REGULAR CODES ARE NOT ASYMPTOTICALLY GOOD

NAVIN KASHYAP

ABSTRACT. In this note, we prove that the family of regular codes is not asymptotically good.

The notation follows that in [2]. All codes considered are binary linear codes. $\mathcal{H}_7$ refers to the $[7, 4]$ binary Hamming code.

Definition 1. *A binary linear code is regular iff it does not contain as a minor any code equivalent to $\mathcal{H}_7$ or $\mathcal{H}_7^\perp$.*

It follows from the theorem that the family of regular codes, which we will denote by $\mathfrak{R}$. Furthermore, $\mathfrak{R}$ is closed under the taking of code duals, *i.e.*, the dual of a regular code is also regular. This is because a code $\mathcal{C}$ contains $\mathcal{H}_7$ as a minor iff its dual $\mathcal{C}^\perp$ contains $\mathcal{H}_7^\perp$ as a minor. It can further be shown [3, p. 437] that $\mathfrak{R}$ is closed under the operations of direct sum, 2-sum, 3-sum and $\overline{3}$-sum; these operations are defined further below.

Recall from coding theory that a code family $\mathfrak{C}$ is called *asymptotically good* if there exists a sequence of $[n_i, k_i, d_i]$ codes $\mathcal{C}_i \in \mathfrak{C}$, with $\lim_i n_i = \infty$, such that $\liminf_i k_i/n_i$ and $\liminf_i d_i/n_i$ are both strictly positive. Informally, in an asymptotically good code family, minimum distance and dimension can both grow linearly with the length of the code.

The purpose of this note is to show the following theorem.

Theorem 1. *The family of regular codes is not asymptotically good.*

To prove Theorem 1, we need the following results.

Theorem 2 ([6])**.** *A code is graphic if and only if it does not contain as a minor any code equivalent to one of the codes $\mathcal{H}_7$, $\mathcal{H}_7^\perp$, $\mathcal{C}(K_5)^\perp$ and $\mathcal{C}(K_{3,3})^\perp$.*

Corollary 3. *A code is cographic if and only if it does not contain as a minor any code equivalent to one of the codes $\mathcal{H}_7$, $\mathcal{H}_7^\perp$, $\mathcal{C}(K_5)$ and $\mathcal{C}(K_{3,3})$.*

In the statement of the above theorem and corollary, K_5 is the complete graph on five vertices, while $K_{3,3}$ is the complete bipartite graph with three vertices on each side. $\mathcal{C}(K_5)^\perp$ is the $[10, 4, 4]$ code with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix},$$

Date: January 6, 2009.
This work was supported by a Discovery Grant from the Natural Sciences and Engineering Research Council (NSERC), Canada.
N. Kashyap is with the Department of Mathematics and Statistics, Queen's University, Kingston, ON K7L 3N6, Canada. Email: nkashyap@mast.queensu.ca.

while $\mathcal{C}(K_{3,3})^{\perp}$ is the $[9,5,3]$ code with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

We recall the definition of the 2-sum of codes $\mathcal{C}$ and $\mathcal{C}'$. (For the definition of $\mathcal{S}_1(\mathcal{C},\mathcal{C}')$, see [2].)

Definition 2 (2-sum)**.** *Let $\mathcal{C}$, $\mathcal{C}'$ be codes of length at least three, such that*

(P1) $0\ldots01$ *is not a codeword of $\mathcal{C}$, and the last coordinate of $\mathcal{C}$ is not identically zero;*
(P2) $10\ldots0$ *is not a codeword of $\mathcal{C}'$, and the first coordinate of $\mathcal{C}'$ is not identically zero.*

Then, $\mathcal{S}_1(\mathcal{C},\mathcal{C}')$ is called the 2-sum *of $\mathcal{C}$ and $\mathcal{C}'$, and is denoted by $\mathcal{C}\oplus_2\mathcal{C}'$.*

We following properties of 2-sum were proved in [2].

Proposition 4. *Let $\mathcal{C}$ and $\mathcal{C}'$ be codes for which $\mathcal{C}\oplus_2\mathcal{C}'$ can be defined.*
(a) $\dim(\mathcal{C}\oplus_2\mathcal{C}') = \dim(\mathcal{C})+\dim(\mathcal{C}')-1$.
(b) *If $\dim(\mathcal{C})>1$, then $d(\mathcal{C}\oplus_2\mathcal{C}')\le d(\mathcal{C}\setminus\{n\})$, where n is the length of $\mathcal{C}$. Similarly, if $\dim(\mathcal{C}')>1$, then $d(\mathcal{C}\oplus_2\mathcal{C}')\le d(\mathcal{C}'\setminus\{1\})$.*

We give below definitions of 3-sum and $\overline{3}$-sum that may be verified to be equivalent to the definitions given in [2].

Definition 3 (3-sum)**.** *Let $\mathcal{C}$, $\mathcal{C}'$ be codes of length at least seven, such that*

(A1) *$\mathcal{C}$ punctured at all but its last three coordinates yields $\{0,1\}^3$, and $\mathcal{C}$ shortened at all but its last three coordinates yields $\{000,111\}$; and*
(A2) *$\mathcal{C}'$ punctured at all but its first three coordinates yields $\{0,1\}^3$, and $\mathcal{C}'$ shortened at all but its first three coordinates yields $\{000,111\}$.*

Then, $\mathcal{S}_3(\mathcal{C},\mathcal{C}')$ is called the 3-sum *of $\mathcal{C}$ and $\mathcal{C}'$, and is denoted by $\mathcal{C}\oplus_3\mathcal{C}'$.*

Definition 4 ($\overline{3}$-sum)**.** *Let $\mathcal{C}$, $\mathcal{C}'$ be codes of length at least seven, such that*

(B1) *$\mathcal{C}$ punctured at all but its last three coordinates yields $\{000,011,101,110\}$, and $\mathcal{C}$ shortened at all but its last three coordinates yields $\{000\}$; and*
(B2) *$\mathcal{C}'$ punctured at all but its first three coordinates yields $\{000,011,101,110\}$, and $\mathcal{C}'$ shortened at all but its first three coordinates yields $\{000\}$.*

Then, $\mathcal{S}_3(\mathcal{C},\mathcal{C}')$ is called the $\overline{3}$-sum *of $\mathcal{C}$ and $\mathcal{C}'$, and is denoted by $\mathcal{C}\,\overline{\oplus}_3\,\mathcal{C}'$.*

The following properties of 3-sum and $\overline{3}$-sum are important.

Proposition 5 ([2])**.** *For codes $\mathcal{C}$ and $\mathcal{C}'$ be codes for which $\mathcal{C}\oplus_3\mathcal{C}'$ can be defined, we have*

$$(\mathcal{C}\oplus_3\mathcal{C}')^{\perp} = \mathcal{C}^{\perp}\,\overline{\oplus}_3\,\mathcal{C}'^{\perp}.$$

Proposition 6. *Let $\mathcal{C}$ and $\mathcal{C}'$ be codes for which $\mathcal{C}\,\overline{\oplus}_3\,\mathcal{C}'$ can be defined.*

(a) $\dim(\mathcal{C}\,\overline{\oplus}_3\,\mathcal{C}') = \dim(\mathcal{C})+\dim(\mathcal{C}')-2$.
(b) *If $\dim(\mathcal{C})>2$ or if $\mathcal{C}$ is 3-connected, then $d(\mathcal{C}\,\overline{\oplus}_3\,\mathcal{C}')\le d(\mathcal{C}\setminus\{n-2,n-1,n\})$, where n is the length of $\mathcal{C}$. Similarly, if $\dim(\mathcal{C}')>2$ or if $\mathcal{C}'$ is 3-connected, then $d(\mathcal{C}\,\overline{\oplus}_3\,\mathcal{C}')\le d(\mathcal{C}'\setminus\{1,2,3\})$.*

Proof. (a) was proved in [2].

(b). It was shown in [2] that if $\dim(\mathcal{C})>2$, then $d(\mathcal{C}\,\overline{\oplus}_3\,\mathcal{C}')\le d(\mathcal{C}\setminus\{n-2,n-1,n\})$.

So, suppose that $\mathcal{C}$ is 3-connected. From (B1) in Definition 4, we see that $\dim(\mathcal{C})\ge 2$. Assume that $\dim(\mathcal{C})=2$. By (B1) again, the generator matrix of $\mathcal{C}$ may be taken to be $[A\ \ D]$, where A

is a $2 \times (n-3)$ matrix, and $D = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$. Any column of A induces a 1-separation of $\mathcal{C}$. Furthermore, any non-zero column in A would be a repetition of a column of D, which induces a 2-separation of $\mathcal{C}$. As $\mathcal{C}$ is 3-connected, both of these are impossible. Hence, $\mathcal{C}$ cannot have length greater than three, which means that it cannot be involved in a $\overline{3}$-sum.

Thus, if $\mathcal{C}$ is 3-connected, we must have $\dim(\mathcal{C}) > 2$. □

The following is a celebrated decomposition theorem of Seymour [4].

Theorem 7 ([3], Theorem 13.2.4)**.** *Every regular code $\mathcal{C}$ can be constructed by means of direct-sums, 2-sums and 3-sums (or, instead, $\overline{3}$-sums) starting with codes each of which is equivalent to a minor of $\mathcal{C}$, and each of which is either graphic, cographic or equivalent to R_{10}, which is the $[10, 5, 4]$ code with parity-check matrix*

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The rest of this note is a proof of Theorem 1.

Let Γ denote the family of graphic codes, co-Γ the family of cographic codes, and $\overline{\Gamma} = \Gamma \cup$ co-Γ. Note that, by virtue of Theorem 2 and Corollary 3, $\overline{\Gamma}$ is minor-closed.

The following result was proved in [2].

Lemma 8. *Let $r \in (0, 1)$. For any code $\mathcal{C} \in \Gamma$ with length $n \geq 2$ and rate $> r$, we have*

$$d(\mathcal{C}) \leq \frac{4 \log n}{\log(1 + r)}. \tag{1}$$

Thus, the family of graphic codes is not asymptotically good. The following shows that the family of cographic codes is also not asymptotically good.

Lemma 9. *Let $r \in (0, 1)$. For any code $\mathcal{C} \in$ co-Γ with rate $> r$, we have $d(\mathcal{C}) < 2/r$.*

Proof. Consider an $[n, k]$ code $\mathcal{C} \in$ co-Γ with rate $> r$. Then, $\mathcal{C} = \mathcal{C}(\mathcal{G})^{\perp}$ for some connected graph $\mathcal{G} = (V, E)$. Therefore, $k/n = (|V| - 1)/|E| > r$, from which we obtain $|V|/|E| > r$.

Now, the average degree of $\mathcal{G}$ is $\overline{\delta} = 2|E|/|V| < 2/r$. Hence, some vertex of $\mathcal{G}$ has degree $< 2/r$. As the edges around any vertex form a cutset of $\mathcal{G}$, the cardinality of the smallest cutset of $\mathcal{G}$ is less than $2/r$. We finish the proof by observing that $d(\mathcal{C})$ is equal to the cardinality of the smallest cutset of $\mathcal{G}$. □

Corollary 10. *$\overline{\Gamma}$ is not an asymptotically good code family.*

Let $\mathfrak{D}$ be a finite collection of codes, and let $\overline{\Gamma} + \mathfrak{D}$ be the set of all codes that can be expressed as $\mathcal{C}_1 \oplus_2 \mathcal{C}_2$ or $\mathcal{C}_1 \,\overline{\oplus}_3\, \mathcal{C}_2$, with $\mathcal{C}_1 \in \overline{\Gamma}$ and $\mathcal{C}_2 \in \mathfrak{D}$. The following result should not be surprising.

Lemma 11. *For any finite collection of codes $\mathfrak{D}$, the family $\overline{\Gamma} + \mathfrak{D}$ is not asymptotically good.*

Proof. Define $d_{\max}(\mathfrak{D}) = \max\{d(\mathcal{C}') : \mathcal{C}' \text{ is a minor of some code in } \mathfrak{D}\}$. We will show that, for $r \in (0, 1)$, if $\mathcal{C}$ is a code in $\Gamma + \mathfrak{D}$ with rate larger than r, then

$$d(\mathcal{C}) \leq \max\left\{ d_{\max}(\mathfrak{D}),\, 2/r,\, \frac{4 \log n}{\log(1 + r)} \right\}. \tag{2}$$

So, let $\mathcal{C}$ be an $[n, k]$ code in $\overline{\Gamma} + \mathfrak{D}$ with $k/n > r$. Now, $\mathcal{C} = \mathcal{C}_1 \oplus_2 \mathcal{C}_2$ or $\mathcal{C} = \mathcal{C}_1 \,\overline{\oplus}_3\, \mathcal{C}_2$ for some $\mathcal{C}_1 \in \overline{\Gamma}$ and $\mathcal{C}_2 \in \mathfrak{D}$. In particular, note that $\mathcal{C}$ must have length at least 4.

Suppose first that $\dim(\mathcal{C}_2) \leq 2$. Then, $\mathcal{C}_2$ cannot contain a minor equivalent to any of the codes $\mathcal{H}_7$, $\mathcal{H}_7^\perp$, $\mathcal{C}(K_5)$, $\mathcal{C}(K_5)^\perp$, $\mathcal{C}(K_{3,3})$ and $\mathcal{C}(K_{3,3})^\perp$, since each of these codes has dimension at least 3. So, by Theorem 2 and Corollary 3, $\mathcal{C}_2$ is graphic as well as cographic.

If $\mathcal{C}_1 \in \Gamma$, then so is $\mathcal{C}$, as Γ is closed under the operations of 2-sum and $\overline{3}$-sum (see *e.g.* [5, Chapter 8]). Therefore, (2) holds by the bound in (1). On the other hand, if $\mathcal{C}_1 \in$ co-Γ, then so is $\mathcal{C}$. This is because Γ is closed under 2-sum and 3-sum, which implies (by duality — cf. Proposition 5) that co-Γ is closed under 2-sum and $\overline{3}$-sum. Hence, (2) holds by Lemma 9.

If $\dim(\mathcal{C}_2) > 2$, then by Propositions 4(b) and 6(b), we have that $d(\mathcal{C}) \leq d(\mathcal{C}')$ for some minor $\mathcal{C}'$ of $\mathcal{C}_2$. So, once again, (2) holds, this time by definition of $d_{\max}(\mathfrak{D})$. □

We have all the preliminary results needed to prove Theorem 1. We can actually prove something slightly stronger at no extra cost, so we might as well do so. We need the following definition.

Definition 5. *Let $\mathfrak{D}$ be a finite family of codes. A minor-closed code family $\mathfrak{C}$ is said to be* $\mathfrak{D}$-regular *if for any connected code $\mathcal{C} \in \mathfrak{C}$, at least one of the following holds:*

(i) *$\mathcal{C} \in \overline{\Gamma} \cup \mathfrak{D}$;*
(ii) *$\mathcal{C}$ is equivalent to $\mathcal{C}_1 \oplus_2 \mathcal{C}_2$ or $\mathcal{C}_1 \,\overline{\oplus}_3\, \mathcal{C}_2$ for some 3-connected code $\mathcal{C}_1 \in \overline{\Gamma} \cup \mathfrak{D}$, $\dim(\mathcal{C}_1) > 1$, and some code $\mathcal{C}_2 \in \mathfrak{C}$.*

The dual form of Theorem 2.5(a) in [1] shows that the following code families are $\mathfrak{D}$-regular:[1]

- regular codes, with $\mathfrak{D} = \{R_{10}\}$
- codes having no minor equivalent to $\mathcal{H}_7$, with $\mathfrak{D} = \{\mathcal{H}_7^\perp, R_{10}\}$
- codes having no minor equivalent to $\mathcal{H}_7^\perp$, with $\mathfrak{D} = \{\mathcal{H}_7, R_{10}\}$

Theorem 2.5(a) in [1] is essentially a more refined version of Seymour's decomposition theorem (Theorem 7).

We can now state our main result which, by the above remark, includes Theorem 1 as a special case.

Theorem 12. *For any finite code family $\mathfrak{D}$, the family of $\mathfrak{D}$-regular codes is not asymptotically good.*

The proof goes as follows. Let $\mathfrak{C}$ be a $\mathfrak{D}$-regular family of codes for some finite code family $\mathfrak{D}$. Without loss of generality, we may assume that $\mathfrak{D}$ is minor-closed. For $r \in (0, 1)$, define N_r to be the least positive integer such that for all $n > N_r$,

$$0 < \frac{1}{\log(1 + r - 2/n)} < \frac{2}{\log(1 + r)} \quad \text{and} \quad 0 < \frac{1}{r - 2/n} < \frac{2}{r}.$$

Note that since $\lim_{n\to\infty} 1/\log(1 + r - 2/n) = 1/\log(1 + r)$, and $\lim_{n\to\infty} 1/(r - 2/n) = 1/r$, such an N_r does exist. Now, define

$$d_{\max}(r, \mathfrak{D}) = \max\{d(\mathcal{C}) : \mathcal{C} \in \mathfrak{C} \text{ and has length at most } N_r, \text{ or } \mathcal{C} \in \mathfrak{D}\}.$$

Note, in particular, that since $\mathfrak{D}$ is taken to be minor-closed, we have $d_{\max}(r, \mathfrak{D}) \geq d_{\max}(\mathfrak{D})$, where $d_{\max}(\mathfrak{D})$ is as defined in the proof of Lemma 11.

We now have the definitions needed to state the next result, which shows that codes in $\mathfrak{C}$ cannot have both dimension and minimum distance growing linearly with codelength. It is clear that Theorem 12 follows directly from this result.

[1]The dual version of Theorem 2.5(a) does not explicitly assert that the 3-connected code $\mathcal{C}_1 \in \overline{\Gamma} \cup \mathfrak{D}$ can be taken to have dimension larger than 1, but this can be readily added to the statement of that theorem.

Lemma 13. *Let $r \in (0,1)$. If $\mathcal{C} \in \mathfrak{C}$ is an $[n,k,d]$ code with $k/n > r$, then*

$$d \leq \max\left\{ d_{\max}(r,\mathfrak{D}),\ 4/r,\ \frac{8\log n}{\log(1+r)} \right\}. \tag{3}$$

Proof. From the definition of $d_{\max}(r,\mathfrak{D})$, and the bounds in (1) and (2), it is obvious that the statement of the lemma holds for all codes in $\overline{\Gamma} \cup \mathfrak{D} \cup (\overline{\Gamma} + \mathfrak{D})$. The proof that the statement holds for all codes in $\mathfrak{C}$ is by induction on codelength for a fixed $r \in (0,1)$.

So, fix an $r \in (0,1)$. If n_0 is the smallest length of a non-trivial code in $\mathfrak{C}$, then a length-n_0 code in $\mathfrak{C}$ cannot be decomposed into smaller codes, and so must be in $\overline{\Gamma} \cup \mathfrak{D}$. Therefore, the statement of the lemma holds for the base case of length-n_0 codes.

Now, suppose that for some $n > n_0$, (3) holds for all codes $\mathcal{C}' \in \mathfrak{C}$ of length $n' \leq n-1$ and rate larger than r. Let $\mathcal{C} \in \mathfrak{C}$ be a $[n,k,d]$ code with $k/n > r$. If $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$ for some (non-empty) codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $\mathfrak{C}$, then at least one of $\mathcal{C}_1$ and $\mathcal{C}_2$ has rate larger than r, and so (3) holds for $\mathcal{C}$ by the induction hypothesis. We may thus assume that $\mathcal{C}$ is connected.

If $\mathcal{C} \in \overline{\Gamma} \cup \mathfrak{D} \cup (\overline{\Gamma} + \mathfrak{D})$, there is nothing further to be proved; so we will henceforth assume that this is not the case. In particular, by Definition 5, $\mathcal{C}$ may be assumed to be either $\mathcal{C}_1 \oplus_2 \mathcal{C}_2$ or $\mathcal{C}_1 \overline{\oplus}_3 \mathcal{C}_2$ for some 3-connected $[n_1,k_1]$ code $\mathcal{C}_1 \in \overline{\Gamma} \cup \mathfrak{D}$, with $k_1 > 1$, and some $[n_2,k_2]$ code $\mathcal{C}_2 \in \mathfrak{C}$. Furthermore, $\mathcal{C}_2 \notin \Gamma \cap \text{co-}\Gamma$, since $\mathcal{C} \notin \overline{\Gamma} \cup (\overline{\Gamma} + \mathfrak{D})$. In particular, this means that $k_2 \geq 3$, since if $k_2 \leq 2$, then it would follow from Theorem 2 that $\mathcal{C}_2$ is both graphic and cographic.

We consider the case $\mathcal{C} = \mathcal{C}_1 \oplus_2 \mathcal{C}_2$ first. By Proposition 4(b), we have $d \leq \min\{d(\mathcal{C}_1'), d(\mathcal{C}_2')\}$, where $\mathcal{C}_1' = \mathcal{C}_1 \setminus \{n_1\}$ and $\mathcal{C}_2' = \mathcal{C}_2 \setminus \{1\}$. Since $\mathcal{C}_1'$ is a minor of $\mathcal{C}_1$, and $\overline{\Gamma} \cup \mathfrak{D}$ is minor-closed, we have $\mathcal{C}_1' \in \overline{\Gamma} \cup \mathfrak{D}$. Similarly, $\mathcal{C}_2'$ is in the minor-closed family $\mathfrak{C}$. Furthermore, note that for $i = 1,2$, $\mathcal{C}_i'$ is an $[n_i', k_i']$ code, where $n_i' = n_i - 1$ and $k_i' = k_i - 1$. Thus, $n = n_1' + n_2'$, and from Proposition 4(a), we also have $k = k_1 + k_2 - 1 = k_1' + k_2' + 1$.

Now, if $k_1'/n_1' > r$, then the statement of the lemma holds for $\mathcal{C}_1'$, since it is in $\overline{\Gamma} \cup \mathfrak{D}$. Similarly, if $k_2'/n_2' > r$, then the statement of the lemma holds for $\mathcal{C}_2'$ by the induction hypothesis, since $n_2' \leq n-1$. In both cases, (3) holds for $\mathcal{C}$, as we have $d(\mathcal{C}) \leq \min\{d(\mathcal{C}_1'), d(\mathcal{C}_2')\}$ and $n_i' < n$.

So, we are left with the situation when $k_i'/n_i' \leq r$ for $i = 1,2$. But in this case, since $k/n = (k_1' + k_2' + 1)/(n_1' + n_2') > r$, we must have $k_1'/n_1' > r - 1/n_1'$; otherwise, we would have $k_2' > (n_1'+n_2')r - 1 - k_1' \geq (n_1'+n_2')r - 1 - (rn_1' - 1) = rn_2'$, which would mean that $k_2'/n_2' > r$. If $\mathcal{C}_1' \in \mathfrak{D}$ or $n_1' \leq N_r$, then $d(\mathcal{C}_1') \leq d_{\max}(r,\mathfrak{D})$. Otherwise, $\mathcal{C}_1'$ is either graphic or cographic, with $n_1' > N_r$, and so, by Lemmas 8 and 9, and the definition of N_r,

$$\begin{aligned} d(\mathcal{C}_1') &\leq \max\left\{ \frac{2}{r - 1/n_1'},\ \frac{4\log n_1'}{\log(1+(r-1/n_1'))} \right\} \\ &\leq \max\left\{ \frac{2}{r - 2/n_1'},\ \frac{4\log n_1'}{\log(1+(r-2/n_1'))} \right\} \\ &\leq \max\left\{ \frac{4}{r},\ \frac{8\log n_1'}{\log(1+r)} \right\}. \end{aligned}$$

Since $d \leq d(\mathcal{C}_1')$ and $n_1' < n$, we have that (3) holds for $\mathcal{C}$.

Finally, we deal with the case when $\mathcal{C} = \mathcal{C}_1 \overline{\oplus}_3 \mathcal{C}_2$. The approach is essentially the same as that in the 2-sum case. This time, we define $\mathcal{C}_1' = \mathcal{C}_1 \setminus \{n_1 - 2, n_1 - 1, n_1\}$ and $\mathcal{C}_2' = \mathcal{C}_2 \setminus \{1,2,3\}$. For $i = 1,2$, we now find that $\mathcal{C}_i'$ is an $[n_i', k_i']$ code, where $n_i' = n_i - 3$ and $k_i' = k_i - 2$. Thus, $n = n_1' + n_2'$, and via Proposition 6(a), $k = k_1' + k_2' + 2$. Furthermore, $\mathcal{C}_1$ is 3-connected and $k_2 \geq 3$ (shown above), and so, by Proposition 6(b), we have $d(\mathcal{C}) \leq \min\{d(\mathcal{C}_1'), d(\mathcal{C}_2')\}$. If either k_1'/n_1' or k_2'/n_2' is larger than r, then (3) holds for $\mathcal{C}$, either because $\mathcal{C}_1' \in \overline{\Gamma} \cup \mathfrak{D}$ or because of the induction hypothesis. So suppose that $k_i'/n_i' \leq r$ for $i = 1,2$. Since $k/n = (k_1' + k_2' + 1)/(n_1' + n_2') > r$, we must have $k_1'/n_1' > r - 2/n_1'$; otherwise, we would obtain $k_2'/n_2' > r$. If $\mathcal{C}_1' \in \mathfrak{D}$ or $n_1' \leq N_r$,

then $d(\mathcal{C}_1') \leq d_{\max}(r, \mathfrak{D})$; otherwise, $\mathcal{C}_1'$ is either graphic or cographic with $n_1' > N_r$, and so, by Lemmas 8 and 9, and the definition of N_r, we have

$$d(\mathcal{C}_1') \leq \max\left\{\frac{2}{r-2/n_1'},\ \frac{4\log n_1'}{\log(1+(r-2/n_1'))}\right\} \leq \max\left\{\frac{4}{r},\ \frac{8\log n_1'}{\log(1+r)}\right\}.$$

Since $d \leq d(\mathcal{C}_1')$, and $n_1' < n$, we see that (3) holds for $\mathcal{C}$. The proof of the lemma is now complete. □

REFERENCES

[1] M. Grötschel and K. Truemper, "Decomposition and optimization over cycles in binary matroids," *J. Combin. Theory Series B*, vol. 46, pp. 306–337, 1989.

[2] N. Kashyap, "A decomposition theory for binary linear codes," *IEEE Trans. Inform. Theory*, vol. 54, no. 7, pp. 3035–3058, July 2008.

[3] J.G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, UK, 1992.

[4] P.D. Seymour, "Decomposition of regular matroids," *J. Combin. Theory, Series B*, vol. 28, pp. 305–359, 1980.

[5] K. Truemper, *Matroid Decomposition*, Academic Press, San Diego, 1992.

[6] W.T. Tutte, "Matroids and graphs," *Trans. Amer. Math. Soc.*, vol. 90, pp. 527–552, 1959.