left(\frac{1-\mu(U(\mathcal{F}))}{\mu(U(\mathcal{F}))}\right) \geq 1-\epsilon-\frac{4\epsilon}{1-\epsilon}.$$

∎

4 Further Questions and Remarks

In Theorem 1.2 we showed that Rudich's conjecture is true for all $\epsilon < 3 - 2\sqrt{2} \approx .171$, while the example given in Remark 1.2 shows that the conjecture fails for $\epsilon \geq 1 - 1/e \approx .632$. It is natural to ask if it holds for all $\epsilon < 1 - 1/e$.

Question 4.1 *Is is true that for all $\epsilon < 1 - 1/e$ there exists $\delta > 0$ such that for all $n \geq 1$ and for any set of cylinders $\mathcal{F}$ of $\{0,1\}^n$, if $|U(\mathcal{F})| \geq (1-\epsilon)2^n$, then there is a cylinder $F \in \mathcal{F}$ for which*

$$|\bigcup_{G\in N[F]} G| \geq \delta 2^n?$$

It is natural to ask whether Rudich's conjecture extends to more general probability spaces with cylinders replaced by events satisfying some kind of independence assumption. For a finite family of events $\mathcal{E}$ in an (arbitrary) probability space (Ω, μ), say a graph G on $\mathcal{E}$ is a *strong dependency graph* for $\mathcal{E}$ if for all disjoint $\mathcal{E}', \mathcal{E}'' \subseteq \mathcal{E}$ with $\mathcal{E}' \not\sim \mathcal{E}''$ (that is, no edges of G join $\mathcal{E}'$ and $\mathcal{E}''$), the events in $\mathcal{E}'$ are independent of those in $\mathcal{E}''$; equivalently,

$$\mu(\bigcap_{E\in\mathcal{E}'\cup\mathcal{E}''} E) = \mu(\bigcap_{E\in\mathcal{E}'} E)\mu(\bigcap_{E\in\mathcal{E}''} E) \tag{11}$$

for all such $\mathcal{E}'$, $\mathcal{E}''$. Note this is true when $\mathcal{E}$ is a set of cylinders in a product space and $G = (\mathcal{E}, \sim)$.

Rudich [11] and Tardos [15] asked if Conjecture 1.1 might generalize to this setting. We again use $U(\mathcal{E})$ for the event that a unique member of $\mathcal{E}$ occurs and, given a strong dependency graph G for $\mathcal{E}$, $N[F]$ for the closed neighborhood of F in G.

Conjecture 4.2 *There exists $\epsilon, \delta > 0$ such that for every probability space (Ω, μ), every family $\mathcal{E}$ of events in Ω, and every strong dependency graph G for $\mathcal{E}$, if $\mu(U(\mathcal{E})) \geq 1 - \epsilon$ then $\mu(\bigcup_{E\in N[F]} E) \geq \delta$ for some $F \in \mathcal{E}$.*

In fact it is natural to ask whether this holds at the level of dependency graphs in the sense of the Lovász local lemma ([3] or e.g. [1]), that is, where we only assume (11) when $\mathcal{E}'$ consists of a single event. Szegedy [13] provided a counterexample to this. The following is a simplified version due to Tardos [15].

Example 4.1 Let $k, l > 1$. Let $\omega = (\omega_0, \omega_1, \ldots, \omega_k)$ be selected according to the uniform measure μ on $\Omega = [k] \times [l]^k$. Let $\mathcal{E} = \{A_{ij} : i \in [k], j \in [l]\}$ where $A_{ij} = \{\omega \in \Omega : (\omega_0 = i \text{ and } \omega_i = j) \text{ or } (\omega_0 \neq i \text{ and } \omega_i = 1)\}$.

We first check that the graph on $\mathcal{E}$ obtained by taking A_{ij} adjacent to $A_{i'j'}$ iff $i = i'$ (and $j \neq j'$) is a dependency graph, that is, that for any $A_{i_0j_0}, \ldots, A_{i_kj_k} \in \mathcal{E}$ with $i_1, \ldots, i_k \neq i_0$, the events $E = A_{i_0j_0}$ and $E' = \bigcap_{l=1}^k A_{i_lj_l}$ are independent. We have

$$\begin{aligned} \mu(E \cap E') &= \mu(E' \cap \{\omega_0 = i_0, \omega_{i_0} = j_0\}) + \mu(E' \cap \{\omega_0 \neq i_0, \omega_{i_0} = 1\}) \\ &= \mu(E' \cap \{\omega_0 = i_0\})\mu(\omega_{i_0} = j_0) + \mu(E' \cap \{\omega_0 \neq i_0\})\mu(\omega_{i_0} = 1) \\ &= \mu(E')\mu(E), \end{aligned}$$

where the second equality holds because the events $E' \cap \{\omega_0 = i_0\}$ and $E' \cap \{\omega_0 \neq i_0\}$ do not depend on ω_{i_0}, and the third because $\mu(\omega_{i_0} = j) = l^{-1}$ for any j (so also $\mu(E) = l^{-1}$).

Let $A = A_{i_0j_0}$ and notice that

$$A' \ (= A \setminus \bigcup\{A_{ij} : (i,j) \neq (i_0, j_0)\}) = \{\omega_0 = i_0, \omega_{i_0} = j_0, \omega_i \neq 1 \forall i \neq i_0\},$$

which, using symmetry, gives

$$\mu(U(\mathcal{E})) = kl\mu(A') = (1 - l^{-1})^{k-1}.$$

On the other hand, noting that $N := N[A_{i_0,j_0}] = \{A_{i_0,j} : j \in [l]\}$, we have

$$\mu(\textstyle\bigcup_{B \in N} B) = \mu(\omega_0 = i_0) + \mu(\omega_0 \neq i_0, \omega_{i_0} = 1) = \frac{1}{k} + \frac{k-1}{kl}. \qquad (12)$$

The conclusion of Rudich's Conjecture then fails, since k, l can be chosen to make $\mu(U(\mathcal{E}))$ arbitrarily close to 1 and the right side of (12) arbitrarily close to 0.

As noted above, there is an obvious symmetry between Reimer's inequality (2) and the dual inequality (4). The formal dual of the strong dual inequality, (3), is $\mu(A \cap^c B)$ $(= \mu(A \cap B)) \leq \mu(A)\mu(B)$ which is of course not true in general. Can one find stronger versions of Reimer's inequality and the dual inequality that are dual to each other in some natural sense?

Note that the definitions and properties of cylinders, partial selection functions, relations $\sim$ and $\sim'$, and operations $\Box$, $\times^d$, and $\times^c$ apply to any product space. In [4], Goldstein and Rinott proved that each of Theorems 1.3 and Corollary 1.5 can be extended to general product probability spaces.[1] Their methods also work for Theorem 1.4.

Theorem 4.3 *For $(\Gamma, \nu) = \prod_{i=1}^n (\Gamma_i, \nu_i)$, a product of probability spaces, and for all measurable $A, B \subseteq \Gamma$*

$$\nu(A \Box B) \leq \nu(A)\nu(B),$$

$$(\nu \times \nu)(A \times^c B) \leq \nu(A \cap B).$$

In follows that Rudich's conjecture and Theorem 1.2 easily extend to general product probability spaces.

Corollary 1.5 was used by one of the authors to prove a theorem about boolean decision tree complexity [12]. That result is a strengthening of several conjectures on approximate decision tree complexity due to Impagliazzo and Rudich [6,7] and Tardos [14]. The conjectures of Impagliazzo and Rudich stemmed from investigations in the foundations of cryptography and were the motivation for Rudich's conjecture. Tardos' motivation was, in part, to explore the relation between deterministic and non-deterministic query complexity classes.

References

[1] Noga Alon and Joel H. Spencer, *The probabilistic method*, third ed., Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons Inc., Hoboken, NJ, 2008, With an appendix on the life and work of Paul Erdős. MR MR2437651 (2009j:60004)

[2] J. van den Berg and H. Kesten, *Inequalities with applications to percolation and reliability*, J. Appl. Probab. **22** (1985), no. 3, 556–569. MR MR799280 (87b:60027)

[1] Note the present results were proved some years ago and appeared in preliminary form in [8].

[3] P. Erdős and L. Lovász, *Problems and results on* 3*-chromatic hypergraphs and some related questions*, Infinite and finite sets (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday), Vol. II, North-Holland, Amsterdam, 1975, pp. 609–627. Colloq. Math. Soc. János Bolyai, Vol. 10. MR MR0382050 (52 #2938)

[4] Larry Goldstein and Yosef Rinott, *Functional BKR inequalities, and their duals, with applications*, J. Theoret. Probab. **20** (2007), no. 2, 275–293. MR MR2324531 (2008b:60030)

[5] T. E. Harris, *A lower bound for the critical probability in a certain percolation process*, Proc. Cambridge Philos. Soc. **56** (1960), 13–20. MR MR0115221 (22 #6023)

[6] Russell Impagliazzo and Steven Rudich, personal communication.

[7] ———, *Limits on the provable consequences of one-way permutations*, Advances in cryptology—CRYPTO '88 (Santa Barbara, CA, 1988), Lecture Notes in Comput. Sci., vol. 403, Springer, Berlin, 1990, pp. 8–26. MR MR1046378 (91i:94028)

[8] Jeff Kahn, Michael Saks, and Cliff Smyth, *A dual version of Reimer's inequality and a proof of Rudich's conjecture*, 15th Annual IEEE Conference on Computational Complexity (Florence, 2000), IEEE Computer Soc., Los Alamitos, CA, 2000, pp. 98–103. MR MR1823529 (2002a:68044)

[9] Daniel J. Kleitman, *Families of non-disjoint subsets*, J. Combinatorial Theory **1** (1966), 153–155. MR MR0193020 (33 #1242)

[10] David Reimer, *Proof of the van den Berg-Kesten conjecture*, Combin. Probab. Comput. **9** (2000), no. 1, 27–32. MR MR1751301 (2001g:60017)

[11] Steven Rudich, unpublished, ca. 1990.

[12] Clifford Smyth, *Reimer's inequality and Tardos' conjecture*, Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing (New York), ACM, 2002, pp. 218–221 (electronic). MR MR2121145

[13] Mario Szegedy, unpublished, ca. 1990.

[14] Gábor Tardos, *Query complexity, or why is it difficult to separate* $\mathrm{NP}^A \cap \text{co-}\mathrm{NP}^A$ *from* P^A *by random oracles* A*?*, Combinatorica **9** (1989), no. 4, 385–392. MR MR1054014 (91h:68070)

[15] ______, unpublished, ca. 1990.

[16] J. van den Berg and U. Fiebig, *On a combinatorial conjecture concerning disjoint occurrences of events*, Ann. Probab. **15** (1987), no. 1, 354–374. MR MR877608 (88d:60052)