Sharper Upper Bounds for Unbalanced Uniquely Decodable Code Pairs*

Per Austrin † *Petteri Kaski* ‡ *Mikko Koivisto* § *Jesper Nederlof* ¶

Abstract

Two sets $A, B \subseteq \{0,1\}^n$ form a Uniquely Decodable Code Pair (UDCP) if every pair $a \in A$, $b \in B$ yields a distinct sum $a+b$, where the addition is over $\mathbb{Z}^n$. We show that every UDCP A, B, with $|A| = 2^{(1-\epsilon)n}$ and $|B| = 2^{\beta n}$, satisfies $\beta \leq 0.4228 + \sqrt{\epsilon}$. For sufficiently small ϵ, this bound significantly improves previous bounds by Urbanke and Li [Information Theory Workshop '98] and Ordentlich and Shayevitz [2014, arXiv:1412.8415], which upper bound β by 0.4921 and 0.4798, respectively, as ϵ approaches 0.

1 Introduction

A canonical problem in multi-user communication theory is how to coordinate unambiguous communication through a channel, such that several independent senders can simultaneously send as much information as possible to a single receiver (see, e.g., the book by Schleger and Grant [14]); this could for example occur when several satellites need to send their data to a single terminal.

Unfortunately, despite vast research in the last decades, even in some of the simplest models the exact capacity of such communication channels remains far from clear. An extensively investigated and fundamental example is the *two-user Binary Adder Channel (BAC)*. The zero-error capacity of the BAC is equal to the maximum size of the product of the code sizes of a *Uniquely Decodable Code Pair (UDCP)*: a pair $A, B \subseteq \{0,1\}^n$ such that $|A+B| = |A| \cdot |B|$ where $A+B$ denotes the sumset $\{a+b : a \in A, b \in B\}$, and $a+b$ denotes addition over $\mathbb{Z}^n$.

Most previous research on UDCPs has focused on constructions. A basic observation is that, if $A_1, B_1 \subseteq 2^{[n]}$ is a UDCP[1] and $A_2, B_2 \subseteq 2^{[n]}$ is a UDCP, then $A_1 \times A_2, B_1 \times B_2$ is also a UDCP. Therefore, for finding asymptotically good constructions for every n, it is sufficient to focus on finite n. Letting α and β denote respectively $\log_2(|A|)/n$ and $\log_2(|B|)/n$, a natural and popular goal is to find a UDCP maximizing $\alpha + \beta$. The first and simplest construction, $A = \{00, 01, 11\}, B = \{10, 01\}$ giving $\alpha + \beta = (\log_2(3) + 1)/2 \approx 1.29248$, was presented by Kasami and Lin [7]. This was the best until 1985. Then it was improved to 1.30366 by van den

*Full version of an extended abstract to appear at the 2016 IEEE International Symposium on Information Theory.

†School of Computer Science and Communication, KTH Royal Institute of Technology, Sweden. austrin@csc.kth.se

‡Helsinki Institute for Information Technology HIIT, Department of Computer Science, Aalto University, Finland. petteri.kaski@aalto.fi

§Helsinki Institute for Information Technology HIIT, Department of Computer Science, University of Helsinki, Finland. mikko.koivisto@helsinki.fi

¶Department of Mathematics and Computer Science, Technical University of Eindhoven, The Netherlands. j.nederlof@tue.nl

[1] In this work, we freely interchange vectors with sets in the natural way.

Braak and van Tilborg [17], and after subsequent improvements by Ahlswede and Balakirsky [1] (1.30369), van den Braak [16] (1.30565), Urbanke and Li [15] (1.30999), the current record is 1.31781 by Mattas and Östergård [11]. Several of these results were obtain by computer searches for finite n. More relevant to our study is the important work by Kasami et al. [8], which shows that for sufficiently large n there exist (somewhat surprisingly) UDCPs with $\alpha \geq 1 - o(1)$ and $\beta \geq 0.25$.

Considering upper bounds, the rather direct $\alpha + \beta \leq 1.5$ has been independently found by at least Liao [9], Ahlswede [2], Lindström [10] and van Tilborg [18]. Somewhat unsatisfactory, 1.5 is, to the best of our knowledge, still the best known upper bound on $\alpha + \beta$ in general. However, Urbanke and Li [15] managed to break through the 1.5 bound in the *unbalanced case*: assuming $\alpha \geq 1 - \epsilon$ for a sufficiently small value of ϵ, they showed that $\beta \leq 0.4921$. On a high level, their approach works as follows: a result of van Tilborg [18] (see also Lemma 1 below) shows there are not many pairs $(a, b) \in A \times B$ of small Hamming distance, and if A and B are sufficiently large, then the number of such pairs is lower bounded by an *isoperimetric inequality* for which the authors use Harper's theorem. Later, this result was improved to $\beta \leq 0.4798$ by Ordentlich and Shayevitz [13]. Their proof idea is somewhat more involved: the authors give a procedure that, given a UDCP $A, B \subseteq \{0,1\}^n$, constructs another UDCP $C, C \in \{0,1\}^{(1-\gamma)n}$ with some $\gamma > 0$. This was achieved by proving the existence of a subset $L \subseteq [n]$ with $|L| = \gamma n$ such that for some $c \in \{0,1,2\}^{|L|}$, the projection $(a+b)_L$ equals c for many pairs a, b. The existence of such a subset is proved using a variant of the Sauer–Perles–Shelah lemma. Unfortunately, both the referred bounds [13, 15] converge fast to $(1 - \epsilon) + \beta \leq 1.5$ as ϵ increases (see Figure 1 of Ordentlich and Shayevitz [13]).

The present authors [3] gave a novel and direct connection between UDCPs and additive number theory. Motivated by algorithm design for the Subset Sum problem, they observed the following: if $w \in \mathbb{Z}^n, t \in \mathbb{Z}$ and $A \subseteq \{0,1\}^n$ such that $a \cdot w = a' \cdot w$ implies $a = a'$ for every $a, a' \in A$, and $B = \{b \in \{0,1\}^n : w \cdot b = t\}$, then A, B is a UDCP. Here '$\cdot$' denotes the inner product.

The channel capacity application has also inspired studies of several variants of the basic setting of this paper, for example, with both sets being the same [5, 10], with noise [14], or with more than two users [2, 4, 6].

Our Contribution

Motivated by the unsatisfactory slow progress on the large gap between the current lower and upper bounds for UDCPs, we propose to restrict attention to the case $|A| \geq 2^{(1-\epsilon)n}$ for small values of ϵ: before we can understand the exact tradeoff between α and β, we first need to understand this tradeoff for large values of α. An intriguing question is whether $\alpha \geq 1 - o(1)$ implies $\beta \leq 0.25 + o(1)$; in other words, is the construction of Kasami et al. [8] optimal, or could it be improved? We make significant progress on this question, and our main result is:

Theorem 1 (Main Theorem)**.** *If $A, B \subseteq \{0,1\}^n$ is a UDCP with $|A| \geq 2^{(1-\epsilon)n}$ and $|B| = 2^{\beta n}$, then $\beta \leq 0.4228 + \sqrt{\epsilon}$.*

Our proof combines ideas from both previous upper bounds with new ideas. We will present our proof by first providing a "warm-up" bound of $\beta \leq 0.4777 + O(\sqrt{\epsilon})$ (Theorem 2). To establish this bound, we study the joint probability $\Pr[a \in A, b \in B]$ for two *correlated* random strings $a, b \in \{0,1\}^n$. We upper and lower bound this probability using, respectively, van Tilborg's lemma (Lemma 1) and an isoperimetric inequality due to Mossel et al. [12]. This approach is similar to that of Urbanke and Li [15], but improves their bound for small values of ϵ.

The intuition behind our main bound (and, partially, the bounds of Urbanke and Li [15] and Ordentlich and Shayevitz [13]) is as follows. The above strategy does not give a good bound if A and B are antipodal Hamming balls: the studied probability is very small in this case, so the upper bound is not really stringent. However, intuitively such a pair cannot form a large UDCP since the pairwise sums will be concentrated on the sum of the two centers of the Hamming balls. Our novel approach is that we use the encoding argument from van Tilborg's lemma to show that if A is large enough, then B needs to be sufficiently spread out over the hypercube. Specifically, we show that there exists a set $L \subseteq [n]$ of size close to $n/2$ such that L has an almost maximum number of projections on B. Subsequently, we use this set L to define a refined distribution of the strings x and y. In the refined distribution, x, y are only correlated in the coordinates from L, and for applying the isoperimetric inequality the large number of projections is then essential.

2 Notation and Preliminaries

2.1 Notation

Given reals a, b with $b \geq 0$, we write $a \pm b$ for the interval $[a-b, a+b]$. If n is an integer, we denote $[n] = \{1, \ldots, n\}$. For $x \in \mathbb{R}^n$, we denote by $x^{-1}(z) \subseteq [n]$ the set of coordinates i such that $x_i = z$.

For binary vectors, we extend notation for subsets of $[n]$ in the obvious way (by interpreting $x \in \{0,1\}^n$ as the set $x^{-1}(1) \subseteq [n]$). Thus e.g. $x \setminus y$ is a vector which is 1 in the coordinates i where $x_i = 1$ and $y_i = 0$, $x \triangle y$ denotes the symmetric difference (or alternatively, the componentwise XOR) of x and y, and $|x|$ denotes the Hamming weight of x.

Given $x \in \{0,1\}^n$ and $P \subseteq [n]$, we let x_P denote the *projection* of x on P: $x_P \in \{0,1\}^P$ such that x_P agrees with x on all coordinates in P. For a family $X \subseteq \{0,1\}^n$ we also write $X_P = \{x_P : x \in X\}$.

2.2 Entropy

For $x \in [0,1]$ we let $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ denote the *binary entropy* of x. It is well known that $h(x)$ is monotone increasing for $x \in [0,1/2]$, monotone decreasing for $x \in [1/2,1]$, and that $\binom{n}{t} \leq 2^{h(t/n)n}$. The following elementary inequality can be shown by standard calculus:

Observation 1. *For all $x \in (0,1/2]$, $h\big(\frac{1}{2}+x\big) < 1 - \frac{2}{\ln 2}x^2$.*

This observation implies another useful bound:

Observation 2. *Let $\epsilon > 0$ be a constant. Suppose $X \subseteq \{0,1\}^n$ such that $|X| \geq 2^{(1-\epsilon)n}$, $z \in \{0,1\}^n$, and $\gamma \geq \sqrt{\frac{\ln 2}{2}\epsilon}$. Then for sufficiently large n, we have that $|\{x \in X : |x \triangle z| \in (\frac{1}{2} \pm \gamma)n\}| \geq |X|/2$.*

2.3 UDCPs

We will use the following well known property of UDCPs that directly follows from noting that whenever $a - b = a' - b'$ we have $a + b' = a' + b$:

Observation 3. *If A, B is a UDCP, then $|A - B| = |A| \cdot |B|$.*

We will also use the following bound. Since the proof is elegant and highly instructive for understanding our approach, we provide a (known) proof.

Lemma 1 (van Tilborg [18])**.** *Let $A, B \subseteq \{0,1\}^n$ be a UDCP and let $W_d = |\{(a,b) \in A \times B : |a \triangle b| = d\}|$. Then $|W_d| \le \binom{n}{d} 2^{\min\{d, n-d\}}$.*

Proof. Let us bound the number of possibilities for $a+b$ and $b-a$ for pairs $(a,b) \in W_d$. Note that

$$a \triangle b = (a+b)^{-1}(1) = [n] \setminus (b-a)^{-1}(0)\,.$$

Thus, since $|a \triangle b| = d$, fixing $a \triangle b$ (in one of the $\binom{n}{d}$ possible ways) leaves either 2^{n-d} possible choices for $(a+b)^{-1}(0)$ and $(a+b)^{-1}(2)$, or 2^d possible choices for $(b-a)^{-1}(-1)$ and $(b-a)^{-1}(1)$. By the UDCP property, either of these two completely determines $(a,b) \in W_d$, and the bound follows. □

2.4 ρ-correlation and isoperimetry

For $x \in \{0,1\}^U$, we write $y \sim_\rho x$ for a *ρ-correlated random copy* of x, i.e., a string where, independently for each $e \in U$,

$$y_e = \begin{cases} x_e, & \text{with probability } \frac{1+\rho}{2}\,, \\ 1 - x_e, & \text{with probability } \frac{1-\rho}{2}\,. \end{cases}$$

If x is not fixed, we use $y \sim_\rho x$ to denote the joint distribution over (x, y) where x is a uniformly random string and y is ρ-correlated copy of x. Our bounds will rely on the reverse Small Set Expansion Theorem, an isoperimetric inequality of the noisy Boolean hypercube:

Lemma 2 (Reverse Small Set Expansion, [12, Theorem 3.4][2])**.** *Let $F, G \subseteq \{0,1\}^U$ with $|F| \ge 2^{f|U|}$, $|G| \ge 2^{g|U|}$. Then*

$$\Pr_{y \sim_\rho x}[x \in F, y \in G] \ge 2^{-|U|\left(\frac{(1-f)+(1-g)+2\rho\sqrt{(1-f)(1-g)}}{1-\rho^2}\right)}\,.$$

3 Simple UDCP Bound Using Isoperimetry

In this section we give a warm-up to our main result, showing how a simple application of Theorem 2 suffices to obtain improved UDCP bounds.

Theorem 2. *If $A, B \subseteq \{0,1\}^n$ is a UDCP with $|A| \ge 2^{(1-\epsilon)n}$ and $|B| \ge 2^{\beta n}$, then $\beta \le 0.4777 + \epsilon + 0.7676\sqrt{\epsilon(1-\beta)}$.*

Proof. Let $W_d = \{(a,b) \in A \times B : |a \triangle b| = d\}$. By definition of ρ-correlation it is easy to see that

$$\begin{aligned} \Pr_{a \sim_\rho b}[a \in A, b \in B] &= 2^{-n} \sum_{d=0}^{n} \left(\frac{1+\rho}{2}\right)^{n-d} \left(\frac{1-\rho}{2}\right)^{d} |W_d| \\ &\le 2^{-2n} \sum_{d=0}^{n} (1+\rho)^{n-d} (1-\rho)^d \binom{n}{d} 2^d \\ &= 2^{-2n} (3-\rho)^n\,, \end{aligned}$$

[2] In the notation of [12] where $|F| \ge e^{-s^2/2} 2^{|U|}$ and $|G| \ge e^{-t^2/2} 2^{|U|}$ we have $s = \sqrt{2 \ln 2 (1-f)|U|}$ and $t = \sqrt{2 \ln 2 (1-g)|U|}$.

where the inequality follows from Lemma 1,[3] and the last equality follows from the Binomial Theorem. On the other hand, using Theorem 2, we have that

$$\Pr_{a\sim_\rho b}[a\in A, b\in B] \geq 2^{-n\left(\frac{\epsilon+(1-\beta)+2\rho\sqrt{\epsilon(1-\beta)}}{1-\rho^2}\right)}.$$

Combining the bounds, taking logs, and dividing by n, we see that for any $0\leq\rho<1$,

$$-\left(\frac{\epsilon+1-\beta+2\rho\sqrt{\epsilon(1-\beta)}}{1-\rho^2}\right)\leq \log_2(3-\rho)-2\,,$$

or equivalently,

$$\beta\leq(\log_2(3-\rho)-2)(1-\rho^2)+1+\epsilon+2\rho\sqrt{\epsilon(1-\beta)}\,.$$

Setting $\rho=0.3838$ we obtain

$$\beta\leq 0.4777+\epsilon+0.7676\sqrt{\epsilon(1-\beta)}\,.$$

□

4 Proof Overview of Main Bound

The proof of our main bound follows the same blueprint as the proof of Theorem 2, but we use a more refined version of the noise distribution. In particular, we only apply the noise on a subset of $[n]$ where both A and B are sufficiently dense.

Definition 1. *Fix $L\subseteq[n]$. Given $x\in\{0,1\}^n$ we let $y\sim^L_\rho x$ denote that $y\in\{0,1\}^n$ is the random variable distributed as follows:*

$$y_i=\begin{cases} y_i\sim_\rho x_i & \text{if } i\in L\\ y_i\sim_0 x_i & \text{if } i\notin L.\end{cases}$$

(I.e., y is a ρ-correlated copy of x on the coordinates of L, and uniformly random outside L.)

We proceed to give upper and lower bounds on the quantity $\Pr_{a\sim^L_\rho b}[a\in A, b\in B]$. In order for these bounds to hold, we need a mild density condition on A with respect to the split $(L,[n]\setminus L)$. In particular, we make the following definition.

Definition 2. *We say that $A\subseteq\{0,1\}^n$ is ϵ-dense with respect to $L\subseteq[n]$ if $|A_L|\geq 2^{|L|-\epsilon n-1}$, and for every $a\in A$, the number of $a'\in A$ such that $a_L=a'_L$ is at least $2^{n-|L|-\epsilon n-1}$.*

As the following simple claim shows, our set A is guaranteed to have a dense subset.

Claim 1. *Let $A\subseteq\{0,1\}^n$ such that $|A|\geq 2^{(1-\epsilon)n}$. Then for any $L\subseteq[n]$, there is an $A'\subseteq A$ that is ϵ-dense with respect to L.*

Proof. For $a,a'\in A$ note that the condition $a_L=a'_L$ is an equivalence relation partitioning A into at most $2^{|L|}$ equivalence classes, each of size at most $2^{n-|L|}$. It follows that there must be at least $|A|/2^{n-|L|+1}\geq 2^{|L|-\epsilon n-1}$ equivalence classes of size at least $|A|/2^{|L|+1}=2^{n-|L|-\epsilon n-1}$ and we can take A' to be the union of these. □

[3] Here we did not use the full strength of Lemma 1. In particular we only use that $|W_d|\leq\binom{n}{d}2^d$. However, using the sharper bound of $\binom{n}{d}2^{\min(d,n-d)}$ does not yield any improvement in the exponent because the dominating terms in the exponential sum are those where $d\leq n/2$.

With these definitions in place, we are ready to state the precise upper and lower bounds on the refined noise probability.

Lemma 3. *Fix $L \subseteq [n]$ and let $\lambda = |L|/n$. Then for any $0 \le \rho \le 1$ and UDCP (A, B) such that $|A|$ is ϵ-dense with respect to L, we have*

$$\frac{\log_2 \Pr_{a \sim_\rho^L b}[a \in A, b \in B]}{n} \le \sqrt{\tfrac{\ln(2)\epsilon}{2}} - \tfrac{1}{2} + \lambda \cdot \left(\log_2(3-\rho) - \tfrac{3}{2}\right) + o(1).$$

The proof appears in Section 6.

Lemma 4. *Fix $L \subseteq [n]$ with $|L| = \lambda n$. Then for any constant $0 \le \rho < 1$ the following holds. Let (A, B) be a UDCP such that A is ϵ-dense with respect to L, and $|B_L| = 2^{\pi n}$ for some $0 \le \pi \le \lambda$. Then*

$$\frac{\log_2 \Pr_{a \sim_\rho^L b}[a \in A, b \in B]}{n} \ge \frac{\pi - \lambda - \epsilon - 2\rho\sqrt{\epsilon(\lambda - \pi)}}{1-\rho^2} + \lambda - 1 - \epsilon - o(1).$$

The constant in the $o(1)$ term depends on λ, ρ, ϵ and π, and is finite assuming ϵ is bounded away from 0 and ρ is bounded away from 1.

The proof appears in Section 7.

The quality of the lower bound depends on the size of $|B_L|$ and in particular we would like to find a split L such that $|B_L| \approx |B|$. At the same time we would like $|L|$ to be as small as possible. The following Lemma shows that we can take $|L| \approx n/2$ and still have $|B_L| \approx |B|$.

Lemma 5. *For sufficiently large n and UDCPs (A, B) such that $|A| \ge 2^{(1-\epsilon)n}$, $|B| = 2^{\beta n}$, there exists $L \subseteq [n]$ such that $\frac{|L|}{n} \in \frac{1}{2} \pm \sqrt{\ln(2)\epsilon/2}$ and $|B_L| \ge 2^{(\beta-\epsilon)n-1}$.*

Proof. Let $P \subseteq A \times B$ consist of all pairs (a, b) such that $|a \triangle b| \in \left(\frac{1}{2} \pm \sqrt{\ln(2)\epsilon/2}\right)n$. We have that

$$\begin{aligned} |P| &= \sum_{b \in B} \left|\left\{a \in A : |a \triangle b| \in \left(\tfrac{1}{2} \pm \sqrt{\ln(2)\epsilon/2}\right)n\right\}\right|, \\ &\ge \sum_{b \in B} |A|/2 \quad = \quad |A| \cdot |B|/2, \end{aligned}$$

where the inequality is by Observation 2. Similarly as in the proof of Lemma 1, consider the encoding

$$\eta : (a, b) \mapsto (a \triangle b, b \setminus a).$$

By Observation 3, $|A - B| = |A| \cdot |B|$, and since $a - b$ can be computed from $\eta(a, b)$, it follows that η is injective and $|\eta(P)| = |P|$. We now upper bound $|\eta(P)|$. To this end, note that $b \setminus a \subseteq a \triangle b$, and so $b \setminus a \in B_{a \triangle b}$.[4] Therefore, by summing over the possible values of $X = a \triangle b$ we have that

$$|\eta(P)| \le \sum_{\substack{X \subseteq [n] \\ |X| \in \left(\frac{1}{2} \pm \sqrt{\ln(2)\epsilon/2}\right)n}} |B_X|.$$

This means that there must be an $X \subseteq [n]$ with $|X| \in \left(\frac{1}{2} \pm \sqrt{\ln(2)\epsilon/2}\right)n$ and $|B_X| \ge |\eta(P)|/2^n = |P|/2^n \ge |A| \cdot |B|/2/2^n \ge 2^{(\beta-\epsilon)n-1}$. ☐

[4] More precisely, $b \setminus a$ projected to $a \triangle b$ is in $B_{a \triangle b}$; we only need that $b \setminus a$ can be described by a single element of $B_{a \triangle b}$.

5 Combining the Bounds

In this section we show how Lemmata 3, 4, and 5 combine to yield our main theorem.

Theorem 1 (restated)**.** *If $A, B \subseteq \{0,1\}^n$ is a UDCP with $|A| \geq 2^{(1-\epsilon)n}$ and $|B| = 2^{\beta n}$, then $\beta \leq 0.4228 + \sqrt{\epsilon}$.*

Proof. Without loss of generality, we may assume that n is sufficiently large for all estimates to hold, since a lower bound for large n also holds for small n: if (A_1, B_1) and (A_2, B_2) are UDCPs, then so is $(A_1 \times A_2, B_1 \times B_2)$.

By Lemma 5, there exists a partition L, R of $[n]$ such that $\lambda = |L|/n \in \frac{1}{2} \pm \sqrt{\ln(2)\epsilon/2}$ and $2^{\pi n} := |B_L| \geq 2^{(\beta-\epsilon)n-1}$. By Claim 1, there is an $A' \subseteq A$ such that A is ϵ-dense with respect to L.

Applying Lemmata 3 and 4 to the UDCP (A', B) we then obtain that

$$\begin{aligned}\frac{\pi - \lambda - \epsilon - 2\rho\sqrt{\epsilon(\lambda-\pi)}}{1-\rho^2} + \lambda - 1 - \epsilon - o(1) &\leq \frac{\log_2 \Pr_{a \sim_\rho^L b}[a \in A', b \in B]}{n} \\ &\leq \sqrt{\tfrac{\ln(2)\epsilon}{2}} - \tfrac{1}{2} + \lambda \cdot \left(\log_2(3-\rho) - \tfrac{3}{2}\right) + o(1).\end{aligned}$$

Simplifying, we get

$$\begin{aligned}\pi \leq{}& \left(\sqrt{\tfrac{\ln(2)\epsilon}{2}} + \tfrac{1}{2} + \epsilon + \lambda \cdot \left(\log_2(3-\rho) - \tfrac{5}{2}\right)\right)(1-\rho^2) \\ &+ 2\rho\sqrt{\epsilon(\lambda-\pi)} + \epsilon + \lambda + o(1).\end{aligned} \tag{1}$$

We now set $\rho = 0.654$. Plugging in this value and simplifying, (1) becomes

$$\pi \leq 0.2861421 + 0.2733156\lambda + 1.573\epsilon + 0.33691\sqrt{\epsilon} + 1.308\sqrt{\epsilon(\lambda-\pi)} + o(1).$$

Using $\lambda \leq \frac{1}{2} + \sqrt{\ln(2)\epsilon/2}$ and simplifying further, we get

$$\pi < 0.4228 + 1.573\epsilon + \left(0.4979 + 1.3080\sqrt{0.5 + \sqrt{\ln(2)\epsilon/2} - \pi}\right)\sqrt{\epsilon} + o(1). \tag{2}$$

Since $\beta \leq \pi + \epsilon + o(1)$, we would like to show that $\pi < 0.4228 + \sqrt{\epsilon} - \epsilon$. Assume for the sake of contradiction that $\pi \geq 0.4228 + \sqrt{\epsilon} - \epsilon$. Plugging this into (2) gives

$$0 < 2.573\epsilon + \left(0.4979 - 1 + 1.308\sqrt{0.0772 + \sqrt{\ln(2)\epsilon/2} - \sqrt{\epsilon} - \epsilon}\right)\sqrt{\epsilon} + o(1). \tag{3}$$

For $0 \leq \epsilon \leq 0.01$, it can be verified using a computer that the right hand side of (3) is non-positive, yielding the desired contradiction (for sufficiently large n), and proving that $\beta < 0.4228 + \sqrt{\epsilon}$. For $\epsilon > 0.01$, we have $\beta < 0.5 + \epsilon < 0.4228 + \sqrt{\epsilon}$ (the first inequality being the classic $|B| \leq 2^{1.5n}/|A|$ upper bound). □

6 Upper Bound Proof

In this section, we prove the upper bound on the refined noise probability stated in Lemma 3.

Lemma 3 (restated)**.** *Fix $L \subseteq [n]$ and let $\lambda = |L|/n$. Then for any $0 \leq \rho \leq 1$ and UDCP (A, B) such that $|A|$ is ϵ-dense with respect to L, we have*

$$\frac{\log_2 \Pr_{a \sim_\rho^L b}[a \in A, b \in B]}{n} \leq \sqrt{\tfrac{\ln(2)\epsilon}{2}} - \tfrac{1}{2} + \lambda \cdot \left(\log_2(3-\rho) - \tfrac{3}{2}\right) + o(1).$$

Proof. Let $R = [n] \backslash L$ be the coordinates not in L. Let W_d be the set of pairs $a_L a_R \in A, b_L b_R \in B$ such that $|a_L \triangle b_L| = d$.

Claim 2. *For sufficiently large n, we have that $|W_d| \leq \binom{|L|}{d} 2^d 2^{1.5|R|} 2^{n\sqrt{\ln(2)\epsilon/2}+1}$.*

Proof. Let $\epsilon' = \sqrt{\frac{\ln(2)\epsilon}{2(1-\lambda)}}$, and let $W'_d \subseteq W_d$ be all pairs from W_d such that $\frac{|a_R \triangle b_R|}{|R|} \in \frac{1}{2} \pm \epsilon'$. Similarly as in the proof of Lemma 5, we see that

$$\begin{aligned} |W'_d| &= \sum_{\substack{b_L b_R \in B \\ a_L \in A_L \\ |a_L \triangle b_L| = d}} \left| \left\{ a_R \in \{0,1\}^R : a_L a_R \in A, |a_R \triangle b_R| \in (\tfrac{1}{2} \pm \epsilon')|R| \right\} \right|, \\ &\geq \sum_{\substack{b_L b_R \in B \\ a_L \in A_L \\ |a_L \triangle b_L| = d}} \tfrac{1}{2} |\{a_R \in \{0,1\}^R : a_L a_R \in A\}| \quad = \quad \tfrac{1}{2}|W_d|. \end{aligned}$$

The inequality follows from Observation 2 combined with the ϵ-dense property $|\{a_R \in \{0,1\}^R : a_L a_R \in A\}| \geq 2^{|R| - \epsilon n}/2 = 2^{(1-\epsilon/(1-\lambda))|R|}/2$.

We proceed with upper bounding $|W'_d|$. Similarly as in the proof of Lemma 1, we define an encoding η on elements (a, b) of W'_d:

$$\eta : (a_L a_R, b_L b_R) \mapsto (a_L \triangle b_L, a_L \setminus b_L, a_R \triangle b_R, a_R \setminus b_R).$$

Since the image $\eta(a, b)$ directly gives $a - b$ and we know that $|A - B| = |A||B|$ by Observation 3, we have that η is injective and thus

$$|W'_d| = |\eta(W'_d)| \leq \binom{|L|}{d} 2^d \sum_{i \in (0.5 \pm \epsilon')|R|} \binom{|R|}{i} 2^i,$$

where the inequality follows by bounding the number of possibilities in every coordinate of $\eta(\cdot)$. The claim is then implied for sufficiently large n from the easy observation that

$$\sum_{i \in (0.5 \pm \epsilon')|R|} \binom{|R|}{i} 2^i \leq 2^{(1.5+\epsilon')|R|} \leq 2^{1.5|R| + n\sqrt{\ln(2)\epsilon/2}}.$$

□

By the refined definition of $\sim_\rho^L$ we have that

$$\Pr_{a \sim_\rho^L b}[a \in A, b \in B] = 2^{-n} \sum_{d=0}^{|L|} \left(\frac{1+\rho}{2}\right)^{|L|-d} \left(\frac{1-\rho}{2}\right)^d 2^{-|R|} W_d. \tag{4}$$

To see that this is true, note that W_d counts exactly the pairs $a \in A, b \in B$, such that $|a_L \triangle b_L| = d$, and that the probability that such pair is picked can be computed as the probability that a is picked (which is 2^{-n}), times the probability that b is picked given that a is picked. The probability that b_R is picked is simply $2^{-|R|}$ since it is picked uniformly at random, and the probability that b_L is picked is $\left(\frac{1+\rho}{2}\right)^{|L|-d}\left(\frac{1-\rho}{2}\right)^{d}$, similarly as in the proof of Theorem 2.

Using Claim 2, we upper bound (4) by

$$\begin{aligned}\Pr_{a\sim_\rho^L b}[a\in A, b\in B] &\le 2^{-2n}\sum_{d=0}^{|L|}(1+\rho)^{|L|-d}(1-\rho)^d\binom{|L|}{d}2^d 2^{1.5|R|+n\sqrt{\ln(2)\epsilon/2}+1}\\ &= 2^{-2n+1.5|R|+n\sqrt{\ln(2)\epsilon/2}+1}\sum_{d=0}^{|L|}(1+\rho)^{|L|-d}(2-2\rho)^d\binom{|L|}{d}\\ &= 2^{\left(\sqrt{\ln(2)\epsilon/2}-2\right)n+1.5|R|+1}(3-\rho)^{|L|},\end{aligned}$$

where the last equality follows from the Binomial Theorem. Using $|R| = n - |L|$, taking logs, and dividing by n, we get

$$\frac{\log_2 \Pr_{a\sim_\rho^L b}[a\in A, b\in B]}{n} \le \sqrt{\frac{\ln(2)\epsilon}{2}} - \frac{1}{2} + \lambda\left(\log_2(3-\rho) - \frac{3}{2}\right) + 1/n.$$

□

7 Lower Bound Proof

In this section, we prove the lower bound on the refined noise probability.

Lemma 4 (restated)**.** *Fix $L \subseteq [n]$ with $|L| = \lambda n$. Then for any constant $0 \le \rho < 1$ the following holds. Let (A, B) be a UDCP such that A is ϵ-dense with respect to L, and $|B_L| = 2^{\pi n}$ for some $0 \le \pi \le \lambda$. Then*

$$\frac{\log_2 \Pr_{a\sim_\rho^L b}[a\in A, b\in B]}{n} \ge \frac{\pi - \lambda - \epsilon - 2\rho\sqrt{\epsilon(\lambda-\pi)}}{1-\rho^2} + \lambda - 1 - \epsilon - o(1).$$

The constant in the $o(1)$ term depends on λ, ρ, ϵ and π, and is finite assuming ϵ is bounded away from 0 and ρ is bounded away from 1.

Proof. Due to the chain rule, $\Pr_{a\sim_\rho^L b}[a\in A, b\in B]$ equals

$$\Pr_{a\sim_\rho^L b}[a\in A, b\in B \mid a_L\in A_L, b_L\in B_L]\cdot \Pr_{a_L\sim_\rho b_L}[a_L\in A_L, b_L\in B_L]\,. \tag{5}$$

We proceed with lower bounding the first term of (5). Let $R = [n]\setminus L$. For the first factor, note that if $b_L \in B_L$, there is at least one b_R such that $b_Lb_R \in B$ by the definition of B_L, and such a b_R is picked with probability $2^{-|R|}$ since it is uniformly distributed over 2^R. Similarly, if $a_L \in A_L$, there are at least $2^{|R|-\epsilon n}/2$ sets $a_R \subseteq R$ such that $a_La_R \in A'$ by the definition of A', and so such an a_R is picked with probability at least $2^{-\epsilon n}/2$. In summary, we have that

$$\Pr_{a\sim_\rho^L b}[a\in A, b\in B \mid a_L\in A_L, b_L\in B_L] \ge 2^{-|R|-\epsilon n}/2 = 2^{(\lambda-1-\epsilon-o(1))n}.$$

For the second term, apply Theorem 2 with $U = L$ and

$$F = A_L, \qquad f = \frac{|L|-\epsilon n-1}{|L|} = 1 - \frac{\epsilon}{\lambda} - o(1),$$

$$G = B_L, \qquad g = \frac{\pi}{\lambda},$$

which gives that

$$\log_2 \Pr_{a_L \sim_\rho b_L}[a_L \in A_L, b_L \in B_L] \geq -|L| \left(\frac{(1-\frac{\pi}{\lambda}) + \frac{\epsilon}{\lambda} + o(1) + 2\rho\sqrt{(1-\frac{\pi}{\lambda})(\frac{\epsilon}{\lambda}+o(1))}}{1-\rho^2} \right),$$
$$= n\left(\frac{\pi - \lambda - \epsilon - 2\rho\sqrt{\epsilon\lambda - \epsilon\pi}}{1-\rho^2} - o(1) \right).$$

The statement now follows by multiplying the two lower bounds following (5). □

Acknowledgements This research was funded by the Swedish Research Council, Grant 621-2012-4546 (PA), the European Research Council, Starting Grant 338077 "Theory and Practice of Advanced Search and Enumeration" (PK), the Academy of Finland, Grant 276864 "Supple Exponential Algorithms" (MK), and NWO VENI project 639.021.438 (JN).

References

[1] R. Ahlswede and V. Balakirsky, "Construction of uniquely decodable codes for the two-user binary adder channel," *IEEE Trans. Inform. Theory*, vol. 45, no. 1, pp. 326–330, 1999.

[2] R. Ahlswede, "Multi-way communication channels," in *Second International Symposium on Information Theory, ISIT 1971*, 1973, pp. 23–52.

[3] P. Austrin, P. Kaski, M. Koivisto, and J. Nederlof, "Subset sum in the absence of concentration," in *32nd International Symposium on Theoretical Aspects of Computer Science, STACS 2015*, 2015, pp. 48–61.

[4] S.-C. Chang and E. Weldon, "Coding for T-user multiple-access channels," *IEEE Trans. Inform. Theory*, vol. 25, no. 6, pp. 684–691, 1979.

[5] G. Cohen, S. Litsyn, and G. Zémor, "Binary B_2-sequences," *J. Comb. Theory Ser. A*, vol. 94, no. 1, pp. 152–155, 2001.

[6] B. Hughes and A. Cooper, "Nearly optimal multiuser codes for the binary adder channel," *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 387–398, 1996.

[7] T. Kasami and S. Lin, "Coding for a multiple-access channel," *IEEE Trans. Inform. Theory*, vol. 22, no. 2, pp. 129–137, 1976.

[8] T. Kasami, S. Lin, V. Wei, and S. Yamamura, "Graph theoretic approaches to the code construction for the two-user multiple-access binary adder channel," *IEEE Trans. Inform. Theory*, vol. 29, no. 1, pp. 114–130, 1983.

[9] H. H. Liao, "Multiple access channels," Ph.D. dissertation, Department of Electrical Engineering, University of Hawaii, Honolulu, 1972.

[10] B. Lindström, "On B_2-sequences of vectors," *Journal of Number Theory*, vol. 4, no. 3, pp. 261–265, 1972.

[11] M. Mattas and P. R. J. Östergård, "A new bound for the zero-error capacity region of the two-user binary adder channel," *IEEE Trans. Inform. Theory*, vol. 51, no. 9, pp. 3289–3291, 2005.

[12] E. Mossel, R. O'Donnell, O. Regev, J. E. Steif, and B. Sudakov, "Non-interactive correlation distillation, inhomogeneous Markov chains, and the reverse Bonami–Beckner inequality," *Israel Journal of Mathematics*, vol. 154, no. 1, pp. 299–336, 2006.

[13] O. Ordentlich and O. Shayevitz, "An upper bound on the sizes of multiset-union-free families," 2014, CoRR, arXiv:1412.8415.

[14] C. Sleger and A. Grant, *Coordinated Multiuser Communications.* Springer, 2006.

[15] R. Urbanke and Q. Li, "The zero-error capacity region of the 2-user synchronous BAC is strictly smaller than its Shannon capacity region," in *IEEE Information Theory Workshop, 1998*, 1998, p. 61.

[16] P. van den Braak, "Constructions and an existence result of uniquely decodable codepairs for the two-access binary adder channel," Department of Mathematica and Computing Science, Michigan State University, Eindhoven University of Technology, Tech. Rep. 83-WSK-01, 1984.

[17] P. van den Braak and H. van Tilborg, "A family of good uniquely decodable code pairs for the two-access binary adder channel," *Information Theory, IEEE Transactions on*, vol. 31, no. 1, pp. 3–9, 1985.

[18] H. van Tilborg, "An upper bound for codes in a two-access binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 1, pp. 112–116, 1978.