Journal of Combinatorial Theory, Series A **100**, 232–249 (2002)
doi:10.1006/jcta.2002.3290

Asymmetric Binary Covering Codes

Joshua N. Cooper[1] and Robert B. Ellis

Department of Mathematics, University of California, San Diego, 9500 Gilman Drive 0112, La Jolla, California 92093-0112
E-mail: jcooper@math.ucsd.edu; rellis@math.ucsd.edu

and

Andrew B. Kahng

Department of Computer Science and Engineering, University of California, San Diego, La Jolla, California
E-mail: abk@cs.ucsd.edu

Received January 28, 2002

An asymmetric binary covering code of length n and radius R is a subset $\mathscr{C}$ of the n-cube Q_n such that every vector $x \in Q_n$ can be obtained from some vector $c \in \mathscr{C}$ by changing at most R 1's of c to 0's, where R is as small as possible. $K^+(n, R)$ is defined as the smallest size of such a code. We show $K^+(n, R) \in \Theta(2^n/n^R)$ for constant R, using an asymmetric sphere-covering bound and probabilistic methods. We show $K^+(n, n-\bar{R}) = \bar{R}+1$ for constant coradius $\bar{R}$ iff $n \geqslant \bar{R}(\bar{R}+1)/2$. These two results are extended to near-constant R and $\bar{R}$, respectively. Various bounds on K^+ are given in terms of the total number of 0's or 1's in a minimal code. The dimension of a minimal asymmetric linear binary code ($[n, R]^+$-code) is determined to be $\min\{0, n-R\}$. We conclude by discussing open problems and techniques to compute explicit values for K^+, giving a table of best-known bounds.
Key Words: covering code; binary code; minimal code; probabilistic method.

1. INTRODUCTION

Suppose we wish to have a small set of binary n-vectors with the property that *every* binary n-vector is no more than R bit flips from one of them. This is the classical question of finding "covering codes." Recent surveys of results on covering codes appear in [4, 6], and earlier important results appear in [5, 8]. The topic of covering codes continues to be an active area of

[1] To whom correspondence should be addressed.

research, and the interested reader is referred to [9] for a comprehensive bibliography of the subject.

Let Q_n be the set of binary n-vectors $\{x = (x_1, x_2, \dots, x_n): x_i \in \{0, 1\}\}$ with algebraic structure inherited from the vector space $\mathbb{F}_2^n$ and the partial ordering inherited from the boolean lattice (i.e., $x \preccurlyeq y$ if $x_i \leqslant y_i$ for all $1 \leqslant i \leqslant n$). We denote the "top" and "bottom" elements, i.e., $(1, \dots, 1)$ and $(0, \dots, 0)$, by $\hat{1}$ and $\hat{0}$, respectively. Define the *weight*, or *level*, of $x \in Q_n$ as $w(x) = \sum_{i=1}^{n} x_i$, where each coordinate is treated as an ordinary integer (equivalently, $w(x)$ is the number of ones in x). Define the Hamming distance between x and y as $d(x, y) = w(x + y)$. The *undirected ball* in Q_n with center x and radius R, denoted by $B_n(x, R)$, is the set $\{y \in Q_n: d(x, y) \leqslant R\}$. The *covering radius* of a set $\mathscr{C} \subseteq Q_n$ is the smallest integer $R \geqslant 0$ such that $Q_n = \bigcup_{c \in \mathscr{C}} B_n(c, R)$. The ordinary definition of a binary covering code, which for our purposes we refer to as a *symmetric binary covering code* of length n and radius R, or more simply an (n, R)-code, is a set of "codewords" $\mathscr{C} \subseteq Q_n$ with covering radius R. We use $K(n, R)$ to denote the minimum size of any (n, R)-code.

We now consider the additional restriction of requiring the bit flips used to go from a vector to its covering codeword to be in only one direction. This restriction arises in a problem of layout data compression in VLSI design which motivated the present work [7]. Data encoding the placement of certain metal features on a microchip can be transmitted with at most R errors per n bits using a covering code, except that metal may only be removed (to an extent controlled by R) and not added, so as to avoid causing a short circuit. This simple variation on ordinary ("symmetric") covering codes opens up a world of questions, with many of the answers quite different from the symmetric case. The dual problem of "unidirectional" error-correcting/detecting codes has been studied in [10–12].

The extra restriction is now formalized in the definition of an asymmetric covering code. The *upward directed ball* in Q_n with center x and radius R is $B_n^+(x, R) = B_n(x, R) \cap \{y \in Q_n: x \preccurlyeq y\}$, and the corresponding *downward directed ball* is $B_n^-(x, R) = B_n(x, R) \cap \{y \in Q_n: y \preccurlyeq x\}$. We write $b_n^+(x, R)$ and $b_n^-(x, R)$ for the sizes of the directed balls $B_n^+(x, R)$ and $B_n^-(x, R)$, respectively. We sometimes instead say $b_n^+(l, R)$ or $b_n^-(l, R)$, where l is the weight of x, since b_n^+ and b_n^- depend only on the weight of the ball's center. Indeed, we have

$$\begin{aligned} b_n^+(l, R) = b_n^-(n - l, R) &= \sum_{j=0}^{R} \binom{n-l}{j} \leqslant \sum_{j=0}^{R} \binom{n-l}{j} \binom{R}{R-j} \\ &= \binom{n-l+R}{R}. \end{aligned} \tag{1}$$

A set $\mathscr{C} \subseteq Q_n$ *downward R-covers* Q_n provided that $Q_n = \bigcup_{c \in \mathscr{C}} B_n^-(c, R)$, and the *asymmetric covering radius* of $\mathscr{C}$ is the smallest R for which $\mathscr{C}$ downward R-covers Q_n. We define an *asymmetric binary covering code* of length n and radius R, or more simply an $(n, R)^+$-code, to be any set $\mathscr{C} \subseteq Q_n$ with covering radius R. We sometimes refer to the *coradius* $\bar{R} := n - R$ of an $(n, R)^+$-code when R is large. Our main object of study is the function $K^+(n, R)$, defined to be the minimum size of any $(n, R)^+$-code.

Finally, denote the concatenation of two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_m)$ by $(x|y) = (x_1, \ldots, x_n, y_1, \ldots, y_m)$, in precisely the same way as it is defined for symmetric codes. The *direct sum* of two sets X and Y is $X \oplus Y := \{(x|y) : x \in X,\ y \in Y\}$. Note that if $\mathscr{C}$ is an $(n_1, R_1)^+$-code and $\mathscr{C}'$ is an $(n_2, R_2)^+$-code, then $\mathscr{C} \oplus \mathscr{C}'$ is an $(n_1 + n_2, R_1 + R_2)^+$-code, and so

$$K^+(n, R) \leqslant K^+(n_1, R_1) K^+(n - n_1, R - R_1). \tag{2}$$

We will use this observation several times in the course of our discussion.

In this paper, we explain several substantive differences and similarities between symmetric and asymmetric binary covering codes, and offer directions for further investigation. Section 2 gives the exact asymptotic order of magnitude of the size of minimal codes with constant radius and gives exact asymptotics in the case of constant coradius. The bounds we provide are then used to derive somewhat weaker bounds in a completely general setting. The topic of Section 3 is the increase that the size of a minimal code experiences when its length or radius is incremented or decremented, respectively. We tackle linear asymmetric codes in Section 4—a surprisingly simple matter, given the complexity of the issue in the symmetric case—and we finish with several open problems and a table of our best known bounds in Section 5.

2. ASYMPTOTIC BOUNDS

We can achieve a lower bound for the asymptotic order of magnitude of $K^+(n, R)$ for constant R by considering a variant of the traditional sphere-covering bound. Sphere-covering lower bounds are achieved by examining the size of the (directed or undirected) balls of a given radius centered at each vector. The straightforward sphere-covering bound in the symmetric case appears as [6, Theorem 6.1.2], which we state here for completeness, and then extend to the asymmetric case.

THEOREM 1 (Sphere-Covering Bound)

$$K(n,R) \geqslant \left\lceil \frac{2^n}{\sum_{j=0}^{R} \binom{n}{j}} \right\rceil. \tag{3}$$

THEOREM 2 (Asymmetric Sphere-Covering Bound). *Let* $0 \leqslant R \leqslant n$. *Then*

$$K^+(n,R) \geqslant \left\lceil \sum_{l=0}^{n} \frac{\binom{n}{l}}{\sum_{j=0}^{R} \binom{\min(n,l+R)}{j}} \right\rceil. \tag{4}$$

Proof. For any $(n,R)^+$-code $\mathscr{C}$, we may write

$$|\mathscr{C}| = \sum_{c \in \mathscr{C}} 1 = \sum_{c \in \mathscr{C}} \sum_{v \in B_n^-(c,R)} b_n^-(w(c),R)^{-1}.$$

Switching the order of summation yields

$$|\mathscr{C}| = \sum_{v \in Q_n} \sum_{c \in B_n^+(v,R) \cap \mathscr{C}} b_n^-(w(c),R)^{-1}.$$

For a vector v of weight l, the largest directed ball of radius R that could contain it is centered at a vector of weight $l+R$ and has size $\sum_{j=0}^{R} \binom{l+R}{j}$. However, if $l+R > n$, then the largest ball that could contain v is the one which is centered at $\hat{1}$. Therefore, since every vector in Q_n must be covered by at least one $c \in \mathscr{C}$,

$$\begin{aligned} |\mathscr{C}| &\geqslant \sum_{v \in Q_n} \sum_{c \in B_n^+(v,R) \cap \mathscr{C}} \left(\sum_{j=0}^{R} \binom{\min(n, w(v)+R)}{j} \right)^{-1} \\ &\geqslant \sum_{v \in Q_n} \left(\sum_{j=0}^{R} \binom{\min(n, w(v)+R)}{j} \right)^{-1}. \end{aligned}$$

Noting that $\binom{n}{l}$ vertices have weight l gives the desired result. ∎

The desired lower bound for $K^+(n,R)$ is determined by bounding the denominator of each term in (4). Using the bound on ball size from (1), for all $0 \leqslant l \leqslant n$ and a fixed R,

$$b_n^-(l,R) \leqslant \binom{n+R}{R} \in O(n^R).$$

Therefore, we find the following as an immediate consequence of Theorem 2.

COROLLARY 3. *Fix* $R \geqslant 0$. *Then*

$$K^{+}(n, R) \in \Omega\left(\frac{2^{n}}{n^{R}}\right).$$

We can count more carefully than we did in Theorem 2 by specifying a system of inequalities that the code must satisfy. For an arbitrary $(n, R)^{+}$-code, define the sequence $(a_0, a_1, \ldots, a_n)$ by letting a_l be the number of codewords of weight l. Whenever necessary, define $a_{n+1} = \cdots = a_{n+R} = 0$. We have the following lemma.

LEMMA 4. *Let* $\mathscr{C}$ *be an* $(n, R)^{+}$*-code. Then the number of codewords* a_l *of weight* l *must satisfy*

$$a_l \geqslant \binom{n}{l} - \sum_{j=1}^{R} a_{l+j} \binom{l+j}{j}. \tag{5}$$

Proof. There are $\binom{n}{l}$ vertices on level l to be covered. At most $a_{l+j}\binom{l+j}{j}$ of these points can be R-covered by the a_{l+j} codewords of weight $l+j$. The rest must be included as codewords themselves. ∎

In fact, (5) must hold for all $0 \leqslant l \leqslant n$ for all $(n, R)^{+}$-codes. Therefore, we may construct an integer program based on these restrictions to provide another lower bound for $K^{+}(n, R)$. This is what was done (with some minor refinements) to find most of the lower bounds presented in the table at the end of this paper.

PROPOSITION 5. *Let* $IP^{+}(n, R)$ *be the result of the following integer program*:

$$\text{Minimize} \quad \sum_{l=0}^{n} a_l$$

$$\text{subject to} \quad \sum_{j=0}^{R} a_{l+j} \binom{l+j}{j} \geqslant \binom{n}{l}, \qquad \textit{for } 0 \leqslant l \leqslant n, \tag{6}$$

and

$$a_l \geqslant 0, \ \text{integer}, \qquad \text{for } 0 \leqslant l \leqslant n.$$

Then $K^+(n,R) \geqslant IP^+(n,R)$. *Furthermore, this bound is at least as good as the asymmetric sphere-covering bound* (4).

Proof. We have already established that the program yields a lower bound for $K^+(n,R)$. It remains to show that it is at least as good as (4). Let $(a_0,\ldots,a_n)$ be a solution vector which achieves $IP^+(n,R)$. Applying the conventions that $b_n^-(l,R)=b_n^-(n,R)$ when $l \geqslant n$, all indices vary over those integers not excluded explicitly, and $a_l=0$ for $l<0$ and $l>n$, we have

$$\sum_l a_l = \sum_l \sum_{i\leqslant R} \frac{a_l\binom{l}{i}}{b_n^-(l,R)} = \sum_{l'} \sum_{i\leqslant R} \frac{a_{l'+i}\binom{l'+i}{i}}{b_n^-(l'+i,R)}$$

by making the substitution $l'=l-i$. Then, using the fact that downward ball sizes are monotone increasing in the weight of their centers, and applying (6),

$$\sum_l a_l \geqslant \sum_{l'} \sum_{i\leqslant R} \frac{a_{l'+i}\binom{l'+i}{i}}{b_n^-(l'+R,R)} \geqslant \sum_{l'} \frac{\binom{n}{l'}}{b_n^-(l'+R,R)}$$

which is the asymmetric sphere covering bound. ∎

Note that the IP is relatively small, since its coefficient matrix is just $(n+1)\times(n+1)$.

2.1. *Asymptotic Order of Magnitude for Small Radius*

Clearly, $K^+(n,0)=2^n$ since all 0-balls contain only their centers. For positive R, however, the issue is much more complicated. In particular, we wish to understand the growth of $K^+(n,R)$ in n for constant R. The lower bound given by Corollary 3 says that the density $|\mathscr{C}|/2^n$ of a minimal $(n,R)^+$-code $\mathscr{C}$ is $\Omega(n^{-R})$; the probabilistic arguments given in this section show that this is, in fact, achievable.

Define a *patched asymmetric covering code of radius* R, or a patched $(n,R)^+$-code, to be a pair (S,T) with $S,T\subset Q_n$ such that S has covering radius R with respect to covering only $Q_n\backslash T$. Thus, every vector in the cube is either in $B_n^-(s,R)$ for some $s\in S$ or in the "patch" T. We say that the δ-weight of the patched asymmetric covering code (S,T) is $|S|+\delta|T|$, and define $p(n,R,\delta)$ to be the minimum δ-weight over all patched $(n,R)^+$-codes.

For a given patched $(n, R)^+$-code (S, T) and a $(k, R)^+$-code $\mathscr{C}$, we define the *semi-direct sum* of (S, T) and $\mathscr{C}$, denoted by $(S, T) \boxplus \mathscr{C}$, to be $(S \oplus Q_k) \cup (T \oplus \mathscr{C})$. It is easy to verify that $(S, T) \boxplus \mathscr{C}$ is an $(n+k, R)^+$-code. In the next two propositions, we will generate a small cover for Q_{2n} first by showing in Proposition 6 the existence of a patched $(n, R)^+$-code (S, T) with low δ-weight, and then by building in Proposition 7 a $(2n, R)^+$-code $\mathscr{C}$ from the semi-direct sum of the patched $(n, R)^+$-code and a small $(n, R)^+$-code found inductively.

PROPOSITION 6. *Let $R \geqslant 0$ be fixed. For some absolute constant $\alpha_R > 0$ and any $\delta > 0$,*

$$p(n, R, \delta) \leqslant \frac{\alpha_R 2^n}{n^R} (\max\{\log(\delta n^R/\alpha_R), 0\} + 1).$$

Proof. A standard argument (pointed out by Bell [3]) permits us to choose α_R to be the least real number so that for all positive integers n,

$$\sum_{j=0}^{n} \binom{n}{j} b_n^+(j, R)^{-1} \leqslant \alpha_R \frac{2^n}{n^R}.$$

If $\delta < \alpha_R/n^R$, then choosing T be all of Q_n yields the desired result. Thus, we may assume $\delta \geqslant \alpha_R/n^R$. Randomly choose a patched asymmetric cover (S, T) as follows. Let $p_j = \min\{\log(\delta n^R/\alpha_R) b_n^+(j, R)^{-1}, 1\}$ for $j = 0, \ldots, n-1$, and let $p_n = 1$. For each vector v in the cube, add it to S with probability $p_{w(v)}$. Then, add all the uncovered points to T. The expected δ-weight of (S, T) is, by linearity of expectation,

$$\mathbf{E}(|S|) + \delta \mathbf{E}(|T|) \leqslant \sum_{j=0}^{n} \binom{n}{j} p_j + \delta \sum_{v \in Q_n} \mathbf{P}(v \text{ is uncovered}).$$

The probability that a vector v is uncovered is the product, over each of the $b_n^+(v, R)$ vertices that could cover v, of the probability that each vertex is not chosen. Thus,

$$\mathbf{P}(v \text{ is uncovered}) = \prod_{u \in B_n^+(v,R)} (1 - p_{w(u)}) \leqslant (1 - p_{w(v)})^{b_n^+(v,R)}$$

and we have (using the formula $(1-1/x)^x \leqslant e^{-1}$ which is valid for all $x \geqslant 1$)

$$\begin{aligned}\mathbf{E}(|S|)+\delta\mathbf{E}(|T|) &\leqslant \log\left(\frac{\delta n^R}{\alpha_R}\right)\sum_{j=0}^{n}\frac{\binom{n}{j}}{b_n^+(j,R)}+\delta\sum_{j=0}^{n}\binom{n}{j}(1-p_j)^{b_n^+(j,R)}\\ &\leqslant \log\left(\frac{\delta n^R}{\alpha_R}\right)\alpha_R\frac{2^n}{n^R}+\delta\sum_{j=0}^{n}\binom{n}{j}\frac{\alpha_R}{\delta n^R}\\ &\leqslant \alpha_R\frac{2^n}{n^R}\left(\log\left(\frac{\delta n^R}{\alpha_R}\right)+1\right),\end{aligned}$$

and so there exists a patched cover of the desired δ-weight. ∎

This leads immediately to the following.

PROPOSITION 7. *For each $R \geqslant 0$, there exists a $\beta_R > 0$ such that for every nonnegative integer m,*

$$K^+(2^m,R) \leqslant \frac{\beta_R 2^{2^m}}{2^{mR}}.$$

Proof. If $R=0$, the result is trivial, so we may assume that $R>0$. We proceed by induction on m. We require the constant β_R defined as

$$\beta_R = \max\{\tfrac{1}{2}, \min\{x{:}x \geqslant \alpha_R \text{ and } x \geqslant 2^R\alpha_R(\log(x/\alpha_R)+1)\}\}.$$

The statement certainly holds for $m=0$, since $K^+(1,R)=1$. Assume it is true for m. We construct a cover for $Q_{2^{m+1}}$ by taking the semi-direct sum of a patched $(2^m,R)^+$-code (S,T) achieving $p(2^m,R,K^+(2^m,R)/2^{2^m})$ and a minimal $(2^m,R)^+$-code. The result is a $(2^{m+1},R)^+$-code of size

$$|(S,T)\boxplus\mathscr{C}| = |S|2^{2^m}+|T|K^+(2^m,R) = 2^{2^m}p\left(2^m,R,\frac{K^+(2^m,R)}{2^{2^m}}\right).$$

By the previous proposition, then,

$$K^+(2^{m+1},R) \leqslant 2^{2^m}\alpha_R\frac{2^{2^m}}{2^{mR}}\left(\max\left\{\log\left(\frac{K^+(2^m,R)2^{mR}}{\alpha_R 2^{2^m}}\right),0\right\}+1\right).$$

If we apply the inductive hypothesis to bound $K^+(2^m,R)$, we find that

$$K^+(2^{m+1},R) \leqslant \frac{2^{2^{m+1}}}{(2^{m+1})^R}2^R\alpha_R\left(\max\left\{\log\left(\frac{\beta_R}{\alpha_R}\right),0\right\}+1\right) \leqslant \beta_R\frac{2^{2^{m+1}}}{(2^{m+1})^R}$$

by the choice of β_R. ∎

A straightforward application of the direct sum formula (2) allows us to generalize this result to all nonnegative integers n from those which are powers of 2.

COROLLARY 8. *Let $R \geqslant 0$ be fixed. For some absolute constant $\gamma_R > 0$ and every integer n,*

$$K^+(n, R) \leqslant \frac{\gamma_R 2^n}{n^R}.$$

Proof. Set $\gamma_R = 2^R \beta_R$, and let $m = \lfloor \log_2(n) \rfloor$. Then by the direct sum formula,

$$\begin{aligned} K^+(n, R) &\leqslant K^+(2^m, R) K^+(n - 2^m, 0) = K^+(2^m, R) 2^{n-2^m} \\ &\leqslant \frac{\beta_R 2^n}{2^{mR}} \leqslant \frac{2^R \beta_R 2^n}{n^R} = \frac{\gamma_R 2^n}{n^R}, \end{aligned}$$

since $n/2^m \leqslant 2$. ∎

This, combined with Corollary 3, gives us the following characterization of the asymptotic behavior of $K^+(n, R)$ for R constant.

THEOREM 9. *For a fixed $R \geqslant 0$, $K^+(n, R) \in \theta(2^n / n^R)$.*

The probabilistic technique used above, reminiscent of the so-called "deletion method" (see, for instance [1]), applies in a more general setting, although the results are significantly weaker. The following proof is essentially a very simple version of the proof of Proposition 6, with $\delta = 1$, but we include it because the bound achieved is of independent interest. Define $v(n, R)$ by

$$v(n, R) = \sum_{j=0}^{n} \frac{\binom{n}{j}}{b_n^+(j, R)}.$$

Then we have the following, analogous to [6, Theorem 12.1.2].

PROPOSITION 10. *For any $n, R \geqslant 0$, $K^+(n, R) \leqslant (n \log 2 + 1) v(n, R)$.*

Proof. We construct an $(n, R)^+$-code probabilistically. Add vectors $x \in Q_n$ to $\mathscr{C}$ independently with probability

$$p_{w(x)} = \min\left\{1, \frac{\log(2^n / v(n, R))}{b_n^+(w(x), R)}\right\},$$

and then add to $\mathscr{C}$ all points not covered by directed balls of radius R centered at the chosen x's. Just as in the proof of Proposition 6, the resulting code has expected size

$$\begin{aligned}\mathbf{E}(|\mathscr{C}|) &\leqslant \sum_{j=0}^{n}\binom{n}{j}p_j + \sum_{j=0}^{n}\binom{n}{j}(1-p_j)^{b_n^+(j,R)}\\ &\leqslant (\log(2^n/v(n,R))+1)v(n,R) \leqslant (n\log 2+1)v(n,R).\end{aligned}$$

Therefore, there exists an $(n,R)^+$-code of at most this size. ∎

The preceding proposition can be used to achieve upper bounds in specific cases comparable to those known for symmetric covering codes. For example, a routine calculation gives that $K^+(n,R)$ is within a multiplicative factor of $O(n)$ of the asymmetric sphere-covering lower bound whenever $R \in O(\sqrt{n})$.

2.2. *Asymptotics for Large Radius*

Since $R \geqslant n$ implies $K^+(n,R)=1$, another region of interest in the space of possible n's and R's is the case of constant (and positive) coradius $\bar{R}=n-R$. The very precise asymptotics we achieve for this case also permit a much rougher analysis of $K^+(n,R)$ for general n and R, with the best results occurring when R is close to n.

A few trivial values are immediate. $K^+(n,n)=1$, since the downward n-ball at $\hat{1}$ covers everything, and $K^+(n,n-1)=2$ by considering the code $\mathscr{C}=\{(1,1,\ldots,1),(0,1,\ldots,1)\}$. In fact, for fixed $\bar{R}$, the sequence $\{K^+(n,n-\bar{R})\}_n$ converges to $\bar{R}+1$ in a manner we now characterize.

LEMMA 11. *$K^+(n,n-\bar{R}) \leqslant \bar{R}+1$ for $n \geqslant \bar{R}(\bar{R}+1)/2$ and $\bar{R} \geqslant 0$.*

Proof. Construct the $(n,n-\bar{R})^+$-code

$$\mathscr{C}=\{(1,1,1,1,\ldots,1),(0,1,1,1,\ldots,1),(1,0,0,1,\ldots,1),\ldots\}$$

of size $\bar{R}+1$, where the $(i+1)$th codeword has i consecutive 0's starting in position $(i-1)i/2+1$. Having $n \geqslant \bar{R}(\bar{R}+1)/2$ is required in order for there to be enough positions to place all the 0's. To see that $\mathscr{C}$ is an $(n,n-\bar{R})^+$-code, let $x \in Q_n$. If $w(x) \geqslant \bar{R}$, x is covered by $(1,\ldots,1)$. Otherwise, x could only avoid being covered by the $w(x)+1$ codewords on levels $(n-\bar{R}+w(x)),\ldots,(n-\bar{R})$ by having, for each codeword $c \in \mathscr{C}$ on these levels, a 1 in a position where c has a 0. This is impossible, since x has $w(x)$ 1's and the positions of 0's in the $w(x)+1$ codewords are disjoint. ∎

The same set $\mathscr{C}$ is a symmetric $(n, n-\bar{R})$-code, and therefore yields an upper bound on $K(n, n-\bar{R})$ for $n \geqslant \bar{R}(\bar{R}+1)/2$. This bound is not tight in the symmetric case, but is in fact tight in the asymmetric case, due to the additional structure imposed by requiring vectors to be covered by codewords above them. (In fact, $K(n, R) = 2$ whenever $R+1 \leqslant n \leqslant 2R+1$.) We summarize the behavior of $K^+(n, n-\bar{R})$ in the theorem below. Before we proceed, however, we have the following definition and lemma.

For a set of vectors $\mathscr{C} \subset Q_n$ and an index $i \in \{1, \ldots, n\}$, define $\mathscr{C}^i \subset Q_{n-1}$, the *contraction of* $\mathscr{C}$ *at* i, to be the set of points of $\mathscr{C}$ with a "1" at position i, projected into Q_{n-1} by deletion of that bit.

LEMMA 12. *If $\mathscr{C}$ downward R-covers Q_n, then for each $i \in \{1, \ldots, n\}$, $\mathscr{C}^i$ downward R-covers Q_{n-1}.*

Proof. Let Q_n' be the set of points in Q_n with a "1" at coordinate i. Note that if $x \in Q_n'$, $y \in Q_n$, and $y \succ x$, then $y \in Q_n'$. Thus, the union of all the downward-directed Hamming balls of radius R centered at the points of $\mathscr{C} \cap Q_n'$ must contain Q_n'. If we project Q_n' onto Q_{n-1} in the natural way, then the image of $\mathscr{C} \cap Q_n'$ downward R-covers Q_{n-1}. ∎

THEOREM 13. *$K^+(n, n-\bar{R}) \geqslant \bar{R}+1$ for $n \geqslant 1$ and $\bar{R} \geqslant 0$, with equality when $n \geqslant n_{\bar{R}} := \bar{R}(\bar{R}+1)/2$. Furthermore, $n_{\bar{R}}$ is the least integer n for which equality holds.*

Proof. First, we show by induction on $\bar{R}$ that if $\mathscr{C}$ downward $(n-\bar{R})$-covers Q_n, then there are at least x codewords of $\mathscr{C}$ with weight $< n-\bar{R}+x$, for all nonnegative $x \leqslant \bar{R}$. This is certainly true for $\bar{R} = 0$; assume it is true for $\bar{R}-1$. Now consider a general $\bar{R} > 0$. There is at least one codeword c at or below level $n-\bar{R}$, since we must cover the vertex $\hat{0}$. Because $\bar{R} > 0$, we may choose some coordinate i where c has a zero. Lemma 12 gives that the contraction $\mathscr{C}^i$ downward $((n-1)-(\bar{R}-1))$-covers Q_{n-1}. By induction, there are at least x points in $\mathscr{C}^i$ with weight $< (n-1)-(\bar{R}-1)+x = n-\bar{R}+x$, for all $x \leqslant \bar{R}-1$. However, level l in the $(n-1)$-cube corresponds to level $l+1$ in the original cube, which has an additional codeword at or below level $n-\bar{R}$. Therefore, $\mathscr{C}$ has at least x codewords with weight $< n-\bar{R}+x$ for each x with $0 \leqslant x \leqslant \bar{R}$. Taking $x = \bar{R}$ gives us the desired lower bound, and combining this with Lemma 11 yields $K^+(n, n-\bar{R}) = \bar{R}+1$ for $n \geqslant n_{\bar{R}}$. It remains to show that $K^+(n, n-\bar{R}) > \bar{R}+1$ for $n < n_{\bar{R}}$.

To that end, suppose $n < n_{\bar{R}}$. Since the number of codewords below level $n-\bar{R}+x$ (or, having at least $(\bar{R}-x)$ 0's) is at least x, a minimal code $\mathscr{C}$ achieving $K^+(n, n-\bar{R})$ has at least $\sum_{x=0}^{\bar{R}} (\bar{R}-x) = n_{\bar{R}}$ total 0's in its codewords. Since $n < n_{\bar{R}}$, two of the codewords must have 0's in a common position. If we contract $\mathscr{C}$ at that coordinate, the resulting code is at least 2 smaller than the original one, and so $K^+(n, n-\bar{R}) \geqslant K^+(n-1, n-\bar{R}) + 2 \geqslant (\bar{R}-1) + 1 + 2 = \bar{R} + 2$. ∎

By combining this theorem with the direct sum construction, we can bound $K^+(n, R)$ from above for a wide range of parameters.

Theorem 14. *For any nonnegative n and $\bar{R}$, $K^+(n, n-\bar{R}) \leqslant (2n/\bar{R})^{\lceil \bar{R}^2/(2n-\bar{R}) \rceil}$.*

Proof. Note that by the direct sum construction, for any $0 \leqslant n \leqslant n'$ and $0 \leqslant R \leqslant R'$, we have

$$K^+(n, R) \leqslant K^+(n, R) K^+(n'-n, R'-R) \leqslant K^+(n', R'),$$

so that $K^+(n, R)$ is nondecreasing in both parameters. Therefore, applying the direct sum construction again for any integer $M > 0$,

$$\begin{aligned} K^+(n, n-\bar{R}) &\leqslant K^+(M\lceil n/M \rceil, M(\lceil n/M \rceil - \lfloor \bar{R}/M \rfloor)) \\ &\leqslant K^+(\lceil n/M \rceil, \lceil n/M \rceil - \lfloor \bar{R}/M \rfloor)^M. \end{aligned}$$

If we choose $M \geqslant \bar{R}^2/(2n-\bar{R})$, then it is straightforward to see that

$$\left\lceil \frac{n}{M} \right\rceil \geqslant \frac{n}{M} \geqslant \frac{\bar{R}}{2M}\left(\frac{\bar{R}}{M}+1\right) \geqslant \frac{1}{2}\left\lfloor \frac{\bar{R}}{M} \right\rfloor \left(\left\lfloor \frac{\bar{R}}{M} \right\rfloor + 1\right) = n_{\lfloor \bar{R}/M \rfloor}.$$

Therefore, Theorem 13 applies when $M = \lceil \bar{R}^2/(2n-\bar{R}) \rceil$, and we have

$$\begin{aligned} K^+(n, n-\bar{R}) &\leqslant K^+(\lceil n/M \rceil, \lceil n/M \rceil - \lfloor \bar{R}/M \rfloor)^M \\ &= \left(\left\lfloor \frac{\bar{R}}{M} \right\rfloor + 1\right)^M \leqslant (2n/\bar{R})^{\lceil \bar{R}^2/(2n-\bar{R}) \rceil}. \end{aligned}$$ ∎

We get the following corollary by letting $\bar{R} = (1-\lambda)n$.

Corollary 15. *For any λ with $0 \leqslant \lambda < 1$ and λn integral,*

$$K^+(n, \lambda n) \leqslant \left(\frac{2}{1-\lambda}\right)^{\lceil n(1-\lambda)^2/(1+\lambda) \rceil}.$$

For each λ, this gives an exponential upper bound on $K^+(n, \lambda n)$. For example, when $\lambda = 1/2$, we have $K^+(n, n/2) \leqslant 4^{\lceil n/6 \rceil} < 1.26^{n+5}$.

3. DIFFERENCE BOUNDS

In the discussion of asymptotic behavior above, we repeatedly used the fact that $K^+(n,R)$ increases as n increases or R decreases. In fact, a cursory examination of the table included at the end of this paper reveals that, at least above the diagonal, the increase from entry to adjacent entry (i.e., to the right or upward) is strict, and grows with increasing n and decreasing R. Here, we examine these "difference" patterns in more detail, by considering the number of 0's or 1's in minimal codes.

PROPOSITION 16. *Let $\phi(n,R)$ be the maximum total number of 0's in a minimal $(n,R)^+$-code, and let $\bar{\phi}(n,R)$ be the minimum number of 1's in a minimal $(n,R)^+$-code. Furthermore, assume that $R \leqslant n$. Then we have the following*:

(1) $K^+(n,R) - K^+(n-1,R) \geqslant \phi(n,R)/n$,

(2) $K^+(n-1,R) \leqslant \bar{\phi}(n,R)/n$,

(3) $K^+(n,R) < K^+(n+1,R)$, *and*

(4) $K^+(n,R) > K^+(n,R+1)$.

Proof. (1) The proof is similar to that of Theorem 13. Let $\mathscr{C}$ be a minimal $(n,R)^+$-code. Then the codewords of $\mathscr{C}$ contain at least $\phi(n,R)$ 0's, and we may choose a coordinate i at which at least $\phi(n,R)/n$ codewords of $\mathscr{C}$ have a 0. The contraction $\mathscr{C}^i$ has at most $K^+(n,R) - \phi(n,R)/n$ codewords, and downward R-covers Q_{n-1} by Lemma 12. Condition (1) follows since $K^+(n-1,R) \leqslant |\mathscr{C}^i|$.

(2) Let $\mathscr{C}$ be a minimal (n,R)-code achieving $\bar{\phi}(n,R)$, and thus achieving $\phi(n,R)$, since $\bar{\phi}(n,R) = nK^+(n,R) - \phi(n,R)$. Let a_l be the number of codewords of $\mathscr{C}$ at level l. Then by part (1) we have

$$\begin{aligned} K^+(n,R) - K^+(n-1,R) &\geqslant \frac{1}{n}\sum_{l=0}^{n}(n-l)a_l \\ &= K^+(n,R) - \frac{1}{n}\sum_{l=0}^{n} l a_l, \end{aligned}$$

and so

$$K^+(n-1,R) \leqslant \frac{1}{n}\sum_{l=0}^{n} l a_l = \bar{\phi}(n,R)/n.$$

(3) If $R \leqslant n$, then any $(n+1,R)^+$-code has at least two codewords in it. It must therefore contain a vector other than $\hat{1}$, so that

$$\phi(n+1,R) \geqslant 1,$$

and applying part (1) gives the desired result.

(4) Applying the direct sum bound (2),

$$\begin{aligned} K^+(n, R+1) &\leqslant K^+(n-1, R)K^+(1,1) \\ &= K^+(n-1, R) \\ &< K^+(n, R). \quad \blacksquare \end{aligned} \tag{7}$$

In order to get more out of Proposition 16.1 than a difference of 1, we must more carefully analyze the number of 0's in a code. A trivial lower bound is obtained by noting that there are at most $\binom{n}{j}$ codewords with j 0's. A much better lower bound is obtained by modifying the objective function in Proposition 5 to count the total number of 0's in the code, as follows.

PROPOSITION 17. *Let $IP^+_\phi(n, R)$ be the result of the integer program in Proposition* 5 *with objective function $\sum_{l=0}^n a_l$ replaced by $\sum_{l=0}^n (n-l)a_l$. Then for any $n, R \geqslant 1$, $\phi(n, R) \geqslant IP^+_\phi(n, R)$.*

4. LINEAR ASYMMETRIC CODES

Up to this point, we have been considering general asymmetric codes. However, a large portion of what is known about the symmetric case concerns linear codes, so it is natural to ask what can be said about asymmetric linear codes. For example, for a fixed radius, symmetric linear codes are asymptotically just as efficient at covering the cube as nonlinear ones (up to a multiplicative constant). The same statement is decidedly false, however, in the asymmetric case. We will need some definitions before we proceed with our results.

Let $\bar{\mathscr{C}}$, the 1'*s complement* of $\mathscr{C}$, be the set $\{\hat{1} - x \mid x \in \mathscr{C}\}$. We say that an $(n, R)^+$-code $\mathscr{C}$ is a *downward-asymmetric linear covering code of radius R* (for short, an $[n, R]^+$-code) if it is a vector subspace of $\mathbb{F}_2^n$, and $\mathscr{C}$ is an *upward-asymmetric linear covering code of radius R* (for short, an $[n, R]^-$-code) if its 1's complement is an $[n, R]^+$-code. Define $k^+[n, R]$ to be the dimension of the smallest $[n, R]^+$-code, and $k^-[n, R]$ to be the dimension of the smallest $[n, R]^-$-code. In contrast with the nonlinear case, we actually need to distinguish upward and downward codes, as will become apparent shortly.

Call a code $\mathscr{C}$ *self-complementary* if $\mathscr{C} = \bar{\mathscr{C}}$, and define $k^\pm[n, R]$ to be the minimal dimension of a self-complementary asymmetric linear code (for short, an $[n, R]^\pm$-code). We do not need to specify "upward" or "downward" here, since a self-complementary code covers the cube in one direction iff it covers it in the other. Finally, for a code $\mathscr{C}$ and a coordinate i, define the *shortening* $\mathscr{C}_i \subset Q_{n-1}$ of $\mathscr{C}$ to be the set of points of $\mathscr{C}$ with a "0" at position i, projected into Q_{n-1} by deletion of that bit. Thus C_i is the 1's complement of the contraction at i of the 1's complement of $\mathscr{C}$.

We begin with a lemma which says that the dimension of a downward-asymmetric linear covering code increases by at least 1 when n is incremented.

LEMMA 18. $k^-[n-1,R] \leqslant k^-[n,R]-1$, *for* $n > R$.

Proof. Let $\mathscr{C}$ be a minimal $[n,R]^-$-code. Since $n > R$, one R-ball cannot itself upward R-cover the entire n-cube. Therefore, $\mathscr{C}$ has at least two elements, and there exists a coordinate i where some vector $x \in \mathscr{C}$ has a 1. The shortening $\mathscr{C}_i$ of a linear code $\mathscr{C}$ is linear, and $|\mathscr{C}_i| < |C|$ gives that $\dim(\mathscr{C}_i) < \dim(\mathscr{C})$. ∎

The following theorem says exactly how large k^+, k^-, and $k^\pm$ are.

THEOREM 19. *For* $n > 0$, $k^+[n,R] = k^\pm[n,R] = k^-[n,R] = \max\{1, n-R\}$.

Proof. We begin with the first equality. Every $[n,R]^+$-code is an $(n,R)^+$-code, so it must contain $\hat{1}$. Containing $\hat{1}$ is equivalent to being self-complementary for linear codes, however, so every $[n,R]^+$-code is self-complementary. That every $[n,R]^\pm$-code is an $[n,R]^+$-code is trivial, and we have $k^+[n,R] = k^\pm[n,R]$.

Since every self-complementary asymmetric linear code is also an upward-asymmetric linear code, we have $k^-[n,R] \leqslant k^\pm[n,R]$. By induction using the previous lemma, we have $k^-[n,R] \geqslant k^-[R,R] + n - R = n - R$ for $n > R$. Furthermore, when $n \leqslant R$, $k^-[n,R] = 0$. Thus, for any $n > 0$, $k^\pm[n,R] \geqslant k^-[n,R] \geqslant \max\{1, n-R\}$, since all downward-directed codes include $\hat{1}$.

To complete the proof, it suffices to find an $[n,R]^\pm$-code $\mathscr{A}(n,R)$ of dimension $\max\{1, n-R\}$. We construct one inductively. For $n \leqslant R+1$, let $\mathscr{A}(n,R) = \{\hat{0}, \hat{1}\}$. For larger n, let $\mathscr{A}(n,R)$ be the $[n,R]^\pm$-code $\mathscr{A}(n-1,R) \oplus \{0,1\}$. ∎

5. CONCLUSION

Open questions abound concerning asymmetric covering codes, since the entirety of the theory of symmetric covering codes could be reexamined in the asymmetric case. However, several questions stand out as particularly interesting.

It remains to determine the asymptotic order of magnitude of $K^+(n,R)$ when neither R nor $\bar{R}$ is constant (e.g., R is linear in n). Additionally, the analysis above concerned only the case of binary codes. It seems a natural next step to investigate asymmetric covering codes on more symbols than two. Perhaps, an interesting way to define the notion of R-balls in that case would be to take the set of vectors in $\mathbb{Z}_a^n$ which differ from a given vector by *increasing* at most R of its coordinates. Or, maybe what should be asked for is that the sum of the "increases" in each coordinate add up to at most R. In fact, one could imagine asking similar questions of much more general classes of posets: geometric lattices, Cartesian products of some base set of posets, etc. Furthermore, the definition of R-ball used here certainly is not the only imaginable one. Perhaps, it would interesting to look at sets which permit R_1 changes from 0's to 1's and R_2 changes from 1's to 0's, or which permit $\alpha \cdot w(x)$ (asymmetric or symmetric) changes to x for some $\alpha \in [0,1)$. Clearly, there is a lot of room for generalization.

The questions about classification of codes that arise in the context of symmetric codes are relevant here as well. What possible forms do $[n,R]^{\pm}$-codes take? Can anything be said about how *many* minimal $(n,R)^+$-codes there are? How close to perfect—i.e., no overlap between R-balls centered at codewords—can an $(n,R)^+$-code be? Since linear codes, which provide easily computable examples of efficient symmetric covering codes, are so far from the sphere-covering lower bound in the asymmetric case, does there exist a family of asymmetric codes which are polynomial-time computable (in n) and which are within a constant of optimal?

One important concrete problem stands: to find better upper and lower bounds on $K^+(n,R)$ for small n and R. Table 1 demonstrates our best-known bounds, to be interpreted as follows. All entries weakly to the left or weakly below a subscript of "d" are determined by Theorem 13. A subscript of "i" denotes a lower bound found by the integer program in Proposition 5. An "e" means an explicit code was found exhaustively. The subscript "m" indicates that Proposition 17, with the integer program modified by an extra combinatorial constraint, was used to compute a lower bound for $\phi(n,R)$, and then a lower bound for $K^+(n,R)$ was found with Proposition 16(1). An "s" means the upper bound is from a direct sum of codes of the type in (2). In particular, $K^+(10,4) \leqslant K^+(5,2)$ $K^+(5,2)$. Otherwise, no subscript on the left means the lower bound was found using Proposition 16(1) with $\phi(n,R)$ bounded below by Proposition 17, and no subscript on the right means the upper bound corresponds to a code found greedily. We note that Applegate *et al.* [2] already claim the improvements $K^+(7,1) = 31$, $K^+(8,1) = 58$, $K^+(9,1) \leqslant 106$, $K^+(10,1) \leqslant 196$, $K^+(11,1) \leqslant 352$ and $K^+(12,1) \leqslant 670$.

TABLE 1
Best-Known Bounds for $K^+(n, R)$

$R\backslash n$	2	3	4	5	6	7
1	2	3_d	${}_i6_e$	10_e	${}_m18_e$	30–34
2	1	2	3_d	5_e	${}_m8_e$	$13–15_e$
3	1	1	2	3	4_d	${}_i6–7$
4	1	1	1	2	3	4_d
5	1	1	1	1	2	3
6	1	1	1	1	1	2

$R\backslash n$	8	9	10	11	12	13
1	52–67	93–121	162–229	306–433	563–813	$1046–1626_s$
2	20–25	32–46	52–81	87–141	148–262	$254–524_s$
3	${}_i9–13$	${}_i14–21$	22–36	34–64	54–105	88–210
4	6	8–11	$12–16_s$	17–30	26–49	40–83
5	4_d	6	8–9	11–16	15–27	22–48
6	3	4	5_d	7–8	10–15	14–23
7	2	3	4	5_d	7_e	9–12
8	1	2	3	4	5_d	7
9	1	1	2	3	4	5_d
10	1	1	1	2	3	4
11	1	1	1	1	2	3

REFERENCES

1. N. Alon and J. H. Spencer, "The Probabilistic Method," John Wiley & Sons, Inc., New York, 2000.
2. D. Applegate, E. Rains, and N. Sloane, On asymmetric coverings and covering numbers, preprint.
3. J. Bell, Private communication.
4. R. Brualdi, S. Litsyn, and V. Pless, Covering Radius, "Handbook of Coding Theory," Vols. I, II, pp. 755–826, North-Holland, Amsterdam, 1998.
5. G. Cohen, M. Karpovsky, H. Mattson, and J. Schatz, Covering radius—survey and recent results, *IEEE Trans. Inform. Theory* **31** (1985), 328–343.
6. G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, "Covering Codes," North-Holland Mathematical Library, Vol. 54, Elsevier, Amsterdam, 1997.
7. R. B. Ellis, A. B. Kahng, and Y. Zheng, Compression algorithms for "Dummy Fill" VLSI layout data, preprint.
8. R. Graham and N. Sloane, On the covering radius of codes, *IEEE Trans. Inform. Theory* **31** (1985), 385–401.
9. A. Lobstein, Rayon de Recouvrement: La Bibliographie, "*Manuscript*," http://perso.enst.fr/~lobstein/biblio.html.
10. T. R. N. Rao, "Error Coding for Arithmetic Processors," Academic Press, New York/London, 1974.

11. D. K. Ray-Chaudhuri, N. M. Singhi, S. Sanyal, and P. S. Subramanian, Theory and design of t-unidirectional error-correcting and $d(d \geqslant t)$-unidirectional error-detecting codes, *IEEE Trans. Comput.* **43** (1994), 1221–1226.
12. N. M. Singhi, I. Shriniwas, and T. A. Anthony, Combinatorial techniques and objects in computer science: Fault-tolerance and other interesting applications, *European J. Combin.* **17** (1996), 97–111.